Emerson Statement on the EU Cyber Resilience Act (CRA)

Strengthening Trust Through Secure by Design Innovation

At Emerson, our customers rely on us to deliver automation technologies that are engineered for performance, reliability, and security. Cybersecurity is an essential part of that commitment. As regulatory expectations continue to evolve, we support the European Union's Cyber Resilience Act (CRA) as an important framework for strengthening the security of products with digital elements placed on the EU market.

We recognize the CRA's role in improving the protection of industrial systems and critical infrastructure. Emerson is incorporating the CRA's requirements into our product development, engineering, and support processes so that our solutions remain secure throughout their lifecycle, ensuring our technologies help enable safer, more resilient operations around the world.

Our Approach to CRA Implementation

Monitoring the Regulatory Landscape

Emerson continuously monitors EU policy developments, including the CRA's implementation roadmap and related guidance. This proactive stance ensures early visibility into obligations and timelines, such as:

- CRA reporting requirements coming into force on 11 September 2026, and
- Full regulatory applicability, including CE marking, beginning 11 December 2027.

We also track adjacent frameworks, including NIS2 and EU cybersecurity certification schemes, to ensure interoperability and avoid duplicated or conflicting obligations.

Embedding CRA Requirements into Emerson's Cybersecurity Framework

Emerson has established incident-response processes designed to detect, triage, and respond to cybersecurity incidents in a timely manner. These processes include defined escalation paths, decision making authority, and communication procedures to support compliance with applicable incident notification and reporting obligations, including those introduced by NIS2.

Secure Development and Engineering Practices

Emerson is integrating CRA requirements directly into our existing secure development lifecycle practices. This includes strengthening our alignment with industry standards such as **IEC 62443**, used throughout our automation portfolio.

Multiple Emerson brands and products are supported by externally validated certifications of their secure development lifecycle (e.g., **IEC 62443-4-1**) and/or product technical cybersecurity requirements (e.g., **IEC 62443-4-2** or **3-3**).

Emerson incorporates structured secure by design and secure by default principles into our development practices to:

- Ensure threat identification, misuse-case assessment and security control selection is embedded early in the design;
- Integrate security requirements into system architectures and product specifications, including hardened default configurations, access controls and data protection; and
- Design default configurations and architectures to reduce exposure (e.g., via segmentation and layered defenses) aligned with defense-in-depth and **IEC 62443**.

Product Security Throughout the Lifecycle

Continuous Vulnerability Management

Emerson maintains dedicated security personnel who monitor and analyze product-related vulnerabilities and issues- reviewing newly identified concerns and issuing timely advisories, mitigations, or updates when appropriate.

When necessary, Emerson may report vulnerability and incident information to governments (e.g., US CISA or EU ENISA) or publicly. Reporting responsibilities rest with Emerson's **Product Security Incident Response Team (PSIRT)**, in coordination with Legal and Regulatory/Compliance teams, ensuring accuracy, completeness, and traceability.

Customers will continue to receive updates via Security Notifications, service bulletins, and direct communication channels. Vulnerability assessment is integrated into Emerson lifecycle security services where applicable.

Secure Updates and Digital Distribution

Emerson delivers firmware, software, and documentation through authenticated, encrypted portals such as **MySoftware**, with published cryptographic hashes to allow customers to validate integrity.

Our digital platforms enforce modern transport security, including portal level enforcement of **TLS 1.2+** and deactivation of outdated protocols.

Operational Hardening and Network Security

Emerson offers device hardening and monitoring capabilities in applicable product environments. See product or system component details for more information about availability.

User Information and Transparency

Emerson provides product specific cybersecurity information, including secure installation and configuration guidance, security hardening recommendations, network architecture guidance and incident/vulnerability response contact points to help our customers use our products securely and meet their cybersecurity objectives. Our websites and digital portals provide up-to-date support resources, cybersecurity advisories, and vulnerability-related notices for our products.

Supply Chain and Third-Party Security

Recognizing the impacts of supply chain risk, Emerson applies due-diligence and security assurance practices to suppliers and service providers that support our products and product development activities. This includes evaluating the security maturity of our third-party providers and their components and incorporating security expectations into contractual arrangements where appropriate.

Cyber Resilience Act

Governance and Oversight
Stewardship for CRA compliance sits with Emerson's **Director of Product Security and CTO**, supported by Product Management, R&D, IT/OT Operations, and Legal/Compliance.

Product security is treated as an ongoing program, not a one-time activity. In addition to the EU CRA preparedness activities, Emerson continues to monitor for other regulatory guidance and requirements issued by jurisdictions globally and adjust our internal controls, documentation and processes accordingly.

This Statement will be reviewed annually, or earlier if CRA implementing acts or harmonized standards evolve.

Our Position Moving Forward
Emerson is committed to meeting all applicable CRA requirements ahead of enforcement timelines. We view the CRA not merely as regulation, but as an opportunity to further strengthen the cybersecurity posture of the industrial ecosystem, reinforce customer trust, and ensure our technologies continue to support safe, resilient operations.

Emerson
8027 Forsyth Blvd.
St. Louis, MO 63105
www.Emerson.com