hackerone

CODE OF CONDUCT

Version 3.0

Effective Dec. 2023

A Message from the CEO

Everyone when joining HackerOne signs up for and commits to our values to lead with integrity, default to disclosure, respect all people, execute with excellence, and win as a team. These values are powerful because they apply to all hackeronies in all their doings at all times. The HackerOne values guide us in moments both small and large when we choose our path forward.

Although the environment in which we operate is dynamic and fast-moving, we stand firm on our commitment to acting with the highest ethical standards, cultivating a workplace of collaboration, respect, and accountability, and conducting business fairly and truthfully.

We all have a responsibility to the HackerOne community, customers, partners and each other to be a company that leads with integrity. Our mission to empower the world to build a safer internet is a weighty responsibility and a worthy endeavor. What we do is important, and how we do it is equally important. The future of our business relies on building and maintaining the trust of those we interact with.

This Code of Conduct is your guide to ethically navigating business issues you may encounter at HackerOne. Start by familiarizing yourself with the entire text, and come back to it whenever you are unsure about something. If the Code of Conduct does not provide guidance in a situation you are encountering, talk to someone on the Legal, Compliance or People teams, or use our anonymous ethics reporting form. We will continue to learn, adapt, and update this Code of Conduct as part of our commitment to our mission and values.

Thank you for being a part of our team and for joining us on the journey to create a safer Internet.

Sincerely,
Marten Mickos

Code Of Conduct

HackerOne strives to do business ethically and responsibly. This Code of Conduct is foundational to our mission to empower the world to build a safer internet and reflects the Company's foundational Values.

HackerOne's Code of Conduct is intended to create and promote a culture of transparency, honesty, and accountability; honest and ethical conduct; integrity and accuracy of Company records and reporting; compliance with all applicable laws, rules, and regulations; and good-faith reporting of internal violations of this Code, HackerOne Policy, or applicable law without fear of retaliation. This Code of Conduct applies to all HackerOne employees, members of our contingent workforce program, consultants and independent contractors, officers, and directors of HackerOne Inc. and its subsidiaries.

HackerOne is committed to continuously reviewing and updating our policies and procedures, and may amend, alter, or terminate this Code of Conduct at any time, subject to applicable law. Although it is impossible to predict or specify every situation that may arise, this Code of Conduct sets minimum standards. In addition, HackerOne team members that occupy special positions of trust, leadership, or responsibility (*e.g.*, executive team members, Board of Directors, etc.) may be subject to additional or more stringent policies than those articulated in this Code of Conduct. To the extent you are faced with an issue and/or find yourself in a situation that this Code does not address, or if you feel that compliance with this Code of Conduct or HackerOne policy will conflict with compliance with the law, you should not hesitate to consult your manager, a member of the Talent Strategy team, or a member of the Legal team.

General behavioral guidelines are:

- You should not be in a situation where loyalty to HackerOne could be compromised due to a personal or financial interest, including an interest in a competitor, supplier, or customer ("customers" include clients, hackers, and any other users of HackerOne's platform or services).
- Tools, equipment, facilities, inventions, knowledge, patents, technology, market information, and business plans are valuable assets. It is your responsibility to see that they are not misused or made available to third parties to protect company interests and prevent them from being adversely impacted.

- You are responsible for the accurate and complete reporting of financial information within your respective areas of responsibility and for the timely notification to senior management of financial and non-financial information that may be material to the Company.
- No false or misleading entries, including misclassification of transactions as to accounts, business units, or accounting periods, will be made in HackerOne's records for any reason.
- HackerOne will refrain from requesting current or future employees to divulge valuable confidential and proprietary information obtained from other companies where the employee has worked.
- You are not permitted to make particulars or details known publicly that you knew or reasonably could have known would cause damage to HackerOne or the group of companies to which HackerOne is associated, and/or customers or partners of HackerOne, unless specified otherwise by law.
- Unless otherwise permitted by law, you are prohibited from making defamatory, false, or disparaging remarks externally about HackerOne or the group of companies to which HackerOne is associated and/or customers or partners of HackerOne to third parties, either verbally or in writing. This includes publishing remarks on the internet, such as in blogs and social media like LinkedIn, Facebook, and Twitter.
- HackerOne forbids you from offering and/or taking bribes or reimbursements that unjustly place HackerOne or yourself in a privileged position. If you are in a situation where payments could be deemed bribes, you should immediately contact your supervisor and a member of the Verification & Risk Monitoring ("VRM") and/or Legal teams. Gifts valued less than €50 or $50 are acceptable because they cannot be deemed bribes or reimbursements.
- You are expected to refrain from discriminatory, harassing, and/or intimidating behavior toward customers, partners, supervisors, employees, service providers, and guests of HackerOne.
- You are bound to comply with strict regulations regarding the use of drugs and smoking at work or Company-sponsored events, regardless of local law.
- Bribery, theft, and fraud are prohibited.

