



# i2Coalition VPN Trust Initiative (VTI) Principles for Commercial VPN Providers



## About the VPN Trust Initiative (VTI)

The VTI was established in 2019 as an industry-led & member-driven consortium of leading VPN providers focused on educating consumers on the privacy and security benefits of VPN providers, and establishing standard practices for VPN providers that foster trust.

## Introduction

VTI members are united by common principles of privacy and security, and the use of robust secure encryption and VPN protocols. How we implement VPN technology and mitigate risks sets us apart in the industry. Our VTI Principles for Commercial VPN providers sets out the base principles on which our members operate to ensure consumer trust and accountability. We encourage and champion members to go beyond these essentials, but it is important to establish a clear foundation of best practices for the VPN industry.

## Purpose of the Principles Document

These principles offer a framework for the development of a comprehensive set of voluntary best practices for VPN providers. The framework was developed by the VTI and the i2Coalition through a collaborative process, but it has also been informed by input from civil society and other outside experts. The goal of these Principles is to set forth best practices that meaningfully protect the privacy and security of individuals using VPN technologies; that offer practical and policy guidelines for VPN providers; and that provide policymakers, regulators, and civil society with realistic benchmarks for evaluating these technologies.



# Key Principles

This principles document focuses on five key areas:

1. **Security**
2. **Privacy**
3. **Advertising Practices**
4. **Disclosure and Transparency**
5. **Social Responsibility**

## 1. Security

VTI members use the necessary security measures and protocols to appropriately address the risks. Members are not prescribed specific technologies since the threat landscape is subject to change and innovation may produce new, more effective technologies.

The guidelines we set forth apply to various security scenarios.

- **Strong encryption and authentication protocols:** VPN providers should have reasonable transparency to users around what types of strong encryption and authentication protocols are used. VPN providers should use token-based authentication when possible, and never use plain text usernames and passwords. VPN providers should take measures to ensure that keys are unique for each account. VPN providers should be able to explain the privacy and security impact of different protocols to users upon request.
- **Suspension, revocation, or destruction of tokens relating to a compromised account** should occur as promptly as practical following a security incident.
- **Proactive measures to detect problems:** VPN providers will take the means deemed necessary to detect problems ranging from security audits and penetration tests to “bug bounty” programs that encourage security researchers to identify and report potential vulnerabilities. VPN providers should commit to regular security audits to identify new and emerging security vulnerabilities including those relating to new features<sup>1</sup>, as well as out-of-sync security audits when deemed necessary. The results of these audits should be released publicly to the extent that would not undermine user privacy or security, and include information such as the name of the auditor(s) personnel, the name of their firm,

---

<sup>1</sup> For instance, new features that address issues such as IPv6 and UDP traffic must assess relevant user information concerns.



the expertise of the auditor(s); the scope of the audit; and any limitations placed on auditors.<sup>2</sup>

## 2. Privacy

A VPN service should protect users' online privacy throughout all aspects of the VPN service.

- **Explain logging practices:** Service providers will say what connection logs they keep, why they keep them, and how long they keep them.
- **Keep only necessary data:** VPN providers will keep as little data as they deem necessary to provide the service, and only produce data to law enforcement when legally required.
- **Make disclosure and transparency commonplace:** VPN providers will be transparent about what legal jurisdiction they operate in, and where extra-jurisdictional considerations apply such as the case of GDPR. When aware of instances where data is disclosed, VPN providers will be transparent with the affected client(s). VPN providers will explain data storage and data retention, and commit to notify users of a potential data breach or security incident within a reasonable timeframe. If user information is shared for reasons other than for providing the service, network management and analytics, and for billing or payment reasons, provide an explanation.
- **VPN providers should ensure private keys are not shared:** User-level authentication is important in ensuring users are able to manage their privacy.
- **Specifically describe stealth features:** “Stealth” typically refers to methods of disguising or obfuscating VPN traffic as regular web traffic. If a specific “stealth mode” or “stealth VPN” is offered as an additional service or in the core service, provide specific information on what protection is offered.
- **Allow random token or number-based IDs:** Allow users to be identified internally using tokenized or number-based accounts to protect their personal identity.
- **Provide mechanisms for anonymous payment:** When possible, allow for payment through cash, cryptocurrencies (such as Monero or Zcash privacy mode) and other mechanisms to help users obscure their relationship with a VPN provider.
- **Explain handling of IP addresses:** Explain where IP addresses related to users are used and what information is associated with other technical identifiers (e.g. a user session token).
- **Provide detailed privacy information and assurances tailored to vulnerable users:** Provide explicit information around collection and use of both identifiers and quasi-identifiers. This is especially relevant for VPN users with particularly sensitive

---

<sup>2</sup> It is common practice to discuss with auditors beforehand what areas would be subject to disclosure. Another common practice is performing an audit, then fixing the discovered vulnerabilities, then performing another audit only to publish the second one. The report must provide the full scope and context of the audit including the disclosure of these sorts of practices.



threat models such as journalists and activists, but also for anyone who self-identifies as vulnerable.

- **Explain limits to anonymity:** Do not claim VPN providers guarantee anonymity. VPN providers provide privacy, but cannot ensure complete anonymity because other user behaviour could give hints or reveal the user's identity.<sup>3</sup>

### 3. Advertising Practices

To help ensure clear understanding of the functionality of VPN providers and what expectations individuals should have from providers, it's important to establish norms around VPN advertising practices.

