Acceptable Use Policy (AUC)

für Hosting-, Domain-, E-Mail-, Server- und IT-Dienstleistungen

Version 1.0
Juni 2026

[~] WDNS.at
KRATOCHWILL – IT Dienstleistungen u. D. V.
Inhaber: Alois Kratochwill
Kieslingerstraße 9/1/4
8430 Kaindorf an der Sulm
Österreich

§ 1 Zweck dieser Richtlinie

1.1 Diese Acceptable Use Policy (AUP) ergänzt die Allgemeinen Nutzungsbedingungen (ANB).

1.2 Ziel dieser Richtlinie ist der Schutz:

- der Infrastruktur des Auftragnehmers,
- anderer Kunden,
- des Internets als Kommunikationsnetz,
- von Rechten Dritter,
- der Verfügbarkeit und Integrität der angebotenen Dienstleistungen.

1.3 Jeder Kunde verpflichtet sich zur Einhaltung dieser Richtlinie.

§ 2 Allgemeine Nutzungspflichten

2.1 Die angebotenen Dienste dürfen ausschließlich für rechtmäßige Zwecke verwendet werden.

2.2 Der Kunde ist für sämtliche über seine Dienste veröffentlichten, gespeicherten oder übertragenen Inhalte verantwortlich.

2.3 Der Kunde hat angemessene technische und organisatorische Maßnahmen zur Absicherung seiner Systeme zu treffen.

§ 3 Verbotene Inhalte

3.1 Die Speicherung, Veröffentlichung oder Verbreitung folgender Inhalte ist untersagt:

rechtswidrige Inhalte,

- strafbare Inhalte,
- betrügerische Inhalte,
- urheberrechtsverletzende Inhalte,
- Inhalte zur Begehung von Straftaten,
- Inhalte mit Schadsoftware,
- Inhalte zur Umgehung gesetzlicher Vorschriften.

§ 4 Spam und unerwünschte Nachrichten

4.1 Verboten ist insbesondere:

- Versand von Spam,
- Versand unverlangter Werbe-E-Mails,
- Massenmailings ohne Einwilligung,
- Nutzung gekaufter Adresslisten,
- Betrieb offener Mail-Relays,
- E-Mail-Bombing,
- Header-Manipulationen,
- Blacklist-Umgehungen

4.2Der Auftragnehmer kann entsprechende Dienste unverzüglich sperren.

§ 5 Phishing und Betrug

5.1 Untersagt sind insbesondere:

- Phishing-Webseiten,
- gefälschte Login-Portale,
- Identitätsdiebstahl,
- Social-Engineering-Kampagnen,
- betrügerische Zahlungsaufforderungen,
- gefälschte Supportangebote

5.2 Eine sofortige Sperre erfolgt ohne Vorankündigung.

§ 6 Schadsoftware

6.1 Verboten sind:

- Viren,
- Trojaner,
- Würmer,
- Ransomware,
- Spyware,
- Keylogger,
- Rootkits,
- Backdoors,
- Command-and-Control-Systeme

6.2 Dies gilt unabhängig davon, ob die Schadsoftware aktiv oder inaktiv eingesetzt wird.

§ 7 Netzwerkmissbrauch

7.1 Untersagt sind insbesondere:

- DDoS-Angriffe,
- DoS-Angriffe,
- Port-Scanning fremder Systeme,
- Schwachstellen-Scans ohne Berechtigung,
- Spoofing,

- ARP-Manipulation,
- DNS-Manipulation,
- Routing-Manipulation.

§ 8 Botnetze und automatisierte Angriffe

8.1 Verboten sind:

- Betrieb von Botnetzen,
- Steuerung von Botnetzen,
- automatisierte Angriffe,
- Credential-Stuffing,
- Brute-Force-Angriffe,
- Passwort-Spraying,
- Account-Hijacking.

