Vulnerability Disclosure Policy

We **Wuxi Solinteg Power Co., Ltd.**

Building H1-1001, No. 6 Jingxian Road, Xinwu District, Wuxi, 214135 Jiangsu P.R. China

attach great importance to security issues and welcome you to report potential security vulnerabilities to us to improve the security of our products and services.

This vulnerability disclosure policy applies to any vulnerabilities you are considering reporting to us. We recommend reading this vulnerability disclosure policy fully before you report a vulnerability and always acting in compliance with it.

We value those who take the time and effort to report security vulnerabilities according to this policy. However, we do not offer monetary rewards for vulnerability disclosures.

Reporting

If you believe you have found a security vulnerability, please submit your report to us via the following email: service@solinteg.com

The email should include at least the following information:

- Your organization and contact information
- Products and versions affected (web address, IP Address, product or service name)
- Description of the potential vulnerability
- Information about known exploits
- Additional information, if any

Response Time

After you have submitted your report, we will respond to your report within 10 working days and aim to triage your report within 20 working days. We will also aim to keep you informed of our progress. Priority for remediation is assessed by looking at the impact, severity and exploit complexity. Vulnerability reports might take some time to triage or address. You are welcome to enquire on the status but should avoid doing so more than once every 20 days. This allows our teams to focus on the remediation. We will notify you when the reported vulnerability is remediated, and you may be invited to confirm that the solution covers the vulnerability adequately.

Guidance

Do NOT:

• Break any applicable law or regulations

• Access unnecessary, excessive or significant amounts of data

• Modify data in our systems or services

• Use high-intensity invasive or destructive scanning tools to find vulnerabilities

• Attempt or report any form of denial of service, e.g. overwhelming a service with a high volume of requests

• Disrupt the our services or systems