CODE OF BUSINESS CONDUCT AND ETHICS FOR DIRECTORS, OFFICERS, EMPLOYEES AND CONTRACTORS

THIS CODE WAS AMENDED AND RESTATED BY THE BOARD ON SEPTEMBER 14, 2021

GitLab Inc. (collectively with its subsidiaries, "*GitLab*", "*we*", "*our*") is committed to the highest standards of legal and ethical business conduct and has long operated its business consistent with written operating principles and policies that reinforce this commitment. This Code of Business Conduct and Ethics (this "*Code*") adopted by GitLab's Board of Directors (the "*Board*"), acting through authority delegated to its Audit Committee (the "*Audit Committee*"), summarizes the ethical standards for all directors, officers, employees and contractors of GitLab and of its direct and indirect subsidiaries ("*Team Members*") and is a reminder of the seriousness of our commitment to our values. Compliance with this Code is mandatory for every Team Member. In addition to this Code, Team Members are subject to and must comply with other policies and programs of GitLab, as applicable.

INTRODUCTION

- Our business is complex in terms of the geographies and cultures in which we function and the laws with which we must comply. To help Team Members understand what is expected of them and to carry out their responsibilities, we have created this Code. Responsibility for overseeing adherence to this Code shall rest with the Chief Legal Officer of GitLab ("*CLO*"), as instructed by the Audit Committee.

- This Code is not intended to be a comprehensive guide to all of our policies or to all responsibilities under law or regulation. All Team Members are expected to be familiar with applicable laws and regulations in their area of operation, and GitLab expressly prohibits any activity by Team Members that violates any applicable law or regulation. This Code is a guideline, or a minimum requirement, that must always be followed.

- We expect each Team Member to read and become familiar with the ethical standards described in this Code. Violations of the law, our corporate policies, or this Code may result in disciplinary action, including dismissal.

KEY CORPORATE VALUES

- GitLab values and wishes to hold its Team Members to a code of conduct that seeks alignment with the following key corporate values:

Collaboration & Transparency

- Collaboration is one of our core values. It encompasses kindness, respect, positive intent, and fostering a supportive environment among other key beliefs. Collaboration means that we value people equally, regardless of their seniority level at GitLab, race, religion, ethnic

background, gender or other personal attributes such as age, physical appearance and so on. People are to be treated with dignity, kindness and common courtesy.

- Collaboration also pertains to truthfulness and transparency of motives. By being transparent, we reduce the threshold to contribution and make collaboration easier. We want to be truthful always, but most so when the other party needs to know the truth, regardless of how it may disadvantage us. We wish to be upfront about the motives that drive our goals, strategies, and behaviors.

Results, Efficiency & Iteration

- GitLab strives to do what we promised to each other, our customers, users and investors. We reward, recognize and celebrate superior performance across all business disciplines. We want to excel and be the best at what we do. We will continually raise the bar on ourselves and communicate explicitly with our operating units and our Team Members on their performance.

- We not only focus on our results but our customers' results. Our customers are the people who buy and use our products and services. We would not be here without our customers, we would not be a business without our customers, and we could not continue to exist without our customers.

- Our daily choices center on what's best in the aggregate for our collective group of customers. We care about working on the right things, not doing more than needed, and not duplicating work.

- We endeavor to have a culture of iteration, one that is invested in continually improving our abilities to execute our stated strategies in all disciplines, in contrast to a culture that obsesses more with strategy, than execution. When we take smaller steps, ship smaller and start with simpler features, we get feedback sooner.

Diversity, Inclusion and Belonging

- Diversity, inclusion and belonging are principles fundamental to the success of GitLab. We aim to make a significant impact in our efforts to foster an environment where everyone can thrive. We actively chose to build and institutionalize a culture that is inclusive and supports all Team Members equally in the process of achieving their professional goals. We also work to make everyone feel welcome and to increase the participation of underrepresented minorities and nationalities in our community and GitLab.

