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.

August 5, 2026

Company name: Sodick Co., Ltd.
Name of representative: Yuji Akutsu
CEO President and Representative Director
(Securities code: 6143; TSE Prime Market)
Inquiries: Masato Takagi
Director Managing Executive Officer
(Telephone: +81-45-942-3111)

Notice Regarding Unauthorized Access to the Company's Server (Final Report)

Sodick Co., Ltd. (the "Company") hereby provides the following update regarding the unauthorized access to the Company's server by a third party, which was previously announced in the "Notice Regarding Unauthorized Access to the Company's Server" dated May 21, 2026. Following the discovery of the incident, the Company conducted an investigation and implemented remedial measures. As the investigation has now been completed, the Company announces the results of the investigation and measures to prevent recurrence as follows.

We would also like to express our sincere apologies to our customers and all other stakeholders for the significant concern and inconvenience caused by this incident. We take this matter very seriously and are committed to thoroughly implementing measures to prevent recurrence and further strengthening our information security framework.

1. Overview

On May 15, 2026, suspicious activity was detected in certain systems of the Company, and subsequent investigations confirmed unauthorized access by a third party to the Company's server. Following confirmation of the incident, the Company worked with an external cybersecurity firm to isolate the relevant server and investigate matters including the intrusion route and evidence of unauthorized access.

In addition, the Company has reported and consulted with the relevant police station and the Personal Information Protection Commission.

2. Results of the Investigation

- Identification of the intrusion route used by the unauthorized third party
- Identification of the servers and equipment affected by the unauthorized access
- Identification of the extent of the compromise and the scope of information potentially subject to leakage

As a result of a detailed investigation conducted by an external cybersecurity firm, unauthorized access was confirmed to have occurred via the network of one of our overseas locations. The investigation found no evidence of information leakage or exfiltration of data. In addition, no leakage of personal information, no secondary damage resulting from unauthorized use, and no disclosure of the Company's information by the attacker or any other third party have been confirmed.

3. Personal Information Potentially Subject to Leakage

Although the investigation found no evidence indicating the leakage of information, including personal information, the Company has decided, as a precautionary measure, to treat any information for which the possibility of leakage cannot be completely ruled out as information that may have been compromised.

The personal information that may have been affected by this incident includes the following information relating to the Company's business partners and employees of the Company and its group companies.

Categories of Personal Information Potentially Affected

- Scope of Personal Information: Names, postal codes, addresses, telephone numbers, and email addresses

The Company has been individually notifying those whose personal information may have been affected by this incident. For individuals whom the Company is unable to contact directly, such as where contact information is unavailable, this announcement shall serve as notification from the Company in lieu of individual notification.

4. Cause

The unauthorized access to the Company’s server was carried out by exploiting a vulnerability in network equipment.

5. Measures to Prevent Recurrence

Taking into account the findings of the investigation, the Company has already implemented the following measures:

- Reconfirmation and review of personal information handling procedures
- Reinforcement of employee education regarding personal information protection
- Review of access authority management
- Enhancement of monitoring systems for systems handling personal information
- Thorough vulnerability management and security updates for systems and network devices
- Strengthening of internal reporting mechanisms

The Company will continue to work closely with external cybersecurity experts to further strengthen its cybersecurity measures and monitoring framework in order to prevent recurrence.

6. Impact on Business Performance

At this time, no material impact of this incident on the business performance or operations of the Company and its group companies has been identified. Should any matters requiring disclosure arise in the future, the Company will promptly provide an update.