NETZFABRIK GMBH

System Policies

Stand: November 2026 · NETZFABRIK GmbH, Barthelstraße 4, 50823 Köln

1. Geltungsbereich und Nutzungsregeln

Diese System Policies beschreiben die Betriebs- und Nutzungsregeln für die Dienste der NETZFABRIK GmbH. Sie ergänzen unsere Allgemeinen Geschäftsbedingungen sowie unsere Angaben nach dem Digital Services Act (DSA) und unsere KI-Richtlinien.

Erfasste Dienste

- Cloud Services (Cloud Server, Object Storage, Cloud Backup)
- Managed Hosting (u. a. GitLab, GitLab Runner, Rocket.Chat, Sentry, Tableau, Nextcloud, Zammad)
- Managed Services (u. a. Microsoft 365, Endpoint Security, Cloud PBX, E-Mail-Archivierung)
- Infrastruktur (Colocation, Dedicated Server, DDoS Protection, Domain Reselling)

Allgemein untersagte Nutzung

Für alle Dienste gilt: Untersagt ist jede Nutzung, die gegen geltendes Recht, Rechte Dritter oder diese Regeln verstößt. Dazu gehören insbesondere:

- das Speichern, Bereitstellen oder Verbreiten illegaler Inhalte im Sinne des DSA
- die Verletzung von Urheber-, Marken-, Persönlichkeits- oder sonstigen Schutzrechten Dritter
- der Versand unerwünschter Massen- oder Werbe-E-Mails (Spam) sowie Phishing
- die Verbreitung von Schadsoftware oder Angriffe auf fremde Systeme
- eine übermäßige Ressourcennutzung, die den Betrieb für andere Kunden beeinträchtigt
- das Umgehen von Sicherheits- oder Zugangsbeschränkungen

Bei Verstößen können wir die betroffenen Inhalte oder Dienste im gebotenen Umfang sperren, beschränken oder beenden und, sofern erforderlich, das Vertragsverhältnis kündigen. Meldungen zu rechtswidrigen Inhalten richten Sie bitte an abuse@netzfabrik.com; das weitere Verfahren beschreibt unsere DSA-Seite.

Stand: August 2026. Diese Angaben stellen keine Rechtsberatung dar.

2. Cloud Services

Damit wir für unsere Kunden ein performantes und zuverlässiges Netzwerk betreiben können, sind folgende Aktionen untersagt:

- Der Betrieb von Applikationen zum Mining von Kryptowährungen
- Das Scannen von fremden Netzen oder fremden IP-Adressen
- Die Verwendung von gefakten Source-IPs

3. Dedicated (Dedicated Server)

Damit wir für unsere Kunden ein performantes und zuverlässiges Netzwerk betreiben können, sind folgende Aktionen untersagt:

- Der Betrieb von Applikationen zum Mining von Kryptowährungen
- Das Scannen von fremden Netzen oder fremden IP-Adressen
- Das manuelle Ändern der Hardwareadresse (MAC)
- Die Verwendung von gefakten Source-IPs

4. Managed Hosting

Damit wir für unsere Kunden ein performantes und zuverlässiges Netzwerk betreiben können, sind folgende Aktionen untersagt:

- Der Betrieb von Applikationen zum Mining von Kryptowährungen
- Das Scannen von fremden Netzen oder fremden IP-Adressen
- Das manuelle Ändern der Hardwareadresse (MAC)
- Die Verwendung von gefakten Source-IPs

5. Managed Services

Für Managed Services (u. a. Microsoft 365, Endpoint Security, Cloud PBX, E-Mail-Archivierung) gelten die allgemeinen Nutzungsregeln dieser System Policies sowie die Nutzungsbedingungen der jeweils eingesetzten Hersteller und Plattformen. Untersagt ist insbesondere der Versand unerwünschter Massen- oder Werbe-E-Mails (Spam), Phishing sowie jede Nutzung, die gegen geltendes Recht oder Rechte Dritter verstößt.

6. Colocation

Für Colocation gelten die allgemeinen Nutzungsregeln, die Netzwerkregeln dieser Seite sowie zusätzlich die folgenden Punkte. Sie sichern den Betrieb im Rechenzentrum für alle Kunden ab.

- Es wird ausschließlich betriebssichere, für den Rechenzentrumsbetrieb geeignete Hardware in üblicher Rack-Bauform eingebracht
- Die vereinbarten Grenzen für Höheneinheiten, Anschlüsse und elektrische Leistung sind einzuhalten; Erweiterungen sind vorher abzustimmen
- Der Zutritt erfolgt nur nach vorheriger Anmeldung und nur durch benannte, ausgewiesene Personen unter Beachtung der Hausordnung
- Arbeiten an fremder Hardware, an der Gebäudeinfrastruktur und an der Verkabelung außerhalb des eigenen Racks sind untersagt
- Foto- und Videoaufnahmen im Rechenzentrum sind nur mit vorheriger Zustimmung zulässig

Damit wir für unsere Kunden ein performantes und zuverlässiges Netzwerk betreiben können, sind folgende Aktionen untersagt:

- Der Betrieb von Applikationen zum Mining von Kryptowährungen

- Das Scannen von fremden Netzen oder fremden IP-Adressen
- Das manuelle Ändern der Hardwareadresse (MAC)
- Die Verwendung von gefakten Source-IPs

7. DDoS Protection

Die Filterinfrastruktur schützt den Betrieb aller angeschlossenen Kunden. Damit sie zuverlässig arbeitet, gilt zusätzlich:

- Lasttests, Angriffssimulationen und Penetrationstests gegen die eigene Umgebung sind vorher mit uns abzustimmen
- Das Umgehen oder Deaktivieren von Filterregeln sowie das Verschleiern von Angriffsverkehr sind untersagt
- Der Schutz darf nicht dazu genutzt werden, Dienste zu betreiben, die selbst Angriffe ermöglichen oder verschleiern
- Auffällige Angriffe und Änderungen am Datenverkehrsprofil sind uns zeitnah zu melden, damit wir die Filter anpassen können

8. Domain Reselling

Für Domains gelten zusätzlich die Vergabebedingungen und Richtlinien der jeweiligen Vergabestelle, für .de-Domains die der DENIC eG. Ergänzend gilt:

- Angaben zu Domaininhaber und Kontakten sind vollständig, richtig und aktuell zu halten
- Domains dürfen nicht zur Verletzung von Marken-, Namens- oder sonstigen Rechten Dritter registriert oder genutzt werden
- Untersagt ist die Nutzung für Phishing, Schadsoftware, Betrug oder die Verschleierung solcher Angebote
- Anordnungen und Richtlinien der Vergabestelle, etwa zur Sperrung oder Löschung einer Domain, setzen wir um