- GitLab is committed to creating a discrimination-free work environment, and each Team Member is expected to create a respectful workplace culture that is free of harassment, intimidation, bias and unlawful discrimination. We strive to make all employment decisions based on a principle of mutual respect and dignity consistent with applicable laws.

FAIR DEALING

- Team Members are required to deal honestly, ethically and fairly with customers, partners, suppliers, competitors and other third parties. We:

  o prohibit bribes, kickbacks or any other form of improper payment, direct or indirect, to any representative of a government, labor union, customer or supplier in order to obtain a contract, some other commercial benefit or government action;

  o prohibit Team Members from accepting any bribe, kickback or improper payment from anyone;

  o prohibit gifts or favors to or from any customer or supplier, except for promotional material of nominal value and gifts of modest value that are related to commonly recognized events or occasions; limit marketing and client entertainment expenditures to those that are necessary, prudent, job related and consistent with our policies;

  o require clear and precise communication in our contracts, advertising, literature and other public statements and seek to eliminate misstatement of fact or misleading impressions; reflect accurately on all invoices to customers the sale price and terms of sale for products and services sold or rendered;

  o protect all proprietary data our customers, partners or suppliers provide to us as reflected in our agreements with them or as compelled by law; and prohibit our representatives from otherwise taking unfair advantage of our customers, partners or suppliers, or other third parties, through manipulation, concealment, abuse of privileged information or any other unfair-dealing practice.

CONFLICTS OF INTEREST

- GitLab recognizes and respects Team Members' rights to engage in outside activities that they may deem proper and desirable, provided that these activities do not impair or interfere with the performance of their duties to GitLab or their ability to act in GitLab's best interests. However, all Team Members must avoid situations in which their personal interests may conflict, or appear to conflict, with the interests of GitLab.

- It is not possible to list every situation that might give rise to a conflict of interest, but the information that follows serves as a guide, pointing out important areas where conflicts may arise. The responsibility for conduct within the letter and the spirit of this Code regarding conflicts of interest rests with each individual. It is, however, important to avoid not only any situation that is an obvious conflict of interest, but also to be aware of situations that might appear to be a conflict.

Use of GitLab Property

In the absence of prior GitLab approval, assets of GitLab should be used for legitimate business purposes and for personal purposes only to the extent allowed by GitLab policy. All Team

Members have an obligation to use GitLab property efficiently and to report any theft or damage to GitLab property to appropriate GitLab management personnel.

By using any GitLab electronic equipment or systems or by accessing the Internet or any GitLab intranet using a GitLab sign-on ID or any GitLab computer equipment or systems, a Team Member acknowledges that they represent GitLab and agree to comply with our Internal Acceptable Use Policy. The Internal Acceptable Use Policy specifies requirements related to the use of GitLab computing resources and data assets by Team Members so as to protect GitLab and its customers, Team Members, contractors, and other partners from harm caused by both deliberate and inadvertent misuse.

Dealings with Partners, Suppliers and Competitors

Team Members shall select and deal with suppliers, customers, partners and other persons doing or seeking to do business with GitLab in an impartial manner, without favor or preference based upon any considerations other than the best interests of GitLab. Team Members shall not seek or accept, directly or indirectly, any payments, fees, services, or loans from any person or business entity that does or seeks to do business with GitLab. This does not, however, prohibit a Team Member from receiving compensation for outside services that GitLab permits such person to render, when such outside services will not affect the impartial discharge of such person's duties or obligations to GitLab. In the absence of prior GitLab approval, with regard to any person or business entity that does or seeks to do business with GitLab, Team Members shall not seek or accept for themselves, or any member of their families, any gifts, entertainment, or other favors of a character that goes beyond common courtesies consistent with ethical and accepted business practices and are consistent with our internal policies.

Interests In or Relationships with Other Companies

Team Members shall not own, directly or indirectly, a financial interest (other than the ownership of less than 1.00% of the capital stock of a competitor whose common stock is publicly traded) in any business entity that is in competition with, or a significant financial interest in any business entity that does or seeks to do business with, GitLab except where such interest has been fully disclosed to GitLab and a determination has been made by GitLab that such interest will not influence any decision that such person might be required to make performing duties for GitLab. Team Members shall not accept a directorship or other managerial position in, or serve as a consultant or employee of, a business entity, organized for profit, that does or seeks to do business with, or is in competition with, GitLab, without receiving specific approval from their direct supervisor.

