# Vulnerability Disclosure Policy (VDP)

Tödi AG welcomes reports of security vulnerabilities from public sources, including researchers, bug bounty hunters, and IT experts.
Tödi AG is particularly interested in issues affecting the confidentiality, integrity, or availability of user data or our services.
Tödi AG highly values the contributions of the security community and appreciates your efforts to help strengthen our systems.

## SCOPE

- Any public-facing surfaces
- Any of our services

## LEGAL

Tödi AG will not take legal action against activities aimed at improving our systems, provided they comply with this policy. If a third party initiates legal action against you, Tödi AG will take measures to prevent further processing, as long as your activities comply with our policies and do not cause harm.

## HOW TO REPORT VULNERABILITIES

To report a vulnerability to Tödi AG, please use one of the following methods:

1. Submit the form available on the page https://eliohz.com/awareness/toedi-vdr-froms.html
2. Send an email to security@toedi.com

Tödi AG expects vulnerability reports to include the following:

1. The report must be written in either English or German
2. A clear description of the vulnerability or bug
3. A proof of concept (PoC)
4. Please do not submit reports based on automated tools or publicly known vulnerabilities
5. Ensure your actions comply with our policy to avoid any legal consequences

## WHAT TÖDI AG WILL DO

Tödi AG will:

1. Respond within seven days
2. Engage in an open dialogue to confirm the vulnerability or bug
3. Provide an expected timeline for patches within 180 days

## PREFERENCE

Tödi AG does not permit:

- Any actions that compromise the confidentiality, integrity, or availability of data or systems
- Social engineering targeting our employees or customers
- The use of automated tools or auto-generated reports

In the event of violations of our guidelines, Tödi AG will take legal action in accordance with Swiss law.