EU Cyber Resilience Act (CRA) Readiness Statement

1. Purpose

This statement outlines how ADLINK prepares and operates its product development and security processes in alignment with the EU Cyber Resilience Act (CRA) for products supplied to the European Union market. It aims to provide transparency into our cybersecurity practices, governance, and ongoing readiness activities.

2. Scope of Products

The CRA applies to products with digital elements placed on the EU market. Within ADLINK, this may include industrial PCs, embedded boards, computer-on-modules, firmware, BIOS, BMC, device drivers, and pre-installed operating system images. Each product family is assessed to determine CRA applicability and classification.

3. CRA Compliance Responsibility and ADLINK's Role

Under the EU Cyber Resilience Act, the primary compliance obligation lies with the manufacturer of the end product placed on the EU market.

ADLINK typically acts as a platform, module, or system supplier, supporting our customers—who are the end product manufacturers—in meeting their CRA obligations. To enable this, ADLINK ensures that its product development activities, cybersecurity processes, and technical measures are aligned with recognized international standards, particularly IEC 62443-4-1 (Secure Product Development Lifecycle).

4. Security-by-Design and Secure Development

ADLINK applies security-by-design and security-by-default principles throughout the product lifecycle. This includes a secure development lifecycle (SDLC), cybersecurity risk assessments, secure coding practices, code review, security testing, and controlled change management.

Our development processes are aligned with IEC 62443-4-1 and supported by an ISO/IEC 27001-certified information security management system.

5. Software and Supply Chain Security

ADLINK manages third-party and open-source software risks through component identification, supplier risk evaluation, and Software Bill of Materials (SBOM) generation using recognized formats (e.g., SPDX, CycloneDX). SBOMs can be provided to customers upon request, subject to applicable contractual and regulatory terms.

6. Vulnerability Management and Coordinated Disclosure

ADLINK operates a structured vulnerability management process supported by a Product Security Incident Response Team (PSIRT). This process covers vulnerability intake, impact analysis, remediation planning, coordinated disclosure, and customer communication, supporting customers' CRA vulnerability handling and reporting obligations.

7. Secure Updates and Product Lifecycle Support

ADLINK designs its products to support secure software and firmware updates, including integrity protection and controlled distribution mechanisms.

In alignment with CRA expectations, ADLINK commits to providing security updates and vulnerability fixes throughout the defined support period of the product, enabling customers to maintain compliance during the product's operational lifecycle. Product support periods and end-of-life policies are defined and communicated transparently.

8. Governance and Continuous Improvement

CRA readiness is supported by internal governance involving engineering, product management, quality, and security functions, with management oversight. ADLINK continuously improves its cybersecurity practices based on risk assessments, audits, regulatory guidance, and evolving threat landscapes.

9. Current Status and Roadmap

ADLINK has obtained ISO/IEC 27001:2022 and IEC 62443-4-1 certifications, demonstrating alignment of its development processes with key CRA principles. ADLINK will continue to monitor CRA implementation acts and guidance and adapt its processes accordingly to support customers' ongoing compliance needs.

10. Contact Information

Product Security: Mr. Fencer Kao at fencer.kao@adlinktech.com

Information Security/Cybersecurity: Mr. Felix Ho at felix.ho@adlinktech.com

11. Legal Disclaimer

• Informational Purpose Only: This document is provided for informational purposes to describe ADLINK's cybersecurity readiness and does not constitute a legal guarantee, warranty, or contractually binding commitment regarding the compliance of any specific product.

• Customer Responsibility: Under the EU Cyber Resilience Act, the legal responsibility for the conformity of the end product—including the assessment of all components—remains solely with the manufacturer who places that product on the EU market.

• Scope of Support: ADLINK's support for customer compliance is limited to the provision of available technical documentation, such as SBOMs, and the maintenance of security updates during the product's defined support period.

• Regulatory Evolution: The information provided reflects ADLINK's understanding of the CRA as of the date of issuance. As implementing acts and official EU guidance continue to emerge, ADLINK reserves the right to update its processes and this statement accordingly.

• No Third-Party Liability: This statement does not create any third-party beneficiary rights for the customer's end-users or any other third parties.

簽署人：
Yi-Nan Chen
5BF01831369F40E...

2/23/2026

Mannheim,
Germany

Mr. Yi-Nan Chen
Managing Director
ADLINK Technology GmbH