Personal Data Security Measures of the SEC Office

The Office of the Securities and Exchange Commission, Thailand (the "SEC Office") maintains your personal data as follows:

1. Storage

Personal data is stored in the SEC Office's centralized database, where data security is maintained and access rights are defined through access control.

2. Storage location

Personal data is stored in the SEC Office's central data center, where access to the data center room is controlled, and on cloud systems provided by cloud service providers engaged by the SEC Office. The cloud service providers engaged by the SEC Office are recognized providers that meet accepted standards. The SEC Office also regularly monitors the services provided by such cloud service providers.

Category of Security Measures	Security Measures
Data Center and Cloud Service Providers of the SEC Office	• The information security management system of the SEC Office's data center and cloud service providers complies with ISO/IEC 27001 and the NIST Cybersecurity Framework (NIST CSF). • The privacy information management of the SEC Office's data center and cloud service providers complies with ISO/IEC 27701.
Online systems through which the SEC Office provides digital services, including: • Approval systems • Licensing systems • Directors and executives of	• Access control to personal data and components of key information systems is implemented on a need-to-know basis and in accordance with the principle of least privilege. • User access management is implemented.

Category of Security Measures	Security Measures
listed companies and securities-issuing companies database systems • Systems for approving issuers and offerors, including reporting results of offerings • Filing systems • Systems for approval of fund establishment and management	● User responsibilities are defined to prevent unauthorized or unlawful access to, use, modification, alteration, deletion, or disclosure of personal data. ● Audit trail mechanisms are in place to enable retrospective verification of access to, modification, alteration, or deletion of personal data.

3. Retention period

The SEC Office has established retention periods for personal data in accordance with its Data Retention Policy. Documents are classified into seven categories as follows:

Category	Retention Period	Examples of Documents
1.	Retained at the SEC Office for 2 years Subsequently stored at the warehouse for 8 years	Circulars, outgoing correspondence, memoranda, and external documents (non-confidential)
2.	Retained at the SEC Office for 5 years Subsequently stored at the warehouse for 5 years	Circulars, outgoing correspondence, memoranda, and external documents (confidential)
3.	Retained at the SEC Office for 10 years Subsequently stored at the warehouse for 10 years	Memoranda, letters to complainants signed by SEC executives, and monthly complaint summary reports by the SEC Complaint Center

Category	Retention Period	Examples of Documents
4.	Retained at the SEC Office for 10 years Not subsequently stored at the warehouse	Summonses for clarification, orders requiring parties to appear, and court orders
5.	Permanently retained at the SEC Office	Settlement case records / letters to offenders
6.	Not retained at the SEC Office Stored at the warehouse for 10 years	Documents designated by the responsible department as not requiring receipt
7.	Retained at the SEC Office for 2 years Not subsequently stored at the warehouse	Seminar and event documents