STRATEQ GENERATIVE ARTIFICIAL INTELLIGENCE (GEN AI) POLICY

1. INTRODUCTION

Generative (Gen) Artificial Intelligence (AI) is a revolutionary leap in artificial intelligence, which enables machines to create content such as text, images, music, and combination of audio video that mimics human. Unlike traditional AI, which processes and analyses data, Generative AI can produce new, original content by learning from vast amounts of existing information.

Technology is transformative in nature, potentially across industries, driving innovation, enhancing personalization, and unlocking new ways of solving complex problems. However, with its power comes the responsibility to navigate ethical, security, and regulatory challenges, ensuring that Generative AI is used safely and effectively.

2. PURPOSE

The purpose of this policy is to establish guidelines and guardrails for the safe and ethical use of Generative AI (GenAI) technologies within the organization.

This policy aims to protect the organization's data, maintain compliance with relevant regulations, and mitigate potential risks associated with the use of GenAI.

3. SCOPE

This policy applies to all employees, contractors, temporary workers, and third- party vendors who use, develop, or interact with Generative AI systems in the course of their work for Strateq.

4. ACCOUNTABILITY

1) Read, understand, and comply with this policy.
2) Understand that policy violations can lead to investigation and disciplinary action.
3) Report any suspected deviations or issues immediately.

5. GENERATIVE AI SECURITY REQUIREMENTS

5.1 Regulatory and Compliance

Strateq must ensure that the use of GenAI solutions developed or outsourced complies with relevant laws, regulations, and industry standards, such as Cybersecurity Act and applicable Personal Data Protection Act (PDPA).
Strateq must ensure that content generated by GenAI systems does not infringe on intellectual property rights and is properly attributed when necessary.

5.2 Ethical Considerations

a) Functions involving 'Secret' and 'Confidential' information classification must not use a GenAI solutions for decision-making requirements.
b) Strateq must regularly diversify the training data to identify and mitigate biases in GenAI models, ensuring fairness and impartiality in generated content.
c) Strateq must enable transparency and clearly communicate to users when they are interacting with AI-generated content, ensuring transparency in the use of GenAI technologies.
d) The businesses considering the GenAI solution must enable human oversight and human review to have an oversight of critical decisions made based on GenAI outputs.

5.3 Data Handling

Strateq classified information other than "Public", must not be input into any GenAI system without explicit approval from the Data Protection Officer (DPO) and Strateq Top Management.

All data used in training or interacting with GenAI systems must be anonymized or de-identified to prevent the exposure of Strateq classified information.

Data generated by GenAI systems must be stored securely in accordance with Strateq's data protection requirements.

5.4 GenAI Model Usage

Third-party providing the GenAI models and services must undergo Strateq vendor risk assessment before use.

The assessment must be extended to evaluate the vendor's data protection and training data update practices.

Process must be in place for continuous monitoring of GenAI models on cloud and on premises to ensure the models behave as expected and do not generate harmful, biased, or inaccurate content.

Strateq must restrict access to GenAI systems and models to authorized team managing the service. Any changes to the model must go through approval from DPO and Strateq Top Management.

5.5 User Training and Awareness

Businesses which have planned to use the GenAI solution and models, must have trained their employees on the safe and ethical use of GenAI technologies.

The team must be briefed on regulatory requirements around the usage of GenAI services and privacy and compliance requirements to recognize potential risks and adhering to GenAI policy.

Strateq must establish communication channels to regularly update the businesses using the GenAI on developments in GenAI, training data updates, data models and any changes to the policy.

6. INCIDENT MANAGEMENT

Strateq businesses planned to leverage GenAI solutions must establish procedures for identifying reporting and mitigation the negative impacts, misuses, and breaches.

Strateq established an incident response plan for the GenAI solution incidents through various methods. Incident can be lodged with the use of the Incident Repose Form or emailing the Compliance Department.

7. DEVIATION AND EXCEPTION

Deviation and exceptions may be considered upon review and approval by the DPO and/or the Compliance Department.

This Policy yields to statutory law where conflicts arise. Deviation authorized as legal requirements prevail, ensuring no breach of enforceable obligations.