Vulnerability Disclosure Policy

1. Purpose

EGO Europe GmbH (hereinafter referred to as "the Organization") is committed to receiving, assessing and addressing cybersecurity vulnerability reports concerning its products with digital elements. This Policy describes our coordinated vulnerability disclosure process and supports our compliance with the applicable requirements of Regulation (EU) 2024/2847 (the "EU Cyber Resilience Act" or "CRA").

We are dedicated to continuously improving our products, focusing on evolving market demands, addressing emerging threats, and adapting to new attack vectors.

2. Scope

You may report a potential cybersecurity vulnerability found in the following products during use:

- Applications (APP) and products that can connect to APPs
- Products with diagnostic interfaces and their associated remotely controllable diagnostic tools

3. How to Report a Vulnerability

3.1 Submission Channel

Please do not send any issue information to us through insecure channels. Instead, vulnerability reports should be submitted via our **email**:

Product Security Incident Response Team Contact: psirt@egopowerplus.eu

If your report contains exploit code, access credentials, personal data or other sensitive information, please contact us first so that we can provide an appropriate secure transfer method.

This contact point is monitored by qualified personnel and is not limited to automated tools.

3.2 Report Content

Reporters should provide the following information to the extent possible for efficient triage:

- **Affected Product or App**: Exact name and version, firmware or software version (Essential)
- **Vulnerability Description**: A detailed description of the vulnerability and its potential impact
- **Steps to Reproduce**: Step-by-step instructions, including tools and environment details
- **Supporting Evidence**: Screenshots, network captures, logs, or Proof of Concept (PoC) code
- **Severity Assessment**: Recommended CVSS v3.1 or v4.0 score
- **Contact Information**: Email or other contact details for follow-up communication (Essential)

3.3 Security Research Guidelines

When conducting security research or testing, please:

- avoid accessing, copying, altering or deleting data belonging to other users;
- do not use social engineering, phishing, denial-of-service attacks, physical attacks or other methods that may disrupt our products, services or users;
- limit testing to what is reasonably necessary to confirm and document the vulnerability;
- stop testing and notify us promptly if you access personal data, credentials, confidential information or systems beyond the intended scope; and
- do not publicly disclose the vulnerability before we have had a reasonable opportunity to investigate and remediate it, subject to applicable law.

This Policy does not authorize conduct that is unlawful or otherwise exceeds the access permissions granted to you.

4. Vulnerability Handling Process

The Product Security Incident Response Team (PSIRT) will conduct the vulnerability assessment and risk evaluation upon receiving a vulnerability report. Verified vulnerabilities will be remediated and disclosed, with necessary communication maintained with the reporter. If the vulnerability is confirmed to reside in an upstream component, PSIRT will notify the supplier.

Prior to any public disclosure, both parties should reach agreement on the following:

- Disclosure date
- Content of any public announcement or statement

- Embargo period required to protect users

5. Confidentiality

The Organization will keep vulnerability reports confidential and will not share the reporter's personal information with third parties without explicit consent, except as required by law.

Reporters may also remain anonymous; however, anonymity may limit the Organization's ability to provide follow-up communication.

6. Acknowledgment

{ Organization / Individual }

7. Fixed Vulnerability Disclosure

Vulnerability ID / Vulnerability	Impact	Affected Product(s)	Severity	Recommendations
No fixed vulnerabilities on record				