MARKET RESOURCE

Clear and Precise Usage Policies

How companies can address genuine harm without reserving unlimited discretion over lawful expression.

7-minute read • Market • Updated July 2026

WHY IT MATTERS

Customers, users, sellers, creators, developers, advertisers, nonprofits, and other external stakeholders need to know what conduct may result in content removal or loss of service. Clear rules protect users from arbitrary enforcement, help employees apply policies consistently, and reduce legal, reputational, and operational risk.

The Core Principle

A company may prohibit fraud, credible threats, targeted harassment, exploitation, infringement, and other unlawful or clearly defined harmful conduct. But the rule should identify the conduct and the harm precisely. Users should not have to guess what terms such as "offensive," "inappropriate," "misinformation," or "reputational harm" mean.

A vague term is especially concerning when it can be applied to lawful religious, political, ideological, or social views while comparable expression remains permitted.

What This Resource Covers

This resource applies to operative policies governing a company's core products or services when those policies allow the company to:

- Refuse, suspend, restrict, or terminate access to a product or service;
- Remove, downrank, demonetize, reject, or otherwise suppress user content; and
- Exclude a seller, creator, developer, advertiser, or other external stakeholder.

Relevant sources may include terms of service, acceptable-use policies, community or content standards, seller and advertising rules, deposit or service agreements, end-user license agreements, and any linked enforcement policy incorporated into those documents.

REVIEW THE COMPLETE POLICY SET

Do not stop with the main terms of service. A company may revise its primary agreement while leaving the same language in incorporated community standards, product-specific rules, advertising policies, seller requirements, or enforcement documents.

Two Different Drafting Problems

1. Unclear terms

A term is unclear when an ordinary user cannot determine what it prohibits, or when two reasonable reviewers could apply the same rule differently because the policy lacks objective standards.

QUICK TEST

Could two reasonable reviewers read the same rule and reach opposite conclusions about whether the same lawful statement is allowed? If so, the term may be too unclear.

2. Imprecise terms

A term is imprecise when it may describe a real concern but reaches substantially more speech or conduct than necessary. A rule aimed at fraud, for example, should not sweep in satire, opinion, religious teaching, political advocacy, or a disputed factual claim.

QUICK TEST

Does the rule prohibit a broad category of expression when a narrower conduct-based rule would address the actual harm? If so, the term may be too imprecise.

What Strong Policy Language Looks Like

Stronger approach	Higher-risk approach
Uses words with ordinary, commonly understood meanings.	Relies on undefined labels that users must interpret for themselves.
Targets specific conduct and identifies the resulting harm.	Prohibits broad categories such as “offensive,” “intolerant,” or “controversial.”
Explains who is covered, what evidence is relevant, and what context matters.	Allows enforcement whenever the company believes content creates “brand damage” or “social risk.”
Publishes the operative rules and narrow exceptions.	Reserves the right to act for any reason, at any time, or without notice.

Context Matters

The presence of a particular word does not always determine the result. Some terms may be appropriate when they are defined and limited to a specific commercial, technical, or legal harm.

- “Fraudulent” may be appropriate when limited to intentional material misrepresentation in a transaction.
- “Inaccurate” may be appropriate when referring to incorrect account, billing, or product information.
- “Infringing” may be appropriate when tied to identifiable intellectual-property rights.

Review the substance of the rule, not only the exact words used. Replacing “offensive” with “unwelcome,” “unsuitable,” “contrary to our values,” or “inconsistent with community expectations” does not solve the problem if the substitute remains undefined.

Access Rules and Content Rules

Access to a product or service

Review provisions governing account denial, payment restrictions, seller removal, suspension, termination, or loss of product functionality. The policy should identify the objective condition that justifies the restriction and, where appropriate, provide notice and a reason.

Content restrictions

Review rules governing removal, downranking, demonetization, advertising rejection, visibility limits, and other moderation. The rule should describe observable conduct rather than whether a reviewer agrees with or approves of the speaker's viewpoint.

Before-and-After Examples

Hate speech

Higher risk	Users may not post hate speech or hateful content.
More precise	Users may not direct a credible threat of violence at an identifiable person or group, or repeatedly target an identifiable person with unwanted communications intended to cause substantial disruption.

Misinformation

Higher risk	We may remove misinformation, disinformation, or unsubstantiated claims.
More precise	Do not make a materially false statement in a commercial transaction when the statement is likely to cause financial loss and the speaker knows it is false.

Offensive content

Higher risk	We may remove material we consider inappropriate, objectionable, or offensive.
More precise	Do not post sexually explicit material involving minors, credible threats, or content that unlawfully discloses another person's private identifying information.

Brand or reputational harm

Higher risk	We may terminate service for conduct that creates reputational risk or harms our brand.
More precise	We may restrict service when a user impersonates the company, falsely claims company endorsement, or unlawfully uses company trademarks in a way likely to confuse consumers.

What Unclear Policies Look Like in Practice

The examples below illustrate different drafting risks in policies governing access to core products or services. They do not establish that a company enforced the provision against any particular person or viewpoint.

