CYBER SECURITY POLICY

1.0 CYBERSECURITY GOVERNANCE

(i) Aztech Global Ltd. and its subsidiaries (collectively, "**the Group**") are committed to maintaining robust cybersecurity governance to manage cyber risks effectively, comply with applicable regulatory requirements and safeguard the Group against cyber threats and incidents, thereby preserving the integrity, continuity and resilience of the Group's operations.

(ii) The Group's Chief Operating Officer provides strategic oversight and direction for the Group's cybersecurity framework, strategy and governance, including ensuring that appropriate governance structures, reporting arrangements and risk oversight processes are in place to support the effective management of cybersecurity risks.

(iii) The Group's IT department, under the guidance of the Head of IT, is responsible for working with the various departments across the Group to implement, maintain and enhance cybersecurity measures, embed cybersecurity policies and practices within day-to-day operations, and escalate material cybersecurity risks and incidents to senior management in a timely manner.

2.0 MANAGING CYBER RISKS

(i) The Group maintains internal cybersecurity policies and practices designed to align with applicable regulatory requirements and recognised industry standards. These policies and practices are reviewed regularly and, where appropriate, enhanced to remain effective, relevant and responsive to evolving cyber threats, regulatory developments and advancements in cybersecurity technologies.

(ii) The Group is committed to strengthening its cybersecurity defences on an ongoing basis through the adoption and implementation of appropriate measures, including the following:

(a) maintaining appropriate information security controls to protect the confidentiality, integrity and availability of the Group's data and information assets;

(b) monitoring, detecting, assessing and responding promptly to cybersecurity threats, incidents and suspicious activities;

(c) reviewing and enhancing, on a continuous basis, the Group's cybersecurity systems, processes, procedures and controls;

(d) reinforcing employees' responsibilities in safeguarding the Group's cybersecurity, including through training and awareness initiatives designed to promote employees' understanding of, and adherence to, applicable security protocols, policies and practices; and

(e) establishing appropriate cybersecurity requirements for third parties which access, process or otherwise handle the Group's data, systems and/or information assets, with a view to ensuring alignment with the Group's cybersecurity policies and practices.

3.0 REPORTING INCIDENTS, THREATS AND SUSPICIOUS ACTIVITIES

The Group's Incident Response Management Policy establishes the framework and procedures for the prompt identification, assessment, escalation, management and reporting of cybersecurity incidents, threats and suspicious activities. Material cybersecurity incidents and risks are to be assessed in a timely manner and escalated to senior management and, where appropriate, the Board or relevant Board committee, with due consideration given to applicable regulatory, statutory and disclosure obligations.