มาตรฐานเกี่ยวกับการซื้อขายหลักทรัพย์ผ่านระบบการซื้อขาย

ตามที่ข้อ 6 ของประกาศตลาดหลักทรัพย์แห่งประเทศไทย เรื่อง วิธีปฏิบัติที่เกี่ยวกับการซื้อขาย การชำระราคาและการส่งมอบหลักทรัพย์ในตลาดหลักทรัพย์ พ.ศ. 2560 กำหนดให้สมาชิกต้องจัดให้มีระบบส่งคำสั่งซื้อขายของสมาชิกที่มีการทำงานและที่มีระบบการบริหารและควบคุมความปลอดภัยในการปฏิบัติงาน (Security Management) ที่ได้มาตรฐานตามที่ตลาดหลักทรัพย์กำหนด

ตลาดหลักทรัพย์เห็นควรกำหนดมาตรฐานของระบบส่งคำสั่งซื้อขายของสมาชิก ดังต่อไปนี้

ส่วนที่ 1 : การต่อเชื่อมระบบส่งคำสั่งซื้อขาย

1. <u>การต่อเชื่อมระบบส่งคำสั่งซื้อขายของสมาชิก (Broker Front Office) เข้ากับระบบการซื้อขาย</u>

ระบบส่งคำสั่งซื้อขายของสมาชิกที่ต่อเชื่อมกับระบบการซื้อขายต้องมีลักษณะและเป็นไปตามหลักเกณฑ์ดังต่อไปนี้

1.1 สมาชิกต้องมีการบันทึกการทำงานของ Broker Front Office ที่สามารถนำมาตรวจสอบได้ทันทีเมื่อตลาดหลักทรัพย์ร้องขอ

1.2 สมาชิกต้องมีการบริหารจัดการด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ รวมทั้งมีระบบรักษาความปลอดภัยในการปฏิบัติงานที่ปลอดภัยเพียงพอ และเป็นไปตามมาตรฐานความปลอดภัยสำหรับระบบที่ต่อเชื่อมกับระบบการซื้อขาย

2. <u>การต่อเชื่อมระบบสำหรับการซื้อขายหลักทรัพย์ผ่านระบบอินเทอร์เน็ต</u>

การซื้อขายหลักทรัพย์ผ่านระบบอินเทอร์เน็ต เป็นการซื้อขายที่กระทำผ่านระบบที่มีลักษณะและเป็นไปตามหลักเกณฑ์ ดังต่อไปนี้

2.1 เป็นการส่งคำสั่งซื้อขายของลูกค้าที่ผ่าน Broker Front Office

2.2 สมาชิกต้องมีการบันทึกการทำงานของ Broker Front Office ที่สามารถนำมาตรวจสอบได้ทันทีเมื่อตลาดหลักทรัพย์ร้องขอ

2.3 สมาชิกต้องมีการบริหารจัดการด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ รวมทั้งมีระบบรักษาความปลอดภัยในการปฏิบัติงานที่ปลอดภัยเพียงพอ และเป็นไปตามมาตรฐานความปลอดภัยสำหรับระบบที่ต่อเชื่อมกับระบบการซื้อขาย

2.4 สมาชิกต้องจัดให้มีระบบหรือกระบวนการตรวจสอบคำสั่งซื้อขายของลูกค้าก่อนส่งเข้ามาในระบบการซื้อขาย

2.5 ในกรณีที่สมาชิกพัฒนาหน้าจอในการส่งคำสั่งซื้อขายให้ลูกค้าสามารถส่งคำสั่งได้มากกว่า 1 คำสั่งต่อหน้าจอ สมาชิกต้องมีการจำกัดจำนวนคำสั่งให้ไม่เกินจำนวนที่ตลาดหลักทรัพย์กำหนด และมีระบบป้องกันความเสี่ยงอย่างเหมาะสม

การซื้อขายหลักทรัพย์ด้วยโทรศัพท์เคลื่อนที่หรืออุปกรณ์ประเภทเดียวกัน จัดเป็นการซื้อขายหลักทรัพย์ผ่านระบบอินเทอร์เน็ตเช่นกัน จึงมีโครงสร้างระบบเช่นเดียวกับที่กล่าวมาข้างต้น

3. <u>การต่อเชื่อมระบบสำหรับการซื้อขายหลักทรัพย์ที่ลูกค้าส่งคำสั่งซื้อขายทางอิเล็กทรอนิกส์ผ่านระบบ Direct Market Access (DMA)</u>

การซื้อขายหลักทรัพย์ผ่านระบบ DMA ให้กระทำผ่านระบบที่มีลักษณะและเป็นไปตามหลักเกณฑ์ ดังต่อไปนี้

3.1 เป็นการส่งคำสั่งซื้อขายจากระบบของลูกค้ามายังระบบของสมาชิกก่อนส่งเข้ามายังระบบการซื้อขาย โดยคำสั่งซื้อขายดังกล่าวต้องผ่านระบบตรวจสอบคำสั่งซื้อขายที่สมาชิกมีอำนาจควบคุมและบริหารจัดการได้

