ATLASSIAN

Atlassian Customer Agreement

Effective starting: October 15, 2024

This Agreement is between Customer and Atlassian. "**Customer**" means the entity on behalf of which this Agreement is accepted or, if that does not apply, the individual accepting this Agreement. "**Atlassian**" means the Atlassian entity that owns or operates the Products that Customer uses or accesses listed in the Atlassian Product-specific Terms attached hereto as Exhibit E and available at https://www.atlassian.com/legal/product-terms .

If you (the person accepting this Agreement) are accepting this Agreement on behalf of your employer or another entity, you agree that: (i) you have full legal authority to bind your employer or such entity to this Agreement, and (ii) you agree to this Agreement on behalf of your employer or such entity.

If you are accepting this Agreement using an email address from your employer or another entity, then: (i) you will be deemed to represent that party, (ii) your acceptance of this Agreement will bind your employer or that entity to these terms, and (iii) the word "you" or "Customer" in this Agreement will refer to your employer or that entity.

By executing a written order forthe Products, you confirm you are bound by this Agreement. If you do not wish to be bound by this Agreement, do not click "Agree" (or similar button or checkbox), download the Products, or use or access the Products.

1. Overview. This Agreement applies to Customer's Orders for Products and related Support and Advisory Services. The terms of this Agreement apply to both Cloud Products and Software Products, although certain terms apply only to Cloud Products or Software Products, as specified below. In addition, some Products are subject to additional Product-Specific Terms, and Support and Advisory Services are subject to the applicable Policies.

2. Use of Products.

2.1. Permitted Use. Subject to this Agreement and during the applicable Subscription Term, Atlassian grants Customer a non-exclusive, worldwide right to use the Products and related Support and Advisory Services for its and its Affiliates' internal business purposes, in accordance with the Documentation and subject to Customer's Scope of Use, as specified in the Order and the Product-Specific Terms.

2.2. Restrictions. Except to the extent otherwise expressly permitted by this Agreement, Customer must not (and must not permit anyone else to): (a) rent, lease, sell, distribute or sublicense the Products or (except for Affiliates) include them in a service bureau or outsourcing offering, (b) provide access to the Products to a third party, other than to Users, (c) charge its customers a specific fee for use of the Products, but Customer may charge an overall fee for its own offerings (of which the Products are ancillary), (d) use the Products to develop a similar or competing product or service, (e) reverse engineer, decompile, disassemble or seek to access the source code or non-public APIs to the Products, (f) modify or create derivative works of the Products, (g) interfere with or circumvent Product usage limits or Scope of Use restrictions, (h) remove, obscure or modify in any way any proprietary or other notices or attributions in the Products, or (i) violate the Acceptable Use Policy.

2.3. DPA. The DPA applies to Customer's use of Products and related Support and Advisory Services and forms part of this Agreement.

3. Users.

3.1. Responsibility. Customer may authorize Users to access and use the Products, in accordance with the Documentation and Customer's Scope of Use. Customer is responsible for its Users' compliance with this Agreement and all activities of its Users, including Orders they may place, apps and Third Party-Products enabled, and how Users access and use Customer Data.

3.2. Login Credentials. Customer must ensure that each User keeps its login credentials confidential and must promptly notify Atlassian if it becomes aware of any unauthorized access to any User login credentials or other unauthorized access to or use of the Products.

3.3. Domain Ownership. Where a Cloud Product requires Customer to specify a domain (such as www.example.com) for the Cloud Product's or a feature's operation, Atlassian may verify that Customer or an Affiliate owns or controls that domain. Atlassian has no obligation to provide that Cloud Product or feature if Atlassian cannot verify that Customer or an Affiliate owns or controls the domain. Product administrators appointed by Customer may also take over management of accounts previously registered using an email address belonging to Customer's domain, which become "managed accounts" (or similar term), as described in the Documentation.

3.4. Age Requirements. The Products are not intended for use by anyone under the age of 16. Customer is responsible for ensuring that all Users are at least 16 years old.

4. Cloud Products. This Section 4 only applies to Cloud Products.

4.1. Customer Data. Atlassian may process Customer Data to provide the Cloud Products and related Support or Advisory Services in accordance with this Agreement.

4.2. Security Program. Atlassian has implemented and will maintain an information security program that uses appropriate physical, technical and organizational measures designed to protect Customer Data from unauthorized access, destruction, use, modification or disclosure, as described in its Security Measures. Atlassian will also maintain a compliance program that includes independent third-party audits and certifications, as described in its Security Measures. Further information about Atlassian's security program is available on the Atlassian Trust Center at https://www.atlassian.com/trust, as updated from time to time.

4.3. Service Levels. Where applicable, service level commitments for the Cloud Products are set out in the Service Level Agreement.

4.4. Data Retrieval. The Documentation describes how Customer may retrieve its Customer Data from the Cloud Products.

4.5. Removals and Suspension. Atlassian has no obligation to monitor Customer Data. Nonetheless, if Atlassian becomes aware that: (a) Customer Data may violate Law, Section 2.2 (Restrictions), or the rights of others (including relating to a takedown request received following the guidelines for Reporting Copyright and Trademark Violations at https://www.atlassian.com/legal/copyright-and-trademark-violations), or (b) Customer's use of the Cloud Products threatens the security or operation of the Cloud Products, then Atlassian may: (i) limit access to, or remove, the relevant Customer Data, or (ii) temporarily suspend Customer's or any User's access to the relevant Cloud Products. Atlassian may also take any such measures where required by Law, or at the request of a governmental authority. When practicable, Atlassian will give Customer the opportunity to remedy the issue before taking any such measures.

5. Software Products. This Section 5 only applies to Software Products.

5.1. Modifications. Atlassian may provide some portions of the Software Products in source code form for Customer to use internally to create bug fixes, configurations or other modifications of the Software Products, as permitted in the Documentation ("**Modifications**"). Customer must keep such source code secure (on computer devices and online repositories controlled by Customer), confidential, and only make it available to Customer's employees who have a legitimate need to access and use the source code to create and maintain Modifications. Customer may only use Modifications with the Software Products, and only in accordance with this Agreement, including the Third-Party Code Policy, the Documentation, and Customer's Scope of Use. Customer must not distribute source code or Modifications to third parties. Customer must securely destroy the source code at the earliest of: (a) Customer no longer needing to use source code to create or maintain Modifications, (b) termination or non-renewal of a relevant Subscription Term, or (c) Atlassian's request for any reason. Notwithstanding anything else in this Agreement, Atlassian has no support, warranty, indemnity or other responsibility for Modifications.

5.2. License Verification. Upon Atlassian's written request, Customer will promptly confirm in writing whether its use of the Software Products is in compliance with the applicable Scope of Use. Atlassian or its authorized agents may subject to Government security requirements audit Customer's use of the Software Products no more than once every twelve (12) months to confirm compliance with Customer's Scope of Use, provided Atlassian gives Customer reasonable advance notice and uses reasonable efforts to minimize disruption to Customer. If Customer exceeds its Scope of Use, Atlassian may invoice for that excess use, and Customer will pay Atlassian promptly after invoice receipt.

5.3. Number of Instances. Unless otherwise specified in the Order or the Product-Specific Terms, Customer may install up to one (1) production instance of each Software Product included in an Order on systems owned or operated by Customer or its Users.

6. Customer Obligations.

6.1. Disclosures and Rights. Customer must ensure it has made all disclosures and obtained all rights and consents necessary for Atlassian to use Customer Data and Customer Materials to provide the Cloud Products, Support or Advisory Services.

6.2. Product Assessment. Customer is responsible for determining whether the Products meet Customer's requirements and any regulatory obligations related to its intended use.

6.3. Sensitive Health Information and HIPAA. Unless the parties have entered into a 'Business Associate Agreement,' Customer must not (and must not permit anyone else to) upload to the Cloud Products (or use the Cloud Products to process) any patient, medical or other protected health information regulated by the Health Insurance Portability and Accountability Act.

7. Third-Party Code and Third-Party Products.

7.1. Third-Party Code. This Agreement and the Third-Party Code Policy apply to open source software and commercial third-party software Atlassian includes in the Products.

7.2. Third-Party Products. Customer may choose to use the Products with third-party platforms, apps, add-ons, services or products, including offerings made available through the Atlassian Marketplace ("**Third-Party Products**"). Use of such Third-Party Products with the Products may require access to Customer Data and other data by the third-party provider, which, for Cloud Products Atlassian will permit on Customer's behalf if Customer has enabled that Third-Party Product. Customer's use of Third-Party Products is subject to the relevant provider's terms of use, not this Agreement. Atlassian does not control and has no liability for Third-Party Products.

8. Support and Advisory Services. Atlassian will provide Support and Advisory Services as described in the Order and applicable Policies. Atlassian's provision of Support or Advisory Services is subject to Customer providing timely access to Customer Materials and personnel reasonably requested by Atlassian.

9. Ordering Process and Delivery. No Order is binding until Atlassian provides its acceptance, including by sending a confirmation email, providing access to the Products, or making license or access keys available to Customer. No terms of any purchase order or other business form used by Customer will supersede, supplement, or otherwise apply to this Agreement or Atlassian. Atlassian will deliver login instructions or license keys for Products electronically, to Customer's account (or through other reasonable means) promptly upon receiving payment of the fees. Customer is responsible for the installation of Software Products, and Atlassian has no further delivery obligations with respect to the Software Products after delivery of license keys.

10. Billing and Payment.

10.1. Fees.

(a) Direct Purchases. If Customer purchases directly from Atlassian, fees and any payment terms are specified in Customer's Order with Atlassian.

(b) Resellers. If Customer purchases through a Reseller, Customer must pay all applicable amounts directly to the Reseller, and Customer's order details (e.g., Products and Scope of Use) will be specified in the Order placed by the Reseller with Atlassian on Customer's behalf.

(c) Renewals. Unless otherwise specified in an Order and subject to the Product, Support or Advisory Services continuing to be generally available, a Subscription Term may be renewed at Atlassian's then current GSA Schedule rates for: (i) if Customer's prior Subscription was for a period less than twelve (12) months, another Subscription Term of a period equal to Customer's prior Subscription Term, or (ii) if Customer's prior Subscription Team was for twelve (12) months or more, twelve (12) months.

(d) Increased Scope of Use. If Customer exceeds the Scope of Use purchased, unless otherwise agreed with Atlassian in writing, Customer must upgrade its subscription or pay for the increased Scope of Use. Unless otherwise specified in an applicable Order, Atlassian will charge Customer for any increased Scope of Use at Atlassian's then-current rates, which may be prorated for the remainder of the then-current Subscription Term.

(e) Refunds. All fees and expenses are non-refundable, except as otherwise provided in this Agreement. For any purchases Customer makes through a Reseller, any refunds from Atlassian payable to Customer relating to that purchase will be remitted by that Reseller, unless Atlassian specifically notifies Customer otherwise at the time of refund.

(f) Credit Cards. If Customer uses a credit card or similar online payment method for its initial Order, then Atlassian may bill that payment method for renewals, additional Orders, overages to scopes of use, expenses, and unpaid fees, as applicable.

10.2. Taxes.

(a) Taxes Generally. (Reserved).

(b) Withholding Taxes. To the extent Customer is required to withhold tax from payment to Atlassian in certain jurisdictions, Customer must provide valid documentation it receives from the taxing authority in such jurisdictions confirming remittance of withholding. This documentation must be provided at the time of payment of the applicable invoice to Atlassian.

(c) Exemptions. If Customer claims exemption from any sales tax, VAT, GST or similar taxes under this Agreement, Customer must provide Atlassian a valid tax exemption certificate or tax ID at the time of Order, and after receipt of valid evidence of exemption, Atlassian will not include applicable taxes on the relevant Customer invoice.

10.3. Return Policy. Within thirty (30) days of its initial Order for a Product, Customer may terminate the Subscription Term for that Product, for any or no reason, by providing notice to Atlassian. Following such termination, upon request (which may be made through Customer's Atlassian account), Atlassian will refund Customer the amount paid for that Product and any associated Support under the applicable Order. Unless otherwise specified in the Policies or Product-Specific Terms, this return policy does not apply to Advisory Services.

10.4. Reserved.

11. Atlassian Warranties.

11.1. Performance Warranties. Atlassian warrants to Customer that: (a) the Products will operate in substantial conformity with the applicable Documentation during the applicable Subscription Term, (b) Atlassian will not materially decrease the functionality or overall security of the Products during the applicable Subscription Term, and (c) Atlassian will use reasonable efforts designed to ensure that the Products, when and as provided by Atlassian, are free of any viruses, malware or similar malicious code (each, a "**Performance Warranty**").

11.2. Performance Warranty Remedy. If Atlassian breaches a Performance Warranty and Customer makes a reasonably detailed warranty claim within 30 days of discovering the issue, Atlassian will use reasonable efforts to correct the non-conformity. If Atlassian determines such remedy to be impracticable, either party may terminate the affected Subscription Term. Atlassian will then refund to Customer any pre-paid, unused fees for the terminated portion of the Subscription Term. These procedures are Customer's exclusive remedy and Atlassian's entire liability for breach of a Performance Warranty.

11.3. Exclusions. The warranties in this Section 11 (Atlassian Warranties) do not apply to: (a) the extent the issue or non-conformity is caused by Customer's unauthorized use or modification of the Products, (b) unsupported releases of Software Products or Cloud Clients, or (c) Third-Party Products.

11.4. Disclaimers. **Except as expressly provided in this Section 11 (Atlassian Warranties), the Products, Support and Advisory Services and all related Atlassian services and deliverables are provided "AS IS." Atlassian makes no other warranties, whether express, implied, statutory or otherwise, including warranties of merchantability, fitness for a particular purpose, title or non-infringement. Atlassian does not warrant that Customer's use of the Products will be uninterrupted or error-free. Atlassian is not liable for delays, failures or problems inherent in use of the internet and electronic communications or other systems outside Atlassian's control.**

12. Term and Termination.

12.1. Term. This Agreement commences on the date Customer accepts it and expires when all Subscription Terms have ended.

12.2. Termination for Convenience. Customer may terminate this Agreement or a Subscription Term upon notice for any reason. Subject to Section 10.3 (Return Policy), Customer will not be entitled to any refunds for Services provided as a result of exercising its rights under this Section 12.2, and any unpaid amounts for the then-current Subscription Terms and any related service periods will become due and payable immediately upon such termination.

12.3. Termination for Cause. 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, Atlassian 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.

12.4. Effect of Termination. Upon expiration or termination of this Agreement or a Subscription Term: (a) Customer's rights to use the applicable Products, Support or Advisory Services will cease, (b) Customer must immediately cease accessing the Cloud Products and using the applicable Software Products and Cloud Clients, and (c) Customer must delete (or, on request, return) all license keys, access keys and any Product copies. Following expiration or termination, unless prohibited by Law, Atlassian will delete Customer Data in accordance with the Documentation.

12.5. Survival. These Sections survive expiration or termination of this Agreement: 2.2 (Restrictions), 4.2 (Security Program), 10.1 (Fees), 10.2 (Taxes), 11.4 (Disclaimers), 12.4 (Effect of Termination), 12.5 (Survival), 13 (Ownership), 14 (Limitations of Liability), 15 (Indemnification by Atlassian), 16 (Confidentiality), 17.4 (Disclaimer), 18 (Feedback), 20 (General Terms) and 21 (Definitions).

13. Ownership. Except as expressly set out in this Agreement, neither party grants the other any rights or licenses to its intellectual property under this Agreement. As between the parties, Customer owns all intellectual property and other rights in Customer Data and Customer Materials provided to Atlassian or used with the Products. Atlassian and its licensors retain all intellectual property and other rights in the Products, any Support and Advisory Services deliverables and related source code, Atlassian technology, templates, formats and dashboards, including any modifications or improvements.

14. Limitations of Liability.

14.1. Damages Waiver. **Except for Excluded Claims or Special Claims, to the maximum extent permitted by Law, neither party will have any liability arising out of or related to this Agreement for any loss of use, lost data, lost profits, interruption of business or any indirect, special, incidental, reliance or consequential damages of any kind, even if informed of their possibility in advance.**

14.2. General Liability Cap. **Except for Excluded Claims or Special Claims, to the maximum extent permitted by Law, each party's entire liability arising out of or related to this Agreement will not exceed in aggregate the amounts paid to Atlassian for the Products, Support and Advisory Services giving rise to the liability during the twelve (12) months preceding the first event out of which the liability arose. Customer's payment obligations under Sections 10.1 (Fees) and 10.2 (Taxes) are not limited by this Section 14.2.**

14.3. Excluded Claims. "**Excluded Claims**" means: (a) Customer's breach of Section 2.2 (Restrictions) or Section 6 (Customer Obligations), (b) either party's breach of Section 16 (Confidentiality) but excluding claims relating to Customer Data or Customer Materials, or (c) amounts payable to third parties under Atlassian's obligations in Section 15 (Indemnification by Atlassian). The foregoing limitation of liability shall not apply to fraud.

14.4. Special Claims. For Special Claims, Atlassian's aggregate liability under this Agreement will be the lesser of: (a) two times (2x) the amounts paid to Atlassian for the Products, Support and Advisory Services giving rise to the Special Claim during the twelve (12) months preceding the first event out of which the Special Claim arose, and (b) US$5,000,000. "**Special Claims**" means any unauthorized disclosure of Customer Data or Customer Materials caused by a breach by Atlassian of its obligations in Section 4.2 (Security Program).

14.5. Nature of Claims and Failure of Essential Purpose. The exclusions and limitations in this Section 14 (Limitations of Liability) apply regardless of the form of action, whether in contract, tort (including negligence), strict liability or otherwise and will survive and apply even if any limited remedy in this Agreement fails of its essential purpose.

15. Indemnification by Atlassian.

15.1. IP Indemnification. Atlassian must: (a) have the right to intervene to defend Customer from and against any third-party claim to the extent alleging that the Products, when used by Customer as authorized by this Agreement, infringe any intellectual property right of a third party (an "**Infringement Claim**"), and (b) indemnify and hold harmless Customer against any damages, fines or costs finally awarded by a court of competent jurisdiction (including reasonable attorneys' fees) or agreed in settlement by Atlassian resulting from an Infringement Claim. 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.

15.2. Procedures. Atlassian's obligations in Section 15.1 (IP Indemnification) are subject to Customer providing: (a) sufficient notice of the Infringement Claim so as to not prejudice Atlassian's defense of the Infringement Claim, (b) the exclusive right to control and direct the investigation, defense and settlement of the Infringement Claim, and (c) all reasonably requested cooperation, at Atlassian's expense for reasonable out-of-pocket expenses. Customer may participate in the defense of an Infringement Claim with its own counsel at its own expense.

15.3. Settlement. Atlassian may not settle an Infringement Claim without Customer's prior written consent if settlement would require Customer to admit fault or take or refrain from taking any action (other than relating to use of the Products).

15.4. Mitigation. In response to an actual or potential Infringement Claim, Atlassian may, at its option: (a) procure rights for Customer's continued use of the Products, (b) replace or modify the alleged infringing portion of the Products without reducing the overall functionality of the Products, or (c) terminate the affected Subscription Term and refund to Customer any pre-paid, unused fees for the terminated portion of the Subscription Term.

15.5. Exceptions**.** Atlassian's obligations in this Section 15 (Indemnification by Atlassian) do not apply to the extent an Infringement Claim arises from: (a) Customer's modification or unauthorized use of the Products, (b) use of the Products in combination with items not provided by Atlassian (including Third-Party Products), (c) any unsupported release of the Software Products or Cloud Clients, or (d) Third-Party Products, Customer Data or Customer Materials.

15.6. Exclusive Remedy. **This Section 15 (Indemnification by Atlassian) sets out Customer's exclusive remedy and Atlassian's entire liability regarding infringement of third-party intellectual property rights.**

16. Confidentiality.

16.1. Definition. "**Confidential Information**" means information disclosed by one party to the other under or in connection with this Agreement that: (a) is designated by the disclosing party as proprietary or confidential, or (b) should be reasonably understood to be proprietary or confidential due to its nature and the circumstances of its disclosure. Atlassian's Confidential Information includes any source code and technical or performance information about the Products. Customer's Confidential Information includes Customer Data and Customer Materials.

16.2. Obligations. Unless expressly permitted by the disclosing party in writing, the receiving party must: (a) hold the disclosing party's Confidential Information in confidence and not disclose it to third parties except as permitted in this Agreement, and (b) only use such Confidential Information to fulfill its obligations and exercise its rights in this Agreement. The receiving party may disclose such Confidential Information to its employees, agents, contractors and other representatives having a legitimate need to know (including, for Atlassian, the subcontractors referenced in Section 20.11 (Subcontractors and Affiliates)), provided the receiving party remains responsible for their compliance with this Section 16 (Confidentiality) and they are bound to confidentiality obligations no less protective than this Section 16 (Confidentiality).

16.3. Exclusions. These confidentiality obligations do not apply to information that the receiving party can demonstrate: (a) is or becomes publicly available through no fault of the receiving party, (b) it knew or possessed prior to receipt under this Agreement without breach of confidentiality obligations, (c) it received from a third party without breach of confidentiality obligations, or (d) it independently developed without using the disclosing party's Confidential Information. The receiving party may disclose Confidential Information if required by Law, subpoena or court order, provided (if permitted by Law) it notifies the disclosing party in advance and cooperates, at the disclosing party's cost, in any reasonable effort to obtain confidential treatment. Atlassian recognizes that Federal agencies are subject to the Freedom of Information Act, 5 U.S.C. 552, which may require that certain information be released, despite being characterized as "confidential" by the vendor, but under no circumstances will any Federal agency disclose Atlassian's source code without prior written consent by Atlassian.

16.4. Remedies. Unauthorized use or disclosure of Confidential Information may cause substantial harm for which damages alone are an insufficient remedy. Each party may seek appropriate equitable relief, in addition to other available remedies, for breach or anticipated breach of this Section 16 (Confidentiality).

17. Free or Beta Products.

17.1. Access. Customer may receive access to certain Products or Product features on a free, fully discounted or trial basis, or as an alpha, beta or early access offering ("**Free or Beta Products**"). Use of Free or Beta Products is subject to this Agreement and any additional terms specified by Atlassian, such as the applicable scope and term of use.

17.2. Termination or Modification. At any time, Atlassian may terminate or modify Customer's use of (including applicable terms) Free or Beta Products or modify Free or Beta Products, without any liability to Customer. For modifications to Free or Beta Products or Customer's use, Customer must accept those modifications to continue accessing or using the Free or Beta Products.

17.3. Pre GA. Free or Beta Products may be inoperable, incomplete or include errors and bugs or features that Atlassian may never release, and their features and performance information are Atlassian's Confidential Information.

17.4. Disclaimer. **Notwithstanding anything else in this Agreement, to the maximum extent permitted by Law, Atlassian provides no warranty, indemnity, service level agreement or support for Free or Beta Products and its aggregate liability for Free or Beta Products is limited to US$100.**

18. Feedback. If Customer provides Atlassian with feedback or suggestions regarding the Products or other Atlassian offerings, Atlassian may use the feedback or suggestions without restriction or obligation. Atlassian acknowledges that the ability to use this Agreement and any Feedback provided as a result of this Agreement in advertising is limited by GSAR 552.203-71.

19. Publicity. Atlassian may identify Customer as a customer of Atlassian in its promotional materials to the extent permitted by the General Services Acquisition Regulation (GSAR) 552.203-71. Atlassian will promptly stop doing so upon Customer request sent to sales@atlassian.com.

20. General Terms.

20.1. Compliance with Laws. Each party must comply with all Laws applicable to its business in its performance of obligations or exercise of rights under this Agreement.

20.2. Code of Conduct. Atlassian must comply with its Code of Conduct in its performance of obligations or exercise of rights under this Agreement.

20.3. Assignment.

(a) Customer may not assign or transfer any of its rights or obligations under this Agreement or an Order without Atlassian's prior written consent. However, Customer may assign this Agreement in its entirety (including all Orders) to its successor resulting from a merger, acquisition, or sale of all or substantially all of Customer's assets or voting securities, provided that Customer provides Atlassian with prompt

written notice of the assignment and the assignee agrees in writing to assume all of Customer's obligations under this Agreement and complies with Atlassian's procedural and documentation requirements to give effect to the assignment.

(b) Any attempt by Customer to transfer or assign this Agreement or an Order, except as expressly authorized above, will be null and void.

(c) Atlassian may assign its rights and obligations under this Agreement (in whole or in part) in accordance with the provisions set forth at FAR 42.1204.

20.4. Governing Law, Jurisdiction and Venue.

(a) This Agreement is governed by the Federal laws of the United States.

(b) This Agreement will be governed by such laws without regard to conflicts of laws provisions, and both parties submit to the personal jurisdiction of the applicable courts. The United Nations Convention on the International Sale of Goods does not apply to this Agreement.

20.5. Notices.

(a) Except as specified elsewhere in this Agreement, notices under this Agreement must be in writing and are deemed given on: (i) personal delivery, (ii) when received by the addressee if sent by a recognized overnight courier with receipt request, (iii) the third business day after mailing, or (iv) the first business day after sending by email, except that email will not be sufficient for notices regarding Infringement Claims, alleging breach of this Agreement by Atlassian, or of Customer's termination of this Agreement in accordance with Section 12.3 (Termination for Cause).

(b) Notices to Atlassian must be provided according to the details provided at https://www.atlassian.com/legal#how-do-i-provide-legal-notices-to-atlassian, as may be updated from time to time.

(c) Notices to Customer must be provided to the billing or technical contact provided to Atlassian, which may be updated by Customer from time to time in Customer's account portal. However, Atlassian may provide general or operational notices via email, on its website or through the Products. Customer may subscribe to receive email notice of updates to this Agreement, as described at https://www.atlassian.com/legal#notification-of-updates-in-terms-and-policies.

20.6. Entire Agreement. This Agreement is the parties' entire agreement regarding its subject matter and supersedes any prior or contemporaneous agreements regarding its subject matter. In the event of a conflict among the documents making up this Agreement, the main body of this Agreement (i.e., Sections 1 through 21, inclusive) will control, except that the Policies, Product-Specific Terms and DPA will control for their specific subject matter.

20.7. Other Atlassian Offerings. Atlassian makes available other offerings that can be used with the Products which, in some cases, are subject to separate terms and conditions, available at https://www.atlassian.com/legal. These other offerings include training services, developer tools and the Atlassian Marketplace. For clarity, this Agreement controls over any such terms and conditions with respect to Customer's use of the Products (including any Atlassian Apps).

20.8. Interpretation, Waivers and Severability. In this Agreement, headings are for convenience only and "including" and similar terms are to be construed without limitation. Waivers must be granted in writing and signed by the waiving party's authorized representative. If any provision of this Agreement is held invalid, illegal or unenforceable, it will be limited to the minimum extent necessary so the rest of this Agreement remains in effect.

