ACCEPTABLE USE POLICY

Remote Physical Phones and Customer-Owned SIM Cards

Version 1.0 | Effective date: 20 October 2026
Last updated: 20 October 2026

1. PURPOSE, SCOPE AND CONTRACT DOCUMENTS

1.1 **Provider and contact.** HiveReach is operated by Yevgeniy Kovalev, a sole trader registered in Poland in the Central Register and Information on Economic Activity, trading as HiveReach. NIP: 5272991183. REGON: 521331015. Correspondence address: ul. Okólnik 11A, lok. 77, 00-368 Warszawa, Poland. For service questions, misuse reports and appeals, contact support@hivereach.app. Customer-service telephone: +48 507 275 570.

1.2 **Scope.** This Acceptable Use Policy (AUP) sets the conduct rules for the HiveReach website, accounts, supported access applications, remote physical phones, shared access, demonstrations and SIM-related services. It applies to Account Holders and Authorised Users, including during free access and approved extensions. You must not knowingly assist another person to carry out prohibited conduct through the service.

1.3 **Defined terms and acceptance.** Capitalised terms have the meanings given in the Terms of Service (Terms). In particular, a Device is the assigned physical Android handset, and an Authorised User is an individual invited through HiveReach sharing controls. Acceptance and contract formation follow section 3 of the Terms; changes for existing customers follow section 25 of the Terms.

1.4 **Relationship with other documents.** This AUP forms part of the agreement described in section 2 of the Terms and provides specific use restrictions. It does not expand HiveReach's enforcement powers beyond the Terms or reduce contractual remedies or mandatory rights. An applicable Data Processing Agreement (DPA) prevails for its subject matter, subject to mandatory law and binding transfer clauses. Specifically negotiated arrangements have the priority stated in the Terms. The Privacy Policy explains personal-data processing; this AUP does not authorise additional processing.

2. PERMITTED USE AND THIRD-PARTY SERVICES

2.1 **Legitimate use.** Subject to this AUP, the Terms and the functionality included in your order, you may use the service for lawful business and personal activities, including managing your own or authorised client accounts, publishing content, customer communications and application testing. You must have authority to access the accounts and information involved. Agency work and management of multiple authorised accounts are not, by themselves, prohibited.

2.2 **Third-party obligations.** You remain responsible for obligations you owe to applications, social networks, advertising platforms, marketplaces and other third parties. A breach of a platform rule does not solely for that reason become an AUP violation; the specific restrictions in this AUP still apply. A platform complaint or account block is information to assess, not automatic proof of misconduct. HiveReach does not supply campaigns, artificial-engagement services or assistance defeating platform restrictions.

2.3 **Automation and location.** Automation, scheduling and ordinary use of a VPN are not prohibited solely because of the method used; the same conduct and security restrictions apply. HiveReach does not guarantee compatibility or third-party permission. A Device's physical location does not establish your residence, personal location or eligibility for a third-party service. Do not use it as false evidence of those facts.

3. ACCOUNTS, SHARING AND VERIFICATION

3.1 **Eligible and accurate accounts.** Individual Account Holders and Authorised Users must be at least 18 years old and have the required legal capacity. Organisations must act through duly authorised adult representatives. Provide accurate identity, contact and billing information and keep it current. Do not impersonate another person, submit forged documents, misrepresent your authority or use someone else's identity or payment details without lawful authority.

3.2 **Secure individual access.** Protect credentials, authentication codes and session access. Do not sell, lend or share your main HiveReach login. Use the sharing controls so each Authorised User has an individual HiveReach identity, accepts the Terms and AUP, and completes any applicable verification. Invite only people you are entitled to authorise and revoke access promptly when that authority ends. Do not transfer or resell paid access or the contract outside authorised sharing or an express agreement with HiveReach.

