

RESPONSIBLE REPORTING OF SECURITY VULNERABILITIES

# Found a vulnerability? Report it responsibly.

How to report suspected security vulnerabilities in ITO products, services and digital infrastructure.

| DOCUMENT ID       | VERSION | CLASSIFICATION | DOCUMENT OWNER       | REVIEW CYCLE | EFFECTIVE    |
|-------------------|---------|----------------|----------------------|--------------|--------------|
| ITO-TRUST-VDP-001 | 1.0     | PUBLIC         | Information Security | Annual       | October 2026 |

# A clear channel for security reports

ITO is committed to maintaining the security of its software products, services and digital infrastructure.

Despite careful engineering, security testing and ongoing maintenance, vulnerabilities may still be discovered.

We value responsible security research and encourage security researchers, customers, partners and other parties to report suspected security vulnerabilities to ITO through the process described in this policy.

Our objective is to provide a **clear and responsible channel** for reporting potential security issues so they can be investigated and, where necessary, remediated.

## AT A GLANCE

REPORT TO

**security@ito.dev**

SUBJECT LINE

**SECURITY VULNERABILITY REPORT**

CUSTOMER SYSTEMS

**Not authorised for testing**

PROGRAMME TYPE

**Disclosure programme, not bug bounty**

| CONTENTS |                          |    |
|----------|--------------------------|----|
| 01       | Purpose                  | 02 |
| 02       | How to report            | 03 |
| 03       | Scope                    | 04 |
| 04       | Responsible research     | 05 |
| 05       | Activities not permitted | 05 |
| 06       | After a report           | 06 |
| 07       | Response times           | 06 |
| 08       | Coordinated disclosure   | 07 |
| 09       | Customer environments    | 07 |
| 10       | Third-party technologies | 08 |
| 11       | Privacy of reports       | 08 |
| 12       | Recognition              | 08 |
| 13       | Contact                  | 09 |

## DOCUMENT CONTROL

|                |                      |
|----------------|----------------------|
| DOCUMENT ID    | ITO-TRUST-VDP-001    |
| VERSION        | 1.0                  |
| CLASSIFICATION | PUBLIC               |
| OWNER          | Information Security |
| REVIEW CYCLE   | Annual               |
| EFFECTIVE DATE | October 2026         |

# Send your report to the security team

REPORT SUSPECTED SECURITY VULNERABILITIES TO

**security@ito.dev**

SUBJECT LINE, WHERE POSSIBLE    **SECURITY VULNERABILITY REPORT**

## Information to include

To help us understand and investigate a report, please provide as much relevant information as reasonably possible, including:

01

The affected product, service or URL

02

A description of the suspected vulnerability

03

Steps required to reproduce the issue

04

Potential security impact

05

Relevant screenshots, logs or technical information

06

Any proof-of-concept material necessary to understand the issue



Please avoid including personal, confidential or operationally sensitive information unless it is necessary to explain the vulnerability.

## Systems covered by this policy

This policy applies to ITO-owned and ITO-operated publicly accessible systems that are explicitly identified as being within the scope of this vulnerability disclosure programme.

### IN SCOPE FOR AUTHORISED TESTING

#### Explicitly identified ITO systems

ITO-owned and ITO-operated publicly accessible systems that are explicitly identified as being within the scope of this programme.

### NOT AUTOMATICALLY IN SCOPE

#### ITO software in customer environments

ITO software deployed within customer-controlled environments is not automatically included within the scope of authorised security testing under this policy.

Security issues identified in ITO products deployed within customer environments may still be reported to ITO, but researchers must not perform testing against customer systems without explicit authorisation from the organisation responsible for those systems.