20.9. Changes to this Agreement.

(a) Atlassian may modify this Agreement (which includes the Policies, Product-Specific Terms and DPA) from time to time, by posting the modified portion(s) of this Agreement on Atlassian's website. Atlassian must use commercially reasonable efforts to post any such modification at least thirty (30) days prior to its effective date.

(b) For free subscriptions, modifications become effective during the then current Subscription Term, in accordance with Atlassian's notice.

(c) For paid subscriptions:

(i) except as specified below, modifications to this Agreement will take effect at the next Order or renewal unless either party elects to not renew pursuant to Section 10.1(c) (Renewals), and

(ii) Atlassian may specify that modifications will become effective during a then-current Subscription Term if: (A) required to address compliance with Law, or (B) required to reflect updates to Product functionality or introduction of new Product features. If Customer objects, Customer may terminate the remainder of the then-current Subscription Term for the affected Products as its exclusive remedy. To exercise this right, Customer must notify Atlassian of its termination under this Section 20.9(c) within thirty (30) days of the modification notice, and Atlassian will refund any pre-paid fees for the terminated portion of the applicable Subscription Term.

20.10. Force Majeure. In accordance with GSAR Clause 552.212-4(f), neither party is liable for any delay or failure to perform any obligation under this Agreement (except for a failure to pay fees) due to events beyond its reasonable control and occurring without that party's fault or negligence.

20.11. Subcontractors and Affiliates. Atlassian may use subcontractors or its Affiliates in the performance of its obligations under this Agreement, but Atlassian remains responsible for its overall performance under this Agreement and for having appropriate written agreements in place with its subcontractors to enable Atlassian to meet its obligations under this Agreement.

20.12. Independent Contractors. The parties are independent contractors, not agents, partners or joint venturers.

20.13. Export Restrictions. The Products may be subject to U.S. export restrictions and import restrictions of other jurisdictions. Customer must comply with all applicable export and import Laws in its access to, use of, and download of the Products or any content or records entered into the Products. Customer must not (and must not allow anyone else to) export, re-export, transfer or disclose the Products or any direct product of the Products: (a) to (or to a national or resident of) any U.S. embargoed jurisdiction, (b) to anyone on any U.S. or

applicable non-U.S. restricted- or denied-party list, or (c) to any party that Customer has reason to know will use the Products in violation of U.S. export Law, or for any restricted end user under U.S. export Law.

20.14. Government End-Users. If Customer is a United States federal, state or local government customer, this Agreement is subject to, and is varied by, the Government Amendment attached hereto as Exhibit A and available at https://www.atlassian.com/legal/government-amendment.

20.15. No Contingencies. The Products, Support and Advisory Services in each Order are purchased separately and not contingent on purchase or use of other Atlassian products and services, even if listed in the same Order. Customer's purchases are not contingent on delivery of any future functionality or features.

21. Definitions.

"**Acceptable Use Policy**" means Atlassian's acceptable use policy attached hereto as Exhibit F and available at https://www.atlassian.com/legal/acceptable-use-policy.

"**Advisory Services**" means advisory services as described in the Advisory Services Policy.

"**Advisory Services Policy**" means Atlassian's advisory services policy attached hereto as Exhibit G and available at https://www.atlassian.com/legal/advisory-services-policy.

"**Affiliate**" means an entity that, directly or indirectly, owns or controls, is owned or is controlled by or is under common ownership or control with a party, where "ownership" means the beneficial ownership of more than fifty percent (50%) of an entity's voting equity securities or other equivalent voting interests and "control" means the power to direct the management or affairs of an entity.

"**Agreement**" means this Atlassian Customer Agreement, as well as the Product-Specific Terms, the DPA and the Policies.

"**Atlassian Apps**" means apps developed by Atlassian for use with Cloud Products or Software Products, as designated by Atlassian in the Atlassian Marketplace.

"**Atlassian Marketplace**" means the online platform to purchase apps for Atlassian products currently branded the Atlassian Marketplace and accessible at https://marketplace.atlassian.com/.

"**Cloud Products**" means Atlassian's cloud products, including client software for its cloud products ("**Cloud Clients**").

"**Code of Conduct**" means the Atlassian Code of Business Conduct & Ethics, attached hereto as Exhibit H and available at https://investors.atlassian.com/governance/governance-documents/default.aspx.

"**Customer Data**" means any data, content or materials provided to Atlassian by or at the direction of Customer or its Users via the Cloud Products, including from Third-Party Products.

"**Customer Materials**" means materials and other resources that Customer provides to Atlassian in connection with Support or Advisory Services.

"**Documentation**" means Atlassian's usage guidelines and standard technical documentation for the applicable Product, available at https://support.atlassian.com/, unless otherwise specified in the Product-Specific Terms.

"**DPA**" means the Atlassian data processing addendum attached hereto as Exhibit D and available at https://www.atlassian.com/legal/data-processing-addendum.

"**Laws**" means all applicable laws, regulations, conventions, decrees, decisions, orders, judgments, codes and requirements of any government authority (federal, state, local or international) having jurisdiction.

"**Order**" means Atlassian's ordering document, online sign-up or other ordering process that Atlassian enables specifying the Products, Support or Advisory Services to be provided under this Agreement, accepted by Atlassian in accordance with Section 9 (Ordering Process and Delivery).

"**Policies**" means the Acceptable Use Policy, Advisory Services Policy, guidelines for Reporting Copyright and Trademark Violations, Privacy Policy, Security Measures, Service Level Agreement, Support Policy, Third-Party Code Policy and any additional Atlassian policies specified in Product-Specific Terms.

"**Privacy Policy**" means Atlassian's privacy policy attached hereto as Exhibit I and available at https://www.atlassian.com/legal/privacy-policy.

"**Products**" means the applicable Cloud Products or Software Products made available by Atlassian in connection with an Order. Products also include Atlassian Apps.

"**Product-Specific Terms**" means product-specific terms that apply only to certain Products, attached hereto as Exhibit E and available at https://www.atlassian.com/legal/product-terms.

"**Reseller**" means a partner authorized by Atlassian to resell Atlassian's Products, Support and Advisory Services to customers.

"**Scope of Use**" means Customer's entitlements to the Products. Such entitlements may be based on: (a) number of licenses, copies or instances, (b) entity, division, business unit, website, or field of use, (c) number and type of Users, (d) number of queries, requests or other usage-based subscription units, or (e) other restrictions or billable units.

"**Security Measures**" means Atlassian's security practices attached hereto as Exhibit C and available at https://www.atlassian.com/legal/security-measures.

"**Service Level Agreement**" means the service level commitments, if any, for a Cloud Product as described in Exhibit J, attached hereto and available at https://www.atlassian.com/legal/sla.

"**Software Products**" means Atlassian's installed software products and any generally-available bug fixes, updates and upgrades it provides to Customer, including through Support.

"**Subscription Term**" means the term for Customer's use of or access to the Products and related Support and Advisory Services as identified in an Order.

"**Support**" means the level of support for the Products corresponding to Customer's Scope of Use, as identified in the Support Policy.

"**Support Policy**" means the Atlassian support offerings documentation available at https://confluence.atlassian.com/support/atlassian-support-offerings-193299636.html.

"**Third-Party Code Policy**" means Atlassian's third-party code policy attached hereto as Exhibit K and available at https://www.atlassian.com/legal/third-party-code-policy.

"**User**" means any individual that Customer authorizes to use the Products. Users may include: (i) Customer's and its Affiliates' employees, consultants, contractors and agents (ii) third parties with which Customer or its Affiliates transact business (iii) individuals invited by Customer's users (iv) individuals under managed accounts, or (v) individuals interacting with a Product as Customer's customer.

Exhibit A

ATLASSIAN

Government Amendment

Effective starting: April 1, 2024

This Government Amendment (this "**Amendment**") modifies the Atlassian Customer Agreement or a written agreement executed by Atlassian (each, the "**Agreement**") and applies to United States federal, state, and local government Customers ("**Government**") only to address statutory restrictions that apply to the Agreement.

The Government and Atlassian are together referred to as the "**Parties**." Accordingly, the Agreement is hereby modified as set forth below as it pertains to use by the Government. Atlassian may update or modify this Amendment from time to time as set forth in the Agreement.

All capitalized terms used and not defined in this Amendment have the meanings given to them in the Agreement. Except as expressly set forth herein, all of the terms and conditions of the Agreement remain in full force and effect.

1. Commercial Items. The Products, Documentation, and related Support and Advisory Services are commercial in nature and available in the open marketplace. For U.S. federal Government Customers, the Products are "commercial computer software" as defined at 48 C.F.R. §§ 2.101 and 252.227-7014(a)(1) and as the term is used in 48 C.F.R. §§ 12.212 and 227.7202; the related Support and Advisory Services are "commercial services" as defined in 48 C.F.R. § 2.101; and the Documentation is commercial "computer software documentation" as defined in 48 C.F.R. §§ 2.101 and 252.227-7014(a)(5) and as used in 48 C.F.R. §§ 12.212 and 227.7202. The Products, Documentation, and related Support and Advisory Services are provided to all Government Customers and Users, for use by the Government or on its behalf, subject to the terms of this Agreement, and all sales to U.S. federal Government Customers must be consistent with 48 C.F.R. §§12.212, 227.7202, and 252.227-7015, as applicable. The Products, Documentation, and related Support and Advisory Services are licensed to the Government with only those rights as granted to all other Customers and Users, according to the terms and conditions contained in the Agreement.

2. Government Purpose. Government's use of Products, Documentation, and related Support and Advisory Services under the Agreement as amended herein must only be for a governmental purpose. Any private, personal, or non-governmental purposes are not subject to this Amendment.

3. Liability, Statute of Limitations. Claims and liabilities arising from the Agreement will be determined under the Contract Disputes Act, the Federal Tort Claims Act, or the equivalent governing state or local legal authority and procedure. Federal statute of limitations provisions or, if applicable, state statute of limitations, apply to any breach or claim.

4. Governing Law. Any terms regarding choice of law and venue in the Agreement are hereby waived. The Agreement and this Amendment are governed by, and interpreted and enforced in accordance with, the laws applicable to Government without reference to conflict of laws. The laws of the State of California will apply in the absence of applicable law.

5. Intellectual Property Ownership. Except as expressly stated in the Agreement, no rights to any derivative works, inventions, products or product modifications, or documentation are conferred to Government or any other party. All such rights belong exclusively to Atlassian.

6. Publicity Rights. No publicity rights are granted by either Party in this Agreement. Any publicity must be authorized in writing by the Parties prior to name or logo use.

7. Order of Precedence and Severability.

7.1. Order of Precedence. If there is any conflict between this Amendment and the Agreement, or between this Amendment and other terms, rules or policies on the Atlassian website or related to the Products or related services, this Amendment will prevail.

7.2. Severability. The terms and conditions of this Amendment and the Agreement apply except to the limited extent prohibited by Law. If and to the extent any term or condition of this Amendment or the Agreement is so prohibited, such term or condition will be deemed modified only to the extent reasonably necessary to conform to Law but to give maximum effect to the term or condition as written.

Exhibit B

ATLASSIAN

Government Cloud FedRAMP Moderate Terms

Effective starting: April 21, 2025

These FedRAMP Moderate Terms (these "Terms") modify the Atlassian Customer Agreement or a written agreement executed by Atlassian (as applicable, the "Agreement"). In the event of a conflict between these Terms and any other provisions contained in any Agreement, these Terms will control.

1. Overview

1.1. Atlassian Government Cloud (AGC) Products. These Terms apply to Customer's use of Cloud Products that are hosted in the Atlassian FedRAMP environment, as described here ("AGC Products").
1.2. Government Amendment. The Government Amendment applies to United States federal, state, and local government customers (each, a "U.S. Government Entity").

2. Limited Usage

2.1. Government Use. AGC Products may only be used by (a) a U.S. Government Entity, or (b) a government contractor using AGC for the fulfillment of a U.S. government contract (federal, state, or local) (a "U.S. Government Contractor").
2.2. Termination for Prohibited Usage. Any use of AGC Products in breach of this Section 2 (Limited Usage) will be deemed a breach of the Agreement and Atlassian may terminate Customer's Subscription Term for such AGC Products in accordance with the Disputes Clause (Contract Disputes Act). Atlassian may also terminate this Agreement upon notice for any breach of this Section 2 (Limited Usage) in accordance with the Disputes Clause (Contract Disputes Act). Customer will not be entitled to any refunds as a result of such termination for Services provided, and any unpaid amounts for the applicable Subscription Terms and any related service periods will become due and payable immediately upon such termination.

3. Atlassian Obligations

3.1. Maintaining authorization status. During the Subscription Term for AGC Products, Atlassian will use commercially reasonable efforts to: (a) Maintain its FedRAMP Moderate authorization at the current or higher authorization level; and (b) Maintain an information security program designed to provide at least the same level of protection as required by its FedRAMP Moderate authorization.
3.2. Lapse or Revocation. If Atlassian's FedRAMP Moderate authorization lapses or is revoked, Atlassian will provide prompt notice to Customer of such lapse or revocation.

4. Customer Obligations

4.1. Compliance with AGC Documentation.
(a) Customer must use AGC Products, and only upload Customer Data to AGC Products, in accordance with the Documentation. "Documentation" means Atlassian's usage guidelines and standard technical documentation for the applicable AGC Product, available at Atlassian Support, further supplemented by any documents attached to the Order.
(b) If Customer uploads data to AGC Products that is prohibited by the Documentation, then Customer will be solely responsible for sanitization costs incurred by Atlassian and its agents, without application of any limitation of liability or damages caps in the Agreement.
4.2. Reserved.

Exhibit C

ATLASSIAN

Atlassian's Technical and Organisational Measures

Effective starting: October 7, 2025

Introduction

Security is an essential part of Atlassian's offerings. This page describes Atlassian's security program, certifications, policies, and physical, technical, organizational and administrative controls and measures to protect Customer Data and, where indicated below, Customer Materials from unauthorized access, destruction, use, modification or disclosure (the "Security Measures"). The Security Measures are consistent with the commonly-accepted industry standards and practices, including NIST 800-53 controls.

Any capitalized terms used but not defined have the meanings set out in the Agreement or the Data Processing Addendum. Further details on Atlassian's security posture can be found in our Trust Center and Compliance Resource Center.

1. Access Control

Atlassian maintains a comprehensive set of formal policies, controls, and practices for the appropriate access control when processing Customer Data and Customer Materials, which includes:

1.1. access management policy addressing access control standards, including the framework and the principles for user provisioning;

1.2. designated criticality tiers based on a Zero Trust Model architecture, including the requirements for multi-factor authentication on higher-tier services;

1.3. user provisioning for access to Atlassian systems, applications and infrastructure based on the relevant job role and on the least privilege principle that is enforced through the authentication processes, enabling only authorized personnel to have access to development and build environments (including source code repositories) associated with the Products;

1.4. strict role-based access controls for Atlassian staff, allowing access to Customer Data only on a need-to-know basis;

1.5. segregation of duties including but not limited to (i) access controls reviews, (ii) HR-application managed security groups, and (iii) workflow controls;

1.6. a prior approval of all user accounts by Atlassian's management before granting access to data, applications, infrastructure, or network components based on the data classification level; regular review of access rights as required by relevant role;

1.7. use of technical controls such as virtual private network (VPN) and multi-factor authentication (MFA) where relevant based on information classification and Atlassian's Zero Trust Model architecture;

1.8. centrally managed mobile device management (MDM) solution, including defined lockout periods and posture checks for endpoints and mobile devices;

1.9. identifying and removing redundant and dormant accounts, promptly revoking access through automated and regular review processes.

2. Awareness and Training

Atlassian maintains a comprehensive set of formal policies, controls, and practices for conducting appropriate trainings and security awareness activities, which includes:

2.1. extensive awareness training on security, privacy, and compliance topics for all employees at induction and annually, utilizing diverse formats (online, in-person, and pre-recorded sessions, phishing simulations);

2.2. targeted role-specific training and documentation for employees with elevated privileges to address relevant risks and enhance their specific knowledge as required for their respective roles;

2.3. maintaining all training records in a designated learning management system;

2.4. an automated reminder for training deadlines, with a built-in escalation process to respective managers;

2.5. continuous security awareness trainings (extending to contractors and partners), covering current threats and best security practices;

2.6. secure coding trainings by security champions embedded within engineering teams;

2.7. annual mandatory security trainings and events to reinforce security principles through different activities, emphasizing the collective responsibility for security;

2.8. annual secure development training to Atlassian developers in alignment with industry standards.

3. Audit and Accountability

Atlassian maintains a comprehensive set of formal policies, controls, and practices for proper auditing and accountability purposes, which includes:

3.1. comprehensive logging standards as part of Atlassian's policy management framework, with annual reviews and senior management approvals;

3.2. secure forwarding and storage of relevant system logs to a centralized log platform of the cloud infrastructure with read-only access;

3.3. monitoring of security audit logs to detect unusual activity, with established processes for reviewing and addressing anomalies;

3.4. regular updates to the logging scope of information and system events for Cloud Products and related infrastructure in order to address new features and changes;

3.5. utilizing time sync services from relevant cloud service providers (e.g. AWS or Microsoft Azure) for reliable timekeeping across all deployed instances.

4. Assessment, Authorisation and Monitoring

Atlassian maintains a comprehensive set of formal policies, controls, and practices for consistent system monitoring and security assessments, which includes:

4.1. extensive audit and assurance policies with annual reviews and updates;

4.2. a centralized internal policy program categorising the global policies into different domains including annual review, and senior management approval of the program;

4.3. audit management encompassing the planning, risk analysis, security control assessment, conclusion, remediation schedules, and review of past audit reports;

4.4. internal and independent external audits conducting annual evaluations of legal and contractual requirements, as well as effectiveness of controls and processes to validate compliance;

4.5. ongoing verification of compliance against relevant standards and regulations, e.g. ISO 27001 or SOC 2;

4.6. systematically addressing any nonconformities found through audit findings taking into account the root-cause analysis, severity rating, and corrective actions;

4.7. annual penetration testing on Cloud and Software Products and proactive bug bounty programs for the detection and mitigation of vulnerabilities;

4.8. continuous vulnerability scanning consistent with commonly-accepted standards and practices for security testing with subsequent remediation of identified vulnerabilities based on the Common Vulnerability Scoring System (CVSS) in line with Atlassian's Security Bugfix Policy;

4.9. security testing, privacy risk and vulnerability assessments of the relevant Cloud Products and processes at least annually.

5. Configuration Management

Atlassian maintains a comprehensive set of formal policies, controls, and practices for appropriate configuration management, which includes:

5.1. change management policies covering the risk management for all internal and external asset changes, reviewed annually;

5.2. standard procedures for change management applicable to encryption and cryptography for the secure handling of data (e.g. encryption keys) according to its security classification, including but not limited to key rotation, defining key ownership, secure storage;

5.3. a centralized internal policy program categorising the global policies into different domains including annual review, and senior management approval of the program;

5.4. stringent policies encompassing (i) encryption, (ii) cryptography, (iii) endpoint management, and (iv) asset tracking inline with industry standards;

5.5. established baselines and standards for change control that require testing documentation prior to implementation and authorized approval;

5.6. a peer review and green build process requiring multiple reviews and successful testing for production code and infrastructure changes;

5.7. a strict post-implementation testing and approval process for emergency changes to the code;

5.8. comprehensive automated system supplemented by an Intrusion Detection System (IDS), managing and protecting against unauthorized changes;

5.9. cataloguing and tracking of all physical and logical assets with annual reviews ensuring up-to-date asset management;

5.10. continuous monitoring and managing the health (including capacity) and availability of assets and Cloud Products, including their underlying components.

6. Contingency Planning

Atlassian maintains a comprehensive set of formal policies, controls, and practices for appropriate contingency planning for business continuity and disaster recovery purposes, which includes:

6.1. a skilled workforce and robust IT infrastructure, including telecommunications and technology essential for Product delivery;

6.2. business continuity and disaster recovery plans ("BCDR Plans"), including defined recovery time objectives (RTOs) and recovery point objectives (RPOs);

6.3. business continuity plans encompassing data storage and continuity of use, reasonably designed to prevent interruption to access and utilization;

6.4. geographic diversity as a result of our global workforce and cloud infrastructure;

6.5. reinforcing business operations through resilience controls, such as daily backups, annual restoration testing, and alternative cloud infrastructure storage sites;

6.6. a resilience framework and procedures for response and remediation of cybersecurity events in order to maintain business continuity;

6.7. quarterly disaster recovery tests and exercises to enhance response strategies, with post-test analyses for continuous improvement aligned with applicable BCDR Plans;

6.8. continuous capacity management across Cloud Products, with internal monitoring and adjustments to maintain service availability and processing capacity, for example distributed denial-of-service attack (DDoS) mitigation for Cloud Products and related infrastructure;

6.9. a centralized internal policy program for annual reviews and updates of all global policies related to business continuity;

6.10. robust backup protocols, including (i) data encryption, (ii) redundancy across data centers, and (iii) regular testing to bolster contingency planning.

7. Identification and Authentication

Atlassian maintains a comprehensive set of formal policies, controls, and practices for appropriate identification and authentication purposes which includes:

7.1. employee identification uniquely through active directory, utilising single sign-on (SSO) for application access;

7.2. utilising of MFA for secure access, specifically for VPN and application launch via SSO based on Atlassian's Zero Trust Model architecture;

7.3. password policies following the NIST 800-63B guidelines, focusing on the security aspects of password creation and management;

7.4. ensuring the security of stored credentials using advanced encryption methods, e.g. password and secret management systems;

7.5. documented approvals, regular reviews of users and accounts, and automatic syncs between the relevant identity system and human resources systems to maintain the integrity and accuracy of identification data.

8. Security Incident Response

Atlassian maintains a comprehensive set of formal policies, controls, and practices for appropriate Security Incident response purposes, which includes:

8.1. security Incident response plans emphasizing preparedness, containment, eradication and recovery, as well as focus on data protection and other regulatory requirements;

8.2. dedicated cross-functional teams handling Security Incidents, ensuring effective communication and collaboration, including well-defined processes for triaging security events;

8.3. regular testing of response plans with established metrics to track and improve Security Incident management effectiveness;

8.4. annual reviews of company-wide incident response plans and policies to reflect and share current best practices across the company;

8.5. post-incident review with root cause analysis conducted for high-severity Security Incidents, focusing on systemic improvements and learning;

8.6. incident response procedures and plans embedded in critical business processes to minimize downtime and security risks;

8.7. published system availability information to aid in Security Incident handling and reporting at https://status.atlassian.com/, and https://www.loomstatus.com/, as applicable;

8.8. the ability for Customer to report incidents, vulnerabilities, bugs, and issues, ensuring prompt attention to concerns related to system defects, availability, security, and confidentiality;

8.9. commitment to Customer notification of the Security Incident without undue delay as set forth in Atlassian's Data Processing Addendum, including the obligation to promptly assist the Customer with necessary information for compliance with Applicable Data Protection Laws.

9. Maintenance

Atlassian maintains a comprehensive set of formal policies, controls, and practices for continued effectiveness of its Cloud Products, which includes:

9.1. regular testing of BCDR Plans with quarterly evaluations, validated by external auditors;

9.2. real-time monitoring of the availability of multiple regions with performing of regular tests for infrastructure availability and reliability;

9.3. measures outlined in Section 4 (Assessment, Authorisation and Monitoring), Section 6 (Contingency Planning) and Section 18 (System and Communications Protection).

10. Media Protection

Atlassian maintains a comprehensive set of formal policies, controls, and practices to ensure the protection of media (internal and external), which includes:

10.1. using reliable third party services (e.g. Microsoft Azure or AWS) to operate the physical infrastructure for processing Customer Data as a Sub-processor;

10.2. sanitization and degaussing of used equipment by the third party cloud service providers, including hard drives with Customer Data in line with industry standards (e.g. NIST 800-88);

10.3. full disk encryption using industry standards (e.g. AES-256) employed for data drives on servers and databases storing Customer Data, Customer Materials, and on endpoint devices;

10.4. access to Customer Data and Customer Materials is strictly limited to Atlassian-owned machines configured under a mobile device management solution, following Atlassian's Zero Trust Model architecture;

10.5. internal bring your own device (BYOD) policy ensuring that access to permitted Atlassian networks and systems is only possible via secure and compliant devices;

10.6. unattended workspaces are required to have no visible confidential data, aligning with the secure workplace guidance.

11. Physical and Environmental Protection

Atlassian maintains a comprehensive set of formal policies, controls, and practices for the physical and environmental protection of Customer Data and Customer Materials, which includes:

11.1. a safe and secure working environment with controls implemented globally at Atlassian's offices;

11.2. employing badge readers, camera surveillance, and time-specific access restrictions for enhanced security;

11.3. implementing and maintaining access logs at office buildings for investigative purposes;

11.4. multiple compliance certifications and robust physical security measures, including biometric identity verification and on-premise security, implemented by third party data center providers;

11.5. controlled access points and advanced surveillance systems as well as protective measures for power and telecommunication cables, alongside with environmental control systems, implemented by third party data center providers;

11.6. positioning critical equipment in low-risk environmental areas for added safety (both by Atlassian and its third party data center providers);

11.7. precautions to protect physical infrastructure of facilities where Customer Data or Customer Materials are hosted or otherwise processed against environmental threats, both naturally occurring and man-made, such as excessive ambient temperature, fire, flood, humidity, theft, and vandalism.

12. Planning

Atlassian maintains a comprehensive set of formal policies, controls, and practices for appropriate planning of business operations, which includes:

12.1. active monitoring and documentation by legal and compliance teams on regulatory obligations;

12.2. a detailed system security plan with comprehensive documentation on system boundaries and product descriptions;

12.3. communication to internal users and customers about significant changes to key products and services;

12.4. periodic reviews and updates of the security management program.

13. Program Management

Atlassian maintains a comprehensive set of formal policies, controls, and practices for appropriate program management, which includes:

13.1. supporting the security management program at the executive level, encompassing all security-related policies and practices;

13.2. documented information security policies, including (i) defined roles, (ii) risk mitigation, and (iii) service provider security management program;

13.3. periodic risk assessments of systems processing Customer Data, with prompt reviews of Security Incidents for corrective action;

13.4. formal security controls framework aligning to standards such as SOC 2, ISO27001, and NIST 800-53;

13.5. processes for identifying and quantifying security risks, with mitigation plans approved by the Chief Trust Officer and regular tracking of implementation;

13.6. comprehensive and diverse approach to security testing to cover a wide range of potential attack vectors;

13.7. regular review, testing and updating of the information security management program and policies integral to Atlassian's business (annually, at a minimum);

13.8. an information security management program that requires security by design approach, secure development, secure engineering, and secure operations that are consistent with industry standards;

13.9. development program for security staff with regular trainings; organizational chart that delineates roles and responsibilities;

13.10. setting and review of strategic operational objectives by the executive management;

13.11. annual review of the Enterprise Risk Management (ERM) framework, including the risk management policy, risk assessments, and fraud risk assessments, by the Head of Risk and Compliance.

