

## **PUBLIC NOTICE ON CYBERSECURITY INCIDENT**

14 April 2026

We, Microlink Solutions Berhad and our wholly owned subsidiary, Formis Computer Services Sdn Bhd, issue this notice in relation to a cybersecurity incident involving certain personal data. We take the privacy and security of personal data entrusted to us very seriously, and this notice sets out the relevant information regarding the incident, the actions taken in response, and the precautionary steps that individuals may wish to consider, where appropriate.

### **1. Incident**

On 10 February 2026, we experienced a cybersecurity incident affecting part of our IT systems. Following further investigation, we determined that certain documents comprising of limited personal data stored within some of the impacted IT systems may have been potentially accessed and/or exfiltrated without our authorisation.

### **2. The types of personal data which were involved in the impacted IT systems**

Investigations have revealed that the affected records may have contained a combination of the following basic personal data categories: full name; designation; corporate email address; NRIC/passport number; mobile number and residential address. Based on the information presently available, the affected personal data does not include any sensitive personal data, financial information, payment details, or account credentials.

### **3. Potential Consequences**

At this time, we have not identified any confirmed misuse of the affected personal data, and based on the information currently available, the overall risk to affected individuals is assessed to be very low. Given the limited nature of the personal data involved, we do not presently foresee any material adverse consequences arising from the incident, and we are not aware of any actual harm or misuse resulting from it to date.

### **4. Our actions**

We took immediate and comprehensive steps to contain and remediate the incident, including isolating impacted systems, strengthening access credentials, and further hardening our security measures. We also engaged independent external IT security and forensic specialists to support our response and conduct a thorough investigation. Additional security monitoring and safeguards have since been implemented. We have also notified the relevant regulator in Malaysia and are cooperating fully as required.

### **5. Precautionary measures**

We recommend that you remain vigilant against incidents of identity theft and fraud, and continue to:

- Be cautious with calls, emails, or messages from unknown sources.
- Avoid clicking on suspicious links or downloading attachments from unverified senders.
- Verify email sender addresses carefully, as scams often use subtle variations.
- Stay informed of email, telephone and text-based scams.
- Refrain from sharing sensitive personal or financial information with unverified parties.
- Review your bank account statements for suspicious activity and immediately report anything unusual to your financial institution.
- Implement multi-factor authentication for key personal online accounts.
- Report suspicious company emails to [cybersecurity.taskforce@microlink.com.my](mailto:cybersecurity.taskforce@microlink.com.my) immediately.
- Any email asking for payments, wire transfers, or change of accounts relating to Microlink's business partners need to be reported to [cybersecurity.taskforce@microlink.com.my](mailto:cybersecurity.taskforce@microlink.com.my) immediately.

We regret that this incident occurred. Please be assured that we have treated this matter with the utmost seriousness and have taken prompt and careful steps to investigate, contain, and address it.

Based on the information presently available, we are not aware of any actual harm or misuse arising from the incident, and the overall risk to affected individuals remains very low. This notice is being issued out of an abundance of caution and as part of our commitment to transparency and responsible stewardship of personal data. Should you have any questions or concerns, please do not hesitate to contact us at [cybersecurity.taskforce@microlink.com.my](mailto:cybersecurity.taskforce@microlink.com.my).

Yours Sincerely,

**Microlink Solutions Berhad**  
and  
**Formis Computer Services Sdn Bhd**