3.3 **Applicable identity checks.** Stripe Identity is required for the purchasing Account Holder only where the selected carrier does not require customer identity verification. Where the carrier requires identification, complete its procedure yourself; HiveReach does not require a routine duplicate Stripe check or documentary proof of the carrier check. The purchaser requirement does not automatically impose Stripe checks on every invitee. Separately applicable phone verification and proportionate re-verification follow section 6 of the Terms.

3.4 **No verification abuse.** Do not bypass required identity or age checks through impersonation, falsified information, manipulated documents or substituted verification evidence. Do not ask a Host Manager or another person to impersonate you or complete a personal identity check in your place. Follow any lawful representative procedure provided by the carrier or verification provider. A verification difficulty or inconclusive result alone is not proof of dishonesty.

3.5 **Responsibility and compromise.** Each user is responsible for their own conduct. Account Holder responsibility for authorised users follows section 7 of the Terms and applicable law, including consumer and protected sole-trader safeguards. You are not automatically responsible for every action of an unrelated attacker. Report suspected compromise promptly to support@hivereach.app and take reasonable steps to protect or revoke affected access.

4. SIM CARDS, CARRIERS AND VERIFICATION CODES

4.1 **Your carrier relationship.** The catalogue SIM is acquired for you and is to be registered to you with the carrier. You control your carrier account and complete activation, registration, required identity checks and mobile-plan payments directly with the carrier using your own device, not the rented Device. HiveReach and Host Managers do not activate the SIM or complete identity checks for you. New SIM purchases are catalogue-only; reuse of a SIM already held for you follows the Terms.

4.2 **No telecommunications or code abuse.** Do not clone a SIM, carry out an unauthorised SIM swap or number transfer, misrepresent the lawful subscriber, or intercept another person's calls, messages or verification codes. Do not sell or supply access to received codes to facilitate fraud, unauthorised account access or identity-check evasion. Receiving codes for accounts you own or are authorised to administer is permitted unless another specific restriction applies, including the financial-services prohibition below.

4.3 **Handling and service limits.** Protect SIM identifiers, PINs, PUKs and activation materials. Send physical handling or maintenance requests through HiveReach. Do not ask a Host Manager to use their identity, address or personal accounts as if they were yours. Carrier connectivity, account rights and charges remain subject to your separate carrier arrangement. Do not rely on a remotely hosted Device to contact emergency responders at your location.

5. PROHIBITED CONDUCT

5.1 **Unlawful activity and fraud.** Do not use the service to commit, facilitate or knowingly conceal unlawful activity, including scams, phishing, identity theft, payment-card testing, use of stolen payment details, fraudulent purchases, extortion or money laundering. Do not create false claims, messages or websites to obtain money, credentials, identity documents or other information by deception. Applicable sanctions and legal restrictions must be respected.

5.2 **Unauthorised access and malicious software.** Do not access accounts, devices, networks or information without authority; attempt account takeovers, credential stuffing or password attacks; or steal credentials, tokens or sessions. Do not install, distribute or operate malware, ransomware, spyware, botnets or software intended to compromise others. Do not exploit vulnerabilities or conduct intrusive security testing against HiveReach, hosts, other customers or third parties without the relevant owner's prior authorisation.

5.3 **Spam and abusive communications.** Do not send unsolicited bulk messages, automate abusive contact, flood comments or inboxes, harvest contacts unlawfully, or evade a recipient's block to harass them. Respect applicable consent, sender-identification and opt-out requirements. After a clear opt-out or request to stop, do not continue marketing or harassing contact. Necessary service, legal and security communications remain permitted where lawful.

5.4 **Deceptive manipulation.** Do not fabricate customer reviews, testimonials, ratings, endorsements or interactions to mislead others about genuine independent experience or interest. Do not use coordinated false identities, undisclosed impersonation or manufactured account activity to defraud people, manipulate transactions or conceal another violation of this AUP. Managing several authorised accounts or using a scheduling tool is not, by itself, deceptive manipulation.