- **Accurate marketing claims:** Ensure that prominent advertising and marketing claims are not misaligned with privacy disclosures and terms of use.
- **Clear and transparent language:** Clearly present accurate claims about privacy and security practices in ways that are understandable and not hidden in legalese and/or technical jargon.
- **Affiliate programs:** Monitor and ensure compliance with affiliate program terms. Additionally, a VPN affiliate program must be clearly and conspicuously disclosed to users and terms be made publicly accessible to both users and potential affiliates in line with the U.S. Federal Trade Commission's Guides Concerning the Use of Endorsements and Testimonials in Advertising or locally relevant regulations and guidelines.
- **Explain limits to anonymity:** As mentioned in the Privacy section, do not claim VPN providers guarantee anonymity. VPN providers provide privacy, but cannot ensure complete anonymity because other user behaviour could give hints or reveal the user's identity.

### 4. Disclosure and Transparency

In order to drive trust, member companies must take steps towards informing users and the public about their actions and procedures.

- **Adherence to Generally Accepted Data Privacy Regulations:** Abide by the disclosure and transparency guidelines set out in the data privacy regulations in jurisdictions that a VPN provider operates in at minimum. This includes but is not limited to the guidelines set out in the General Data Protection Regulation (GDPR).
- **Disclosure of how data is used across all business units and with third-parties:** VPN providers will provide transparency into how customer data is used in relation to their business model and operations, and if/how information is used between business units or brands and/or third-parties.

---

<sup>3</sup> user identity could be revealed through online activity by means of cookies, login details, browser fingerprints, session data, and other indicators.



- **Business model transparency:** The VPN will provide transparency around its own business which can include information about but is not limited to: location of data center(s), place of incorporation/governing law, financial stakeholders and/or corporate owners, separate product lines or brand names, and names of third-party service providers.
- **Use of advertising identifiers:** Disclose if advertising identifiers, e.g., UDIDs, mobile device identifiers, or other pseudointifiers are collected, used, or shared in any way.
- **Abide by valid legal requests and no more:** Specify clear processes for how requests for information from public authorities, courts, and parties in litigation are conducted. Processes should include:
  - Process for handling law enforcement requests for data.
  - Process for handling civil requests for data.
  - Process for handling copyright<sup>4</sup> and/or other abuse complaints.
- **Transparency reporting:** Providers should, to the extent possible, disclose the number of government requests for information via search warrants, subpoenas, and other court orders. This may include publishing annual transparency reports.
- **Third-party server providers:** If servers are operated by a third-party, the provider should contractually place and disclose limits on access to user information. It is unnecessary, but encouraged to disclose information about ownership, control, and physical location of DNS servers.
- **Special DNS services:** Disclose the use of any special DNS services such as any DNS-level filtering or error responses (e.g., DNS typo assistance, DNS RPZ).
- **Help users avoid security issues:** Provide users with information that will help them further secure their DNS queries and/or avoid DNS leaks while using the VPN service, including providing user-specified DNS entries, and the potential consequences of changing the default DNS settings.
- **IP addresses:** Disclose if/how IP addresses are collected, used, stored, and/or shared.

## 5. Social Responsibility

VPN providers provide greater security and privacy, which is a social good that is vitally important to those who are trying to make the digital sphere a better place. These individuals' Internet activities could lead to unwanted and potentially dangerous surveillance. In this regard, VPN providers have particular social responsibilities to break down barriers towards the use of these technologies.

---

<sup>4</sup> The relevant copyright laws for the jurisdiction such as the US Digital Millennium Copyright Act (DMCA)



- **Provide education:** VPN providers should support public education around VPN providers with truthful and honest information. Promote VPN best practices to technology providers beyond the VTI with a spirit of collaboration and education.
- **Contribute to VPN technology:** VPN providers will contribute to the advancement of VPN technology. This can be done by contributing to open source projects; and helping establish business ethics around VPN providers through public comments and industry forums.
- **Support freedom of expression:** When possible, VPN providers will promote freedom of expression through technology.



## Appendix A: Definitions

**Analytics:** Aside from using aggregate information to track and understand user behavior on a VPN provider's website, analysis of logging data/connection logs exclusively for service improvement.

**Independent Security Audit:** An audit conducted by an individual or organization that may be directed in scope but should entail complete access to the VPN provider's systems and code. Compensation should be limited to usual and customary fees. The audit (and auditor) must be made public within a reasonable time of the audit.

**Logging / Connection Logs:** Data collected at the time a connection is established or during a session that is retained for X period by any party, including dates and timestamps corresponding to each user's VPN session duration, amount of data transferred, and incoming and outgoing IP addresses.

**Virtual Private Network:** A virtual network that is built on top of existing networks that can provide a secure communications mechanism for data and IP information transmitted between networks. [Wikipedia Definition: A virtual private network (VPN) extends a private network across a public network, and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Applications running across the VPN may therefore benefit from the functionality, security, and management of the private network.]

**VPN Provider:** An individual or organization that offers a commercial VPN service to individual users as a method to protect for safeguarding their privacy and security against other internet service providers and the VPN provider itself.