Responsible Disclosure Policy

Document number: 61
Version: 1.0
Author: Amy Jennings
Approved by: Sarah Whitla
Approved on: 19 November 2025
Status: Final

Change log

Version	Date	Who	Details
1.0	19/09/2025	Amy Jennings	Initial draft of policy
1.0	19/09/2025	Sarah Whitla	Approval v1.0

Responsible Disclosure Policy

Version: 1.0
Last reviewed: 19 November 2025

If you would like to report a vulnerability or have a security concern regarding visual-meaning.com or the mapping Shared Meaning Platform / Compass, please email security@visual-meaning.com.

We take the security of our customers' data very seriously. If you believe you've discovered a potential security vulnerability within visual-meaning.com or the mapping Shared Meaning Platform / Compass, we strongly encourage you to disclose it to us as quickly as possible and in a responsible manner, and we commit to dealing in good faith with reporting parties who comply with this policy.

To encourage responsible disclosure, we will not take legal action against security researchers in relation to the discovery and reporting of a potential security vulnerability. This is provided that all such potential security vulnerabilities are discovered and reported strictly in accordance with this Responsible Disclosure Policy. In the event of any non-compliance, we reserve all of our legal rights. If in doubt, please contact us by sending an email to security@visual-meaning.com.

How to Report a Potential Security Vulnerability

To report vulnerabilities related to visual-meaning.com or the mapping Shared Meaning Platform / Compass:

- Privately share details of the suspected vulnerability with Visual Meaning by submitting them to security@visual-meaning.com.
- Include as much information as possible about the suspected vulnerability so the Visual Meaning team may validate and reproduce the issue, including:
    - An explanation of the potential security vulnerability;
    - Which site/s are affected (IP address or URL);
    - Steps to reproduce the vulnerability;
    - Screenshots or logs (where applicable);
    - Proof-of-concept code or a recommended fix (where applicable); and
    - Your contact information.

What happens next?

Once you have reported a potential security vulnerability (of high quality and in compliance with this policy), we will contact you within 2 UK working days with an initial response. We'll try to assess your report within 10 UK working days and provide feedback. Going forward, we will keep you informed on our progress towards addressing the potential security vulnerability and will also notify you when the matter has been addressed. We prioritise fixes by impact, severity, and exploit complexity.

Subject to any regulatory and legal requirements, all reports will be kept strictly confidential, including the details of the potential security vulnerability as well as the identity of all researchers involved in reporting it. In the event of any law enforcement or civil action brought by anyone other than Visual Meaning Ltd, Visual Meaning will take reasonable steps to make known that the activities of the reporting parties were conducted pursuant to and in compliance with this Responsible Disclosure Policy.

Once the vulnerability has been fixed, we can work with you to disclose and publish the report. If a report is found to be a duplicate or is otherwise already known to us, the report may not be eligible for public recognition.

Reporting parties must allow Visual Meaning an opportunity to correct a potential vulnerability within a reasonable timeframe before publicly disclosing the identified issue, to ensure that Visual Meaning has developed and thoroughly tested the solution to such issue.

Please note that we do not compensate individuals or organisations for identifying potential or confirmed security vulnerabilities.

Discovering Potential Security Vulnerabilities

We encourage you to conduct responsible security research on our products and services. Activities conducted under this Responsible Disclosure Policy must be limited exclusively to the following:

- Testing on services or products to which you have authorised access to detect a potential vulnerability or to identify an indicator related to a potential vulnerability; or
- Sharing information with Visual Meaning, or receiving information from Visual Meaning, related to a potential vulnerability.

Visual Meaning does not authorize, permit, or otherwise allow (expressly or impliedly) anyone to engage in any illegal activity. If you engage in any activities that are inconsistent with this Responsible Disclosure Policy or any applicable law, you may be subject to criminal and/or civil liabilities.

Parties conducting activities subject to the Responsible Disclosure Policy must do no harm. The following are strictly prohibited:

- Exploiting any security vulnerability beyond the minimal amount of testing required to demonstrate that a potential vulnerability exists;
- exfiltrating, accessing, or attempting to access accounts or data that is not already available to you;
- modifying or destroying any data;
- executing or attempting to execute a denial of service (DoS) attack for example, overwhelming a site with a high volume of requests;
- sending or attempting to send unsolicited or unauthorised email, spam or any other form of unsolicited messages;
- conducting social engineering, phishing, or physically attacking our staff, contractors or infrastructure;
- testing third party websites, applications or services that integrate with our services or products;
- the use of high-intensity invasive or destructive scanning tools;
- compromising the privacy or safety of Visual Meaning employees & contractors, Visual Meaning customers, or any third parties;
- intentionally compromising the intellectual property or other commercial or financial interests of Visual Meaning, Visual Meaning employees & contractors, Visual Meaning customers, or any third parties;
- posting, transmitting, uploading, linking to, sending, executing, or storing any malware, viruses, or harmful software on any Visual Meaning network(s) or system(s); or
- demands for money to disclose a vulnerability.

Reporting parties are asked to please allow Visual Meaning an opportunity to correspond in good faith and correct a potential vulnerability within a reasonable timeframe before publicly disclosing the identified issue, to ensure that Visual Meaning has developed and thoroughly tested the solution to such issue.

To the extent that any security research or vulnerability disclosure activity involves the networks, systems, information, applications, products, or services of any third party (i.e. not Visual Meaning Ltd), such third party may independently determine whether to pursue legal action or remedies related to such activities.

End of Document