



## Responsible Disclosure Policy Komatsu

### 1. Purpose of Responsible Disclosure Policy

Komatsu cares deeply about maintaining the trust and confidence that our customers place in us. The security of our online platforms is of paramount importance.

We encourage security researchers that have discovered vulnerabilities in our services to disclose this to us in a responsible manner.

Komatsu will engage with security researchers when vulnerabilities are reported to us in accordance with this Responsible Disclosure Policy.

We will validate and fix vulnerabilities in accordance with our commitment to (information) security and privacy.

We will not take legal action against, or suspend or terminate the accounts of, researchers who discover and report security vulnerabilities in accordance with this Responsible Disclosure Policy.

Komatsu reserves all legal rights in the event of any non-compliance.

### 2. Reporting of (suspected) vulnerabilities

We encourage security researchers to share the details of suspected vulnerabilities with Komatsu's Security Office by sending an email to [securityoffice@komatsu.eu](mailto:securityoffice@komatsu.eu).

Komatsu will review the submission to determine if the finding is valid and has not been previously reported.

We ask security researchers to include detailed information along with reproducible steps for us to validate vulnerabilities.

### 3. Komatsu's commitment

If you identify a valid security vulnerability in compliance with this Responsible Disclosure Policy, Komatsu commits to:

- Working with you to understand and validate the issue.
- Addressing the risk (if deemed appropriate by Komatsu).

### 4. Non-compliance

Public disclosure of the submission details of any identified or alleged vulnerability without express written consent from Komatsu will deem the submission as noncompliant with this Responsible Disclosure Policy.

Don't disclose the vulnerability until we have been able to correct it.

Don't exploit any vulnerability by unnecessarily copying, deleting, adapting or viewing data. Or, for example, by downloading more data than is necessary to demonstrate vulnerability.

Don't perform attacks such as breaching physical security, social engineering, distributed denial of service, and spamming.

Immediately erase all data obtained through demonstrating the vulnerability as soon as it is reported to Komatsu.

Don't perform actions that could have an impact on the proper functioning of the system, both in terms of availability and performance, but also in terms of confidentiality and integrity of the data.

Don't apply the following actions:

- Placing malware (virus, worm, Trojan horse, etc.).
- Copying, modifying or deleting data in a system.
- Making changes to the system.
- Repeatedly accessing the system or sharing access with others.
- Using automated scanning tools.
- Using the so-called "brute force" to access systems.
- Using denial-of-service or social engineering (phishing, vishing, spam...)

Acts under this Responsible Disclosure Policy should be limited to conducting tests to identify potential vulnerabilities and sharing this information with Komatsu. If, after the vulnerability has been removed, you wish to publish information about the vulnerability, we ask you to notify us at least one month before publication, and to give us the opportunity to respond.

Identifying us in a publication is only possible after we have given our explicit approval to do so.

#### **4.1. What we promise**

If you have complied with the above terms of the Responsible Disclosure Policy and have not committed any other breaches, we will not take any legal action against you.

- We will respond to your report within a short period of time, if possible, within maximum 15 working days, with our review of the report and any expected date for resolution.
- We will treat your report confidentially and will not share your personal data with third parties without your consent unless this is necessary to comply with a legal obligation.
- We will keep you informed of the progress of solving the problem.
- We strive to solve all problems within a short period of time.
- We may choose to ignore low-quality reports.

If you have any questions, we encourage you to address them to [securityoffice@komatsu.eu](mailto:securityoffice@komatsu.eu)  
In case of doubt about the applicability of this policy, please contact us first via this e-mail address  
We reserve the right to change the content of this Policy at any time.

#### **4.2. 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 (GDPR). Further information on how Komatsu

processes personal data is available in our Privacy Notice, which can be found on our website ([www.komatsu.eu](http://www.komatsu.eu)).