3.2 ระบบของสมาชิกที่ให้บริการซื้อขายหลักทรัพย์ผ่านระบบ DMA ต้องมีการบันทึกการทำงานของระบบส่งคำสั่งซื้อขาย เช่น Order Log และ Message ระหว่างระบบตามมาตรฐานที่ตลาดหลักทรัพย์กำหนด เป็นต้น ซึ่งสามารถนำมาตรวจสอบได้ทันที และนำส่งให้ตลาดหลักทรัพย์ได้เมื่อตลาดหลักทรัพย์ร้องขอ

3.3 มีระบบตรวจสอบคำสั่งซื้อขายก่อนส่งเข้ามาในระบบการซื้อขาย โดยมีการตรวจสอบอย่างน้อยในเรื่องดังต่อไปนี้

(1) วงเงินซื้อขาย (Credit / Exposure Limit)

(2) มูลค่าเสนอซื้อขายสูงสุดต่อ 1 คำสั่ง (Maximum Value Per Order)

(3) ปริมาณหุ้นที่เสนอซื้อขายสูงสุดต่อ 1 คำสั่ง (Maximum Volume Per Order)

(4) ราคาเสนอซื้อขาย (Order Price Check)

3.5 สมาชิกต้องมีการบริหารจัดการด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ รวมทั้งมีระบบรักษาความปลอดภัยในการปฏิบัติงานที่ปลอดภัยเพียงพอ และเป็นไปตามมาตรฐานความปลอดภัยสำหรับระบบที่ต่อเชื่อมกับระบบการซื้อขาย

4. <u>การต่อเชื่อมระบบส่งคำสั่งซื้อขายสำหรับบริษัทหลักทรัพย์ที่มิใช่สมาชิก</u>

สมาชิกที่จะให้บริษัทหลักทรัพย์ที่มิใช่สมาชิก (Sub-Broker) ต่อเชื่อมอุปกรณ์คอมพิวเตอร์เข้ากับระบบส่งคำสั่งซื้อขายของสมาชิก ต้องปฏิบัติตามหลักเกณฑ์ ดังต่อไปนี้

4.1 สมาชิกต้องมีระบบบริหารจัดการคำสั่งซื้อขายที่ได้รับจากบริษัทหลักทรัพย์ที่มิใช่สมาชิกที่ปลอดภัยเพียงพอ และเป็นไปตามมาตรฐานความปลอดภัยสำหรับระบบที่ต่อเชื่อมกับระบบการซื้อขาย

4.2 ระบบบริหารจัดการคำสั่งซื้อขายต้องสามารถจำแนกคำสั่งและรายการซื้อขายของบริษัทหลักทรัพย์ที่มิใช่สมาชิกจากคำสั่งและรายการซื้อขายของสมาชิกได้ และต้องมีการบันทึกการทำงานของ Broker Front Office โดยสามารถนำมาตรวจสอบได้ทันทีเมื่อตลาดหลักทรัพย์ร้องขอ

4.3 สมาชิกต้องมีระบบในการกำกับดูแลการส่งคำสั่งซื้อขายของบริษัทหลักทรัพย์ที่มิใช่สมาชิก

4.4 สมาชิกต้องจัดให้มีระบบ/ฟังก์ชันที่สามารถหยุดการส่งคำสั่งซื้อขายใหม่ และยกเลิกคำสั่งซื้อขายที่ส่งเข้ามาแล้วได้ทันทีในกรณีจำเป็น (Kill switch)

4.5 ในกรณีที่บริษัทหลักทรัพย์ที่มิใช่สมาชิกได้รับอนุญาตให้เป็นนายหน้าซื้อขายหลักทรัพย์เฉพาะประเภทหลักทรัพย์ตามที่กฎหมายกำหนด บริษัทสมาชิกต้องจัดให้มีระบบป้องกันมิให้บริษัทหลักทรัพย์ที่มิใช่สมาชิกซื้อขายหลักทรัพย์อื่นนอกเหนือจากหลักทรัพย์ที่ได้รับอนุญาต

ส่วนที่ 2 : มาตรฐานความปลอดภัยสำหรับระบบที่ต่อเชื่อมกับระบบการซื้อขาย

วัตถุประสงค์หลักในการรักษาความมั่นคงปลอดภัยสำหรับระบบที่ต่อเชื่อมกับระบบการซื้อขาย มุ่งเน้นให้มีการบริหารจัดการที่เหมาะสมภายใต้หลักการ ดังนี้

- Confidentiality หมายถึง การรักษาความลับของระบบเทคโนโลยีสารสนเทศและข้อมูลอย่างเหมาะสม รวมถึงมีการจำกัดสิทธิ (Authorization) และการพิสูจน์ตัวตนอย่างครบถ้วน (Authentication)
- Integrity หมายถึง ระบบเทคโนโลยีสารสนเทศและข้อมูลจะต้องมีความถูกต้องครบถ้วน เช่น การไม่ถูกเปลี่ยนแปลงโดยไม่ได้รับอนุญาต ไม่มีการปลอมแปลงการใช้งาน ไม่เกิดการสูญหายโดยไม่ทราบสาเหตุ
- Availability หมายถึง ระบบเทคโนโลยีสารสนเทศและข้อมูลมีความพร้อมใช้งานสอดคล้องตามความจำเป็นและความต้องการของผู้ใช้งาน

