## PURPOSE

All of the policies listed below are important for GitLab team members to read and understand as they deal with people benefits, entity specific issues, and procedures and requirements of the company. If you have any questions around the internal policies, please reach out to People Operations at people-connect@gitlab.com.

## SCOPE

These policies apply to all GitLab team members, contractors, advisors, and contracted parties interacting with GitLab computing resources and accessing company or customer data.

## ROLES AND RESPONSIBILITIES

| Role | Responsibility |
| --- | --- |
| GitLab Team Members | Responsible for following the requirements in these policies |
| PeopleOps | Responsible for implementing and executing these policies |
| Legal & PeopleOps Management (Code Owners) | Responsible for approving significant changes and exceptions to these policies |

# GENERAL EMPLOYMENT PRACTICES

## Open Door Policy

We encourage communication between team members at all levels of the organization. This is an important part of our culture. Whenever problems or concerns arise, it is expected that they will be addressed as quickly as possible. Your immediate manager is the person on the management team who is closest to you and your work. When you need help or have questions, concerns, problems, or suggestions, please contact your manager first. It is your manager’s responsibility to assist you - so please ask, and be willing to work the issue out with your manager. They are interested in your success, the success of every team member in their department, and the overall success of GitLab.

If your manager cannot help you or answer your questions, your questions will be referred to someone who can. If you feel your particular question, concern, or suggestion cannot be discussed with your manager, you are encouraged to contact your manager’s manager, your assigned People Business Partner or Team Member Relations. It is important to remember that a team member who takes these steps will not be subject to retaliation. You can expect to be treated fairly and with respect.

## Background Screenings

GitLab uses appropriate controls to ensure that its assets and its customer relationships and information are protected. To reduce these risks, GitLab will obtain and review background information of covered prospective, and, as applicable, current team members as allowed by local law. Contractors will also be required to complete a background screening per GitLab’s [Third Party Risk Management Policy](https://about.gitlab.com/handbook/security/security-assurance/security-risk/third-party-risk-management.html#independent-contractors) and as allowed by local law. GitLab will run background screenings for independent contractors that are hired directly, but otherwise, will defer to each contractor’s hiring agency’s background screening policies and processes. GitLab will complete a background screening for contractors employed by agencies that do not conduct their own background screenings.

GitLab currently contracts with Sterling Talent Solutions to provide background screenings. For all candidates being considered for a position at GitLab, an employment history for the last 5 years and/or the three most recent employers will be verified in accordance with applicable local law (if applicable local law limits the review of employment history to fewer years and/or employers, then GitLab follows local law) and screening will be performed against various denied party lists including but not limited to the Office of Foreign Asset Control’s Specially Designated Nationals and Blocked Persons List. In jurisdictions where criminal records may be reviewed, criminal records will be requested. Additional screenings may include, where applicable and in accordance with local law, a search against the U.S. Department of Health and Human Services Office of Inspector General’s List of Excluded Individuals/Entities and/or screening for financial related offenses and credit checks, when relevant to the position. GitLab may use the returned background information to make decisions regarding employment, where allowed by local law. No background screening will be run until a conditional offer has been made, unless local law explicitly requires otherwise.

In the event the background screening is not available on the scheduled hire date due to delays in processing, GitLab will run the background screening as soon as possible. The same adjudication guidelines will apply to current employees as they do with prospective employees. The Senior Background Check Specialist will monitor background screenings for completion and accuracy and will follow up accordingly regarding any concerns or issues.

The Candidate Experience Specialists will [initiate](https://about.gitlab.com/handbook/hiring/talent-acquisition-framework/coordinator/#background-screenings) all employment verifications and background screenings for candidates. The Senior Background Check Specialist will initiate any applicable retroactive background screenings or requested enhanced background screenings for current team members.

Please contact the Senior Background Check Specialist at backgroundchecks@gitlab.com regarding any questions.

