6. MANAGING STAKEHOLDER RELATIONSHIPS

Engagement with Stakeholders

StarHub continues to maintain effective stakeholder communication by holding our engagements in different modes, making ourselves more accessible and for greater flexibility. Events such as investor show cases and employee townhalls have been held physically. Active engagement with stakeholders enables us to understand our stakeholders' needs, gain better insights on our business risks and opportunities, and create value for all. Our key stakeholders' views have been identified through a stakeholder mapping exercise and are reviewed annually to assess their potential impact on our business. We promote and manage our stakeholder relations through regular and proactive engagement with our stakeholders, at the corporate level and functional divisions across the Group. In FY2024, the Group's key areas of focus in relation to the management of stakeholder relationships included transformation and growth.

Further details on StarHub's communication with our shareholders and other stakeholders can be found in the Investor Relations section and Sustainability Report on pages 150 to 151 and 75 to 77 of the Annual Report respectively.

7. OTHER CORPORATE GOVERNANCE PRACTICES AND POLICIES

A. DEALINGS IN SECURITIES

Insider Trading Policy

StarHub has adopted an enhanced insider trading policy with respect to dealings in StarHub securities by the Directors and Group employees. The policy imposes trading blackout periods which exceed the requirements of the SGX-ST Listing Manual, pursuant to which:

- All Directors and Group employees are prohibited from dealing in StarHub securities during the period:

  (a) commencing two weeks prior to the announcement of the Group's business performance update for each of the first and third quarters of our financial year and ending on the date of announcement of the relevant business performance update; and

  (b) commencing one month prior to the announcement of the Group's half-yearly and full-year results and ending on the date of announcement of the relevant results.

- All Management and employees directly involved in the preparation of the Group's quarterly business performance updates and the half-yearly and full-year results are prohibited from dealing in StarHub securities during the period commencing one month prior to the announcement of each of the Group's business performance updates and financial results and ending on the date of announcement of the relevant update or results.

All Directors, Management and Group employees are notified by email prior to the commencement of each trading blackout period and upon the lifting of the restrictions after the announcement of the respective business performance updates and financial results. The policy discourages trading on short-term considerations and reminds Directors, Management and Group employees of their obligations under insider trading laws.

Share Trading Policy

In addition, in order to facilitate compliance by the Directors and Management, StarHub has adopted a share trading policy which requires them to give prior notice of their intended dealing in StarHub securities to the Chairman and Chief Executive through the Company Secretaries.

StarHub also prohibits the acquisition of any StarHub shares pursuant to our Share Purchase Mandate where a price-sensitive development has occurred or been the subject of a decision, until the development has been publicly announced.

For the issue of new StarHub securities, while the SGX-ST Listing Manual permits the Board to seek a general mandate from shareholders to allot and issue up to 20% of StarHub's total issued share capital other than on a *pro rata* basis to existing shareholders, the Board has continued to voluntarily limit such mandate to 15% only.

In addition, for the specific mandate from shareholders to allot and issue StarHub shares under the RSP and the PSP, the Board has limited the aggregate number of StarHub shares available for grant under the RSP and the PSP to 8% of StarHub's total issued share capital (instead of the permitted 15% under the SGX-ST Listing Manual), taking into account any outstanding unvested share awards.

B. WHISTLE BLOWING POLICY

StarHub adopts a zero-tolerance policy against ethical and legal violations. The Group has instituted a robust procedure which provides accessible channels for employees and external parties (such as our customers, suppliers, contractors and other stakeholders who may have a business relationship with the Group) to report in a responsible manner, anonymously or otherwise, any concern or complaint in relation to any irregularity, inappropriate behavior, legal or ethical violation or other serious breaches of internal processes. Such reporting channels have been communicated, and include a dedicated whistle blowing email and a direct channel to the AC Chairman and the General Counsel (via email and/or mail).

All complaints will be promptly and thoroughly investigated in confidence and on a need-to-know basis. The investigation outcome together with a recommendation on the necessary actions to be taken will be reported to the AC Chairman and the General Counsel, who will decide on the appropriate course of action. On a quarterly basis, a consolidated report of all whistle blowing cases for the quarter (if any) will be submitted for review by the AC.