Loans

Under SEC rules, we are not allowed to provide loans (or guarantee loans) to our executive officers and directors or their family members. The Compensation and Leadership Development Committee of the Board must approve any GitLab loan to any other service provider. No supervisor shall solicit a loan from a subordinate or accept a loan from a subordinate.

Reporting Obligations

Team Members shall report in writing to their direct supervisor any personal ownership interest or other relationship that might affect their ability to exercise impartial, ethical business judgments in their area of responsibility. Each situation reported shall be reviewed by the Team Member's supervisor, and the supervisor shall make a determination, with guidance from the Compliance Officer, as to whether a conflict of interest exists or may arise from such a situation. All Team Members shall give GitLab their fullest cooperation in the correction of any situation in which a conflict exists or may arise. If the Team Member to whom the ownership interest or relationship relates is an officer of GitLab, such relationship shall be reviewed by the CLO in the manner prescribed by GitLab's Related Party Transaction Policy.

Outside Employment

You may not engage in any outside employment that would interfere with your job performance or responsibilities. You must inform your manager, as well as our CLO, before you take on any outside employment that might cause a potential conflict.

Business with Related Parties

- You should avoid conducting any Company business with a relative or significant other, or with a business with which you, a relative or significant other is significantly associated. A potential conflict of interest can arise if you direct business from the Company to these types of related parties. To prevent a conflict of interest, employees directing business to or from the Company should discuss the situation with their manager and remove themselves from the decision-making process.

- Even if a related-party transaction appears to be in the Company's best interests, you must first fully disclose the transaction to our Chief Legal Officer, and receive approval from our Audit Committee, before engaging in that transaction. If you discover after the fact that we have done business with a related party, you must promptly report it to our Chief Legal Officer, who will refer the matter for approval from our Audit Committee. If you are an executive officer, a member of the Board or a significant shareholder, please also refer to our Related Party Transactions Policy for more information.

Outside Advisory or Board Service

You must obtain approval from our CLO for certain outside activities that could present an actual or potential conflict of interest with your professional responsibilities at GitLab. For example, serving on advisory boards or boards of directors, or being appointed to industry groups may present actual or potential conflicts. Board members must notify our CLO either in advance of, or promptly after, accepting a new board directorship. Team Members must disclose to their manager, in advance, outside activities that may or will impact the Team Member's ability to perform the essential functions of their position at the expected level.

CONFIDENTIALITY AND CORPORATE ASSETS AND CORPORATE OPPORTUNITIES

Team Members are, on occasion, entrusted with GitLab confidential information and with the confidential information of GitLab suppliers, customers or other business partners. This information may include: (1) technical or scientific information about current and future services or research; (2) business or marketing plans or projections; (3) earnings and other internal financial data; (4) personnel information; (5) supply and customer lists; and (6) other non-public information that, if disclosed, might be of use to competitors, or harmful to GitLab's suppliers, customers or other business partners. This information is the property of GitLab, or the property of its suppliers, customers or business partners, and in many cases was developed at great expense. All Team Members, upon commencement of employment with GitLab, shall sign offer letters or contractor agreements that contain confidentiality provisions (the "*Confidentiality Agreement*") provided by GitLab. Strict adherence to the Confidentiality Agreement is required of each Team Member.

Team Members shall not take for themselves, or for family members or any other entities with which they are affiliated, any opportunity of which they become aware through the use of GitLab property or information, or through their position with GitLab, and shall not use GitLab property or information, or their position with GitLab, for personal gain other than actions taken for the overall advancement of the interests of GitLab.