### Disclosure and Authorization

Candidates (and, as applicable, current team members) will receive an email to fill out the background screening application. The application will ask for personal and professional information. The application process includes signing a disclosure and a consent form which explains the rights of an individual undergoing a background screening. The application process is designed to take less than fifteen minutes to complete.

To prepare for the employment verification for those candidates being considered for Director level positions or higher, candidates should gather each previous employer’s name and address, position title held, employment start and end dates, manager’s name and title, their phone number, and email address. Details for a Human Resources contact can be entered instead of a manager’s contact details. Occasionally, and where permitted by law, Sterling will reach out to the candidate to retrieve additional information, such as backup documentation to act as proof of previous employment or picture IDs. Proof of employment can typically be provided in various ways, such as tax returns (e.g. W2s), pay stubs, LLC documentation, official company registrations, etc. In certain circumstances, the Senior Background Check Specialist may also reach out to candidates and/or team members for additional documentation.

Background screenings will act as an additional mechanism of transparency and will help to build trust with our clients.

### Review Criteria for Candidates and Team Members

Reviews of the background screening are conducted by the Senior Background Check Specialist in accordance with the applicable law of the candidate’s jurisdiction. The Senior Background Check Specialist will first review the report for omissions, inaccuracies, and/or discrepancies with employment, including, but not limited to, dates of employment, employer names, or positions held. If the report includes discrepancies related to employment, the Senior Background Check Specialist will take the necessary steps to investigate and adjudicate the discrepancies and/or reach out to Team Member Relations for additional support and collaboration. The Senior Background Check Specialist and Team Member Relations may escalate the report, as necessary, to the Legal Employment team. Employment decisions based on the employment verification portions of the background screening report shall be finalized before any review of the criminal records information takes place.

If criminal record information has been provided, then it will be adjudicated in accordance with applicable local law. Generally, and subject to local law, criminal records are reviewed to determine if criminal convictions have a direct connection with an applicant’s ability to fulfill the job duty with competence and integrity, while also considering the safety and/or security of Gitlab team members, customers, vendors, and/or overall business. Decisions are made that are job related and consistent with business necessity. Arrest records are not considered during the adjudication process, nor is any criminal conviction information that is prohibited from being reviewed by applicable local law.

## Romantic and Family Relationships at Work

**Hiring Significant Others or Family Members**

GitLab is committed to a policy of opportunities based on **qualifications and merit** and does not discriminate in favor of or in opposition to the employment or affiliation of significant others or family members. Due to the potential for perceived or actual conflicts, such as favoritism or personal conflicts from outside the work environment, which can be carried into the daily working relationship, GitLab will hire or consider for hire significant others and/or family members of persons currently serving as team members only if **all** points below are true:

* Candidates for open roles or current team members will not be working directly for or supervising a significant other or family member.
* Candidates for open roles or current team members will not occupy a position in the same line of authority in which team members can initiate or participate in decisions involving a direct benefit to the significant other or family member. Such decisions include hiring, retention, transfer, promotion, wages, talent assessment, and leave requests.
* The team member does not have access to sensitive company and/or personal information including payroll, compensation, personnel reviews/files, job performance, etc., unless the team member’s job duties require access to such information. If the position in question requires access to such information, the team member in that position shall comply with the duty to maintain confidentiality as governed by applicable law and policy, and must seek approval from the team member’s direct manager for any decisions affecting the significant other or family member’s personnel information.

This policy applies to all current team members and candidates for open roles. In the spirit of our [Transparency](https://handbook.gitlab.com/handbook/values/#transparency) value, we ask the team member and the candidate to disclose the family relationship to the recruiter at the beginning of the hiring process. For purposes of this policy, a significant other or family member is any person who has a relation by blood, marriage, adoption, or domestic partnership within the third degree of our team member. If the candidate progresses through the process as a final candidate, and prior to any offer, the recruiter should notify the hiring manager and the People Business Partner of the family relationship to ensure there is not a conflict of interest. In addition, the GitLab team member should not be part of their family member’s interview process. If there is a concern that either the team member or the candidate may progress to a position that would trigger one of the conditions above, a waiver will be signed by both parties acknowledging that future work assignments, promotions, etc may be impacted by enforcement of this policy.

