MWANGI.DEV / VIBECHECK

Vibecheck Terms and Conditions

Version v1 | Effective 2 November 2026

Ian Mwangi, trading as Mwangi.dev
Legal notices: ian@mwangi.dev

Read before every scan

You must have permission to scan the target. By selecting the checkbox and submitting, you agree to these terms and appoint Vibecheck to perform the defined scan on your behalf. Your declaration cannot grant rights you do not hold. Optional report purchases are separate.

Contents

1. Agreement, provider and eligibility
2. Your permission and representations
3. Authority to act and good-faith reliance
4. What the scanner does and does not do
5. Operational risks, preparation and user control
6. Acceptable use and responsible handling
7. Reports, interpretation and intellectual property
8. Free previews, purchases, delivery and remedies
9. Privacy, service providers and international processing
10. Retention, privacy requests and legal holds
11. Responsibility, indemnity and limits of liability
12. Disputes, changes, termination and interpretation

Online version: https://www.mwangi.dev/vibecheck/terms
This document preserves mandatory consumer and privacy rights. See clauses 9-12 for personal-data handling, responsibility and disputes.

1. Agreement, provider and eligibility

1.1 These Vibecheck Terms and Conditions govern each public website scan requested through Mwangi.dev, the resulting preview, any purchased full report, and associated report delivery and support. The provider is Ian Mwangi, trading as Mwangi.dev, based in Nairobi, Kenya ("we", "us" or "our"). Legal notices, permission concerns, privacy requests and service complaints may be sent to ian@mwangi.dev. We publish an email contact rather than a street or postal service address; this does not displace any further disclosure required by applicable law.

1.2 "You" means the individual requesting a scan and, where that individual has authority to contract for an organisation, that organisation. "Target" means the public website URL you submit and the same-origin pages and resources sampled within the scanner's limits. "Scan" means the automated observations described in these terms, not unrestricted testing of the target's infrastructure. "Report" includes scores, observations, explanations, limitations and suggested fixes. A website being publicly reachable does not establish permission to test it.

1.3 You must be at least eighteen years old and have legal capacity to enter this agreement. If acting for an employer, client or other organisation, you represent that you are authorised both to accept these terms and to commission the specified scan. Access to an account, employment, a customer relationship or possession of a website URL does not by itself establish that authority. If you cannot make these confirmations accurately, do not request a scan.

1.4 Before each scan, you must positively select the acceptance checkbox and submit the request. This records your agreement to the displayed version and your instruction to perform that scan. Acceptance is not inferred from browsing the site, receiving an unsolicited message or silence. You can read and download the terms before deciding. Do not select the checkbox if you disagree; you may leave without starting a scan or purchasing a report.

1.5 The acceptance declaration is: "I agree to the Vibecheck Terms and Conditions. I confirm I own this website or have permission to scan it, and authorize Vibecheck to perform this scan on my behalf." It must be read with the scope, safeguards and legal exceptions in this document. We record a user declaration, not a verified identity, digital-signature certificate, ownership certificate or independent determination that all required permissions exist.

2. Your permission and representations

2.1 Before submitting a target, you must own the relevant website and have authority to commission the scan, or hold prior permission from the person or entity entitled to authorise the activities involved. Permission must cover the actual target, public pages, linked resources and automated browser activity within the scope described here. Where your authority is limited to a particular environment, host, path, time or method, request a scan only if this service can respect those limits.

2.2 You represent that your instruction does not violate a law, court order, contract, confidentiality obligation, hosting rule, platform rule or restriction imposed by an affected owner. Website ownership may not include authority over a hosting provider, shared server, content-delivery network, software vendor or another tenant. Obtain any additional approval necessary from those parties. Permission to browse or use a service is not necessarily permission to commission automated assessment of that service.

2.3 If you act as a consultant, employee, agency, managed-service provider or security researcher, ensure the relevant engagement expressly permits you to appoint a scanning service on the owner's behalf. Retain an appropriate record of that permission and its scope. Do not present a client's confidential permission letter publicly; if we reasonably request evidence, contact us so that an appropriate, limited disclosure can be arranged.

