Explanation of Major Events in 2021

Two events of major concern to stakeholders occurred at GIGABYTE in 2021. For the sake of balanced reporting, the details of the two events and the follow-up responding and management actions are provided below.

Response to MIT Incident

In May 2021, the following text appeared on the GIGABYTE website: "Made-in-Taiwan and strict quality control which is different from other Brands that find OEMs in China with lower cost and quality". The resultant backlash led to GIGABYTE products being pulled down from shelves by Chinese e-retailers such as JD and Tmall.

▶ Management Mechanism and Responding Measure

GIGABYTE has a variety of product types, including motherboards, graphics cards, notebooks, and computer peripherals. We have two important manufacturing factories in China which have supported GIGABYTE to produce and provide quality products and consumer experiences to the world for a long time.

The incident was the result of flawed internal management and marketing strategy. GIGABYTE will therefore continue to strengthen internal employee management and training. Because the incident severely impacted the company, Mr. Dandy Yeh resigned from the Chairman of G-Style, a GIGABYTE subsidiary. The personnel responsible for this incident violated work rules and caused significant damages to company. Thus GIGABYTE terminated the employment relationships in accordance with the Labor Standards Act.

Response to Cyberattack Incident

In August 2021, GIGABYTE detected anomalies in system services and an investigation revealed that some servers had been compromised by hacker attacks. Ransomware installed by the hacker led to the encryption of some company files but our production, sales, and routine operations were not affected.

▶ Management Mechanism and Responding Measures

When the hacker attack was confirmed, information security defenses and audits were immediately activated by GIGABYTE. We also worked with external IT security experts to deal with this attack against partial servers. The relevant law enforcement and cybersecurity agencies were also notified and kept updated on the network anomalies we detected.

Information security is now a risk that no enterprises around the world can ignore. As a result of the incident, we thoroughly reviewed and upgraded the existing management structure and targets. The network security level was also strengthened to ensure the security and integrity of our data and prevent any further recurrence.