

Sustainability Pillars

Governance and Business Ethics



VTech promotes a culture of integrity, accountability and innovation throughout the Company. It also ensures that its corporate governance framework complies with the applicable laws and regulations as well as industry best practice with effective internal control and risk management systems in place.

Highlights:

- Provided training on code of conduct, cyber security and intellectual property right protection
- Provided training on anti-corruption for directors, senior management and general staff



VTech has developed a comprehensive management structure throughout the years. We have continuously reviewed our company policies and procedures to ensure our corporate governance structure meets the applicable laws and regulations, industry best practice, global trends, and market expectation. To achieve these goals requires both broad ranging and in-depth governance structures and risk management processes.

Corporate Governance



Risk Management and Sustainability Committee

Effective risk management is crucial for maintaining our stable daily operation and indicates our ability to respond and adapt to the changing environment. In order to minimise the possible disturbances to our operation during the event of disruptions, it is important to be prepared for emergency and to build resilience in the face of adversity. VTech has implemented an organisational structure with formal and clearly defined lines of responsibility and delegation of authority. There are also established procedures for financial planning, capital expenditure, treasury transactions, information and reporting systems, and monitoring the Group's businesses and their performance.

The RMSC is chaired by Dr. Allan WONG Chi Yun – Chairman and Group Chief Executive Officer (Chairman & Group CEO) with Dr. PANG King Fai – Group President, Mr. Andy LEUNG Hon Kwong – Chief Executive Officer of CMS (CMS CEO), Mr. WONG Kai Man – independent non-executive Director (INED), Mr. Hillson CHEUNG Hoi – President of TEL Products (TEL President), Ms. Shereen TONG Ka Hung – Group Chief Financial Officer (Group CFO) and Mr. CHANG Yu Wai – Company Secretary and Head of Internal Audit (Co Sec & Head of IA), as members – a combination of executive Directors, an INED and senior management.



The RMSC is responsible for monitoring and reviewing the risk management and internal control systems, as well as the sustainability strategies, performance and activities of the Group on a regular basis.

The RMSC has also developed an internal risk management structure at both management and operational levels, which has clearly defined the roles and responsibilities in managing potential risks in the respective areas, and set up procedures for execution of the Group's Business Continuity Plan in the event of disruptions.

The Company maintains a Risk Register to record the major and identifiable risks in the critical functions in the operation of the Company. The Risk Register is reviewed by the RMSC on a biannual basis. At management level, department representatives of each key business unit/function maintain a risk register documenting the key risks and the mitigation measures for the relevant risk. To facilitate the review of the Risk Register by the RMSC, the Internal Audit Department will review the effectiveness and operation of the risk management framework, including the frequency of reporting to the Board, and the continuing operation of appropriate mitigation measures.

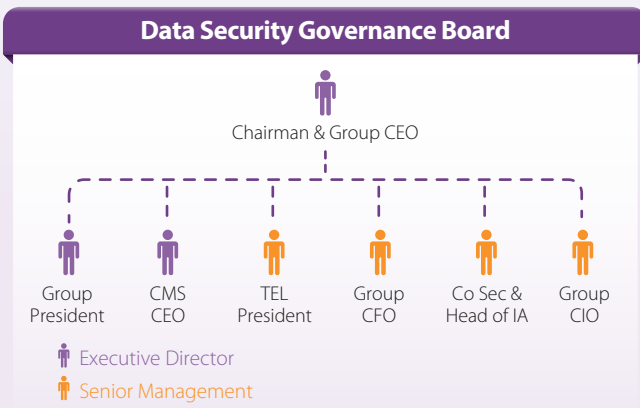
Sustainability Pillars



The RMSC has held two meetings during the financial year to review the Group’s risk management and internal control systems, and its sustainability strategies, policies and activities.

Data Security Governance Board

The Data Security Governance Board was established with defined terms of reference reporting to the RMSC. The Data Security Governance Board is chaired by Chairman and Group CEO and comprises the Group President, CMS CEO, TEL President, Group CFO, Co Sec & Head of IA, and Group Chief Information Officer (Group CIO). It is responsible for decision-making, implementation, enforcement, oversight, compliance and periodic review of the Data Security Policy and practices, as well as the cybersecurity risks and mitigation measures of the Group. It also ensures that the Group’s data security practices are compliant with international and local laws and regulations, including but not limited to, the applicable privacy ordinances and data protection regulations in the respective countries such as the General Data Protection Regulation in Europe. The Data Security Governance Board has held two meetings during the financial year. It has reviewed and monitored the implementation and execution of the Data Security Policy and practices of the Group for the compliance with the latest privacy ordinances and data protection regulations in the respective countries. It has also reviewed the implementation progress of the additional preventive measures, technologies enhancement and staff trainings for the mitigation of cybersecurity risks of the Group. In addition, the Data Security Governance Board has reviewed and monitored the remedial actions of the identified security related issues which have been brought to its attention.



