

# CORPORATE GOVERNANCE

➔ Further details on StarHub's communication with our shareholders and other stakeholders can be found in the Investor Relations section on pages 56 to 57 of the Annual Report, and the 'Stakeholder Engagement' chapter in the Sustainability Report.



## 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 the Directors, Management and Group employees of their obligations under insider trading laws.

#### Share Trading Policy

To facilitate compliance by the Directors and Management with applicable laws and regulations, StarHub has adopted a share trading policy governing dealings in the Company's securities. Under this policy, the Directors and members of Management are required to provide prior notice of their

intended dealings in StarHub securities to the Chairman and the Chief Executive through the Company Secretaries.

StarHub also prohibits the acquisition of any StarHub shares pursuant to our Share Purchase Mandate during periods when a price-sensitive development has occurred or is the subject of a decision, until such information has been publicly announced. This safeguard reinforces the Company's commitment to fair and orderly trading in its securities.

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 voluntarily limited 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 capped the aggregate number of StarHub shares available for grant under the RSP and the PSP at 8% of StarHub's total issued share capital, taking into account any outstanding unvested share awards. This is below the maximum limit of 15% permitted under the SGX-ST Listing Manual and reflects the Board's prudent approach to equity dilution.

### B. WHISTLE BLOWING POLICY

StarHub adopts a zero-tolerance policy towards unethical conduct, misconduct and legal and regulatory violations. The Group has instituted a robust whistle blowing procedure which provides accessible and secure channels for employees and external parties (including customers, suppliers, contractors and other stakeholders who may have a business relationship with the Group) to report concerns in a responsible manner, whether anonymously or otherwise. Such concerns or complaints may relate to any irregularity, inappropriate behavior, legal or ethical violation or other serious breaches of the Group's policies and internal processes. The reporting channels have been clearly communicated, and include a dedicated whistle blowing email address, as well as direct channels to the AC Chairman and the General Counsel via email and/or mail.

All whistle blowing reports are promptly and thoroughly investigated in confidence and on a need-to-know basis. Investigation findings, together with recommendations on appropriate follow-up actions, are reported to the AC Chairman and the General Counsel, who determine the appropriate course of action. A consolidated report of whistle blowing cases (if any) is submitted to the AC on a quarterly basis for its review and oversight.

The Group's Whistle Blowing Policy is designed to encourage the reporting of concerns in good faith, by providing assurance that whistle blowers will be treated fairly and protected against retaliation, reprisal or victimisation. The policy is made available on StarHub's intranet and corporate website to ensure accessibility to 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
- Procurement Policy and 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 Procurement Policy and 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 conducting our business with integrity, accountability and respect for people and the planet, we have refreshed our Responsible Sourcing Policy to embed ESG considerations into our procurement and supply chain management and evaluate our suppliers based on their alignment with internationally recognised standards, in accordance with local laws.

The Employee Code of Conduct and Ethics, the Management and Staff Diversity Policy, the Procurement Policy and 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 the Group, and any other persons or interests.

### D. INFORMATION CLASSIFICATION AND HANDLING POLICY

StarHub recognises that information relating to the Group's business, activities and operations is a critical asset. The Information Classification and Handling Policy establishes a consistent framework to classify, protect and manage such information across physical and electronic media. It guides employees in applying need-to-know access controls and prescribes handling, transmission and secure disposal requirements based on defined sensitivity levels.

### E. CYBERSECURITY AND DATA PROTECTION

Cybersecurity and data protection are strategic priorities for the Group and an integral part of the Board's oversight of enterprise risk and control. The Group recognises that cyber and data threats have grown in sophistication and potential impact, affecting confidentiality, integrity and availability of information assets, customer trust, operational continuity and regulatory compliance.

The Board, supported by the RSC, oversees the cybersecurity and data protection governance framework and ensures that cybersecurity and data protection risk management is embedded within the Group's enterprise risk management and strategic planning processes. Cybersecurity and data protection oversight forms part of the Group's broader risk governance structure alongside other operational and technology risks.

In support of this, the Group has established cybersecurity and data protection frameworks to safeguard its networks, systems and information assets, including customer and employee data and other sensitive or confidential information. These frameworks comprise policies, procedures and controls designed to manage cybersecurity risks, respond to potential threats and safeguard systems and data.

The frameworks are aligned with applicable laws and regulatory requirements, including the Cybersecurity Act 2018, the Personal Data Protection Act 2012 (PDPA) and sector-specific cybersecurity requirements issued by the Infocomm Media Development Authority such as the Telecommunications Cybersecurity Code of Practice and the Broadcasting Cybersecurity Code of Practice. The Group reviews and enhances its policies, procedures, guidelines and checklists, on an ongoing basis to remain aligned with evolving threats, technological developments and regulatory expectations. 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.

