# POJAZDY SZYNOWE PESA BYDGOSZCZ S.A. COORDINATED VULNERABILITY DISCLOSURE POLICY

## Introduction and legislative base

The purpose of this policy is to establish the principles and procedures for the secure reporting, receiving, analysis, coordination, and disclosure of vulnerability information relating to the products of **Pojazdy Szynowe PESA Bydgoszcz S.A.** This policy defines vulnerability management procedures, ensuring compliance with the **essential requirements** set out in **Annex I of the Cyber Resilience Act (CRA)**.

This policy constitutes a cornerstone of the cybersecurity strategy of **Pojazdy Szynowe PESA Bydgoszcz S.A.**, reflecting the company's commitment to fully implementing all relevant regulatory requirements by the end of 2027. The company's activities are based on internationally recognized standards, particularly the **IEC 62443 series**, ensuring a systematic approach to the protection of users and digital infrastructure.

## Scope of the policy

Polityka obejmuje wszystkie „produkty z elementami cyfrowymi" (sprzęt i oprogramowanie z możliwością komunikacji) wprowadzane do obrotu pod marką PESA.

This policy includes every „product with digital elements" (hardware and software with communication capabilities) that are placed on the market under the PESA brand

## Vulnerability disclosure procedure

Any identified vulnerabilities shall be reported directly to the **Cybersecurity Team** and/or to **CSIRT NASK**. **Pojazdy Szynowe PESA Bydgoszcz S.A.** commits not to take legal action against security researchers who act in good faith and comply with the principles set forth in this policy (**Safe Harbor**).

e-mail: csirt@pesa.pl

Phone number: +48 882 477 302

- **Encryption:** Due to the sensitive nature of the information involved, **Pojazdy Szynowe PESA Bydgoszcz S.A.** requires vulnerability reports to be encrypted (a **PGP key** is available upon request).
- Required information
    - Device model and serial number.
    - Firmware or application version.
    - Detailed technical description and steps to reproduce the issue (Proof of Concept (PoC))
- **Security requirements:** We accept only textual descriptions and screenshots in secure formats (**PNG/JPG**). Submission of executable files is prohibited.
- **Anonymous reporting:** Anonymous vulnerability reports are accepted

## PSIRT (Product Security Incident Response Team) Handling and Coordination Process

The **Cybersecurity Team** is responsible for coordinating remediation activities in accordance with the following process:

1. **Acknowledgement:** Formal acknowledgement of receipt of the vulnerability report within **48 hours**
2. **Verification and Classification:** Assessment of the vulnerability severity using the **Common Vulnerability Scoring System (CVSS)**
3. **Remediation Development:** Engineering efforts to develop a software update, patch, or an appropriate workaround.
4. **Testing and Release:** Validation of the effectiveness of the remediation measures and their official distribution.
5. **Customer Notification:** Publication of an official **Security Advisory** informing customers of the vulnerability and the available remediation measures.

## Zobowiązania producenta w ramach CRA

As a responsible manufacturer, **PESA** fulfills the requirements of the **Cyber Resilience Act (CRA)** through the following measures:

- **Vulnerability Reporting:** Proactively reporting exploited vulnerabilities to **ENISA** within the required timeframes.
- **Security by Design:** Applying the **IEC 62443-4-1** standard throughout the product development lifecycle and implementing security capabilities in accordance with **IEC 62443-4-2**.

- **Documentation:** Providing clear and comprehensive instructions for secure configuration and operation to minimize risks on the user side

## Rules of collaboration (Safe Harbor)

The organization will not initiate legal action against individuals conducting security research in good faith and in accordance with this policy within the scope of systems, products, and services under PESA's control. To maintain **Safe Harbor** status, researchers must comply with an information disclosure embargo for a period of up to **90 days** from the date the vulnerability is reported until its public disclosure. During this period, the researcher is required to maintain confidentiality, allowing **PESA** sufficient time to develop, test, and deploy an appropriate remediation before public disclosure of the vulnerability.

## Access to updates and communication

Official security communications are published in the **"Security Advisories"** section of the company's website. For **legacy products** whose hardware specifications do not allow full compliance with the new **Cyber Resilience Act (CRA)** requirements, **PESA** ensures transparency by publishing **End-of-Support Statements** with adequate advance notice and by offering appropriate replacement solutions where applicable.

## Contact and Administrative Details

Dedicated communication channel for informing about vulnerabilities:

E-mail: csirt@pesa.pl

Telephone: +48 882 477 302