14. Personnel Security

Atlassian maintains a comprehensive set of formal policies, controls and practices for the security of all Atlassian's employees who have access to Customer Data and Customer Materials, which includes:

14.1. pre-hire background checks, including criminal record inquiries, for all in-scope employees, with heightened reviews performed for senior executive and accounting roles to the extent permissible under applicable local laws;

14.2. an onboarding process that includes in-scope employees' execution of confidentiality agreements, employment contracts, and acknowledgement of applicable policies and codes of conduct;

14.3. global and local employment policies, maintained and reviewed annually;

14.4. processes for role changes and terminations including automatic de-provisioning and checklists for employee exits, with managerial approval required for re-provisioning the access;

14.5. ongoing security and compliance training for employees, with targeted training for specific roles and the presence of security champions in teams;

14.6. established disciplinary processes to manage violations of Atlassian's policies.

15. Personal Data Processing and Transparency

Atlassian maintains a comprehensive set of formal policies, controls, and practices for the compliance of personal data processing in line with Applicable Data Protection Laws, which includes:

15.1. a global privacy compliance program for reviewing and adapting to applicable data protection laws including necessary safeguards and processes;

15.2. maintaining an internal personal data processing policy with clear definitions of personal data categories, processing purposes, and processing principles;

15.3. detailed standards for processing of various categories of personal data covering the topics such as processing principles, applicable legal basis, privacy by design/by default principles, retention, and destruction;

15.4. an established method to create pseudonymised data sets using industry standard practices and appropriate technical and organisational measures governing the systems capable of remapping pseudonymous identifiers;

15.5. transparent privacy policies for its users and customers, as well as internal guidelines for employees;

15.6. comprehensive compliance documentation, including but not limited to, and where applicable, (i) a record of processing activities, (ii) privacy impact assessments, (iii) transfer impact assessments, (iv) consents, and (v) data processing agreements with customers and vendors;

15.7. secure development practices across all development lifecycle stages, focusing on security and data protection from the initial design phase;

15.8. ensuring Atlassian’s compliance with data subjects' rights to access, correct, and delete their personal data in accordance with applicable data protection laws.

16. Risk Assessment

Atlassian maintains a comprehensive set of formal policies, controls, and practices for a robust Information Security Management System, which includes:

16.1. a comprehensive risk management program for identifying, assessing, and addressing various risks to support informed risk management decisions;

16.2. a policy program aligning company-wide policies with ISO 27001 and other relevant standards to mitigate associated risks;

16.3. continuous security testing and vulnerability identification, including (i) penetration tests, (ii) bug bounties, and (iii) proactive threat mitigation;

16.4. processes and metrics for reporting vulnerability management activities;

16.5. thorough security evaluations, including independent external and internal audits.

17. System and Services Acquisition

Atlassian maintains a structured, security-centric methodology for the system development, maintenance, and change management, which includes:

17.1. an agile secure software development life cycle, including the review and documentation of system and infrastructure changes;

17.2. secure, standardized application deployment with automated processes for system configuration changes and deployment;

17.3. defined development process with peer-reviewed pull requests and mandatory automated tests prior to merging;

17.4. segregated responsibilities for change management among designated employees;

17.5. emergency change processes, including "break glass" procedures, ensuring readiness for rapid response during critical incidents;

17.6. robust compliance settings in Atlassian’s source code and deployment systems preventing unauthorized alterations;

17.7. clear documentation and monitoring of all configuration changes, with automatic alerts for non-compliance or alterations in peer review enforcement;

17.8. supporting documentation for Cloud and Software Products including instructions on how to securely use and configure them;

17.9. strict controls over modifications to vendor software;

17.10. regular scanning and updates of third-party or open-source libraries as well as ongoing scanning of the code base.

18. System and Communications Protection

Atlassian maintains a comprehensive set of formal policies, controls, and practices for system and communication protection which includes:

18.1. cryptographic mechanisms to safeguard sensitive information stored and transmitted over networks, including public internet, using reliable and secure encryption technologies;

18.2. encryption of Customer Data at rest using AES-256 and in transit using Transport Layer Security (TLS) 1.2+ with Perfect Forward Secrecy (PFS) across public networks;

18.3. zone restrictions and environment separation limiting connectivity between production and non-production environments;

18.4. continuous management of workstation assets including (i) security patch deployment, (ii) password protection, (iii) screen locks, and (iv) drive encryption through asset management software;

18.5. restricting access to only known and compliant devices enrolled in the MDM platform, adhering to the principles of Zero Trust Model architecture;

18.6. maintaining firewalls at corporate edges for both platform and non-platform hosted devices for additional layers of security;

18.7. maintaining network and host defense, including operating system hardening, network segmentation, and data loss prevention technologies;

18.8. established measures to ensure Customer Data and Customer Materials are kept logically segregated from other customers' data.

19. System and Information Integrity

Atlassian maintains formally established policies and practices that include the following controls and safeguards relevant for system and information integrity, in particular:

19.1. adherence to stringent data disposal protocols in line with applicable laws, reasonably ensuring that data from storage media is irrecoverable post-sanitization;

19.2. strict policies to prevent the use of production data in non-production environments, ensuring the data integrity and segregation;

19.3. centrally managed, read-only system logs; monitoring for Security Incidents; retention policies aligned with security best practices;

19.4. generating and retaining logs that record access by Atlassian personnel to Customer Data or Customer Materials with respect to systems used in providing the Products, and protection of such logs against unauthorized access, modification, and accidental or deliberate destruction;

19.5. managing endpoint compatibility with systems and applications, enhancing network security and reliability;

19.6. deploying anti-malware strategies on the relevant infrastructure and Atlassian devices for robust protection against malware threats with regular updates to malware protection policies and detection tools;

19.7. unique identifiers and token-based access control to ensure logical isolation of, and secure, limited access to, Customer Data;

19.8. segregation of production and non-production environments;

19.9. protection of Customer Data within a sandbox environment (for example, to reproduce an error) utilising similar measures to those in the production environment.

20. Supply Chain Risk Management

Atlassian maintains formally established policies and practices for supply chain risk management, which includes:

20.1. a formal framework for managing vendor relationships, and aligning the security, availability, and confidentiality standards of suppliers throughout their lifecycles;

20.2. a robust third party risk management (TPRM) assessment process including risk assessments, due diligence, contract management, and ongoing monitoring of all third parties;

20.3. dedicated teams, including legal, procurement, security, and risk departments for the review of contracts, service level agreements, and security measures to manage risks related to security and data confidentiality;

20.4. functional risk assessments of suppliers before onboarding and periodically, based on risk levels, with revisions during policy renewals or significant relationship changes;

20.5. an inventory of all suppliers detailing ownership and risk levels associated with the services provided to Atlassian;

20.6. annual review of audit reports (e.g. SOC 2) and regular reviews of information technology governance policies and security assessments of supply chain providers to ensure applicable controls are compliant;

20.7. measures to secure third-party endpoints, focusing on compliance monitoring and selective restrictions.

Exhibit D

ATLASSIAN

Atlassian Data Processing Addendum

Effective starting: October 7, 2025

This Data Processing Addendum ("**DPA**") supplements the Atlassian Customer Agreement, or other agreement in place between Customer and Atlassian covering Customer's use of Atlassian's Products and related Support and Advisory Services (the "**Agreement**"). Unless otherwise defined in this DPA or in the Agreement, all capitalized terms used in this DPA will have the meanings given to them in Section 9 of this DPA.

1. Scope and Term.

1.1. Roles of the Parties. For the purposes of the Agreement, the Parties agree that:

(a) Customer is either a Controller of Customer Data, or a Processor of Customer Data acting on another Controller's behalf (e.g. Customer's Affiliate) while passing down relevant processing instructions to Atlassian. Processing details are stated in Schedule 1 (Description of Processing).

(b) Atlassian is a Processor (or respectively, a Sub-processor) of Customer Data. Processing details are stated in Schedule 1 (Description of Processing).

1.2. Term of the DPA. The term of this DPA coincides with the term of the Agreement and terminates upon expiration or earlier termination of the Agreement (or, if later, the date on which Atlassian ceases all Processing of Customer Personal Data).

1.3. 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) Schedule 1 (Description of Processing); (3) the main body of this DPA; and (4) the Agreement.

2. Processing of Personal Data.

2.1. Customer Instructions.

(a) This DPA, the Agreement, applicable Orders and Customer's use of the Products (including relevant configurations and settings) and related Support and Advisory Services constitute Customer's documented instructions regarding Atlassian's Processing of Customer Data ("**Documented Instructions**").

(b) Atlassian must Process Customer Data solely in accordance with the Documented Instructions, as further stated in Section 6.1 of Schedule 1 (Description of Processing). Customer:

(i) must ensure its Documented Instructions comply with Applicable Data Protection Law. Atlassian is not responsible for monitoring Customer's compliance with Applicable Data Protection Law; and

(ii) is responsible for determining whether the Products and related Support and Advisory Services are appropriate for the Processing of Customer Data under Applicable Data Protection Law.

2.2. Confidentiality. Atlassian must treat Customer Personal Data as Customer's Confidential Information under the Agreement. Atlassian must ensure personnel authorized to Process Personal Data are bound by written or statutory obligations of confidentiality.

3. Security.

3.1. Security Measures. Atlassian has implemented and will maintain appropriate technical and organizational measures designed to protect the security, confidentiality, integrity and availability of Customer Data and protect against Security Incidents. Customer is responsible for configuring the Products and using features and functionalities made available by Atlassian to maintain appropriate security in light of the nature of Customer Data. Atlassian's current technical and organizational measures are described here. Customer acknowledges that the Security Measures are subject to technical progress and development and that Atlassian may update or modify the Security Measures from time to time, provided that such updates and modifications do not materially decrease the overall security of the Cloud Products during a Subscription Term.

3.2. Security Incidents. Atlassian must notify Customer without undue delay and, where feasible, no later than seventy-two (72) hours after becoming aware of a Security Incident. Atlassian must make reasonable efforts to identify the cause of the Security Incident, mitigate the effects and remediate the cause to the extent within Atlassian's reasonable control. Upon Customer's request and taking into account the nature of the Processing and the information available to Atlassian, Atlassian must assist Customer by providing information reasonably necessary for Customer to meet its Security Incident notification obligations under Applicable Data Protection Law. Atlassian's notification of a Security Incident is not an acknowledgment by Atlassian of its fault or liability.

4. Sub-processing.

4.1. General Authorization. By entering into this DPA, Customer provides general authorization for Atlassian to engage Sub-processors to Process Customer Personal Data. Atlassian must: (i) enter into a written agreement with each Sub-processor imposing data protection terms that require the Sub-processor to protect Customer Personal Data to the standard required by Applicable Data Protection Law and to the same standard provided by this DPA; and (ii) remain liable to Customer if such Sub-processor fails to fulfill its data protection obligations with regard to the relevant Processing activities under the Agreement.

4.2. Notice of New Sub-processors. Atlassian maintains an up-to-date list of its Sub-processors here, which contains a mechanism for Customer to subscribe to notifications of new Sub-processors. Atlassian will provide such notice, to those emails subscribed, at least thirty (30) days before allowing any new Sub-processor to Process Customer Personal Data (the "**Sub-processor Notice Period**").

4.3. Objection to New Sub-processors. Customer may object to Atlassian's appointment of a new Sub-processor during the Sub-processor Notice Period. If Customer objects, Customer, as its sole and exclusive remedy, may terminate the applicable Order for the affected Cloud Product and related Support and Advisory Services in accordance with Section 12.2 (Termination for Convenience) of the Agreement.

5. Assistance and Cooperation Obligations.

5.1. Data Subject Rights. Taking into account the nature of the Processing, Atlassian must provide reasonable and timely assistance to Customer to enable Customer to respond to requests for exercising a data subject's rights (including rights of access, rectification, erasure, restriction, objection, and data portability) in respect to Customer Personal Data.

5.2. Cooperation Obligations. Upon Customer's reasonable request, and taking into account the nature of the Processing, Atlassian will provide reasonable assistance to Customer in fulfilling Customer's obligations under Applicable Data Protection Law (including data protection impact assessments and consultations with regulatory authorities), provided that Customer cannot reasonably fulfill such obligations independently with help of available Documentation.

5.3. Third Party Requests. Unless prohibited by Law, Atlassian will promptly notify Customer of any valid, enforceable legal process or governmental request compelling Atlassian to disclose Customer Personal Data. Atlassian will follow its law enforcement guidelines in responding to such requests. In the event that Atlassian receives an inquiry or a request for information from any other third party (such as a regulator or data subject) concerning the Processing of Customer Personal Data, Atlassian will redirect such inquiries to Customer, and will not provide any information unless required to do so under Law.

6. Deletion and Return of Customer Personal Data.

6.1. During Subscription Term. During the Subscription Term, Customer and its Users may, through the features of the Cloud Products, access, retrieve or delete Customer Personal Data.

6.2. Post Termination. Following expiration or termination of the Agreement, Atlassian must, in accordance with the Documentation, delete all Customer Personal Data. Notwithstanding the foregoing, Atlassian may retain Customer Personal Data (i) as required by Applicable Data Protection Law or (ii) in accordance with its standard backup or record retention policies, provided that, in either case, Atlassian will maintain the confidentiality of, and otherwise comply with the applicable provisions of this DPA with respect to, retained Customer Personal Data and not further Process it except as required by Applicable Data Protection Law.

7. Audit.

7.1. Audit Reports. Atlassian is regularly audited by independent third-party auditors and/or internal auditors, including as described here. Upon request, and on the condition that Customer has entered into an applicable non-disclosure agreement with Atlassian, Atlassian will supply a summary copy of relevant audit report(s) to Customer, so Customer can verify Atlassian's compliance with the audit standards against which it has been assessed, and this DPA. If Customer cannot reasonably verify Atlassian's compliance with the terms of this DPA, Atlassian will provide written responses (on a confidential basis) to all reasonable requests for information made by Customer related to Atlassian's Processing of Customer Personal Data, provided that such right may be exercised no more than once every twelve (12) months.

7.2. On-site Audits. Only to the extent Customer cannot reasonably satisfy Atlassian's compliance with this DPA through the exercise of its rights under Section 7.1 above, or where required by Applicable Data Protection Law or a regulatory authority, Customer, or its authorized representatives, may, at Customer's expense, conduct audits (including inspections) during the term of the Agreement to assess Atlassian's compliance with the terms of this DPA. Any audit must (i) be conducted during Atlassian's regular business hours, with reasonable advance written notice of at least sixty (60) calendar days (unless Applicable Data Protection Law or a regulatory authority requires a shorter notice period); (ii) be subject to reasonable confidentiality controls obligating Customer (and its authorized representatives) to keep confidential any information disclosed that, by its nature, should be confidential; (iii) occur no more than once every twelve (12) months; and (iv) restrict its findings to only information relevant to Customer.

8. International Provisions. To the extent Atlassian Processes Personal Data protected by Applicable Data Protection Laws in one of the regions listed in Schedule 2 (Region-Specific Terms), the terms specified for the applicable regions will also apply, including the provisions relevant for international transfers of Personal Data (directly or via onward transfer).

9. Definitions.

"**Applicable Data Protection Law**" means all Laws applicable to the Processing of Personal Data under the Agreement.

"**Controller**" 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.

"**Customer Personal Data**'' means Personal Data contained in Customer Data and/or Customer Materials that Atlassian Processes under the Agreement solely on behalf of Customer. For clarity, Customer Personal Data includes any Personal Data included in the attachments provided by Customer or its Users in any technical support requests.

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

"**Processing**" (and "**Process**" and "**Processed**") means any operation or set of operations which is performed on Personal Data or on sets of Personal 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.

"**Processor**" means the entity which Processes Personal Data on behalf of the Controller.

"**Security Incident**'' means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data Processed by Atlassian and/or its Sub-processors, and for the purposes of this definition, "Processing" includes Personal Data and Customer Data.

"**Sub-processor**" means any third party (inc. Atlassian Affiliates) engaged by Atlassian to Process Customer Personal Data.

Schedule 1 Description of Processing

1. Categories of data subjects whose Personal Data is Processed: Customer and its Users.

2. Categories of Personal Data Processed: Customer Personal Data, the content of which is determined and controlled solely by Customer and its Users.

3. Sensitive data transferred: Subject to Section 6.3 of the Agreement (Sensitive Health Information and HIPAA), Customer or its Users may upload content to the Cloud Products which may include (i) data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, (ii) genetic data, biometric data Processed for the purposes of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation, or (iii) data relating to criminal convictions and offences (collectively "**Sensitive Data**"), which is determined and controlled solely by Customer and its Users.

4. The frequency of the transfer: Continuous.

5. Nature of the Processing: Atlassian will Process Personal Data in order to provide the Products and related Support and Advisory Services in accordance with the Agreement, including this DPA. Additional information regarding the nature of the Processing (including transfer) is described in respective Orders for relevant Products and Documentation referring to technical capabilities and features, including but not limited to collection, structuring, storage, transmission, or otherwise making available of Personal Data by automated means.

6. Purpose(s) of the Processing:

6.1. Customer Data. Atlassian will Process Customer Data as a Processor in accordance with Customer's Documented Instructions to:

(a) provide and improve the Products and related Support and Advisory Services for Customer, and enable the use of various features and functionalities in accordance with the Documentation and as directed by Users through the Cloud Products, including investigating Security Incidents, and resolving issues, bugs and errors;

(b) enforce the Acceptable Use Policy;

(c) comply with Atlassian's legal obligations.

6.2. Controller Activities. Atlassian is a Controller of Personal Data as specified in Atlassian's Privacy Policy. This DPA does not limit or prohibit Atlassian from acting in that capacity.

7. Duration of Processing: Atlassian will Process Customer Personal Data for the term of the Agreement as outlined in Section 6 (Deletion and Return of Customer Personal Data).

8. Transfers to Sub-processors: Atlassian will transfer Customer Personal Data to Sub-processors as permitted in Section 4 (Sub-processing).

Schedule 2 Region-Specific Terms

Unless otherwise defined in this DPA or in the Agreement, all capitalized terms used in this Schedule will have the meanings given to them in Section 4 of this Schedule.

1. Europe, United Kingdom and Switzerland.

1.1. Customer Instructions. In addition to Section 2.1 (Customer Instructions), and Schedule 1 (Description of Processing) of the DPA above, Atlassian will Process Customer Personal Data only on Documented Instructions from Customer, including with regard to transfers of such Customer Personal Data to a third country or an international organisation, unless required to do so by Applicable Data Protection Law to which Atlassian is subject; in such a case, Atlassian shall inform Customer of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest. Atlassian will promptly inform Customer if it becomes aware that Customer's Processing instructions infringe Applicable Data Protection Law.

1.2. European Transfers. Where Personal Data protected by the EU Data Protection Law is transferred, either directly or via onward transfer, to a country outside of Europe that is not subject to an adequacy decision, the following applies:

(a) The EU SCCs are hereby incorporated into this DPA by reference as follows:

(i) Customer is the "data exporter" and Atlassian is the "data importer."

(ii) Module Two (Controller to Processor) applies where Customer is a Controller of Customer Personal Data and Atlassian is Processing Customer Personal Data as a Processor.

(iii) Module Three (Processor to Processor) applies where Customer is a Processor of Customer Personal Data and Atlassian is Processing Customer Personal Data as another Processor.

(iv) By entering into this DPA, each party is deemed to have signed the EU SCCs as of the commencement date of the Agreement.

(b) For each Module, where applicable:

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

(ii) In Clause 9, Option 2 applies, and the time period for prior notice of Sub-processor changes is stated in Section 4 (Sub-processing) of this DPA.

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

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

(v) In Clause 18(b), disputes will be resolved before the courts of Ireland.

(vi) The Appendix of EU SCCs is populated as follows:

- The information required for Annex I(A) is located in the Agreement and/or relevant Orders.
- The information required for Annex I(B) is located in Schedule 1 (Description of Processing) of this DPA.
- The competent supervisory authority in Annex I(C) will be determined in accordance with the Applicable Data Protection Law; and
- The information required for Annex II is located here.

1.3. Swiss Transfers. Where Personal Data protected by Swiss Data Protection Law is transferred, either directly or via onward transfer, to any other country that is not subject to an adequacy decision, the EU SCCs apply as stated in in Section 1.2 (European Transfers) above with the following modifications:

(a) All 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 "Regulation (EU) 2016/679" will be replaced with the equivalent article or section of Swiss Data Protection Law; all references to the EU Data Protection Law in this DPA will be interpreted as references to Swiss Data Protection Law.

(b) In Clause 13, the competent supervisory authority is the Swiss Federal Data Protection and Information Commissioner.

(c) In Clause 17, the EU SCCs are governed by the laws of Switzerland.

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

(e) 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).

1.4. United Kingdom Transfers. Where Personal Data protected by the UK Data Protection Law is transferred, either directly or via onward transfer, to a country outside of the United Kingdom that is not subject to an adequacy decision, the following applies:

(a) The EU SCCs apply as set forth in Section 1.2 (European Transfers) above with the following modifications:

(i) Each party shall be deemed to have signed the UK Addendum.

(ii) For Table 1 of the UK Addendum, the parties' key contact information is located in the Agreement and/or relevant Orders.

(iii) For Table 2 of the UK Addendum, the relevant information about the version of the EU SCCs, modules, and selected clauses which this UK Addendum is appended to is located above in Section 1.2 (European Transfers) of this Schedule.

(iv) For Table 3 of the UK Addendum:

- The information required for Annex 1A is located in the Agreement and/or relevant Orders.
- The Information required for Annex 1B is located in Schedule 1 (Description of Processing) of this DPA.

- The information required for Annex II is located here.
- The information required for Annex III is located in Section 4 (Sub-processing) of this DPA.

(b) In Table 4 of the UK Addendum, both the data importer and data exporter may end the UK Addendum.

1.5. Data Privacy Framework. Atlassian participates in and certifies compliance with the Data Privacy Framework. As required by the Data Privacy Framework, Atlassian (i) provides at least the same level of privacy protection as is required by the Data Privacy Framework Principles; (ii) will notify Customer if Atlassian makes a determination it can no longer meet its obligation to provide the same level of protection as is required by the Data Privacy Framework Principles, and (iii) will, upon written notice, take reasonable and appropriate steps to remediate any unauthorized Processing of Personal Data.

2. United States of America. The following terms apply where Atlassian Processes Personal Data subject to the US State Privacy Laws:

2.1. To the extent Customer Personal Data includes personal information protected under US State Privacy Laws that Atlassian Processes as a Service Provider or Processor, on behalf of Customer, Atlassian will Process such Customer Personal Data in accordance with the US State Privacy Laws, including by complying with applicable sections of the US State Privacy Laws and providing the same level of privacy protection as required by US State Privacy Laws, and in accordance with Customer's Documented Instructions, as necessary for the limited and specified purposes identified in Section 6.1 of Schedule 1 (Description of Processing). Atlassian will not:

(a) retain, use, disclose or otherwise Process such Customer Personal Data for a commercial purpose other than for the limited and specified purposes identified in this DPA, the Agreement, and/or any related Order, or as otherwise permitted under US State Privacy Laws;

(b) "sell" or “share” such Customer Personal Data within the meaning of the US State Privacy Laws; and

(c) retain, use, disclose or otherwise Process such Customer Personal Data outside the direct business relationship with Customer and not combine such Customer Personal Data with personal information that it receives from other sources, except as permitted under US State Privacy Laws.

2.2. Atlassian must inform Customer if it determines that it can no longer meet its obligations under US State Privacy Laws.

2.3. Customer may take reasonable and appropriate steps to stop and remediate any unauthorized Processing of Customer Personal Data.

2.4. To the extent Customer discloses or otherwise makes available Deidentified Data to Atlassian or to the extent Atlassian creates Deidentified Data from Customer Personal Data, in each case in its capacity as a Service Provider, Atlassian will:

(a) adopt reasonable measures to prevent such Deidentified Data from being used to infer information about, or otherwise being linked to, a particular natural person or household;

(b) publicly commit to maintain and use such Deidentified Data in a de-identified form and to not attempt to re-identify the Deidentified Data, except that Atlassian may attempt to re-identify such data solely for the purpose of determining whether its de-identification processes are compliant with the US State Privacy Laws; and

(c) before sharing Deidentified Data with any other party, including Sub-processors, contractors, or any other persons (“Recipients”), contractually obligate any such Recipients to comply with all requirements of this Section 2.3 (including imposing this requirement on any further Recipients).

3. South Korea.

3.1. Customer agrees that it has provided notice and obtained all consents and rights necessary under South Korea Privacy Law for Atlassian to Process Personal Data pursuant to the Agreement.

3.2. To the extent Customer discloses or otherwise makes available Deidentified Data to Atlassian, Atlassian will:

(a) maintain and use such Deidentified Data in a de-identified form and not attempt to re-identify the Deidentified Data; and

(b) before sharing Deidentified Data with any other party, including Sub-processors, contractors, or any other persons (“**Recipients**”), contractually obligate any such Recipients to comply with all requirements of this Section 3.2 (including imposing this requirement on any further Recipients).

4. Definitions.

“**Deidentified Data**” means data that cannot reasonably be used to infer information about, or otherwise be linked to, a data subject.

“**Data Privacy Framework**” means 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 self-certification program operated by the US Department of Commerce.

“**Europe**” includes, for the purposes of this DPA, the Member States of the European Union and European Economic Area.

“**EU Data Protection Law**” includes (i) the Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data (General Data Protection Regulation, or GDPR) and (ii) the EU e-Privacy Directive (Directive 2002/58/EC) as amended, superseded or replaced from time to time.

“**EU SCCs**” means the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, as amended, superseded, or replaced from time to time.

“**Service Provider**” has the same meaning as given in the CCPA.

“**South Korea Privacy Law**” means the South Korean Personal Information Protection Act and its Enforcement Decrees.

"**Swiss Data Protection Law**" means the Swiss Federal Act on Data Protection and its implementing regulations as amended, superseded, or replaced from time to time.

"**UK Addendum**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner, Version B1.0, in force 21 March 2022, as amended, superseded or replaced from time to time.

"**UK Data Protection Law**" means the Data Protection Act 2018 and the GDPR as saved into United Kingdom law by virtue of Section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 as amended, superseded or replaced from time to time.

"**US State Privacy Laws**" means all applicable state laws relating to the protection and Processing of Personal Data in effect in the United States of America, which may include, without limitation, the California Consumer Privacy Act, as amended by the California Privacy Rights Act, and its implementing regulations ("**CCPA**").