§ 9 DNS-Dienste

9.1 Nicht zulässig sind:

- offene Resolver,
- DNS-Amplification-Dienste,
- missbräuchliche DNS-Nutzung,
- DNS-Tunneling zu rechtswidrigen Zwecken.

§ 10 Kryptomining

10.1 Kryptomining ist ausschließlich nach ausdrücklicher schriftlicher Zustimmung zulässig.

10.2 Ohne Zustimmung ist jede Form von Mining untersagt.

10.3 Dies umfasst insbesondere:

- Bitcoin-Mining,
- Monero-Mining,
- Ethereum-Mining,
- Mining-Pools,
- versteckte Mining-Software.

§ 11 Ressourcenmissbrauch

11.1 Der Kunde darf keine Nutzung vornehmen, welche:

- die Infrastruktur beeinträchtigt,
- andere Kunden beeinträchtigt,
- außergewöhnliche Last erzeugt,
- die Systemsicherheit gefährdet.

11.2 Der Auftragnehmer ist berechtigt, technische Maßnahmen zur Lastbegrenzung zu ergreifen.

§ 12 Sicherheitsanforderungen

12.1 Der Kunde verpflichtet sich insbesondere:

- sichere Passwörter einzusetzen,
- Mehrfaktor-Authentifizierung zu nutzen,
- Software aktuell zu halten,
- Sicherheitsupdates zeitnah einzuspielen,
- Zugangsdaten geheim zu halten.

§ 13 Abuse-Meldungen

13.1 Hinweise auf Missbrauch oder Sicherheitsvorfälle werden durch den Auftragnehmer geprüft.

13.2 Der Kunde ist verpflichtet, bei der Aufklärung mitzuwirken.

13.3 Der Kunde hat auf Abuse-Anfragen innerhalb angemessener Frist zu reagieren.

§ 14 Sofortmaßnahmen

14.1 Der Auftragnehmer ist berechtigt, ohne Vorankündigung Maßnahmen zu ergreifen, wenn:

- die Infrastruktur gefährdet wird,
- andere Kunden beeinträchtigt werden,
- gesetzliche Verpflichtungen bestehen,
- akute Sicherheitsrisiken vorliegen.

§ 15 Sperrung von Diensten

15.1 Der Auftragnehmer kann Dienste insbesondere sperren bei:

- Spamversand,
- Malware-Verbreitung,
- Phishing,
- DDoS-Angriffen,
- rechtswidrigen Inhalten,

schwerwiegenden Verstößen gegen diese Richtlinie.

§ 16 Außerordentliche Kündigung

16 .1 Schwerwiegende oder wiederholte Verstöße gegen diese Richtlinie berechtigen den Auftragnehmer zur fristlosen Kündigung des Vertragsverhältnisses.

§ 17 Kostenersatz

17.1 Verursacht ein Kunde durch vertragswidrige Nutzung zusätzliche Aufwendungen, kann der Auftragnehmer die dadurch entstandenen Kosten geltend machen.

Dies umfasst insbesondere:

- Abuse-Bearbeitung,
- Incident Response,
- Blacklist-Entfernungen,
- Wiederherstellungsmaßnahmen,
- externe Dienstleisterkosten.

§ 18 Meldung an Behörden

18.1 Der Auftragnehmer ist berechtigt und gegebenenfalls verpflichtet, rechtswidrige Aktivitäten den zuständigen Behörden zu melden.

§ 19 Schlussbestimmungen

19.1 Diese Acceptable Use Policy ist Bestandteil sämtlicher Verträge über Hosting-, Server-, E-Mail- und IT-Dienstleistungen.

19.2 Ergänzend gelten die Allgemeinen Nutzungsbedingungen sowie gegebenenfalls die Zusatzbedingungen für Unternehmer.

19.3 Es gilt österreichisches Recht.

§ 20. Änderungen

20.1. Chronologische Aufstellung der Änderungen der ANB

2026.06.06 – Initiale Neufassung der Version 1.1,