มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลของสำนักงาน

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน) เก็บรักษาข้อมูลส่วนบุคคลของท่าน ดังนี้

1. การจัดเก็บ

จัดเก็บข้อมูลในฐานข้อมูลกลางของสำนักงานที่มีการดูแลและรักษาความมั่นคงปลอดภัยของข้อมูล (Security) รวมถึงมีการกำหนดสิทธิในการเข้าถึงข้อมูล (Access Control)

2. สถานที่จัดเก็บ

ข้อมูลส่วนบุคคลถูกจัดเก็บในศูนย์คอมพิวเตอร์กลางของสำนักงานที่มีการควบคุมสิทธิการเข้าห้องศูนย์คอมพิวเตอร์ และจัดเก็บบนคลาวด์ (Cloud) โดยผู้ให้บริการระบบคลาวด์ (Cloud Service Provider) ที่สำนักงานใช้บริการเป็นผู้ให้บริการที่ได้มาตรฐานเป็นที่ยอมรับ อีกทั้งสำนักงานมีการตรวจสอบการให้บริการของผู้ให้บริการระบบคลาวด์อย่างสม่ำเสมอ

ลำดับของ มาตรการรักษาความมั่นคงปลอดภัย	มาตรการรักษาความมั่นคงปลอดภัย
Data Center และ Cloud Service Provider ของสำนักงาน	● ระบบการบริหารจัดการความมั่นคงปลอดภัย (Information Security Management System) ของ Data Center และ Cloud Service Provider ของสำนักงาน ได้มีการปฏิบัติตามมาตรฐาน ISO/IEC 27001 และ NIST CSF ● การบริหารจัดการข้อมูลส่วนบุคคล (Privacy Information Management) ของ Data Center และ Cloud Service Provider ของสำนักงาน ได้มีการปฏิบัติตามมาตรฐาน ISO/IEC 27701
ระบบงานออนไลน์ที่สำนักงานให้บริการด้านดิจิทัล (Digital Services) ได้แก่ ● ระบบให้ความเห็นชอบ ● ระบบให้ใบอนุญาต	● มีการควบคุมการเข้าถึงข้อมูลส่วนบุคคลและส่วนประกอบของระบบสารสนเทศที่สำคัญ (access control) โดยคำนึงถึงสิทธิเท่าที่จำเป็น (need-to-know-basis) ตามหลักการให้สิทธิที่น้อยที่สุดเท่าที่จำเป็น (principle of least privilege) ● มีการบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management)

● ระบบข้อมูลรายชื่อกรรมการและผู้บริหารของบริษัทจดทะเบียนและบริษัทที่ออกหลักทรัพย์ ● ระบบอนุญาตเป็นผู้ออก ผู้เสนอขาย รวมถึงรายงานผลการขาย ● ระบบรับแบบรายงาน ● ระบบอนุมัติจัดตั้งและจัดการกองทุน	● มีการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข ลบ หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ● มีการจัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง แก้ไข หรือลบข้อมูลส่วนบุคคล (audit trails)

3. ระยะเวลาจัดเก็บ

มีการกำหนดระยะเวลาจัดเก็บข้อมูลส่วนบุคคลตามนโยบายการเก็บรักษาข้อมูลส่วนบุคคล (Data Retention Policy โดยได้แบ่งเอกสารเป็น 7 กลุ่ม ดังนี้

กลุ่ม	ความหมาย	ตัวอย่างประเภทเอกสาร
1.	เก็บที่สำนักงาน 2 ปี เก็บต่อที่โกดัง 8 ปี	หนังสือเวียน/หนังสือออก/บันทึก/เอกสารจากภายนอก (ไม่ลับ)
2.	เก็บที่สำนักงาน 5 ปี เก็บต่อที่โกดัง 5 ปี	หนังสือเวียน/หนังสือออก/บันทึก/เอกสารจากภายนอก (ลับ)
3.	เก็บที่สำนักงาน 10 ปี เก็บต่อที่โกดัง 10 ปี	บันทึก/หนังสือตอบผู้ร้องเรียนที่ลงนามโดยผู้บริหารระดับสูง/รายงานสรุปเรื่องร้องเรียนของ Help Center รายเดือน
4.	เก็บที่สำนักงาน 10 ปี ไม่ได้เก็บที่โกดัง	หมายเรียกให้ทำคำชี้แจง / คำสั่งเรียกคู่กรณี / คำสั่งศาล
5.	เก็บที่สำนักงานตลอดไป	วาระเปรียบเทียบ / หนังสือถึงผู้กระทำความผิด
6.	เก็บที่สำนักงาน 0 ปี เก็บต่อที่โกดัง 10 ปี	งานที่ฝ่ายงานแจ้งว่าไม่รับเอกสาร
7.	เก็บที่สำนักงาน 2 ปี ไม่เก็บต่อที่โกดัง	เอกสารการจัดสัมมนา