Vulnerability Disclosure Policy

Revision History

Version	Review Date	Types of Changes	Approver
1.0	07.01.2021	Original Version	Juan Mera
1.1	11.27.2023	Minor Updates	Juan Mera
1.2	11.29.2024	Minor Updates	Juan Mera
1.2	11.28.2025	Revision – No changes	Juan Mera

Purpose

Avature is committed to ensuring the security of their users by protecting their information from unwarranted disclosure. 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 want security researchers to feel comfortable reporting vulnerabilities they've discovered – as set out in this policy – so we can fix them and keep our users safe. We have developed this policy to reflect our values and uphold our sense of responsibility to security researchers who share their expertise with us in good faith.

Guidelines

We request that you:

- Notify us as soon as possible once you discover a real or potential security issue.
- Avature may take up to 180 days for low severity issues. Check with us if the issue is fixed before public disclosure.
- 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 command line access and/or persistence, or use the exploit to "pivot" to other systems.
- Once you've established that a vulnerability exists or 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.
- Do not submit a high volume of low-quality reports.

Authorization

If you comply with this policy during your security research, we will consider your research to be authorized, we will reasonably work with you to understand and resolve the issue quickly and Avature will not recommend or pursue legal actions related to your good faith research.

Due our confidentiality procedure, (a) any findings should be reported to us as soon as possible and without disclosing to third parties that Avature has or may have been affected by it, and (b) any vulnerability found may not be exploited and any data acquired through it should be kept confidential and may not be used for any purpose of the researcher or a third party.

Scope

www.avature.net

Any service not expressly listed above, such as any connected services, are excluded from scope and are not authorized for testing. If you aren't sure whether a system or endpoint is in scope or not, contact us at security@avature.net 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.

Types of testing

The following test types are not authorized:

- Network denial of service (DoS or DDoS) tests.
- Physical testing (e.g. office access, open doors, tailgating).
- Social engineering (e.g. phishing, vishing), or any other non-technical vulnerability testing.

Reporting a vulnerability

Information submitted under this policy will be used for defensive purposes only – to mitigate or remediate vulnerabilities.

We accept vulnerability reports via security@avature.net. Reports may be submitted anonymously.

What we would like to see from you

To help us triage and prioritize submissions, we recommend that your reports:

- Describe the vulnerability, where it 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.

- 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 issues or challenges that may delay resolution.
- We will maintain an open dialogue to discuss issues.