July 27, 2026

FOR IMMEDIATE RELEASE

Company Name: Asahi Group Holdings, Ltd.
Representative: Atsushi Katsuki, President and Group CEO
Securities Code: 2502
Stock Listings: Tokyo Stock Exchange, Prime Market
Contact: Sasana Nemoto, Head of Corporate Communications
Phone: +81-3-5608-5126

Notice Regarding a Material Weakness in Internal Control over Financial Reporting

Asahi Group Holdings, Ltd. (the “Company”) announces that, in the Internal Control Report for the fiscal year ended December 31, 2025, submitted today to the Kanto Local Finance Bureau pursuant to Article 24-4-4, Paragraph 1 of the Financial Instruments and Exchange Act, the Company identified that there is a material weakness that should be disclosed and stated that its internal control over financial reporting was not effective, as described below.

1. Material Weakness

In the early morning of September 29, 2025, a system disruption occurred in information systems managed by the Group in Japan. During the course of investigation, it was discovered that data on certain servers had been encrypted, confirming that the system disruption was caused by a cyberattack. In response to this incident, and in order to prevent further damage, the Group disconnected internal and external networks and isolated the data center on the same day. Thereafter, investigations conducted with the assistance of external experts confirmed that the attacker had gained administrative privileges without authorization, used compromised accounts to explore the internal network, and then executed ransomware on multiple servers. The impact of the system disruption caused by this cyberattack was limited to systems managed and operated within the Japan Region (the Group's business operations in Japan).

In light of the urgency of the situation and its significant impact on management, the Group established an Emergency Response Headquarters immediately following the cyberattack in accordance with its Group Crisis Management Policies and Business Continuity Plan (BCP). Efforts were made to minimize operational disruption and restore internal networks and information systems necessary to support business operations and financial closing activities. In addition, the Group reviewed and rebuilt the network architecture in the Japan Region and engaged external experts to assess vulnerabilities in the newly established environment.

Despite these efforts, responding to disruptions in access to accounting-related data and carrying out activities under alternative business processes required significant time. As a result, the Company was unable to complete, on a timely basis, the procedures necessary for financial reporting, including the retrieval and verification of financial reporting-related data required for the financial closing process. Consequently, the Company was required to obtain an extension of the statutory filing deadline for its Annual Securities Report.

The Company recognizes that this incident occurred because the operation and management of information systems based on rules governing information systems and information security were not sufficiently implemented in certain parts of the information system infrastructure used for business operations in the Japan Region, allowing the attacker to gain unauthorized access. As a result, this led to an event that had a significant impact on the timeliness of financial disclosures. Accordingly, the Company

assessed that a material weakness existed in the operating effectiveness of entity-level controls relating to "policies for the development and maintenance of information systems" in the Japan Region.
In the Japan Region, rules governing information systems and information security, including the Asahi Group Information Systems Management Regulation and the Asahi Group Information Security Regulation, had comprehensively defined requirements for integrated security management and prescribed compliance requirements and specific technical measures to ensure the protection and security of information systems used in business operations and to mitigate the risks of cyberattacks and unauthorized access. However, it was identified that within part of the information system infrastructure used for business operations in the Japan Region, certain operational management activities, including access rights management required under these rules, had not been sufficiently implemented.

2. Reason Why the Material Weakness Could Not Be Remediated by the End of the Fiscal Year

This matter was caused by a cyberattack. Following the discovery of the incident, the Company prioritized preventing further damage, restoring affected systems, and investigating the root cause of the incident, and subsequently implemented response measures in stages based on the results of the investigation. Therefore, remediation and evaluation could not be completed by the end of the fiscal year.

3. Remediation Plan for the Material Weakness

The Group recognizes that the material weakness was caused by insufficient implementation of operational management based on rules governing information systems and information security within the Japan Region. To remediate the material weakness and prevent recurrence, the Group has been implementing the following measures:

- Remediation of deficiencies in access privilege management;
- Establishment of a framework for monitoring operational status under the supervision of the Information Security Committee; and
- Implementation of Fit & Gap analyses for critical information systems to identify gaps between regulatory requirements and actual operational practices, and promotion of necessary remediation measures.

As of the date of the submission of this report, the following measures have been implemented.
First, in response to the deficiencies in access privilege management identified in this incident, the Group has implemented measures, from the perspective of reinforcing controls over administrative privileges, across all systems identified as being within the scope of internal control evaluations over financial reporting, in accordance with regulations governing information systems and information security. These measures include the strengthening of access management controls and enhancement of password requirements.
In addition, to ensure that these measures continue to function effectively, periodic monitoring under the supervision of the Information Security Committee established by the Group has commenced in the Japan Region. Such monitoring includes confirmation of compliance with relevant rules and management of the progress of remediation measures.

4. Impact on the Consolidated Financial Statements

The Company has determined that all necessary corrections resulting from the material weakness described above have been reflected in the consolidated financial statements.

5. Audit Opinion on the Consolidated Financial Statements and Financial Statements

The auditor issued an unqualified opinion.

-END-