# Acceptable Use Policy

dnswatchdog.io

This Acceptable Use Policy ('AUP') sets out the rules for using the DNS Watchdog platform and Services. It is designed to keep the platform safe, reliable, and fair for everyone. By using the Services, you agree to follow this policy alongside our Terms and Conditions.

If you have questions about whether a particular use is permitted, please contact us at contact@dnswatchdog.io — we're happy to help.

## 1. Fair Use

DNS Watchdog is designed for businesses to monitor, govern, and secure their DNS portfolio. You are welcome to use the Services for any lawful purpose that falls within the scope of your subscription plan. We ask that you use the platform responsibly and considerately, keeping in mind that the Services are shared infrastructure.

## 2. Your Account

- You are responsible for keeping your account credentials secure. Use a strong password and enable multi-factor authentication where available.
- Do not share your login credentials with others. If you need to grant access to colleagues, use the organisation and team features provided by the platform.
- You are responsible for all activity that occurs under your account. If you suspect unauthorised access, please notify us immediately at contact@dnswatchdog.io.

## 3. Permitted Use

You may use the Services to:

- Monitor and manage DNS records for domains you own or are authorised to manage.
- Connect DNS providers that you have legitimate access to and authority over.
- Run security scans, certificate checks, and other monitoring features against your own infrastructure.
- Export your data for your own business purposes.
- Access the API in accordance with your subscription plan and any applicable rate limits.

## 4. Prohibited Activities

You agree not to use the Services to:

- **Violate any law or regulation**, including data protection, export control, or sanctions laws.
- **Infringe the rights of others**, including intellectual property rights, privacy rights, or contractual rights.
- **Monitor infrastructure you do not own or control**, or for which you do not have explicit authorisation from the owner.
- **Attempt to access other customers' data**, accounts, or resources, or circumvent tenant isolation or access controls.
- **Interfere with the Services**, including by introducing malware, overloading systems, or attempting to disrupt service availability for other users.
- **Reverse engineer, decompile, or disassemble** any part of the Services, except to the extent permitted by applicable law.
- **Scrape, crawl, or systematically extract data** from the Services beyond what is provided through the API and export features.
- **Resell, sublicence, or redistribute** the Services or any data obtained through the Services, unless we have given you written permission.
- **Use the Services for competitive analysis** or to build a competing product or service.
- **Misuse our support channels**, including by submitting false reports or abusing support staff.
- **Send spam or unsolicited communications** using information obtained through the Services.

## 5. Rate Limits and Resource Usage

To keep the platform running smoothly for all customers, we apply fair usage limits including API rate limits and scan frequency limits. These limits are set according to your subscription plan. If you need higher limits for a legitimate use case, please contact us and we will do our best to accommodate you.

Automated access to the Services (for example, through the API or integrations) must respect the published rate limits. Excessive or abusive usage that degrades the experience for other customers may result in temporary throttling or suspension of access.

## 6. DNS Provider Credentials

When you connect a DNS provider to the platform, you entrust us with API credentials for that provider. We take this responsibility seriously:

- We store your provider credentials securely using encrypted storage (AWS SSM Parameter Store with KMS encryption).

- We access your provider credentials only to perform the DNS synchronisation and monitoring operations you have requested.
- You are responsible for ensuring that the credentials you provide have appropriate permissions and that you are authorised to grant us access to the provider account.

For more details on how we handle your data, please see our Data Protection Policy and Privacy Policy.

## 7. Security and Vulnerability Reporting

If you discover a security vulnerability in the DNS Watchdog platform, we would appreciate your help in disclosing it responsibly. Please report any security concerns to security@dnswatchdog.io. We will acknowledge your report promptly and work with you to understand and address the issue.

We ask that you:

- Give us reasonable time to investigate and fix the issue before making any public disclosure.
- Do not access or modify other customers' data as part of your research.
- Do not degrade the availability of the Services for other users.

## 8. Enforcement

We want to work with you, not against you. If we believe your use of the Services may violate this policy, we will generally try to contact you first and give you a reasonable opportunity to address the issue.

However, we reserve the right to take immediate action — including suspending or terminating your access — if we reasonably believe that:

- Your use poses a security risk to the platform or other customers.
- Your use is causing or is likely to cause harm to others.
- We are required to act by law or regulation.
- You are engaging in clearly prohibited activities as described in Section 4.

If your account is suspended, we will notify you of the reason and, where appropriate, provide guidance on how to resolve the issue. Termination of your account for a policy violation is subject to the terms set out in our Terms and Conditions.

## 9. Changes to This Policy

We may update this Acceptable Use Policy from time to time. The 'Last Updated' date at the top of this page indicates when this policy was last revised. We encourage you to review this policy periodically. Continued use of the Services after changes are posted constitutes acceptance of the updated policy.

## 10. Contact Us

If you have questions about this policy or need to report a potential violation, please contact us:

- **Email:** contact@dnswatchdog.io
- **Security issues:** security@dnswatchdog.io
- **Website:** https://dnswatchdog.io