1. Non-Disclosure

You must treat the information made available by HackerOne or its customers/partners as confidential. Sensitive information gathered in service of HackerOne should not be disclosed to third parties or used without permission. It is also forbidden to use non-public supplied information for any purpose other than the work of HackerOne, and, more specifically, it is forbidden to disclose it in any way whatsoever to third parties.

Notwithstanding the foregoing, nothing in this Code of Conduct, HackerOne policy, or any employment agreement is intended to prohibit, restrict, or discourage you from disclosing confidential information to any government or regulatory agency to the extent provided for by law.

2. Confidentiality

It is critical to HackerOne to maintain the absolute confidence of our customers, partners, and the public. Confidential and private information must be held inviolate by those to whom it is entrusted. You must maintain the confidentiality of information about the Company and other parties entrusted to you by the Company, use the information for permissible business purposes and in accordance with any restrictions imposed by the disclosing party, and limit dissemination of confidential information, both inside and outside the Company, to people who need to know the information for business purposes and who are bound by similar obligations of confidentiality, unless disclosure is authorized or legally mandated. HackerOne is committed to doing everything in its power to maintain the confidentiality and security of all proprietary information and non-public information that is developed internally, entrusted to the Company, or in its possession, and to avoid even the appearance of any impropriety. You are prohibited from disclosing to any third-party, including hackers on the platform, any information regarding internal investigations, audits, or reviews unless explicitly authorized in writing by the Company's VRM team. The obligation to protect confidential information does not end when your relationship with HackerOne is terminated.

Social media (including personal and professional websites, blogs, chat rooms, and bulletin boards; social networks, such as Facebook, LinkedIn, and Twitter; and video-sharing sites such as YouTube) are a common means of communication and self-expression. Do not disclose the Company's non-public, confidential, or proprietary information or personal identifying information of anyone at the Company in online postings, social media, or

publications. Sharing these types of information, even unintentionally, could harm the Company and result in legal action against you or the Company. If you choose to disclose your affiliation with the Company in an online communication, you must clarify that the views you express are your own, not a representation on behalf of the Company, and treat all communications associated with the disclosure as professional communications governed by this Code of Conduct. All statements the Company makes to the public should be complete, accurate, and truthful, and not false or misleading. Do not identify a customer or co-worker in an online posting without their prior written permission. Obey the law and ethics rules. Do not post any information or engage in any online activity that violates applicable local, state, or federal laws or professional codes of conduct. Avoid hostile or harassing communications in any posts or other online communications involving the Company. Harassment can be considered any unwelcome, offensive conduct based on a person's race, sex, gender, gender identity, national origin, color, disability, age, sexual orientation, veteran status, marital status, religion, or any other status protected by law.

All employees must sign a confidentiality agreement upon being hired, and any breach of confidentiality may result in immediate termination and/or referral of the matter to law enforcement authorities, if appropriate.

Notwithstanding, nothing in this Code of Conduct is intended to restrict or otherwise interfere with your: (i) obligation to testify truthfully in any forum; (ii) right and/or obligation to contact, cooperate with, provide information to – or testify or otherwise participate in any action, investigation or proceeding of – any government agency or commission; (iii) obligation to disclose any information or produce any documents as is required by law or legal process; or (iv) rights under Section 7 of the National Labor Relations Act.

3. Use Of Business Assets

To the extent your work requires you to have HackerOne business assets in your possession, custody, or control, you must take care of property made available to you and ensure their efficient use. You must prevent HackerOne business property from being damaged and ensure property made available to you is properly safeguarded and kept in a safe place. If the business property becomes or appears to be damaged, then this will be considered a loss of HackerOne property and should be reported directly to [email removed]. Use of HackerOne business assets is governed by the Company's Acceptable Use Policy, Access Control Policy, Asset Management Policy, Information Security Policy, Mobile Device Policy, and any other applicable Company policy that may be enacted from

time to time. Any suspected incidents of fraud, theft, loss, or misuse of Company assets should be reported immediately to your manager and [email removed].

