Safeguarding Data

Data Privacy

Policy and Principle

We are dedicated to protecting and respecting the data we hold and process, in accordance with the laws and regulations of the markets in which we operate. Our approach rests on having the right talent, technology, systems, controls, policies and processes to help ensure the appropriate management of privacy risk. Our Group-wide privacy policy and principles aim to provide a consistent global approach to managing data privacy risks, and must be applied in all of our global businesses and global functions.

We have procedures in place to articulate the actions required in data privacy considerations. These include notifying regulators, customers or other data subjects, as required under applicable privacy laws and regulations, in the event of a reportable incident occurring.

Our policy covers a number of principles, including the Group's Data Privacy Principles, that set out the ways we manage data privacy risks at a high level. The implementation of these principles and the risk management methodology is kept on track with our control mechanisms.

We regularly perform risk and control assessments on data privacy risks and capture the details in our non-financial risk record system. Formal governance forums have been established on data risks, including data privacy risks, which allow our senior leaders to make active risk management decisions.

Data Privacy Principles are set out to manage our data privacy risks. These principles are intended to:

- Set out good data privacy practices
- Show our accountability and compliance with the data privacy laws and regulations
- Outline the Bank's commitment to how it processes identifiable data

The following controls have been implemented in order to manage our data privacy risks.

Records of Processing	To understand the identifiable data processed by the Bank, record the details of how the Bank processes such identifiable data, and keep evidence of the process, in order to make sure the Bank can demonstrate that it complies with the relevant data privacy laws.
Privacy Impact Assessments	To make sure that there is timely identification of data privacy risks arising from a new form of use, or a change in the processing of the identifiable data, and to make sure that the risks identified are properly managed before any new form of use, or changes in the processing of the identifiable data.
Internal and External Data Transfers	To make sure that any transfers of identifiable data are approved, and such transfers are compliant with the data privacy laws and the Bank's policies with respect to data privacy. This includes both internal transfers (transfers between the Group entities in any jurisdiction) and external transfers.
Data Disclosures	To make sure that external disclosures of identifiable data are processed in a timely, consistent, compliant and accurate manner, and in compliance with the relevant data privacy laws. These disclosures are usually made in response to external requests.
Rights of Individuals	To make sure the Bank can respond in a timely and compliant way to an exercise of rights by, or on behalf of, an individual relating to the data we hold about them, and to comply with the relevant data privacy laws.
Privacy Notice	To make sure we provide individuals with a clear, transparent statement about the fair and lawful processing of identifiable data in line with the relevant data privacy laws.
Consent and Choice	To make sure any 'consent' required for the processing of identifiable data is obtained, tracked and managed on an ongoing basis in line with the relevant data privacy laws.

Safeguarding Data

Customer Privacy

Our customers are notified about our collection and use of personal data, as well as the classes of transferees, classes of marketing subjects, their data access and their right to correct personal data. Customers can easily access our Privacy Policy, Notice to Customers and Other Individuals relating to the Personal Data (Privacy) Ordinance, and the Cookies Policy on our website.

We understand that our people play an important role in protecting our stakeholders from data security and data privacy risks. Our mission is to equip every one of our colleagues with the appropriate tools and behavioural guidelines they need to keep our organisation and customers safe. We provide cybersecurity and data privacy training to all of our staff, ranging from our top executives to front-line relationship managers, in order to increase their awareness of data security and privacy.

We also organise annual training programmes for our staff, covering specific topics on data security and data privacy risks and controls.

Our website includes a dedicated section on security controls, which is aimed at reminding our customers to stay vigilant of any fraudulent activities, in which fraudsters could use deceptive tactics to gain access to their personal information. The website section also covers tips on how to avoid falling victim to bogus calls and SMS.

Following the procedures in our Material Incidents Escalation Manual, our staff members are required to report the case details immediately after becoming aware of material incidents to the Business Risk and Control Management or Chief Control Office team. Our experts will investigate and, where appropriate, escalate the matter to the core team. To support our ongoing improvements, these experts also provide guidance on how to contain and respond to cases, and identify remedies and lessons learned.