5.5 **Abuse, exploitation and harmful content.** Do not create, obtain, store, distribute or facilitate child sexual abuse material or sexual exploitation; non-consensual intimate imagery, including synthetic imagery; human trafficking; credible threats; targeted harassment; or incitement to violence. Do not publish private information to facilitate stalking, intimidation or harm. Do not use the service to arrange unlawful trade in goods or services, or regulated activity without the permissions required by law.

5.6 **Privacy and intellectual property.** Do not steal, unlawfully collect, disclose or sell personal data, confidential information, trade secrets or copyrighted material. Do not infringe another person's copyright, trade mark or other rights, or falsely claim affiliation with HiveReach, a carrier or another organisation. Do not use shared access or HiveReach monitoring to conduct covert surveillance of employees, clients or other people.

5.7 **Disruption and restriction evasion.** Do not deliberately overload, damage or disrupt HiveReach equipment, communications, another user's service or a third-party system. Do not defeat HiveReach access controls, session limits, security measures or a lawful restriction by using another identity, invitation or account. This does not prevent a bona fide appeal, a lawful security report or restoration expressly permitted by HiveReach.

6. BANKING AND FINANCIAL SERVICES

6.1 **Device-wide prohibition.** You must not use banking or financial-service applications or websites through a rented Device, whether through an app, browser, embedded web view or another method. This includes banking, payment and money-transfer services, financial wallets, investment or brokerage services, cryptocurrency services, and credit or lending services.

6.2 **Activities covered.** Creating or verifying such accounts, signing in, accessing balances or financial records, and initiating transactions are prohibited even if the activity is lawful and the account belongs to you. This restriction concerns the rented Device; it does not prevent you from paying HiveReach through its checkout using your own device. Carrier activation and plan payments must also be completed using your own device, as described in section 4.1 above.

7. DEVICE INTEGRITY AND ACCESS BOUNDARIES

7.1 **Preserve device management.** Do not root the Device, unlock its bootloader, install replacement firmware, alter protected hardware identifiers or factory-reset it without HiveReach's prior express authorisation. Do not remove, disable or tamper with HiveReach management, remote-access, authentication, security, logging or monitoring components, or deliberately falsify their records. Ordinary app installation and settings changes remain permitted within the supplied access and this AUP.

7.2 **Respect the assigned environment.** Do not attempt to access another customer's Device or data, a host machine, the Host Manager's local network or personal equipment, or HiveReach administrative systems outside your granted authority. Do not install an undisclosed access method to let another person bypass individual HiveReach identities, sharing controls or applicable verification.

7.3 **Restricted hardware functions.** Camera and microphone access and outgoing voice calls are not included unless expressly stated in your order. Do not bypass a disabled function or use hardware to observe or record the host premises or people there without the required authority and lawful basis. Owning the SIM does not give you ownership of the handset, its IP address or IMEI, or control over host premises.

7.4 **Security reports.** If you discover a vulnerability or unintended access, stop activity beyond what is necessary to identify the issue, avoid viewing or copying other people's information, and report it to support@hivereach.app. A good-faith report is not itself an AUP breach. Reporting does not authorise further exploitation, disruption or access beyond the relevant owner's permission or applicable statutory rights.

8. PERSONAL DATA AND SHARED CONTENT

8.1 **Authority, notices and a required DPA.** Have the rights, authority and lawful basis needed for information you introduce or access. Businesses and agencies must give required notices to employees, clients and other affected people. Where HiveReach processes personal data on your documented instructions and a DPA is required, arrange it through support@hivereach.app before that processing begins. The AUP and Privacy Policy do not replace a required DPA.

8.2 **Shared visibility and data care.** Invitees may see apps, files and accounts already present on the same Device; sharing does not itself create isolated Android profiles or sign existing accounts out. Grant access accordingly. Avoid placing unnecessary sensitive information on a Device, maintain independent backups, and remove or export important material before access expires. Do not use the Device as the sole repository of important records.