Exhibit E

ATLASSIAN

Atlassian Product-Specific Terms

Effective starting: April 1, 2024 (unless otherwise indicated below)

The following Product-Specific Terms apply to the Products specified in the table below, and, where Customer orders such Products, supplement the attached Atlassian Customer Agreement or another agreement entered between Customer and Atlassian (the "**Agreement**"). Capitalized terms used and not defined in the Product-Specific Terms have the meanings given to them in the Agreement.

The Atlassian contracting entity for each of the Products is specified in the table below and is "Atlassian" for purposes of the relevant terms, the Agreement and any associated Orders.

Product(s)	Atlassian Contracting Entity	Product-Specific Terms
All Products not named elsewhere in this table, including Confluence, Jira* and Rovo	Atlassian Pty Ltd	Here
Jira Align	AgileCraft LLC	Here
Loom	Loom, Inc.	Here
Opsgenie	OpsGenie, Inc.	Here
Statuspage	Dogwood Labs, Inc., d/b/a StatusPage.io	Here
Trello	Trello, Inc.	Here
* Halp functionality is now part of Jira Service Management and may not be purchased separately. Any Customer with a standalone Halp subscription should refer to the Archives (below) for the governing Product-Specific Terms.		

Archived versions of the product-specific terms are available here, for Customers that purchased under the Atlassian Cloud Terms of Service or Software License Agreement, and here, for Customers that purchased under an Atlassian Subscription Agreement (or predecessor agreement).

* * * *

Atlassian Pty Ltd Products

Atlassian Intelligence and Rovo

Effective starting: The earlier of (i) October 6, 2024 and (ii) date of enablement on an existing cloud plan or purchase

1. AI Offerings.

1.1. Atlassian Intelligence and Rovo. Atlassian makes Atlassian Intelligence and Rovo available to customers as described in these Product-Specific Terms (together, the "**AI Offerings**").

1.2. Loom AI. Loom AI is not covered by these Product-Specific Terms. It is covered separately, attached hereto and here.

2. Input and Output.

2.1. Atlassian Obligations. Each of the AI Offerings provides Output in response to Input. Input and Output are Customer Data under the Agreement. Atlassian may **not** use Input or Output to train or improve the AI Offerings across customers. Atlassian will not permit its subcontractors to use Input or Output to train or improve their models.

2.2. Additional Customer Obligations, Restrictions and Disclaimers.

(a) Output Use and Assessment. Customer is responsible for its use of Output, including determining whether Output is appropriate for that use.

(b) Restrictions. Customer must not (and must not permit anyone else to): (i) provide Input that either violates third-party rights or Law or is intended, or would reasonably be expected, to generate Output that does so; (ii) provide Input that includes Personal Data of children under 13 or any age of digital consent under Law; (iii) use Output in a manner that Customer knows, or reasonably should know, violates third-party rights or Law or (iv) represent that Output is human generated or approved or endorsed by Atlassian or its subcontractors.

(c) Disclaimers. **Output is generated by artificial intelligence, including by using technology provided by third-party subcontractors. Atlassian makes no warranty as to the accuracy, completeness or reliability of Output or that it does not violate third-party rights or Law**. Due to the nature of the AI Offerings, (i) Output may not be unique or exclusive to Customer and its Users, (ii) the same or similar Input may yield differing Output, and (iii) Output does not represent Atlassian's or its subcontractors' views.

(d) Responsible Use of AI Technologies. Atlassian will use commercially reasonable efforts to comply with its Responsibility Technology Principles. A copy of which is attached to the Agreement as Exhibit L and available at: https://www.atlassian.com/trust/responsible-tech-principles.

3. Rovo. This Section 3 applies only to Rovo.

3.1. Connection to Other Products.

(a) Interoperation. Rovo includes features designed to connect and interoperate with other Atlassian Products and Third-Party Products. Atlassian does not make any warranties about future Rovo connection and interoperation with any specific Third-Party Products.

(b) Data Sharing with Third-Party Products. When Customer connects Rovo to a Third-Party Product, Customer may instruct Rovo to send Customer Data and other data to that Third-Party Product. The provider of the Third-Party Product will process that data according to its terms and, when Customer instructs, will send data back to Rovo. Data sent to Rovo may continue to be subject to the third party's terms and is subject to the Agreement.

3.2. Agents.

(a) In General. Agents are features of Rovo that Users may direct to take certain actions on behalf of Customer ("**Agents**"). These actions are not Output. Agents may be provided by third parties as Third-Party Products, Customer or Atlassian.

(b) Additional Customer Obligations and Restrictions. Customer is responsible for its use of Agents, including determining whether any actions Agents may take are appropriate for that use. Customer must not use Agents in a manner that either violates third-party rights or Law or is intended, or would reasonably be expected, to do so.

3.3. Scope of Use. As described in the Documentation, Customer's Scope of Use may vary by Rovo feature.

3.4. Output Indemnification. This Section 3.4 applies only when Customer has an active, paid-up subscription to Rovo at the time of the first event out of which the Output Claim arose.

(a) Indemnification. Atlassian will defend Customer from and against any third-party claim to the extent alleging that Output of Rovo, when used by Customer as authorized by the Agreement, directly infringes any copyright of a third party (an "**Output Claim**") and indemnify and hold harmless Customer against any damages, fines or costs finally awarded by a court of competent jurisdiction (including reasonable attorneys' fees) or agreed in settlement by Atlassian resulting from an Output Claim.

(b) Procedures. Atlassian's obligations in Section 3.4(a) (Indemnification) are subject to Customer providing Atlassian: (i) sufficient notice of the Output Claim so as to not prejudice Atlassian's defense of the Output Claim, (ii) the exclusive right to control and direct the investigation, defense and settlement of the Output Claim, and (iii) all reasonably requested cooperation (including preserving and sharing the relevant Input and Output), at Atlassian's expense for reasonable out-of-pocket expenses. Customer may participate in the defense of an Output Claim with its own counsel at its own expense.

(c) Settlement. Customer may not settle an Output Claim without Atlassian's prior written consent. Atlassian may not settle an Output Claim without Customer's prior written consent if settlement would require Customer to admit fault or take or refrain from taking any action (other than relating to use of the Output or Rovo).

(d) Exceptions. Atlassian's obligations in this Section 3.4 do not apply:

(i) where Customer does not have an active, paid-up subscription to Rovo at the time of the first event out of which the Output Claim arose or

(ii) to the extent an Output Claim arises from: (A) Customer's breach of the Agreement (which includes the Acceptable Use Policy) or unauthorized use of Output or Rovo; (B) Customer's modification of Output; (C) use of Output in combination with items not provided by Atlassian (including Third-Party Products); (D) Output that, or its use in a manner that, Customer knew, or reasonably should have known, was likely to violate the third-party rights or Laws that are the subject of the Output Claim; (E) any use of Output after Atlassian has instructed Customer to cease use or after Customer has received notice of alleged infringement; or (F) Third-Party Products or their output, Input or other non-Output Customer Data or Customer Materials.

(e) Limitation of Liability and Exclusive Remedy. **To the maximum extent permitted by Law, Atlassian's entire liability arising out of or related to all Output Claims will not exceed in aggregate the amounts paid to Atlassian for Rovo during the twelve (12) months preceding the first event out of which an Output Claim arose. This Section 3.4 sets out Customer's exclusive remedy and Atlassian's entire liability regarding Output.**

4. Definitions.

"**Atlassian Intelligence**" means the artificial intelligence features made available by Atlassian as part of certain Cloud Products and plans, including those features labeled or identified by Atlassian as Atlassian Intelligence. Atlassian Intelligence is a set of features and is not a standalone Cloud Product.

"**Input**" means any input (for instance, textual, audiovisual or other content) Customer or a User provides or makes available to an AI Offering.

"**Output**" means any output (for instance, textual, audiovisual or other content) generated and returned to Customer or a User by an AI Offering based on Input.

"**Rovo**" means the artificial intelligence features made available by Atlassian as a standalone Cloud Product(s) that is labeled or identified by Atlassian as Atlassian Rovo or Rovo.

Other Products

1. Secondary Users. As described in the Documentation, certain of the Products may be used as part of Customer's external support or similar resources related to its or its Affiliates' own offerings. End users for such resources are Users under the Agreement. Customer must not permit such Users to use the Products for purposes unrelated to supporting its own offerings or grant such Users administrator, configuration or similar use of the Products.

2. Additional Software Terms. For clarity, importing a back-up from an authorized production instance of one of the Products that is a Software Product into an authorized staging environment of such Software Product does not itself violate the requirement in the "Number of Instances" Section of the Agreement. Atlassian may also make available "developer" licenses for certain of such Software Products to allow Customer to deploy non-production instances, such as for staging or QA purposes.

3. Additional Bitbucket Cloud Terms. The following additional terms apply to Bitbucket Cloud.

3.1. Repositories. Customer Data uploaded to Bitbucket Cloud is stored in "repositories." Customer must designate whether the repositories are public (meaning that anyone coming to the Bitbucket website can view them) or private (meaning that access to those repositories will be limited to those who have permission to access the repositories). For each public repository that Customer maintains, Customer must indicate the license under which Customer is making the contents of the repository available to others, as well as the license under which Customer will accept contributions to the repository.

3.2. Storage Rules. The Documentation specifies pre-defined storage limits for Customer Data. For clarity, Atlassian may enforce those limits in accordance with the Agreement and the Acceptable Use Policy. Similarly, Atlassian may remove Customer Data from Bitbucket Cloud under the Agreement and Acceptable Use Policy where that content is consuming an unreasonable amount of storage in a way that is unrelated to Bitbucket Cloud's purpose as a source code repository (for instance, music, abhorrent content, videos or pornography). Since Atlassian does not maintain access to Customer's repositories, any removal of Customer Data by Atlassian means removal of the entire repository in which the offending data resides, not just the offending portions.

3.3. Accessing Repositories. If Customer is accessing code in a third party's repository, Customer should carefully read all the licenses applicable to that repository before using or contributing any code. **Atlassian is not the licensor of any third-party code made available through Bitbucket and is not responsible for the use or contents of such code.**

3.4. Granting Permissions. When Customer grants permissions to its repositories, Atlassian will not be able to prevent the applicable users from taking the actions allowed under those permissions, even if Customer does not approve of those actions. Some of these actions may be irreversible. For example, if Customer grants someone permission that allows them to move data in Customer's repository to another account, Atlassian will not be able to recover the data without permission from the owner or administrator of the other account, as Atlassian is not in a position to arbitrate disputes among users. In that case, Customer's only recourse may be requesting a takedown under the guidelines for Reporting Copyright and Trademark Violations or pursuing legal action against the other user directly. For clarity, submitting a takedown request does not grant Customer access to the moved data or mean Atlassian can transfer that data back to Customer's repository.

* * * *

Jira Align

Effective starting: April 9, 2025

1. Interoperation with Third-Party Products. As an enterprise agility tool, Jira Align contains functionality or features designed to interoperate with, or that are contingent on access to or use of, other products, some of which may be provided by third parties. For clarity, Atlassian does not control and is not responsible for Customer's use of any such Third-Party Products.

2. Return Policy. If Customer exercises its rights under the "Return Policy" Section of the Agreement with respect to its initial Order of Jira Align, Atlassian will refund Customer any pre-paid, unused fees for Advisory Services for Jira Align purchased as part of such initial Order (and any corresponding Subscription Terms or consumption periods for such Advisory Services will be terminated).

3. Service Level Agreement for Jira Align Cloud.

3.1. Service Level Commitment. Atlassian must make Jira Align Cloud accessible to one or more Users at least 99.5% of the time during a calendar month (the "**Service Level Commitment**").

3.2. Service Credit Eligibility. To be eligible to receive a service credit for Atlassian's failure to meet the Service Level Commitment, Customer must submit a ticket at https://support.atlassian.com with all fields fully and accurately completed within thirty (30) days after the end of the calendar month in which the alleged failure occurred and provide any other reasonably requested information or documentation. Atlassian's monitoring and logging infrastructure is the sole source of truth for determining whether Atlassian has met the Service Level Commitment.

3.3. Service Credit Issuance. If Atlassian confirms a failure to meet the Service Level Commitment, Atlassian will apply the service credit (calculated as described in the table below) against a future payment due from Customer for Jira Align, provided that Customer's account is fully paid-up, without any overdue payments or disputes. No refunds or cash value will be given for unused service credits. Service credits may not be transferred or applied to any other Atlassian account or Product. The aggregate maximum service credit applied to an invoice will not exceed 100% of the amount invoiced for Jira Align in that invoice billing period (which, since service credits are applied to future payments, is not the month in which Jira Align was unavailable).

Monthly Uptime Percentage*	Service Credit (% of the monthly fees**)
Less than 99.5% but greater than or equal to 98.0%	5%
Less than 98.0% but greater than or equal to 95.0%	10%
Less than 95.0%	15%

* The monthly uptime percentage is determined by subtracting from 100% the percentage of minutes that Jira Align did not meet the Service Level Commitment out of the total minutes in the relevant calendar month. All calendar months are measured in the UTC time zone.

** The percentage of monthly fees attributable to Jira Align when purchased together with other Products under one SKU will be determined by Atlassian.

3.4. Service Credits and Reseller Purchases. If Customer purchased Jira Align through a Reseller, (a) Customer or the Reseller may submit a ticket as specified above; and (b) any service credits will be based on the fees invoiced by Atlassian to the Reseller for Customer's use of Jira Align under the Reseller's applicable order(s) with Atlassian. Atlassian will issue any associated service credits to the Reseller (not directly to Customer), and the Reseller will be solely responsible for issuing the appropriate amounts to Customer.

3.5. Exclusions. Customer is not entitled to a service credit if Customer is in breach of the Agreement or has not provisioned Jira Align. The Service Level Commitment does not include unavailability to the extent due to (a) Customer's use of Jira Align in a manner not authorized under the Agreement; (b) force majeure events or other factors outside of Atlassian's reasonable control, including internet access or related problems; (c) Customer equipment, software, network connections or other infrastructure; (d) Customer Data or Customer Materials (or similar concepts defined in the Agreement); (e) Third-Party Products; or (f) routine scheduled maintenance or reasonable emergency maintenance as stated in the Atlassian Maintenance Policy. The Service Level Commitment does not apply to (i) sandbox instances or Free or Beta Products (or similar concepts in the Agreement) or (ii) features excluded from the Service Level Commitment in the applicable Documentation.

3.6. Exclusive Remedy. Service credits are Customer's exclusive remedy and Atlassian's entire liability for Atlassian's failure to meet the Service Level Commitment.

4. Support for Jira Align Software. If Customer uses Jira Align as a Software Product, Customer must remain on the most recent release or the immediately prior release of Jira Align. Prior releases are not supported.

* * * *

Loom

1. Support, Specific Policies, and Documentation. For purposes of Loom:

1.1. Support Policy. "**Support Policy**" means the Loom support offerings documentation available here.

1.2. Return Policy. The "Return Policy" Section of the Agreement does not apply to Loom.

1.3. Documentation. "**Documentation**" means the content located here.

1.4. "Services." On any URL referenced in these Product-Specific Terms that is a child page of www.loom.com or www.loom.com/support, the term "Services" is replaced by the term "Loom."

2. Loom AI. Customer's use of any features or functionality made available as part of Loom or labeled as Loom AI that utilize data models trained by machine learning ("**Loom AI**") is subject to the following additional terms.

2.1. Definitions.

"**Input**" means any input provided by Customer or Users to be processed by Loom AI.

"**Loom AI Suite**" means the suite of Loom AI offerings as outlined on Loom's website, in the Documentation, or in the applicable Order for the Loom AI Suite.

"**Output**" means any output generated and returned to Customer or its Users by Loom AI based on the Input.

2.2. Customer Responsibilities.

(a) Input and Output. Input and Output are Customer Data. Customer must ensure that its Input, Output, and use of Loom AI does not (i) violate any Law; (ii) violate the Agreement or an applicable Order; or (iii) infringe, violate, or misappropriate any Atlassian or third-party rights. Customer acknowledges that due to the nature of machine learning and the technology powering Loom AI, Output may not be unique, and Loom AI may generate the same or similar output for third parties.

(b) Restrictions. Customer must not use Loom AI: (i) to mislead any person that Output was solely human generated; or (ii) in violation of OpenAI's Usage Policy, or any other third party terms, guidelines, policies or the like to which Loom links in connection with generation of Output.

(c) Atlassian recognizes that the use of Government data 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.

2.3. Disclaimer. **Atlassian does not make any warranty as to Loom AI, Output, the results that may be obtained from the use of Loom AI or the accuracy of any information obtained through Loom AI, including with respect to the factual accuracy of any Output or suitability for Customer's use case. Use of any material and/or data obtained through the use of any Loom AI feature is at Customer's sole risk. Customer should not rely on factual assertions in Output without independently fact checking their accuracy. No information or advice, whether oral or written, obtained by Customer from Atlassian or through Loom AI creates any such warranty.**

2.4 Responsible Use of AI Technologies. Atlassian will use commercially reasonable efforts to comply with its Responsibility Technology Principles. A copy of which is attached to the Agreement as Exhibit L and available at: https://www.atlassian.com/trust/responsible-tech-principles

* * * *

Opsgenie

1. **Intended Use**. Opsgenie is not intended for providing alerts on disaster scenarios or any other situations directly related to health or safety, including but not limited to acts of terrorism, natural disasters, or emergency responses, and Customer must not use Opsgenie for any such purposes.

2. **Service Level Agreement for Opsgenie**.

2.1. Service Level Commitment. Atlassian must make Opsgenie available at least 99.9% of the time during a calendar month (the "**Service Level Commitment**").

2.2. Service Credit Eligibility. To be eligible to receive a service credit for Atlassian's failure to meet the Service Level Commitment, Customer must open a case in the Opsgenie support center by the end of the second billing cycle after the cycle in which the incident occurred and provide the date and time of each alleged failure to meet the Service Level Commitment and any other reasonably requested information or documentation. Atlassian's monitoring and logging infrastructure, which consists of both internal and third party services, is the sole source of truth for determining whether Atlassian has met the Service Level Commitment.

2.3. Service Credit Issuance. If Atlassian confirms a failure to meet the Service Level Commitment, Atlassian will apply the service credit (calculated as described in the table below) against a future payment due from Customer for Opsgenie, provided that Customer's account is fully paid up, without any overdue payments or disputes. No refunds or cash value will be given for unused service credits. A service credit will be issued only if the credit amount for the applicable calendar month is greater than one U.S. dollar ($1 USD). Service credits may not be transferred or applied to any other Atlassian account or Product. The aggregate maximum service credit applied to an invoice will not exceed 100% of the amount invoiced for Opsgenie in that invoice billing period (which, since service credits are applied to future payments, is not the month in which Opsgenie was Unavailable (as defined below)).

Monthly Uptime Percentage*	Service Credit (% of the monthly fees)
Less than 99.9% but greater than or equal to 99.0%	5%
Less than 99% but greater than or equal to 97.0%	10%
Less than 97.0%	20%
***** The monthly uptime percentage is determined by subtracting from 100% the percentage of Unavailable minutes out of the total minutes in the relevant calendar month. All calendar months are measured in the UTC time zone. "**Unavailable**" means that Opsgenie was not able to process incoming alerts and send notifications within five (5) minutes of receiving the alerts, according to the policies and notification rules defined by Customer within the Opsgenie service.	

2.4. Service Credits and Reseller Purchases. If Customer purchased Opsgenie through a Reseller, (a) Customer or the Reseller may open a case as specified above; and (b) any service credits will be based on the fees invoiced by Atlassian to the Reseller for Customer's use of Opsgenie under the Reseller's applicable order(s) with Atlassian. Atlassian will issue any associated service credits to the Reseller (not directly to Customer), and the Reseller will be solely responsible for issuing the appropriate amounts to Customer.

2.5. Exclusions. Customer is not entitled to service credits if Customer is in breach of the Agreement or has not provisioned Opsgenie. The Service Level Commitment does not include unavailability to the extent due to: (a) Customer's use of Opsgenie in a manner not authorized under the Agreement; (b) force majeure events or other factors outside of Atlassian's reasonable control, including internet access or related problems; (c) Customer equipment, software, network connections or other infrastructure; (d) Customer Data or Customer Materials (or similar concepts defined in the Agreement); (e) Third-Party Products; or (f) routine scheduled maintenance. The Service Level Commitment does not apply to (i) sandbox instances or Free or Beta Products (or similar concepts in the Agreement) or (ii) features excluded from the Service Level Commitment in the applicable Documentation.

2.6. Exclusive Remedy. Service credits are Customer's exclusive remedy and Atlassian's entire liability for Atlassian's failure to meet the Service Level Commitment.

* * * *

Statuspage

1. Status Pages and Scope of Use.

1.1. Status Pages. Statuspage enables Customer to create pages hosted by Atlassian that display both current and historical status and uptime information of Customer's products and services, while also allowing Users to subscribe to status notifications ("**Status Pages**"). There are different types of Status Pages and different subscription plans for each of these page types. This includes Status Pages that are available to the public, meaning they are not confidential or private to Customer.

1.2. Scope of Use. Customer's Scope of Use (and the related fees) may vary depending on Status Page type and plan. See more information here.

2. Status Page Configuration. As described in the Documentation, Customer may configure its Status Pages by including look and feel elements (like company brand or logo) and any links or permissions required to collect information from individuals (internal or external to Customer) who view a Status Page ("**Statuspage End Users**") or for these individuals to acknowledge that they are subscribing to status notifications (collectively, "**Customer Configurations**"). Customer Configurations are "Customer Data" under the Agreement.

3. Collection of Statuspage End User Information. As discussed above, Statuspage allows Customer to collect information from Statuspage End Users in order to send these end users status notifications. This may include email addresses and phone numbers. Statuspage End Users are Customer's Users under the Agreement, and any information collected about Customer's Statuspage End Users is "Customer Data" under the Agreement.

* * * *

Trello

1. Settings, Profile Information and Free Plans.

1.1. Settings and Profile Information. Trello permits users to collaborate via workspaces, boards and cards and includes certain membership and privacy settings that may differ according to Customer's Trello plan. These settings may include designating who can access or view Customer's Trello workspaces, boards and cards. Customer is responsible for configuring these settings. For instance, where a workspace is "public," it is available to the public, meaning it (and any Customer Data it contains) is not confidential or private to Customer. In addition, profile information within Trello (for instance, a User's username, full name, avatar and bio) is available to the public.

1.2. Free Plans. For clarity, the Subscription Term for free Trello plans continues until the applicable plan (and any associated workspace) is terminated.

2. Account Activity. Atlassian may make boards "private" where Atlassian would otherwise have rights to limit access to or remove Customer Data or suspend access to Trello under the Agreement. Atlassian may create limits on use and storage at any time with or without notice for free Trello plans. If Customer's plan is terminated, Atlassian may withdraw and reallocate the public web address of the corresponding workspace(s). Atlassian may also log off users who are inactive for an extended period of time.

3. Power-Ups and Featured Power-Ups.

3.1. Power-Ups. Atlassian may make available or provide links to optional tools and other features or services that Customer may enable for use with Trello, called "Power-Ups" ("**Power-Ups**"). Power-Ups may be provided by third parties ("**Third-Party Power-Ups**") or by Atlassian ("**Trello Power-Ups**"). Third-Party Power-Ups are Third-Party Products, and Trello Power-Ups are Free or Beta Products. There may be limits on the number of Power-Ups Customer may use based on Customer's applicable Trello plan. For certain Power-Ups, Customer must obtain a subscription to the third-party product or service integrated with Trello or pay a fee to enable the Third-Party Power-Up. Atlassian or the third-party provider of a Power-Up may update, modify or remove the Power-Up at any time. Atlassian does not make any promises or guarantees about future price, availability or functionality of Power-Ups.

3.2. Featured Power-Ups. From time to time, Atlassian may feature certain Power-Ups more prominently than others on its website (for instance, by designating Power-Ups as "Featured," "Essential" or "Taco's Picks"). This may be based on popularity in the Trello community or positive user reviews. In so featuring a Power-Up, Atlassian does not endorse, or make any warranty or guarantee regarding, the Power-Up.

Exhibit F

ATLASSIAN

Acceptable Use Policy

Effective starting: The earlier of (i) October 6, 2024 and (ii) the date the Atlassian Intelligence and Rovo Product-Specific Terms are effective

Here at Atlassian, our goal is to help you and your team do the best work of your lives, every day. To do this, we need to keep our products and services running smoothly, quickly, and without distraction. For this to happen, we need help from you, our users. We need you not to misuse or abuse our products and services.

To describe exactly what we mean by "misuse" or "abuse" – and help us identify such transgressions and react accordingly – we've created this Acceptable Use Policy. Under this policy, we reserve the right to take action if we see objectionable content that is inconsistent with the spirit of the guidelines, even if it's something that is not forbidden by the letter of the policy. In other words, if you do something that isn't listed here verbatim, but it looks or smells like something listed here, we may still take action.

You'll see the word "services" a lot throughout this page. That refers to all products and websites owned or operated by Atlassian, and any related websites, sub-domains and pages, as well as any cloud services operated by Atlassian.

Use your judgment, and let's be kind to each other so we can keep creating great things. You can find all the legal fine print at the bottom of this page.