Customer privacy upheld complaints identified*

Incoming Channel	
Outside parties	0
By the Bank	8
Regulatory bodies	0
Total	**8**

Type	
Leaks	6
Thefts	0
Losses of customer data	2
Others	0
Total	**8**

* Upheld means the cases were considered legitimate after an internal investigation.

Cybersecurity

The cyber threat landscape continues to evolve at a fast pace, while controls designed to effectively mitigate cybersecurity risks become outdated over time. Our stakeholders expect us to take the necessary steps in order to protect the markets, as well as their data and business interests to the best standards. Over the years, we have invested in attaining good practice standards for cybersecurity and we are dedicated to maintaining this position in the future.

It is necessary to conduct ongoing reviews of our cyber risk appetite and maintain the ongoing effectiveness of our controls in mitigating these risks, in order to maintain good practice standards under the current dynamic environment, in which cyber threats evolve over time. While in most cases, it is extremely difficult to reduce the potential impact of a cyberattack, it is however possible, through an investment in ongoing controls, to reduce the overall likelihood of a cyber risk being realised. A continued re-evaluation of the effectiveness and an investment in the maintenance and enhancement of these controls can enable the Bank to keep the residual risk at an acceptable level.

We make an ongoing investment in our defence against ever more sophisticated cyberattacks. Specifically, we have enhanced our event detection, incident responses, secure development, vulnerability remediation and protection against malware, application layer attacks and data leakages. We have also strengthened our third party management by including cybersecurity due diligence, through which a stricter governance system and measures including enforced third party security testing prior to the approval of a contract are implemented.

The entire IT infrastructure of our operations has adopted the National Institute of Standards and Technology ('NIST') framework, which is an industry standard. Banks are high-profile targets for criminals seeking financial gain, personal information and disruption, which may potentially lead to financial loss, reputational damage and customers loss. Protecting our customers and the Bank from such threats is a key component in our strategy to become a connected business.

Risk governance forums, such as the Board-delegated Risk Committee and Risk Management Meeting, are regular meetings held to ensure our governance and control framework is properly discharged, managed, sustained and communicated. To protect our operations against compliance risks, we have strong and transparent corporate governance measures in place.

Regular reporting on our strategic programme and key indicators supports the Board and senior management in exercising their oversight of cybersecurity. Our cybersecurity strategy is reviewed and the business risk profiles, mitigation awareness, internal and external cybersecurity incidents, as well as the regulatory requirements are discussed.

Safeguarding Data

Cybersecurity drills are also conducted with the Board and senior management, to rehearse the types of decisions that may need to be taken, and to reconfirm the individual roles and responsibilities during a major cyber incident. These drills are conducted periodically to enhance the level of understanding in terms of the roles, protocols, internal communication paths and escalation procedures across the business landscape in the event of a cyberattack. Phishing tests are also conducted on a regular basis to raise the level of security awareness throughout the organisation.

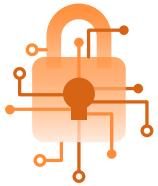
A 24/7 hotline is available for our staff to report a cybersecurity incident immediately upon its occurrence. These incidents are handled by our cybersecurity analyst and Security Operations Centre, then they are reported to our management personnel to seek direction on the remediation. Cybersecurity incident response procedures have also been established and are tested regularly.

In terms of cybersecurity training, automated cybersecurity assessment tools are available to all users, such as executives and their assistants, IT end users, software developers, third party service providers, etc. Vulnerabilities across the network, operating systems, application layers and in-house custom software are managed through a centralised platform, and are remedied according to their priority.

Throughout 2023, cybersecurity awareness and training regarding data security was delivered to all staff, including the security community, on a regular or as needed basis. It covered topics such as data security, email security and phishing, access control, incident reporting and escalation, secure use of communication devices and social media, information classification and labelling, etc.

Cybersecurity training or communication in 2023 included:

- Mandatory e-learning for all employees
- Briefings to the Board and Executive Committee members
- Role-specific training for staff who play an integral part in the Global Businesses and Global Functions and are responsible in the effective management of information security risks
- Training for executive assistants and IT staff
- Seminars hosted by senior leaders which also featured expert speakers



>99%

Employees who completed the mandatory cybersecurity training in the correct timeframe

>90%

IT developers who hold at least one of our internal secure developer certifications