ตลาดหลักทรัพย์กำหนดให้สมาชิกต้องจัดให้มีมาตรฐานความปลอดภัยสำหรับระบบที่ต่อเชื่อมกับระบบการซื้อขายตามประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ว่าด้วย การจัดให้มีระบบเทคโนโลยีสารสนเทศ[1] หรือประกาศที่เกี่ยวข้องกับเรื่องดังกล่าวที่อาจมีการแก้ไขหรือเพิ่มเติมในอนาคต

นอกจากการปฏิบัติตามมาตรฐานความปลอดภัยสำหรับระบบที่ต่อเชื่อมกับระบบการซื้อขายตามข้างต้นแล้ว สมาชิกต้องจัดให้มีมาตรฐานความปลอดภัยของแอพพลิเคชั่น (Application Security) เพิ่มเติมดังต่อไปนี้

1. มีการจำกัดการเข้าถึงข้อมูลและฟังก์ชันต่าง ๆ ของแอพพลิเคชั่นเฉพาะผู้ที่ได้รับอนุญาตเท่านั้น และการเข้าถึงจะต้องแยกตามประเภทของผู้ใช้งาน (User Role) รวมทั้งมีระบบการบันทึกข้อมูลการทำงานของแอพพลิเคชั่น (Audit Trail Log) อย่างเหมาะสม
2. ผู้ใช้งานระบบซื้อขายจะต้องผ่านการตรวจสอบและยืนยันความเป็นตัวตนว่าเป็นบุคคลที่ได้รับอนุญาตจริง (KYC – Know Your Customer) อีกทั้งการเข้าใช้งานระบบจะต้องมีการรักษาความปลอดภัยอย่างเพียงพอ โดยสามารถจัดหาวิธีการหรือเทคโนโลยีใด ๆ เช่น รหัสผู้ใช้งานและรหัสผ่าน การใช้ OTP (One-time Password) หรือการควบคุม Session เป็นต้น
3. ในการส่งคำสั่งซื้อขายผ่านระบบซื้อขาย จะต้องมีการยืนยันว่าเป็นลูกค้ารายนั้นจริงก่อนการส่งคำสั่ง โดยสามารถจัดหาวิธีการ หรือเทคโนโลยีใด ๆ ในการระบุความเป็นตัวตนได้ชัดเจน เช่น PIN ID เป็นต้น ซึ่งควรพิจารณาความยาวของ PIN ID ให้สอดคล้องกับการให้บริการและมีความปลอดภัยเพียงพอ
4. มีข้อความแจ้งเตือนผู้ใช้งานระบบเกี่ยวกับความเสี่ยงที่เกิดจากการกระทำของผู้ใช้งานระบบอย่างชัดเจนและครบถ้วน (Agreement / Disclaimer) รวมถึงการเก็บข้อมูลที่แสดงการยอมรับความเสี่ยงเหล่านั้นอย่างเหมาะสม
5. สมาชิกต้องมีมาตรการดำเนินการควบคุมการใช้โปรแกรมหรือแอพพลิเคชั่นที่เหมาะสม เพื่อให้การซื้อขายเป็นธรรมและไม่ก่อให้เกิดความเสียหายต่อการซื้อขายโดยรวม
6. มีขั้นตอนการส่งมอบรหัสผู้ใช้งานและรหัสผ่านที่มีความปลอดภัยเพียงพอ และมีการให้ความรู้กับผู้ใช้งานในการเก็บรักษารหัสผ่านของตนไว้เป็นความลับ เพื่อให้มีความตระหนักถึงประเด็นของความปลอดภัย

[1] ประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ที่ สธ. 37/2559 เรื่อง ข้อกำหนดในรายละเอียดเกี่ยวกับการจัดให้มีระบบเทคโนโลยีสารสนเทศ และประกาศแนวปฏิบัติ ที่ นป. 3/2559 เรื่อง แนวปฏิบัติในการจัดให้มีระบบเทคโนโลยีสารสนเทศ

เช่น การแนะนำให้ใช้รหัสผ่านที่ซับซ้อนหรือเดาได้ยาก การแนะนำไม่ให้เปิดเผยรหัสผ่านใด ๆ ให้บุคคลอื่นทราบ การแนะนำให้มีการ Logout ออกจากระบบทุกครั้งที่ไม่ได้ใช้งานทั้งแบบชั่วคราวและเมื่อเลิกใช้งาน การแนะนำความเสี่ยงในการบันทึกรหัสผ่านไว้บนเครื่องหรือระบบ เป็นต้น

ทั้งนี้ สมาชิกจะต้องสามารถส่งรายละเอียดมาตรฐานความปลอดภัยของสมาชิกให้แก่ตลาดหลักทรัพย์ทันทีเมื่อตลาดหลักทรัพย์ร้องขอ