Here's what we won't allow:

Disruption

- Compromising the security or operation of our systems. This could include probing, scanning, or testing the vulnerability of any system or network that hosts our services. This prohibition does not apply to security assessments expressly permitted by Atlassian
- Tampering with, reverse-engineering, or hacking our services, circumventing any security or authentication measures, or attempting to gain unauthorized access to the services, related systems, networks, or data
- Modifying, disabling, or compromising the integrity or performance of the services or related systems, network or data
- Deciphering any transmissions to or from the servers running the services
- Overwhelming or attempting to overwhelm our infrastructure by imposing an unreasonably large load on our systems that consumes extraordinary resources (CPUs, memory, disk space, bandwidth, etc.), such as:
    - Using "robots," "spiders," "offline readers," or other automated systems to send more request messages to our servers than a human could reasonably send in the same period of time by using a normal browser
    - Going far beyond the use parameters for any given service as described in its corresponding documentation
    - Consuming an unreasonable amount of storage for music, videos, or other content in a way that's unrelated to the purposes for which the services were designed

Wrongful activities

- Misrepresentation of yourself, or disguising the origin of any content (including by "spoofing", "phishing", manipulating headers or other identifiers, impersonating anyone else, or falsely implying any sponsorship or association with Atlassian or any third party)
- Using the services to violate the privacy of others, including publishing or posting other people's private and confidential information without their express permission, collecting or gathering other people's personal information (including account names or information) from our services, or inferring characteristics or personal information (including sensitive information) about other people using our services
- Using our services to stalk, harass, bully, intimidate, or post direct, specific threats of violence against others

- Using the services in furtherance of any illegal purpose, or in violation of any laws (including without limitation data, privacy, and export control laws)
- Accessing or searching any part of the services by any means other than our publicly supported interfaces (for example, "scraping")
- Using meta tags or any other "hidden text" including Atlassian's or our suppliers' product names or trademarks
- Using the services for the purpose of providing alerts on disaster scenarios or any other situations directly related to health or safety, including but not limited to acts of terrorism, natural disasters, or emergency response
- Using the services to engage in, promote or facilitate practices or behaviors that could lead to discriminatory, unfair or harmful treatment of individuals or groups of people, particularly on the basis of sensitive or protected attributes or characteristics

Inappropriate communications

- Using the services to generate or send chain letters or spam
- Soliciting our users for commercial purposes, unless expressly permitted by Atlassian
- Disparaging Atlassian or our partners, vendors, or affiliates
- Promoting or advertising products or services other than your own without appropriate authorization

Inappropriate content

- Posting, uploading, sharing, submitting, using the services to generate, facilitate, promote, or otherwise provide content that:
    - Violates or infringes Atlassian's or a third party's intellectual property or other rights, including any copyright, trademark, patent, trade secret, moral rights, privacy rights of publicity, or any other intellectual property right or proprietary or contractual right, or where we receive notice of alleged violation or infringement in accordance with our Reporting Guidelines
    - You don't have the right to submit
    - Is false, misleading, deceptive, fraudulent, illegal, obscene, defamatory, libelous, threatening, harmful, sexually explicit (including child sexual abuse or exploitation material, which we will remove and report to law enforcement and the National Center for Missing and Exploited Children), indecent, harassing, or hateful
    - Depicts or encourages serious harm or any form of violent, illegal, tortious, fraudulent, malicious, or dangerous conduct
    - Attacks or discriminates against others based on their race, ethnicity, national origin, religion, sex, gender, sexual orientation, disability, medical condition, or other similar status
    - Contains viruses, bots, worms, scripting exploits, or other similar materials
    - Is intended to be inflammatory
    - Could otherwise cause injury, damage, death, or credible risk of harm to Atlassian, the services, its users, or any third party
    - Has been previously removed for violating the policy

Artificial intelligence offerings and features

When you use any of our artificial intelligence offerings and features, such as Atlassian Intelligence, Rovo and Loom AI, we also won't allow any use of those services to:

- Seek or provide advice that would ordinarily be provided by a qualified or licensed professional, including legal, medical/health, financial or other professional advice of any kind
- Make automated decisions with legal or similarly significant effects, including in any domains that may affect an individual's rights, safety, health or well-being (for example, in the domains of finance, credit, insurance, employment, housing, education, essential services, law or law enforcement, migration, management of critical infrastructure, judicial proceedings or social scoring)
- Engage in political campaigning or lobbying, including generating campaign materials to influence a political process, or to interfere with participation in electoral, democratic or civic processes
- Mislead individuals into believing that they are communicating with a human when they are not, or claim that content generated through our artificial intelligence offerings and features was generated by a human

In the context of using our artificial intelligence offerings and features, we consider it a violation of this policy if you use those services to:

- Seek to override or circumvent the technical or safety measures designed to safeguard our services, or intentionally prompt our services to act in a manner that violates this policy
- Depict or impersonate any other individual or organization without their consent, authorization or legal right to do so
- Engage in, generate or promote disinformation, misinformation, false online engagement (such as fake reviews), plagiarism or academic dishonesty
- Engage in erotic, romantic or sexually explicit chat with any of our artificial intelligence offerings and features

In this Acceptable Use Policy, the term "**content**" means: (1) any information, data, text, software, code, scripts, music, audio, sound, images, graphics, videos, recordings, messages, tags, interactive features, or other materials that you create, post, upload, share, submit, or otherwise provide in any manner to the services and (2) any other materials, content, or data you provide to Atlassian or use with the services. "**Content**" also includes submissions by others that you authorized or facilitated to use the services.

Atlassian reserves the right to interpret the guidelines and take (or refrain from taking) action in its discretion. Without affecting any other remedies available to us, Atlassian may permanently or temporarily remove or disable access to unacceptable content, without notice or liability if Atlassian (in its discretion) determines that a user has violated this Acceptable Use Policy. You agree to cooperate with us to investigate and remedy any violation.

Exhibit G

Advisory Services Policy

Effective starting: January 8, 2025

This Advisory Services Policy (this "**Policy**") supplements the Atlassian Customer Agreement, or another agreement entered between Customer and Atlassian (the "**Agreement**") and governs Atlassian's provision of advisory services in connection with Atlassian Products ("**Advisory Services**"). This Policy controls in the event of a conflict with the Agreement. Capitalized terms used and not defined in this Policy have the meanings given to them in the Agreement.

Advisory Services include (a) standalone service offerings (such as plays, assessments and workshops) ("**Catalog Services**") and (b) subscription plans ("**Subscription Services**"). A full description of the Advisory Services offerings is available here, as updated from time to time. The scope of particular Advisory Services is indicated in the Order and in the applicable Advisory Services datasheet (available via the link above).

1. Subscription Term and Consumption Period.

1.1. Subscription Services. Subscription Services begin on the start date indicated in the applicable Order and are provided on a continuing basis for the duration of the Subscription Term. Any Subscription Term for Advisory Services may only be renewed by mutual written agreement of the parties. Any renewal terms and conditions, including pricing, are subject to change.

1.2 Catalog Services. Catalog Services must be consumed within 12 months from the date of the Order. After this period, Customer will no longer have any access to the Catalog Service.

2. Availability of Advisory Services Representatives. Advisory Services are offered during Business Hours (as defined below) and are delivered by Atlassian product specialists such as engagement managers, solution strategists and/or technical architects (each, an "**Advisory Services Representative**") following a kick-off meeting to be scheduled within 30 days from the date of the Order or the start of the Subscription Term, whichever is later. Atlassian may designate different Advisory Services Representatives to provide Advisory Services (or portions of Advisory Services), depending on the particular services and Atlassian Products in scope. Advisory Services may be provided remotely or, for certain types and/or Subscription Services plans, on site, in each case, on a schedule mutually agreed between Atlassian and Customer's Account Representatives (as defined below). More information regarding on-site services delivery is included in Section 5 (Travel & Living Expenses). For Subscription Services, Advisory Services Representatives will be available to provide the Subscription Services for up to the number of hours per three-month period specified in the table below. "**Business Hours**" means 9 am to 5 pm in a mutually agreed primary location for service delivery on any day that is not an Atlassian-designated holiday or weekend in such location.

Tier of Subscription Services	Hours per Three-Month Period*
Essential	60
Signature	140
Elite	230
* Hours not consumed in a given three-month period cannot be banked, accumulated or saved for subsequent periods	

3. Account Representatives. Customer must designate up to two individuals to serve as key points of contact with the Advisory Services team (the "**Account Representatives**"). Customer must submit all requests through its Account Representatives, and Atlassian will rely and act upon each Account Representative's instructions. Customer must ensure that the Account Representatives have baseline technical knowledge of the Products associated with the Advisory Services.

4. Limitations of Advisory Services. Fees for Advisory Services are to secure the availability, time and effort of Advisory Services Representatives. Atlassian will use commercially reasonable efforts to provide Advisory Services in a professional manner and to address Customer requests, but Atlassian does not guarantee resolution of such requests. Actual areas of advice and guidance will depend on the ordered Advisory Services, as well as on Customer's requests and needs. Topics that are not explicitly listed in an Advisory Services description or in an applicable Advisory Services datasheet are outside the scope of the related services.

5. Travel & Living Expenses. As indicated in the table below, certain Advisory Services offerings include on-site services.

Advisory Services	Tier or Type	Included On-Site Visits*
Subscription Services	Signature	Two
Subscription Services	Elite	Four
Catalog Services	For Jira Align (workshops)	Two
* Each on-site visit to be for two business days unless otherwise agreed		

Otherwise, on-site services are not included in the Advisory Services unless agreed on a case-by-case basis. In such case, any pre-approved travel, lodging and meal expenses incurred by an Advisory Services Representative may be invoiced directly to Customer, at minimum monthly, and Customer will reimburse Atlassian for those expenses in accordance with the payment terms in the applicable Order for the Advisory Services.

6. Catalog Services.

6.1. General. Catalog Services are standalone service offerings (such as plays, assessments and workshops) to discuss the design and implementation of Customer's deployment of Atlassian Products or solutions, as described in the applicable Catalog Services datasheet.

6.2. Jira Align. In the case of workshop Catalog Services for Jira Align, the services include demonstration of how Jira Align will work with a compatible product (like Jira Software) specified here, as updated from time to time (each, a "**Compatible Product**"). Certain aspects of Catalog Services delivery for Jira Align cannot begin until Customer establishes connectivity between one Compatible Product and one Jira Align instance so that data is able to transit between the Compatible Product and Jira Align ("**System and Data Connectivity**"). Customer is solely responsible for establishing the required System and Data Connectivity, and Section 1.2 (Catalog Services) applies. In addition, if Customer orders workshop Catalog Services for Jira Align through an authorized partner or reseller, all or any portion of the services may be provided by such partner or reseller.

6.3. Refund Policy. Customer may request a refund for Catalog Services if Customer provides notice to Atlassian via Customer's Account Representative within 30 days of the date of the Order and before Atlassian has commenced delivery.

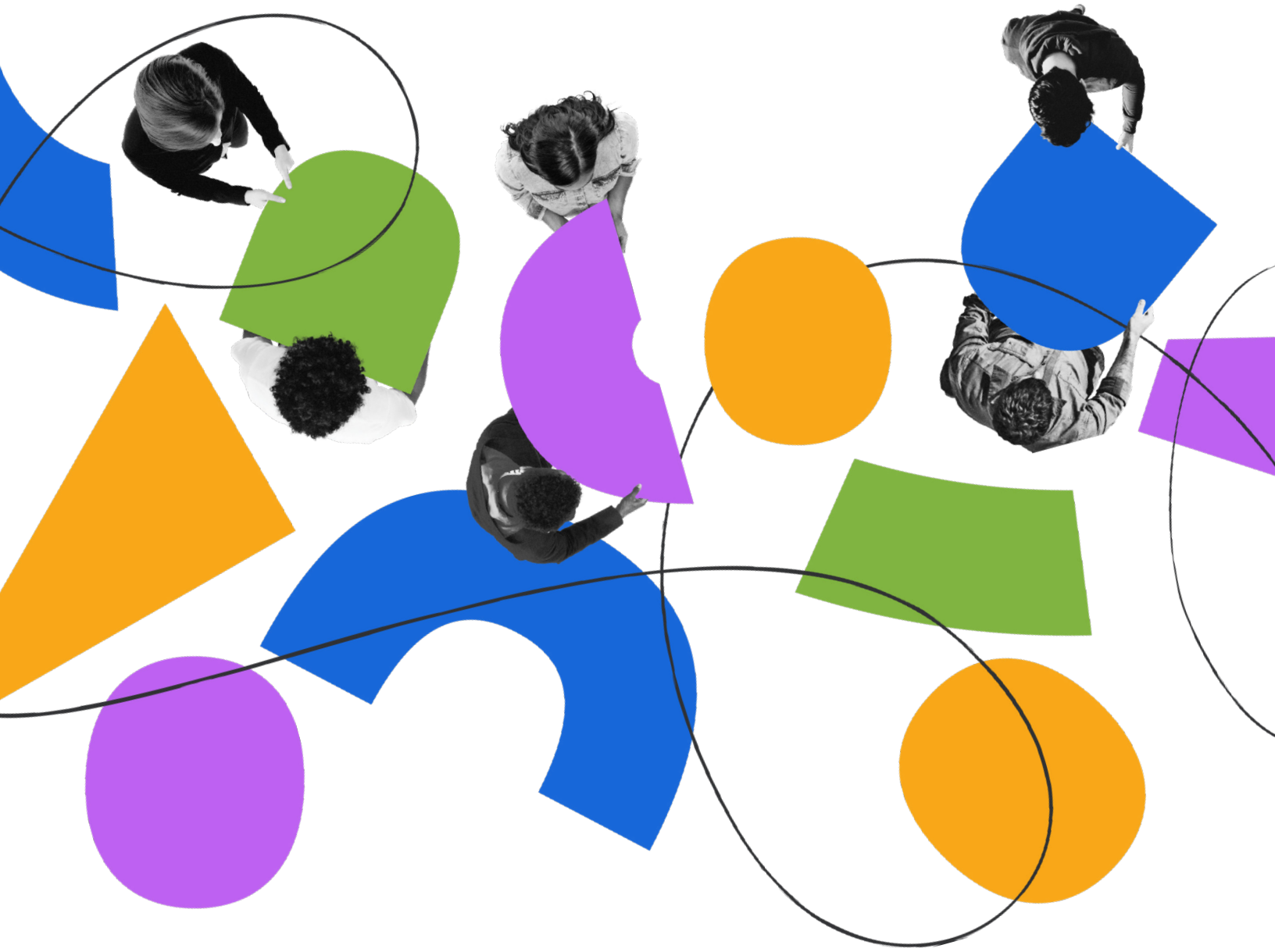
7. Change Control Procedure. Changes to an Advisory Services engagement may be made only in a writing executed by both parties, and Atlassian has no obligation to commence work in connection with any change request until such time.

8. Customer Use Rights. As part of the Advisory Services, Atlassian may provide reports, analyses, templates, technology, or other deliverables. Customer may use such deliverables only as part of its authorized use of the Products.

Exhibit H

ATLASSIAN

Code of Business Conduct and Ethics



Atlassian's mission is to unleash the potential of every team, and we must act with integrity to achieve it. Each of us is responsible for behaving ethically, honestly, and respectfully. Each of us has a part to play – our employees, directors, officers, agents, partners, representatives, contractors, and consultants.

Our unique values describe what we stand for at the most fundamental level. They shape our culture and influence who we are, what we do, and even who we hire. They're hard-wired into our DNA and will stay the same as we continue to grow.

Open company, no bullshit

Build with heart and balance

Don't #@!% the customer

Play, as a team

Be the change you seek

Our values are reflected in the Atlassian Code of Business Conduct and Ethics. The Code guides our actions across every part of the company, from our Board of Directors to our interns.

In addition to Atlassian's policies and practices, the Code addresses how to properly interact with people and organizations. We are all responsible for holding our contractors, consultants, partners, suppliers, and every Atlassian to the standards in our Code. Our future success depends on following these principles and taking them seriously. Without them, we risk creating significant liability for Atlassian and even threatening our ability to do business.

So please ensure you familiarize yourselves with the Code and remember that we expect you to know and comply with the legal requirements relating to your job and the services you are providing to Atlassian. We trust and expect you to use common sense and the highest ethical standards when making business decisions – even when there is no stated guideline.

Above all, we should always focus on doing the right thing. We all have a role to play.

Mike Cannon-Brookes
CEO and Co-Founder, Atlassian

Content

01 Prioritize Ethics & Compliance

This Code applies to Atlassian employees, directors, officers, partners, representatives, contractors, and consultants.

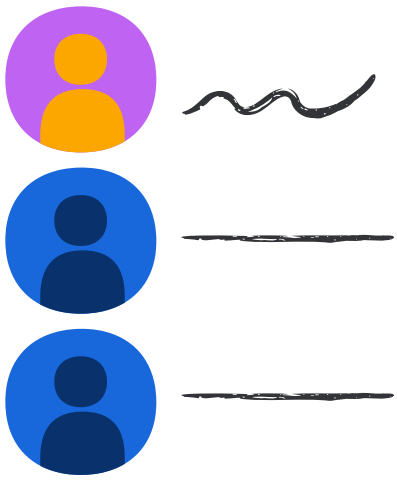
Atlassian takes compliance with applicable laws, rules, and regulations seriously. You are prohibited from engaging in any unlawful activity when conducting Atlassian business or in carrying out your day-to-day duties or services.

It is your responsibility to read, understand, and acknowledge this Code (including the policies, standards, and guidelines referenced in the Code) on an annual basis or as requested by Atlassian. This Code does not change any legal or contractual obligations that you may otherwise have with Atlassian. Instead, the standards in this Code should be viewed as the minimum standards that Atlassian expects from you. Also, as a global company, Atlassian expects that you will comply with all local laws and customs of the location where you work or visit.

MANAGERS ARE ROLE MODELS

Managers at all levels are responsible for being role models for ethical behavior and ensuring that employees reporting to them understand and comply with Atlassian's Code, policies, and practices. This includes making sure that they complete all required training. Here are your responsibilities as a manager:

- Review the Code at least annually
- Regularly reinforce and discuss the Code with team members
- Promptly seek guidance from your own manager or business partners if you have any questions
- *Promptly report* violations of the Code, policies, and practices



Reporting Possible Violations

We rely on you to recognize potential problems and ask questions if you are ever unsure about the appropriateness of an action or occurrence. Whenever you are unsure, always ask.

> Be proactive if you believe this Code, any of Atlassian's policies or practices, or the law are being violated. You have an obligation to report this. But please do not conduct your own investigation.

If you have a question or would like to report a violation, please read Reporting Concerns & Receiving Advice below. It explains how reports can be made.

Non-Retaliation & Disciplinary Action

You should feel free to ask questions or make a report without fear of retaliation. We will not tolerate retaliation against anyone who reports a suspected violation in good faith or cooperates in an investigation. Anyone who engages in any form of retaliation will be subject to disciplinary action, which may include termination of employment or services. If you believe you have been subject to retaliation as a result of reporting a suspected violation in good faith, please report it immediately to the resources listed at Reporting Concerns & Receiving Advice.

WHAT IF I MAKE A REPORT ABOUT A SUSPECTED VIOLATION AND I AM WRONG?

If you made the report in good faith and believe that the information provided is accurate, you will not be subject to disciplinary action. You do not need to be right – but you do need to believe that the information you are providing is truthful.

Standards of Conduct

We want to ensure that Atlassian is a place where our team can thrive. We expect you to follow basic, common-sense rules of conduct that will protect everyone's interests. If you are found to have violated this Code or any of the policies or practices referenced in it, you will be subject to disciplinary action, up to and including termination of your employment or services.

02 Treat Others Respectfully

Consistent with our values, we strive to create an environment that is open, supportive, and safe.

> Respect for others should always be prioritized in your in-person and online interactions with others, whether they be colleagues, partners, suppliers, customers, or the general public.

Equal Opportunity: Anti-Discrimination, Harassment, Bullying, & Retaliation

Atlassian's Play, as a Team value demands that we treat each other with respect, dignity, and professionalism. We care about our community, and we're counting on you to help ensure a safe and comfortable environment for all Atlassians, which is made up of individuals with diverse beliefs and viewpoints.

Every Atlassian has the right to work in an environment that is respectful, professional, and free from all forms of discrimination, harassment, bullying, and retaliation. Atlassian expects that all interactions among Atlassians, either in person or over digital spaces, will be business-like and free of bias, prejudice, and harassment. The same is required when Atlassians interact with our community, customers, and partners. In addition to being the right thing to do, this is key to upholding our responsibility to respect human rights. We will not tolerate discrimination against or harassment of employees, consultants, contractors, or customers based on any characteristic protected by law, such as age, gender, gender identity, sexual orientation, race, national origin, citizenship, or disability. You can find more information at Policy – Equal Employment Opportunity: Anti-Discrimination, Harassment, Bullying, and Retaliation.

If you witness or experience discrimination, harassment, bullying, or retaliation, please report it immediately to any of the available resources listed in the Policy – Grievance. The channels described in Policy – Grievance are appropriate for submitting matters concerning unfair treatment in an Atlassian work environment that causes undue concern, distress, or a feeling of injustice.

Maintaining Health & Safety

Atlassian is committed to maintaining a healthy, safe, and productive workplace. This requires your continuous cooperation. If you have any health or safety concerns, you should immediately contact your manager and Workplace Experience Team. If a work-related injury occurs, please immediately report it and follow the instructions on how to make a report at Policy – Workplace Health and Safety.

Drugs, Controlled Substances, & Alcohol

Being under the influence of a drug or alcohol while on company premises or while conducting company business may interfere with a safe and healthy work environment and may pose serious risks to the user and to those around them.

We expect you to act responsibly when it comes to consuming alcohol. You represent Atlassian – whether in the office, at an after-hours work activity, an offsite, or Atlassian-sponsored event. Never drink to the point of impairment or in a way that may lead to inappropriate behavior or endanger the safety of others. Regardless, always follow the local laws of your location.

Atlassian has a zero-tolerance policy against illegal drugs. Employees are not allowed to possess, trade, or use illegal drugs or report to work under the influence of illegal drugs. Please read Atlassian's Policy – Alcohol and Drug Use for more information.

Weapons & Violence

Atlassian is committed to a violence-free work environment. We do not tolerate any level of violence or the threat of violence in the workplace. Under no circumstances should you bring a weapon to work, a customer site, or any other offsite location where Atlassian business is conducted. In case of potential violence or danger, immediately contact local law enforcement and report it to your manager and employee-relations@atlassian.com.

Communications with Others

Our values and our products encourage open communication. However, we must all be cognizant of how our communications are received and interpreted within and outside of Atlassian and our responsibilities listed in Policy – Equal Employment Opportunity: Anti-Discrimination, Harassment, Bullying, and Retaliation. When you post on social media, whether through an official Atlassian account or not, please first read the Atlassian Social Media Guidelines.

We expect our internal and external communications to reinforce Atlassian values:

- Communication and content shared between Atlassians should be respectful and in line with our Play, As a Team value
- All Atlassians deserve to work in an environment where they feel safe and like they belong on the TEAM
- In an open company, we must consider our impact - this requires each team member to take ownership of both the intent and impact of their actions on their teammates.

Check out the Global - Community Guidelines for more information.

03 Engage in Ethical Business Practices

Free & Fair Competition

Competing vigorously, yet lawfully, with competitors and establishing advantageous, but fair, business relationships with customers and suppliers is a part of the foundation for Atlassian's long-term success. On the other hand, unlawful and unethical conduct, which may lead to short-term gains, may damage Atlassian's reputation and long-term business prospects. You must deal ethically and lawfully with the company's customers, suppliers, competitors, and employees in all business dealings on the company's behalf. You should not take unfair advantage of another person through the abuse of privileged or confidential information or through improper manipulation, concealment, or misrepresentation of material facts.

No Insider Trading

If you learn of any material, nonpublic information about Atlassian or any other company (for example, a customer, supplier, or other party with which Atlassian is negotiating a major transaction, such as an acquisition, investment, or sale), you may not trade in Atlassian's securities or that other party's securities or "tip" others who might make an investment decision based on such information until the information becomes public or is no longer material.

Information is "material" if there is a substantial likelihood that a reasonable investor would consider it important in making a decision to buy, sell, or hold a security and it is "nonpublic" if it has not been disseminated in a manner making it available to investors generally. Trading stock or encouraging others to trade stock on the basis of material nonpublic information, regardless of how small or large the trade, may constitute insider trading, insider dealing, or stock tipping and constitute a criminal offense in most countries where we do business and a violation of U.S. federal securities law.

Like many public companies, Atlassian has adopted specific trading restrictions to guard against insider trading. Do not confuse these trading restrictions with the broader prohibition on trading when in possession of material nonpublic information. In other words, the company's "trading window" may be open but you may nonetheless be in possession of material nonpublic information that makes it inappropriate to trade. For more information, please read Policy – Insider Trading and Disclosure.

Anti-Bribery

We are committed to complying with all anti-bribery laws, including the United States Foreign Corrupt Practices Act (FCPA) and the United Kingdom Bribery Act. Any form of bribery, direct or indirect, is strictly prohibited. That means you must not offer a bribe to, or accept one from, any person, at any time, for any reason. Any third party, supplier, contractor, consultant, agent, or intermediary acting on Atlassian's behalf is also prohibited from offering, giving, or accepting bribes. You have a continuing and independent obligation to ensure compliance with these laws and Atlassian's Policy – U.S. Foreign Corrupt Practices Act and Anti-Corruption.

> Cultural "norms" are never an excuse to make a bribe.

Failure to comply with the FCPA, the Bribery Act, and other similar anti-corruption laws may result in civil and/or criminal fines and penalties to Atlassian, as well as significant harm to the company's reputation. It may also result in civil and criminal penalties being imposed against any company personnel, agents, and business partners involved. Your non-compliance with the Policy – U.S. Foreign Corrupt Practices Act and Anti-Corruption will result in disciplinary action being taken, up to and including termination of employment or services.

Dealing with Public or Government Officials

When Atlassian does business with any government entity, state-owned enterprise, or public international organization on a country, state, or local level, we must abide by all applicable laws and regulations related to these types of transactions. In dealing with public sector customers in the United States or other countries, you are required to understand the special rules that may apply. Please read Policy – U.S. Foreign Corrupt Practices Act and Anti-Corruption for more information on what is appropriate. If you seek an exception to this rule (the approval of which will be rare), please see the Compliance Officer (Atlassian has designated its Deputy General Counsel - Corporate as its Compliance Officer for the purposes of this Code).

> Never provide a gift, including meals, entertainment, or other items of value, to a government official

Customers, Partners, and Suppliers

We expect that our customers, partners, suppliers, and other third parties (we call them "business partners" in this section) will comply with all laws and act ethically in all respects. In light of that, when you engage any business partners, consider how they align with our values and conduct their businesses.

> Select good business partners. Who we do business with directly impacts our reputation and may have legal and business implications.

Many business partners will represent Atlassian and may be a customer's or the public's only interaction with Atlassian. When engaging a business partner, only select those parties who you trust will represent Atlassian well and that are aligned with our values. Watch out for suspicious business practices, which include:

- refusals to provide information about a partner or consultant's end customers
- requests for commissions that are unusually large in relation to the work to be performed
- references by local agents to "special accommodations" that have to be made with local officials or statements that you should not ask too many questions about how business gets done in the local jurisdiction
- hesitation on the part of agents or consultants to provide the details of the services to be performed and statements that they will "do what it takes to get the deal done" in the local jurisdiction
- requests for "up front" payments when such payments are not expressly required by a written business agreement
- requests for payment to an offshore bank account, in cash, in a different name, to a shell corporation, to an account in a different country, through private payment procedures, or to an unrelated third party
- refusal by a prospective agent to commit to comply with Atlassian's compliance policies
- refusal to submit to or respond to Atlassian's due diligence requests without a reasonable explanation
- refusal by a consultant to provide written reports of its activities
- a history of illegal or questionable behavior by a prospective consultant
- family or business relationships between Atlassian's agent and government officials
- proposals for consulting or lobbying contracts by persons who claim to have "special arrangements" with government officials
- requests for commission payments prior to announcement of an award decision
- requests by government officials that specific parties be engaged to provide services or materials to Atlassian
- requests that Atlassian bid for services to be made through a specific representative or partner

04 Avoid Conflicts of Interest

Atlassian recognizes and respects that you have responsibilities and interests outside of work. However, it is your responsibility to avoid situations where a conflict of interest could occur with respect to your obligations to Atlassian.