**Active Team Member Relationships (Significant Other or Family Members)**

Please report any relationship with a significant other or family member to your People Business Partner, if you find yourself in a reporting relationship with the significant other or family member. Furthermore, if two team members who are in a reporting relationship become significant others or family members in the course of their employment, they should also report the relationship to the People Business Partner. Transfers, promotions, and future work assignments will be made in accordance with all applicable anti-discrimination laws and policies.

## WORKPLACE CONDUCT

## Confidentiality

As stated in the **Confidentiality and Corporate Assets and Corporate Opportunities** section of the [Code of Business Conduct and Ethics](https://ir.gitlab.com/static-files/7d8c7eb3-cb17-4d68-a607-1b7a1fa1c95d), team members are, on occasion, entrusted with confidential GitLab 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

This information, 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 their role 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.

Team members also have obligations to protect the personal and sensitive information of our fellow team members. Therefore, you may not access and/or disseminate any team member’s personal information (i.e. address, personal phone number, salary, etc.) that the team member has not made publicly available, unless the team member has provided written permission to share this information. An exception to this restriction would be when access is a necessary function of your job duties. A violation of this obligation is considered severe and could result in disciplinary action, up to and including termination.

### Exceptions

Exceptions to this procedure will be tracked as per the [Information Security Policy Exception Management Process] (https://about.gitlab.com/handbook/security/#information-security-policy-exception-management-process). For reference see the [Parent Policy: Information Security Policy](https://about.gitlab.com/handbook/security/).

## Anti-Harassment

Please see the [Anti-Harassment Policy](https://about.gitlab.com/handbook/anti-harassment/).

## Anti-Retaliation

Please see the [Anti-Retaliation Policy](https://about.gitlab.com/handbook/legal/anti-retaliation-policy/).

## Complaint Procedure

Please see the [Complaint Procedure](https://about.gitlab.com/handbook/people-group/#how-to-report-violations).

## Social Responsibility

Please see our [Environmental, Social, and Governance](https://about.gitlab.com/handbook/esg/) page.

## Personal Appearance

The image GitLab projects to the public is reflected in the appearance of our team members. Simply stated, team members should be dressed and groomed appropriately for their specific duties. Team members are expected to use good judgment in their appearance and grooming. Read our [GitLab Events Code of Conduct](https://about.gitlab.com/company/culture/ecoc/) for more information. Please read our GitLab Events Code of Conduct for more information regarding team member responsibility during attendance at company-sponsored events.

## Job Abandonment

When a team member is absent from work for three consecutive workdays, there is no entry on the availability calendar for time off, and fails to contact their supervisor, they may be [terminated](https://about.gitlab.com/handbook/people-group/offboarding/#involuntary-terminations) for job abandonment unless otherwise required by law. If a manager is unable to reach a team member via email or slack within a 24 hour period they should contact their [People Business Partner](https://about.gitlab.com/handbook/people-group/#how-to-reach-the-right-member-of-the-people-group). The People Business partner will access the team member’s information to obtain additional contact methods and numbers. The manager and People Business Partner will create an action plan to make all attempts to contact the team member.

### Exceptions

GitLab understands there are extenuating circumstances that can occur. In the instance that a team member is absent from work for three consecutive workdays due to an emergency outside of the team members’ control (ex. an internet outage in their country of residence), the recommendation is:

* The team member should notify their manager about the situation, should a period of unavailability be a foreseen possibility.
* The team member and manager should consider exchanging cell phone numbers to stay in contact as much as possible in the case that the situation should escalate. If you are based in different countries, consider ensuring you and your manager both have an app that facilitates international communication (ex. Whatsapp, Zalo, etc.). If costs are incurred when trying to contact your manager, this can be considered a business expense and can be submitted for reimbursement through [Navan Expense](https://about.gitlab.com/handbook/finance/expenses/).
* Consider leveraging GitLab’s flexible [time off policy](https://about.gitlab.com/handbook/paid-time-off/) to take the time you need.

