

Policy di utilizzo dei Servizi

Regole di condotta e limiti di utilizzo — documento contrattuale ai sensi dell'art. 2.1 delle Condizioni Generali di Fornitura, Rev. 02 — versione 1.0

Regole di condotta e limiti di utilizzo — documento contrattuale ai sensi dell'art. 2.1 delle Condizioni Generali di Fornitura, Rev. 02

Campo	Valore
Versione	1.0
In vigore dal	6 ottobre 2026
Pubblicato in	https://iweblab.it/policy-di-utilizzo/
Segnalazioni di abuso	abuse@iweblab.it
Punto di contatto per le	iweblabsrl@pec.it
autorità	

La presente Policy integra le Condizioni Generali di Fornitura ("CGF"). La sua violazione legittima iWebLab alla sospensione del Servizio ai sensi dell'art. 16 CGF e costituisce causa di risoluzione ai sensi dell'art. 19.1, lett. c) CGF. In caso di contrasto prevalgono le CGF.

1. Principi generali

Il Cliente utilizza i Servizi nel rispetto della legge, dei diritti dei terzi e della presente Policy. Il Cliente risponde di tutte le attività svolte tramite i Servizi, anche da parte di terzi cui abbia consentito l'accesso o che vi abbiano avuto accesso per effetto di sua negligenza nella custodia delle credenziali. iWebLab non esercita un controllo preventivo generalizzato sui contenuti caricati dal Cliente e non ne ha conoscenza. Sull'infrastruttura operano sistemi automatizzati di rilevamento di codice malevolo e di anomalie tecniche, che non compiono alcuna valutazione sul merito dei contenuti. iWebLab interviene su segnalazione, su ordine dell'autorità o all'esito di tali rilevamenti, secondo la procedura di cui alla sezione 8.

2. Contenuti vietati

È vietato caricare, pubblicare, conservare, trasmettere o rendere accessibili tramite i Servizi:

- contenuti che integrano reato o violano la legge italiana, la legge sammarinese o la legge del luogo di destinazione del Servizio;
- materiale che ritrae abusi su minori in qualsiasi forma: la violazione comporta la cessazione immediata del Servizio e la segnalazione alle autorità competenti, senza preavviso;
- materiale pornografico o a carattere sessuale esplicito, anche ove lecito;

- contenuti che incitano alla violenza, alla guerra, all'odio o alla discriminazione per motivi razziali, etnici, religiosi, di genere, di orientamento sessuale o di disabilità; contenuti di propaganda o apologia del terrorismo;
- contenuti che promuovono o agevolano lo sfruttamento di persone, la tratta di esseri umani, il lavoro forzato o qualsiasi forma di sfruttamento sessuale;
- contenuti che violano diritti d'autore, marchi, brevetti o altri diritti di proprietà intellettuale, ivi compresa la distribuzione di software, chiavi di licenza, contenuti audiovisivi o editoriali privi di autorizzazione;
- contenuti finalizzati alla frode, quali pagine di phishing, siti che imitano soggetti terzi, offerte ingannevoli, farmacie e prodotti sanitari privi delle autorizzazioni di legge, schemi piramidali;
- software malevolo, strumenti di intrusione, exploit e materiale che ne agevola l'impiego contro sistemi di terzi;
- gioco d'azzardo e scommesse privi delle autorizzazioni richieste dalla legge del luogo di destinazione;
- contenuti diffamatori, minacciosi o lesivi della riservatezza di terzi, ivi compresa la pubblicazione non autorizzata di dati personali;
- dati personali appartenenti a categorie particolari ai sensi degli artt. 9 e 10 GDPR, in assenza del preventivo accordo scritto previsto dall'accordo sul trattamento dei dati.

