



# HACKTHEBOX

# ACCEPTABLE USE POLICY

You should download a [copy](#) for future reference.

## Table of Contents

<b>Frequently Asked Questions</b>	<b>2</b>
<b>Our 10 Rules</b>	<b>3</b>
Section 1 - Compliance	4
<b>Part A - Platform Rules</b>	<b>4</b>
Section 2 - Your account	4
Section 3 - Stay in bounds	5
Section 4 - Don't disrupt or circumvent	5
Section 5 - No malicious code	6
Section 6 - AI and Programmatic Access	6
Section 7 - Use the Services for their intended purpose	7
Section 8 - Protect content and data	7
<b>Part B - Community Conduct</b>	<b>8</b>
Section 9 - Content and conduct standards	8
Section 10 - Be honest about who you are	10
Section 11 - Integrity and Fair Play	11
Section 12 - Community space rules	12
Section 13 - Use your skills responsibly	12
<b>PART C - Reporting, Enforcement and Appeals</b>	<b>13</b>
Section 14 - Reporting	13
Section 15 - How we detect violations	13
Section 16 - Enforcement	14
Section 17 - Appeals	15
Section 18 - Changes to this policy	16

## Frequently Asked Questions

**What is this policy?** This Acceptable Use Policy ("AUP") sets out the rules for using the Hack The Box platform, services, content, and infrastructure. It tells you what you can and cannot do - both with our technology and systems, and in your interactions with other people in the Hack The Box community. It also explains what happens if you break these rules.

**Why does this policy exist?** Hack The Box provides cybersecurity training and lab environments designed to build real-world skills in a controlled, legal, and ethical setting. This policy protects the integrity of the platform for all users, establishes clear ethical and legal boundaries, safeguards the community, ensures compliance with applicable laws, and supports our enterprise customers and partners.

**Who must follow this policy?** Everyone. This policy applies to every individual and entity that accesses or uses any Hack The Box service, regardless of account type, subscription, or how access is obtained. This includes registered users, visitors, business customers, event participants, employers using our services, contractors, partners, and any third parties interacting with the Services.

**What happens if I break a rule?** We explain enforcement in detail in Part C. In short: any failure to comply is a material breach of your Service Agreement. Depending on the severity, we may issue a warning, restrict your reputation, remove content, suspend or permanently ban your access, or take credential action. We may also refer matters to law enforcement or pursue legal proceedings where appropriate. We aim to be fair and proportionate.

**Can I appeal?** Yes. If we take enforcement action against your account, content, or credentials, you can appeal. Your enforcement notice will tell you how. Appeals are reviewed by a person not involved in the original decision, and we provide a written outcome within 10 business days. For permanent bans or suspensions of two years or more, a second-level review by an independent panel is available.

**How often is this policy updated?** We review and update this policy periodically. When changes occur, we will notify you by email or by posting the revised version on our website. Material changes take effect 30 days after posting. Where a change is urgently required by law, a court order, or a regulatory requirement, it may take immediate effect - and we will explain why.

**How do I report a violation?** You can report content or behaviour that violates this policy through in-platform reporting tools (where available) or by email to [customerops@hackthebox.com](mailto:customerops@hackthebox.com). You don't need an account to report. For security vulnerabilities in Hack The Box infrastructure, use our vulnerability disclosure programme at [https://hackerone.com/hack\\_the\\_box](https://hackerone.com/hack_the_box).

## Our 10 Rules

Everything in this document flows from ten rules. If you remember nothing else, remember these.