4. Use Of Information Systems And Resources

HackerOne information resources, including the internet and email, should only be used for business purposes. These resources may be used for personal purposes on a limited basis. You must exercise good judgment in using these resources. Specifically, you must not use these resources to access websites such as porn sites, gambling sites, or sites with inflammatory, offensive, or obscene content. Illegal downloads or installing bootleg, cracked, or otherwise unofficial software is prohibited.

5. Information Security And Monitoring

You should be aware that HackerOne has software and systems in place that are capable of monitoring and recording all activity that occurs on HackereOne networks, devices, systems, and third-party systems. HackerOne reserves the right to access, review, copy, and/or delete any information, data, or messages accessed through HackerOne systems with or without notice to you and/or in your absence if there is good reason to monitor. This includes but is not limited to all email messages sent or received, all website visits, all chat sessions, all newsgroup activity (including groups visited, messages read, and employee postings), and all file transfers into and out of HackerOne's internet networks. HackerOne further reserves the right to retrieve previously deleted content from any Company system or application. In addition, HackerOne may review internet and technology systems activity and analyze usage patterns to ensure that technology systems are devoted to legitimate business purposes. It may choose to publicize this data. Accordingly, no team member should have any expectation of privacy regarding their internet or technology systems usage and should not use these systems for information they wish to keep private.

There are also a number of policies in place to keep our information safe regarding information technology and security, including policies and/or restrictions regarding device access and management when traveling (See International Travel Policy). You are responsible for familiarizing yourself with these policies. We encourage you to check out the Policies & Procedures page. Team members are obligated to comply with these policies to secure HackerOne's information.

6. Political Activities and Lobbying

HackerOne's business model and the cybersecurity and vulnerability testing industry are rapidly evolving and are raising important issues of consideration at local, state, federal, and international levels of government. Political contributions and lobbying activities are highly regulated and, in some cases, subject to disclosure and reporting requirements. Certain political contributions and lobbying activities may be limited or prohibited in certain areas or from certain sources.

To the extent that you choose to be involved in personal political activities, they must be clear that such activities and your participation is voluntary and at your own election, and not an endorsement from the Company. Any political contributions on behalf of HackerOne must be approved in writing by the Chief Legal Officer. Political contributions are not limited to cash donations. Paying for a public official or candidate to attend an event or using HackerOne resources (e.g., computers, supplies, employee time, etc.) to support a campaign could also be considered improper political contributions. To the extent you have any questions in this regard, please contact a member of the Legal team.

7. Theft, Fraud, and Bribery

HackerOne does not permit theft, fraud, and bribery in any form or fashion. You must transact business on behalf of HackerOne in foreign markets and with foreign government officials only in accordance with the Company's Anti-Bribery and Corruption Policy and any applicable law, including the United States Foreign Corrupt Practices Act and the United Kingdom Bribery Act 2010. You are strictly prohibited from engaging in any bribery, kickbacks, or other types of corruption when dealing with government officials, customers, suppliers, or other third parties regardless of local practices or competitive urgency. Specifically, you must never directly or indirectly via a third party make, offer, or authorize a payment (including cash or any other items of value such as meals, gifts, travel, entertainment, etc.) to an official of any government or private sector company to corruptly influence that person, obtain or retain business for the Company, or to acquire any improper advantage.

Any questions regarding the legal rules involving these activities should be directed to the Legal or VRM team prior to taking any action. If there has been an instance and/or suspicion of unfair dealing practices, theft, fraud, or bribery, this must be reported directly to HackerOne Legal.

8. Conflicts of Interest

A conflict of interest is any activity or interest that is inconsistent with or opposed to the best interests of the Company. You must never use or attempt to use your position with the Company to obtain improper personal benefits.

The following are some examples of conflicts of interest that should be avoided:

- Family Members: You may not conduct business on behalf of the Company with family members or an organization with which a family member is associated unless such business relationship has been disclosed to and authorized by the Company, and is a bona fide arms-length transaction. "Family Members" include a spouse, domestic partner, parents, grandparents, children, siblings, and in-laws. HackerOne also strongly discourages romantic, sexual, or familial relationships between a manager or other supervisory employee and their staff (an employee who reports directly or indirectly to that person) because such relationships tend to create compromising conflicts of interest or the appearance of such conflicts. For more information in this regard, please see the Employee Handbook ("Relationships at HackerOne").

