VULNERABILITY DISCLOSURE POLICY

Introduction

In this Policy, "**Validus**", "**we**", "**our**" or "**us**" means Validus Investment Holdings Pte. Ltd., its subsidiaries and affiliates. Validus is committed to ensuring the security of our customers' data, and the reliability of our products and services. While we aim to design and make our products and services with the highest levels of security and reliability, we also recognise that due to the highly complex and sophisticated nature of our products and services, vulnerabilities or errors may still be present in our products and services.

This Policy sets out our approach to requesting and receiving reports related to potential vulnerabilities and errors. It includes details on how you can submit a vulnerability report and how we will work with you after a vulnerability has been reported.

Reporting of Vulnerabilities

Validus highly appreciates the efforts made by the reporting party in identifying the vulnerability or error. Reporting of such vulnerabilities and errors will contribute to improving the security and reliability of our products and services.

Any customers, users, researchers, partners or any other persons, who interacts or accessing our online services (through our public facing websites or mobile applications) are encouraged to report any identified actual or potential security vulnerabilities or errors to us by using the process below. By submitting a vulnerability report to us, you are deemed to have already read, understood and accepted all terms and conditions set out herein in this Vulnerability Disclosure Policy.

For reporting of a suspected vulnerability, please email us at security@validusgrp.com. To assist us with the validation, we appreciate if you can provide adequate information in your report, including the following:

- Your name and contact number to facilitate clarifications.
- Date and time of the vulnerability discovery.
- Description of the suspected vulnerability and the reason(s) why you believe the suspected vulnerability may impact the subject service/product.
- Description of the methods, steps, tools and artifacts used leading to the discovery.
- IP address and/or URL of the subject service.
- Any other information such as network packet captures, crash reports, screenshots, or video recording providing evidence of codes or commands that were used in the discovery of the suspected vulnerability.

Your Information and Consent

Please note that supplying your contact information with your report is entirely voluntary and at your discretion. By providing your contact information to Validus, you agree for your contact information to be processed in accordance with Validus' Privacy Policy.

By submitting a report to Validus regarding vulnerabilities and errors, you agree to the following terms:

- Validus may use your report for any purpose deemed relevant by Validus, including without limitation, for the purpose of correcting any vulnerabilities and errors that are reported and that Validus deems to exist and to require correction.
- To the extent that you propose any changes and/or improvements to a Validus' product or service in your report, you assign to Validus all use and ownership rights to such proposals.

Your Undertakings

You confirm to Validus that:

- You have not exploited or used in any manner and will not exploit or use in any manner (other than for the purposes of reporting to Validus), the discovered vulnerabilities and/or errors.

- You have not engaged, and will not engage, in testing/research of systems with the intention of harming Validus, its customers, employees, partners or suppliers.
- You have not used, misused, deleted, altered or destroyed, and will not use, misuse, delete, alter or destroy, any data that you have accessed or may be able to access in relation to the vulnerability and/or error discovered.
- You have not conducted, and will not conduct, social engineering, spamming, phishing, denial-of-service or resource-exhaustion attacks.
- You have not tested and will not test the physical security of any property or building of Validus.
- You have not breached and will not breach any applicable laws (including the Computer Misuse Act 1993) in connection with your report and your interaction with Validus product or service that led to your report.
- You agree not to disclose to any third party any information related to your report, the vulnerabilities and/or errors reported, nor the fact that vulnerabilities and/or errors have been reported to Validus unless you have prior written consent from Validus.
- You agree that you are making your report without any expectation or requirement of reward or other benefit, financial or otherwise, for making such report, and without any expectation or requirement that the vulnerabilities and/or errors reported are corrected by Validus.
- Validus will not be liable or assume any responsibility for any expense, damage or loss of any kind which you may incur in relation to any vulnerability report.
- Nothing in this Policy creates an agency, partnership, association, joint venture or similar relationship between you and Validus.

Our Actions

Upon receiving your report, we will work to validate the reported vulnerability. If necessary, we will contact you to clarify the details of your report. However, we do not guarantee that you will receive any response from Validus related to your report. Please also note that our acknowledgment or processing of any vulnerability report shall not constitute any kind of acceptance or endorsement of the contents therein.

For vulnerabilities affecting services of our third-party service providers, we reserve the right to forward the details of the vulnerability to that party without seeking your approval. We also reserve the rights to release the details of the vulnerability to our customers or to the public for awareness. We are not obliged to consult with you about any public statement should we elect in our sole discretion to release statement in relation to a vulnerability report submitted by you.