eduVPN compliance statement

This document outlines the minimum technical and organisational standards for eduVPN National Organisations (eduVPN NOs) and eduVPN Instance Operators (eduVPN IOs) to provide the **eduVPN service**.

It is necessary to comply with this document to appear in the eduVPN apps.

The technical governance of the eduVPN software lies in the Commons Conservancy. https://dracc.commonsconservancy.org/0018/

This document is subject to change by the Global eduVPN governance committee (Gegoc), based on feedback from operators or individual eduVPN users

Any feedback regarding this document should be directed to <eduvpn-support@lists.geant.org**> for consideration.**

In case of a dispute regarding the status of an entity (eduVPN IO, eduVPN NO) in the eduVPN service that cannot be resolved by the responsible eduVPN NO (first instance) or the Gegoc (second instance), the GÉANT General Assembly will give the final ruling.

1. Terminology

1.1. eduVPN

eduVPN is a federated VPN service that provides privacy and security enhancing access to the Internet by authenticating a user with their own credentials issued by their Identity Provider (IdP).

eduVPN can also be used for creating a secure and trusted path into the institution network/datacenter in order to provide secure access to internal services. For this specific use case only items 3.1 till 3.5 are relevant.

1.2. Guest access

Guest access is the situation in which the eIO or eNO lets users from a different country use their instance of eduVPN to access the Internet.

1.3. eduVPN instance

A server or a set of servers running the eduVPN software.

1.4. eduVPN instance operator (eIO)
An entity that is responsible for running an eduVPN instance.

1.5. eduVPN national operator (eNO)
An entity that is responsible for ensuring the eduVPN service operation within a particular country. In many cases the eduVPN national operator is also an eduVPN instance operator.

1.6. Gegoc
The Gegoc is an instance composed of 5 members designated by the eNOs for a period of 2 years. It is responsible for defining the global service framework.

2. User identification process
2.1. eduVPN uses national research and education identity federations (and eduGAIN). eduVPN instances are Service Providers in identity federations.

2.2 Respect user privacy: eduVPN instance operators must only ask for minimal information about end users and always choose privacy preserving attributes where possible. eIOs shall not communicate any attribute/identifier that could be directly linked to a person without the help of their Identity Provider.

2.3 Logging users and sessions is only allowed for a period of 30 days unless there is a documented legal reason to do otherwise. eIOs may log user ID (usually a pseudonym), time of client connect, time of client disconnect, issued VPN IP address.

2.4 Every eIO must publish a privacy statement describing precisely what is logged and in which conditions.

3. Security and incident response compliance for eduVPN instance operators

3.1 Information
The eduVPN mailing list: eduvpn-deploy@list.surfnet.nl is the main channel of communication about the service and its requirements: security, upgrades, policies, inter alia. At least one person from the eduVPN instance operator organisation has to subscribe to the mailing list of eduVPN.

3.2 Software updates

eIO have to keep their instance of eduVPN software up to date. Updates have to be applied within two weeks of their release or following the best practice of the eIO organisation (whichever is the shortest).

Operators SHOULD be available for coordinated installation of updates, i.e. on the same date/time in case of certain updates that may otherwise break “guest access”, or for security reasons. These coordinated updates will be scheduled at least 2 weeks in advance, unless they are critical security updates.

3.3 Security of the instance

Security patches in operating system and application software must be applied within two weeks of their release.
A process must be used to manage vulnerabilities in software operated by the organisation.
Mechanisms must be deployed to detect possible intrusions and protect information systems from significant and immediate threats.
A user’s access rights can be suspended, modified or terminated in a timely manner.
Security incident response capability must exist within the organisation with sufficient authority to mitigate, contain the spread of, and remediate the effects of a security incident.

3.4 Incident response

eIOs must provide security incident response contact information.
eIOS must respond to requests for assistance with a security incident from other organisations participating in the eduVPN service in a timely manner.

3.5 Security of the user

eduVPN instance operators have to prioritise end-user security and privacy in their implementation choices. They should at least offer offer one VPN profile that routes all connected users’ traffic through the VPN. The VPN must give access to the public Internet.

3.6 Filtering

The eIO can restrict access to content or services. These restrictions can be named “filtering” or “blocking” [as defined in RFC 7754]. The purpose of the filtering has to be as explicit as possible (security reasons, legal reasons) and must be published on the eduVPN.org website.

3.7 Guest access

eIOs should allow guest access on their eduVPN instance for users from other countries. If they do not allow guest access, it has to be clearly stated.

4. Administrative and technology compliance for eduVPN national operators (eNO)

4.1 The eduVPN national operator is responsible for ensuring the eduVPN service operation within a particular country, region or economy.

4.2 The eNO has the authority to determine the eligibility of IdPs to connect to eduVPN, being organisations engaged in research and/or education, in its country, region or economy.

4.3 The eNO has the authority to determine the eligibility of eduVPN instance in its country , region or economy. There are no restrictions for the eligibility of eduVPN instances as long as the **Security and incident response requirements for eduVPN instance operators** are met.

4.4 The eNO can be an eduVPN instance operator.

4.5 The eNO must establish communication channels to all other eNO.

4.6 The eNO should publish information about the available eduVPN instances in its country, region or economy in an adequate manner defined by the global eduVPN committee.

4.7 The eNO must establish communication channels to the eduVPN instance operators in its country, region or economy to be able to communicate changes in requirements and resolve problems.

4.8. The eNO must publish information about eduVPN service on dedicated web pages containing the following minimum information:

> **4.8.1.** Text that confirms adherence (including a url link) to eduVPN policy (if applicable);
>
> **4.8.2.** The contact details of the appropriate technical support that is responsible for eduVPN service and mailing list(s).

4.9. The eNO must make sure that the eIOs in its country, region or economy comply with the requirements expressed in this document.

By signing this document, an eIO or eNO unilaterally declares to implement and adhere to the rules set forth herein. By signing this document, an eNO commits to ensure that the eduVPN eIOs in its country, region or economy implement and adhere to the rules set forth herein.

Failure to adhere may result in the removal of an entity's recognition as an eNO or eIO, including removal of the right to use the eduVPN name, logo and trademark.

Acting as eIO/eNO for: Signed by: Signature:
(country, region or economy / multiple of) (Name of eIO/eNO)