2.4 You must provide an accurate target and a contact address you are entitled to use. Check the spelling, hostname and environment before accepting. Do not submit passwords, access tokens, private account URLs, personal information in query strings, or addresses intended to trigger actions. If you discover a mistaken target, expired permission, an ownership dispute or a change in scope, stop submitting new requests and notify ian@mwangi.dev promptly with the scan identifier.

2.5 Your confirmations apply separately to every scan, even if you previously scanned the same target. A previous scan, payment or report does not establish continuing permission. You are responsible for your target selection, commissioning decision and authorised use of the results. This responsibility does not relieve us of duties imposed on us by law, extend your authority beyond its lawful limits, or bind a third party that did not authorise you.

3. Authority to act and good-faith reliance

3.1 By accepting and submitting, you appoint us to carry out the defined scan on your behalf and grant us the permissions and authority necessary to receive your instruction, access the authorised public target within that scope, execute the scanner, analyse permitted observations, prepare the report, and operate associated queue, storage and delivery systems. This grant extends only to rights you lawfully hold or are empowered to delegate. It is a limited service appointment, not a general power of attorney.

3.2 You authorise the use of service providers reasonably needed to perform those activities, subject to applicable privacy and security obligations. Their involvement does not create permission to access unrelated systems or reuse confidential target information for unrelated purposes. We do not acquire ownership of your website or a right to alter it. An expanded assessment, authenticated review, source-code audit or remediation engagement requires a separately agreed scope and any additional permissions it needs.

3.3 We operate on good-faith reliance on the user's express declaration. The standard public flow does not require DNS verification, a website-file challenge, a signed owner letter or an account login. We do not routinely establish the identity of a submitter or investigate the chain of authority before every request. This approach simplifies authorised use; it is not a representation that unauthorised scans become lawful, or a commitment to ignore credible warnings or legal obligations.

3.4 We may refuse or suspend a request, restrict targets, ask for reasonable proof, investigate apparent abuse or cooperate with a lawful investigation. We may contact an affected owner where necessary and lawful. We need not begin or complete a scan simply because you have selected the checkbox, received a scan identifier or offered payment. We will not knowingly treat a false declaration as valid authority after a relevant lack of permission becomes apparent.

3.5 You may withdraw instructions for future scans by making no further submissions. To raise a permission concern about a queued or running scan, email us promptly. The current public interface does not provide an immediate stop button, and we cannot guarantee that an email will be read before automated work completes. Withdrawal cannot reverse requests already sent or require destruction of evidence that must lawfully be preserved. Notify relevant owners and take protective action directly if urgent harm is suspected.

4. What the scanner does and does not do

4.1 Vibecheck performs a bounded automated assessment of publicly accessible website material. Depending on reachability and available resources, it observes DNS and TLS configuration, HTTP response headers, browser security policies, cookie attributes, public HTML and sampled scripts, metadata, publicly exposed credential patterns, loading measurements, browser errors, responsive overflow and automated accessibility indicators. Some checks may be skipped, unavailable or incomplete. The report should identify significant measurement and coverage limitations.

4.2 An automated browser may load the submitted page, execute its public JavaScript and observe same-origin resources requested during that load. The scanner may follow a limited set of same-origin public links, inspect sampled scripts and referenced source maps, and make limited header requests relevant to cross-origin policy observations. It does not promise to discover every route, asset, subdomain, deployment, API or vulnerability. Current implementation and safety budgets determine the actual sample.

4.3 The public scanner does not log into private accounts, request your source repository or database credentials, submit forms, perform credential guessing, intentionally exploit vulnerabilities, conduct denial-of-service tests or perform an unrestricted penetration test. It does not establish the security of authenticated workflows, tenant isolation, server-side permissions, payment processing, private storage or database policies. Those areas require separately authorised access and a distinct assessment.

4.4 The scanner applies public-destination restrictions and excludes recognised government or military targets. It uses its own scanner identity and conservative pacing and blocking rules. It may skip resources because of robots restrictions, rate limits, target responses, inaccessible dependencies, timeouts or safety controls. A request does not entitle you to bypass those controls, rotate identities, defeat a CAPTCHA or compel a host to allow scanning. Policies may become more restrictive when reasonably necessary for safe operation.