> Generally, a conflict of interest exists when a personal interest or activity interferes, or appears to interfere, with your professional judgment or your responsibilities to Atlassian.

Transparency is key. Even the appearance of a conflict of interest can be damaging and harmful to Atlassian and your reputation. Such a conflict may arise directly, or indirectly, as a result of the personal interests or activities of a family member (or significant other) or organization with which you are affiliated.

> If you think you might be faced with a conflict of interest, it is important to address the situation immediately. Talk to your manager or the Compliance Officer, immediately cease the activity until you confirm whether a conflict exists, and remove yourself from any decision-making responsibilities that are related to the conflict.

You have an obligation to conduct Atlassian's business in an honest and ethical manner, including the ethical handling of actual or apparent conflicts of interest between personal and professional relationships. Any transaction or relationship that reasonably could be expected to give rise to a conflict of interest should be reported promptly to the Compliance Officer. The Compliance Officer may notify the Board of Directors or its Audit Committee as they deem appropriate.

Members of the Board of Directors should disclose actual or potential conflicts of interest in accordance with Atlassian's Policy – Related Person Transactions and, if necessary, seek the appropriate authorization for the conflict situation. Actual or potential conflicts of interest involving an executive officer other than the Compliance Officer should be disclosed directly to the Compliance Officer. Actual or potential conflicts of interest involving the Compliance Officer should be disclosed directly to the Chief Financial Officer.

WHERE CAN CONFLICTS OF INTEREST ARISE?

Some examples include:

- Competing with Atlassian by working for a competitor
- Accepting gifts from (or offering gifts to) customers, suppliers, partners, government representatives, or public organizations
- Personally benefiting from Atlassian's property or information or your position at Atlassian

Outside Employment & Other Affiliations

We are proud of Atlassians' innovative spirit and curiosity and recognize it's what makes you a great part of Atlassian. However, employees may not work at another company as an employee, independent contractor, or consultant, or serve on its board of directors, where the affiliation gives or appears to give rise to a conflict of interest or interferes with your ability to perform services for Atlassian. For example, you are prohibited from simultaneous employment with a competitor of Atlassian or from participating in any activity that enhances or supports a competitor's position. If you are unsure if your outside work or affiliation with an outside interest could create or appear to create a conflict of interest, please review Atlassian's Global – Guidelines for Outside Activities.

Serving on a Board of Directors

In general, Atlassian employees are prohibited from serving on the board of directors of competitors but may be permitted to serve as a board member of other entities, including non-profit organizations. If you are considering serving on a board of directors, discuss it with your manager, read Atlassian's Global – Guidelines for Outside Activities, and follow the Guidelines' instructions for requesting approval.

Financial Interests in Other Businesses

> You may not have a personal or family financial interest in an Atlassian customer, channel partner, supplier, other business partner, or competitor that could improperly influence your judgment, has the potential to cause the appearance of divided loyalty, or might result in personal benefit because of your role at Atlassian. Financial interests include investment, ownership, or creditor interests.

Many factors may be considered in determining whether a conflict situation exists, including the size and nature of the investment, your ability to influence Atlassian decisions or decisions by third parties affecting Atlassian, your access to Atlassian confidential information or of the other company, and the nature of the relationship between Atlassian and the other company.

Personal Benefit or Gain from Business

> Conflicts of interest may also occur when you or an immediate family member receive some personal benefit in connection with any transaction involving Atlassian or as a result of your position at Atlassian.

There are limited exceptions to this rule described in the Gifts and Entertainment section below. In addition, you must disclose to the Compliance Officer all situations where you may be conducting Atlassian business with members of your family, your friends, or others with whom you have a close personal relationship.

Corporate Opportunities

You should not knowingly pursue or participate in a business opportunity where Atlassian has an interest or which is closely related to Atlassian's current business or its anticipated future plans. You should not take advantage personally of business or investment opportunities that are discovered through the use of Atlassian property, business or information. If you believe you may be pursuing such an opportunity, disclose it to the Compliance Officer.

Political Contributions

Business contributions to political campaigns are strictly regulated by federal, state, provincial, and local law in Australia, the United Kingdom, the United States, and other jurisdictions where Atlassian operates. Accordingly, all political contributions proposed to be made with Atlassian's funds or on Atlassian's behalf must be coordinated through and approved by the Compliance Officer. You may not, without the approval of the Compliance Officer, use any of Atlassian's funds for political contributions of any kind to any political candidate or holder of any national, state, provincial, or local government office. You may make personal contributions but should not represent that you are making any such contribution at Atlassian's request or on Atlassian's behalf. Similar restrictions on political contributions may apply in other countries. Specific questions should be directed to the Compliance Officer. You may not receive any reimbursement from corporate funds for a personal political contribution.

Gifts & Entertainment When Dealing with Non-Governmental or Non-Public Third Parties

> Atlassian expects that you will use good judgment, discretion, and moderation when giving or accepting gifts or entertainment in business settings.

Employees of, and third parties representing, Atlassian should not request, accept, offer to give, or give anything of significant value that would give the appearance of impropriety or suggest that it was intended in any way to influence a business relationship. Gifts in the form of cash payments are not allowed, regardless of amount. Please see Policy - Procurement for up to date information on what is considered appropriate amounts for gifts and entertainment.

Any gifts and entertainment involving government or government-related individuals must be in compliance with the law in that country and the United States Foreign Corrupt Practices Act (FCPA). For further information, please see the Dealing with Public or Government Employees section in this Code.

Side Deals & Side Letters

All the terms and conditions of agreements entered into by Atlassian must be formally documented. Contract terms and conditions define the key attributes of Atlassian's rights, obligations, and liabilities, and can also dictate the accounting treatment given to a transaction. Making (or agreeing to make in the future) business commitments outside of the formal contracting process, through side deals, side letters, or otherwise, is unacceptable. You should not make any oral or written commitments that create a new agreement or modify or propose to modify an existing agreement without approval through the formal contracting process.

05 Adopt Sustainability

Atlassian is built to be open, inclusive, fair, and just.

When we face tough questions about ethics, people, or the planet, we let those principles guide us. Whether you call it corporate social responsibility, corporate citizenship, or sustainability, this is just about being human. Atlassian has public commitments and invests in making progress when it comes to our planet, people, community, and customers.

> Atlassian respects human rights, and we implement this commitment using approaches based on the UN Guiding Principles on Business and Human Rights.

Planet – a Net-Zero Future

What we believe

(We can't believe we need to say this, but...) Climate change is caused by humans, and without immediate intervention, it will fundamentally disrupt the environment, society, and the economy in very painful ways. Working together, the private sector, public sector, and citizens must play as a team and take bold action. As part of our commitment to combat climate change, Atlassian has achieved its goal to run our operations on 100% renewable electricity, starting in fiscal year 2020. We've also set science-based targets to limit warming to 1.5°C and achieve net-zero emissions by no later than 2040. Finally, we are focusing on inspiring Atlassians and companies alike to act.

Our near-term targets

Atlassian has committed to being net zero by 2040 and has set near-term targets for 2025 to reduce emissions, validated by the Science Based Targets initiative. These targets are:

- Reducing our operational emissions (scope 1-2) by 50% by 2025
- Encouraging suppliers making up 65% of emissions to adopt SBTis
- Reduce our business travel emissions by 25% by 2025

Read about our progress in our annual Sustainability Report To help contribute, learn about how our suppliers can help us achieve our goals.

People – Unleashing the Potential of Our Team

What we believe

Atlassian is for everyone. We believe in the power of diversity. We aim for nothing short of equity for every Atlassian and are committed to an authentic culture of inclusion. Our vision is to integrate this across everything we do, which will drive the structural shifts needed to unleash the potential of our own team, deliver on our promise of openness to our customers, and build the kind of world we want to live in.

Inclusion through ERG communities

Our ERG community groups are remote-first and representative of our global team.

Interested in joining one of Atlassian's Employee Resource Groups? Read the Employee Resource Group Guidelines. And learn more about our progress and hiring goals in Atlassian's Sustainability Report.

Community – In It For Good

Long before we had a stock ticker symbol – and even before we'd formally adopted our company values – co-founders Mike and Scott built giving back into Atlassian's operations, with a belief that both business and education can serve as forces for good and help transform our world. Atlassian contributes 1% of its equity, profit, employee time, and products to the Atlassian Foundation to do good on a global scale and in our own backyards.Learn more about how to participate in the Atlassian Foundation.

Customers – Moving Forward as a Rights-Aligned Business

What we believe

Businesses have a responsibility to respect human rights. As we continue to assess and address Atlassian's impact, we are guided by our values, mission, and the UN Guiding Principles on Business and Human Rights. We know that every decision we make has a real impact on our employees, customers, business partners, and community. Transparency and accountability live at the core of our business and form the foundation of our human rights approach.

Our commitment to rights-aligned business practices

Atlassian has a public Human Rights Statement that outlines our commitment and responsibility to the rights of employees, contingent workers, customers, suppliers, business partners, community, and the planet, aligned with the UN Guiding Principles on Business and Human Rights. We also have Responsible Technology Principles that guide how we develop, deploy, and use AI and other emerging technologies.

Along with the statement and principles, you can also refer to our Supplier Code of Conduct and details within this Code of Business Conduct and Ethics to learn more about ways you can support and uphold human rights as an Atlassian.

06 Protect Confidential Information

Atlassian Confidential Information

Confidential Information generated and gathered in Atlassian's business plays a vital role in our business, prospects, and ability to compete.

> "Confidential Information" is any material that Atlassian does not make or want to make publicly known at a given time. It includes all non-public information that might be of use to competitors or harmful to Atlassian or its customers if disclosed.

At the least, Atlassian Confidential Information includes information such as Atlassian's proprietary source code, nonpublic technical information about Atlassian systems and products, nonpublic information about Atlassian's product roadmap or partnerships, nonpublic financial information, and nonpublic information relating to employees and compensation.

You are expected to protect Atlassian Confidential Information and any trade secrets to which you may have access during the course of your work, as set out in your employment agreement and/or non-disclosure agreement. This agreement is in effect throughout your engagement and has obligations that continue even after you no longer provide services to Atlassian.

Confidential Information should be used solely for legitimate company purposes. You may not disclose or distribute Atlassian's Confidential Information, except when disclosure is authorized by the company or required by applicable law, rule, regulation, or pursuant to an applicable legal proceeding. You must return all of the company's Confidential Information and proprietary information to Atlassian when your engagement with the company ends.

Third Party Confidential Information

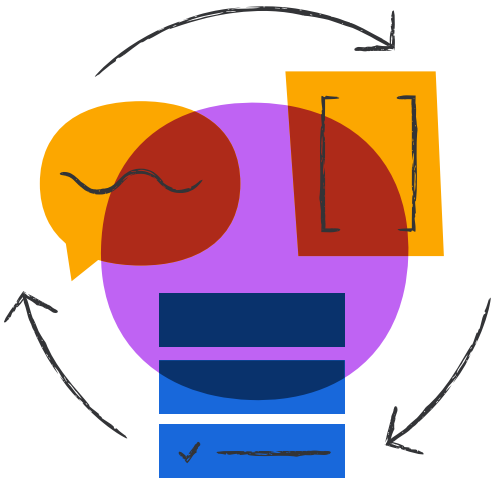
Just as Atlassian protects its own confidential materials, Atlassian respects the rights of other people or companies to protect their confidential information and trade secrets.

> If you have information that might reasonably be considered confidential information or a trade secret of another person or company, you must not reveal it to Atlassian without authorization from the owner of the information. This includes information from a prior employer.

You may, under an authorized non-disclosure agreement, become aware of another company's confidential information or trade secrets in the context of exploring a business relationship with that company. You must respect the proprietary nature of this information and not use it or disclose it publicly without authorization.

If you require assistance in determining the proper course of action with respect to third party confidential information, including the requirements imposed by a non-disclosure agreement, please contact the Atlassian Legal team.

Read our Policy - Data Classification to learn more about the various types of information that we have at Atlassian and how each should be treated.



07 Use Atlassian & Third Party Assets Appropriately

We all have a responsibility to ensure that Atlassian assets are not misused, shared with unauthorized employees or other third parties, or sold without appropriate authorization.

Atlassian's assets include its intellectual property rights, source code, technical know-how and documentation, information systems, computers, servers, other equipment, and communication facilities. Loss, theft, and misuse of Atlassian's assets have a direct impact on the company's business and its profitability. You are expected to comply with all of Atlassian's policies related to protecting its assets (found at go/policies) and take steps to ensure that Atlassian's assets are protected and used only for legitimate business purposes.

Computer & Other Equipment

If you use Atlassian equipment at your home or off-site, take precautions to protect it from theft or damage, just as if it were your own. If your employment or engagement with Atlassian terminates for any reason, you must immediately return all Atlassian resources, assets, and equipment in normal operating condition.

Use of Email & Other Forms of Electronic Communication

Always use emails and other forms of electronic communication (for example, Slack, texting, tweeting, etc.) appropriately. Please remember that the electronic systems and devices are owned by Atlassian and may be subject to monitoring and inspection by Atlassian even if protected by password, as permitted by applicable laws. For further details please consult Policy – Electronic Systems and Communications and Policy – Workplace Surveillance.

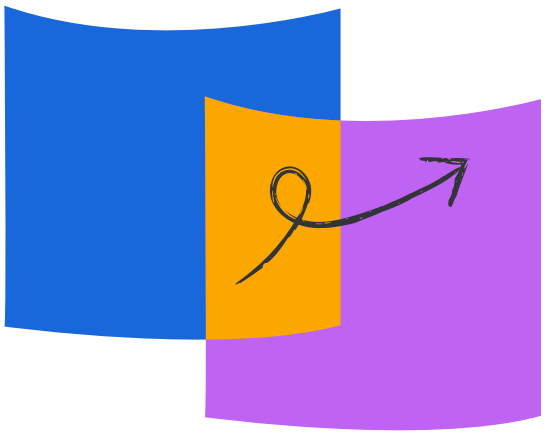
Use of Third Party Software

We respect the intellectual property rights of third parties. All software used to conduct Atlassian business must be authorized, for example, by purchasing a commercial software license or by licensing under an appropriate open source license. Using or copying software without a valid license constitutes copyright infringement and may expose you and Atlassian to civil and criminal liability.

If you require assistance in determining what is an appropriate open source license for your work at Atlassian, please consult Standard - Using Open Source or other Third Party Code in Atlassian Product or the Atlassian Legal team.

Other Copyrighted Materials

Published works such as photographs, screen shots, videos, music, articles, white papers, web sites, whether in hardcopy or electronic format, are generally protected by copyright. At times, Atlassians may want to use such publicly available materials in presentations or promotional materials or at trade shows or Atlassian events. These works are generally protected by copyright law and their unauthorized use may constitute copyright infringement. Do not use any portion of them without obtaining permission from the copyright holder. If you need assistance in such matters please consult with the Atlassian Legal team.



08 Respect Privacy & Personal Information

Atlassian is responsible for protecting and securing the personal information of our employees, contractors, vendors, customers, and partners.

We take this role seriously and require all Atlassians to take a role in safeguarding the information that has been entrusted to Atlassian. You must know and comply with your responsibilities under all of Atlassian's internal and external privacy and data security policies, processes, and standards (we will refer to these as the "data security and privacy policies") and applicable global data protection laws. You may only access, collect, use, transfer, dispose of, or otherwise process personal information as permitted under Atlassian's data security and privacy policies. You must always honor the individual's choice to keep their personal information confidential and secure.

If you ever become aware of the misuse or unauthorized access of any personal information, it is your responsibility to report this to the Privacy and Security teams immediately.

Privacy and Your Use of Atlassian Resources

We seek to respect your personal privacy. However, as permitted by local law, it is important for you to understand that information created, accessed, transmitted, or stored using Atlassian's technology resources, such as email messages, computer files, instant messages, or websites in your browsing history, are company resources and assets. We may access, monitor, or inspect Atlassian resources, assets, and property at any time without your prior approval, knowledge, or consent to the extent allowed by law. This includes monitoring and retrieving information that is stored or transmitted on Atlassian's electronic devices, computers, equipment, and systems. For further information, please read Policy – Electronic Systems and Communications and Policy – Workplace Surveillance.

WE ARE COMMITTED TO PROTECTING THE PERSONAL DATA PROVIDED TO US. WE MUST ENDEAVOR TO KEEP THIS DATA SECURE, USE IT ONLY FOR INTENDED PURPOSES, AND FOLLOW THESE SIMPLE GUIDELINES:

Notice: We provide clear and easy-to-understand information about how Atlassian collects, manages, uses, processes, and shares your data in Standard - Global Workplace Privacy Notice (or other applicable notice)

Choice: Where it is optional to provide your personal data to us (e.g., voluntary opt-in program), you may choose whether to provide personal data to us and we will respect your decisions

Access: If you request access to your personal data, we will provide you with your personal data to the extent required by applicable law

Use: We will store, use, and transfer your personal data in accordance with Standard - Global Workplace Privacy Notice

Security: We safeguard your personal data in accordance with Standard - Global Workplace Privacy Notice (see "Section 9. How We Store and Secure Information We Collect")


09
Keep
Accurate
Business
Records

Managing & Retaining Business Records

The integrity, reliability, and accuracy in all material respects of Atlassian's books, records, and financial statements are fundamental to its continued and future business success. You may not cause Atlassian to enter into a transaction with the intent to document or record such transaction in a deceptive or unlawful manner. In addition, you may not create any false or artificial documentation or book entry for any transaction entered into by Atlassian. Similarly, officers, employees, consultants, contractors, and others working on behalf of the company who have responsibility for accounting and financial reporting matters have a responsibility to accurately record all funds, assets, and transactions on Atlassian's books and records.

It is equally important to know when to save information and when to periodically dispose of documents that are no longer useful or do not need to be retained. If litigation is pending or threatened, you must retain all pertinent documents in accordance with instructions received from the Legal team. Local laws regarding record retention and disposal may vary.

Quality of Public Disclosures

Atlassian is committed to providing its stockholders with information about its financial condition and results of operations as required by the securities laws of the United States. It is Atlassian's policy to provide full, fair, accurate, timely, and understandable disclosures in its public communications, including the reports and documents that it submits to the Securities and Exchange Commission and other authorities. Officers, employees, consultants, contractors, and others working on behalf of the company who are involved with these filings and disclosures, including Atlassian's principal executive, financial, and accounting officers, must use reasonable judgment and perform their responsibilities honestly, ethically, and objectively in order to ensure that this disclosure policy is fulfilled and maintain familiarity with the disclosure requirements, processes and procedures that apply to Atlassian. You must not knowingly misrepresent, omit or cause others to misrepresent or omit, materials facts about Atlassian to others, including Atlassian's inepended auditors, governmental regulators and self-regulator organizations. Members of Atlassian's Disclosure Committee are primarily responsible for monitoring the company's public disclosures.

10 Comply with Global Trade Controls

Atlassian is subject to global trade controls, including United States export controls and economic sanctions regulations and laws regulating international transactions. In addition, United States law prohibits Atlassian from participating in foreign boycotts and unsanctioned embargoes (in other words, embargoes that are not supported by the United States). It is Atlassian's policy, as outlined in its Policy - Export Controls Compliance, to comply with these laws and regulations even if it may result in the loss of some business opportunities. You are responsible for being familiar with the basic elements of these laws and to comply with them at all times. You should learn and understand the extent to which Australian, United Kingdom, United States, and international trade controls apply to transactions conducted by Atlassian. Violation of these laws can lead to severe penalties, even for unintentional violations. If you have any questions about global trade controls, please contact the Compliance Officer.

Export Controls

Generally, an export can include the sharing of any product or technology (including hardware, software, or source code), which is located within, created within, or traveling through a country and then sent, disclosed, made available for download, or otherwise transferred beyond the country's borders or to a foreign country or customer via shipping, electronic or digital transmission, verbal communication, or other means. Exports can also include "deemed exports," which are sharing of source code or technology to foreign nationals, wherever located, even within your own country. Many countries maintain controls on the destinations to which, and individuals to whom, products, including software, may be exported, and certain products may require a license for Atlassian to export.

> The United States maintains some of the strictest export controls in the world. United States law forbids doing business with certain countries and their nationals without obtaining prior United States governmental approval. United States sanctions restrictions prohibit Atlassian from conducting business with certain sanctioned countries and also specific companies and individuals identified on various restricted party lists. It is critical that you ask questions if you are unsure about the rules pertaining to the product, country, or customer.

Unsanctioned Embargoes & Anti-Boycott Rules

United States federal law prohibits Atlassian from participating in any foreign boycott or embargo against countries, companies, or individuals that is not approved by the United States government. We must report any requests to participate in such unsanctioned boycotts or embargoes. Perhaps the most common unsanctioned boycott is the Arab League's boycott of Israel. This might include a request to insert a contractual clause into an agreement that obligates a party to boycott any country, confirm that a product was not originated or developed in a country, or that prohibits doing business with, or traveling to, certain countries.

WHAT COUNTRIES ARE CONSIDERED "UNFRIENDLY" COUNTRIES?

The United States government maintains a number of boycotts against countries considered unfriendly to United States interests. The prohibited countries list changes frequently due to world events and changes in United States foreign policy. Never assume that a country is not on the list. If you are unsure if you can transact business with a particular country, company, or individual, please contact Atlassian's Legal team.

11 Keep the Appropriate Teams Informed

Media Requests

Atlassian designates specific individuals or teams to speak with the media, financial analysts, and governmental authorities regarding Atlassian matters. Unless you are a designated person, you must refer all inquiries as follows:

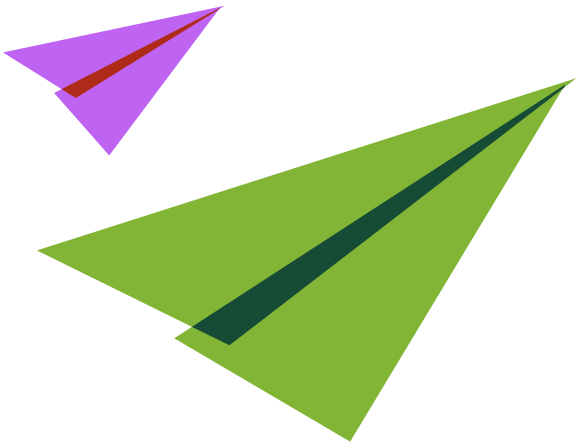
- Media inquiries must be directed to our Corporate Communications team
- Financial analyst inquiries must be directed to our Investor Relations team
- Government inquiries must be directed to the Compliance Officer

Social Media

If you post information in public forums such as social networking sites, blogs, or chat rooms, you are prohibited from sharing confidential, private, or proprietary information about Atlassian. You are not permitted to speak on behalf of Atlassian when making any statements in these forums.

Law Enforcement / Government

You must also seek Atlassian approval to speak to government or law enforcement officials regarding Atlassian or Atlassian's business activities. If a disclosure is required by law, you must promptly notify the Compliance Officer of such disclosure requirement. Nothing in this Code of Conduct is intended to prevent you from filing a charge with or participating in any investigation or proceeding conducted by a government agency.



12 Reporting Concerns & Receiving Advice

First Seek Guidance

The best starting point for you to seek advice on ethics-related issues or reporting potential violations of the Code will usually be your manager or supervisor. However, if the conduct in question involves your manager or supervisor, or if you believe your manager or supervisor has not dealt with the matter properly, or if you do not feel that you can discuss the matter with your manager or supervisor, you may raise it with the Compliance Officer.

Reporting Ethics-Related Issues or Potential Violations of the Code

You may communicate with the Compliance Officer (Atlassian has designated its Deputy General Counsel - Corporate as its Compliance Officer for the purposes of this Code), or report potential ethics-related issues and violations of the Code, by any of the following methods (most of which may be done anonymously subject to local laws):

- in writing by email to Compliance-Officer@atlassian.com (this option does not allow for anonymous reporting)
- Anonymously via the Atlassian Ethics and Compliance Portal by:

  Calling 1.800.461.9330 in the United States or 1.800.763.983 in Australia; for other locations, visit https://www.atlassian.com/ethics; or

  Submitting a report at https://www.atlassian.com/ethics which is a secure web portal powered by Convercent, a third party provider.

  Special Rules for Our Portal Internationally. Please note that certain countries in the Americas, EMEA, and APAC where Atlassian does business may not allow certain concerns to be reported at all or to be reported anonymously via the portal. Also, Atlassian may be obligated to inform the person who is the subject of a reported concern or violation that the report was filed and that the person may exercise their right to access and respond to the information regarding the allegation.

- The above methods are preferred, but you may also send an anonymous message by mail, addressed to:

  Compliance Officer, Atlassian Corporation
  350 Bush Street, 13th Floor
  San Francisco, California 94104 USA

Reporting Work-Related Grievances

Atlassian's Policy – Grievance sets out the appropriate channels for submitting matters concerning unfair treatment in an Atlassian work environment that causes undue concern, distress, or a feeling of injustice. Before reporting these types of matters via Atlassian's Ethics and Compliance Portal, to the extent possible, please use the channels described in Policy – Grievance.

Notes about Reporting

Anonymity. When reporting suspected violations of the Code, Atlassian prefers that you identify yourself; this helps facilitate an effective and timely investigation and appropriate remedial action. However, Atlassian also recognizes that some people may feel more comfortable reporting a suspected violation anonymously.

If you wish to remain anonymous, you may do so (to the extent allowed by local law), and Atlassian will use reasonable efforts to protect your confidentiality subject to applicable law, rule, or regulation or any applicable legal proceedings. In the event the report is made anonymously, however, Atlassian may not have sufficient information to look into or otherwise investigate or evaluate the allegations. Accordingly, you should provide as much detail as is reasonably necessary to permit Atlassian to evaluate the matter(s) set forth in the anonymous report and, if appropriate, commence and conduct an appropriate investigation.

Cooperation. You are expected to cooperate with Atlassian in any investigation of a potential violation of the Code, any other Atlassian policy or practice, or any applicable law, rule, or regulation.

Misuse of Reporting Channels. You must not use these reporting channels in bad faith, or to report false or frivolous grievances. Please use the Ethics and Compliance Portal only to report grievances that involve the Code or other ethics-related issues.

Director Communications. A director on the Board of Directors may also communicate concerns or seek advice with respect to this Code by contacting the Board of Directors through its Chairperson or the Audit Committee.

13 Appendix

Monitoring Compliance & Disciplinary Action

Atlassian's Board of Directors, in conjunction with its Audit Committee, is responsible for administering this Code. Atlassian's Deputy General Counsel - Corporate, has been appointed Atlassian's Compliance Officer under this Code. The Board has delegated day-to-day responsibility for administering and interpreting the Code to the Compliance Officer.

