Responsible Disclosure Policy

At Scratch Fix Pro, we've built our business on the simple principle that our customers come first. We aim to keep our website, mobile site and related software applications ("**Website**"), as well as the service offered on our Website ("**Service**") safe for everyone to use, and data security is of the utmost importance. If you have discovered a security vulnerability in our Website or Service, we encourage you to contact us and disclose it to us in a responsible manner.

When security vulnerabilities are reported to us in compliance with this policy, Scratch Fix Pro will validate and fix such vulnerabilities as soon as reasonably possible, in line with our commitment to the privacy, safety and security of our customers. We will not take legal action against you or terminate your access to the Service if you discover and report security vulnerabilities responsibly in compliance with this policy. Scratch Fix Pro reserves all of its legal rights in the event of any noncompliance with this policy.

If you are looking to report another type of issue, which falls outside of the scope of this policy, for example if you are a current customer and you suspect fraudulent activity or suspect that your account may have been compromised, please contact our support team here. Your issue will be investigated immediately and thoroughly.

Reporting a Security Vulnerability

If you think that you have found a security vulnerability in our Website or Service, please contact us immediately via info@scratchfixpro.co.za. When reporting a security vulnerability, you must do the following:

- Include as much information as possible in your report, as we require a way to reproduce the security vulnerability in order to validate and fix it. "Proof-of-Concept" programs, tools, or test accounts that you've created are welcome, and the following information is required:
    - the URL where the vulnerability occurs;
    - if applicable, the parameter where the vulnerability occurs;
    - the type of the vulnerability;
    - a step-by-step instruction how to reproduce the vulnerability;
    - a demonstration of the vulnerability, by screenshots or video; and
    - if applicable, an attack scenario (an example attack scenario may help demonstrate the risk and get the issue resolved faster).
- Do not share your findings with anyone until Scratch Fix Pro has had adequate time to investigate and deploy a fix. We will notify you when the security vulnerability has been patched.
- Consider telling us how to identify you.

We're particularly interested in:

- XSS attacks
- SQL injection
- Remote code execution
- Circumventing permission limitations

- CSRF attacks

Restrictions

At Scratch Fix Pro, we welcome “white hat” security researchers, and appreciate your research and proactive responsible disclosure. Please note however that Scratch Fix Pro does not permit you to do any of the following:

- access, modify or destroy a Scratch Fix Pro customer’s account or data;
- interrupt or degrade our Service;
- execute a “Denial of Service” attack;
- post, transmit, upload, link to, send or store any malicious software;
- send any unsolicited or unauthorized mail or messages;
- violate any applicable law;
- perform any testing that would result in any of the above; or
- attempt to do any of the above.

Contravening this policy in any way may result in us suspending or terminating your access to the Service, contacting the relevant authorities and/or pursuing any other remedies we have at law.

Our Commitment

If you identify a security vulnerability in compliance with this policy, Scratch Fix Pro commits to:

- acknowledging receipt of your vulnerability report in a timely manner;
- confirming the validity of your report; and
- notifying you when the vulnerability is fixed.

We will unfortunately not offer any monetary rewards.