- Interests in Other Businesses: Holding a significant or controlling interest (whether personal or financial) in one of HackerOne's competitors, customers, or suppliers could create a divided loyalty, or the appearance of divided loyalty. You may not accept compensation in any form for services performed for HackerOne from any source other than HackerOne. You should not have an undisclosed financial interest in a competitor, supplier, customer, or business partner of the Company. Outside business activities (e.g., advisory roles) are only permissible if they do not give rise to any conflict with HackerOne's business or negatively impact your ability to do your job at the Company. If you have been asked to sit on the Board of Directors or Advisory Board of any company, including any non-profit company, you must obtain approval from the Legal team. If there is any question or potential for conflicts of interest, you must reach out to Legal for clarification prior to proceeding with the opportunity.

- Corporate Opportunities: You are not permitted to take advantage of a business opportunity discovered through use of Company property, information, or position,

or take/direct such opportunity to a third party unless the Company has already been offered it and turned it down.

- Improper Conduct and Activities: You must not engage in any conduct or activities that are inconsistent with the Company's best interests or that materially disrupt or impair the Company's relationship with any person or entity with which the Company has or proposes to enter into a business or contractual relationship.

- Gifts and Gratuities. This Code of Conduct does not prohibit normal, appropriate, and modest hospitality to or from third parties. However, it is important to keep in mind that gifts are subject to limits and disclosure requirements. Gifts on behalf of HackerOne or in your capacity as a HackerOne representative should only be made in compliance with the HackerOne Anti-Bribery and Corruption Policy. You must contact the Legal and VRM teams for approval prior to giving any gifts to government or public officials, which includes officials of public international organizations to make sure they do not violate the law or Company policies.

An integral part of HackerOne's culture is to default to disclosure. When you are open about potential conflicts, it is easier to find a way to minimize potential issues. Any situation, transaction, or relationship that may give rise to an actual or potential conflict of interest must be disclosed to the Company immediately. You must refrain from engaging in a disclosed conflict of interest while the request is being evaluated.

9. Financial Integrity, Records, and Accounting

You are responsible for the accurate and complete recording of financial information within your respective areas of responsibility and for the timely notification to senior management of financial and non-financial information that may be material to the Company. Company records, accounts, and financial statements, including tracking work hours, expenses, sales contracts, etc., must be maintained accurately and in appropriate detail to properly reflect HackerOne's business activities.

When deciding what documents to save, archive, or delete, always check the HackerOne Data Retention Policy for details about how long various documents should be retained. This policy applies to both paper and electronic documents and information.

10. Fair Dealing

As part of HackerOne's commitment to Leading with Integrity and Executing with Excellence, the Company is committed to success through honest business competition and fair dealing. The Company does not seek competitive advantages through illegal or unethical business practices. You are expected to deal fairly with each other and with the Company's customers, service providers, suppliers, business partners, and competitors. You are not permitted to take unfair advantage of anyone through manipulation, concealment, deception, abuse of privileged information, misrepresentation of material facts, or any other unfair dealing practice. If you receive another company's confidential or proprietary information by mistake, you must return or destroy it. For any questions in this regard, contact a member of the Legal team.

11. Competing Fairly

Competition laws throughout the world are designed to foster a competitive marketplace, ensure a level playing field for all business, and prohibit activities that restrain trade. In general, actions taken in combination or agreement with other companies that restrain competition may violate antitrust laws. Some examples of unlawful agreements include:

- Price fixing agreements where competitors or partners agree to charge a certain price for certain products or services;
- Agreements adhering to specific practices around recruiting, compensation, payments, or benefits to employees or independent contractors;
- Agreements to divide or allocate markets where competitors agree to limit their sales presence so each company can be the only available choice for buyers in a given market;
- Group boycotts where competitors agree to avoid a particular customer or supplier;
- Bid rigging where competitors agree to bid for contracts in a way that allows a certain bidder to win.