- 1. Respect every person.** This community works because people treat each other with dignity. No harassment, hate speech, threats, discrimination, or abuse - regardless of who someone is, where they are from, or how they identify.
- 2. Use the platform to learn.** We are here to build skills - yours and each other's. Use the Services for cybersecurity training, education, and upskilling. Contribute to the community. Share knowledge generously. Help someone who is stuck. Do not use the platform to build competing products, for unauthorised commercial purposes, or to train, test or build AI systems.
- 3. Earn it yourself.** Your skills are your reputation. Do your own work, pass your own exams, solve your own challenges. Never cheat, plagiarise, or claim credit you did not earn. Rankings and competitions only matter if they are real. Do not manipulate scores, collude, sabotage others, or game the system.
- 4. Share knowledge, not harm.** Sharing is how this community grows - but think before you post. Do not share illegal content, malware, spam, deepfakes, or anything harmful to others, especially minors. Respect content lifecycles and intellectual property.
- 5. Protect others' data.** As cybersecurity professionals, we hold ourselves to a higher standard on privacy. Other people's personal information is not yours to collect, use, or monetise. Respect data protection law - it is not just a rule, it is the craft.
- 6. Follow the law.** Everything you do on Hack The Box must be legal. No exceptions. If an action would be unlawful outside the Services, it is unlawful on them.
- 7. Stay in bounds.** Hack only what we authorise you to hack. Stay within assigned labs, machines, and IP ranges. Never use the Services as a launchpad to attack anything else.
- 8. Don't break the house.** Protect the infrastructure that serves everyone. Do not disrupt, degrade, exploit, reverse engineer, or circumvent the security and availability of Hack The Box systems. Do not use bots, scrapers, or automated tools to access or extract from the platform.
- 9. Use your skills responsibly.** The techniques you learn here carry real-world consequences. Do not use them to attack systems, offer unauthorised hacking services, or claim your activities are endorsed by Hack The Box. If you find a vulnerability in the real world, disclose it responsibly.
- 10. Own your account.** Your account is yours alone. Keep it secure, keep it honest, keep it one. Do not share credentials, sell access, impersonate others, misrepresent your identity or qualifications, or evade enforcement.

### About This Policy

This Acceptable Use Policy (AUP) governs your use of all Hack The Box platforms, infrastructure, content, and community spaces to ensure our cybersecurity training environments remain safe, legal, and fair for everyone. Working alongside your overarching Service Agreement, this policy outlines the standards for your behavior, content, and everyday platform use. If a violation occurs, we review the context and severity to ensure any enforcement action is fair, proportionate, and respects your fundamental rights. Please note that if your access is provided by an employer, university, or other organization, they are responsible for ensuring you follow these rules. Finally, if you require this policy, reporting mechanisms, or appeal processes in an alternative format for accessibility reasons, please contact us at [accessibility@hackthebox.com](mailto:accessibility@hackthebox.com).

## Section 1 - Compliance

**1.1 Comply with the law.** You must not use or access the Services in any way that breaks applicable local, national, or international laws, regulations, or governmental orders.

**1.2 No unlawful activity.** You must not use the Services to plan, promote, facilitate, or carry out any unlawful activity. Without limiting this, you must not use the Services to offer, promise, give, request, or accept a bribe or other improper advantage, launder money or process the proceeds of criminal activity, finance terrorism, evade or circumvent tax obligations, violate applicable data protection or privacy laws, breach applicable cybersecurity or computer misuse laws, or contravene any court order, regulatory direction, or lawful legal process that affects your use of the Services.

**1.3 Export controls and sanctions.** You must not use or access the Services in any way that violates applicable export control laws, trade sanctions, or embargoes. You must not make the Services available - directly or indirectly - to any person, entity, or jurisdiction subject to applicable sanctions.

**1.4 Professional obligations and compliance.** The Services are provided for cybersecurity training, education, and upskilling. The Services do not constitute legal, regulatory, or compliance advice, and do not guarantee that your use will satisfy any particular certification, regulatory, or compliance requirement. If your professional certifications, security clearance, or licences impose their own rules on how you train, test, or research, you are responsible for meeting those obligations.

## Part A - Platform Rules

These rules govern how you use the platform, its infrastructure, its systems, and its content. Part A applies to everyone who accesses the Services.

### Section 2 - Your account

**2.1 Keep your credentials secure.** Keep your account credentials confidential. Do not allow any third party to access your account, exam environment, or any part of the Services - whether by sharing credentials, granting remote access, or other means. Enable multi-factor authentication where available. You are responsible for all activity under your account. This

includes VPN configuration files, session tokens, and any other access method tied to your account. If you become aware of any unauthorised use of your account, notify Hack The Box at [security@hackthebox.com](mailto:security@hackthebox.com) without undue delay and in any event within 24 hours, identifying the affected credentials.

**2.2 One account only.** You may hold only one account. Do not create or use additional accounts for any reason - including to circumvent restrictions, gain an unfair advantage, manipulate rankings, or misrepresent your identity. If you have lost access to an existing account, contact customer support.

**2.3 No transferring accounts.** Do not sell, rent, trade, or transfer your account or account privileges without express prior written authorisation.

### **Section 3 - Stay in bounds**

**3.1 Stay within designated environments.** Confine all hacking, testing, and exploitation activity to the specific labs, challenges, machines, and IP ranges assigned to you. Do not target anything outside those boundaries, including third-party systems. Do not attempt to access, view, or interact with data, configurations, or environments belonging to any other tenant or user.

