Cybersecurity Vulnerability Management Policy

■ Cybersecurity Vulnerability Management Policy

HDRE is committed to rigorous product [1] security vulnerability management and provides customers with reliable product cybersecurity vulnerability guidance and solution to minimize the risks associated with product cybersecurity vulnerabilities. Therefore, HDRE has established a Product Security Incident Response Team (PSIRT) to handle product information security incidents and related product vulnerability reports submitted to HDRE.

If you find a vulnerability, **please send a description of the vulnerability (including the specific product model, software version, etc.) to hd.psirt@hdrenewables.com and leave your contact information.** Generally, you will receive an initial response email within 2 working days and an investigation result email within 10 working days. Throughout the vulnerability handling process, we will keep you updated on the progress and sincerely request that you keep the information confidentially. We will not provide any received information to any third party except as required by law or by a formal request from our clients. We will comply with applicable laws and regulations and take all reasonable measures to protect information security.

Note [1]：The 'Product' as mentioned in this document refers to standard HDRE product in the market. Maintenance and responses to vulnerability of project-based products will be carried out as stipulated in the contract.

Cybersecurity Vulnerability Management Process

■ Cybersecurity Vulnerability Management Process

Upon receiving a suspected vulnerability report, the Product Security Incident Response Team (PSIRT) will work closely with the relevant product team to respond according to the following management process:

1. **First Incident Response:** Upon receiving an external vulnerability report for its product, PSIRT will send an initial response email to the reporter within 2 working days generally.
2. **Triage and Analysis:** The reported vulnerability is reviewed to assess its existence and technical effectiveness. The severity is determined based on the vulnerability's actual impact on the product. The response priority is determined based on the assessment results.
3. **Investigation:** PSIRT collaborates with the product development department to identify the root cause of the vulnerability and further analyzes mitigation and resolution methods. PSIRT will keep the reporter updated progress and reports the investigation results [**Note 2**] within 10 working days.
4. **Remediation:** This includes proposing risk mitigation measures, providing customers with implementable temporary risk management measures, or releasing patches and software updates.

Note [2]：As the products are sold globally, the investigation results are usually written in English.

■ Disclaimer

The content of the "Cybersecurity Vulnerability Management Policy" is subject to change based on specific circumstances. It is not guaranteed to address any specific issue or category of issue. You assume all risks associated with using the information in this document or any content linked to from this document. HDRE reserves the right to change the content of this document at any time without notice.