The Group's Whistle Blowing Policy aims to encourage the reporting of such matters in good faith, by lending confidence that employees and other persons making such reports will be treated fairly and accorded due protection against reprisals or victimisation. The Group's Whistle Blowing Policy is available on StarHub's intranet and corporate website for easy access by all employees and the public.

C. EMPLOYEE CODE OF CONDUCT AND RULES ON BUSINESS CONDUCT

StarHub has put in place the following policies and procedures to guide employees in carrying out their duties and responsibilities with high standards of personal and corporate integrity when dealing with StarHub, our competitors, customers, suppliers and the community:

- Employee Code of Conduct and Ethics
- Anti-Corruption, Corporate Gift and Hospitality Policy
- Supplier Code of Conduct
- Responsible Sourcing Policy
- Management and Staff Diversity Policy
- Purchasing Procedure
- Request for Proposal/Tender Procedure

These policies and procedures cover (a) business conduct (including employees' compliance with anti-corruption and anti-bribery laws), (b) conduct in the workplace, (c) protection of StarHub's assets, proprietary and confidential information as well as intellectual property, (d) conflicts of interest, (e) anti-corruption and anti-bribery, (f) diversity of Management and staff, (g) non-solicitation of customers and employees and (h) workplace health and safety. In parallel, the Purchasing Procedure and Request for Proposal/Tender Procedure cover internal controls on tenders, vendor selection and purchasing to ensure transparency, objectivity and compliance. Given the importance of sustainability, StarHub also adopted the Responsible Sourcing Policy, which is aligned with the UN principles for universally recognised principles on human rights, including labour rights, the environment and corruption.

The Employee Code of Conduct and Ethics, the Management and Staff Diversity Policy, the Purchasing Procedure and the Request for Proposal/Tender Procedure are available on StarHub's intranet, while the Anti-Corruption, Corporate Gift and Hospitality Policy, the Supplier Code of Conduct and the Responsible Sourcing Policy are available on StarHub's intranet and corporate website for easy access by all employees and the public.

In addition, employees are also required to undergo a mandatory Code of Conduct e-learning course covering, *inter alia*, anti-corruption training, and complete an annual declaration which includes the declaring of any potential, apparent or actual conflict of interest between their official duties at StarHub Group, and any other persons or interests.

D. DOCUMENT CLASSIFICATION POLICY

StarHub's confidential information is one of its most important assets. To this end, StarHub has established a Document Classification Policy to guide employees on how to properly classify and apply the adequate level of protection on the information and documents they are entrusted with that relate to the Group's business, activities and operations. This helps to safeguard such information and documents, and ensures that only appropriate persons have access on a need-to-know basis.

E. CYBERSECURITY AND DATA PROTECTION

Cybersecurity and data protection remain vital strategic priorities for StarHub, particularly with the acceleration of digital transformation, adoption of cloud technology and new hybrid working model. Appropriate cybersecurity and data protection frameworks have been put in place to safeguard our networks/ systems and customer and employee data and sensitive and/ or confidential information from security risks and breaches, as well as to ensure the Group's compliance with all applicable laws, including the Cybersecurity Act 2018, the Personal Data Protection Act 2012 (PDPA) and sector-specific cybersecurity requirements imposed by the Infocomm Media Development Authority such as the Telecommunications Cybersecurity Code of Practice and the Broadcast Cybersecurity Code of Practice. Our cybersecurity and data protection frameworks, which include policies, procedures, guidelines and checklists, are continually enhanced to enable StarHub to keep pace with the evolving cyber threats landscape. This proactive approach is designed to instil confidence in our stakeholders, assuring them that we are always one step ahead in protecting against cybersecurity and compliance risks.

StarHub implements a comprehensive cybersecurity posture improvement plan as part of our unwavering commitment to cybersecurity best practices. This plan, executed from a 'People, Process, and Technology' perspective, includes periodic audits by third party assessors and risk assessments to ensure all potential risks are within an acceptable level. This comprehensive approach should reassure our stakeholders of our steadfast commitment to cybersecurity.

