Code of Conduct for Abuse Prevention 2026

Version 2.1 – July 2026

The Digital Services Act (DSA) places due diligence obligations on providers of intermediary services, such as cloud and hosting companies, to address illegal content, online disinformation and other societal risks. In addition, there are forms of misuse of digital infrastructure that are not covered by the DSA.

Society must be able to trust that providers of digital infrastructure make efforts to prevent the misuse of their services. This Code of Conduct supports providers in preventing and combating such misuse.

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; and all activities classified as mere conduit and hosting services under the DSA.
- **Abuse**: the misuse of internet-connected digital infrastructure in its broadest sense. This includes, among other things, the misuse of vulnerable systems, sending spam or phishing emails, distributing malware, DDoS attacks, running a botnet or fraudulent website, and storing or distributing CSAM, terrorist content or other information that is in violation of the law, for example due to a connection with prohibited content, products, services or activities. Abuse includes, at minimum, manifestly unlawful or criminal activities, as well as conduct that the relevant provider expressly considers undesirable.

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, make this publicly known on their website and communicate this to their customers and employees.
- 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 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 publish abuse contact details on their website and in relevant whois registrations, in accordance with applicable regulations.
- Providers ensure correct contact information for their customers so that in the event of Abuse or suspected Abuse, direct contact can be established with the customer.
- Providers implement industry best practices for Abuse prevention appropriate to their activities and role, such as the M3AAWG code of conduct for cloud/hosting providers, and make these practices publicly known to their customers.
- Providers implement verification measures to ensure customers are identifiable (Know Your Customer (KYC) policy). They implement verification measures to ensure that when a new

customer registers, including customers wishing to pay with cryptocurrency, a successful verification procedure has taken place before the service is delivered, such as, but not limited to: personal details, bank details (one-time transfer of 1 cent), Chamber of Commerce details, Ultimate Beneficial Ownership (UBO), Legal Entity Identifier (LEI), or identity document authentication.

- Providers adhere to the Notice-and-Take-Down Code of Conduct and implement the associated processes in their organization.

Obligations

- 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 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 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.
- Providers take actual action upon receiving a formal order to act regarding illegal content from competent authorities, report back on actions taken to these authorities, and provide information about individual service recipients when legally required.
- A provider that becomes aware of information giving rise to a suspicion that a criminal offence has been committed or is about to be committed, in which the life or safety of a person or persons is threatened, shall immediately notify the law enforcement or judicial authorities of the relevant state or states and provide all available relevant information.
- Providers keep informed about their performance in Abuse prevention by consulting available sources and implement policies to continuously improve their performance in Abuse prevention.

Notices

- For notices regarding unlawful or criminal content, such as defamation, hate speech or copyright infringement, a separate procedure applies as established in the Notice-and-Take-Down Code of Conduct. See: [url]

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 and commit to promoting and adhering to these standards:

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

Revision History

Version 2.1 – July 2026

- Reorganization into Policy and Obligations for improved readability and practical applicability
- Simplification of the Notices section with reference to the Notice-and-Take-Down Code of Conduct

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