



## Vulnerability Disclosure Policy – VDP

### Introduction

In order to succeed in a more complex and digitising world, you'll need a helping hand when it comes to finding out exactly what your customers want and need. Mopinion provides an all-in-one user feedback software solution that makes difficult decision-making easy across all digital touchpoints (web, mobile and email).

Mopinion is committed to ensuring the security of its clients by protecting their information. This policy is intended to give security researchers clear guidelines for conducting vulnerability discovery activities and to convey our preferences in how to submit discovered vulnerabilities to us.

This policy describes what systems and types of research are covered under this policy, how to send us vulnerability reports, and how long we ask security researchers to wait before publicly disclosing vulnerabilities.

We encourage you to contact us to report potential vulnerabilities in our systems.

### Authorization

If you make a good faith effort to comply with this policy during your security research, we will consider your research to be authorized. We will work with you to understand and resolve the issue quickly, and Mopinion will not recommend or pursue legal action related to your research. Should legal action be initiated by a third party against you for activities that were conducted in accordance with this policy, we will make this authorization known.



## Guidelines

Under this policy, “research” means activities in which you:

- Notify us as soon as possible after you discover a real or potential security issue.
- Make every effort to avoid privacy violations, degradation of user experience, disruption to production systems, and destruction or manipulation of data.
- Only use exploits to the extent necessary to confirm a vulnerability’s presence. Do not use an exploit to compromise or exfiltrate data, establish persistent command line access, or use the exploit to pivot to other systems.
- Provide us a reasonable amount of time to resolve the issue before you disclose it publicly.
- Do not submit a high volume of low-quality reports.

Once you’ve established that a vulnerability exists or you encounter any sensitive data (including personally identifiable information, financial information, or proprietary information or trade secrets of any party), **you must stop your test, notify us immediately, and not disclose this data to anyone else.**

## Test methods

The following test methods are not authorized:

- Network denial of service (DoS or DDoS) tests or other tests that impair access to or damage a system or data
- Physical testing (e.g. office access, open doors, tailgating), social engineering (e.g. phishing, vishing), or any other non-technical vulnerability testing



## Scope

Before adding a system or service to the scope, ensure you are permitted to authorize security testing on the system or service. Confirm whether Mopinion has explicitly authorized such testing, such as in your contract or terms. If not, you should work with Mopinion to obtain authorization. If it is not possible to obtain authorization, you may not include those systems or services in scope of your policy.

This policy applies to the dedicated testing environment Mopinion provides via: [kpn-test.mopinion.com](https://kpn-test.mopinion.com)

Any product or service not expressly listed above, such as the Mopinion public website ([mopinion.com](https://mopinion.com)), any connected services and client production stages (for example, [\[client-name\].mopinion.com](https://[client-name].mopinion.com)), are excluded from scope and are not authorized for testing.

Also excluded from scope are web services and API's provided by Mopinion via \*.[mopinion.com](https://mopinion.com) sub-domains (i.e. [api.mopinion.com](https://api.mopinion.com)).

Additionally, vulnerabilities found in systems from our vendors fall outside of this policy's scope and should be reported directly to the vendor according to their disclosure policy (if any). If you aren't sure whether a system is in scope or not, contact us at [security\[@\]mopinion.com](mailto:security[@]mopinion.com) before starting your research.

Though we develop and maintain other internet-accessible systems or services, we ask that active research and testing only be conducted on the systems and services covered by the scope of this document. If there is a particular system not in scope that you think merits testing, please contact us to discuss it first. We will increase the scope of this policy over time.



## Reporting a vulnerability

Information submitted under this policy will be used for defensive purposes only – to mitigate or remediate vulnerabilities. If your findings include newly discovered vulnerabilities that affect all users of a product or service and not solely Mopinion, we may share your report with relevant and/or involved organisations, where it will be handled under their coordinated vulnerability disclosure process. We will not share your name or contact information without express permission.

We accept vulnerability reports via [security\[@\]mopinion.com](mailto:security[@]mopinion.com). Reports may be submitted anonymously. If you share contact information, we will acknowledge receipt of your report within three business days.

We do not support PGP-encrypted emails. For particularly sensitive information, please contact us via the above email address to discuss the most secure way of transferring the data.

*By submitting a vulnerability, you acknowledge that you have no expectation of payment and that you expressly waive any future pay claims against Mopinion related to your submission.*

## What we would like to see from you

In order to help us triage and prioritize submissions, we recommend that your reports:

- Describe the location the vulnerability was discovered and the potential impact of exploitation.
- Offer a detailed description of the steps needed to reproduce the vulnerability (proof of concept scripts or screenshots are helpful).
- Be in English, if possible.



## **What you can expect from us**

When you choose to share your contact information with us, we commit to coordinating with you as openly and as quickly as possible.

Within three business days, we will acknowledge that your report has been received.

To the best of our ability, we will confirm the existence of the vulnerability to you and be as transparent as possible about what steps we are taking during the remediation process, including on issues or challenges that may delay resolution.

We will maintain an open dialogue to discuss issues.

## **Questions**

Questions regarding this policy may be sent to [security\[@\]mopinion.com](mailto:security[@]mopinion.com). We also invite you to contact us with suggestions for improving this policy.