3. Condotte vietate

È vietato utilizzare i Servizi per:

- accedere o tentare di accedere senza autorizzazione a sistemi, reti, account o dati di terzi o di iWebLab, ivi comprese scansioni di porte e vulnerabilità non autorizzate;
- condurre o partecipare ad attacchi di negazione del servizio, o mantenere sistemi che vi partecipino;
- operare proxy aperti, relay aperti, nodi di uscita VPN o Tor, o servizi di anonimizzazione destinati a terzi;
- eseguire attività di estrazione di criptovalute o elaborazioni intensive estranee alla finalità di hosting del Servizio;
- mantenere reti di bot, client IRC automatizzati o processi di controllo remoto di sistemi terzi;
- raccogliere in modo automatizzato indirizzi o dati di terzi senza autorizzazione;
- aggirare i limiti di risorse, le misure di sicurezza o i sistemi di isolamento dell'infrastruttura;
- falsificare intestazioni, identità o origine delle comunicazioni;
- utilizzare i Servizi di hosting condiviso come deposito di file, archivio di backup o distribuzione di contenuti non collegati a un sito web ospitato.

4. Posta elettronica

L'invio di comunicazioni tramite i Servizi è consentito esclusivamente verso destinatari che abbiano prestato consenso o con i quali esista un rapporto che lo legittimi ai sensi della normativa applicabile. In particolare:

- è vietato l'invio di comunicazioni commerciali non sollecitate e l'impiego di elenchi di indirizzi acquistati, noleggiati o raccolti senza consenso;
- ogni comunicazione commerciale deve consentire al destinatario di opporsi a invii successivi con modalità semplici e gratuite, e le richieste in tal senso devono essere onorate senza ritardo;
- i limiti di invio orari e giornalieri sono quelli previsti dal piano attivo, come indicati nelle Specifiche tecniche;

- iWebLab può sospendere temporaneamente la facoltà di invio da un account in presenza di tassi di mancato recapito superiori al 5% o di segnalazioni di abuso superiori allo 0,1% dei messaggi inviati, ovvero in caso di inserimento degli indirizzi di iWebLab in liste di blocco per causa riconducibile al Cliente;
- la configurazione dei record SPF, DKIM e DMARC per i domini del Cliente è a carico del Cliente, con l'assistenza di iWebLab.

5. Uso delle risorse

I limiti di risorse — spazio, traffico, CPU, memoria, processi concorrenti, inode, connessioni, invii di posta — sono quelli previsti dal piano attivo, come indicati nelle Specifiche tecniche del Servizio, e sono applicati mediante meccanismi tecnici di isolamento. Sui servizi di hosting condiviso l'infrastruttura è ripartita fra più Clienti. Al fine di garantire a tutti un livello di servizio uniforme:

- non sono ammessi processi persistenti in esecuzione continua, operazioni pianificate con cadenza inferiore a 5 minuti salvo diversa autorizzazione di iWebLab, o elaborazioni che impegnino le risorse assegnate in modo continuativo;
- iWebLab può limitare temporaneamente le risorse di un account che degradi le prestazioni dell'infrastruttura per altri Clienti, dandone comunicazione al Cliente e indicando le opzioni disponibili, ivi compreso il passaggio a un piano superiore;
- il superamento sistematico dei limiti del piano, dopo comunicazione, legittima la sospensione ai sensi dell'art. 16 CGF.

6. Sicurezza a carico del Cliente

Il Cliente è tenuto a:

- mantenere aggiornati i software, i CMS, i temi e i plugin installati, applicando gli aggiornamenti di sicurezza senza ritardo;
- adottare credenziali robuste, non riutilizzate, e attivare l'autenticazione a più fattori ove disponibile;
- non trasmettere credenziali o chiavi di accesso a webservice in chiaro nelle URL, privilegiando l'autenticazione tramite intestazioni HTTP;
- dare seguito alle segnalazioni di sicurezza di iWebLab entro 72 ore dal ricevimento, rimuovendo le vulnerabilità o i contenuti compromessi indicati;
- non ospitare, nemmeno temporaneamente, file o script di provenienza non verificata.