4.5 A public page load is not guaranteed to be free of side effects. The target's own code can perform actions, call services, create analytics events or load costly resources even without form submission. A badly designed endpoint may change state when read. You must consider that behaviour before commissioning a scan and use a suitable test environment if required. We retain responsibility for reasonable care in how we implement and operate our own scanner; these limitations do not excuse unlawful conduct.

5. Operational risks, preparation and user control

5.1 You control whether to request a scan, which eligible target to submit, whether to purchase a full report, and what action to take after reviewing findings. You do not control the scanner's internal scheduling, exact requests, source network address, instantaneous execution or third-party responses through the public interface. We do not represent that you have full technical control of the feature. Select the checkbox only after deciding that the available scope is appropriate for your authority and environment.

5.2 Automated requests may appear in server logs, monitoring tools and security alerts. Hosts may throttle or block traffic, incur ordinary bandwidth or compute costs, or investigate activity. A scan may be delayed, interrupted, incomplete or repeated internally following a recoverable delivery failure. We apply bounded safeguards but cannot guarantee zero operational impact, continuous availability, a particular completion time or acceptance by every hosting provider.

5.3 Before requesting an assessment of an important production site, consider traffic limits, owner restrictions, backups, recovery arrangements, monitoring and the timing of maintenance or business activity. If public browser loading could trigger dangerous or expensive behaviour, do not use this public feature for that target. Arrange a scoped engagement instead. You remain responsible for the target owner's operational decisions and for obtaining any required allowlisting through an authorised channel.

5.4 Do not interpret a report or suggested code as an instruction to change production immediately. Confirm findings, understand dependencies, test changes in a suitable environment and maintain a recovery path. We do not make changes to your application through this feature. You decide whether to implement a recommendation, seek specialist help or commission additional review. An example fix may need adaptation to your architecture and current library versions.

5.5 If you believe the service is causing an incident, take reasonable measures available to you as the target operator, including applying appropriate network controls, and notify us with the scan identifier and a concise description. Do not send secrets or sensitive log dumps by email. We may suspend further work while investigating. No clause requires you to leave a harmful request unblocked, waive emergency relief, or delay a report to a regulator or law-enforcement authority.

6. Acceptable use and responsible handling

6.1 Use Vibecheck only for lawful, authorised assessment and constructive remediation. Do not submit a competitor's, employer's, customer's or stranger's website without sufficient permission. Do not use it for harassment, surveillance, extortion, fraud, disruption, competitive sabotage, evasion of access controls or discovery intended to support unauthorised exploitation. A claim that a website is public, that the scan is free or that you are merely curious does not substitute for permission.

6.2 Do not attempt to evade target exclusions, private-network restrictions, queue controls, per-network limits, payment controls or report access protections. Do not supply misleading contact details, conceal an unauthorised target behind redirects or interfere with other users' reports. Do not probe the scanner itself beyond any separately published and applicable disclosure policy. We may preserve relevant evidence, restrict access and exercise lawful remedies when investigating abuse.

6.3 Reports can reveal weaknesses, architecture hints and sensitive business information. Treat them as confidential where appropriate. Share a report or its access link only with people entitled to see it. Do not publish another party's weaknesses or claim their endorsement. If you discover an exposed credential, do not test, spend, transfer or exploit it; inform the authorised owner through an appropriate private channel and recommend revocation and rotation.

6.4 Report-access links and owner tokens may control access to previews, payment status or unlocked findings. Protect them as you would other private links. Avoid placing them in public issue trackers, analytics payloads or screenshots. Contact us if a link is disclosed unintentionally. We cannot undo copies already made by a recipient or a third party outside our control, but will consider reasonable protective steps available within the service.

6.5 You may use reports for legitimate internal improvement and authorised client work. Do not alter a report to conceal limitations or imply that we certified compliance, approved a target or verified the authority of a submitter. Respect third-party intellectual property and confidentiality obligations. Nothing here restricts a truthful review, legally protected reporting, consultation with an adviser, or disclosure required by law, provided you do not unlawfully disclose another person's protected information.

7. Reports, interpretation and intellectual property

7.1 A report is a snapshot of sampled observations at a particular time and from a particular scanner environment. Websites, dependencies and network conditions change. Scores are product heuristics, not actuarial measures, certifications, regulatory approvals or promises that an application is safe to launch. A high score does not establish absence of vulnerabilities; a low score does not establish that a website has been compromised or that every flagged pattern is exploitable.

