

Note: This document has been translated from the Japanese original for reference purposes only. In the event of any discrepancy between this translated document and the Japanese original, the original shall prevail.



July 3, 2025

Company name: Yodogawa Steel Works, Ltd.
Representative: Eiichi Tanaka,
President and Representative Director
Listing: Tokyo Stock Exchange, Prime Market
Stock code: 5451
Inquiries: Takayuki Deguchi,
General Manager of IR Department
Tel: +(81)6-6245-1113

Notice Regarding the Occurrence of Ransomware Infection Damage and the Possibility of Information Leakage at Consolidated Subsidiaries (Third Report)

As reported in “Notice Regarding the Occurrence of Ransomware Infection Damage and the Possibility of Information Leakage at Consolidated Subsidiaries (Second Report)” dated June 18, 2025, Sheng Yu Steel Co., Ltd. (“SYSCO”), a consolidated subsidiary of Yodogawa Steel Works, Ltd. (the “Company”) in Taiwan, has been investigated by the Industrial Development Administration, the Ministry of Economic Affairs, the Executive Yuan, the Republic of China (Taiwan) (the “Industrial Development Administration”), and the Company hereby announces that SYSCO has recently received the investigation result from the Industrial Development Administration.

1. Regarding the Investigation Result from the Industrial Development Administration

SYSCO has been investigated by the Industrial Development Administration regarding the actions taken in response to the ransomware attack, and has been evaluated that there was no violation of the local Personal Information Protection Law.

The Group will continue to work on enhancing its security measures.

Furthermore, the Company has not confirmed any secondary damage related to this incident.

2. Impact on Business Performance

The Company believes that this incident will only have a negligible impact on the Group’s business performance. We will promptly disclose any information that could materially impact our business results.

We would like to extend our deepest apologies to all stakeholders for the significant concerns and inconveniences caused.