## TEAM MEMBER SAFETY

### Preventing Unsafe Situations

While GitLab is 100% remote, there may be times when team members travel for work-related functions or co-working events. GitLab is committed to the value of a safe, violence-free work environment and ensuring and exhibiting equal commitment to the safety and health of team members.

In general, please consider the following recommendations to ensure safety when traveling or coworking:

1. Do the research. Have some familiarity with the destination before you arrive. Check with your country’s government department that provides advice for traveling overseas:

* United States: check the State Department’s website for country updates and enroll in a Traveler Program such as [Smart Traveler Enrollment Program (STEP)](https://step.state.gov/step/).
* New Zealand: [Safe Travel](https://safetravel.govt.nz/).

1. Try not to draw attention. People who appear to be from out of town are more vulnerable to crimes. Try to respect the culture you are visiting by blending in. Consider protective clothing to avoid pickpockets or other theft. Do not flash money or credit cards unnecessarily.
2. Make copies of important documents. Consider carrying hard copies of important documents (passport, driver’s license) in a separate location in the event your documents are misplaced or stolen.
3. Keep friends and family updated. No matter whether you’re going on an overnight jaunt or a week-long international journey, it’s always a good idea to let friends or family know your plans. Before you leave, send a copy of your itinerary to a few trusted people who can keep tabs on your whereabouts. Check in regularly with your contacts so they know you’re where you’re supposed to be.
4. Be wary of public Wi-Fi. Be aware that hackers can steal sensitive information in the public forum. Use a VPN or other secure access if you plan to access sensitive data. More information on [VPN usage at GitLab](https://about.gitlab.com/handbook/security/#why-we-dont-have-a-corporate-vpn) and the [Personal VPN](https://about.gitlab.com/handbook/tools-and-tips/personal-vpn/) page.
5. Safeguard your hotel. Lock and deadbolt the door while you are in the room. Ensure the door is locked when you leave. Keep the windows closed. Try to give the impression that you’re in your room even when you’re away, such as placing the Do Not Disturb sign on the outside of your door and keeping the blinds or windows closed. Don’t let any strangers into your room, even if they say they work for the hotel. You can always call the front desk to check whether someone was ordered by hotel staff to come to your room.
6. Be aware of your surroundings. Always keep an eye on your personal belongings and use good judgment when talking to strangers. A big part of the joy of traveling is the opportunities it affords to meet new people and learn about their cultures. But if someone near you is acting suspiciously, or if you feel uncomfortable, leave the area immediately. Trust your instincts.
7. Adhere to any recommended safety recommendations made by the GitLab group. For all large self-hosted events we (jointly completed by our internal security team and our contracted security agency) will do a full risk assessment before we converge. It will be up to employees to read said risk assessment and adhere to recommendations outlined.
8. If you are sick please do not come or participate in person workplace activities. This is for your safety and for others. We recommend that GitLab team members not travel while sick.

### Measures GitLab Takes to Aid Employee Health and Safety

* Hand sanitizers placed around the venue of live events or attendees are given hand sanitizer.
* Team members can expense masks for traveling if suggested in the risk assessment outlined above.
* Sick team members should not travel per our travel policy.
* Team members who become sick while traveling should expense masks if flying back home.
* If health risk is considered high, all food to be served by food health professionals rather than team.
* Fist bumps over handshakes.

### Responding to Unsafe Situations

The following are GitLab’s procedures in the event a team member feels threatened or unsafe:

1. If at any point, a team member feels that they are in danger of physical harm, please contact the local authorities immediately. Local law enforcement can act quickly to protect the individual and neutralize any threats.
2. If at any point, a team member feels like they or another team member may require immediate medical assistance, please contact the local authorities.
3. Once the immediate threat is controlled, team members should report any safety concerns to People Connect.
4. If you believe that a certain location, event or area presents greater risk or exposure to individuals, please notify People Connect. People Connect will strive to proactively communicate the concerns to other potentially affected team members.
5. If at any point you believe you, personally, may commit an unsafe act, People Connect can assist in providing information about available [Employee Assistance](https://about.gitlab.com/handbook/total-rewards/benefits/general-and-entity-benefits/#employee-assistance-program) options.

