Product Vulnerability Disclosure Policy

1 Purpose

This policy defines how Dukosi receives, assesses, and responds to reported product security vulnerabilities from external parties.

The objective of this policy is to:

- Provide a clear and secure mechanism for reporting vulnerabilities
- Ensure consistent, timely, and risk-based handling of reported issues
- Support compliance with applicable regulations, including the EU Cyber Resilience Act (CRA)
- Promote responsible disclosure and collaboration with security researchers

2 Scope

This policy applies to:

- All Dukosi products and product deliverables, including:
  - Embedded software and firmware executed on Dukosi hardware
  - Customer-integrated software components provided for use within customer systems
  - Product communication mechanisms and interfaces
  - Security-relevant product features (for example, cryptography, authentication, debug access)
- All externally reported product security vulnerabilities
- All individuals or organizations reporting vulnerabilities to Dukosi

2.1 Out of Scope

This policy does not apply to:

- Internal vulnerability discovery: vulnerabilities identified through Dukosi's own internal security review, development, or testing activities are handled through Dukosi's internal vulnerability management process, not this policy
- IT infrastructure and website vulnerabilities: vulnerabilities affecting Dukosi's corporate IT systems, internal networks, or website (as distinct from Dukosi products) are handled separately. Please report these to support@dukosi.com rather than to psirt@dukosi.com
- Third-party components outside Dukosi's responsibility: vulnerabilities in third-party software or components are out of scope unless they affect the security of a Dukosi product or deliverable. If you believe a third-party component affects a Dukosi product, please report it to us and we will determine applicability; otherwise, we recommend reporting directly to the relevant third-party vendor

2.2 Scope Clarification

A vulnerability is considered in scope if it:

- Affects the security of a Dukosi product or deliverable, or
- Could impact customers or downstream systems through product usage

For customer-integrated software components:

- Dukosi is responsible for vulnerabilities within the software provided
- Customers are responsible for the security of their system environment and integration

3 Policy Statement

3.1 General Principles

Dukosi shall provide a mechanism for external parties to report product security vulnerabilities in a responsible and secure manner.

Dukosi shall handle all vulnerability reports in a consistent, risk-based, and timely manner.

Dukosi shall treat all reporters respectfully and shall not take legal action against individuals who:

- Act in good faith
- Follow this policy
- Do not exploit vulnerabilities beyond what is necessary to demonstrate the issue

3.2 Vulnerability Reporting Mechanism

Dukosi shall provide a publicly accessible vulnerability reporting channel.

The reporting mechanism shall:

- Allow submission of vulnerability details securely
- Support confidential communication with the reporter
- Include guidance on the information required to support investigation

Where appropriate, Dukosi provides:

- An email-based reporting channel (psirt@dukosi.com)
- Support for encrypted communication (PGP key)

3.3 Information Requirements

Vulnerability reports should include where possible:

- Description of the vulnerability
- Affected products and versions
- Steps to reproduce the issue
- Potential impact
- Proof-of-concept or supporting evidence

3.4 Acknowledgement and Communication

Dukosi will acknowledge receipt of a vulnerability report and aim to respond promptly.

Dukosi shall:

- Maintain communication with the reporter throughout the investigation
- Provide status updates where appropriate
- Notify the reporter when the issue has been resolved or mitigated

Response times may vary depending on the complexity of the issue, availability of reproduction information, and potential impact and risk.

3.5 Vulnerability Assessment and Handling

All reported vulnerabilities shall be:

- Assessed using a risk-based approach (CVSS or equivalent)
- Managed through Dukosi's internal, risk-based vulnerability management process
- Tracked to resolution with appropriate traceability

3.6 Disclosure and Remediation

Dukosi shall:

- Determine appropriate remediation actions based on risk
- Communicate relevant information to affected customers
- Support coordinated disclosure where appropriate

Public disclosure shall be:

- Coordinated with affected stakeholders
- Performed only after mitigation or agreed timelines

3.7 Regulatory Reporting

Where a reported vulnerability meets regulatory requirements, Dukosi shall ensure reporting is performed in accordance with applicable regulations, including the EU Cyber Resilience Act (CRA).

3.8 Prohibited Activities

The following activities are not permitted under this policy:

- Exploitation of vulnerabilities beyond proof-of-concept
- Accessing, modifying, or deleting customer or production data
- Disruption of services or systems
- Violation of applicable laws or regulations

3.9 References

Dukosi's approach to coordinated disclosure follows the principles set out in the CERT® Guide to Coordinated Vulnerability Disclosure.

4 Roles and Responsibilities

4.1 Dukosi

Dukosi shall:

- Maintain a vulnerability reporting channel
- Assess and manage reported vulnerabilities
- Communicate with reporters and stakeholders
- Ensure compliance with regulatory obligations

4.2 Reporter

Individuals reporting vulnerabilities are expected to:

- Act in good faith
- Avoid causing harm or disruption
- Provide sufficient information to support investigation
- Allow reasonable time for remediation before public disclosure

5 Compliance

Failure to comply with this policy may result in:

- Delayed or rejected vulnerability handling
- Escalation through legal or regulatory channels where appropriate

6 Review and Maintenance

This policy shall be reviewed periodically and updated to reflect:

- Changes in regulatory requirements
- Updates to Dukosi products or processes
- Lessons learned from vulnerability handling activities

7 Revision History

Table 1: Revision History

Revision	Description	Updated by	Date
1	First Issue	Francis Bain	13th August 2026
2	Updated out of scope email address.	Máté Zámori	17th August 2026

Distribution and Confidentiality

Material presented here may not be copied, reproduced, modified, merged, translated, stored or used without prior consent from the copyright owner. All products and groups mentioned are trademarks or registered trademarks of their respective organizations.

Information presented here by Dukosi Limited is believed to be correct and accurate. Dukosi Limited shall not be liable to any recipient or third part for any damages, including (but not limited to) personal injury, property damage, loss of profits, loss of business opportunity, loss of use, interruption of business, or indirect, special, incidental or consequential damages of any kind in connection with, or arising from, the use or performance of the data herein.

No obligation or liability to the recipient or third party shall arise from Dukosi Limited providing technical or other services.

Contact Dukosi

www.dukosi.com

support@dukosi.com