Code of Conduct for Abuse Prevention 2024

Version 2.0 – October 2024

Society must be able to trust that providers of digital infrastructure make efforts to prevent and spread the use of their facilities for unlawful activities, including but not limited to illegal content. To this end, such providers adhere to this Code of Conduct for Abuse Prevention ("Code of Conduct").

For the application of this Code of Conduct, the following definitions apply:

- **Provider:** a natural or legal person who offers or manages digital infrastructure.
- **Digital infrastructure:** internet-connected facilities that facilitate digital online services, in a broad sense, including data centers, hosting and cloud platforms, domains, networks (AS), internet access, as well as all activities classified as mere-conduit or hosting services under the European Digital Services Act (DSA)*
- **Abuse**: The misuse of internet-connected digital infrastructure in its broadest sense; including sending spam or phishing emails, distributing malware, DDoS attacks, operating botnets, running fraudulent websites, storing and distributing CSAM, terrorist content or other illegal content or information that is illegal because it relates to illegal content, products, services or activities, etc. (hereinafter "Abuse"). Abuse includes, at minimum, clearly unlawful activities and anything considered undesirable by the Provider.

** The Digital Services Act (DSA) is a European Union regulation that came into effect in 2024. It creates a comprehensive framework for digital services, setting out clear responsibilities and accountability for providers of intermediary services, particularly online platforms. The DSA aims to create a safer digital space where the fundamental rights of users are protected and establishes a powerful framework for online platform transparency and accountability*

Policy

- Providers are not primarily liable or responsible for the activities of their customers. Nevertheless, they will do everything within their capabilities to combat Abuse.
- Providers implement this Code of Conduct and will clearly communicate this on their website and to their customers and employees.
- Providers maintain an Abuse Policy for their customers and/or service users, which establishes what is expected of them if Abuse is detected in their activities.
- Providers maintain an Acceptable Use Policy for their customers and/or service users, which establishes how their services may be used or for which purposes.
- Providers adhere to the Notice and Take Down Code of Conduct and implement the associated processes in their organization.
- Providers take actual action upon receiving formal orders from authorized authorities regarding illegal content, report back on actions taken to these authorities, and provide information about individual service recipients when legally required.
- Providers implement industry best practices for Abuse prevention appropriate to their activities, services, and role under the DSA, such as the M3AAWG code of conduct for cloud/hosting providers, and make these practices known online to their customers.

- Providers do everything reasonably within their capabilities to reduce the effects of Abuse within their networks and services for other internet users. Autonomous Systems do this by at least implementing the measures described in MANRS.
- Providers implement policies to continuously improve their performance in Abuse prevention.
- Providers implement policies to properly and effectively apply Know Your Customer principles. This means knowing who their customers are, understanding where and how they can be involved in combating Abuse, and doing everything reasonably within their capabilities to ensure they always know who is responsible for their customers' accounts.

Know Your Customer Policy

- Providers implement measures to prevent customers from being unidentifiable.
- Providers implement verification measures to ensure that when a new customer registers, including customers paying with cryptocurrency, successful verification occurs before the first payment.
- Providers implement verification methods including, but not limited to:
    - Personal information
    - Bank details (one-time transfer of 1 cent)
    - Chamber of Commerce details
    - Ultimate Beneficial Ownership (UBO)
    - Legal Entity Identifier (LEI)
    - Identity document authentication

Information

- Providers publish abuse contact details on their website and in relevant whois registrations as required by applicable regulations.
- Providers do everything reasonably within their capabilities to obtain information about vulnerabilities and Abuse in their networks and facilities. They do this by at least subscribing to Abuse feeds, joining Clean Networks, or consulting/connecting to other information sources that provide insight into these matters.
- Providers reasonably accept all Abuse reports received through automated systems and individually composed reports.
- Providers keep informed about their performance in Abuse prevention by consulting available sources.

Notifications

- Providers ensure correct contact information for their customers so that in case of Abuse or suspected Abuse, direct contact can be established with the customer.
- Providers are proactive towards customers; meaning they take action when informed of Abuse in their services.

- For those forms of Abuse where the Provider has become aware of the nature of the Abuse and its continuation would cause serious harm to individuals, they will take immediate measures to prevent or limit further damage.
- Providers commit to suspending services, implementing quarantine measures, or terminating contracts with customers in cases of prolonged, substantial, or repeated violations of the Acceptable Use Policy.

Non-Compliance

- Providers, and thus users of this Code of Conduct, can report reasonable suspicion of non-compliance with this Code of Conduct to (one of the) organizations representing this Code of Conduct.
- Participants in this Code of Conduct will, where possible, refrain from business relationships with organizations known to evidently act in violation of this Code of Conduct, or which can reasonably be considered to intentionally facilitate unlawful activities.

Revision and management

This Code of Conduct for Abuse Prevention will be reviewed annually, based on regulations, feedback, and experiences of the participants in this Code of Conduct. With each revision, the version number will be updated and changes will be documented in the revision history. NBIP is the owner of this Code of Conduct and responsible for version control.

Code of Conduct Representatives

The following organizations have actively contributed to establishing this Code of Conduct:

- Stichting Digitale Infrastructuur Nederland (DINL)
- Dutch Cloud Community (DCC)
- Nationale Beheersorganisatie Internet Providers (NBIP)
- Vereniging van Registrars (VvR)

Code of Conduct Endorsers

The following organizations endorse the principles and objectives of this Code of Conduct for Abuse Prevention and commit to promoting and adhering to these standards:

- Dutch Data Center Association (DDA)
- Anti Abuse Netwerk (AAN)

Revision History

Version 2.0 - October 2024

- Comprehensive revision of the entire Code of Conduct
- Addition of new sections: Know Your Customer Policy, Non-Compliance, and Code of Conduct Endorsers
- Adjustment of definitions and policy to align with recent developments and regulations

Version 1.0 - November 2021

- Initial publication of the Code of Conduct