## Workers’ Compensation

If you have been injured at work, at a co-working site, or traveling to a customer location please contact the Absence Management team (leaves@gitlab.com). The Absence Management team will provide you with paperwork to file your claim and explain your benefits.

**CA Team Members Only**: Complete this [form](https://www.dir.ca.gov/dwc/DWCForm1.pdf) and email to the Absence Management Team at leaves@gitlab.com.

The following states are considered “monopolistic” workers compensation states, meaning employers must purchase workers compensation coverage directly from the state. If a team member in these states is injured, they may file the claim themselves or the Absence Management Team will file on their behalf. **Team members in these States are still required to contact the Absence Management Team, even if they file their own claim through the State**:

* [Ohio](https://info.bwc.ohio.gov/)
* [Washington](https://www.lni.wa.gov/)
* [North Dakota](https://www.workforcesafety.com/)

## Substance Abuse

GitLab strives to maintain a workplace that is free from illegal use, possession, sale, or distribution of alcohol or controlled substances. Legal or illegal substances shall not be used in a manner that impairs a person’s performance of assigned tasks. This will help to maintain the efficient and effective operation of the business, and to ensure customers receive the proper service. GitLab team members must also adhere to the local laws of where they reside and where they travel to for company-sponsored events.

## Mental Health Awareness Statement

1. Why is awareness of Mental Health important at GitLab?

* It can affect any and all of us. Statistics indicate that [1 in 4](http://www.who.int/whr/2001/media_centre/press_release/en/) of us will be affected by mental or neurological disorders at some point in our life. That said, we are all subject to periods where we or those around us find the “the normal stresses of life” harder than usual to deal with.
* The more we are aware of mental health, the more inclusive we are. That will help encourage any colleagues currently experiencing mental health issues to talk about it.
* Our business at its core is a group of people working together towards a common goal. With awareness of what might affect our colleagues, we are better equipped to help them if they do discuss it with us and therefore help our business.
* Mental health has so much emotional baggage as a topic that it can initially seem scary to talk about. Promoting mental health awareness helps to remove the stigma and taboos associated with it.
* GitLab can offer “productive and fruitful” work for all of our employees. That should not be [underestimated](https://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwitr7eP18_XAhWIORoKHY2_CA4QFggrMAA&url=https%3A%2F%2Fcardinal-management.co.uk%2Fwp-content%2Fuploads%2F2016%2F04%2FBurton-Waddell-is-work-good-for-you.pdf&usg=AOvVaw0ROXJdWquGML5bIsBEIRLo).
* In the cold-light of business metrics, the healthier we are, [the more productive we are](https://www.rand.org/randeurope/research/projects/workplace-health-wellbeing-productivity.html).

1. At GitLab we strive to create a stigma-free workplace. In accordance with the National Mental Health Association and the National Council for Behavioral Health we would like to:

* Educate employees about the signs and symptoms of mental health disorders.
* Encourage employees to talk about stress, workload, family commitments, and other issues.
* Communicate that mental illnesses are real, common, and treatable.
* Discourage stigmatizing language, including hurtful labels such as “crazy,” “loony” or “nuts.”
* Help employees transition back to work after they take leave.
* Encourage consultation with our employee assistance programs.