These agreements do not have to be signed contracts to be illegal. Even an informal understanding between HackerOne team members and a competitor, or even a conversation that implies an understanding, creates risk of antitrust violations. If any topics around price, employment practices, costs, supply, bids, group boycotts, and/or operational decisions arise during the course of communications with a competitor, you must stop the conversation immediately and contact the Legal department.

12. Worker Health and Safety

To the extent HackerOne maintains a physical workplace, the Company is committed to providing a healthy, safe, and secure environment to employees, contractors, and visitors. Compliance with all applicable laws, rules and regulations governing physical and mental health, safety, and the environment are a responsibility of management and employees in all functions.

13. Fair Employment Practices

As part of the Company's commitment to Respecting All People, HackerOne strives to maintain a workplace that promotes respect, professionalism, and inclusivity where discriminatory practices, including harassment, are prohibited. HackerOne expressly prohibits discrimination and harassment on the basis of any protected category, including race (including traits historically associated with race, including hair texture, hair type and protective hairstyles), color, religion, religious creed (including religious dress and grooming practices), sex, sexual orientation, gender (including gender identity and gender expression), national origin, age, disability, genetic information, marital status, military status, veteran status, or any other status protected by applicable law.

Employees found in violation of this section may be subject to discipline up to and including termination. For more information on HackerOne's commitment to fair employment practices, see the Employee Handbook.

14. Whistleblower

A whistleblower is someone who reports an activity in good faith that they consider illegal, unsafe, unethical, fraudulent, or otherwise in violation of law or Company policy to one or more of the parties specified in this Policy or otherwise. The whistleblower is not responsible for investigating the activity or determining fault or corrective measures; appropriate management officials are charged with these responsibilities.

Examples of illegal activities include, without limitation, violations of federal, state or local laws; fraudulent billing for products/services not performed or for goods not delivered; and other fraudulent financial reporting or activities.

If you have knowledge of or a concern regarding the Company's accounting, internal controls, or audit matters, or concerns regarding illegal, unethical, or fraudulent conduct or activity that violates this Company's Code of Conduct or other Company policies, you must report your concerns to your immediate supervisor and the Chief People Officer or the Chief Legal Officer. You may also submit an anonymous concern via [anonymous ethics reporting tool]. HackerOne expects any individual making such a report to do so in good faith. An employee who intentionally files a false report of wrongdoing or otherwise knowingly misuses the reporting process will be subject to discipline up to and including termination.

Whistleblower protections are provided in two important areas -- confidentiality, to the extent practicable, and freedom from retaliation.

Insofar as practicable, the confidentiality of the whistleblower will be maintained. However, no absolute guarantee of confidentiality can be provided, as, for example, the identity of the reporter may need to be disclosed to conduct a thorough investigation, to comply with legal obligations, and/or to provide accused individuals their legal rights of defense.

HackerOne will not retaliate against a whistleblower. This includes but is not limited to, protection from retaliation in the form of an adverse employment action such as termination, compensation decreases, poor work assignments, and threats of physical harm. Any whistleblower who believes they are being retaliated against must contact the Chief People Officer or the Chief Legal Officer immediately. The right of a whistleblower for protection against retaliation does not include immunity for any separate wrongdoing that is alleged, investigated, or uncovered.

15. Investigations

Reported violations of policy or law will be promptly and thoroughly investigated by the People Team, Legal Team, and/or a designated third-party investigator, as appropriate. You are expected to cooperate fully with any appropriately authorized investigation, whether internal or external. You must not withhold, tamper with, or fail to communicate relevant information in connection with an appropriately authorized investigation. Knowingly providing false or misleading statements to an authorized investigator or to any external auditor or agency may be grounds for immediate termination of employment and may constitute a criminal act subject to criminal penalties.

You are expected to maintain and safeguard the confidentiality of an investigation to the extent possible, unless otherwise required by law. Team members that participate in any such investigation are protected by HackerOne's Whistleblower policy against retaliation.

16. Violations

Violation of this Code of Conduct, HackerOne policy, or applicable law by team members may result in disciplinary action up to and including termination. Any manager who directs, approves, or ratifies conduct in violation of this Code of Conduct, HackerOne policy, or applicable law may similarly be subject to disciplinary action up to and including termination.

To the extent your violation of this Code of Conduct or HackerOne policy constitutes violation of the law, HackerOne may be required to refer your conduct to appropriate law enforcement officials.

Any questions regarding this policy may be directed to People Operations, Legal, or Compliance teams.