7.2 Findings may include false positives, false negatives and incomplete evidence. A token-shaped string may be a harmless public identifier; a missing header may have contextual explanations; a loading measurement may reflect network or scanner overhead. Confirm important findings against the target's actual configuration and intended behaviour. An unavailable or skipped check is not a passing result. Read the report's scope, timing and limitations before relying on its summary.

7.3 The public scan is not a legal, financial, compliance or insurance opinion, a comprehensive security audit, a substitute for incident response, or a guarantee of accessibility for all users. Automated accessibility observations do not replace manual testing and assistive-technology review. Loading observations are not a substitute for representative real-user measurements. Obtain suitable specialist advice where the consequences of error justify it.

7.4 You retain rights you or the target owner hold in submitted material. You grant us a limited right to process it for the requested service, secure operation, support and lawful record keeping as described here. We retain rights in our software, templates, methodology and original explanatory content. After any applicable payment, you may download and use your report for authorised purposes. This licence does not grant rights to third-party code or material beyond those independently available to you.

7.5 We may update the scanner or report presentation for future requests, but will not rewrite the terms version recorded for an earlier acceptance. Reports may disclose their own scoring or template version. A change in score between runs may reflect target changes, reachability or methodology rather than a confirmed new vulnerability. Contact us to query a suspected material error. We will consider the evidence and any remedy required by applicable law without promising a particular outcome before review.

8. Free previews, purchases, delivery and remedies

8.1 Submitting a permitted public scan provides the free preview described at the point of use. A full report is a separate optional purchase. At initial publication, the advertised full-report price is KSh 2,400 with M-Pesa or USD 19 with card where card checkout is available. Supported methods, availability, any applicable discount, currency and the final payable amount must be shown before you confirm payment. Displaying a method in descriptive text does not guarantee that checkout is currently enabled.

8.2 We will not charge you merely because you accept the scan terms or view a free preview. Do not approve a payment unless you recognise the amount, currency, service and recipient. Your bank or payment provider may apply disclosed charges or exchange rates under its own agreement. Payment credentials are handled through the applicable payment process; do not send card numbers, M-Pesa PINs or one-time passwords to our legal or support email.

8.3 A full report unlocks or is delivered after the service verifies a successful qualifying payment. A payment-provider delay may postpone confirmation. An entered telephone number or a browser redirect alone is not proof of successful payment. Keep the provider's transaction reference and contact us if payment appears successful but delivery has not occurred. We may request limited information necessary to reconcile the transaction, without asking for your PIN or password.

8.4 Where email delivery is offered, use an address you control and check spam or quarantine folders. Delivery can fail because of incorrect details, mailbox policies or provider incidents. A completed or incomplete scan may produce a report whose limitations affect its usefulness; review the preview and available limitations before purchasing. We do not guarantee that a scan will identify a fixed number of useful problems or that a purchase will improve your website automatically.

8.5 For duplicate charges, non-delivery, a materially defective report or another complaint, contact ian@mwangi.dev with the scan identifier and payment reference. We will investigate and provide any correction, replacement, refund or other remedy required by applicable law. These terms do not impose a blanket no-refund policy, remove statutory cancellation rights, or deem a digital-service right waived solely because you ticked the scan checkbox. Any additional consent legally required for immediate paid supply must be obtained separately at checkout.

9. Privacy, service providers and international processing

9.1 Ian Mwangi is responsible for personal data processed to operate this service, including submitted contact details and acceptance records. We process the target URL, scan observations, report and payment/delivery metadata to perform your requested service; protect the queue and reports; investigate abuse; provide support; reconcile purchases; comply with legal obligations; and establish, exercise or defend legal claims. We rely on the applicable contractual, legitimate-interest or legal-obligation basis where available, and obtain separate consent when law requires it.

9.2 Before a scan starts, we record its identifier, normalised target, submitted contact details, server acceptance time, terms version, document checksum, declaration version and an existing keyed hash of the requesting network address. This feature adds no raw IP field to the acceptance record. Network addresses may nevertheless be processed transiently for requests and may appear in infrastructure security logs under separate provider controls. A network hash is not proof of an individual's identity and is still treated as protected information where applicable.

