Vulnerability Disclosure Policy

1. Policy introduction & policy purpose

The purpose of this policy is to establish a method all Hitachi Vantara customers and external stakeholders should follow to report any potential vulnerabilities and threats.

This policy's objective is to ensure Hitachi Vantara's customers trust by continuously addressing potential vulnerabilities and threats to reduce potential risks that may have an impact to Hitachi Vantara operations, infrastructure, and services.

2. Scope

This policy applies to all divisions and geographies, unless noted otherwise within this document, and is intended for all employees with a direct or indirect relationship with customers and third parties to whom Hitachi Vantara does business.

The following situations are excluded from this policy:

- When a Hitachi Vantara customer or third-party requests actions beyond a valid contract extension.

3. Process to report potential vulnerabilities and threats

3.1. Any Hitachi Vantara customer or third party may submit a report to notify about potential vulnerabilities or threats. A report submission should include the following information, but not limited to:

- Details of affected Hitachi Vantara product or solution
- Versions of software and/or microcode of Hitachi Vantara components
- A detailed description of the identified vulnerability or threat, and
- Any other relevant information such as evidence or proof of concept, where the identified vulnerability is already published, and where the individual reporting is committed to coordinated disclosure.

3.2. Contact information to report any potential vulnerability or threat:

- When a potential security vulnerability in Hitachi Vantara's products is discovered, customers or third parties are encouraged to report the vulnerability by contacting Hitachi Vantara's Global Support Center (GSC).
- The GSC team will work in conjunction with Hitachi Vantara's Cybersecurity team to investigate the issue in accordance with customer contract requirements and GSC standard operating procedures. This collaborative approach ensures robust data network security measures are upheld.
- Hitachi Vantara recommends using an encryption program to securely transmit any confidential and personal data.
- While Hitachi Vantara will review reports submitted through the GSC, weaknesses in existing customer installation due to their individual designs, third-party components, or compromised access credentials are not considered a vulnerability within Hitachi Vantara's products.
- For all entities without a customer relationship with Hitachi Vantara, you can report security vulnerabilities to the Cybersecurity team here. (security.vulnerabilities@hitachivantara.com)

3.3. With the agreement of the reporting customers or third party, Hitachi Vantara must recognize the customer or third party with credit for the discovery of the vulnerability as part of the official Hitachi Vantara process. Hitachi Vantara does not have a "Bug Bounty" program in place. Therefore, Hitachi Vantara does recognize the vulnerability researchers through the vulnerability (CVE - Common Enumeration of Vulnerabilities) publication when applies, or a recognition letter for their contributions.

3.4. Hitachi Vantara's product vulnerability handling generally consists of the following:

- First response,
- Initial triage,
- Investigation and planning,
- Remediation, and
- Disclosure & notification.

This structured process reinforces our commitment to maintaining high standards in data and network security.

While Hitachi Vantara makes all effort to timely remediate vulnerabilities posing a high risk for Hitachi Vantara, its customers, and third parties, remediation times may vary depending on vulnerability complexity or threat conditions. Assuming the reported information is not known publicly, it is the intention of the customer or third-party reporting a vulnerability and Hitachi Vantara do not release any related information until there is remediation.

4. Disclaimer

The information contained herein is subject to change at any time without notice. The statements in this policy do not modify, supersede, or otherwise amend any customer rights, obligations, or terms between Hitachi Vantara LLC and any other party. The use of the information or links included in this policy is done at your own risk.