**3.2 No pivoting to external systems.** Do not use any Hack The Box environment - including labs, Pwnbox, or VPN connections - to attack, scan, or access any system outside the Services.

**3.3 Event-specific boundaries.** Events and competitions may designate specific IP ranges, entry points, or targets. Stay within those boundaries. Where an event publishes rules stricter than this policy, the event rules apply.

**3.4 Report what you find.** If you discover a vulnerability in Hack The Box infrastructure, report it through our Hack The Box Vulnerability Disclosure Program at [https://hackerone.com/hack\\_the\\_box](https://hackerone.com/hack_the_box). If you encounter data, systems, or access that should not be present in a training environment - such as personal data, production credentials, or access to real-world systems - stop immediately and report it through the same process.

### **Section 4 - Don't disrupt or circumvent**

**4.1 No disruption.** Do not overload, disrupt, degrade, or impair the Services - whether through denial-of-service attacks, excessive requests, resource exhaustion, or other means.

**4.2 No interfering with other users.** Do not interfere with other users' access to the Services, their submissions, their progress, or their competitive environment. Do not intercept, redirect, monitor, or interfere with communications or data intended for others. This includes tampering with team-specific environments, dedicated servers, or shared resources that form part of a competitive exercise.

**4.3 No circumventing controls.** Do not bypass or disable any security, access control, content moderation, enforcement, or monitoring feature of the Services - whether by technical means or through social engineering, including phishing, fake login portals, or similar deceptive techniques designed to obtain credentials, personal information, or unauthorised access. This

includes authentication mechanisms, content protection measures, rate limits, usage quotas, and storage restrictions.

**4.4 No attacking or exploiting platform systems.** Do not attack, scan, test, or exploit vulnerabilities in any Hack The Box production system or any part of the Services outside designated training environments. This includes all user-facing websites, APIs, payment systems, scoring systems, and administrative infrastructure.

**4.5 No manipulating Hack The Box systems.** Do not attempt to manipulate, exploit, or probe any Hack The Box feature, AI system, API, or internal service - whether through reverse engineering, decompilation, disassembly, automated tools, or any other means - with the intent or effect of:

- (a) causing those systems to act outside their intended purpose or operational scope;
- (b) revealing proprietary system prompts, model architecture, configuration, training data, or internal logic;
- (c) extracting, exfiltrating, or reconstructing data beyond what the system is designed to provide to the user in normal operation; or
- (d) enabling any activity prohibited under this policy.

**4.6 No reverse engineering.** Without limiting Section 4.5, do not attempt to derive the source code, architecture, algorithms, data models, or proprietary datasets of the Services by any means - including reverse engineering, decompilation, or disassembly. This prohibition applies regardless of intent.

**4.7 No falsifying technical identifiers.** Do not falsify, conceal, or alter technical identifying information - including source IP addresses, routing information, and header data.

## **Section 5 - No malicious code**

**5.1 No uploading malware.** Do not upload or distribute malicious code through the Services. This includes malware, viruses, ransomware, trojans, worms, and spyware.

**5.2 No distributing attack tools.** Do not share, sell, or distribute any exploit, attack tool, or method whose intended use is to harm systems outside designated training environments.

## **Section 6 - AI and Programmatic Access**

**6.1 No automated access.** Do not deploy, operate, or permit any bot, crawler, scraper, AI agent, large language model, reinforcement learning agent, multi-agent system, or similar technology ("Automated Systems") to directly access, interact with, or extract data from any part of the Services, except where expressly authorised under a Service Agreement with Hack The Box.

**6.2 Prohibition on AI training and content exploitation.** You shall not use any content from the Services - including challenges, solutions, write-ups, hints, flags, methods, or any content or data output by the Services - to train, evaluate, fine-tune, test, benchmark, or develop any machine learning model, artificial intelligence system, large language model, or similar technology ("AI System"); compile any such content into a dataset for AI purposes; or

generate synthetic training data that replicates or mimics our content or Services. This prohibition applies regardless of the means of acquisition, format, or whether the use is commercial or non-commercial. It extends equally to content obtained through third parties or through authorised API access. This restriction does not apply where expressly authorised under a Service Agreement with Hack The Box.