SPECIAL ETHICS OBLIGATIONS FOR TEAM MEMBERS WITH FINANCIAL REPORTING RESPONSIBILITIES

The Chief Executive Officer, Chief Financial Officer, and Finance Department personnel bear a special responsibility for promoting integrity throughout the organization, with responsibilities to stakeholders both inside and outside of GitLab. The Chief Executive Officer, Chief Financial Officer, and members of the Finance Department have a special role not only to adhere to these principles themselves but also to ensure that a culture exists throughout GitLab as a whole that ensures the fair, accurate, comprehensive and timely reporting of financial results. Because of this special role, the Chief Executive Officer, Chief Financial Officer, all members of the Finance Department and all other Team Members, must:

- act with honesty and integrity, avoiding actual or apparent conflicts of interest in personal and professional relationships;

- provide information that is accurate, complete, objective, timely and understandable to ensure full, fair, accurate, timely, and understandable disclosure in reports and documents that GitLab files with, or submits to, government agencies and in other public communications;

- comply with applicable governmental laws, rules and regulations, and acquire appropriate knowledge of such laws, rules and regulations relating to GitLab' duties sufficient to enable the Team Member to recognize potential dangers and to know when to seek legal advice;

- promptly report to the CLO and/or the Chairman of the Audit Committee any conduct believed to be a violation of law or business ethics or of any provision of this Code, including any transaction or relationship that reasonably could be expected to give rise to such a conflict; and

- promote accountability to this Code among all Team Members.

COMPLIANCE WITH ALL LAWS, RULES AND REGULATIONS

GitLab will comply with all laws and governmental regulations that are applicable to its activities and expects all Team Members to obey the law. Laws can be complex and at times, even counterintuitive. Although it's impossible to know all aspects of every law, you should understand the major laws, rules and regulations that apply to your work. You should consult with our CLO if you are unsure or have any questions or concerns related to your work. A few specific areas of legal compliance are discussed in greater detail below.

Insider Trading

Because we believe firmly in transparency and trust across the organization, you may find yourself in possession of inside information. The definition of inside information is any material nonpublic information, positive or negative, about GitLab or other organizations with which we work. For a definition of "material non-public information," please see our Insider Trading Policy. Remember that we also may possess confidential information about our customers, partners or other third parties. It is equally important that we treat this information with the same care that we treat our own.

The bottom line is that we never buy or sell securities based on inside information, nor do we tip off others to do so. It doesn't matter how we learned the information—using material nonpublic information to trade securities is never acceptable. Doing so violates the law and the trust we have built with our fellow Team Members, and with our customers, partners and investors, and others.

To learn more, please review our Insider Trading Policy, which explains how you lawfully can trade in our stock, as well as our trading windows, blackout periods and trading plans.

No Bribery or Corruption

All forms of bribery and corruption are prohibited. We will not tolerate bribery or corruption in any form or for any purpose. There is no potential benefit that can justify damaging our integrity and reputation or the trust others place in us.

All persons subject to this Code must comply fully with the Foreign Corrupt Practices Act (FCPA) and other applicable laws that prohibit bribery and corruption. Many of these laws are very broad and apply to both government and private or commercial bribery and corruption.

You are responsible for ensuring that you understand the applicable laws and our Anti-Corruption Policy. If you have a question regarding any gift, entertainment or other expense, consult with our CLO before you incur or authorize the expense.

Unlawfully Obtaining Business Intelligence

Gathering information about our competitors, often called competitive intelligence, is a legitimate business practice. It helps us stay competitive. However, we must always obtain business intelligence appropriately from legitimate sources. You must not steal or unlawfully use the

information, material, products, intellectual property or proprietary or confidential information of others, including that of business partners and customers. These rules also apply to consultants, vendors and other partners we retain.

Fair Sales and Marketing Practices

We compete vigorously for business based solely on the merits of our products and services. We do not participate in any activities that unfairly harm competition. We want to win, but win fairly.

We will accurately represent GitLab and our products and services in our marketing, advertising and sales materials. We can promote our products and services and make comparisons between us and our competitors.

Deliberately misleading messages, leaving out important facts or false claims about our products and services or competitors are inconsistent with our policies.