StarHub has also appointed a Chief Information Security Officer (CISO) and established the Information Security Office (ISO), which reports to executive management. CISO is responsible for overseeing the overall security strategy and ensuring that it aligns with the business objectives. The ISO, on the other hand, is tasked with implementing the security strategy and managing day-to-day security operations. Together, they form a robust team that will help StarHub navigate the cyber threat landscape.

People: Various cybersecurity virtual workshops and phishing email campaigns are conducted to strengthen our employees' awareness of cybersecurity risks. These workshops cover a range of topics, from identifying phishing emails to best practices for securing personal and company data. The phishing email campaigns are designed to simulate real-world cyber-attacks and test employees' ability to recognize and respond to them. All StarHub employees are required to go through a series of cybersecurity e-learning modules covering different topics to fortify the last layer of security defense.

Process: The existing cybersecurity governance framework has been reviewed and revised. Amongst other things, StarHub has implemented a vulnerability disclosure program (VDP) to enable security researchers to report potential vulnerabilities to StarHub via a publicly accessible website. Since FY2023, StarHub launched a new Bug Bounty Program (BBP) to augment the existing VDP. The BBP will leverage on security professionals and experts to uncover security vulnerabilities in StarHub's Information Technology (IT) applications, is a proactive measure to identify and address potential threats.

Technology: StarHub has implemented different technology stacks to strengthen multilayer defense for both external and internal threats. These technologies work in concert to identify and neutralise potential threats, ensuring the security of our networks and systems.

The Group, including Ensign, is committed to providing end to end support for all segments within the enterprise sector, including large enterprises, government, small and medium-sized enterprises, and retail consumers. Our comprehensive support is designed to make our stakeholders feel valued and reassured that we are here for them.

As a Critical Information Infrastructure (CII) owner, StarHub continues to strengthen its security posture in compliance with applicable regulatory requirements.

StarHub has achieved the Data Protection Trustmark (DPTM) certification, a voluntary enterprise-wide accreditation that signifies an organisation's commitment to accountable data protection practices. The DPTM framework, adapted from the PDPA, international benchmarks and best practices, requires that certified organisations implement robust data protection policies and practices to manage and protect personal data in accordance with its stringent criteria.

To maintain compliance with all applicable data protection laws and regulations, StarHub conducts regular reviews and updates of its data protection frameworks and awareness programmes. In FY2024, StarHub updated its PDPA training materials, instituting an annual mandatory data protection training programme for all employees. StarHub has also partnered with OneTrust to enhance its privacy management initiatives. This collaboration includes the management of privacy impact assessments and the maintenance of a personal data inventory, which is updated annually. Through the OneTrust platform, StarHub streamlines the oversight of vendors processing personal data, ensuring a unified and efficient approach to data protection across its operations.

Further details on StarHub's approach to cybersecurity and data protection can be found in the Data and Cybersecurity section of the Sustainability Report on pages 98 to 102 of the Annual Report.

F. COMPLIANCE LEAVE POLICY

StarHub has voluntarily put in place a Compliance Leave Policy as an additional risk mitigation measure to enhance corporate governance. The policy is applicable to employees who hold Senior Manager positions and above, finance advocates and employees with sensitive job functions such as handling monies, inventories, payroll processing and approvals, risk management as well as purchasing of goods and services. Under the policy, relevant employees are required to go on mandatory block leave for a period of at least five consecutive working days per calendar year, thereby allowing covering officers to fully step into their duties and act as an additional check and balance against any breaches.

G. WORKPLACE SAFETY AND HEALTH

StarHub remains dedicated to supporting the health, safety and well-being of all employees across its business activities and operations. In FY2024, StarHub continued its hybrid working arrangements, allowing greater flexibility and work-life balance for employees.

StarHub's Workplace Safety and Health (WSH) Committee actively enhances our work health and safety programme by regularly reviewing policies and procedures to align with best practices, and comply with applicable laws, including the Workplace Safety and Health Act and regulations.

Further details on StarHub's approach to workplace safety and health can be found in the Employee Engagement and Well-being section of the Sustainability Report on pages 106 to 111 of the Annual Report.