**6.3 Programmatic Access Through APIs.** Where Hack The Box authorises access through its APIs, MCP, or integration protocols, such access is subject to the Service Agreement and this AUP. You must not circumvent any technical constraints or rate limits, nor systematically harvest, aggregate, or compile data from API responses into any dataset or knowledge base. You are responsible for the security of any integration you connect and for all access originating from your credentials, including delegation chains.

## **Section 7 - Use the Services for their intended purpose**

**7.1 Intended use only.** Do not use the Services or Hack The Box computing resources - including Pwnbox - for purposes other than cybersecurity training, education, and upskilling.

**7.2 No competitive misuse.** Do not use the Services, or any data or output from the Services, to build, improve, or contribute to a competing product or service. Do not use the Services for systematic competitive benchmarking or intelligence gathering without prior written authorisation.

**7.3 No unauthorised commercial exploitation.** Do not use the Services, or any content, materials, or outputs derived from the Services, to provide external consulting, paid training, or commercial services to third parties without explicit authorisation through a relevant agreement with Hack The Box.

## **Section 8 - Protect content and data**

**8.1 Exam content.** Exam content is permanently protected. Do not: (i) share, sell, or publish exam content - publicly or privately - at any time; (ii) participate in groups, forums, or platforms dedicated to sharing or selling exam content; or (iii) stream, record, or publicly share any portion of an exam attempt.

**8.2 Active challenge content.** Do not share, publish, sell, or disclose solutions, flags, answers, write-ups, hints, or spoilers for any active content or event.

**8.3 Retired content - what you can share.** You may publish solutions, write-ups, walkthroughs, videos, and streams for Retired Content only, and only for the purpose of community knowledge-sharing, education, and discussion, in accordance with this Acceptable Use Policy and the User Agreement. For the purposes of this section, "Retired Content" means any content that no longer counts towards season points or active rankings, as indicated on the platform. Without limitation, this includes:

(a) Retired Machines, Sherlocks, and Challenges;

(b) Starting Point Machines;

(c) Tier 0 Academy Modules; and

(d) the Mini Pro Labs for which an official write-up is published on the platform, namely: POO, Xen, Ascension, RPG, and Hades.

This permission does not authorise the use of Retired Content for any purpose prohibited elsewhere in this Acceptable Use Policy or the User Agreement. Sharing solutions for any content not falling within the definition of Retired Content is prohibited. If you are unsure whether specific content qualifies, contact [customerops@hackthebox.com](mailto:customerops@hackthebox.com) before publishing.

**8.4 Enterprise-exclusive content.** Content available exclusively to one or all business customers through dedicated enterprise environments may not be shared outside the Customer Organisation, regardless of lifecycle stage. You may discuss solutions and provide hints to other authorised users within your organisation through internal channels, and create internal documentation for purposes such as skill-gap analysis or incident-response simulations.

**8.5 Hack The Box proprietary content.** Do not distribute, reproduce, or make available training materials, challenge designs, code, documentation, or any other Hack The Box content outside the Services without authorisation. Do not remove, obscure, or alter any copyright, trademark, or proprietary rights notices. Do not frame, mirror, or replicate any part of the Services on another website or platform.

**8.6 No data harvesting or extraction.** Without limiting 6.1, do not systematically collect or compile content or data from the Services - whether by manual or automated means - beyond what is necessary for your ordinary, authorised use. Do not access, collect, or process personal data from the Services - or relating to any Hack The Box customer or user - in any manner, including through keyloggers, screen scrapers, spy-pixels, or similar tools.

## **Part B - Community Conduct**

These rules govern how you behave in the Hack The Box community - your honesty, the integrity of your work, how you treat people, how you engage in shared spaces, and the standards that apply to content you post, upload, or share.

The rules in Part B apply to your conduct on the Services and, unless stated otherwise, to conduct off the platform when that conduct affects the Services, targets another Hack The Box user in connection with their participation in the community, or poses a credible risk to community safety. Hack The Box enforces Part B directly in community spaces that it operates or controls. In Customer Organisation controlled environments, the Customer Organisation is responsible for enforcing conduct standards through its own policies and procedures. However, where a user uses a community account to access the Services, their access to community services may be restricted under Part B.

## **Section 9 - Content and conduct standards**

When you post, upload, or share content through the Services - including text, images, video, audio, job listings, reviews, and profile information - that content must comply with this AUP. Nothing here restricts good-faith criticism, honest reviews, legitimate security research, or reports to regulatory authorities.

