# Schneider Electric's approach to digital policy implementation

## A focus on the Cyber Resilience Act (CRA)

At Schneider Electric, trust is the cornerstone of our business, with cybersecurity being one of its fundamental pillars. We are committed to upholding a strong cybersecurity posture across Schneider Electric and our value chain. By focusing on growing resilience, building trust, and continuously improving our cybersecurity posture, compliance is an outcome of our approach.

Schneider Electric recognizes that every nation has the duty and right to protect its critical infrastructure and citizens from cyberattacks, necessitating the creation of enforceable cybersecurity regulations, guidelines, and frameworks. We embrace these regulations and respond with transparency and alignment. Our commitment to compliance with applicable digital policies and alignment with international cybersecurity standards and best practices reflect our dedication to cybersecurity and to safeguarding the data and privacy of our employees, partners, and customers. We continually strive to ensure that compliance arises from a robust cybersecurity posture that goes beyond a mere compliance-driven approach.

### Approach to the regulatory landscape

Schneider Electric actively engages in the policymaking process from the outset, collecting intelligence and leveraging relationships with government authorities and trade associations to ensure early detection of emerging policies. Detailed impact analyses of key digital policies are then conducted and findings communicated internally to prepare for implementation. By anticipating developments and collaborating with policymakers and trade associations throughout the policy lifecycle, Schneider Electric maintains a comprehensive view of the global policy landscape, focusing on interoperability and mutual recognition of regulations and policies wherever possible.

## Understanding the Cyber Resilience Act

Cybersecurity is a major challenge for the European Union (EU) due to the increasing number of connected devices and the impact of cyberattacks on the EU market and critical infrastructure. To address this, the EU aims to strengthen its cybersecurity approach by creating a uniform legal framework for essential cybersecurity requirements for products with digital elements. The CRA is an EU regulation aimed at enhancing the cybersecurity of products with digital elements. This includes both hardware and software products that are connected directly or indirectly to another device or network. It introduces mandatory cybersecurity requirements for manufacturers and retailers, covering the entire lifecycle of these products.

### The CRA addresses two main challenges:

1. The low level of cybersecurity in digital products
2. The insufficient information available to users to make informed choices

The CRA seeks to ensure that digital products are developed with fewer vulnerabilities and that manufacturers prioritize security throughout the product lifecycle. The CRA will be applicable from 11th of December 2027, with an exception for reporting requirements which will be applicable as of the 11th of September 2026.

## Cyber Resilience Act at Schneider Electric

As a global leader in energy management and industrial automation, Schneider Electric's products, hardware and software, serve a wide range of sectors and environments. Schneider Electric welcomes the EU's objective to establish the baseline level of cybersecurity of products with digital elements placed on the EU market by defining essential cybersecurity requirements.

As part of its digital policy strategy, Schneider Electric actively engages with authorities in the development of standards to ensure that requirements are pragmatic and contribute to the overall cybersecurity capacity building of all stakeholders. Schneider Electric has been actively involved in the CRA's legislative process as well as in the current implementation roadmap of the European Commission (notably with the expected implementing act on the technical descriptions of important and critical products).

1. At Schneider Electric, we take a structured and forward-looking approach to regulatory compliance in product cybersecurity, ensuring alignment with both existing and emerging regulatory frameworks. Our strategy is deeply integrated into our scalable R&D and industrial playbooks, enabling a robust compliance process that evolves with industry advancements. The first step is evaluation, where we map requirements to internal initiatives from our cybersecurity roadmap as well as common cybersecurity standards such as IEC 62443. A key element of this standard is guidance on a secure development lifecycle (SDL), which includes steps like threat modeling, secure design, security testing, security requirements, vulnerability management, secure guidelines, and privacy reviews. This process can be externally validated through certification, and many concepts from the standard can also be found in the CRA.
2. The second step is the adherence to essential regulatory requirements, which serve as the backbone of our approach. Rather than reinventing the wheel for each new regulation, we leverage these fundamental principles as a unique referential framework. This ensures consistency, efficiency, and scalability in our security compliance processes. These requirements must remain adaptable, encompassing not only traditional industrial security but also broader domains such as cloud computing, edge architectures, data protection, and privacy.
3. The third step is conducting internal and external gap assessments to ensure alignment and robustness in our regulatory impact assessment. Schneider Electric's secure development lifecycle process is certified according to the IEC 62443-4-1 standard. Additionally, our vulnerability management procedure meets the requirements of IEC 29147 and IEC 30111 standards. Furthermore, our penetration testing lab holds CREST certification.

Compliance cannot exist in isolation. Therefore, Schneider Electric actively promotes a collaborative approach and participates in standardization bodies that promote harmonization of standards to achieve broader compliance. One example of this is our active engagement in CEN-CENELEC's Special Working Group on the CRA (JTC13 WG9), which has been mandated by the European Commission to develop harmonized standards to facilitate conformity assessments of digital products against the CRA's essential requirements. This work is important as these harmonized standards will become industry best practices for implementation and conformance with the CRA.

As the technology policy landscape continuously evolves, Schneider Electric closely monitors emerging trends and regulations worldwide. Our approach focuses on anticipation, impact analysis, and external and engagement, all of which are done in close coordination with internal stakeholders. These efforts ensure that we keep up with the growing body of digital policies, such as the UK Product Security and Telecommunication Infrastructure (PSTI) Act, regulations stemming from the U.S. Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), and Japan's IoT Cybersecurity Standards +++.

## Going forward

In conclusion, Schneider Electric is dedicating focused resources to support our proactive work towards the 2027 effective date of the CRA. While this effort is part of our broader goal to continuously develop and maintain a robust cybersecurity posture, compliance is not optional. To remain a key player in the EU market, we must adhere to these essential requirements. As a global company, the implementation of these requirements will have a significant impact worldwide, reinforcing our commitment to cybersecurity and ensuring our continued leadership in the industry.

se.com

Life Is On Schneider Electric

Schneider Electric Industries SAS
35 rue Joseph Monier
92500 Rueil-Malmaison, France
Tel : +33 (0)1 41 29 70 00