แบบประเมินการทำงานและการรักษาความปลอดภัยของระบบ

แบบประเมินการทำงานและการรักษาความปลอดภัยของระบบ

1. สมาชิกมีมาตรฐานความปลอดภัยสำหรับระบบที่ต่อเชื่อมกับระบบการซื้อขายตามประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ว่าด้วย การจัดให้มีระบบเทคโนโลยีสารสนเทศ (ประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ที่ สธ. 37/2559 เรื่อง ข้อกำหนดในรายละเอียดเกี่ยวกับการจัดให้มีระบบเทคโนโลยีสารสนเทศ และประกาศแนวปฏิบัติ ที่ นป. 3/2559 เรื่อง แนวปฏิบัติในการจัดให้มีระบบเทคโนโลยีสารสนเทศ)	มี	ไม่มี
2. สมาชิกมีการจำกัดการเข้าถึงข้อมูลและฟังก์ชันต่างๆ ของแอพพลิเคชั่นเฉพาะผู้ที่ได้รับอนุญาตเท่านั้น และการเข้าถึงจะต้องแยกตามประเภทของผู้ใช้งาน (user role) รวมทั้งมีระบบการบันทึกข้อมูลการทำงานของแอพพลิเคชั่น (audit trail log) อย่างเหมาะสม	มี	ไม่มี
3. ในการเข้าใช้งานระบบผู้ใช้งานระบบซื้อขายจะต้องผ่านการตรวจสอบและยืนยันความเป็นตัวตนว่าเป็นบุคคลที่ได้รับอนุญาตจริง (KYC – Know Your Customer) อีกทั้งการเข้าใช้งานระบบจะต้องมีการรักษาความปลอดภัยอย่างเพียงพอ โดยสามารถจัดหาวิธีการหรือเทคโนโลยีใดๆ เช่น รหัสผู้ใช้งานและรหัสผ่าน, การใช้ OTP (One-time password) หรือการควบคุม Session เป็นต้น	มี	ไม่มี
4. ในการส่งคำสั่งซื้อขายผ่านระบบซื้อขาย จะต้องมีการยืนยันว่าเป็นลูกค้ารายนั้นจริงก่อนการส่งคำสั่ง โดยสามารถจัดหาวิธีการ หรือเทคโนโลยีใดๆ ในการระบุความเป็นตัวตนได้ชัดเจน เช่น PIN ID เป็นต้น ซึ่งควรพิจารณาความยาวของ PIN ID ให้สอดคล้องกับการให้บริการและมีความปลอดภัยเพียงพอ	มี	ไม่มี
5. ต้องมีข้อความแจ้งเตือนผู้ใช้งานระบบเกี่ยวกับความเสี่ยงที่เกิดจากการกระทำของผู้ใช้งานระบบอย่างชัดเจนและครบถ้วน (Agreement/ Disclaimer) รวมถึงการเก็บข้อมูลที่แสดงการยอมรับความเสี่ยงเหล่านั้นอย่างเหมาะสม	มี	ไม่มี
6. สมาชิกต้องมีมาตรการดำเนินการควบคุมการใช้โปรแกรมหรือแอพพลิเคชั่นที่เหมาะสม เพื่อให้การซื้อขายเป็นธรรมและไม่ก่อให้เกิดความเสียหายต่อการซื้อขายโดยรวม	มี	ไม่มี
7. ต้องมีขั้นตอนการส่งมอบรหัสผู้ใช้งานและรหัสผ่านที่มีความปลอดภัยเพียงพอ และมีการให้ความรู้กับผู้ใช้งานในการเก็บรักษารหัสผ่านของตนไว้เป็นความลับ เพื่อให้มีความตระหนักถึงประเด็นของความปลอดภัย เช่น การแนะนำให้ใช้รหัสผ่านที่ซับซ้อนหรือเดาได้ยาก การแนะนำไม่ให้เปิดเผยรหัสผ่านใดๆ ให้บุคคลอื่นทราบ การแนะนำให้มีการ Logout ออกจากระบบทุกครั้งที่ไม่ได้ใช้งานทั้งแบบชั่วคราวและเมื่อเลิกใช้งาน การแนะนำความเสี่ยงในการบันทึกรหัสผ่านไว้บนเครื่องหรือระบบเป็นต้น	มี	ไม่มี

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