### **9.1 Illegal and harmful content.**

**(a) Prohibited content.** Do not post content that: (i) contains or promotes child sexual abuse material; (ii) contains terrorist content or statements encouraging terrorism-related acts; (iii) promotes or assists any unlawful activity; (iv) violates a court order; or (v) breaches any legal duty owed to a third party, including contractual or confidentiality obligations. For video and audiovisual content, this includes material relating to terrorism, sexual exploitation of children, racism, or xenophobia.

**(b) Protecting vulnerable people.** Do not harm, exploit, or endanger vulnerable people, including minors. Do not encourage, promote, or provide instructions for self-harm, suicide, or eating disorders, or post content that graphically depicts any of these. Do not solicit personal information from a minor or attempt to arrange off-platform or in-person meetings with a minor.

**(c) Obscene, offensive, sexually explicit, and inappropriate content.** Do not post content that is obscene, offensive, or inflammatory. Do not post, link to, or promote sexually explicit or sexually suggestive material, adult content, or content rated for mature audiences. Do not use sexualised, violent, or inappropriate avatars, nicknames, or status messages.

**(d) Reporting obligation.** If you encounter illegal content on the Services, report it immediately through the process described in Section 14.

## 9.2 Honest content and others' rights.

**(a) No deepfakes or synthetic identity content.** Do not create, distribute, or use AI-generated or manipulated media that falsely depicts real individuals or is designed to deceive others about a real person's identity or actions. This applies to images, video, audio, and text. Clearly label AI-generated content as such where a reasonable person could mistake it for authentic.

**(b) No defamatory or misleading content.** Do not post content that is defamatory or that contains false or misleading statements. This includes fabricated security advisories, fake vulnerability disclosures, coordinated disinformation, and listings or postings that misrepresent material facts - such as the nature, terms, location, or availability of an opportunity. For content that violates another person's privacy, see Section 9.3(e).

**(c) No infringing content.** Do not upload or share content that infringes the copyright, trademark, patent, trade secret, or other intellectual property rights of any third party. If you did not create it or have express rights to use it in this way, the content may infringe third-party rights.

**(d) No spam, advertising, or artificial engagement.** Do not send unsolicited bulk messages, spam, or commercial solicitations through the Services. Do not post advertising, promotional content, or sponsored material of any kind unless expressly authorised by Hack The Box. Do not create fake accounts or generate artificial engagement - such as fake follows, likes, votes, or reviews. Do not post undisclosed sponsored content or fake reviews, including reviews that conceal that the reviewer received an incentive.

## 9.3 Respect for others.

**(a) No harassment or abuse.** Do not harass, stalk, or coordinate abusive conduct against other users. Do not sexually harass others or distribute non-consensual sexual content. Do not

coordinate or participate in brigading, harassment campaigns, or organised abuse. Do not persist in contacting a user after they have asked you to stop.

**(b) Respect personal boundaries.** Do not make unsolicited advances, appearance-based comments, or other remarks that may make participants uncomfortable.

**(c) No threats or incitement.** Do not make violent threats or credible threats of harm. Do not glorify, promote, or incite violence.

**(d) No hate speech or discrimination.** Do not post or share content that incites violence or hatred based on race, ethnicity, national origin, religion, sexual orientation, gender identity, disability, or other protected characteristics. Do not share symbols, imagery, or slogans associated with hate groups or ideologies that promote violence or discrimination. Do not discriminate against any person in your use of the Services.

**(e) Protect personal data.** Do not access, collect, process, publish, or share personal data from the Services - or relating to any Hack The Box customer or user - except as expressly authorised. This includes:

- not publishing or sharing another person's private or personal information without their consent, including home addresses, phone numbers, email addresses, identification documents, financial information, medical records, and biometric data;
- not threatening to release another person's personal information to coerce, intimidate, or extort them; and
- not accessing, collecting, or processing personal data in any manner not expressly authorised, including through keyloggers, screen scrapers, spy-pixels, or similar tools. Do not use such data for advertising, marketing, or other commercial purposes without appropriate consent.

## **Section 10 - Be honest about who you are**

**10.1 No impersonation.** Do not impersonate any person, entity, or Hack The Box staff member. Do not misrepresent your identity, qualifications, certifications, affiliation, or age. Using a platform username or handle is fine - this rule targets deceptive identity use, not pseudonymous participation. For the prohibition on falsifying technical identifiers such as IP addresses and routing data, see Section 4.7.

**10.2 Age eligibility.** The Services are targeted at adults. If you are under 18 and wish to use the Services, you may only do so if a parent or guardian reads and accepts the terms of the Service Agreement on your behalf and takes responsibility for your use, including responsible use as set out at Section 13.