8.3 **Independent responsibilities.** Acceptance of this AUP does not waive privacy rights, supply consent for another person or relieve HiveReach of its own security, transparency and data-protection duties. You retain rights you lawfully hold in your content. HiveReach's permissions are limited to those in the Terms and applicable processing arrangements.

9. DEMONSTRATIONS AND PRE-INSTALLATION ACCESS

9.1 **Public demonstration.** A public demonstration phone may be shared with other visitors. Do not sign into personal or client accounts, enter credentials, or leave confidential material on it. Apps, files, logins and settings left behind may remain visible to later visitors. Follow the displayed feature and session limits.

9.2 **Before and after SIM installation.** Pre-installation test access is limited to checking remote control, image quality, responsiveness and connection stability. Do not install apps or sign into personal or client accounts at that stage. Once the SIM is installed and full access is available under the Terms, permitted app installation and authorised account use may begin, including during the initial free period and an approved extension.

10. MONITORING, EVIDENCE AND PRIVACY SAFEGUARDS

10.1 **Disclosed monitoring.** HiveReach uses the connection history and periodic full-screen capture described in the Privacy Policy to protect the service and investigate misuse. Screenshots are captured during authorised remote-control sessions, including idle periods; a temporary disconnect may not stop capture until session authority expires. Images can contain private messages, credentials and sensitive information. Prohibited use does not mean such information is automatically excluded or masked. The public demonstration is outside the rental screenshot-monitoring programme and detailed rental connection-history log.

10.2 **Analysis and human assessment.** Screenshots are analysed on HiveReach's own server in Poland without an external AI service provider or retained Polish screenshot copy after analysis. Images and extracted information are not used to train models. A flag indicates a possible issue, not a finding of a breach or crime. Adverse enforcement based on a flag requires meaningful review by an authorised person able to assess context and reject or reverse the proposed outcome. Urgent protective restrictions remain subject to prompt review.

10.3 **Limited access.** Only authorised HiveReach personnel may review relevant evidence or access a Device for a documented legitimate security or abuse investigation, necessary support or maintenance, or compliance with a lawful obligation. Unrelated or curiosity-driven viewing is prohibited. Host Managers provide local handling and instructed maintenance; their role does not authorise moderation or viewing, copying or using customer content for their own purposes.

10.4 **Screenshot retention.** Screenshots and associated capture metadata, flags and explanations are ordinarily retained for up to 30 days from capture and deleted earlier when no longer necessary. Screenshots are stored at the originating host location, without screenshot backups. Longer retention of selected screenshot evidence follows Privacy Policy section 8.7: an established AUP violation and continuing necessity for that violation, appeal or related legal claim, or an independent binding preservation obligation. An automated flag alone does not extend retention. Holds are scoped, documented, reviewed and ended when no longer justified.

10.5 **Other evidence and its limits.** Detailed connection history follows its separate period of up to 365 days after session termination, or the last established authorisation deadline where termination cannot be confirmed, subject to justified case holds under the Privacy Policy. It does not itself contain message content, passwords or network-traffic content. IP observations and session references are assessed in context and do not conclusively identify the person responsible for every action. Verification and other records follow their own disclosed periods; this AUP does not extend them.

10.6 **Authorities and rights.** Preservation and disclosure to authorities follow section 20 of the Terms and the Privacy Policy, including assessment of authority, scope, lawful basis and applicable transfer rules. A discretionary request alone does not authorise disclosure. Narrow emergency disclosure is possible only where law permits it to address an imminent threat of death or serious physical harm. Applicable notice duties and rights to object, seek access or challenge processing remain available.

11. REPORTING MISUSE

11.1 **How to report.** Send reports to support@hivereach.app with a description, relevant dates and time zone, the account, Device, order or content reference if known, and the reason you believe the conduct is unlawful or breaches this AUP. Include relevant evidence you can lawfully provide and a contact route for follow-up. People without a HiveReach account may also report concerns. A missing reference does not prevent assessment of an otherwise identifiable issue.