Atlassian's management, under the supervision of its Board or Audit Committee, will take reasonable steps from time to time to monitor compliance with the Code, and when appropriate, impose, and enforce appropriate disciplinary measures for violations of the Code. Atlassian's management will periodically report to the Board or Audit Committee, as applicable, on these compliance efforts including, without limitation, periodic reporting of alleged violations of the Code and the actions taken with respect to any such violation.

Exceptions & Amendments

No waiver of any provisions of the Code for the benefit of a director or an executive officer (which includes without limitation, for purposes of this Code, Atlassian's principal executive, financial, and accounting officers) will be effective unless approved by the Board or, if permitted, the Audit Committee, and if applicable, such waiver is promptly disclosed to the company's stockholders in accordance with applicable United States securities laws, any other laws or regulations, and/or the rules and regulations of the exchange or system on which Atlassian's shares are traded or quoted, as the case may be.

Any waivers of the Code for other officers, employees, consultants, contractors, and others working on behalf of the company may be made by the Compliance Officer, the Board or, if permitted, the Audit Committee.

All amendments to the Code must be approved by the Board or the Audit Committee and, if applicable, must be promptly disclosed to Atlassian's stockholders in accordance with applicable United States securities laws, any other laws or regulations, and/or the rules and regulations of the exchange or system on which the company's shares are traded or quoted, as the case may be.

atlassian.com/ethics

ATLASSIAN

Exhibit I

Privacy Policy (October 7, 2025)

Effective starting: October 7, 2025

Your privacy matters to us. This privacy policy explains how Atlassian Pty Ltd, Atlassian US, Inc. and our corporate affiliates (“Atlassian”, “we”, “us”, “our”) collect, use, share, and protect your information when you use our products, services, websites, or otherwise interact with us (a list of Atlassian’s corporate affiliates can be found in the List of Subsidiaries section of Atlassian’s most recent Form 10-K, available under the SEC Filings tab by selecting the “Annual Filings” filter on the page located here). We offer a wide range of products, including our cloud and software products. We refer to all of these products, together with our other services and websites, as "Services" in this privacy policy.

This privacy policy also explains your choices surrounding how we use information about you, which includes how you can object to certain uses of information about you and how you can access and update certain information about you. **If you do not agree with this privacy policy, do not access or use our Services or interact with any other aspect of our business**.

For individuals in the European Economic Area, United Kingdom, or the United States: please refer to the appropriate “Regional disclosures” for additional details that may be relevant to you.

This privacy policy is intended to help you understand:

- Information we collect
- How we use information
- How we disclose information
- How we store and secure information
- How long we keep information
- How to access and control your information
- Our policy towards children
- Regional disclosures
- Changes to our privacy policy
- How to contact us

We offer additional policies tailored for specific audiences and use cases. These include:

- Cookies & Tracking Notice

- Atlassian Careers Privacy Notice – for job applicants
- Former Workplace Privacy Notice – for past employees
- Demographic Survey Privacy Notice – for voluntary survey data

This privacy policy describes Atlassian's data practices as a controller of personal information. Please note that this privacy policy does not apply to the extent that we process personal information in the role of a processor or service provider on behalf of our customers, as further specified in the Data Processing Addendum entered into with those customers. When Atlassian processes personal information on behalf of our customers (such as your employer, if applicable), the customer is the controller of the personal information processed and manages those accounts and any Service sites. In such cases, Atlassian acts as a processor or service provider on behalf of our customer and handles your information according to the instructions of that organization. We are not responsible for the privacy or security practices of our customers, which may differ from those described in this privacy policy. For more information about how an Atlassian customer uses your personal information, or to exercise the rights you may have with respect to that information, please contact that organization directly.

Privacy policy overview

- Atlassian collects information directly from you when you provide it to us, automatically when you use our Services, and from other sources including other users of the Services, other services you link to your account, other Atlassian companies, partners, and third-party providers.
- How we use information depends on which Services you use, how you use them, and any preferences you have communicated to us. We use information for a range of purposes described below, including to provide the Services and personalize your experience, to develop and improve our Services, to communicate with you, to conduct marketing and promotional activities, to provide customer support, to maintain Service safety and security, to protect our interests and rights, with your consent, and to aggregate or de-identify data.
- We disclose information as described below, including to service providers, Atlassian partners, providers of third-party services, for compliance with enforcement requests and applicable laws, to enforce our terms and policies and our rights, to Atlassian affiliated companies or in connection with business transfers, as well as with your consent. Additionally, when you use the Services, we disclose certain information about you to other Service users as described in more detail below.
- Where applicable under local law, you may have certain rights or choices with respect to your personal information, including to request information about our processing of information, to request a copy of your information, to object to our use of information, to request the deletion

or restriction of information, to request a disclosure of information in a portable format, or to opt out of certain disclosures of personal information and targeted advertising. See the "How to access and control your information" section for more detail on specific choices and how to exercise the rights you may have.

- In the "Regional disclosures" section, we provide additional information for individuals in the European Economic Area and United Kingdom, including information about the legal bases for processing information, international transfers, the specific rights applicable in these jurisdictions, and how to contact our EU and UK representatives. We also provide additional information for individuals in the United States, including details about information collected and disclosed in the past 12 months and specific rights available under applicable U.S. state laws.
- We provide details on how to contact us with any questions or concerns, or to exercise your rights, in the "How to contact us" section.

Information we collect

We collect information about you when you provide it to us, when you use our Services, and from other sources, as further described below.

Information you provide

We collect information about you when you input it into the Services or otherwise provide it directly to us. This includes the following categories of information:

Account Information and Profile Information: We collect information when you register for an account, create or modify your profile, set preferences, sign up for or make purchases through the Services. For example, you provide contact information (e.g., name or email address) and, in some cases, billing information (e.g., billing address, email address or name), when you register for the Services. You also have options to add a display name, profile photo, job title, and other details to your profile. We also keep track of your preferences when you select settings within the Services.

You may also provide information to us when you integrate or link a third-party service with our Services. For example, if you create an account or log into the Services using your Google credentials, we receive your name and email address as permitted by your Google profile settings in order to authenticate you. The information we receive when you link or integrate our Services with a third-party service depends on the settings, permissions and privacy policy controlled by that third-party service. You should always check the privacy settings and notices

in these third-party services to understand what information may be disclosed to us or shared with our Services.

Content you provide through our products: The Services include the Atlassian products you use, where we collect and store content that you post, send, receive and share. We process this content in the role of a processor or service provider on behalf of our customers; this privacy policy does not apply to that processing (see above for more information).

Content you provide through our websites: The Services also include websites owned or operated by us. We collect content that you submit to these websites, which include social media or social networking websites operated by us, our support and documentation websites, our Community Forums, and our Marketplace. For example, you provide content to us when you provide feedback, directly to us through our Services or otherwise, or when you participate in any interactive features, surveys, contests, promotions, sweepstakes, activities or events.

Information you provide through our support channels: The Services also include customer support, where you may submit inquiries or other information regarding a problem you are experiencing with a Service. Whether you designate yourself as a technical contact, open a support ticket, speak to one of our representatives directly or otherwise engage with our support team or support features, you will be asked to provide contact information, a summary or description of the problem you are experiencing, and any other documentation, screenshots or information that would be helpful in resolving the issue and/or a Support Entitlement Number (SEN).

Payment Information: We collect payment and billing information when you register for certain paid Services. For example, we ask you to designate a billing representative, including name and contact information, upon registration. You might also provide payment information, such as payment card details, which we collect via secure payment processing services.

Information we collect automatically

We automatically collect information about you when you use our Services, including browsing our websites and taking certain actions within the Services. Information may also be collected about how you interact with and use features in our software products. This includes the following categories of information:

Your use of the Services: We collect information about your use, operation, and interaction with any of our Services, including when you connect third party services to or use those services with ours. This information includes, for example, the features you use, the actions you perform, the links you click on; the type, size and filenames of attachments you upload to the Services;

search terms; the number of words in a Jira ticket or @ mentions in a comment; the type of Loom videos you created and the number of views on your videos; and how you interact with others on the Services. We also collect information about the teams and people you work with and how you work with them, like who you collaborate with and communicate with most frequently. Administrators may enable our collection of this information from software products.

Device and Connection Information: We collect information about your computer, phone, tablet, or other devices you use to access the Services. This device information includes your connection type and settings when you install, access, update, or use our Services. We also collect information through your device about your operating system, browser type, IP address, URLs of referring/exit pages, device identifiers, and diagnostic and crash data. We use your IP address and/or country preference to approximate your location to provide you with a better Service experience. How much of this information we collect depends on the type and settings of the device you use to access the Services.

Cookies and Other Tracking Technologies: Atlassian and our third-party partners, such as our advertising and analytics partners, use cookies and other tracking technologies (e.g., web beacons, device identifiers and pixels) to provide functionality, to recognize you across different Services and devices, or to demonstrate that certain content was viewed or clicked. For more information, please see our Cookies & Tracking Notice, which includes information on how to control or opt out of these cookies and tracking technologies.

Information from other sources

We also receive information about you from other Service users, our related companies, our business and channel partners, and third-party providers, including from social media platforms and public databases. We may combine this information with information we collect through other means described above. This helps us, for example, to update and improve our records, provide and improve our Services, identify new customers, create more personalized advertising, and suggest services that may be of interest to you. This includes information collected from the following sources:

Other users of the Services: We receive your email address from other Service users when they provide it in order to invite you to the Services. Similarly, an administrator may provide your contact information when they designate you as the billing or technical contact on your company's account or when they designate you as an administrator.

Atlassian Companies: We receive information about you from other Atlassian corporate affiliates, in accordance with their terms and policies.

Atlassian Partners: We work with a global network of partners who provide consulting, implementation, training and other services around our products. Some of these partners also help us to market and promote our Services, generate leads for us, and resell our Services. We receive information about you and your activities on and off the Services from these partners, such as billing information, billing and technical contact information, company name, what Atlassian Services you have purchased or may be interested in, evaluation information you have provided, what events you have attended, what country you are in, and information about your interest in and engagement with our Services and online advertisements.

Third-Party Providers: We may receive information about you from third-party providers of business and security information and from publicly available sources (e.g., social media platforms), including physical mail addresses, job titles, email addresses, phone numbers, intent data (or user behavior data), IP addresses and social media profiles.

How we use information

How we use the information we collect depends on which Services you use, how you use them, and any preferences you have communicated to us. We use information for the following purposes:

To provide the Services and personalize your experience: We use information about you to provide the Services to you, including to process transactions, authenticate you when you log in, provide customer support, and operate, maintain, and improve the Services. We may use your email domain to infer your affiliation with a particular organization or industry to personalize the content and experience you receive on our websites. Based on your interactions with different Atlassian products, third-party services you link or install, and advertisements, we will personalize your experience and tailor our communications, recommendations and offers to you.

To develop and improve our Services: We are always looking for ways to make our Services smarter, faster, secure, integrated, and useful. We use information and collective learnings (including feedback) about how people use our Services to troubleshoot, to identify trends, usage, activity patterns and areas for integration, to improve our Services and to develop new products, features and technologies that benefit our users and the public. For example, to improve the @mention feature, we automatically analyze recent interactions among users and how often they @mention one another to surface the most relevant connections for users, or we might analyze Marketplace search terms to improve the accuracy and relevance of suggested apps returned when you use the search feature. In some cases, we apply these learnings across our Services to improve and develop similar features, to better integrate the Services you

use, or to provide you with insights based on how others use our Services. We also test and analyze certain new features with some users before rolling the feature out to all users.

To communicate with you about the Services: We use your contact information to send transactional communications via email and within the Services, including confirming your purchases, reminding you of subscription expirations, responding to your comments, questions and requests, and providing customer support. We also provide tailored communications based on your activity and interactions with us, and we may contact you regarding product feedback. If an opt out is available, you will find that option within the communication itself or in your account settings.

To conduct marketing and promotional activities: We use information about you and how you use the Services for analysis, research and communications relating to marketing (including targeted advertising of products that may interest you), promotional activities, and business development. We may use your contact information and information about how you use the Services to send promotional communications that may be of specific interest to you, including by email and by displaying Atlassian ads on other companies' websites and applications. These communications may be informed by, for example, your interactions (like counting ad impressions), and are aimed at driving engagement and maximizing what you get out of the Services, including information about new features, survey requests, newsletters, and events we think may be of interest to you. We also communicate with you about new Services, product offers, promotions, and contests. You can control whether you receive these communications as described below at “How to access and control your information” under "Opt-out of communications."

To provide customer support: We use your information to resolve technical issues you encounter, to respond to your requests for assistance, to analyze crash information, and to repair and improve the Services, including for development, training, or fine-tuning of machine learning and artificial intelligence models. We may also use generative artificial intelligence in responding to your support related requests. Where you give us express permission to do so, we may disclose information to a third-party expert for the purpose of responding to support-related requests.

To maintain Service safety and security: We use information about you and your use of the Services to verify accounts and activity, to detect, prevent, and respond to potential or actual security incidents, and to monitor and protect against other malicious, deceptive, fraudulent, illegal or inappropriate activity, including violations of Service policies. Detection and response may leverage generative artificial intelligence or machine learning tools.

***To protect our legitimate business interests and legal rights*:** Where required by law or where we believe it is necessary to protect our legal rights and interests, or the legal rights or interests of others, we use information about you in connection with legal claims, compliance, regulatory, and audit functions, and disclosures in connection with the acquisition, merger or sale of a business.

With your consent: We use information about you where you have given us consent to do so for a specific purpose not listed above. For example, we may publish testimonials or featured customer stories to promote the Services, with your permission.

To aggregate or de-identify data*:* We may aggregate or de-identify your information collected through the Services so it can no longer be re-identified by us or another party. We may use and disclose aggregated or de-identified data for a number of purposes, including to develop and improve our Services and to conduct marketing and promotional activities. To the extent we aggregate any data originally based on personal information, we maintain and use such data in de-identified form and will not attempt to re-identify the data.

How we disclose information

We make collaboration tools, and we want them to work well for you. This means disclosing information through the Services and to certain third parties. We disclose information we collect in the ways discussed below.

Disclosing to third parties

We disclose information to third parties that help us operate, provide, improve, integrate, customize, support, and market our Services. All the above categories exclude text messaging originator opt-in data and consent. This information will not be shared with any third parties, excluding aggregators and providers of the text messaging services.

Service Providers: We work with third-party service providers to provide website and application development, hosting, maintenance, backup, storage, virtual infrastructure, payment processing, analysis, marketing, and other services for us, which may require them to access or use information about you. If a service provider needs to access information about you to perform services on our behalf, they do so under close instruction from us, including appropriate security and confidentiality procedures designed to protect your information.

Atlassian Partners: We work with a global network of partners who provide consulting, implementation, training and other services around our products. We may disclose your information to these third parties in connection with their services, such as to assist with billing

and collections, to provide localized support, and to provide customizations. We may also disclose information to these third parties where you have agreed to that disclosure.

Third-Party Services: You, your administrator or other Service users may choose to add new functionality or change the behavior of the Services by installing or connecting third-party services. Doing so may give third-party services access to your account and information about you, like your name and email address. When you intentionally interact with such third-party services, we may disclose certain information to those third parties or receive information from those third parties, consistent with your privacy settings on the third-party service. If you purchase or install a third-party service using Atlassian Marketplace, we will also disclose Order information to the third party in accordance with the Atlassian Marketplace Terms of Use. Third-party service policies and procedures are not controlled by us, and this privacy policy does not cover how third-party services use your information. We encourage you to review the privacy policies of third parties before connecting to or using their applications or services to learn more about their privacy and information handling practices. If you object to information about you being disclosed to these third parties, please do not install or connect the third-party service.

Links to Third-Party Sites: The Services may include links that direct you to other websites or services whose privacy practices may differ from ours. If you submit information to any of those third-party sites, your information is governed by their privacy policies. We encourage you to carefully read the privacy policy of any website you visit.

Third-Party Widgets: Some of our services contain widgets and social media features, such as the Twitter "tweet" button or Facebook "like" button. These widgets and features may collect your IP address, which page you are visiting on the Services, and may set a cookie to enable the feature to function properly. Widgets and social media features are either hosted by a third-party or hosted directly on our Services. You should always check the privacy settings and notices in these third-party services to understand how those third-parties may use your information.

With your consent: We may also disclose information about you to third parties when you give us consent to do so. For example, we often display personal testimonials of satisfied customers on our public websites. With your consent, we may post your name alongside the testimonial.

Compliance with Enforcement Requests and Applicable Laws; Enforcement of Our Terms and Policies; Enforcement of Our Rights: We may disclose information about you to government authorities, law enforcement, or industry peers if we believe that sharing is reasonably necessary to (a) comply with any applicable law, regulation, legal process or enforceable governmental request, or legal obligation, (b) enforce the terms of our agreements

and our policies, (c) protect the security or integrity of our products and services, (d) protect Atlassian, our customers or the public from harm or illegal activities, or (e) respond to an emergency which we believe in good faith requires us to disclose information to assist in preventing the death or serious bodily injury of any person. For more information on how we respond to government requests, see our Guidelines for Law Enforcement and our Transparency Report.

Disclosing to affiliated companies

We disclose information we collect to affiliated companies and, in some cases, to prospective affiliates. Affiliated companies are companies owned or operated by us. The protections of this privacy policy apply to the information we disclose in these circumstances.

Atlassian companies: We disclose information to other Atlassian corporate affiliates in order to operate, maintain, and improve the Services, and to offer you other Atlassian affiliated services. This includes companies that own or operate the Services.

Business Transfers: We may disclose or transfer information we collect under this privacy policy in connection with any merger, sale of company assets, financing, reorganization, dissolution, or acquisition of all or a portion of our business to another company. You will be notified via email and/or a prominent notice on the Services if a transaction takes place, as well as any choices you may have regarding your information.

Disclosing to other Service users

When you use the Services, we disclose certain information about you to other Service users.

Managed accounts and administrators: If you register or access the Services using an email address with a domain that is owned by your employer or organization, or associate that email address with your existing account, and such organization wishes to establish an account or site, certain information about you, including your name, profile picture, contact info, content and past use of your account may become accessible to that organization's administrator and other Service users sharing the same domain. If you are an administrator for a particular site or group of users within the Services, we may disclose your contact information to current or past Service users, for the purpose of facilitating Service-related requests.

Community Forums: Our websites offer publicly accessible blogs, forums, issue trackers, and wikis (e.g., Atlassian Community, Atlassian Developer Community, Trello Community, and Trello Inspiration). You should be aware that any information you provide on these websites - including profile information associated with the account you use to post the information - may be read, collected, and used by any member of the public who accesses these websites. Your posts and

certain profile information may remain even after you terminate your account. We urge you to consider the sensitivity of any information you input into these Services. To request removal of your information from publicly accessible websites operated by us, please contact us as provided below. In some cases, we may not be able to remove your information, in which case we will let you know if we are unable to and why.

How we store and secure information

We use industry standard technical and organizational measures to secure the information we store. For more information on where and how we store your information, please see the Atlassian Trust Center.

While we implement safeguards designed to protect your information, no security system is impenetrable and due to the inherent nature of the Internet, we cannot guarantee that information, during transmission through the Internet or while stored on our systems or otherwise in our care, is absolutely safe from intrusion by others.

How long we keep information

How long we keep information we collect about you depends on the type of information, the purposes for which it was collected, applicable legal or regulatory requirements, and user expectations and preferences. After such time, we will either delete or de-identify your information or, if this is not possible (for example, because the information has been stored in backup archives), then we will securely store your information and isolate it from any further use until deletion is possible.

Account information: We retain your account information for as long as your account is active and a reasonable period thereafter in case you decide to re-activate the Services. We also retain some of your information as necessary to comply with our legal obligations, to resolve disputes, to enforce our agreements, to support business operations, and to continue to develop and improve our Services. Where we retain information to develop and improve our Services, we take steps to de-identify the information.

Information you share on the Services: If your account is deactivated or disabled, some of your information and the content you have provided will remain in order to allow your team members or other users to make full use of the Services. For example, we continue to display messages you sent to the users that received them and continue to display content you provided.

Managed accounts: If the Services are made available to you through an organization (e.g., your employer), we retain your information as long as required by the administrator of your

account. For more information, see "Managed accounts and administrators" at the “How we disclose information” section.

Marketing information: If you have elected to receive marketing emails from us, we retain information about your marketing preferences for a reasonable period of time from the date you last expressed interest in our Services, such as when you last opened an email from us or ceased using your Atlassian account. We retain information derived from cookies and other tracking technologies for a reasonable period of time from the date such information was created.

How to access and control your information

Your Rights:

Where applicable under local law, you may have certain rights with respect to your personal information. For more information about region-specific rights for residents of the European Economic Area, United Kingdom, and the United States, please refer to the “Regional disclosures” section.

Depending on which jurisdiction you live in, you may have the right to request information about our processing of your information, to request a copy of your information, to object to our use of your information (including for marketing purposes), to request the deletion or restriction of your information, to request your information in a structured, electronic format, to request to correct or update your information, to request that we transfer your information to a third party, and to request to opt out of certain disclosures of personal information and targeted advertising.

In the “Your Choices” section, we describe the tools and processes for making different requests associated with these rights. You can exercise some of the choices by logging into the Services and using settings available within the Services or your account. For all other requests, you may contact us as provided in the “How to contact us” section.

Your requests and choices may be limited in certain cases: for example, if fulfilling your request would reveal information about another person, or if you ask to delete information which we are required or permitted by law to retain. Where you have asked us to disclose data to third parties, for example, by installing third-party apps, you will need to contact those third-party service providers directly to have your information deleted or otherwise restricted. If you have unresolved concerns, you may have the right to complain to a data protection authority in the country where you live, where you work, or where you feel your rights were infringed.

Your Choices:

You have certain choices available to you when it comes to your information. Below is a summary of those choices, how to exercise them and any limitations:

Access and update your information: Our Services give you the ability to access and update certain information about you from within the Service. For example, you can access your profile information from your account and update your profile information within your profile settings (see here for instructions on how to do this). You can also make a request to access information that Atlassian holds in relation to your account here. If you don't have an Atlassian account, you can make a request to access your information here.

Delete your information, including your account: Our Services give you the ability to delete certain information about you from within the Services. For example, you can remove certain profile information within your profile settings (see here for instructions on how to do this). If you would like to delete your Atlassian account, see here for more information. If you don't have an Atlassian account, you can make a request to delete your information here. Please note, however, that we may need to retain certain information for record keeping purposes, to complete transactions, or to comply with our legal obligations.

Request that we stop using your information: In some cases, you may ask us to stop accessing, storing, using and otherwise processing your information where you believe we don't have the appropriate rights to do so. For example, if you believe a Services account was created for you without your permission, or you are no longer an active user, you can request that we delete your account as provided in this privacy policy. Where you gave us consent to use your information for a limited purpose, you can contact us to withdraw that consent, but this will not affect any processing that has already taken place at the time. If you object to information about you being disclosed to a third-party service, please disable the service.

Opt out of communications: You may opt out of receiving promotional communications from us by using the unsubscribe link within each email, updating your email preferences within your Service account settings menu, or by contacting us as provided below to have your contact information removed from our promotional email list or registration database. Even after you opt out from receiving promotional messages from us, you will continue to receive transactional messages from us regarding our Services. Please note, you will continue to receive generic ads.

Opt out of targeted advertising: Where applicable under local law, you may have the right to opt out of targeted advertising by clicking "Manage Preferences" and following the instructions. Where required, we also honor requests to opt out submitted via privacy preference signals recognized under applicable law, such as the Global Privacy Control ("GPC"). For more

information on the GPC and how to use a browser or browser extension incorporating the GPC signal, see Global Privacy Control — Take Control Of Your Privacy. Relevant browser-based cookie controls are described in our Cookies & Tracking Notice.

You may also be able to opt out of receiving personalized advertisements from other companies who are members of the Network Advertising Initiative or who subscribe to the Digital Advertising Alliance's Self-Regulatory Principles for Online Behavioral Advertising. For more information about this practice and to understand your options, please visit: http://www.aboutads.info, http://optout.networkadvertising.org/ and http://www.youronlinechoices.eu.

Data portability: Data portability is the ability to obtain some of your information in a format you can move from one service provider to another (for instance, when you transfer your mobile phone number to another carrier). Depending on the context, this applies to some of your information, but not to all of your information. Should you request it, we will provide you with an electronic file of your basic account information and the information you create on the spaces under your sole control, like your personal Bitbucket repository.

Our policy towards children

Our Services are not intended for use by anyone under the age of 16. If we become aware that a child under 16 has provided us with personal information, we will take steps to delete such information.

Regional disclosures

Depending on where you live, you may have specific privacy rights that apply to you. The following privacy representations and disclosures are intended to supplement the main privacy policy and provide additional information about those rights and other information relevant to data subjects located in the following jurisdictions.

- For data subjects located in the European Economic Area or the United Kingdom, please refer to the European Economic Area and United Kingdom privacy disclosures below.
- For residents of the United States, please refer to the U.S. State privacy disclosures below.

European Economic Area and United Kingdom privacy disclosures

If you are an individual in the European Economic Area (EEA) or United Kingdom (UK), we collect and process information about you only where we have legal bases for doing so under applicable data protection laws. The legal bases depend on the Services you use and how you use them. This means we collect and use your information only where:

- We need it to provide you the Services and personalise your experience, provide customer support and to maintain Service safety and security;
- It satisfies a legitimate interest (which is not overridden by your data protection interests), such as to develop and improve our Services, to conduct marketing and promotional activities and to protect our legal rights and interests;
- You give us consent to do so for a specific purpose; or
- We need to process your data to comply with a legal obligation.

If you have consented to our use of information about you for a specific purpose, you have the right to change your mind at any time, but this will not affect any processing that has already taken place. Where we are using your information because we have a legitimate interest to do so, you have the right to object to that use, though, in some cases, this may mean no longer using the Services.

