# Policy för sårbarhetsrapportering

## 1. Syfte

**EGO Europe GmbH** (nedan kallad "Organisationen") åtar sig att ta emot, bedöma och hantera rapporter om cybersäkerhetssårbarheter avseende sina produkter med digitala element. Denna policy beskriver vår samordnade process för sårbarhetsrapportering och stödjer vår efterlevnad av tillämpliga krav i förordning (EU) 2024/2847 ("EU:s cyberresiliensakt" eller "CRA").

Vi är engagerade i att kontinuerligt förbättra våra produkter genom att fokusera på förändrade marknadskrav, hantera nya hot och anpassa oss till nya attackvektorer.

## 2. Omfattning

Du kan rapportera en potentiell cybersäkerhetssårbarhet som upptäckts i följande produkter under användning:

- Applikationer (APP) och produkter som kan anslutas till APP:ar
- Produkter med diagnosgränssnitt och tillhörande fjärrstyrbara diagnosverktyg

## 3. Hur du rapporterar en sårbarhet

### 3.1 Rapporteringskanal

Skicka inte information om ett problem till oss via osäkra kanaler.

Sårbarhetsrapporter bör i stället skickas via vår **e-post**:

Säkerhetskontakt: psirt@egopowerplus.eu

Om din rapport innehåller exploateringskod, åtkomstuppgifter, personuppgifter eller annan känslig information ber vi dig kontakta oss först så att vi kan tillhandahålla en lämplig säker överföringsmetod.

Denna kontaktpunkt övervakas av kvalificerad personal och är inte begränsad till automatiserade verktyg.

### 3.2 Rapportens innehåll

Rapportörer bör i möjligaste mån lämna följande information för en effektiv prioritering:

- **Berörd produkt eller app**: exakt namn och version, firmware- eller programvaruversion (obligatoriskt)
- **Beskrivning av sårbarheten**: en detaljerad beskrivning av sårbarheten och dess potentiella påverkan
- **Steg för att återskapa**: steg-för-steg-instruktioner, inklusive verktyg och miljödetaljer
- **Stödjande bevis**: skärmdumpar, nätverksinspelningar, loggar eller Proof of Concept (PoC)-kod
- **Allvarlighetsbedömning**: rekommenderad CVSS v3.1- eller v4.0-poäng
- **Kontaktuppgifter**: e-post eller andra kontaktuppgifter för uppföljning (obligatoriskt)

### 3.3 Riktlinjer för säkerhetsforskning

Vid genomförande av säkerhetsforskning eller testning ber vi dig att:

- undvika att komma åt, kopiera, ändra eller radera data som tillhör andra användare;
- inte använda social manipulation, nätfiske, överbelastningsattacker, fysiska attacker eller andra metoder som kan störa våra produkter, tjänster eller användare;
- begränsa testningen till vad som rimligen krävs för att bekräfta och dokumentera sårbarheten;
- avbryta testningen och omedelbart meddela oss om du får åtkomst till personuppgifter, autentiseringsuppgifter, konfidentiell information eller system utanför avsett omfång; och
- inte offentliggöra sårbarheten innan vi har haft en rimlig möjlighet att undersöka och åtgärda den, med förbehåll för tillämplig lag.

Denna policy tillåter inte olagligt agerande eller agerande som går utöver de åtkomsträttigheter som beviljats dig.

## 4. Process för hantering av sårbarheter

Product Security Incident Response Team (PSIRT) kommer att genomföra sårbarhetsbedömning och riskutvärdering efter mottagande av en sårbarhetsrapport. Bekräftade sårbarheter kommer att åtgärdas och offentliggöras, med nödvändig kommunikation upprätthållen med rapportören. Om sårbarheten bekräftas finnas i en uppströmskomponent kommer PSIRT att meddela leverantören.

Innan något offentliggörande sker bör båda parter nå en överenskommelse om följande:

- Datum för offentliggörande
- Innehåll i eventuellt offentligt tillkännagivande eller uttalande
- Karensperiod som krävs för att skydda användarna

## 5. Konfidentialitet

Organisationen kommer att behandla sårbarhetsrapporter konfidentiellt och kommer inte att dela rapportörens personuppgifter med tredje part utan uttryckligt samtycke, förutom när det krävs enligt lag.

Rapportörer kan också förbli anonyma; anonymitet kan dock begränsa Organisationens möjlighet att tillhandahålla uppföljande kommunikation.

## 6. Erkännande

**{ Organisation / Individ }**

## 7. Åtgärdade sårbarheter

| Sårbarhets-ID/Sårbarhet | Påverkan | Berörd(a) produkt(er) | Allvarlighetsgrad | Rekommendationer |
|---|---|---|---|---|
| *Inga åtgärdade sårbarheter registrerade* | | | | |