

ARCHIVED COPY

# Acceptable Use Policy

**Version 1.0** | In force 15 November 2025 to 10 September 2026Source: <https://prduct.com/acceptable-use>Superseded by Acceptable Use Policy v1.1 ([prduct.com/acceptable-use](https://prduct.com/acceptable-use))**SUPERSEDED 10 SEPTEMBER 2026: no longer applies to new acceptances***Last Updated: 15. November 2025*

## 1. PURPOSE

**1.1** This Acceptable Use Policy (AUP) defines permitted and prohibited uses of the Prduct Platform. This AUP is incorporated into and forms part of the Terms of Use ([prduct.com/terms](https://prduct.com/terms)).

**1.2** Violation of this AUP may result in immediate suspension or termination of your access to the Platform.

## 2. PERMITTED USES

**2.1** You may use the Platform for lawful business purposes, including:

- (a) Managing product data and specifications
- (b) Tracking compliance with regulations (EUDR, REACH, etc.)
- (c) Collaborating with suppliers and customers in your supply chain
- (d) Generating compliance reports and analyses
- (e) Integrating the Platform with your own business systems via API (if your subscription permits)

## 3. PROHIBITED ACTIVITIES

**3.1 Illegal Activities.** You may not use the Platform:

- (a) In any manner that violates applicable laws or regulations
- (b) To facilitate illegal activities or transactions
- (c) To violate export control laws or sanctions
- (d) To infringe intellectual property rights
- (e) To violate data protection laws (GDPR, etc.)

**3.2 Security Violations.** You may not:

- (a) Upload malicious code, viruses, worms, trojan horses, or other harmful technology
- (b) Attempt to gain unauthorized access to the Platform, other users' accounts, or our systems
- (c) Interfere with or disrupt the integrity or performance of the Platform
- (d) Attempt to bypass any security measures or authentication mechanisms
- (e) Use automated tools to scrape, harvest, or collect data without authorization
- (f) Probe, scan, or test the vulnerability of the Platform
- (g) Conduct penetration testing without prior written approval

**3.3 Reverse Engineering.** You may not:

- (a) Reverse engineer, decompile, or disassemble the Platform
- (b) Attempt to derive source code or algorithms
- (c) Create derivative works based on the Platform
- (d) Remove or obscure proprietary notices or security features

**3.4 Unauthorized Distribution.** You may not:

- (a) Resell, sublicense, rent, lease, or distribute the Platform
- (b) Provide Platform access to third parties as a service (except as explicitly permitted for suppliers/customers)
- (c) Use the Platform to develop or support a competing product
- (d) Share your login credentials with unauthorized persons

**3.5 Content Violations.** You may not upload or transmit:

- (a) Unlawful, harmful, threatening, abusive, or harassing content
- (b) Defamatory, libelous, or fraudulent content
- (c) Content that infringes intellectual property rights
- (d) Pornographic, obscene, or otherwise inappropriate content
- (e) Spam, junk mail, chain letters, or unsolicited communications
- (f) False or misleading information

**3.6 Resource Abuse.** You may not:

- (a) Use the Platform in a manner that places excessive load on our systems
- (b) Send mass invitations without advance notice (see Section 4)
- (c) Perform bulk operations that disrupt service for other users
- (d) Use automated scripts to generate excessive API calls
- (e) Intentionally consume excessive storage or bandwidth

## **4. SYSTEM LOAD MANAGEMENT**

**4.1 Advance Notice Required.** You must notify us at support@prduct.com at least 48 hours in advance of:

- (a) Sending invitations to 100+ suppliers simultaneously
- (b) Bulk uploading 1,000+ products at once
- (c) Performing bulk updates to 500+ records
- (d) Any other extraordinary system load

**4.2 Purpose.** Advance notice allows us to:

- Allocate additional server resources
- Schedule your activities during off-peak hours
- Prevent service degradation for other users
- Ensure platform stability

**4.3 Failure to Notify.** If you perform high-load activities without notice, we may:

- Temporarily throttle your requests
- Suspend your account temporarily

- Contact you to reschedule the activity

## 5. DATA QUALITY AND ACCURACY

**5.1 Your Responsibility.** You are responsible for ensuring that all data you submit to the Platform is:

- (a) Accurate and truthful
- (b) Complete and up-to-date
- (c) Lawfully obtained
- (d) Authorized for upload (you have rights to the data)

