

For everyone

Security and responsible disclosure

How we protect the platform, and how to tell us about a vulnerability without getting into trouble for finding it.

Updated 6 September 2026 · Version 1.0

IN SHORT

- If you find a security hole, tell security@toolbox.africa. We will not pursue anyone who reports in good faith.
- We acknowledge within 2 business days and tell you what we found within 10.
- We do not run a bounty programme yet. We do credit you, if you want that.
- Do not test against real accounts, real homeowners or real tradespeople. Section 4 says what is in bounds.

A plain summary to orient you. The sections below are the agreement.

1. What we do

Section 8 of the **Privacy policy** (toolbox.africa/legal/privacy) sets out the substance: encryption in transit and at rest for sensitive records, access by role and by need, logging of access to sensitive records, sign-in by one-time code so there is no password to steal, and training and confidentiality obligations on the people who handle personal information.

Beyond that:

- We patch our dependencies on a schedule, and immediately for a published critical vulnerability.
- We review changes to anything that touches authentication, verification evidence or payments before they ship.
- We keep production credentials out of the codebase and rotate them.
- We keep backups, encrypted, and we test restoring from them.
- We have a written plan for a security compromise, and section 22 of POPIA sets what we must then tell the Information Regulator and you.

We do not claim a certification we do not hold. If we obtain one, it will be named here with the date.

2. Reporting a vulnerability

Report a vulnerability



Tell us:

- What you found, and where.
- How to reproduce it, step by step.
- What you think an attacker could do with it.
- Whether you have told anyone else.

If the report involves personal information you happened to see, say so, and do not keep a copy.

3. What we promise in return

1. **Within 2 business days** we acknowledge receipt and give you a reference.
2. **Within 10 business days** we tell you whether we have confirmed it and roughly how serious we think it is.
3. **We fix it**, on a timescale that matches the severity, and we tell you when it is done.
4. **We credit you** on this page, if you would like that, once the fix has shipped.
5. **We will not take legal action against you**, and we will not report you to the police, for research that stays inside the bounds in section 4. If a third party asks us to, we will say you were acting responsibly.

We do not pay bounties. We are a small company and would rather say that plainly than run a programme we cannot fund. That may change, and it will be announced here if it does.

4. What is in bounds, and what is not

In bounds:

- Testing against your own account, or an account you created for the purpose.
- Reading, reviewing and reverse-engineering the app on your own device.
- Reporting anything you stumble on in ordinary use.

Out of bounds, and not covered by section 3:

- Accessing, modifying or deleting another person's information. If you find you can, stop, and tell us; do not prove the point.
- Anything that degrades the service for others: load testing, denial of service, or flooding messaging or leads.
- Social engineering our staff, tradespeople or homeowners.
- Physical attacks on our people or premises.

- Publishing the vulnerability before we have fixed it, or 90 days after your report, whichever is sooner.

The **Fair use policy** (toolbox.africa/legal/fair-use) applies alongside this.

5. Coordinated disclosure

We ask for 90 days from your report to fix a vulnerability before you publish it. If we need longer we will ask, with reasons, and we will not be offended if you hold us to a date. If we go silent, publish; silence is not a reason to protect us.

6. Reporting something else

A scam, a fraudulent account, or someone misusing the platform is a matter for **Reporting, blocking and staying safe** (toolbox.africa/legal/community-safety), not this page. A concern about how we handle personal information goes to privacy@toolbox.africa under the Privacy policy.

If anything here is unclear, ask before you rely on it. We would rather explain a clause than argue about it later.