The following chart identifies the applicable legal basis for each processing purpose:

Purpose (see the "How we use information" section for more detail)	**Legal basis**
• To provide the Services and personalize your experience; • To develop and improve the Services, including machine learning and artificial intelligence model training; • To communicate with you about the Services; • To conduct marketing and promotional activities; • To provide customer support; • Verify your account credentials as needed to log you into the Services and help safeguard your account's security; • Protect our rights, privacy, safety, or property, and/or that of our affiliated companies, you, or other	Legitimate interests (Article 6(1)(f) GDPR)

parties, including to enforce this privacy policy and any other agreements or policies; • Detect and prevent fraud, illegal activity, or violations of the terms of our agreements and our Service policies, and to maintain the security of our IT systems, architecture, assets, customers, and networks; and • Aggregate or de-identify data.	
• To provide the Services and personalize your experience; • To develop and improve the Services; • Communicate with you about changes to our terms, conditions, or policies; or to respond to your inquiries, comments, feedback, or questions; • Verify your account credentials as needed to log you into the Services and help safeguard your account's security; • Process payments; • Detect and prevent fraud, illegal activity, or violations of Service policies, and to maintain the security of our IT systems, architecture, assets, customers, and networks; and • Protect our rights, privacy, safety, or property, and/or that of our affiliated companies, you, or other parties, including to enforce this	Contractual necessity (Article 6(1)(b) GDPR)

privacy policy and any other agreements or policies.	
• To develop and improve the Services; • Publish testimonials or featured customer stories; and • To conduct marketing and promotional activities (where you have provided consent to receive such marketing or promotions).	Consent (where legally required) (Article 6(1)(a) GDPR)
• To maintain Service safety and security; • Detect and prevent fraud, illegal activity, or violations of the terms of our agreements and our Service policies; • Authenticate account credentials, as necessary to log you into the Services and help protect the security of your account; and • Comply with legal obligations and legal process and to protect our rights, privacy, safety, or property, and/or that of our affiliated companies, you, or other parties, including to enforce this privacy policy and any other agreements or policies.	Compliance with a legal obligation (Article 6(1)(c) GDPR)

Where applicable under local law and subject to applicable exceptions, you have the following rights regarding your personal information:

- To request access to and/or a copy of certain information we hold about you (including in a portable and/or machine-readable format);
- To object to how we process your personal information;
- To update or correct your personal information;

- To request that we delete certain personal information we hold about you;
- To restrict how we process certain personal information about you;
- To request that we transfer your information to a third-party provider of services;
- To withdraw your consent at any time (where you have provided consent for the processing of your personal information); and
- To lodge a complaint with the relevant supervisory authority.

If you have a complaint or concern about your personal information, we encourage you to contact us first, and we will do our best to resolve your concern. You can submit inquiries to the appropriate representative here:

EU Representative:
Atlassian B.V.
c/o Atlassian, Inc.
350 Bush Street, Floor 13
San Francisco, CA 94104
E-Mail: eudatarep@atlassian.com

UK Representative:
Atlassian (UK) Operations Limited
c/o Herbert Smith Freehills LLP
Exchange House
Primrose Street
London EC2A 2EG
United Kingdom
E-Mail: ukrepresentative@atlassian.com

International transfers: We collect information globally and may transfer, process, and store your information outside of your country of residence, to wherever we or our third-party service providers operate for the purpose of providing you the Services. Whenever we transfer your information, we take steps to protect it.

International transfers within the Atlassian Companies: To facilitate our global operations, we transfer information globally and allow access to that information from countries in which the Atlassian owned or operated companies have operations for the purposes described in this privacy policy. These countries may not have equivalent privacy and data protection laws to the laws of your country. When we disclose information about you within and among Atlassian corporate affiliates, we make use of the Data Privacy Framework to receive personal data transfers from the European Union/European Economic Area to the U.S. (see the “Data Privacy

Framework notice" section below), and the standard contractual data protection clauses (see here), which have been approved by the European Commission, to safeguard the transfer of information we collect from the European Economic Area, the United Kingdom (the "UK"), and Switzerland. Refer to this page for a list of countries to which we regularly transfer personal data.

Data Privacy Framework notice: On July 10, 2023, the European Commission's adequacy decision for the EU-U.S. Data Privacy Framework (EU-U.S. DPF) entered into force.

Atlassian, Inc. and its U.S. subsidiaries (Atlassian Network Service, Inc., Dogwood Labs, Inc., AgileCraft LLC, Halp, Inc., Loom, Inc., Opsgenie, Inc., and Trello, Inc.) adhere to the Data Privacy Framework Principles regarding the collection, use, and retention of personal data that is transferred from the European Union and Switzerland to the U.S.

Atlassian complies with the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) as set forth by the U.S. Department of Commerce. Atlassian has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) with regard to the processing of personal data received from the European Union in reliance on the EU-U.S. DPF and from the United Kingdom (and Gibraltar) in reliance on the UK Extension to the EU-U.S. DPF. Atlassian has certified to the U.S. Department of Commerce that it adheres to the Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) with regard to the processing of personal data received from Switzerland in reliance on the Swiss-U.S. DPF. If there is any conflict between the terms in this policy and the EU-U.S. DPF Principles and/or the Swiss-U.S. DPF Principles, the Principles shall govern. To learn more about the Data Privacy Framework (DPF) program, and to view our certification, please visit https://www.dataprivacyframework.gov/.

In compliance with the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF, Atlassian commits to refer unresolved complaints concerning our handling of personal data received in reliance on the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF to TRUSTe, an alternative dispute resolution provider based in the United States. If you do not receive timely acknowledgment of your DPF Principles-related complaint from us, or if we have not addressed your DPF Principles-related complaint to your satisfaction, please visit Submit a Report - Watchdog for more information or to file a complaint. These dispute resolution services are provided at no cost to you.

The Federal Trade Commission has jurisdiction over Atlassian's compliance with the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF.

For complaints regarding EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and Swiss-U.S. DPF compliance not resolved by any of the other DPF mechanisms, you have the possibility, under certain conditions, to invoke binding arbitration. Further information can be found on the official DPF website: Data Privacy Framework.

In certain situations, Atlassian may be required to disclose personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

In the context of onward transfers, Atlassian is accountable for the processing of personal data it receives, under the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and Swiss-U.S. DPF and subsequently transfers to a third party acting as an agent on its behalf. Atlassian remains liable under the EU-U.S. DPF Principles, and the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF Principles if the Atlassian's agent processes personal information in a manner inconsistent with the EU-U.S. DPF Principles, and the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF Principles, unless the Atlassian proves that it is not responsible for the event giving rise to damage.

U.S. State privacy disclosures

The disclosures in this section apply only to U.S. residents and are intended to supplement this privacy policy with information required by applicable U.S. state laws.

The table below describes the categories of personal information we collected in the past 12 months, the purposes for which we collect and disclose this information, the categories of recipients of disclosures made for business purposes in the past 12 months, and the categories of recipients of disclosures made in the past 12 months that may be considered "sales" of personal information or "sharing" of personal information for cross-context behavioral advertising under U.S. state laws.

Category of Information	**Purpose(s) for Collecting & Disclosing**	**Recipients of Disclosures for Business Purposes**	**Recipients of "Sales" or "Sharing"**
Identifiers, such as name, email address, unique identifiers associated with	• Operate, maintain, and improve the Services	• Atlassian Companies • Atlassian Partners	Third-Party Advertising Providers

user or user account, IP Address	• Verify your account credential as needed to log you into the Services and help safeguard your account's security • Service access controls • Process payments • Develop and improve our Services • Conduct marketing and promotional activities • For safety and security • Debugging • Customer support	• Service Providers • Third-Party Apps	
Commercial information, such as purchase details, transaction records, billing information, billing address, payment card details	• Operate, maintain, and improve the Services • Process payments • Develop and improve our Services	• Atlassian Companies • Atlassian Partners • Service Providers	-NA-

	• Conduct marketing and promotional activities • For safety and security • Debugging • Customer support		
Internet or other electronic network activity information, such as information about your usage of the Services, pseudonymous IDs, clickstream data, device and connection information, browser information, crash data, referring/exit URLs, IP Address	• Operate, maintain, and improve the Services	• Atlassian Companies • Atlassian Partners • Event Sponsors • Service Providers	-NA-
Visual and audio information, such as your image, video and audio recording, with your permission	• Operate, maintain, and improve the Services	• Atlassian Companies • Atlassian Partners • Event Sponsors	-NA-

		• Service Providers	
Professional or employment information, such as job title, company name, company domain	• Operate, maintain, and improve the Services • Conduct marketing and promotional activities • Detecting security incidents • Debugging • Customer support	• Atlassian Companies • Atlassian Partners • Service Providers	-NA-
Geolocation data, such as your approximate location, IP address, time zone	• Operate, maintain, and improve the Services • Conduct marketing and promotional activities • Customer support	• Atlassian Companies • Atlassian Partners • Service Providers	Third-Party Advertising Providers
Inferences (dra wn about you based on other personal information we collect), such as preferences, interests, user behavior data	• Operate, maintain, and improve the Services • Conduct marketing and promotional activities	• Atlassian Companies • Service Providers	Third-Party Advertising Providers

Sensitive personal information, such as login credentials and passwords	• Verify your account credentials as needed to log you into the Services and help safeguard your account's security • Service access controls	• Atlassian Companies • Service Providers	-NA-

If you have questions about the categories of information we may collect about you or the sources of such information, please see the "Information we collect" section. For more details about our processing activities, please see the "How we use information" section. And for more information about how we may disclose information to third parties, please see the "How we disclose information" section.

Sensitive personal information: We do not use or disclose sensitive personal information for purposes other than permitted under applicable law.

Retention: How long we keep information we collect about you depends on the type of information, the purposes for which it was collected, applicable legal or regulatory requirements, and user expectations and preferences. After such time, we will either delete or de-identify your information or, if this is not possible (for example, because the information has been stored in backup archives), then we will securely store your information and isolate it from any further use until deletion is possible. Please see the "How long we keep information" section for more information about specific retention criteria for different categories of personal information.

Your rights: If you are a U.S. resident, you have the following rights regarding your personal information:

- To request information about our processing of your personal information;
- To request access to and/or a copy of certain information we hold about you (including in a portable and/or machine-readable format);
- To update or correct your personal information;

- To request that we delete certain personal information we hold about you, subject to certain exceptions;
- To opt out of the "sale" of personal information, the "sharing" of personal information or "targeted advertising" (as these terms are defined under applicable laws);
- The right not to be discriminated against for exercising your rights; and
- The right to appeal our decision to deny your request, if applicable.

For more information on how to exercise these your rights, please see the "How to access and control your information" section. We encourage you to manage your information, and to make use of the privacy controls we have included in our Services. In order to protect your information from unauthorized access or deletion, we may require you to provide additional information to verify your identity. If we cannot verify your identity, we may not be able to fulfill your request.

Opt out of "sales", "sharing", and "targeted advertising": You may also opt out of "sales" of personal information to third parties, "sharing" of personal information for purposes of cross-context behavioral advertising, and "targeted advertising" by clicking here and following the instructions. Where required, we also honor requests to opt out submitted via privacy preference signals recognized under applicable law, such as the Global Privacy Control ("GPC"). For more information on the GPC and how to use a browser or browser extension incorporating the GPC signal, see Global Privacy Control — Take Control Of Your Privacy . We do not knowingly sell or share the personal information of consumers under 16 years of age.

Authorized agent: You may also authorize an agent to exercise your rights on your behalf. To do this, you must provide the authorized agent with written permission to exercise your rights on your behalf, and we may request a copy of this written permission from the agent when they make a request on your behalf. We may also ask you to verify your own identity or directly confirm with you that you have granted permission to the authorized agent.

Changes to our privacy policy

We may change this privacy policy from time to time. We will post any privacy policy changes on this page and, if the changes are significant, we will provide a more prominent notice by adding a notice on the Services homepages, login screens, or by sending you an email notification where you have subscribed to receive legal updates. We also keep prior versions of this privacy policy in an archive here. We encourage you to review our privacy policy whenever you use the Services to stay informed about our information practices and the ways you can help protect your privacy.

If you disagree with any changes to this privacy policy, you will need to stop using the Services and deactivate your account(s) and/or submit a request to delete your personal information, as outlined in the "How to control and access your information" section.

How to contact us

Your information is controlled by Atlassian Pty Ltd and Atlassian, Inc. If you have questions or concerns about how your information is handled, or if you wish to exercise your rights, please direct your inquiry to Atlassian Pty Ltd, which we have appointed to be responsible for facilitating such inquiries:

Atlassian Pty Ltd
c/o Atlassian, Inc.
350 Bush Street, Floor 13
San Francisco, CA 94104
E-Mail: privacy@atlassian.com

Individuals in the European Economic Area or United Kingdom may also contact the appropriate representatives identified in the "European Economic Area and United Kingdom privacy disclosures" section.

Exhibit J

Atlassian Service Level Agreement

Effective starting: April 30, 2025

1. **Service Level Commitment.** For Eligible Cloud Products (as listed in the table in **Appendix A**) Atlassian must provide the following monthly uptime percentage to Customer (the "**Service Level Commitment**"):

Cloud Plan	Service Level Commitment
Premium	99.9%
Enterprise	99.95%

2. **Service Credits.**

2.1. Eligibility. To be eligible to receive a service credit for Atlassian's failure to meet the Service Level Commitment ("**Service Credit**"), Customer must submit a ticket at https://support.atlassian.com with all fields fully and accurately completed within fifteen (15) days after the end of the calendar month in which the alleged failure occurred and provide any other reasonably requested information or documentation (for instance, as described here). Atlassian's monitoring and logging infrastructure is the sole source of truth for determining whether Atlassian has met the Service Level Commitment.

2.2. Issuance. If Atlassian confirms a failure to meet the Service Level Commitment, Atlassian will apply the Service Credit, which will be calculated as described in Appendix B, against a future payment due from Customer for the affected Cloud Product, provided that Customer's account is fully paid up, without any overdue payments or disputes. No refunds or cash value will be given for unused Service Credits. Service Credits may not be transferred or applied to any other Atlassian account or Product. The aggregate maximum Service Credit applied to an invoice will not exceed 100% of the amount invoiced for the affected Cloud Product in that invoice billing period (which, since Service Credits are applied to future payments, is not the month in which the affected Cloud Product was unavailable).

2.3. Reseller Purchases. If Customer purchased the affected Cloud Product through a Reseller, (a) Customer or the Reseller may submit a ticket as described in Section 2.1 above; and (b) any Service Credit will be based on the fees invoiced by Atlassian to the Reseller for Customer's use of the affected Cloud Product under the Reseller's applicable order(s) with Atlassian. Atlassian will issue any associated Service Credits to the Reseller (and not directly to Customer), and the Reseller will be solely responsible for issuing the appropriate amounts to Customer.

3. **Exclusions.** Customer is not entitled to Service Credits if Customer is in breach of the Agreement (as defined below) or has not provisioned the relevant Cloud Product. The Service Level Commitment does not include unavailability to the extent due to: (a) Customer's use of the Cloud Products in a manner not authorized under the Agreement; (b) force majeure events or other factors outside of Atlassian's reasonable control, including internet access or related problems; (c) Customer equipment, software, network connections or other infrastructure; (d) Customer Data or Customer Materials (or similar concepts defined in the Agreement); (e) Third-Party Products; or (f) routine scheduled maintenance or reasonable emergency maintenance as stated in the Atlassian Maintenance Policy. The Service Level Commitment does not apply to (i) sandbox instances or Free or Beta Products (or similar concepts in the Agreement) or (ii) features excluded from the Service Level Commitment in the applicable Documentation.

4. **Exclusive Remedies.** Service Credits are Customer's exclusive remedy and Atlassian's entire liability for Atlassian's failure to meet the Service Level Commitment.

5. **Definitions**. All capitalized terms used and not defined in this Service Level Agreement have the meanings given to them in the applicable agreement between Customer and Atlassian for the relevant Cloud Products referencing this Service Level Agreement ("**Agreement**").

Appendix A – Eligible Cloud Products and Covered Experiences

Eligible Cloud Product	Covered Experience*
Jira (Premium and Enterprise)	• View Issue • Create Issue • Edit Issue • View Board
Confluence (Premium and Enterprise)	• View Page • Create Page • Edit Page • Add Page Comment
Jira Service Management (Premium and Enterprise)	• View Issue • Edit Issue • View Queue • Raise Request from Help Desk • Receive Alert
Bitbucket (Premium)	• Create Pull Request • Approve Pull Request • View Pull Request DIFF • Git Transactions SSH • Git Transactions HTTPS • Pipeline Started**
Compass (Premium)	• View Component • Create Component • Edit Component
Loom (Business + AI*** and Enterprise)	• View Video
Jira Product Discovery (Premium)	• View Issue • Create Issue • Edit Issue • View Project Board • View Project List • View Project Timeline • View Project Matrix

Notes:

* Except for Bitbucket GIT transactions and Jira Service Management 'Receive Alert', Covered Experiences include browser-based experiences only (not, e.g., integrations, API calls or mobile versions).

** Bitbucket Cloud-hosted builds only (excludes self-hosted runners)

*** For purposes of this Service Level Agreement, Loom Business + AI will be considered a Premium Plan Cloud Product.

Opsgenie and Jira Align Cloud operate under separate Service Level Agreements available here.

Appendix B – Service Credits

- Premium Plan Cloud Products -

Monthly Uptime Percentage	Service Credit*
Less than 99.9% but greater than or equal to 99.0%	10%
Less than 99.0% but greater than or equal to 95.0%	25%
Less than 95.0%	50%

Notes:

* Percentage of the monthly fees attributed to the affected Eligible Cloud Product. The percentage of monthly fees attributable to an Eligible Cloud Product when purchased together with other Products under one SKU will be determined by Atlassian.

- Enterprise Plan Cloud Products -

Monthly Uptime Percentage	Service Credit*
Less than 99.95% but greater than or equal to 99.9%	5%
Less than 99.9% but greater than or equal to 99.0%	10%
Less than 99.0% but greater than or equal to 95.0%	25%
Less than 95.0%	50%

Notes:

* Percentage of the monthly fees attributed to the affected Eligible Cloud Product. The percentage of monthly fees attributable to an Eligible Cloud Product when purchased together with other Products under one SKU will be determined by Atlassian.

Calculation

The monthly uptime percentage indicated in the above tables is determined by subtracting from 100% the percentage of Downtime Minutes (as defined below) out of the total minutes in the relevant calendar month. This calculation is done independently for each Eligible Cloud Product. All calendar months are measured in the UTC time zone.

Example calculation

- Total minutes in a 30-day calendar month: 43,200
- Downtime Minutes in the same month: 60
- Percentage of Downtime Minutes: 0.138889%
- 100% minus 0.138889% results in a monthly uptime percentage of 99.86%
- Subject to the terms of this Service Level Agreement, in this example, the customer is eligible for Service Credits equivalent to 10% of the monthly fees attributable to the affected Eligible Cloud Product for the month in which the failure occurred.

Definitions

- "**Covered Experiences**" are specified for each Eligible Cloud Product in Appendix A.
- "**Downtime Minute**" occurs when the Error Rate in a given minute is greater than 5%.
- "**Error Rate**" means, over a given 1-minute period, the percentage of Customer's requests to Covered Experiences resulting in an error out of Customer's total requests to those Covered Experiences. For example, subject to the terms of this Service Level Agreement, where Atlassian confirms for a given minute that
    - all Covered Experiences were completely inoperable or unable to receive Customer's requests, the Error Rate for that minute is 100%. It counts as a Downtime Minute for the affected Eligible Cloud Product.
    - 10 of 100 requests by Customer to at least one Covered Experience were unsuccessful, the Error Rate for that minute is 10%. It counts as a Downtime Minute for the affected Eligible Cloud Product.
    - 1 of 100 requests by Customer to at least one Covered Experiences were unsuccessful, the Error Rate for that minute is 1%. It does not count as a Downtime Minute for the affected Eligible Cloud Product.
    - Customer attempted no requests to any of the Covered Experiences over a minute, the Error Rate for that minute is 0%. It does not count as a Downtime Minute for the affected Eligible Cloud Product.

Exhibit K

ATLASSIAN

Third-Party Code Policy

Effective starting: November 22, 2024

This Third-Party Code Policy supplements the attached Atlassian Customer Agreement or another agreement entered between Customer and Atlassian (the "**Agreement**"). Any capitalized terms used and not defined below have the meanings given to them in the Agreement. The Products contain code and libraries that Atlassian licenses from third parties.

1. Open Source Software in the Products.

1.1. Open Source Software. The Products include third-party technologies that are subject to separate open source or source available licenses that govern Customer's use, replication, modification or creation of derivative works and redistribution of such third-party technologies ("**Open Source Software**"). Where required, Atlassian provides attribution for the Open Source Software distributed with a Product in accordance with the applicable open source or source available license(s).

1.2. Source Code Requests. For Open Source Software subject to a license that gives Customer the right to receive the source code for the binary distributed to Customer, if the source code for the Open Source Software was not provided with the binary distribution, Customer may request a copy of the source code at ip-law@atlassian.com. To receive a copy, Customer must (a) provide the name of the Open Source Software for which Customer is requesting the source code, (b) identify the relevant Product and the date of Customer's Order for that Product, and (c) provide its entity name (if applicable) and the name of the person making the request, as well as a return mailing address and email. Atlassian may charge a fee to cover the cost of physical media and processing.

2. Combining the Products with Other Software. Customer may only modify the Products as expressly specified in the "Modifications" Section of the Agreement. In connection with any Modifications, Customer must not: (a) combine or distribute the Products with any other software, including Open Source Software, where the combined software would be subject to any license that requires, as a condition of use or distribution, that the combined software be made available in source code form, or (b) grant any third party any rights or waivers relating to any intellectual property or proprietary rights in the Products.

3. Commercial Third-Party Code in the Products.

3.1. Commercial Components. The Products also include components that Atlassian licenses commercially from third parties ("**Commercial Components**"). Customer may use Commercial Components only in conjunction with and through the Products as provided by Atlassian, and the restrictions for the Products in the Agreement also apply to Commercial Components. Commercial Components are also subject to the remainder of this Section 3.

3.2. Restrictions. Customer must not (and must not permit anyone else to): (a) install, access or attempt to access, configure or use any Commercial Component (including any APIs, tools, databases or other aspects of any Commercial Components) separately from the rest of the Product, whether for production, technical support or any other purpose or (b) modify any Commercial Component (even where provided in source code form).

3.3. Commercial Component Licensors. The applicable third-party licensor ("**Commercial Component Licensor**") retains all ownership and intellectual property rights to the Commercial Component. Commercial Component Licensors do not assume any of Atlassian's obligations under the Agreement. To the maximum extent permitted by Law, no Commercial Component Licensor will be liable to Customer for any damages whatsoever.

Exhibit L

Atlassian's Responsible Technology Principles

Our approach to apps and services designed responsibly to fast-track collaboration and unleash the potential of every team.

Explore our resources

What it means to design technology responsibly

Technology is more than just a tool

Technology is the tool that we use to drive our missions forward. It is the means, not the end. In other words, we are excited about technology not because of what it is, but rather what it can do – and what it helps teams get done.

Accountability starts with ownership

Technologies are a reflection of our societies, values, and behaviours. To truly empower teams and contribute to better outcomes across our communities, we have to take accountability for using technology responsibly.

Improvement requires collaboration

Globally, we are at a critical moment for emerging technologies like AI. We believe responsible technology and responsible AI is a challenge that no one company can solve alone. This is why we are open about our efforts and invite feedback and collaboration.

We live Atlassian's mission and values in everything we do. We seek to uphold those values when it comes to understanding what it means to act responsibly in building, deploying, and using new technologies. We pledge to use the following principles to guide our work, decision-making, and communications on the use of responsible technology. As we continue to embed these principles within Atlassian and share with companies and stakeholders, we will **learn**, **iterate**, and **improve**.

Atlassian's Responsible Technology Principles

In the spirit of our values, we are sharing the principles that we use to guide our work and decision-making.

Transparency | Trust | Accountability | Human-centricity | Community

Open communication, no bullshit

We're committed to sharing clear, straightforward details about our products, how we use technologies like AI, and how this contributes to your experiences.

Learn more →

Open communication, no bullshit

Openness is foundational to Atlassian – one of our core values is Open Company, No Bullshit. It's important that anyone who wants to make the most of new technologies is equipped with the right information to do so.

We know that transparency alone isn't enough. But as a start, we will communicate information about our products and their benefits, including what they can and cannot do. We'll let you know when and how we use new technologies like AI, and how this contributes to the way that you experience our company and products. As always, we will provide consistent information around who can access your data and for which purposes. And we'll do all of this in a clear, simple, and straightforward way: no BS.

Build for trust

Trust is at the heart of our work and our products: if someone doesn't trust our company, they won't use our products or want to work here. This extends to the technologies that underpin and power our products and our work.

We know that trust is not just about ensuring the security and privacy of our products, but is also earned and kept through our actions and commitments to reliability and performance.

So, we incorporate our privacy principles into the development and use of our technologies, including by embracing privacy by design in everything we do. In line with these practices, we seek to empower you with choices around the use of data and AI-powered tools. Similarly, we will continue to build security into the fabric of our technologies and processes, through our holistic approach based on industry best practice.

We will build on these commitments by working with our customers and partners where we can to uphold and improve the quality, security, and reliability of our technologies.

Accountability is a team sport

At Atlassian, we know a thing or two about collaboration and teamwork. Our products are powered by our own people, upon the foundational technologies that we use to deliver them – and, of course, by how our customers' teams choose to use them.

While we take ownership over our technologies, true accountability is a team sport.

We see you as part of the team that helps us act responsibly. We are committed to putting processes in place that help us obtain feedback from our stakeholders and take guidance from experts, both internally and externally. We encourage our customers to tell us if something has gone wrong. In those cases, we will investigate and work to fix it. We will also continue to share, participate, educate, and learn from others as circumstances (and standards) evolve – and focus on inspiring others to act too.

Empower all humans

At Atlassian, we want our company and our technologies to be open, inclusive, fair, and just: to reflect the human-centric values and fundamental human rights that we all share. Our journey to build responsibly reflects this goal.

We work for social and environmental progress in whatever we do, which includes a commitment to respect human rights; to invest in building inclusive teams where each Atlassian feels they belong; and to make Atlassian products and experiences fully accessible and usable for everyone.

In line with these commitments, we will assess the potential impacts of our technology on the people who use our products and services or are affected by them. We will strive to identify and mitigate unfair and unjust outcomes on individuals and groups by understanding where these outcomes may arise.

Unleash potential, not inequity

We know that behind every great human achievement, there is a team. We also believe that new technologies can help empower those teams to achieve even more. If we use these technologies responsibly and intentionally, then we can supercharge this vision and contribute to better outcomes across our communities.

We seek to empower all teams in their use of technology. We will look at new technologies through the lens of how they can add value for every team member, and identify ways in which this value can be distributed equitably and accessibly across teams. If a potential use of that technology doesn't achieve that balance, it may require a rethink. Ultimately, we want our use and development of new technologies to contribute to driving growth, prosperity, and more beneficial outcomes across society.

Resources

Join us by applying the practices we use when deploying new technologies across your organization.

Our No BS Guide to Responsible AI Governance

Learn about our approach to embedding responsible technology as a practice, including how a responsible technology review contributes to meaningful AI governance.

Access the guide →

Responsible Technology Review Template

Use our Responsible Technology Review Template as you embed AI governance with your teams.

Download the template →

Build accountability through feedback

We look forward to engaging with you on how technology can help build the world we want to live in.

Contact us