**5.2 Prohibited Data.** You may not upload:

- (a) Knowingly false or misleading product data
- (b) Data that violates confidentiality obligations to third parties
- (c) Personal Data except as permitted by the DPA
- (d) Classified or sensitive government information
- (e) Data obtained through illegal means

**5.3 Personal Data Restrictions.** You must:

- Only upload Personal Data as expressly permitted in our DPA
- Obtain necessary consents before uploading Personal Data
- Comply with GDPR and other data protection laws
- Not upload sensitive Personal Data (health, biometric, etc.) unless explicitly agreed

## 6. ACCOUNT SECURITY OBLIGATIONS

**6.1 Password Security.** You must:

- (a) Use a strong, unique password (minimum 12 characters with mix of letters, numbers, symbols)
- (b) Enable two-factor authentication (2FA) if available
- (c) Never share your password with others
- (d) Change your password immediately if compromised

**6.2 Monitoring Your Account.** You must:

- (a) Monitor your account for unauthorized activity
- (b) Immediately notify us of any security breach at [security@prduct.com](mailto:security@prduct.com)
- (c) Promptly remove access for former employees or contractors

**6.3 Liability for Your Account.** You are responsible for all activities under your account, including activities by:

- Your employees
- Your contractors
- Anyone you've granted access
- Unauthorized users who gained access due to your security failures

## 7. EXAMPLES OF ACCEPTABLE USE

 **Permitted:**

- Uploading your product specifications and compliance data

- Inviting your direct suppliers to share their data
- Generating compliance reports for EUDR, REACH, etc.
- Integrating the Platform with your ERP via API (if your plan permits)
- Sharing relevant product data with your customers
- Conducting internal audits using Platform analytics

## 8. EXAMPLES OF UNACCEPTABLE USE

### Prohibited:

- Uploading competitor's proprietary data without authorization
- Creating fake accounts to test the system
- Using automated bots to scrape product data
- Sending unsolicited marketing emails through the Platform
- Sharing login credentials across multiple users
- Attempting SQL injection or other hacking techniques
- Reselling Platform access to other companies
- Uploading malware or viruses
- Creating accounts under false names
- Using the Platform to build a competing service

## 9. REPORTING VIOLATIONS

**9.1 How to Report.** If you become aware of AUP violations by others, report to:

- **Email:** abuse@prduct.com
- **Subject line:** "AUP Violation Report"
- **Include:** Details of the violation, evidence, dates, affected users

**9.2 We Will Investigate.** We will investigate all reported violations and take appropriate action, which may include:

- Warning the violating user
- Suspending or terminating their account
- Reporting illegal activities to authorities
- Taking legal action if necessary

## 10. CONSEQUENCES OF VIOLATION

**10.1 Enforcement Actions.** If you violate this AUP, we may:

- (a) Issue a warning and require immediate remediation
- (b) Temporarily suspend your access (14 days to cure)
- (c) Permanently terminate your account
- (d) Delete content that violates this AUP
- (e) Report illegal activities to law enforcement
- (f) Pursue legal remedies for damages
- (g) Refuse to provide refunds if terminated for AUP violations

## 10.2 Severity-Based Response:

- **Minor violations:** Warning + 14 days to cure
- **Serious violations:** Immediate suspension + 7 days to cure
- **Critical violations:** Immediate permanent termination (security breaches, illegal activity, malware)

**10.3 No Obligation to Monitor.** We are not obligated to monitor user activity, but we reserve the right to investigate suspected violations.

## 11. COOPERATION WITH AUTHORITIES

**11.1** We will cooperate with law enforcement agencies investigating illegal activities conducted through the Platform.

**11.2** We may disclose user information to authorities when required by law or court order, or when we believe in good faith that such disclosure is necessary to:

- Comply with legal obligations
- Protect our rights or property
- Prevent fraud or illegal activity
- Ensure platform security

## 12. MODIFICATIONS

**12.1** We may update this AUP at any time to address new security threats, legal requirements, or platform changes.

**12.2** Material changes will be notified via email with 30 days' notice.

**12.3** Continued use of the Platform after changes take effect means acceptance.

## 13. CONTACT

Questions or concerns about this AUP?

**General AUP questions:** [support@prduct.com](mailto:support@prduct.com)

**Report violations:** [abuse@prduct.com](mailto:abuse@prduct.com)

**Security issues:** [security@prduct.com](mailto:security@prduct.com)