9.3 The current service uses Vercel for the website, Google Cloud Run and Cloud Tasks for scan processing and scheduling, Supabase-hosted PostgreSQL for application records, Resend for report email, and Safaricom Daraja/M-Pesa for supported M-Pesa transactions. Stripe is used only where card checkout is enabled. The wider Mwangi.dev website uses PostHog analytics; the scan acceptance is not marketing consent. Operational notifications may be processed through Slack. We restrict disclosures to what is necessary for the relevant function and applicable law.

9.4 Scan processing currently uses Google infrastructure in Europe, and the application database uses Supabase infrastructure in Europe. Hosting, email, analytics, payment and support providers may process information in other countries according to their services. International processing remains subject to applicable transfer requirements and appropriate safeguards; selecting the checkbox does not waive those requirements or itself prove that every required safeguard exists. Contact us for information relevant to your request. Do not submit regulated or sensitive personal data that this public feature is not designed to assess.

9.5 The scanner samples public material and aims to redact suspected secrets from report evidence. It does not intentionally collect private accounts or request passwords, and does not retain ordinary target response bodies or screenshots as report artefacts. Accidental public exposure can still be observed; do not treat this statement as a guarantee of perfect redaction. We do not sell your acceptance record or grant a general licence to use confidential findings for advertising. Any optional marketing choice must be separate and must not be required to run a scan.

9.6 We apply access restrictions, private database permissions, protected report access and other reasonable safeguards. No online system is invulnerable. We will handle suspected personal-data incidents and any required notifications under applicable law. If you need a negotiated data-processing agreement, a particular transfer arrangement or an assessment involving non-public personal data, contact us before use; these public terms alone should not be assumed to satisfy every organisation-specific requirement.

10. Retention, privacy requests and legal holds

10.1 The minimal scan-acceptance evidence described in clause 9 is retained for one year from acceptance. Scheduled maintenance removes expired records independently of the report-retention setting. Deleting a report does not itself delete its still-valid acceptance record. The purpose of this limited retention is to document the instruction, respond to permission disputes and defend legitimate claims. It does not establish that every other operational record is automatically deleted after one year.

10.2 Report, payment, delivery, support, security and provider-log records have distinct purposes. Reports and purchase records are retained to support access, delivery, reconciliation and legitimate record keeping, subject to periodic review and any applicable legal requirements. We will not claim that all service data disappears when acceptance evidence expires. Contact us to request the applicable treatment of a particular record. We must assess whether continued retention is necessary and lawful rather than retain personal information indefinitely merely because storage is available.

10.3 A specific acceptance record may be held beyond its ordinary expiry only where a concrete dispute, legal obligation, investigation or reasonably anticipated claim justifies preservation. A hold must identify its reason, responsible operator and review/expiry date; it is not a blanket extension for all users. Holds are limited, reviewed at least every ninety days and renewed only with a recorded continuing justification. When the justification ends, expired evidence becomes eligible for deletion at the next maintenance run.

10.4 Subject to applicable law, you may ask to access, correct or erase your personal data, object to or restrict processing, obtain portability where applicable, or withdraw a separate consent on which processing depends. Contact ian@mwangi.dev with enough information to locate your request, without sending passwords. We may need proportionate identity or authority verification to avoid disclosing another person's report. Some requests may be limited by another person's rights, legal obligations, fraud prevention or the lawful preservation of claims.

10.5 Withdrawal of marketing consent does not cancel a service instruction already carried out. Erasure is not always immediate where payment records, a specific legal hold or another lawful basis requires retention. We will explain a relevant refusal or limitation and provide the response required by applicable law. You may complain to Kenya's Office of the Data Protection Commissioner at https://www.odpc.go.ke/ or another competent supervisory authority. These terms do not require you to complain to us first or restrict statutory remedies.

11. Responsibility, indemnity and limits of liability

11.1 We will exercise the care required by applicable law in providing the service. Subject to that standard and the exceptions below, the service and sampled findings are supplied with the scope and limitations described here, without additional promises of uninterrupted availability, error-free operation, complete detection, fitness for a particular launch decision, or a particular financial or security outcome. Mandatory warranties and service standards continue to apply despite any contrary wording in this agreement.