Investor Communication

All of the Group’s investor communications are governed by a Shareholders Communication Policy. The Policy sets out the procedures for providing shareholders and investment community with ready, equal and timely access to balanced and understandable information about VTech.

For details of our Shareholders Communication Policy, please refer to www.vtech.com/en/investors/corporate-governance/shareholders-communication-policy/

Regulatory Requirements

We are in full compliance of the Listing Rules of the Stock Exchange. Regular training is delivered by professionals to our staff on the update of Listing Rules and requirements. We keep monitoring the update of the Stock Exchange’s ESG Guideline and update our sustainability report accordingly.

Risk management



ESG Risks and Opportunities

The RMSC has oversight of all ESG issues including ESG risks. It is responsible for identifying and evaluating ESG risks and opportunities. ESG risks are reviewed in the RMSC biannual meetings as well as the Board meetings.

ESG risk management and opportunities are integrated into our Sustainability Plan 2025. Please refer to pages 41-45 for details of climate-related risks and opportunities.

Business Continuity Management

Business Continuity Management (BCM) is important for ensuring that we always have a smooth business operation. Our BCM programme not only helps us to identify and mitigate our potential operational risks, but also increases our resilience capability, in the event of disruptions, to resume our operations in an effective and timely manner. VTech’s RMSC has developed an internal risk management structure at both the management and operational levels, which has clearly defined the roles and responsibilities in managing the potential risks in the respective areas, and set up procedures for the execution of our Business Continuity Plan (BCP) in the event of disruptions. At each of our key business functions, the management team who is responsible for BCM, consisting of the senior management at the operational level of the relevant departments, is given the responsibility for developing and executing the BCP to ensure the continuous operation of the critical and essential functions of the Company in the event of emergency or business interruption. We have adopted a four-step BCM framework to identify the events that could affect our operation, assess the identified risks, establish measures and controls to manage the impacts with recovery actions, and review and monitor the BCP for continuous improvement on a regular basis. Facing the unprecedented challenges from COVID-19, we have developed a comprehensive set of precautionary measures and guidelines to tackle the issue following the BCM framework, to ensure the health and safety of the employees and our operation and business continue to run smoothly. For details of the measures, please refer to pages 58-59 under “Environment for our people”.

BCM Framework of VTech

Step 1: Identification of Potential Event of Disruption

Step 2: Assessment of Identified Risks

Step 3: Establish Measures and Controls

Step 4: Monitor and Review the Effectiveness of BCP

Cyber Security

The proliferation of new technologies has significantly changed the ways people access information. VTech has established a multifaceted cyber security programme with data and system security policies and measures in place to protect the data and information from any unauthorized access, accidental loss or destruction.

The Data Security Governance Board reporting to the RMSC established at the Board level, is also responsible for ensuring that our data security practices are compliant and aligned with international and local laws and regulations, including but not limited to the applicable privacy ordinances in the respective countries such as the General Data Protection Regulation in Europe.

To proactively detect cyber threats and system vulnerabilities, VTech has implemented fit-for-purpose security monitoring controls to proactively enhance infrastructure security while maintaining business productivity. These cover our network gateways, computing devices and business systems. We also manage risks of third-party vendors and partners by establishing a process to vet their security practices, ensuring adequate security measures are in place. Proper work-from-home policy under COVID-19 has been established without jeopardising the risk of network security.

For timely threat detection, other than subscribing to threat intelligence, we have engaged best-in-class penetration tester to review our network-connected products before rollout. For internal systems, we have also conducted security assessment regularly in order to meet international security standard. Regular risk assessment, internal and external audits mechanism will provide an extra eye on the threat detection and migration in a timely manner.

In response to the threat and incident handling, a proper procedure for incident escalation and handling have been established. We have also carried out incidence response drills to ensure that our cross-department response team is ready.

To ensure preparedness, our staff are required to attend mandatory cybersecurity awareness training and testing on a yearly basis and are subject to simulated phishing drills to maintain vigilance.

Business Ethics



Code of Conduct and Whistleblowing Policy

Our Code of Conduct serves as one of the cornerstones of our governance and operation, underpins our culture of integrity and represents the Group management's commitment to a vigorous, responsible and forward-looking compliance culture. It spells out the guiding principles for our corporate and staff behaviour and sets the high standards of integrity and honesty we apply in our operation and business. We have additional policies for staff in specific risk-related areas to cover conflicts of interest, bribery, accounting standards and internal management. Staff are required on joining to confirm that they understand and accept the requirements and standards laid down in the Code of Conduct appropriate to their role and position in the Company, and in addition, avail themselves to attend and complete various governance trainings provided online, and provide annual confirmation of compliance of the Code of Conduct in writing. Staff are required to strictly follow the Code of Conduct so that the Group operates to the highest standards of business behaviour and ethics in its engagement with customers, business partners, shareholders, employees and the community at large. Due to a constantly changing business environment and the emergence of increasing demands on responsible corporate behaviour, we assess our Code of Conduct periodically to ensure that it reflects the current industry and global best practices and meets the expectations of all stakeholders.