Antitrust laws govern relationships between a company and its competitors. Collusion among competitors is illegal and the consequences of a violation are severe. You must not enter into an agreement or understanding of any kind with competitors concerning prices, discounts or other terms or conditions of sale; profits or profit margins; costs; allocation of products, services, customers, markets or territories; boycotts of customers or suppliers; or bids or the intent to bid or even discuss or exchange information on these subjects.

RESPECTING HUMAN RIGHTS

We are committed to respecting human rights to ensure that our business plays a positive role in the communities in which we operate. We respect human rights by seeking to avoid infringing on the rights of others and working to address adverse human rights impacts with which we are involved. We expect Team Members, partners, suppliers, customers and governments to share this commitment.

FINANCIAL MATTERS AND BUSINESS PRACTICES

You are expected to act responsibly and exercise sound judgment with respect to our finances and financial reporting. Investors rely on accurate and fair financial and business information to understand our financial results and make informed decisions. You may execute financial transactions only with authorization and in compliance with our policies. You also are expected to record and report all financial transactions and business information honestly and accurately, to comply with our system of internal controls and to follow applicable laws, regulations and accounting practices.

We regularly file reports and other documents with regulatory authorities, including the U.S. Securities and Exchange Commission ("*SEC*"). In addition, we may make other public communications, such as press releases, from time to time.

Depending upon your position with the Company, you may be called upon to provide information to help ensure that our public reports and communications are complete, fair, accurate and understandable. You are expected to use all reasonable efforts to provide complete, accurate, objective, relevant, timely and understandable answers to inquiries related to our public disclosures. Team Members involved in preparing public reports and communications must use all reasonable efforts to comply with our disclosure controls and procedures.

If you believe that any disclosure is materially misleading or if you become aware of any material information that you believe should be disclosed to the public, it is your responsibility to bring this information to the attention of our CLO. If you believe that questionable accounting or auditing conduct or practices have occurred or are occurring, you should follow the procedures set forth in our Whistleblower Policy.

SEC Reporting and Financial Statement Preparation

Our periodic reports and other documents filed with the SEC, including all financial statements and other financial information, must comply with applicable federal securities laws, and SEC rules. If you contribute in any way to the preparation or verification of our financial statements and other financial information, you must ensure that our books, records and accounts are accurately maintained. You must also cooperate fully with our finance department, as well as our independent public accountants and counsel. If you are involved in the preparation of our SEC reports or financial statements, you must:

- Be familiar with and comply with our disclosure controls and procedures and our internal control over financial reporting.

- Take all necessary steps to ensure that all filings with the SEC and all other public communications about our financial and business condition provide full, fair, accurate, timely and understandable disclosure.

Quarterly Compliance Certifications

Depending on your position here at GitLab, we may ask you to certify your knowledge of various facts each quarter. We rely on certifications to record transactions, make legal and accounting determinations and comply with laws. If you do not provide a certification or complete a certification completely, honestly and accurately, you may be in violation of this Code. This will result in disciplinary action up to and including termination of your service with the Company.

Business Expenses

You are expected to incur business expenses wisely. When you submit an expense for reimbursement or spend money on our behalf, you must make sure that the cost is reasonable, directly related to our business, supported by appropriate documentation and in compliance with our policies. Always submit expense reports in a timely manner, record the business purpose and relevant details and comply with all submission requirements. If you are uncertain about whether you should spend money or submit an expense for reimbursement, check with your manager. Managers are responsible for all money spent and expenses incurred by their direct reports and should carefully review such expenses and supporting receipts before approving.

