Vulnerability Disclosure Policy (VDP)

Version	1.1
Owner	CISO
Last updated	16.03.2026
Change log	1.0 - First publication

1. Purpose and Scope

ITX Norge AS (ITX) is committed to maintaining the security of its systems and data. We encourage reports from security researchers, customers, partners, and members of the public who identify potential vulnerabilities in our products and services.

This Vulnerability Disclosure Policy (VDP) sets out:

- how to report a vulnerability to us;
- what you can expect from us in return;
- the scope of the products and services covered by this policy;
- the legal protections we extend to good-faith researchers.

ENISA's Coordinated Vulnerability Disclosure (CVD) guidelines (2022) serve as a reference in establishing this policy.

2. In-Scope Systems and Assets

The following ITX assets are in scope for this policy:

Asset category	Notes
Public web pages	Itxuc.com / itx.no
SaaS product / portal	app.itxuc.com
API and integrations	As documented on https://apidoc.itxuc.com/
Mobile Applications	ITX UC by ITX Norge

3. Out-of-Scope Systems and Assets

The following are explicitly excluded from this policy:

- Third-party services and infrastructure not owned or operated by ITX
- Systems and services belonging to our customers, partners, or suppliers, even if accessible through infrastructure.
- Physical security of offices and data centers.
- Social engineering attacks targeting our customers, employees, or contractors.
- Denial-of-Service (DoS / DDoS) testing of any kind.
- Any system not listed in “In-Scope Systems and Assets”.

4. How to report a vulnerability

Please submit vulnerability reports to:

Email	security@itxuc.com
PGP key	https://itx.no/public-pgp-key.txt
Web form	https://itx.no/<webform-link>
Language	English, any Scandinavian language

What to include in your report

To assist us in triage and reproducing your finding efficiently and correctly, please include:

- A clear description of the vulnerability and its potential impact
- Affected systems or services, URL(s), or component(s)
- Step-by-step reproduction instructions

- Proof-of-concept code, screenshots, or similar, if available
- Your assessment of the vulnerability's severity
- Any suggested remediation, if applicable
- Your contact details (only used for follow-up and credit)

You are free to submit anonymous reports, but then we will be unable to provide any updates or credit.

5. Our commitments to you

Upon receiving a valid report, we commit to:

- acknowledge receipt within 2 business days;
- confirm scope and initial triage within 5 business days;
- provide remediation status updates every 15 business days or upon significant changes;
- give notification of final resolution upon patch or mitigation deployment.

We will not take legal action against any researchers who act in good faith and comply with this policy. We will consider your report in good faith regardless of your geographic location.

6. Safe Harbor / Legal Protections

ITX regards good-faith security research as a valuable contribution to the security of our products and services. We will not initiate or support legal action against researchers for activities that comply with this policy, including:

- Circumvention of access controls solely for the purpose of identifying and reporting vulnerabilities
- Testing that would otherwise constitute a breach of our terms of service, provided no harm is caused
- Incidental access to personal data necessary to demonstrate a vulnerability, provided such data is not retained, used, or disclosed.

This safe harbor applies only to activities conducted within the scope defined in "2. In-scope Systems and Assets" and in compliance with "7. Researcher obligations". It does not authorize and provides no protection for activities outside these bounds.

This safe harbor is a policy commitment, not a legal waiver. It does not bind third parties, including internet service providers or law enforcement.

7. Researcher obligations

To qualify for safe harbor protections and to receive recognition, researchers *must*:

- Promptly report vulnerabilities to us without delay
- Provide sufficient information to reproduce and validate the finding(s).
- Act in good faith throughout the disclosure process
- Keep the vulnerability confidential until we have issued a fix or authorized disclosure (coordinated disclosure)

To qualify for safe harbor protections and receive recognition, researchers *must not*:

- Access, download, modify, or delete data beyond what is strictly necessary to demonstrate the vulnerability
- Exfiltrate personal data or data belonging to third parties
- Conduct denial-of-service attacks (DoS / DDoS)
- Perform social engineering attacks targeting our customers, employees, or contractors
- Introducing backdoors, malware, or other malicious code
- Violate the privacy of individuals whose data may be accessible
- Disclose findings publicly before the agreed disclosure date
- Demand payment or compensation in exchange for not disclosing (extortion)

8. Coordinated Disclosure Timeline

We follow a coordinated vulnerability disclosure (CVD) model aligned with ENISA guidelines and industry norms (e.g. Google Project Zero 90-day policy):

Day	Milestone	Action
Day 0	Report received	Researcher submits report
Day 1-2	Acknowledgement	We confirm receipt
Day 1-5	Initial triage	Scope and validity confirmed, severity assessed
Day 1-30	Remediation (Low/medium)	Patch or mitigation developed and tested

Day 1-15	Remediation (High/Critical)	Accelerated patch development; interim mitigations deployed
Day 90	Default disclosure date	Coordinated public disclosure unless extension agreed

If remediation cannot be completed within 90 days, we will:

- Notify the researcher with a documented reason and revised target date
- Agree a new coordinated disclosure date — maximum extension of 30 additional days without exceptional justification
- Deploy interim mitigations where possible

We may publish security advisories earlier than the agreed date in the following circumstances:

- Active exploitation of the vulnerability in the wild (0-day)
- Vulnerability has been independently discovered and publicly disclosed by a third party
- Researcher and ITX mutually agree that early disclosure serves the public interest

9. Severity and remediation SLAs

We use a simplified classification model for vulnerabilities.

Severity	Remediation target	Example
Critical	ASAP, less than 15 days	Unauthenticated Remote Code Execution (RCE), full authentication bypass, mass data exposure
High	30 days	Authenticated RCE, significant privilege escalation, sensitive data exposure
Medium	60 days	Cross-Site Request Forgery (CSRF), stored Cross Site Scripting (XSS), Insecure Direct Object Reference (IDOR) with limited impact
Low	90 days	Information disclosure (non-sensitive), best practice deviations

10. Recognition and rewards

Hall of fame

Researchers who submit valid, in-scope vulnerabilities will, upon their consent, be listed in our public Security Hall of Fame at [URL]. We credit researchers by name or alias, as they prefer.

Bug bounty

We do not currently offer monetary rewards. We provide public recognition (see previous section) and, where appropriate, a letter of commendation for researchers who make significant contributions.

11. Personal Data and GDPR compliance

Any personal data you share with us in the context of a vulnerability report (including your name, contact details, and any personal data incidentally accessed during testing) will be processed in accordance with General Data Protection Regulation (GDPR) and Personopplysningsloven.

Legal basis for processing: Legitimate interest (GDPR Art. 6(1)(f)) — specifically, the security of our systems and data.

Data minimization: We will retain only the personal data necessary to manage and resolve the reported vulnerability.

Retention: Reporter contact data will be retained for 5 years after case closure for legal purposes, then deleted.

Your rights: You have the right to access, rectify, erase, and restrict processing of your personal data. Contact our Data Protection Officer (DPO) at dpo@itxuc.com.

If a vulnerability you report involves the personal data of third parties, please notify us immediately and do not download, copy, or retain that data. We will assess our GDPR breach notification obligations under Art. 33–34 GDPR accordingly.

12. Policy governance and review

Ownership

This policy is owned by the Chief Information Security Officer (CISO) and is approved by the CEO.

Review Cycle

This policy will be reviewed annually, or following:

- A significant change in the organization's attack surface or technology stack
- A material change in applicable law or regulation
- A significant vulnerability disclosure incident that reveals gaps in this policy