Vulnerability Disclosure Policy

iStaySafe Pty Ltd Vulnerability Disclosure Policy.

We take the security of our systems seriously and are committed to maintaining the security and safety of our customer data. The disclosure of security vulnerabilities helps us ensure the security and the privacy of our users.

This policy details how iStaySafe Pty Ltd will treat the disclosure of reported vulnerabilities that are not publicly known. Our primary goal is to minimise disruption and any potential harm that could be realised by the publication of any vulnerabilities.

If you would like to report a legitimate security vulnerability please email us at techsupport@istaysafe.com.au with your name, company (if not an individual) contact details and your vulnerability report. We will acknowledge your email within 2 business days and provide you with our plan of action and ongoing updates as we progress through our review.

Guidelines

We require that all researchers:

- Make every effort to avoid privacy violations, degradation of user experience, disruption to production systems, and destruction of data during security testing;
- Perform research only within the scope set out below;
- Use the identified communication channels to report vulnerability information to us; and
- Keep information about any vulnerabilities you've discovered confidential between yourself and iStaySafe Pty Ltd until we've had 30 days to resolve the issue.

Vulnerabilities may then be made public after 30 days or sooner if the vulnerability is considered to be exceptionally serious such as threatening public safety.

If you follow these guidelines when reporting an issue to us, we commit to:

- Not pursue or support any legal action related to your research;
- Work with you to understand and resolve the issue quickly (including an initial confirmation of your report within 72 hours of submission);

Please note: iStaySafe Pty Ltd will not provide any monetary compensation to the researcher for sharing any vulnerabilities, however we are happy to credit the researcher with the findings if desired.

Scope

- TicTocTrack iOS and Android App
- TicTocPhone iOS and Android App
- https://tracker.tictoctrack.com
- https://www.tictoctrack.com.au
- TicTocTrack watch

Out of scope

In the interest of the safety of our customers, staff, the Internet at large and you as a security researcher, the following test types are excluded from scope:

- Findings from physical testing such as office access (e.g. open doors, tailgating)
- Findings derived primarily from social engineering (e.g. phishing, vishing)
- Findings from applications or systems not listed in the 'Scope' section
- UI and UX bugs and spelling mistakes
- Network level Denial of Service (DoS/DDoS) vulnerabilities

How to report a security vulnerability?
If you believe you've found a security vulnerability in one of our products or platforms please send it to us by emailing techsupport@istaysafe.com.au Please include the following details with your report:

- Description of the location and potential impact of the vulnerability;
- A detailed description of the steps required to reproduce the vulnerability (POC scripts, screenshots, and compressed screen captures are all helpful to us);