11.2 To the extent lawful and reasonable, neither party is responsible to the other for losses that were not reasonably foreseeable when the relevant scan or purchase was requested. Subject to mandatory law, we exclude liability for indirect or consequential losses and loss of anticipated profits or business opportunity arising from ordinary use of the service. The label applied to a loss does not determine whether an exclusion is legally effective. This clause does not exclude a consumer remedy that cannot lawfully be excluded.

11.3 Subject to clause 11.4, our total aggregate liability arising out of or connected with Vibecheck during any twelve-month period is limited to the greater of KSh 2,400 or the total Vibecheck fees you paid us in the twelve months preceding the event giving rise to the claim. Non-KES fees are assessed at a reasonable documented exchange rate at the relevant payment date. The cap applies only to the extent permitted by applicable law and is not a representation of a court's determination of damages.

11.4 No exclusion, cap, indemnity or disclaimer in these terms limits liability for fraud or fraudulent misrepresentation, deliberate unlawful conduct, gross negligence, death or personal injury caused by negligence where exclusion is prohibited, or any other liability or statutory right that cannot lawfully be excluded or limited. Statutory privacy, consumer, refund and regulatory rights remain effective. No agreement between us can prevent prosecution, bind a regulator or release claims belonging to a non-consenting third party.

11.5 To the extent permitted by law, you will indemnify us against reasonable, documented third-party claims and direct losses caused by your knowingly or negligently false permission declaration, your unlawful commissioning of a target, or your deliberate prohibited use. This obligation applies only to the extent your conduct caused the loss; it does not require you to pay for our own unlawful acts, negligence or independent breach. It is not a general indemnity for every incident connected with a scan.

11.6 For an indemnity claim, we will give reasonably prompt notice, take reasonable steps to reduce avoidable loss, and allow you a reasonable opportunity to participate in the defence. Neither party may agree a settlement imposing admissions, non-monetary obligations or payments on the other without that party's consent, not to be unreasonably withheld. Each party remains responsible for its own legal duties. Nothing requires you to indemnify a penalty where doing so would be unlawful or contrary to public policy.

12. Disputes, changes, termination and interpretation

12.1 These terms are governed by Kenyan law, subject to mandatory protections that apply to you in another jurisdiction. The competent courts of Kenya may hear disputes, without depriving a consumer of a non-waivable right to bring proceedings in another competent court. We do not impose mandatory arbitration, a class-action waiver or a contractual shortening of statutory limitation periods. Urgent protective relief and access to regulators or law enforcement remain available.

12.2 For a service concern, email ian@mwangi.dev with a clear description, scan identifier and any relevant payment reference. We will seek a practical resolution, but informal discussion is not a condition that overrides your legal deadlines or access to a competent authority. Send legal notices in a form and manner required by applicable procedural law; publishing an email contact does not purport to override formal service requirements.

12.3 We may suspend or discontinue access for unlawful use, credible permission concerns, security incidents, non-payment for an optional purchase or operational reasons. Where reasonably practicable and lawful, we will explain material action affecting a purchased service and address any required remedy. Suspension does not automatically forfeit statutory rights, erase evidence or expand the original scan authority. You may stop using the service at any time, subject to obligations already lawfully incurred.

12.4 Future changes receive a new terms version and effective date. A fresh scan requires acceptance of the current version. We retain the published version associated with earlier requests and do not retroactively replace their recorded agreement. A material expansion of scanning activities requires appropriate updated disclosure and authority; a general changes clause is not permission for undisclosed intrusive testing. An optional separately signed engagement governs its stated scope where it expressly overrides these public terms.

12.5 If a provision is invalid or unenforceable, it is limited or severed only to the extent lawful, and the remaining provisions continue where they can operate fairly. A delay in enforcing a right is not a permanent waiver. Neither party may transfer obligations in a way that unlawfully reduces the other's rights. No agency beyond the limited scan appointment is created, and no partnership, employment relationship or third-party endorsement is implied.

12.6 Read this document as a whole. Headings aid navigation and do not conceal exceptions. "Including" introduces examples, not permission to disregard scope. Any legally required consumer-favourable interpretation applies. Clauses concerning accrued payment obligations, confidential findings, lawful record keeping, intellectual property, liability and disputes survive only as necessary and lawful. These terms document the parties' intended agreement; they are not a promise of universal enforceability or a certificate that a particular scan is lawful.