



DISCLOSURE POLICY

I. Purpose.

- 1.1. This Policy applies to the following types of disclosure information which is to be made public or assumed to be made public on website dbaas.victoriametrics.com.
- 1.2. Victoria Metrics has a basic policy on information disclosure to all our customers, potential customers, investors, regarding the appropriate disclosure of information concerning our company.
- 1.3. Maintaining the security, privacy, and integrity of our services time-series database, that is designed to collect, store and observe metrics is a priority at Victoria Metrics.
- 1.4. We disclose information only in compliance with the US laws and regulations.
- 1.5. By Victoria Metrics shall mean a legal entity Victoria Metrics Inc. organized and existing under the laws of State of Delaware, the United States of America, located at: 8 THE GREEN SUITE #11316 DOVER, DE 19901, USA, that provides real-time monitoring services, time-series database services, data hosting services; large-scale, super-load system monitoring platforms support; customer support and consulting services and included but not limited to packaging, mailing and delivering services, other services that may be developed from time to time.
- 1.6. By using the Victoria Metrics services, you agree to the terms and conditions of this Policy.
- 1.7. We will not disclose your personal information except as described in Victoria Metrics Privacy Policy.



II. Scope.

2.1. Services designed to collect, store and observe metrics that Victoria Metrics provides are in scope.

2.2. The scope of this policy includes all who gain information about non-disclosed security vulnerabilities affecting either Victoria Metrics, customers of Victoria Metrics, or 3rd parties associated with Victoria Metrics.

2.3. In addition, external parties who have found vulnerabilities in Victoria Metrics owned systems are strongly recommended to follow the instructions in this policy to avoid any legal consequences of uncontrolled vulnerability disclosure.

2.4. Any of the activities below will result in disqualification from the policy permanently.

- Customers of Victoria Metrics behind our infrastructure.
- Any vulnerability obtained through the compromise of a Victoria Metrics customer accounts.
- Any Denial of Service (DoS) attack against Victoria Metrics and our products.
- Physical attacks against Victoria Metrics employees, offices, and data centers.
- Social engineering of Victoria Metrics employees, contractors, vendors, or service providers.
- Knowingly posting, transmitting, uploading, linking to, or sending any malware.
- Pursuing vulnerabilities which send unsolicited bulk messages (spam) or unauthorized messages.

III. Information Protection.

3.1. To prevent the misuse or inadvertent disclosure of material information, the following procedures is observed by Victoria Metrics at all times:

- Documents and files containing confidential information are kept in a safe place, with access restricted to customers who 'need to know' that information in the necessary course of business. Code names are used if necessary.



- Confidential matters are not to be discussed in places where the discussion might be overheard, such as elevators, hallways, restaurants, airplanes or taxis.
- Confidential matters are not to be discussed on unsecure cell phones.
- Confidential documents are not to be read or displayed in public places and not be discarded where others can retrieve them.
- Employees ensure they maintain the confidentiality of information in their possession outside of the office as well as inside the office.

3.2. Transmission of documents by electronic means, such as by fax, email or directly from one computer to another, are made only where it is reasonable to believe that the transmission can be made and received under secure conditions.

3.3. Unnecessary copying of confidential documents are avoided and documents containing confidential information are promptly removed from conference rooms and work areas after meetings have concluded. Extra copies of confidential documents are shredded or otherwise destroyed.

3.4. Access to confidential electronic data are restricted through the use of passwords and documents that are not stored in a shared directory.

3.5. Victoria Metrics does not comment, affirmatively or negatively, on rumours regarding services provisioning, vulnerabilities and others.

3.6. This policy also applies to rumours on the Internet, including social networking sites.

3.7. If the rumour is true in whole or in part, the rumour might be evidence of a leak, and Victoria Metrics will immediately issue a news release disclosing the relevant material information.

IV. Eligibility and Disclosure.

4.1. Only public information or information that could otherwise be disclosed in accordance with this Policy shall be used to respond to electronic inquiries. Written confirmation from Victoria Metrics shall be received before disclosing any other information related to Victoria Metrics or services.



4.2. In order to protect our customers, Victoria Metrics requests that you not post or share any information about a potential vulnerability in any public setting until we have researched, responded to, and addressed the reported vulnerability and informed customers if needed.

4.3. This policy is not open to any customers or individuals on, or residing in any country on, any U.S. sanctions lists.

4.4. You must not violate any law. You are responsible for any tax implications or additional restrictions depending on your country and local law.

4.5. Requests for disclosure of information must be submitted to the following email address:
security@victoriametrics.com

4.6. Victoria Metrics will endeavour to process requests for disclosure of information as promptly as possible. Depending on the complexity of the request, Victoria Metrics will seek to respond to requests within 60 days of receipt of the request.