VTech operates a Whistleblowing Policy in order to encourage and assist whistleblowers to disclose information relevant to misconduct, malpractices or irregularities through a confidential reporting channel without the fear of recrimination. Any cases are referred to the Group Chief Compliance Officer, who will review the complaints and determine the appropriate mode of investigation and any subsequent corrective action. Recommendations on improvements are communicated to the respective department's senior management for implementation. All reported cases are handled by the Company with care and the concerns are investigated in a fair and proper manner. All reports under the Whistleblowing Policy are reviewed by the Group's Audit Committee on a biannual basis in order to ensure proportionate action and identify the need for any further policy development.

Full details of our Whistleblowing Policy and Code of Conduct are available on

www.vtech.com/en/investors/corporate-governance/whistleblowing-policy/
www.vtech.com/en/investors/corporate-governance/code-of-conduct/

Sustainability Pillars



Business Integrity and Anti-Corruption Policies

The Company is committed to zero tolerance towards corruption and a culture of integrity. It promotes the core values of integrity, honesty, fairness, impartiality and ethical business practices. VTech Group and its officers, employees, agents and intermediaries are prohibited from giving or offering to give money or anything of value to any third party including government officials, political parties, party officials or candidates for political office in order to influence the commercial acts or official duties or decisions of that person or entity, obtain or retain business, or secure any improper advantage. The Company does not make any donations to political parties in any country but it does not restrict employees from joining or participating in individual associations provided that there is no conflict of interest between their role as a member of the association and their role as an employee within VTech. Employees must not represent or purport to represent the Company in any social or political forum and should not use the Company brand, time or assets to advance the interests of any social or political party or group.

Anti-corruption is one of the major governance areas covered by the Code of Conduct. In addition to the anti-corruption policy, the Company has also issued policy on offer and receipt of gifts, entertainment and gratuities. VTech's management ensures that employees are familiar with these policies and the related control procedures in their job areas. Employees receive regular anti-corruption and internal control training to reinforce their awareness and understanding of our Code of Conduct and the relevant policies.

For details of our Code of Conduct and the anti-corruption policy, please refer to www.vtech.com/en/investors/corporate-governance

Anti-Corruption Training to Directors and Staff

Anti-corruption training is provided to our staff via our eLearning platform to facilitate continuous learning on the topic. The training covers anti-corruption laws and common corruption pitfalls in the private sector and the roles of staff in corruption prevention. New joiners are required to complete the online course within their first 3 months. The online training can also be accessed by Directors and senior management, with specific training materials provided. Due to social distancing restrictions, the Independent Commission Against Corruption of Hong Kong (ICAC) representative was invited to deliver a virtual training for Hong Kong staff, with the focus of corruption prone areas at workplace, such as inventory control, procurement process and cross boundary business operations, etc.

Privacy and Data Protection

We acknowledge the importance of privacy security to our stakeholders. Privacy and data protection is also an essential consideration in the workplace. We have developed privacy and data protection policies and data handling practices that cover how we collect, use, disclose, transfer and store stakeholders' personal information.

Consumer personal information is usually collected from our online shop, authorised dealers or agents and media channels for enquiries and complaints whenever necessary to provide services to the consumer. We are committed to using the consumer personal information we have collected only for the purpose intended and notified. VTech will not sell the personal information to a third party for any consideration.

As required by the Data Security Governance Board, a designated Data Protection Officer has been appointed to ensure VTech's compliance with privacy regulations, and VTech privacy and data protection policies. A privacy and data protection team has also been established which assists the Data Protection Officer to prepare any actions needed for the compliance with particular privacy legislation. The privacy and data protection team consists of business managers of different departments regularly involved in the processing of personal data.

Protection of Intellectual Property Right

VTech is devoted to protecting its own intellectual property rights, whilst respecting the intellectual property rights of others as well. VTech has proper policy and protocol in place to protect its intellectual property rights including, but not limited to its patents, designs, technologies, trademarks, trade secrets, copyrights, computer programmes, inventions, product information, video and sound recordings. Without our permission, a third party cannot own or display any related intellectual properties. The Company will take legal actions and seek for judgment against any violations of its intellectual property rights or misuse of its intellectual properties.

For details of our intellectual property rights protection measures, please refer to www.vtech.com/en/investors/corporate-governance

Global Tax Policy

VTech is committed to full compliance with all statutory obligations, full disclosure to relevant tax authorities, and to act in a way which upholds its reputation as a responsible corporate citizen. The Group's tax affairs are managed in a way which takes into account the Group's wider corporate reputation in line with VTech's overall high standards of governance.

Each group company has the responsibility to understand and comply with tax laws and regulations applicable to its business, with support from the external tax advisors. We have implemented a series of processes and controls to identify, manage and report tax risk appropriately. These include regular updates from Finance teams; documented review processes and regular training for staff involved in tax return preparation and review.