Acceptable Use Policy

Politica di utilizzo accettabile dei servizi HyperBit

La presente Acceptable Use Policy (di seguito «AUP») costituisce parte integrante delle Condizioni Generali di Servizio HyperBit. Definisce le regole di utilizzo dei servizi forniti da HyperBit SRLs e si applica a tutti i Clienti, end-user e ospiti della rete AS208437. L'inosservanza dell'AUP può comportare la sospensione o la risoluzione del contratto ai sensi degli artt. 1453 e 1456 c.c.

1. Principio generale e neutralità della rete

HyperBit garantisce il libero accesso a Internet ai propri Clienti senza restrizioni discriminatorie sui contenuti, applicazioni e servizi, in conformità con il Regolamento (UE) 2015/2120 sulla neutralità della rete. La presente AUP non disciplina restrizioni sui contenuti leciti consultati dai Clienti, ma unicamente comportamenti che ledono diritti di terzi, violano la legge o compromettono l'integrità della rete.

HyperBit non monitora attivamente il traffico dei Clienti, non ha obbligo né diritto generale di controllo (art. 17 D.Lgs. 70/2003, «mere conduit») e interviene esclusivamente a fronte di:

- segnalazioni formali da terzi legittimati (titolari di diritto, autorità);
- ordini dell'Autorità Giudiziaria;
- evidenze tecniche di compromissione della rete o di altri Clienti.

2. Comportamenti vietati

Al Cliente è espressamente vietato utilizzare i servizi HyperBit per:

2.1. Attività illecite

- commettere reati di qualsiasi natura, anche informatici (artt. 615-ter e segg. c.p.);
- diffondere materiale pedopornografico (art. 600-ter c.p., L. 269/1998, L. 38/2006);
- istigare al terrorismo o ad atti di violenza (artt. 270-bis e segg. c.p.);
- diffondere contenuti che incitano all'odio razziale, etnico, religioso o di genere (L. 654/1975, L. 205/1993, L. 115/2016);
- diffondere materiale diffamatorio, ingiurioso o lesivo della reputazione altrui;
- violare diritti di proprietà intellettuale e industriale (L. 633/1941, D.Lgs. 30/2005);
- effettuare attività di phishing, frodi, social engineering o impersonificazione.

2.2. Abuso tecnico e sicurezza

- effettuare accessi non autorizzati a sistemi informatici di terzi (port scanning massivo, brute-forcing, sfruttamento di vulnerabilità);
- diffondere malware, virus, ransomware, worm, trojan, spyware o backdoor;
- partecipare a botnet, command-and-control, attività di hosting per malware;
- effettuare attacchi DoS/DDoS (Denial of Service) verso sistemi terzi;

- effettuare attività di spoofing (IP, MAC, ARP, DNS, BGP) o IP-prefix hijacking;
- effettuare amplificazione di attacchi tramite servizi mal configurati (DNS open resolver, NTP monlist, SNMP, Memcached, CharGen, ecc.);
- effettuare attività di cryptojacking non autorizzata su sistemi di terzi;
- bypassare misure di sicurezza, di autenticazione o di filtraggio della rete HyperBit.

2.3. Spam e abusi via email/voce

- inviare messaggi non sollecitati (spam) via email, SMS, MMS in violazione del D.Lgs. 196/2003 (Codice Privacy) e dell'art. 130 (consenso preventivo);
- effettuare campagne di telemarketing in violazione del Registro Pubblico delle Opposizioni (L. 5/2018) e delle Delibere AGCOM in materia;
- effettuare chiamate VoIP automatizzate massive (robocalling) senza autorizzazione;
- effettuare toll fraud (frode telefonica): chiamate massive verso numerazioni a sovrapprezzo, satellitari, internazionali premium con finalità fraudolente;
- effettuare CLI spoofing illecito (presentazione di un Calling Line Identifier falsificato per ingannare il destinatario), in violazione dell'art. 98-vicies-quater D.Lgs. 259/2003 e Delibera AGCOM 9/23/CIR.

2.4. Abusi sulla rete e infrastruttura

- generare traffico anomalo, ripetitivo o automatizzato finalizzato a saturare la rete o gli apparati HyperBit;
- effettuare scansioni massive di intere subnet senza autorizzazione;
- distribuire o esporre servizi noti per essere abusati come amplificatori (open resolver DNS pubblici, server NTP non patchati, server SMTP open relay);
- ridistribuire la connettività HyperBit a terzi non identificati senza preventiva autorizzazione scritta (resale non autorizzato);
- annunciare prefissi IP non assegnati o non autorizzati via BGP.

