

Compliance with National Cybersecurity Laws and Regulations such as the CRA

This document sets forth Mitsubishi Electric Corporation's (hereinafter "the Company") policy for the security of Factory Automation (hereinafter "FA") products*1 that the Company develops and produces in accordance with its "Basic Security Policy for Factory Automation Products". Relevant laws and regulations, including the European Cyber Resilience Act (CRA), are within the scope of this policy.

1. Basic Policy

Because cyber threats increasingly cross national borders and threaten individuals' safety, there is a growing global momentum toward the consideration and promotion of cybersecurity regulations. In light of these changes, the European CRA was enacted in 2024 to set requirements for products that contain digital elements. The Company believes it is important to take appropriate measures to improve the security of FA products (hereinafter "FA product security") to prevent significant damage or adverse impact to customers. Accordingly, the Company will strive to provide safe and secure FA products that comply with domestic and international FA product security standards (such as IEC 62443). In addition, working with our partner companies, we will continue efforts to contribute to the maintenance and improvement of the following six elements in our customers' operating environments:

- Health
- Safety
- Environment
- Availability
- Integrity
- Confidentiality

2. Measures

Legal Compliance

The Company endorses the CRA's values and objectives of "enhancing safety, trust, and transparency for consumers and businesses by ensuring security throughout a product's lifecycle," and will comply with national laws and regulations concerning FA product security.

Establishing an Organization and Structures to Ensure Safety and Security

In order to build organizations and structures that comply with Article 14 of the CRA, the Company has established PSIRTs (Product Security Incident Response Teams) internally, strengthened and promoted technical measures to prevent the introduction of vulnerabilities and will conduct prompt root-cause investigations and reliable corrective actions in the event of vulnerabilities affecting FA products.

Furthermore, the Company will strive to ensure that customers can use FA products with confidence by communicating with customers and sharing information with public agencies quickly, appropriately, and actively to improve FA product security.

Promoting Defense-in-Depth for FA systems

To further enhance the security of customers' FA systems, the Company considers "defense-in-depth" – applying layered measures across human, physical, network, and other domains in accordance with Article 13 of CRA – to be indispensable. Therefore, together with partner companies, the Company will work to strengthen the security of FA products themselves and support customers in implementing and maintaining security measures for the FA systems they build.

Protecting FA Products Throughout the Product Lifecycle

The Company will continuously assess FA product security risks and take measures to protect FA products from evolving attacks across the entire product lifecycle described in the CRA (planning, design, manufacture, operation and maintenance, and disposal, etc.).

Reducing Supply Chain Risk

To raise the overall level of FA product security across the supply chain, including within the Company, we will manage software components of FA products, maintain correct knowledge and high awareness of FA product security, and build and maintain a framework for assessing the security risks of product components sourced from third parties.

*1 : Programmable Controllers, Industrial PCs, HMI GOTs, SCADA, Servo systems, Inverters, Industrial Robots, Numerical Controllers (NCs), Electrical Discharge Machines, Laser Processing Machines, Electron Beam Machines, Low-voltage Power Distribution Products, Power Management Products, and related software and services