**10.3 Payment fraud.** Do not commit payment fraud, refund abuse, or chargeback fraud. Do not use invalid, unauthorised, or stolen payment methods. Use only your own payment methods, or methods you are expressly authorised to use.

**10.4 False information.** Do not submit false, misleading, or fraudulent information - or forged or falsified documentation - during registration, identity verification, disputes, or support enquiries.

**10.5 Fraudulent accommodation claims.** Do not make false claims for accessibility accommodations, assessment modifications, or other benefits based on a disability, medical condition, or other protected characteristic. This targets fraudulent claims only. Legitimate requests are welcome.

**10.6 No misuse of logos or credentials.** Do not misrepresent Hack The Box through misuse of logos or designations acquired through an examination. Do not display revoked credentials or certifications. Do not falsely claim or fabricate any Hack The Box credential, certification, or affiliation - whether or not you have or had a Hack The Box account.

## **Section 11 - Integrity and Fair Play**

Your skills are your reputation. Earn it yourself. Compete fairly.

**11.1 Integrity standard.** The integrity requirements for your work depend on the assessment context. Where specific content, an examination, or an event publishes its own integrity rules, those rules govern and prevail over this section to the extent of any conflict.

**11.2 Earn it yourself.** Every assessment outcome you claim must result from your own effort and ability. You must understand the techniques applied, be able to explain why your solution works, and be capable of reproducing the reasoning independently.

**11.3 No cheating.** Cheating is obtaining, presenting, or attempting to obtain or present any assessment outcome that you did not earn through the effort and competence the assessment was designed to measure. This includes:

(a) Accessing, using, or possessing leaked or stolen assessment content, brain dumps, or content shared in breach of Section 8 - whether or not that content is subsequently submitted.

(b) Having another person, automated system, or any combination of these produce, obtain, or submit work on your behalf or under your credentials. This includes receiving real-time assistance during a proctored assessment through any communication channel, unless the specific assessment rules expressly permit such assistance.

(c) Collaborating on assessments where the rules require independent work, or sharing solutions with or receiving solutions from members of other teams in team-based events.

(d) Manipulating, falsifying, or fabricating any submission, score, timestamp, completion record, ranking position, credential record, progress data, or evidence of competence - whether or not the conduct occurs within a formal assessment.

(e) Exploiting any vulnerability or misconfiguration in assessment delivery, timing, scoring, or proctoring systems, or using automated or systematic methods to guess, brute-force, or derive answers without completing the intended challenge.

**11.4 No enabling cheating.** Do not help others cheat or build the infrastructure for cheating. This includes distributing, selling, or trading solutions, flags, or exam content; offering ghostwriting, exam-completion, or solution-generation services whether human-powered, AI-powered, or hybrid; operating or contributing to any group, channel, service, or repository dedicated to sharing assessment content or answers; developing or distributing tools

purpose-built to automate the completion of Hack The Box assessments; and recruiting or coordinating others to provide or receive unauthorised assistance.

## **Section 12 - Community space rules**

The following additional rules apply in forums, chat channels, and other community spaces owned or operated by Hack The Box. Third-party platforms (such as Discord) are also subject to their own terms of service and community standards. The content and conduct standards in Section 9 apply in full in all community spaces.

**12.1 Be constructive.** Offer thoughtful, well-reasoned counterpoints when disagreeing. Avoid rudeness, deliberate provocation, or personal attacks. If you cannot engage constructively, refrain from commenting.

**12.2 No trolling or disruption.** Do not troll, deliberately disrupt discussions, or participate in bad faith.

**12.3 Stay on topic.** Create appropriately titled threads for new discussions. Start a new thread when a discussion topic shifts substantially.

**12.4 Follow moderator directions.** Follow the directions of forum moderators and community administrators.

## **Section 13 - Use your skills responsibly**

The skills you build here carry real-world consequences. This section sets out your ethical obligations as a member of this community.

**13.1 No malicious application of skills.** Do not use techniques, methods, or knowledge gained through the Services to attack, compromise, or cause harm to any person, system, or organisation outside a designated training environment - whether or not that conduct would separately violate Section 1 or Section 3.

**13.2 No offering unauthorised hacking services.** Do not use the Services or any Hack The Box community space to advertise, offer, solicit, or broker unauthorised hacking, intrusion, surveillance, or attack services - whether for payment or otherwise. For restrictions on distributing exploits and attack tools through the Services, see also Section 5.2.

