ES GROUP (HOLDINGS) LIMITED
(Company Registration No. 200410497Z)
(Incorporated in the Republic of Singapore)

RESPONSE TO SGX QUERIES

The board of directors (the "**Board**") of ES Group (Holdings) Limited (the "**Company**", and together with its subsidiaries, the "**Group**") wishes to respond to the following queries raised by the Singapore Exchange Securities Trading Limited (the "**SGX-ST**") on 8 January 2024 with respect to the Company's announcement dated 5 January 2024 on the cybersecurity incident (the "**Incident**").

Query 1

When and how was the Group made aware of the ransomware incident. Please disclose the affected duration of the Group's network and servers before the recovery operations were completed.

Company's Response

The Incident was detected on 3 January 2024 when the Group's staff reported that they were unable to view some of the files located in the servers. The Group immediately contacted its external information technology consultant to conduct internal checks. Upon detecting the ransomware, the Group's servers were disconnected from the network and the Group activated its business continuity plan to sustain its business and operations. The system was contained immediately. As at the date of this announcement, with the assistance of the Group's external information technology consultant, further investigations into the Incident and data recovery action are still ongoing.

Query 2

What is the nature of the ransomware incident, including but not limited to what was impacted and whether any data was leaked or compromised.

Company's Response

An unknown party had gained unauthorized access to the Group's servers and encrypted information therein. The tool or Ransomware is simply a software similar to WinZip which packs and password protects files, such that antivirus tools with malware protection would get fooled to think that the Ransomware is a legitimate software and allows Ransomware to bypass the antivirus tools.

As disclosed previously, the Group has engaged its external information technology consultant to assist with the investigations. Further investigations into the Incident are still ongoing with the assistance of the Singapore Police Force.

Based on its initial internal investigations together with its external information technology consultant, as at the date of this announcement, the Group is not aware of any evidence where data was leaked or compromised arising from the Incident, and the Group's business and operations continue to be operational as usual.

Query 3

Based on the Group's latest AR in April 2023, both the AC and the Board confirmed that the Group's IT internal controls are adequate and effective. Please provide more details on the basis for such confirmation and enhancements made, in light of the Ransomware incident.

Company's Response

Based on the work performed by both the Group's internal auditors and external auditors, the risk reports and assurance received from the Company's Chief Executive Officer (who is also the Chief Operating Officer) and the Finance Manager, the ongoing review as well as the continuing efforts by the management of the Company in enhancing the Group's controls and processes which are currently in place, the Board, with the concurrence of the Audit and Risk Committee of the Company, is of the opinion that there were no material weaknesses identified and the Group's internal controls (including financial, operational, compliance and information technology controls) and risk management systems are adequate and effective as disclosed in its Annual Report 2022.

Despite the Group's best efforts, the evolving nature of cyber threats poses challenges, even to the latest cybersecurity solutions available in the market. Please refer to the Company's response to Query 4 below on the enhancements to be taken in light of the Incident.

Query 4

Please provide an update on the Group's plans to prevent such incidents moving forward.

Company's Response

Following the Incident, the Group is working with its external information technology consultant to further enhance its cybersecurity measures, which include improving backup and recovery system to be more robust, enhancing anti-virus protection and proactively monitoring cybersecurity. The Group takes information security seriously and is committed to addressing the Incident responsibly.

Query 5

Please provide the Board's assessment of the impact of the ransomware incident on the following:

a) The Group's operations;
b) The Group's financials; and
c) The Quantum of (a) and (b).

Company's Response

Save as disclosed in the Company's response to Query 1 above, to the best of the Group's knowledge and as at the date of this announcement, there is no material impact to the Group's operations and financials arising from the Incident.

Query 6

Please disclose if there are any other material information shareholders should be aware of.

Company's Response

As at the date of this announcement, there is no other material information shareholders of the

Company should be aware of. Investigations into the Incident are still ongoing and the Company will provide further update(s) should there be any other material developments relating to the Incident.

BY ORDER OF THE BOARD
ES GROUP (HOLDINGS) LIMITED

LOW CHEE WEE
Executive Director and Chief Executive Officer
10 January 2024

---

*This announcement has been prepared by the Company and its contents have been reviewed by the Company's sponsor, ZICO Capital Pte. Ltd. (the "**Sponsor**"), in accordance with Rule 226(2)(b) of the Singapore Exchange Securities Trading Limited (the "**SGX-ST**") Listing Manual Section B: Rules of Catalist.*

This announcement has not been examined or approved by the SGX-ST and the SGX-ST assumes no responsibility for the contents of this announcement, including the correctness of any of the statements or opinions made or reports contained in this announcement.

The contact person for the Sponsor is Ms Goh Mei Xian, Director, ZICO Capital Pte. Ltd. at 77 Robinson Road, #06-03 Robinson 77, Singapore 068896, telephone (65) 6636 4201.