Apple

View Evidence

POLICY LANGUAGE	“We will reject apps for any content or behavior that we believe is over the line. What line, you ask? ... I’ll know it when I see it.”
HIGH-RISK TERM	“Over the line” and “I’ll know it when I see it”
WHY IT IS UNCLEAR	The policy openly relies on subjective judgment and gives developers no objective way to determine where the boundary lies.
CLEARER APPROACH	Identify the prohibited conduct, the harm it must cause, and the criteria used to decide whether an app violates the rule.

Bank of America

View Evidence View Evidence

POLICY LANGUAGE	The company may suspend or terminate use of a service when it believes, “in our sole discretion,” that the service creates “risk or liability,” and may restrict requests it considers “offensive or unwelcome.”
HIGH-RISK TERM	“Sole discretion,” “risk or liability,” “offensive,” and “unwelcome”
WHY IT IS UNCLEAR	The clause does not define the relevant risk or limit discretion to identifiable legal, security, financial, or contractual concerns.
CLEARER APPROACH	Limit restrictions to defined fraud, unlawful activity, security threats, contractual violations, or measurable financial risk.

DoorDash

View Evidence

POLICY LANGUAGE	User content may not be “false,” “offensive,” “likely to insult or humiliate,” “harm” others, or “reflect negatively on DoorDash.”
HIGH-RISK TERM	“False,” “offensive,” “harm,” and “reflect negatively”
WHY IT IS UNCLEAR	The provision combines truth judgments, subjective offense, emotional reactions, and reputational concerns in a single broad rule.
CLEARER APPROACH	Separate fraud, credible threats, targeted harassment, impersonation, and infringement into distinct conduct-based rules.

Morgan Stanley

View Evidence

POLICY LANGUAGE	A client or transaction may create “Franchise Risk” if it raises “heightened political concerns,” “regulatory sensitivity,” or “may be subject to media scrutiny.”
HIGH-RISK TERM	“Heightened political concerns” and “media scrutiny”
WHY IT IS UNCLEAR	Lawful clients or activities may be treated as risky because they are controversial or attract criticism, rather than because they create a defined business risk.
CLEARER APPROACH	Tie decisions to specified legal, credit, sanctions, compliance, financial, or operational risks, not controversy alone.

VIEWPOINT DIVERSITY SCORE

Toast [View Evidence](#)

POLICY LANGUAGE	"Objectionable Content" includes material that is "objectionable," "inappropriate," "offensive," or "harmful," as determined in the company's sole discretion.
HIGH-RISK TERM	Circular definitions and "sole discretion"
WHY IT IS UNCLEAR	Repeating the disputed word does not define it. The policy appears detailed but still gives users no objective standard.
CLEARER APPROACH	Define each prohibited category through observable conduct, a specific harm, and any necessary exceptions or thresholds.

A Good Definition Should Answer Six Questions

1. What conduct is prohibited?
2. What objective harm must occur or be reasonably likely?
3. Whose conduct and whose rights are covered?
4. What evidence or context will the company consider?
5. What exceptions or safe harbors apply?
6. What enforcement consequence may follow?

A Seven-Step Policy Review

1. Inventory every operative rule. Include the main agreement, incorporated policies, product-specific terms, third-party standards used for enforcement, and unpublished rules that should be made public.

2. Flag subjective or open-ended language. Search for listed terms, synonyms, and equivalent phrases rather than relying on a fixed word list.

3. Identify the actual harm. State precisely what the company is trying to prevent, such as fraud, credible threats, unauthorized access, privacy violations, or infringement.

4. Rewrite around conduct, not viewpoint. Describe observable behavior and avoid rules that turn on whether a reviewer approves of a speaker's beliefs.

5. Add definitions, examples, and limits. Explain what is covered, what is not covered, and when emergency action without advance notice may be necessary.

6. Test for even application. Use comparable scenarios involving competing political, religious, and ideological viewpoints.

7. Publish and maintain the controlling policy. Users should be able to locate the current rules before a dispute occurs, and outdated versions should be clearly superseded.

Common High-Risk Language

The following are representative examples, not an exhaustive list. When used to regulate expression or access to service, these terms often require a narrow definition, objective criteria, and clear limits.

Subjective reactions	Contested truth claims	Ideological judgments	Undefined social standards
Offensive Objectionable Inappropriate Insensitive	Misinformation Disinformation Fake news Unsubstantiated	Extremist Hate group Controversial Brand damaging	Public morals Good taste Public interest Community expectations

A USEFUL DRAFTING RULE

If a policy can reasonably be enforced against lawful religious or political expression merely because the expression is controversial, unpopular, or embarrassing to the company, the policy needs narrower language.

What the Viewpoint Diversity Score Evaluates

The Viewpoint Diversity Score examines policies governing core products and services that authorize a company to restrict service or suppress content. It evaluates whether those policies avoid unclear or imprecise terms that could be used to suppress lawful expression or favor particular viewpoints.

A listed term is not automatically disqualifying in every context. The key question is whether the term is defined and limited so that it cannot reasonably be used to restrict lawful expression, religious exercise, or access to a core product or service because of viewpoint.

Strong policies:

- Publish all operative rules used in enforcement
- Define prohibited conduct objectively
- Limit restrictions to identifiable harms
- Apply comparable rules across viewpoints
- Reserve discretion for narrow, documented circumstances

Source note: Company examples are drawn from current 2026 Viewpoint Diversity Score research records; links lead to the underlying public evidence.

Back to Resources