In caso di compromissione accertata di un account o di un sito, iWebLab può isolare le risorse interessate, disabilitare i componenti compromessi e sospendere l'esecuzione di codice, nella misura necessaria a proteggere l'infrastruttura e gli altri Clienti, dandone comunicazione al Cliente. Il ripristino della piena operatività è subordinato alla rimozione della causa, a cura del Cliente o, su richiesta, mediante il servizio di bonifica di iWebLab, alle condizioni economiche indicate nel Listino prezzi.

7. Protezione dei dati e conformità

Il Cliente, in qualità di titolare o di responsabile del trattamento dei dati personali gestiti tramite i Servizi, è tenuto a rispettare la normativa applicabile, ivi compresi gli obblighi di informativa, di acquisizione delle basi giuridiche e di gestione dei consensi sui siti ospitati. I rapporti fra il Cliente e iWebLab in materia di trattamento dei dati sono disciplinati dall'accordo sul trattamento dei dati personali incorporato nelle CGF. Il Cliente che registri nomi a dominio tramite i Servizi garantisce l'esattezza dei dati di registrazione e si conforma alle regole del Registro competente e, per le estensioni generiche, alle policy ICANN applicabili.

8. Segnalazioni, verifiche e provvedimenti

8.1 Segnalazioni

Chiunque può segnalare a iWebLab, all'indirizzo abuse@iweblab.it, la presenza di contenuti o condotte ritenuti contrari alla legge o alla presente Policy. Per consentire una valutazione, la segnalazione deve indicare: le ragioni per cui il contenuto è ritenuto illecito o vietato; l'indirizzo esatto del contenuto; nome e indirizzo di posta elettronica del segnalante, salvo che si tratti di contenuti relativi ad abusi su minori; una dichiarazione di buona fede circa l'esattezza delle informazioni fornite. iWebLab conferma il ricevimento della segnalazione, la esamina con diligenza e in modo non arbitrario, e comunica al segnalante la decisione assunta.

8.2 Procedura verso il Cliente

Salvi i casi di cui alla sezione 8.3, prima di adottare un provvedimento iWebLab comunica al Cliente la segnalazione o l'anomalia rilevata, assegnando un termine di 48 ore per la rimozione o la regolarizzazione. Decorso inutilmente il termine, iWebLab può rimuovere o rendere inaccessibile il contenuto, ovvero sospendere il Servizio ai sensi dell'art. 16 CGF. Ogni provvedimento restrittivo è comunicato al Cliente con l'indicazione dei fatti, della base contrattuale o normativa, della misura adottata e delle modalità per contestarla. Il Cliente può contestare il provvedimento tramite il sistema di assistenza; iWebLab riesamina la contestazione e comunica l'esito motivato. Resta salva la tutela giurisdizionale.

8.3 Intervento immediato

iWebLab può intervenire senza preavviso, dandone comunicazione al Cliente non appena possibile, quando ricorra una delle seguenti condizioni: ordine di un'autorità competente; contenuti relativi ad abusi su minori o al terrorismo; attività in corso che arrechino danno a terzi o all'infrastruttura, quali attacchi, invio massivo di comunicazioni non sollecitate, distribuzione di software malevolo, phishing; compromissione di sicurezza in atto.

8.4 Autorità

iWebLab dà seguito agli ordini delle autorità competenti nei termini da queste stabiliti e, ove consentito, ne informa il Cliente. iWebLab segnala alle autorità le condotte di cui abbia notizia che integrino reati gravi contro la vita o la sicurezza delle persone.

8.5 Conservazione delle evidenze

In caso di sospensione o rimozione, iWebLab conserva copia dei contenuti e dei log pertinenti per il tempo necessario alla gestione del procedimento e all'adempimento degli obblighi di legge, e comunque non oltre i termini di conservazione previsti dalle CGF.

9. Modifiche

La presente Policy può essere aggiornata secondo la procedura prevista dall'art. 21 CGF. Le versioni precedenti restano consultabili all'indirizzo di pubblicazione, ciascuna con la propria impronta crittografica.