

Acceptable Use Policy (AUP)

This policy forms part of the [Terms of Service](#) and applies to the Subscriber and every User acting under its account. The definitions in the Terms of Service also apply here.

1. Purpose

The Service runs on shared (multi-tenant) infrastructure. This policy sets out the conditions of use that ensure the Service operates securely, reliably and lawfully for every Subscriber.

2. Prohibited activities

The Subscriber and every User acting under its account must not engage in the following activities:

2.1 Unlawful use

- using the Service for an unlawful purpose or in an unlawful manner;
- uploading data that the Subscriber has no appropriate legal basis to process (including the personal data of third parties);
- storing or distributing content that infringes intellectual property rights;
- deliberately recording false billing source data to deceive a third party.

2.2 Acts against system integrity

- attempting to gain unauthorised access to the Service or other subscribers' data, or testing or circumventing tenant isolation;
- circumventing or manipulating security restrictions, access controls, quotas or rate limits;
- uploading or distributing malicious code (viruses, worms or malware);
- reverse engineering or decompiling the Service's source code, copying the Service or creating derivative works, except where expressly permitted by mandatory law;
- conducting load or penetration tests without the Provider's prior written permission.

2.3 Resource abuse

- making automated bulk queries (scraping or crawling) beyond documented API use;
- reselling, renting out or providing the Service as a white-label service without the Provider's written permission;
- using resources in a way that clearly exceeds normal intended use and jeopardises service to other subscribers;
- sending unsolicited messages (spam) through or with the help of the Service.

2.4 Abuse of the public issue-reporting portal (QR)

- submitting automated, bulk or harassing reports;
- circumventing the reporting interface's anti-spam protection (rate limits and deduplication).

2.5 Abuse of the DCA agent (on-site data collector)

- installing the agent or adding a network range (CIDR) on a network that the Subscriber does not have the network owner's permission to scan (see the [DCA Agent Terms](#) for details);
- modifying or reverse engineering the agent, or using it for an undocumented purpose.

3. Consequences

The Provider applies graduated measures proportionate to the seriousness of the breach:

1. **Warning** by email, setting a deadline to remedy the breach;
2. **Restriction:** temporary suspension of the affected feature or account (while preserving stored data);
3. **Immediate suspension** without prior warning if the breach directly endangers the security of the Service, other subscribers' data or the rights of third parties;
4. **Termination with immediate effect** under the Terms of Service in the event of a serious breach of contract.

The Provider notifies the Subscriber of the measure in advance or, in urgent cases, immediately afterwards.

Suspension does not affect the obligation to pay the subscription fee if it results from the Subscriber's breach of contract.

4. Reporting

Suspected abuse can be reported to support@printerms.com. The Provider does not treat a good-faith report of a vulnerability as a breach of this policy (responsible disclosure).