Information Security Policy

The Komatsu Group regards the proper protection of information assets as a critical responsibility. To earn and maintain the trust of all our stakeholders, we are committed to maintaining and strengthening information security and pursuing continuous improvements based on the following policies:

1. **Establishment of an Information Security Framework**
   We clearly define responsibilities and authorities related to information security across the entire Komatsu Group. Under the leadership of the top management, we promote the establishment, operation, maintenance, and continuous improvement of our information security management system.
2. **Protection of Information Assets**
   To ensure the confidentiality, integrity, and availability of information assets, we conduct systematic risk assessments and implement appropriate measures based on the results. All Komatsu Group employees understand the importance of information security and act responsibly.
3. **Security Measures for Information Systems**
   We implement appropriate measures to protect our information systems and maintain and improve information security. In addition, we appropriately monitor networks and systems and respond promptly to incidents of unauthorized access or abnormal events.
4. **Management of Information Security Incidents**
   In the event of an information security incident, we respond swiftly to minimize damage, restore operations quickly, and prevent recurrence.
5. **Ensuring Information Security Across the Supply Chain**
   We work to identify information security risks across the entire Komatsu Group’s supply chain, including distributors and business partners, and request appropriate information security management.
6. **Education and Training**
   We regularly provide education and training to all Komatsu Group employees to raise awareness of information security and strengthen their ability to respond effectively.
7. **Legal and Regulatory Compliance**
   We take appropriate actions in accordance with the applicable laws, regulations, and contractual obligations in each country and region. Furthermore, we verify the operational status of information security through regular audits and pursue continuous improvements.