**13.3 No recruiting for malicious activity.** Do not use the Services or any Hack The Box community space to recruit, direct, or organise other users to participate in malicious, unauthorised, or unlawful cyber activity.

**13.4 Responsible handling of real-world discoveries.** If your training or research on the platform leads you to discover a vulnerability in a real-world system that is not part of the Services, do not exploit it. Follow the affected organisation's responsible disclosure process where one exists. If no disclosure process exists, consider reporting through a coordinated disclosure programme.

**13.5 No misrepresenting platform affiliation.** Do not claim that any external activity - including unauthorised security testing, penetration testing, or research - is authorised, endorsed, or affiliated with Hack The Box.

## **PART C - Reporting, Enforcement and Appeals**

### **Section 14 - Reporting**

14.1 If you believe any content, action, or behaviour violates this policy, you may report it through in-platform reporting tools (where available) or by email to [customerops@hackthebox.com](mailto:customerops@hackthebox.com). You do not need a Hack The Box account to submit a report. Include enough detail for us to identify and investigate the issue.

14.2 We will acknowledge your report within 7 days and provide an outcome - or a status update - within 30 days. If an issue requires more time, we will tell you.

14.3 Good-faith reporting will never result in enforcement action against you. We may suspend the processing of reports from any person who frequently submits manifestly unfounded reports, after issuing a warning.

14.4 Security vulnerabilities in Hack The Box infrastructure should be reported through our Vulnerability Disclosure Program at [https://hackerone.com/hack\\_the\\_box](https://hackerone.com/hack_the_box), not through this process.

14.5 **Copyright Infringement (DMCA)**. We respect the intellectual property rights of others and expect our users to do the same. If you believe that any content on the Services infringes your copyright, you may submit a notification pursuant to the Digital Millennium Copyright Act (DMCA) or equivalent applicable laws by sending a written notice to [customerops@hackthebox.com](mailto:customerops@hackthebox.com) (cc: [legal@hackthebox.com](mailto:legal@hackthebox.com)). To be effective, your notice must include:

- (a) A physical or electronic signature of a person authorized to act on behalf of the owner of the copyright interest;
- (b) Identification of the copyrighted work claimed to have been infringed;
- (c) Identification of the material that is claimed to be infringing and sufficient information to permit us to locate the material (e.g., a specific URL);
- (d) Your contact information, including your name, address, telephone number, and email address;
- (e) A statement that you have a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law; and
- (f) A statement that the information in the notification is accurate, and under penalty of perjury, that you are authorized to act on behalf of the copyright owner.

We will respond to valid, complete notices by removing or disabling access to the infringing material. In accordance with Section 16, we maintain a policy that provides for the termination of accounts belonging to users who are repeated infringers.

### **Section 15 - How we detect violations**

15.1 We use automated and manual methods to detect potential violations - including platform monitoring, user reports, and collaboration with proctoring services or authorities where lawful. Flagged activity is always reviewed by a person before enforcement action is taken.

## Section 16 - Enforcement

**16.1 Contractual effect.** This policy is incorporated into your Service Agreement. Any violation is a breach of that agreement. Attempted violations and assisting others to commit violations are treated as actual violations.

**16.2 Proportionality.** Every enforcement decision must be proportionate to the violation, necessary to achieve a legitimate aim, and no more restrictive than required. We consider the nature and severity of the violation, intent, prior history, cooperation, and any mitigating or aggravating circumstances. Repeated violations lead to escalating consequences.

**16.3 Interim measures.** While investigating, we may temporarily restrict access or remove content to prevent ongoing harm. Interim measures are not a finding of violation. If no violation is found, we reverse them without undue delay.

**16.4 Available actions.** We determine the appropriate enforcement response based on the factors in Section 16.2, not on which section was violated. Serious violations may result in immediate suspension or permanent ban without prior warning. Enforcement actions may include:

- **Warning:** A formal notice logged on your account, with no immediate access restrictions.
- **Reputational restriction:** Removal from leaderboards, stripping of points or flags, or a restriction on earning future reputation.
- **Content removal:** The removal of any content you uploaded that violates this policy.
- **Suspension:** A time-limited block on some or all access to the Services.
- **Permanent ban:** The permanent removal of access and termination of your account. No new account will be permitted.

**16.5 Notification.** When we take enforcement action, we will tell you: what you did, which section you violated, what action we took and for how long, the evidence we relied on, and how to appeal.