## CORPORATE GOVERNANCE

### Governance and Oversight

The Board, supported by the RSC, provides oversight of cybersecurity and data protection risks as part of the Group's overall risk management framework. The RSC regularly reviews cybersecurity risk profiles, incident trends, technology risk reporting and the adequacy of mitigation measures, with material incidents and residual risk exposures escalated to the Board as appropriate.

Chief Information Security Officer (**CISO**), who reports to the Chief Executive, heads the Information Security Office (**ISO**). ISO oversees the Group's overall information security strategy and its alignment with business objectives, and is responsible for implementing the strategy and managing day-to-day information security operations. Periodic updates are provided to the RSC and the AC on the threat landscape, key risk indicators, incident responses and strategic investments in cybersecurity capabilities.

Cybersecurity risks are managed through a structured three-lines-of-defence model, with business units and IT operations responsible for implementing controls, specialist risk and security functions providing oversight and guidance, and internal audit independently assessing the effectiveness of governance, risk management and controls.

### Cybersecurity Framework and Capabilities

StarHub adopts a comprehensive cybersecurity posture improvement plan anchored on the principles of **People, Process and Technology**. It includes regular internal and external risk assessments, independent audits by third-party assessors and continuous monitoring to ensure that identified risks are managed within acceptable thresholds. This comprehensive approach should reassure our stakeholders of our steadfast commitment to cybersecurity.

**People:** StarHub invests in building a strong cyber-aware culture across the organisation, recognising employees as a critical line of defence against cyber threats. All employees are required to complete mandatory cybersecurity and data protection training, including e-learning modules covering key risk areas and secure data handling practices. These are complemented by targeted awareness initiatives such as virtual cybersecurity workshops and simulated phishing campaigns, which are designed to simulate real-world cyber-attacks and reinforce employees' ability to recognise, respond to and report potential cyber incidents.

**Process:** The Group has strengthened its cybersecurity governance framework and incident management processes. Amongst other things, StarHub has implemented a vulnerability disclosure program to enable security researchers to report potential vulnerabilities to StarHub via a publicly accessible website. Since FY2023, StarHub launched a new Bug Bounty Program to further enhance proactive identification and remediation of security weaknesses in the Group's IT applications.

**Technology:** A multi-layered security architecture has been implemented to protect against internal and external threats. The different technology stacks are designed to enhance prevention, detection, response and recovery capabilities across the Group's 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 is committed to accountable data protection practices and has been certified with the Data Protection Trustmark (**DPTM**) since 2020. The DPTM certification reflects StarHub's adherence to the PDPA, and alignment with the international benchmarks and recognised best practices. To maintain compliance with all applicable data protection laws and regulations, StarHub conducts regular reviews of its data protection frameworks and awareness programmes.

In FY2025, StarHub refreshed its PDPA training materials, and implemented mandatory annual data protection training for all employees and relevant key vendors. The Group has also partnered with OneTrust to enhance its privacy management initiatives, including the conduct of privacy impact assessments, maintenance of a centralised personal data inventory, and enhanced oversight of vendors processing personal data. The OneTrust platform enables a consistent and efficient approach to data protection across the Group's operations.

➡ *Further details on StarHub's approach to cybersecurity and data protection can be found in the 'Cybersecurity' chapter and the 'Our Data Protection' sub-topic under the Ethical Business Practices' chapter of the Sustainability Report 2025.*

## F. 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 FY2025, StarHub continued its hybrid working arrangements, allowing greater flexibility and work-life balance for employees. The Group recognises that a safe and healthy workplace is fundamental to employee welfare, operational resilience and sustainable business performance.

Oversight of workplace safety and health is supported by StarHub's Workplace Safety and Health (**WSH**) Committee, which plays an active role in enhancing the Group's safety

management framework. The WSH Committee regularly reviews workplace safety and health policies, procedures and practices to ensure alignment with industry best practices and compliance with applicable laws and regulations, including the WSH Act and its subsidiary legislation.

Through ongoing monitoring, reviews and continuous improvement initiatives, the Group seeks to maintain a safe working environment, minimise workplace risks and foster a culture of shared responsibility for safety and well-being among employees and Management.

➔ Further details on StarHub's approach to workplace safety and health can be found in the 'People and Workforce Resilience' chapter of the Sustainability Report 2025.



Strengthening cyber resilience is fundamental to maintaining trust. Cybersecurity is a continuous journey that demands constant learning, adaptation and evolution in an increasingly dynamic threat landscape. ”



JOSEPHINE  
CHEN  
Information  
Security