**This policy does not grant permission to test systems operated by ITO customers.**

# Act responsibly and in good faith

## WHEN INVESTIGATING, PLEASE

- ✓ Avoid accessing information beyond what is reasonably necessary to demonstrate the issue
- ✓ Avoid modifying or deleting information
- ✓ Avoid disrupting systems or services
- ✓ Avoid degrading system availability or performance
- ✓ Avoid accessing accounts belonging to other users
- ✓ Avoid social engineering, phishing or physical security testing
- ✓ Stop testing if sensitive, personal or operational information is unintentionally accessed
- ✓ Report the vulnerability to ITO as soon as reasonably possible

The objective should be to demonstrate the existence of a potential vulnerability with the **minimum necessary interaction** with the affected system.

## RESEARCHERS MUST NOT INTENTIONALLY PERFORM

- ✗ Denial-of-service or resource-exhaustion attacks
- ✗ Destructive testing
- ✗ Malware deployment
- ✗ Social engineering
- ✗ Phishing
- ✗ Credential theft
- ✗ Physical intrusion
- ✗ Intentional access to third-party accounts
- ✗ Unnecessary extraction of data
- ✗ Modification or deletion of production information
- ✗ Testing of customer infrastructure without authorisation

Automated vulnerability scanning that creates significant traffic, service degradation or operational risk is also outside the intended scope of this policy.

# Our process

When ITO receives a vulnerability report, our process may include:



ITO WILL MAKE REASONABLE EFFORTS TO



# Prioritised by severity and impact



## Disclose together, not prematurely

We ask researchers not to publicly disclose vulnerability details before ITO has had a reasonable opportunity to investigate and, where necessary, develop and distribute appropriate remediation.

ITO supports responsible and coordinated vulnerability disclosure intended to protect affected users and organisations while recognising the contribution of legitimate security research.

Where appropriate and agreed with the researcher, ITO may publicly acknowledge individuals who responsibly report security vulnerabilities.

## 09 • CUSTOMER ENVIRONMENTS

### Customer systems require customer authorisation

ITO technology may be deployed within infrastructure owned or operated by government institutions, public safety organisations and other customers.



**This policy does not provide authorisation to access, scan, probe, test or otherwise interact with those environments.**

#### YOU MAY

Report a potential vulnerability in an ITO product to ITO, if it was identified without conducting unauthorised testing.

#### AUTHORISATION REQUIRED

Where investigation requires interaction with a customer-controlled environment, appropriate authorisation must be obtained from the responsible organisation.

## Vulnerabilities in third-party products

ITO products may integrate or depend on technologies provided by third parties. If a reported vulnerability originates within a third-party product, ITO may coordinate with the relevant provider where appropriate. Researchers may also need to follow the vulnerability disclosure process established by the responsible third-party vendor.

ITO cannot grant authorisation to test systems or technologies that it does not own or control.

## How report information is handled

### PURPOSE

Information submitted will be handled for the purpose of investigating and responding to the reported security issue.

### MINIMISE

Researchers should avoid submitting unnecessary personal information or third-party confidential data.

### COORDINATION

Where investigation requires coordination with affected customers or technology providers, relevant technical information may need to be shared with those parties.

## A disclosure programme, not a bug bounty

### NOT A BUG BOUNTY

This policy is a vulnerability disclosure programme and does not constitute a bug bounty programme. ITO does not guarantee financial compensation for submitted vulnerability reports unless explicitly agreed otherwise.

### RECOGNITION

Where appropriate, and with the researcher's consent, ITO may recognise responsible contributions publicly.



13 • CONTACT

# Report a security vulnerability.

SECURITY CONTACT

**security@ito.dev**

SUBJECT LINE, WHERE POSSIBLE **SECURITY VULNERABILITY REPORT**

For general support issues, product questions or non-security matters, please use the appropriate ITO support channel rather than the vulnerability reporting address.

DOCUMENT

Responsible Vulnerability Disclosure Policy

ID • VERSION • CLASSIFICATION

ITO-TRUST-VDP-001 • 1.0 • PUBLIC

OWNER • REVIEW • EFFECTIVE

Information Security • Annual • October 2026

TRUST CENTER

[ito.dev/en/trust-center](https://ito.dev/en/trust-center)

COMPANY

IT Odjel Mostar d.o.o., Mostar, Bosnia and Herzegovina