Sunsynk Vulnerability Disclosure Policy

Effective Date: January 29, 2026

At Sunsynk, we are committed to ensuring the security and integrity of our IoT-enabled solar power inverters, batteries, and related products. We recognize the importance of collaboration with the security research community to identify and address potential vulnerabilities. This Vulnerability Disclosure Policy outlines how to report security issues responsibly and how we handle such reports in compliance with applicable regulations, including the UK's Product Security and Telecommunications Infrastructure (PSTI) Act 2022.

Scope

This policy applies to all Sunsynk products with IoT capabilities, including but not limited to solar inverters, battery energy storage systems (BESS), and associated software or firmware. It covers vulnerabilities that could impact the confidentiality, integrity, or availability of our devices, such as unauthorized access, data exposure, or denial-of-service risks.

Out of scope: General product support issues, feature requests, or non-security-related bugs should be reported through our standard customer support channels at support@sunsynk.com.

How to Report a Vulnerability

We encourage responsible disclosure from users, security researchers, and third parties. To report a potential vulnerability:

1. **Contact Information:** Submit your report via email to our compliance team at compliance@sunsynk.com.
2. **Required Details:** Please provide as much information as possible to help us reproduce and assess the issue, including:
    - A clear description of the vulnerability and its potential impact.
    - Steps to reproduce the issue (e.g., affected product model, firmware version, and environment).
    - Any proof-of-concept code, screenshots, or logs (without exploiting live systems).
    - Your contact information for follow-up (optional if anonymous).

3. **Safe Harbor:** If you follow this policy in good faith and avoid actions that harm our users or systems we will not pursue legal action against you to the extent permitted by applicable law, including but not limited to the UK Product Security and Telecommunications Infrastructure (PSTI) Act 2022 and relevant data protection regulations. "Good faith" means conducting security research with the intent to improve the security of our products and services, promptly reporting vulnerabilities to us, and refraining from any activity that would intentionally disrupt, damage, or compromise our systems, data, or users. Actions that void this safe harbor include but are not limited to: unauthorized access to or modification of data, exfiltration or disclosure of confidential information, denial-of-service testing or any testing in production environments, or any activity that violates applicable laws or regulations. We ask that you:
    - Do not access or modify user data without permission.
    - Do not disrupt our services or test on non-test environments.
    - Give us reasonable time to respond before public disclosure.

Our Response Process

Upon receiving your report:

1. **Acknowledgment:** We will confirm receipt within 5 business days and provide a unique tracking ID.
2. **Triage and Validation:** Our security team will investigate and validate the issue within 14 business days. If more time is needed, we will notify you with an updated timeline.
3. **Remediation:** If confirmed, we will prioritize based on severity (using CVSS scoring where applicable) and develop a fix. Critical vulnerabilities will be addressed within 30 days; others within 90 days.
4. **Notification and Resolution:** We will inform you of the remediation plan and timeline. Once resolved, we may issue a security advisory on our website www.sunsynk.com and provide updates via affected product channels.
5. **5. Public Disclosure** We encourage coordinated (responsible) disclosure. You must not publicly disclose the vulnerability (or any details that could allow exploitation) until we have remediated the issue and provided written approval. We aim to complete remediation and grant approval for disclosure within 90 days of validation (or sooner for critical issues). We will generally credit you in

our public security acknowledgments, (if you wish and consent), unless you prefer to remain anonymous.

6. **Non-Validated Reports** If, after thorough investigation, we determine that the reported issue does not qualify as a valid security vulnerability (e.g., it is intended behaviour, out-of-scope, not reproducible, or poses no material security risk), we will notify you in writing within 15 business days of completing our investigation. The notification will include:

    a) A brief, non-confidential explanation of our reasoning.

    b) Any relevant technical details (where appropriate and without compromising security).

You are welcome to provide additional evidence or clarification, and we will promptly reconsider the report.

7. **Dispute Resolution** In cases of disagreement regarding the validity, severity rating (e.g., CVSS), or proposed remediation approach/timeline, we commit to the following collaborative process:
    a) We will arrange a discussion (via email, call, or video conference) between you and our security team to explain our assessment and carefully consider your input.
    b) We will make reasonable, good-faith efforts to reach a mutually acceptable resolution.
    c) If agreement cannot be reached after reasonable discussion, the final decision on validity, severity, and remediation rests with Sunsynk's security team.
    d) Upon your request, we will provide a written summary of the key rationale for our final determination (to the extent possible without disclosing sensitive internal information or creating additional legal risk).

Frivolous, abusive, or persistently unreasonable disputes may result in restricted future participation in our vulnerability disclosure programme.

Response Timelines

- Acknowledgment: Within 5 business days.
- Initial assessment: Within 14 business days.
- Fix for critical issues: Within 30 days.
- Fix for non-critical issues: Within 90 days.

- We aim to resolve all valid reports as quickly as possible and will communicate any delays.

Rewards and Recognition

While we do not currently offer a bug bounty program, we appreciate contributions and may provide recognition, swag, or other incentives at our discretion for significant findings.

Updates to This Policy

This policy may be updated periodically. Changes will be posted on our website with the effective date.

For questions about this policy, contact compliance@sunsynk.com.

By reporting vulnerabilities, you help us protect our users and contribute to a more secure energy ecosystem. Thank you for your support.

This policy is publicly available at www.sunsynk.com.

This policy is governed by and construed in accordance with the laws of England and Wales. Any disputes arising out of or in connection with this policy, including its interpretation, validity, or enforcement, shall be subject to the exclusive jurisdiction of the courts of England and Wales. This policy is intended to comply with the UK Product Security and Telecommunications Infrastructure (PSTI) Act 2022.