Portwell
No. 242, Bo'ai St., Shulin Dist., New Taipei City 238005, Taiwan Tel: +886-2-7731-8888 Fax:+886-2-7731-9888 www.portwell.com.tw info@portwell.com.tw

Portwell's Commitment to EU Cyber Resilience Act (CRA) Compliance

Taipei, Taiwan — August 26, 2026 — As a global provider of industrial computing and embedded computing solutions, Portwell, Inc. continues to closely monitor the evolving cybersecurity regulatory landscape and industry standards. In preparation for the implementation of the European Union Cyber Resilience Act (Cyber Resilience Act, CRA), Portwell has proactively initiated a series of cybersecurity readiness activities.

The cybersecurity requirements under the Cyber Resilience Act (CRA) encompass various stages throughout the lifecycle of digital products. To address these requirements, Portwell is establishing a systematic and sustainable product cybersecurity management and development framework. As IEC 62443-4-1, an internationally recognized cybersecurity standard for industrial automation and control systems, establishes specific requirements for a Secure Product Development Lifecycle, Portwell will adopt IEC 62443-4-1 as an important foundation for establishing and enhancing its product cybersecurity management framework and operational processes. Portwell is currently progressing toward third-party IEC 62443-4-1 certification.

By building upon the Secure Product Development Lifecycle established through IEC 62443-4-1, Portwell is strengthening its ability to systematically and effectively implement the processes and practices required by the CRA. Through close collaboration with suppliers and technology

partners, Portwell is progressively addressing applicable CRA requirements while continuing to deliver secure, reliable, and trusted products and solutions to its customers.

Integrating Product Cybersecurity into the Development Process

Portwell has long maintained rigorous quality management and product development processes. Building upon this foundation, Portwell is further integrating product cybersecurity requirements and risk considerations into its existing development processes, establishing cybersecurity capabilities from the earliest stages of product design.

Product cybersecurity requirements are being systematically incorporated throughout the product development lifecycle, covering overall product security architecture, secure development processes, personnel competency and qualification management, security documentation management, development environment security controls, and the definition and review of product security requirements.

Portwell also takes into consideration customer and market security requirements, as well as each product's intended use, operating environment, and lifecycle, to conduct appropriate cybersecurity risk assessments and implement corresponding security measures. Through a well-managed development process, Portwell continues to strengthen product security testing, verification, and documentation to ensure that cybersecurity requirements are effectively addressed throughout product design, development, verification, and release.

Extending Product Cybersecurity Management Throughout the Product Lifecycle

For Portwell, product cybersecurity is not a one-time certification or regulatory compliance exercise. It is a long-term commitment that extends throughout the entire product lifecycle.

Cybersecurity issue tracking during product design and development, post-release security updates and vulnerability management, and the handling of product security issues reported by customers are all integral parts of Portwell's product lifecycle management.

Portwell will also continue to work closely with suppliers and technology partners to establish and enhance Software Bills of Materials (SBOMs), improving the identification, transparency, and traceability of software components. At the same time, Portwell continues to strengthen its capabilities for vulnerability identification, assessment, remediation, documentation, and communication to effectively maintain product cybersecurity and resilience throughout the product lifecycle.

When vulnerabilities or significant cybersecurity incidents that may affect product security are identified, Portwell will assess and address them through established vulnerability management, disclosure, and regulatory reporting processes. In accordance with applicable CRA requirements, Portwell will carry out the necessary reporting and customer communications concerning actively exploited vulnerabilities and severe security incidents, with the objective of minimizing potential risks and impacts on customer operations.

Providing Customers with Secure, Reliable, and Trusted Products

Portwell products are widely deployed as computing platforms and key components within a broad range of systems, including industrial automation equipment, medical systems, networking and communication solutions, edge computing platforms, and other mission-critical applications.

Portwell recognizes that product cybersecurity and CRA compliance cannot be achieved by a single company alone. They require close collaboration and shared responsibility across the entire technology supply chain.

As an important part of its CRA readiness program, Portwell will continue to enhance the product security information, technical documentation, vulnerability management mechanisms, and product lifecycle support provided to customers and technology partners, helping them address the cybersecurity and regulatory requirements applicable to their end products and solutions.

Looking ahead, Portwell will continue to closely monitor developments related to the EU Cyber Resilience Act, applicable standards, and international cybersecurity best practices. Portwell will continuously enhance its product development processes, cybersecurity management mechanisms, and customer support capabilities as it progresses toward meeting applicable CRA requirements and delivering more secure, reliable, and resilient industrial computing platforms to customers worldwide.

Disclaimer: CRA applicability and conformity assessment requirements may vary depending on product type, product configuration, software, intended use, and the role of each Economic Operator in the final solution. Portwell's CRA readiness and compliance activities are ongoing. Any planned certifications, assessments, and compliance milestones referenced herein remain subject to the successful completion of the applicable audit, assessment, and implementation processes. This statement is intended for general informational purposes only and should not be construed as a certification, warranty, guarantee, or legal representation of compliance with the Cyber Resilience Act (CRA) for any specific product.