1. What are we doing to get there?

* Talk about mental health issues and ideas in the #mental\_health\_aware Slack channel.
* GitLab would also like to encourage GitLab team members to take [time off](https://about.gitlab.com/handbook/paid-time-off) to properly take care of themselves. We encourage the team to go to yoga, take a long lunch, or anything else in their day to day life that assists in their mental and emotional well-being.
* In addition to our current EAP programs available for employees, we encourage GitLab team members to take a look at [Working Through It](https://www.workplacestrategiesformentalhealth.com/employee-resources/working-through-it) for insight into reclaiming well-being at work, off work, and return to work.
* We believe that our values and culture lends itself to being able to discuss mental health open and honestly without being stigmatized, but let’s work together to make it even more inclusive. For example, Finding the right words:
  + “How can we help you do your job?”
  + “You’re not your usual self.”
  + “Do you want to talk about it?”
  + “It’s always OK to ask for help.”
  + “It’s hard for me to understand exactly what you’re going through, but I can see that it’s distressing for you.”
* For additional information, please see the Mental Wellness Services offered through [Modern Health](https://about.gitlab.com/handbook/total-rewards/benefits/modern-health/) and tips on [Leading Through Adversity](https://about.gitlab.com/handbook/leadership/managing-conflict/leading-through-adversity/). Additionally, team members should learn to [recognize burnout](https://about.gitlab.com/handbook/paid-time-off/#recognizing-burnout) and to [prevent it](https://about.gitlab.com/blog/2022/05/03/preventing-burnout-a-managers-toolkit/).

Any questions or concerns? Please feel free to contact the People Connect team in the #people-connect Slack channel or email people-connect@gitlab.com.

## OTHER PEOPLE POLICIES

* [Contracts, Probation Periods, and PIAA](https://about.gitlab.com/handbook/people-group/contracts-probation-periods/#piaa-proprietary-information-and-assignment-agreement)
* [Outside Employment and Activities](https://about.gitlab.com/handbook/people-group/contracts-probation-periods/#outside-employment-paid-or-unpaid-projects-and-potentially-conflicting-activities)
* [Paid Time Off](https://about.gitlab.com/handbook/paid-time-off/)
* [General Benefits](https://about.gitlab.com/handbook/total-rewards/benefits/general-and-entity-benefits/)
* [Leave of Absence](https://about.gitlab.com/handbook/people-policies/leave-of-absence/)
* [Return of Property](https://about.gitlab.com/handbook/people-group/offboarding/#returning-property-to-gitlab)

## GITLAB LEGAL POLICIES

There are a number of GitLab Legal Policies which are important for GitLab team members to read and understand, and they are listed [here](https://about.gitlab.com/handbook/legal/#gitlab-policies).

**Working Time Regulations**

*What are the Working Time Regulations?*

The Working Time Regulations (1998) were introduced to support the health and safety of workers by setting maximum requirements for the number of hours that they can work, paid time off and rest periods.

*The 48-hour working week*

The regulations state it is illegal for you to work any time over a total of 48 hours each week. You can agree to exceed this limit if you want to, but you cannot be mandated to work more than 48 hours per week. Average working hours are calculated over a ‘reference’ period, which is usually 17 weeks. This means you can work more than 48 hours one week, as long as the average over 17 weeks is less than 48 hours a week. For more information about the 48-hour working week restrictions, please visit the [government’s website](https://www.gov.uk/maximum-weekly-working-hours).

*How to opt-out of the 48-hour working week*

It is entirely your decision if you would like to work more than an average of 48 hours a week. GitLab is committed to enabling team members to maintain a healthy work-life balance, but on occasion (for example during periods of high customer demand) you may be asked to work longer hours. To ensure that we remain compliant with the regulations, we ask you to opt out of them, in case such a need arises. If you would like to opt-out, you can do this by signing this written agreement, known as the opt-out agreement. You may have chosen to sign/confirm this agreement already during your onboarding. The duration of the agreement is indefinite. If you haven’t already signed [this agreement](https://docs.google.com/document/d/1DRu62fqQW7OQV0lS6evf_XxdQ-0IVZl1Jk_LmSgEhDo/edit#heading=h.tkxekwf0szl9) but would like to do so, you can make a copy of this document, add your name and sign it, and email a copy to people-connect@gitlab.com, with a request that it be saved with your documents in Workday.

*How do I cancel my opt-out agreement?*

You can choose to cancel your opt-out agreement at any time. The notice period you are required to give is three months.