Pili International Multimedia Co., Ltd.
Implementation of Cybersecurity Governance in 2023

The Information Security Risk Management Framework: The management center has established an Information Department that regularly (quarterly) reviews cybersecurity policies during departmental meetings. [Article 2.24 of the 2023 (10th) Corporate Governance Evaluation, and the letter No. 1070210380 issued by the Securities and Futures Bureau, submitted to the Board of Directors]

1. On August 22, two new firewalls were installed in the Taipei data center, with a High Availability (HA) automation backup mechanism to prevent the company's network from being incapacitated in the event of an external attack.

2. On November 1, the firewall previously used in Taipei was relocated to the Huwei data center and integrated into the existing High Availability (HA) automation backup mechanism to prevent the company's network from being incapacitated in the event of an external attack.

3. Two Cybersecurity Awareness Campaigns：

    (1) Raising Awareness About 5 Types of Cyber Threats that Criminals Can Generate Using ChatGPT. 。

    (2) Raising Awareness That Pop-Up Malware Warnings on Websites May Result from Accidentally Allowing "Site Notifications" from Suspicious Websites.

4. From January to October 2023, there have been no significant attacks or information leakage incidents affecting the company's cybersecurity and operations.

5. Cybersecurity-Related Training from January to October 2023：

    Internal Training：

Date	course	Man*hours
March 22, 2023	New Employee Training (including "Cybersecurity")	8

    外訓：

Date	course	Man*hours
March 17, 2023	Aryan Technology Forum	29
October 26, 2023	2023 NMT Cybersecurity and Future Forum	

【Implementation Status Data Source: Information and Technology Department, Human Resources Department】