POLICY WHISTLEBLOWING

NOTIFICATION WHISTLEBLOWING

In accordance with Legislative Decree 24/2023 regarding Whistleblowing, Fusel has established channels for reporting any company misconduct and irregularities.
Fusel aims to maintain an environment where open and honest communication is the norm rather than the exception, with the desire that all employees and collaborators feel comfortable asking questions or expressing doubts when they believe possible violations have occurred.
The term "Whistleblowing" refers to reporting as an expression of civic duty, which helps to uncover and prevent situations that undermine good administration or public interest.
Anyone aware of irregularities that could involve violations and/or misconduct can make a Whistleblowing report.
Fusel guarantees the confidentiality and anonymity of those who wish to make a report and the information provided in accordance with the law.

REPORTING CHANNELS

The channels for making a report are as follows:

- Through the Signalethic portal at the link https://fusel.signalethic.it/signalethic/home
- By contacting the Reporting Manager at the contact details provided below;
- In the dedicated section of the ANAC website https://whistleblowing.anticorruzione.it/#/

Please note that Whistleblowing reporting channels are not appropriate for handling personal matters or issues related to employment contracts, relationships with supervisors, or other colleagues not falling within violations of the Ethical Code or Legislative Decree 24/2023.
The Whistleblowing Reporting Manager for Fusel is:

DOCUVERSE - VAT Number/Tax Code 04385230240, with legal headquarters in Vicenza (36100), Via dell'Edilizia 11 - PEC docuverse@pec.it - +39 0444 419325

TIPS FOR ANONYMITY

Signalethic has been designed following the principles of privacy and security by design and by default, integrating GDPR requirements into software development and by default settings from the design stage.
Traffic to the Signalethic portal is encrypted in transit, while data stored on the platform is encrypted at rest (or in the database).
To protect *reports:*

- Use private devices that you control to make reports or to access reports already made;
- Use private browsing if possible;
- Store credentials in secure locations where there is no risk of sharing them with anyone;
- Ensure reports are not made or the Signalethic portal is not accessed in public or in places where screen activity can be seen by others;
- Access the Signalethic portal only through a secure internet connection and a private network to protect internet traffic before it reaches the platform.