POL-IT-001

Information Security Policy

Rabbit Holdings Public Company Limited

Version:	1.0
Effective Date:	16 August 2023
Approver:	Board of Directors
Classification:	Internal Use

Table of Contents

Revision History

Revision Date	Author	Revision Summary

Document Approval

Author	Reviewer	Approver
(.....) Title.....	(.....) Title.....	(.....) Title.....
Date.....	Date.....	Date.....

Information Security Policy

Scope

Information Security Management for information system infrastructure of Rabbit Holdings Public Company Limited

Purpose

In pursuit of ensuring the utmost security and dependability of information technology management, achieving internationally recognized standards, and safeguarding the confidentiality, integrity, and availability of the data and information assets held by Rabbit Holdings Public Company Limited ("the Company"), all while adhering to pertinent regulations, rules, and legal statutes governing information security, the Company acknowledges the imperative necessity to formally institute a comprehensive information security policy. This policy functions as a comprehensive framework that governs the security aspects of the information technology system falling under the purview of ISO/IEC 27001:2022 certification, and is delineated as follows:

1. Risk Assessment and Evaluation

   The Company shall establish a systematic process to manage information technology risks, encompassing the stages of risk identification, risk assessment, and risk mitigation within predefined parameters. Furthermore, the Company shall designate proficient individuals who shall assume the responsibility for the effective oversight and management of risks intrinsic to the realm of technology.

2. Information Technology Resource Management

   The Company shall establish a systematic process to govern the management of information technology resources, harmonizing them with the Company's strategic plan. This entails the assurance of adequate resources to facilitate seamless information technology operations, coupled with astute oversight of substantial risks in scenarios where the allotment of resources falls short of operational imperatives.

3. Information Asset Security

   The Company shall implement protocols encompassing preventive, regulatory, and custodial measures to safeguard the physical and environmental facets associated with information assets and information technology hardware. These facets constitute the

fundamental underpinning of the information system's operational framework. The measures are designed to ensure the continual operational preparedness of these assets, while concurrently preempting any unauthorized access to information assets or unwarranted divulgence of classified information.

4. Information Security Standards of Information Technology

   The Company shall establish information security guidelines congruent with the information security policy and effectively communicate them to stakeholders. The guidelines shall encompass comprehensive security protocols addressing organizational, personnel, physical, and technological dimensions.

5. Information Security Policy and Guideline Review

   The Company shall conduct periodic reviews of the information security policy and guidelines, with a minimum frequency of once annually, to ensure their ongoing relevance and effectiveness.

6. Information Security Regulations Compliance

   Every employee of the Company shall be under a binding obligation to rigorously adhere to the information security regulations. Non-adherence to these regulations shall be deemed a transgression, warranting disciplinary measures in consonance with the Company's established disciplinary protocol.

7. Reporting of Compliance with the Information Security Policy

   A formal reporting of adherence to the Information Security Policy, encompassing relevant regulations and mandates, shall be furnished to the Board of Directors on an annual basis, supplemented by immediate reporting in the occurrence of incidents with potential implications on policy compliance.

This policy is applicable to all Company employees and any other individuals who have received authorization from the Company to access the information system. The policy is effective on 16 August 2023.