**16.6 Credential action.** Where a violation relates to integrity or examination conduct, Hack The Box may invalidate exam results, revoke certifications, or impose a permanent ban from future certification attempts. Credential-specific actions are governed by the relevant credentialing agreement.

**16.7 Disclosure to authorities.** We may disclose information to law enforcement or regulatory authorities where we reasonably consider it necessary to protect the Services, users, or third parties. Where we receive a valid order from a court, law enforcement authority, or regulatory body requiring us to act against specific content or provide information about a user, we will comply in accordance with applicable law. We will notify you unless instructed otherwise by the issuing authority.

**16.8 Compliance-based restrictions.** The following restrictions are applied for legal or compliance reasons, not as enforcement action for a policy violation.

(a) **Age restriction.** Accounts identified as belonging to users under the age of 18 are restricted until verified parental or legal-guardian consent is provided in accordance with Section 10.2. On valid consent, the account is reinstated.

(b) **Sanctions and identity verification.** Accounts flagged due to potential sanctions-list matches or identity-verification concerns are restricted until the concern is resolved. On successful verification, the account is reinstated.

**16.9 Other consequences.** Enforcement action under this policy does not limit any other right or remedy available to Hack The Box - including termination of a business relationship under the applicable Service Agreement, or legal proceedings for costs or other appropriate relief. These are separate from individual enforcement and may be pursued independently or in addition to any action under this section.

**16.10 Data rights.** Enforcement does not override your rights under applicable data protection law. You retain the right to access, correct, or request deletion of your personal data in accordance with the Privacy Notice. Where we retain evidence to support an enforcement decision, active appeal, or legal obligation, we retain it only for as long as necessary.

**16.11 Customer Organisation environments.** Where a violation occurs within or relates to an environment controlled by a Customer Organisation, Hack The Box may enforce Part A directly and may restrict the user's access to community services for violations of Part B. Where conduct constitutes a violation of both Part A and Part B, Hack The Box may take enforcement action under Part A in respect of the full conduct. Hack The Box may notify the Customer Organisation to the extent permitted by applicable law and the applicable Service Agreement. A pattern of violations within a Customer Organisation's environment may be addressed under the terms of the Service Agreement.

## **Section 17 - Appeals**

**17.1 Your right to appeal.** If we take enforcement action against your account, content, or credentialing status, you may appeal. Your enforcement notice explains how.

**17.2 How to appeal.** Submit your appeal in writing to the address in your enforcement notice within 30 days. Include your username, the notice reference, your grounds for appeal, and any supporting evidence.

**17.3 Grounds for appeal.** You may appeal on the grounds that you did not commit the violation, we made an error, the action was disproportionate, or new evidence is available.

**17.4 Review.** Your appeal is reviewed by a person not involved in the original decision. We provide a written outcome within 10 business days. The decision may be upheld, modified, or overturned. Where overturned or modified, we reverse restrictions without undue delay. This decision is final, unless Section 17.5 applies.

**17.5 Second-level review.** If a first-level review upholds a permanent ban or a suspension of two years or more, you may request a second-level review within 14 days. A panel with no prior involvement decides within 10 business days. The panel's determination is final.

## Section 18 - Changes to this policy

**18.1 General & Urgent Updates.** We may update this policy at any time to reflect operational, legal, regulatory, or security changes. Non-material modifications - as well as urgent material changes necessary to comply with legal obligations, address security vulnerabilities, or prevent abuse - take effect immediately upon posting. We will notify you of urgent material changes as soon as reasonably practicable.

**18.2 Material Changes.** For all other material changes that significantly alter your rights or our enforcement practices, we will provide at least 30 days' prior notice (e.g., via email or prominent website notification). Your continued use of the Services after the effective date constitutes your acceptance of the updated policy. If you disagree with the changes, you must close your account before they take effect.

### Previous Versions

Version	Link
1.0	<a href="https://resources.hackthebox.com/hubfs/Legal/Terms/AUP/AUPV1.pdf">https://resources.hackthebox.com/hubfs/Legal/Terms/AUP/AUPV1.pdf</a>



**HACKTHEBOX**

---

[www.hackthebox.com](http://www.hackthebox.com)

[customerops@hackthebox.com](mailto:customerops@hackthebox.com)

[legal@hackthebox.com](mailto:legal@hackthebox.com)

[privacy@hackthebox.com](mailto:privacy@hackthebox.com)