Acceptable Use Policy

Extra Special Technologies, Inc. · Version v2026-09-02 · Effective 2026-09-02

Applies to: all use of the ExtraSpecial Service, meaning the platform at `extraspecial.co` and any related applications, APIs, and tooling.

Canonical location of this Acceptable Use Policy: `https://hyperlinked.io/legal/acceptable-use.pdf`

This Acceptable Use Policy ("AUP") sets out the rules that govern your use of the Service. It is incorporated by reference into the Terms of Service by Section 4 of those Terms, which are published at `https://hyperlinked.io/legal/terms.pdf`, and it forms part of the Agreement. Violation of this AUP may result in restriction, suspension, or termination of your account under Section 8 of the Terms of Service, together with any other remedy available under the Terms or applicable law.

1. Prohibited content

You will not use the Service to publish, transmit, store, or link to:

1.1 Content that is unlawful under the laws applicable to you or to us, including, without limitation, content that infringes third-party intellectual-property rights, violates trade-secret protections, or violates export-control or sanctions regulations.

1.2 Child sexual abuse material (CSAM). Any account observed publishing or storing CSAM will be terminated immediately and reported to the National Center for Missing and Exploited Children (NCMEC) and to the relevant law-enforcement authorities.

1.3 Content that promotes or facilitates real-world violence, terrorism, or genocide.

1.4 Content designed to harass, threaten, dox, or stalk an identifiable individual.

1.5 Malware, viruses, worms, ransomware, or any code or links intended to disrupt the integrity of computing systems or networks.

1.6 Phishing, deceptive credential-harvesting, brand-impersonation, or other fraud-furthering content.

1.7 Content that misrepresents you as ExtraSpecial, as our staff, or as one of our service providers.

2. Prohibited activities

You will not:

2.1 Probe, scan, or test the vulnerability of the Service or of any system or network associated with it, except through a coordinated disclosure to `security@extraspecial.co` under the process published at `/.well-known/security.txt`.

2.2 Breach or attempt to breach the authentication or security measures of the Service.

2.3 Interfere with or disrupt the Service or any user's use of it, including by denial-of-service attacks, mass automated requests outside published rate limits, or resource exhaustion.

2.4 Access the Service or its data through automated means in a way that materially exceeds normal interactive use, except through published APIs and within the documented rate limits.

2.5 Reverse-engineer, decompile, or otherwise attempt to derive the source code of any non-open-source component of the Service.

2.6 Use the Service to develop, train, or improve any machine-learning model that competes with the Service.

2.7 Use the Service in a manner that violates the acceptable-use policies of the providers on which the Service depends, currently Amazon Web Services, Stripe, and Google Workspace. Our Subprocessor List, published at `https://hyperlinked.io/legal/subprocessors.pdf`, lists those providers together with the other infrastructure vendors we rely on.

3. Rate limits and resource use

3.1 The Service publishes per-account rate limits for its public APIs. Sustained use exceeding those limits may result in throttling, error responses, or, for repeated abuse, account restriction or suspension.

3.2 If your legitimate use requires higher limits, contact us at `support@extraspecial.co` before pushing past published thresholds.

4. Security and coordinated disclosure

4.1 If you discover a security vulnerability in the Service, **report it to `security@extraspecial.co`** with technical detail sufficient for us to reproduce it. We commit to a 24-hour acknowledgment, a triage assessment within 5 business days, and good-faith collaboration on disclosure timing.

4.2 We do not currently operate a paid bug-bounty program. We will publicly acknowledge contributors who follow coordinated disclosure, with their consent.

4.3 The `/.well-known/security.txt` endpoint on our public hosts is the canonical source for security-contact and reporting information, per RFC 9116 (`https://www.rfc-editor.org/rfc/rfc9116.html`).

5. Reporting abuse

5.1 To report abuse of the Service by another user, including violations of this AUP, email `abuse@extraspecial.co`.

5.2 Include enough detail to identify the offending content, account, or action and the basis for the report. We aim to respond to abuse reports within 5 business days. Confirmed abuse may result in content removal, account restriction, account suspension, or account termination.

6. Consequences

6.1 We may, at our discretion, remove content, restrict or suspend access, or terminate accounts that violate this AUP. For severe or repeated violations, termination is at our sole discretion and without prior notice. Restriction and suspension are governed by Section 8.3 of the Terms of Service, and termination by Section 8.4.

6.2 We reserve the right to report violations to law-enforcement or other relevant authorities where required by law, or where, in our reasonable judgment, the violation poses an imminent risk to safety.

7. Changes to this AUP

We may update this AUP from time to time. The current version is published at `https://hyperlinked.io/legal/acceptable-use.pdf`. ExtraSpecial may publish a clearly identified successor location, and once identified that location is the canonical location.

Each published version carries the version identifier and effective date shown in the document header. Historical versions remain retrievable.

We will communicate material changes by email and through an in-app banner at least 30 days before the effective date.

8. Contact

- Questions about this AUP: `legal@extraspecial.co`
- Abuse reports: `abuse@extraspecial.co`
- Security disclosures: `security@extraspecial.co`, per `/.well-known/security.txt`, with a 24-hour acknowledgment