

ANNEX 6 – PRIVACY POLICY

RESPONSIBLE DISCLOSURE POLICY

1. Introduction

Yusen Logistics Healthcare Group (“we,” “us,” “our”) is committed to the security and integrity of our systems, products, and services, and to protecting user privacy in line with European data protection laws. We encourage responsible reporting of potential vulnerabilities. This policy outlines our expectations and process for responsible disclosure.

2. Reporting

2.1. How to Report

If you believe you have identified a security vulnerability in a Yusen Logistics Healthcare Group product or service (including connected devices such as the Walden Box), please email: ylh.security@eu.yusen-logistics.com

2.2. Information to Include

Please provide:

- Steps to reproduce
- Technical details
- Potential impact
- Suggested remediation (optional)

Avoid including personal data unless strictly necessary.

Any personal data submitted will be processed under GDPR Article 6(1)(f) (legitimate interest in securing our systems).

2.3. Acknowledgement

We will acknowledge your report within **5 working days** and follow up as needed.

2.4. Resolution Timeline

Timelines depend on severity and complexity.

We aim to resolve significant vulnerabilities within **90 days**, where feasible

3. Communication

3.1. Non-Disclosure

Please do not disclose the vulnerability until Yusen Logistics Healthcare Group has had reasonable time to investigate and address it.

3.2. Responsible Conduct

Please refrain from exploiting vulnerabilities, accessing personal data, or causing disruption to services. Testing should not impact system availability.

3.3. Third-Party Components

If a vulnerability concerns a third-party component, we may coordinate with the relevant supplier.

4. Recognition

Development date 16-02-2026

Yusen Logistics Healthcare Group does not offer monetary rewards or bug bounty payments. With your explicit consent, we may acknowledge your contribution internally or publicly. You may opt out at any time, and you may remain anonymous if you choose; we will not seek to identify you.

5. Safe Harbor

If you act in good faith, comply with this policy and applicable laws, Yusen Logistics Healthcare Group will not initiate legal action regarding your research.

This Safe Harbor does not apply to actions involving intentional damage, data exfiltration, or service disruption.

Please avoid including personal data in your report unless necessary. Any personal data provided will be used solely to assess and resolve the vulnerability, retained only for the duration of the investigation, and handled in accordance with GDPR and our Data Privacy Policy.

We appreciate all researchers who contribute to the security and reliability of our systems.