Date issued	09, 11, 2026
Date revised	09, 11, 2026
Document type	Policy
Language	English
Legal entity	Komatsu America Corp
Business unit/division	KNA, KMT, and centralized functions under KMT
Country	United States, EU
Facility/site	North America
Function owner	John Hunter

Coordinated Vulnerability Disclosure Agreement

1. Purpose of Responsible Disclosure Policy

This Responsible Disclosure Policy is for Komatsu America Corp, Komatsu Mining Corp and its group subsidiaries. Komatsu cares deeply about maintaining the trust and confidence that customers, distributors, end users and other stakeholders place in us. The security of our products with digital elements, related services and our online platforms is of paramount importance.

We encourage customers, distributors, end users, security researchers and other third parties that have discovered or suspect vulnerabilities in Komatsu Mining Technology products with digital elements, related services or online platforms, to disclose them to us in a responsible manner.

This Responsible Disclosure Policy explains how third parties can report vulnerabilities to Komatsu Mining Technology and how Komatsu Mining Technology will receive, record, investigate, escalate and respond to those reports, including where a report may require handling under the EU Cyber Resilience Act.

We will assess, validate and address reported vulnerabilities using Komatsu Mining Technology's vulnerability handling and cyber incident reporting processes, and will comply with applicable legal and regulatory obligations.

We will not take legal action against or suspend or terminate the accounts of customers, distributors, end users, security researchers and other third parties who discover and report security vulnerabilities in accordance with this Responsible Disclosure Policy to the extent as a result of the disclosure.

2. Reporting of Suspected Vulnerabilities

We encourage customers, distributors, end users, security researchers and other third parties to share details of suspected vulnerabilities with Komatsu Mining Technology through the approved reporting channel. Reports should be submitted in the first instance by email to CRA_Report@global.komatsu.

To help Komatsu Mining Technology validate and respond to the report efficiently, please include:

- contact details;
- the affected product, model, software, firmware or platform;
- version and configuration information;
- a clear description of the suspected vulnerability;

- steps to reproduce or demonstrate the issue;
- any supporting evidence;
- whether the vulnerability is known or suspected to be actively exploited;
- any suspected impact on safety, availability, confidentiality, integrity or data security; and
- whether any data was accessed, copied, modified or deleted.

3. Komatsu Mining Technology's Commitment

If you identify a valid security vulnerability and report it in accordance with this Responsible Disclosure Policy, including the responsible disclosure conditions in Section 4, Komatsu Mining Technology will:

- log the report and review it within a reasonable period in accordance with Komatsu Mining Technology's vulnerability handling and cyber incident reporting processes;
- assess whether the report is valid, whether it has previously been reported, and the severity and potential impact of the vulnerability;
- work with you, where appropriate, to understand, validate and respond to the reported issue;
- escalate the matter to relevant internal teams where required in accordance with Komatsu Mining Technology's vulnerability handling and cyber incident reporting processes;
- determine appropriate countermeasures, updates, mitigations or other actions based on the nature and impact of the vulnerability;
- where a reported vulnerability or incident may fall within Komatsu Mining Technology's vulnerability handling and cyber incident reporting process, assess and complete any required internal escalation, reporting workflow, executive update or other internal process step in accordance with that process; and
- where legal or regulatory obligations are triggered, including under the EU Cyber Resilience Act, complete any required authority notification, EU reporting or public communication in accordance with applicable legal requirements.

4. Responsible Disclosure Conditions

This section supports Komatsu Mining Technology's vulnerability handling and coordinated disclosure process, including its obligations under the EU Cyber Resilience Act. To allow Komatsu Mining Technology to assess, validate, remediate and, where required, report vulnerabilities safely and effectively, anyone reporting a suspected vulnerability must act responsibly, in good faith and within the conditions set out below:

- do not publicly disclose vulnerability details before Komatsu Mining Technology has had a reasonable opportunity to assess and respond;
- do not exploit a vulnerability beyond what is reasonably necessary to demonstrate it;
- do not access, copy, modify, delete or disclose data except to the minimum extent necessary to identify and report the vulnerability;

- do not disrupt, degrade or attempt to bypass the availability, integrity, confidentiality or safety of any product, system, service or data;
- do not use malware, social engineering, phishing, denial-of-service, brute force, automated high-volume scanning or similar techniques; and
- promptly delete any data obtained while demonstrating the vulnerability once it has been reported to Komatsu Mining Technology, unless preservation is required by law or agreed with Komatsu Mining Technology.

4.1 Our assurance if you follow this Policy

If you act responsibly, in good faith and in accordance with this Policy, including the responsible disclosure conditions in Section 4, Komatsu Mining Technology will not take legal action against you solely for identifying and reporting a suspected vulnerability. This assurance applies only to activity that is necessary to identify and report the vulnerability and does not cause harm, disrupt systems or services, compromise data, breach applicable law, or fall outside the conditions in this Policy.

Where these conditions are not followed, Komatsu Mining Technology may treat the report as outside this Policy and reserves all legal rights. If you are unsure whether an activity is permitted, contact Komatsu Mining Technology through the approved vulnerability reporting channel before taking any further action.

5. Privacy Statement

Any personal data submitted or processed in connection with a report under this Responsible Disclosure Policy will be processed in accordance with applicable data protection laws, including the General Data Protection Regulation (EU) 2016/679 and applicable local data protection laws. Further information on how Komatsu Mining Technology processes personal data is available in the relevant Komatsu Mining Technology group company’s privacy notice which is available via the respective company’s website.

6. Changes to this Policy and Questions

Komatsu Mining Technology reserves the right to change this Policy at any time. Any change of this policy will not affect reporting, escalation or notification obligations that apply under applicable law at the time of a vulnerability report or cyber incident.

If you have any questions about this Policy or are unsure whether it applies to a proposed report or activity, please contact Komatsu Mining Technology through the approved vulnerability reporting channel before taking any further action. Should you have any immediate questions regarding this policy in the first instance please contact the CRA_Report@global.komatsu.