

Notice Regarding Unauthorized Access to an Employee Email Account

Fujisawa, Japan – July 22, 2026 – We have confirmed that a third party gained unauthorized access to an employee email account. As a result of our investigation, we have determined that personal data and confidential information contained in emails stored in that account may have been compromised (the confirmed incident is hereinafter referred to as the "Incident").

We sincerely regret the concern and inconvenience caused by the Incident.

1. Overview, Background and Cause of the Incident

On April 23, 2026, we identified that one of our employees had entered authentication credentials in response to a phishing email. Upon becoming aware of the incident, our IT department immediately implemented initial response measures, including changing the password for the affected account, and reviewed security tool logs and other relevant records.

Subsequently, on May 22, 2026, we detected an unauthorized login to the affected email account by a third party. The account was immediately disabled to block further unauthorized access. We also engaged an external cybersecurity specialist to conduct a forensic investigation and submitted an initial report to the Personal Information Protection Commission of Japan.

2. Investigation Results

After receiving the results of the forensic investigation from the external specialist, we confirmed the affected emails and the scope of impact. We then submitted our final report to the Personal Information Protection Commission of Japan on July 21, 2026, and decided to publicly disclose the Incident.

The investigation identified evidence of unauthorized access by a third party to approximately 7,000 emails stored in the affected email account between April 24 and May 21, 2026. The affected emails were sent or received during the period from November 5, 2025, to May 21, 2026. The affected emails contained personal data relating to our officers and employees, those of our group companies, as well as our customers, business partners and other related parties. They also included information relating to contracts and business transactions with our business partners. We have identified all affected emails.

The unauthorized access to the affected account has already been blocked, and all relevant logs and data associated with the Incident have been preserved.

At this time, we have found no evidence that any personal data or information relating to contracts or business transactions with our business partners has been misused, nor that the Incident has resulted in any secondary harm.

However, we cannot rule out the possibility that the compromised information could be used in fraudulent emails or other communications impersonating our company or our business partners. Accordingly, we ask all affected parties to exercise caution. Please refrain from accessing URLs contained in suspicious emails, opening unexpected attachments or responding to requests to change

bank account information or other payment instructions. Where appropriate, please verify the authenticity of such communications through an alternative contact method. Please also note that we will never ask you to enter your password or other authentication credentials in connection with this Incident.

3. Our Response

We will continue to cooperate with the relevant authorities while contacting individuals and business partners who may have been affected by the Incident to provide the necessary information and guidance.

We will continue to closely monitor the situation and will promptly disclose any new material information that should be made public.

4. Measures to Prevent Recurrence

We take this Incident very seriously and are implementing enhanced measures to prevent recurrence, including strengthening email security, expanding the use of multi-factor authentication, enhancing employee cybersecurity awareness and training, and improving security monitoring.

We are committed to strengthening our information security measures and preventing similar incidents in the future.

5. Contact

For inquiries regarding this Incident, please contact us at the following email address.

Personal Information Inquiry Desk

Email: privacy-contact@axcelead.com

Business Hours: Monday through Friday, 9:00 a.m. to 5:30 p.m. (Japan Standard Time (JST)), excluding Japanese national holidays.

The end of this document