3. Regole specifiche per servizi VoIP

In aggiunta a quanto sopra, per i servizi voce VoIP il Cliente:

- non può utilizzare il servizio per terminazione di traffico di rivendita di terzi senza esplicita autorizzazione contrattuale;
- non può effettuare autodialer/robocall in violazione delle normative GDPR e delle Delibere AGCOM;
- deve comunicare tempestivamente l'eventuale indirizzo di installazione diverso da quello dichiarato, per consentire il corretto routing al NUE 112;
- è responsabile della custodia delle credenziali SIP: HyperBit declina ogni responsabilità per traffico fraudolento generato a seguito di compromissione dell'apparato del Cliente. È raccomandato l'uso di password robuste, SIP TLS, blocco delle destinazioni a rischio e limiti di traffico configurabili.

4. Reverse DNS, SWIP e responsabilità sugli IP

I Clienti business possono ricevere blocchi di indirizzi IPv4 e IPv6 da HyperBit. Tali assegnazioni:

- sono non portabili e revocabili in caso di cessazione del contratto;
- sono utilizzabili esclusivamente per la connettività del Cliente assegnatario;

- devono essere documentate con SWIP (Shared WHOIS Information Project) verso RIPE NCC in caso di sub-assegnazione (obbligo del Cliente, supporto da HyperBit);
- non possono essere annunciate via BGP da AS terzi senza preventivo accordo con HyperBit (LOA esplicita).

In caso di abuso documentato originato da un blocco IP assegnato al Cliente, HyperBit si riserva il diritto di revocare l'assegnazione previa diffida.

5. Gestione degli abusi (procedura abuse)

Punto di contatto: segnalazioni di abuso possono essere inviate a abuse@hyperbit.it (indirizzo registrato in WHOIS RIPE NCC per AS208437).

Procedura HyperBit:

1. ricezione e protocollazione della segnalazione (max 4 ore lavorative);
2. analisi tecnica e correlazione con i log di rete (max 24 ore);
3. notifica al Cliente con richiesta di chiarimenti e/o di rimozione (max 24 ore);
4. in caso di gravità o urgenza: sospensione immediata cautelativa del servizio con notifica contestuale al Cliente;
5. in caso di reiterazione o mancata risposta: risoluzione del contratto ex art. 1456 c.c.;
6. trasmissione alle Autorità competenti se richiesto dalla legge (es. abusi su minori → Polizia Postale, ai sensi della L. 38/2006).

HyperBit collabora attivamente con CSIRT Italia (https://csirt.gov.it), Polizia Postale, NoMoreRansom, Shadowserver Foundation e altri enti di cybersecurity per la mitigazione di abusi diffusi.

6. Limiti di traffico e gestione «fair use»

HyperBit non applica limiti di volume sui piani di connettività residenziale e business flat, in conformità con l'obbligo di trasparenza ex Reg. (UE) 2015/2120. Tuttavia, è vietato un uso abusivo della connettività finalizzato a:

- saturazione persistente del link verso destinazioni illecite;
- rivendita non autorizzata di larghezza di banda;
- effettuazione di attività che la presente AUP qualifica come vietate.

Misure tecniche di gestione del traffico ammesse ex Reg. (UE) 2015/2120 art. 3, par. 3:

- mitigation automatica di attacchi DDoS in ingresso (RTBH, BGP FlowSpec);
- blocco di prefissi malevoli notori (botnet C2, ransomware, scam) tramite feed di threat intelligence pubblici (Spamhaus DROP, etc.);
- prioritizzazione di traffico di emergenza (chiamate NUE 112).

Tali misure sono trasparenti, proporzionate e non discriminatorie.

7. Sanzioni per violazione

In caso di violazione della presente AUP, HyperBit può, con effetto immediato:

- richiamare formalmente il Cliente (prima violazione lieve);
- sospendere totalmente o parzialmente il servizio in via cautelativa;

- risolvere il contratto ai sensi dell'art. 1456 c.c. con addebito al Cliente dei costi non ammortizzati e degli eventuali danni;
- trasmettere il caso alle Autorità competenti (Polizia Postale, Autorità Giudiziaria, Garante Privacy);
- in caso di danno diretto a HyperBit o a terzi: richiedere il risarcimento degli importi non coperti dalle eventuali polizze assicurative del Cliente.

La sospensione cautelativa non solleva il Cliente dall'obbligo di corrispondere i canoni maturati fino alla data di risoluzione del contratto.

8. Modifiche all'AUP

HyperBit si riserva il diritto di aggiornare la presente AUP per esigenze normative, tecniche o operative. Le modifiche saranno comunicate al Cliente con almeno 30 giorni di preavviso via email/PEC e pubblicate su https://hyperbit.it/aup. Il Cliente che non accetti le modifiche può recedere dal contratto senza penali entro 60 giorni dalla notifica, ai sensi della Delibera AGCOM 519/15/CONS.

9. Contatti

Segnalazioni abuso: abuse@hyperbit.it
NOC (24/7): noc@hyperbit.it · +39 0461 1819049
SOC (sicurezza): soc@hyperbit.it
Amministrazione: hello@hyperbit.it · cert@pec.hyperbit.it

Documento parte integrante del Contratto. Aggiornato al 26/01/2026 · Rev. 1.0 — 2026 — HyperBit SRLs.