Vulnerability Disclosure Policy

Version 22.1

October 2022

1 INTRODUCTION

1.1 PURPOSE

Our security vulnerability disclosure policy gives security researchers and the community a point of contact with us. We encourage you to tell us if you find a potential vulnerability within our systems, services or products.

1.2 SCOPE

We take the security of our systems seriously. We take every effort to keep our systems secure. Despite our efforts, there may still be vulnerabilities. The responsible disclosure of security vulnerabilities helps us ensure the security and privacy of our systems and our customers.

We are keen to engage with the security community. Our security vulnerability disclosure policy allows you to responsibly share your findings with us in good faith. If you think you have found a potential vulnerability in one of our systems, services or products, please tell us as quickly as possible by sending an email to cybersecurity@comparthemarket.com.au as detailed in Section 1.4

We will not compensate you for finding potential or confirmed vulnerabilities. If you have not exploited the vulnerability or prematurely disclosed its possible existence, we will not take any legal action against you.

We do not condone any malicious or illegal behaviour in the identification and reporting of security vulnerabilities.

Our policy does not authorise you to conduct security testing against any of our systems, services or products. If you think a vulnerability exists, report it to us. We can test and verify it.

1.3 SECURITY RESEARCH THAT IS NOT ALLOWED

Our Vulnerability Disclosure Policy does not allow for:

- Clickjacking
- Social engineering
- Phishing
- Denial of service (DoS or DDoS) attacks
- Uploading, linking, transmitting, posting or sending of malware.
- Attempts to destroy of modify data
- Attempts to access, extract or exfiltrate data
- Gaining access to unauthorised data
- Weak or insecure ciphers and protocols
- Weak or insecure Certificates
- Physical security breaches or attacks
- Vulnerabilities from automated scanners

This policy does not authorise individuals or groups to undertake hacking or penetration testing against any of our systems, services or products.

This policy does not cover any other action that is unlawful or contrary to legally enforceable terms and conditions for using a product or service.

1.4 How to report a vulnerability

To report a vulnerability please:

- email the content of the vulnerability to cybersecurity@comparthemarket.com.au as quickly as possible.

Please include the following information:

- Your name
- Contact information (optional if you want to be contacted).
- Vulnerability description / explanation
- Time and date that the suspected vulnerability was discovered.
- Listing the systems, services or products that may be affected.
- List of any changes made including submissions of applications / data.
- The IP address used to discover the suspected vulnerability
- Vulnerability details including step by step instructions to reproduce the vulnerability.
- Proof of concept code where applicable

1.5 Evaluation of reported vulnerability

Once a report has been received, the report will be:

- Reviewed within 5 business days to confirm the validity of the report.
- Risk assessed to determine the impact to our systems, services or products.

Compare The Market will then:

- Determine if any further action will be taken.
- Determine if you will be contacted.
- Determine if any third parties including ACSC, Law enforcement, suppliers, Regulators or OAIC need to be informed.
- Determine any remediation activities.
- Determine and agree on public disclosure date and process (if applicable)
- With your consent credit you as the person who discovered the vulnerability. (if required)
- All information will be protected in line with our Privacy Policy.

Compare The Market will not:

- Always contact the person disclosing the vulnerability.
- Detail any remediation activities.
- Provide any compensation for finding and reporting vulnerabilities (confirmed or unconfirmed).
- Disclose your personal information without your consent. Note this does not include Law Enforcement