

Basic Security Policy for Factory Automation Products

This document defines the basic policy with concrete measures for the security of Factory Automation (hereafter referred to as "FA" and "FA products Security") products*1 that Mitsubishi Electric Corporation (hereafter referred to as we or "the Company") develops and produces.

1. Basic Policy

With the rapid spread of the Internet and progress of IT/IoT technology, the productivity of factories is expected to improve due to the progression of cooperation between FA systems and IT systems. On the other hand, threats due to cyber-attacks from inside and outside FA systems will also increase, therefore the necessity to ensure the security for FA products is increasing. We recognize that to avoid serious damages and impact, improvement of the security and introducing possible measures for FA systems become meaningful.

Therefore, we are working to comply with domestic and foreign standards and specifications (IEC 62443, etc.) in order to provide secure and safe FA products.

Furthermore, we are working to maintain and improve the following six elements in our customers' usage environment.

· Health · Safety · Environment · Availability · Integrity · Confidentiality

2. Measures

Legal Compliance

We will comply with all relevant laws and regulations related to Product Security. In addition, we will take appropriate measures to protect personal information in accordance with our "Personal Information Protection Policy."

Building an organization or system to ensure security and safety

To maintain and improve the security for FA products of the company, we have an organization PSIRT (Product Security Incident Response Team) that is dedicated to product security and responsible for rapid root cause detection, coping with security incidents and introducing technical measures to prevent contamination by vulnerabilities.

Furthermore, via immediate, appropriate and positive communication with our customers, we are working to improve reliability for FA products and services of the company.

Promoting defense-in-depth in FA systems

We recognize that for further enhancement of customers' FA system security, it is effective to promote defense-in-depth that implements various measures in multiple layers. Therefore, we are working to improve the security of our FA products and corroborate with our partners to introduce and promote security for customers FA systems installing with our products.

Protecting FA products throughout the product life cycle

We will establish the product life cycle (plan, design, manufacture, operate, and dispose) based on domestic and foreign standards and specifications for security and continue to implement measures to protect our FA products against evolving attacks.

Reducing the supply chain risk

In order to obtain the accurate knowledge and retain a high level of awareness for FA products security, we are working to dissemination of the knowledge and conduct training at our company and throughout our supply chain.

*1 : Programmable Controllers, Industrial PC, GOT, SCADA, Servos, 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/services