11.2 **Safe and truthful reports.** Provide information honestly and distinguish observed facts from suspicions. Do not fabricate evidence or knowingly make false allegations. An honest mistake does not itself establish abuse. Redact unrelated personal data; do not email passwords, identity documents or unlawful imagery. Describe the issue and relevant location instead, and contact appropriate emergency services directly where immediate danger requires it. We assess reports without treating an allegation as proof.

12. RESTRICTIONS, INVESTIGATION AND TERMINATION

12.1 **Evidence and proportionality.** Enforcement follows sections 17 and 18 of the Terms. Where supported by the evidence, we may explain a concern, request correction, restrict affected features, suspend access or end the affected contract. A restriction must have the grounds and proportionate scope required by the Terms. We consider the conduct, seriousness, harm, available explanation and whether correction can address the risk. Non-payment, inability to supply or a carrier restriction does not by itself establish an AUP violation.

12.2 **Correction, urgent action and review.** Where feasible, we explain the issue and allow a reasonable opportunity to correct it. Immediate restriction is possible where delay creates material fraud, security, safety or legal risk. An investigation may use relevant logs, scoped screen evidence, your explanation and proportionate re-verification. We review continuing restrictions and restore access when their grounds cease. Notice may be delayed or limited only as permitted by law and the Terms.

12.3 **Termination and charges.** A material breach that remains uncorrected after reasonable notice may justify termination; immediate termination is available only where the seriousness of the breach or mandatory law justifies it under the Terms. Termination is not an automatic forfeiture of prepaid fees or your SIM. Unused-service refunds and any lawful, explained and supported deductions follow section 18 of the Terms. No new penalty, consumer indemnity or automatic loss of the unused balance is created by this AUP.

12.4 **Data and retained SIMs.** Device assignment, applicable grace and wiping procedures, content retrieval and SIM storage or return follow section 16 of the Terms, the Privacy Policy and any applicable DPA. An allegation does not authorise unrestricted evidence retention or immediate destruction of customer data. Mandatory retrieval rights remain available without requiring a renewal purchase. Unless the purchase is reversed by a full refund, your SIM remains yours; lawful preservation requirements may affect handling.

13. APPEALS, COMPLAINTS AND PROTECTED RIGHTS

13.1 **Free review.** You may challenge a restriction or enforcement decision without charge by emailing support@hivereach.app or writing to the address in section 1.1. Include available account or order details, the decision, your explanation and the outcome requested. You may appeal within 30 days after notice; a later request with a reasonable explanation will also be considered. A missing reference is not a reason to reject an otherwise identifiable complaint.

13.2 **Response and decision-maker.** We acknowledge complaints and appeals promptly and provide a reasoned response on a durable medium within 14 calendar days, subject to any shorter mandatory deadline or statutory consequence for non-response. Clarification does not automatically restart a statutory deadline. A person with authority to change the decision considers the appeal and your evidence; where practicable, this is someone not responsible for the original decision.

13.3 **No retaliation or waiver.** A bona fide complaint, appeal, withdrawal, payment dispute, security report or exercise of privacy rights is not itself an AUP breach. Consumer and qualifying sole-trader protections remain unaffected. This process does not shorten statutory claim periods or any longer mandatory complaint or appeal period, or make court or regulatory remedies conditional on an internal appeal. Data-protection requests retain the separate procedure and deadlines in the Privacy Policy.

14. POLICY CHANGES

14.1 **Notice and applicable rights.** Changes to this AUP follow section 25 of the Terms, including justified and proportionate reasons, clear advance notice of material changes on a durable medium, normally at least 30 days, and express agreement where required. Urgent legal or security changes may take effect sooner only where necessary and lawful. Adverse-change termination and refund rights remain available. Updated rules do not retrospectively turn earlier conduct into a breach.