Money-laundering and Third-party Payments

We are committed to complying fully with all anti money-laundering and antiterrorism laws throughout the world. Money laundering occurs when individuals or organizations attempt to conceal illicit funds or make such funds look legitimate. If you are requesting payments to vendors or potential vendors, or are monitoring payments we receive, you must flag suspicious activity. The following examples may be indications of potential money laundering:

- Attempts to make large cash payments

- Payments by or to someone who is not a party to the relevant contract

- Requests to pay more than provided for in the relevant contract

- Payments made in currencies other than those specified in the relevant contract

- Payments from an unusual, non-business account

QUESTIONS, REPORTING AND EFFECT OF VIOLATIONS

Compliance with this Code is, first and foremost, the individual responsibility of every Team Member. GitLab attempts to foster a work environment in which ethical issues and concerns may be raised and discussed with supervisors or with others without fear of retribution.

If a Team Member is aware of a suspected or actual violation of this Code by others, they have a responsibility to report it in accordance with the procedures outlined below. The Team Member and GitLab will be best served by bringing the concern into the open so that any problems can be resolved quickly, and more serious harm is prevented. GitLab will not allow any retaliation against any Team Member who acts in good faith in reporting any violation of this Code or against any person who is assisting in good faith in any investigation or process with respect to such a report. Any Team Member who participates in any such retaliation is subject to disciplinary action, including termination.

GitLab offers Team Members many ways to get answers to their questions about ethical issues and to raise any concern about a possible violation of this Code:

- Generally, each Team Member's direct supervisor or manager (or another supervisor or manager) will be in the best position to resolve the issue quickly.

- If after raising an ethics or conduct concern the issue is not resolved, raise it with GitLab's People Group or CLO.

- Contact EthicsPoint, GitLab's 24-hour hotline as outlined below.

- Team Members can raise their concerns orally or in writing.

While GitLab prefers that each Team Member gives his or her name and other pertinent information when making a report because it makes the investigation and resolution of the suspected violations being reported more effective and efficient, if Team Members prefer, they may also make a report anonymously.

GitLab has also engaged Navex Global to provide EthicsPoint, its comprehensive and confidential reporting tool, to provide an anonymous hotline for all Team Members. The purpose of the service is to ensure that any Team Member wishing to submit a report anonymously can do so without the fear of retribution.

EthicsPoint toll free numbers and other methods of reporting are available 24 hours a day, 7 days a week for use by Team Members.

• Website: http://gitlab.ethicspoint.com/

• Mobile intake site: http://m.gitlab.ethicspoint.com/

• USA Telephone: toll-free at 1-833-756-0853

• All other countries: to view phone number, please see web intake site and select the country in which you are located from the drop-down menu. If your country is not listed, please select the "Make a Report" link at the top of the page to access the confidential reporting tool.

Reports sent to EthicsPoint are shared with the CLO and the Chairperson of the Audit Committee.

These procedures have been established so that properly trained individuals will be made aware of and can then investigate any alleged violation of this Code. Team Members may not conduct their own investigation either before or after making a report.

Team Members who violate any law, governmental regulation or this Code will face appropriate, case-specific disciplinary action, which may include demotion or discharge. Violating this Code may also mean breaking the law, subjecting such Team Member and/or GitLab to criminal penalties (fines or prison sentences) or civil sanctions (damage awards or fines).

Reporting Contacts:

• **Chief Legal Officer** – Robin Schulman Email: robin@gitlab.com

• **Audit Committee Chairperson** – Karen Blasing Email: karenblasing@gmail.com

ADMINISTRATION, WAIVER AND AMENDMENT

The Audit Committee is responsible for administering the Code. It has established the standards of business conduct contained in this Code and oversees compliance. The Audit Committee has delegated day-to-day responsibility for administering and interpreting the Code to the CLO. While serving in this capacity, the CLO reports directly to the Audit Committee.

Any waiver of any provision of the Code for the benefit of a director or an executive officer (which includes without limitation, for purposes of the Code, GitLab's principal executive, financial and accounting officers), shall be effective only if approved by the Board in its sole discretion. Any waivers of the Code for other Team Members may be made by the CLO or Audit Committee.

We are committed to continuously reviewing and updating our policies and procedures. Therefore, this Code is subject to modification. Any amendment of this Code must be approved in writing by the Audit Committee and will be promptly communicated to you.

Any amendments or waiver may be publicly disclosed if required by applicable laws, rules and regulations.