Control-C Acceptable Use Policy

Last updated: March 20, 2025

1. Purpose

This Acceptable Use Policy ("AUP") describes activities that are prohibited when accessing or using the Control-C platform, APIs, integrations, and support resources (collectively, the "Service"). The AUP protects our customers, partners, and global infrastructure. Capitalized terms not defined here have the meaning given in the Terms & Conditions (./terms-and-conditions).

2. Responsible Use Expectations

- Maintain accurate account information and restrict access to authorized Users.
- Configure least-privilege access controls and review entitlements regularly.
- Promptly notify Control-C of suspected security incidents or credential compromise.
- Respect rate limits, API usage guidelines, and integration partner policies.

3. Prohibited Activities

You may not, and must not allow third parties to:

- Upload or transmit malicious code, ransomware, spyware, or other harmful content.
- Probe, scan, or test the vulnerability of the Service without written authorization from Control-C Security.
- Interfere with or disrupt the integrity or performance of the Service, including deliberate load testing that bypasses documented limits.
- Circumvent authentication, access accounts without permission, or share passwords or multi-factor tokens.
- Use the Service to store or distribute content that is unlawful, defamatory, threatening, harassing, exploitative, hateful, or otherwise objectionable.
- Engage in fraudulent activity, including payment fraud, phishing, or misrepresentation of affiliation with Control-C or another entity.
- Upload or process personal data without obtaining required consent or other lawful basis.

- Violate intellectual property rights or encourage others to do so.
- Employ the Service for unsolicited marketing, spam, bulk messaging, or open relay operations.

4. Platform Integrity

Automated scripts, bots, and integrations must comply with documented APIs and security requirements. Unauthenticated scraping, data harvesting, or use of the Service for benchmarking without permission is prohibited. Customers must not mask source identity or traffic origin except through approved methods such as Control-C gateway integrations.

5. Security Research and Testing

Control-C values responsible disclosure. Security testing must be conducted through our coordinated vulnerability disclosure program outlined in the Security Overview (../company/security). Testing outside of approved scope, techniques causing denial-of-service, or exploitation of customer data is strictly prohibited.

6. Compliance

Use of the Service must comply with applicable laws and regulations, including export controls, sanctions, privacy, and employment laws. Customers responsible for regulated workloads (e.g., HIPAA, PCI) must implement supplementary controls described in their governance program.

7. Enforcement

Control-C may investigate violations of this AUP. We may remove content, suspend access, or terminate accounts to protect the Service or comply with legal obligations. Recurring or egregious violations may result in permanent suspension without refund. Control-C may report unlawful activity to appropriate authorities.

8. Reporting Issues

Report suspected violations or abuse to trust@control-c.com. Security issues should be directed to security@control-c.com with supporting evidence. Include relevant timestamps, IP addresses, and logs when available.