4.7. Victoria Metrics may charge a fee for requests for information, based on the estimated costs of retrieving and supplying the information requested, which will be communicated to the requestor and must be paid in advance. Victoria Metrics reserves the right to charge an additional fee in complex cases.

4.8. Requests for internal Victoria Metrics review should be submitted to the email address mentioned above. Such internal review will be carried out by the first level supervisor of the Victoria Metrics staff who signed the initial response.

4.9. Subject to the complexity of the request, Victoria Metrics will aim to respond within 60 days of receipt of the request for internal Victoria Metrics review.

V. Vulnerability.

5.1. Victoria Metrics committed to creating a safe, transparent environment to report vulnerabilities.

5.2. Therefore, Victoria Metrics appreciates the work of security researchers in order to improve our security posture.

5.3. If you believe you have found a security vulnerability that could impact Victoria Metrics or our users, we encourage you to report this right away. We will investigate all legitimate reports and fix the problem as soon as we can.



5.4. We ask that you follow Victoria Metrics's Disclosure Policy and make a good faith effort to avoid privacy information violations, destruction of data, and interruption or degradation of our service during your research.

5.5. Vulnerability investigations and discoveries made or reported in compliance with this Policy are considered compliant with Victoria Metrics online Terms of Use.

VI. Conditions.

6.1. Victoria Metrics may deny a request for disclosure of information, in whole or in part, if in the judgment of Victoria Metrics, the request is unreasonable, repetitive, abusive or vexatious or If the request is related to one or more similar request(s) that have been denied by Victoria Metrics.

6.2. If only part of the information that is responsive to a particular request for disclosure is subject to one of the limitations set out in this Policy, Victoria Metrics may decide, at its sole discretion, that the remaining part of the information, responsive to that request, will be disclosed. In such cases, Victoria Metrics will take appropriate measures to preserve the confidentiality of the information that is not disclosed.

6.3. The implementation of this Policy is subject to the intellectual property and other proprietary rights of Victoria Metrics and third parties, including but not limited to patents, copyrights, and trademarks, which may, inter alia, limit the right to reproduce or exploit information.

6.4. No representation is made or warranty given, express or implied, as to the completeness or accuracy of information made available by Victoria Metrics.

6.5. Moreover, Victoria Metrics does not warrant that the use of any third party-owned individual component contained in the requested information will not infringe on the rights of those third parties.

6.6. The risk of claims resulting from such infringement rests solely with the requestor/user. It is the responsibility of the requestor/user to determine whether permission is needed for any use of the information and to obtain permission from the copyright holder. In no circumstances will Victoria Metrics be liable for any direct or indirect loss arising from the use of information.

6.7. Nothing contained in or relating to this Policy, or done pursuant to it, shall be construed as a waiver of any of the privileges and immunities enjoyed by Victoria Metrics under national or international law, and/or as submitting Victoria Metrics to any national court jurisdiction.



6.8. Without limiting the generality of the previous sentence, the disclosure of information in response to a request for disclosure, will not constitute a waiver, express or implied, of any of the privileges and immunities of Victoria Metrics.

VII. Privileged information.

7.1. Privileged information of Victoria Metrics is forbidden to disclose, namely:

- Information covered by legal privilege, or the disclosure of which may expose Victoria Metrics to legal risk.
- Legal advice and requests for legal advice.
- Documents, analyses, correspondence or other information prepared for financial and budgetary transactions, or for the development of internal or external financial reports.
- Banking or billing information of Victoria Metrics, Victoria Metrics contractors and vendors (companies or individuals), including consultants.
- Commercial information which, if disclosed, may harm either the financial interests of Victoria Metrics or those of third parties.
- Passwords, pins and other access codes for Victoria Metrics systems.
- Other kinds of information, which because of its nature, content or the circumstances surrounding its creation, use or communication is deemed confidential in the interests of Victoria Metrics or third parties.

VIII. Entry into force and application of this Policy.

8.1. This Policy shall enter into force on the effective date stated here below.

8.2. This policy will be implemented progressively over a period of two years from coming into force, subject to availability of resources, to accommodate revisions of related internal policies and procedures. We reserve the right to change this Policy at any time and from time to time in Victoria Metrics sole and absolute discretion without the duty to notify you.



IX. Contact Information.

VICTORIA METRICS, Inc.

8 The Green Suite #11316, Dover, DE 19901, USA

<https://victoriametrics.com/>

<https://victoriametrics.github.io/>

security@victoriametrics.com

Effective as of October 21, 2021