Responsible Disclosure Policy

Online safety and security are important to Marketplacer and we value the work undertaken by security researchers. This policy outlines how to responsibly disclose security defects or vulnerabilities affecting Marketplacer products and services.

Guideline

The identification and disclosure of security vulnerabilities helps Marketplacer to protect the safety and privacy of everyone using Marketplacer's services.

We require that all researchers:

- Make every effort to avoid privacy violations, degradation of user experience, disruption to production systems, and destruction of data belonging to Marketplacer and our customers during testing;
- Perform research only within the limits of scope set out below and in compliance with applicable laws (which includes laws in the researcher's location, Australia and in some cases the United States);
- Use the identified communication channels to report vulnerability information to us; and
- Keep information about the discovery of any defects or vulnerabilities confidential between yourself and Marketplacer until sufficient time has passed to resolve the matter, but no less than 90 days from the date of notification of the vulnerability to Marketplacer.

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

- Not pursue legal action related to your discovery and reporting of the vulnerability (in relation to any non-compliance with these guidelines, we reserve all of our legal rights);
- Work with you to understand and resolve the issue quickly (including an initial confirmation of your report within 5 working days upon receipt of submission); and
- Recognise your contribution in our Security Researcher Hall of Fame, if you are the first to report an issue that we have not already discovered and we make a code or configuration change based on your report.

Scope

This disclosure policy applies only to vulnerabilities in Marketplacer products and services:

- Which are original, previously unreported and not already discovered by internal procedures; and
- For Marketplacer domains/subdomains which have a security.txt file (i.e. https://<subdomain.domain.tld>/.well-known/security.txt).

Out of scope

Third party providers and services are excluded from scope.

In the interest of the safety of our users, 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 as a result of social engineering (e.g. phishing, vishing);
- Findings from an account that does not belong to you;
- Findings from applications or systems not listed in the 'Scope' section;
- UI and UX bugs including spelling mistakes; and
- Network level Denial of Service (DoS/DDoS) vulnerabilities.

Things we do not want to receive:

- Personally identifiable information (PII);
- Credit card holder data;
- Any other sensitive data as defined by the Australian Privacy Act; and
- Reports indicating that our services do not fully align with "best practice" e.g. missing security headers (CSP, x-frame-options, x-prevent-xss etc.) or suboptimal email related configuration (SPF, DMARC etc.).

This policy is intended to align with all relevant legislative requirements and does not give you permission to breach any laws nor cause Marketplacer to breach any laws.

How to report a security vulnerability?

If you believe you've identified a security defect or vulnerability in one of our products or platforms, please send it to us by emailing security-vulnerability@marketplacer.com

Your report must include the following details:

- 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); and,
- Your name/handle and a link for recognition in our Hall of Fame.

By reporting a vulnerability disclosure to us you consent to us collecting and storing your researcher name and/or handle for the purpose of publishing your details in our responsible disclosure hall of fame and for our internal records.

(If you do not wish to have your details published, please let us know at time of disclosure.)

We request that you encrypt your report by using our PGP key and that you delete any data as soon as it is no longer reasonably required.

If you are unsure whether your actions are in line with our policy, please contact our security team for guidance on security-vulnerability@marketplacer.com.

This document was reviewed on the 27th February, 2025 and was created on 29 July 2021.