มาตรฐานความปลอดภัยสำหรับ ระบบที่ต่อเชื่อมกับระบบการซื้อขายของตลาดสัญญาซื้อขายล่วงหน้า

ตลาดสัญญาซื้อขายล่วงหน้าได้ตระหนักถึงความสำคัญของระบบที่ต่อเชื่อมกับระบบการซื้อขายของตลาดสัญญาซื้อขายล่วงหน้า ซึ่งอาจส่งผลต่อความปลอดภัยต่อระบบการซื้อขายโดยรวม ตลาดสัญญาซื้อขายล่วงหน้าจึงได้จัดทำมาตรฐานในเรื่องความปลอดภัยเพื่อเป็นแนวทางให้สมาชิกนำไปใช้เป็นข้อปฏิบัติในการดำเนินการ และสามารถส่งรายละเอียดให้ตลาดสัญญาซื้อขายล่วงหน้าตามที่ร้องขอ

1. ความปลอดภัยทางกายภาพ และสิ่งแวดล้อม (Physical and Environment Security)

1.1 ห้องคอมพิวเตอร์ส่วนที่ต้องมีการรักษาความปลอดภัย (Secure Areas)

เพื่อป้องกันการเข้าถึงห้องคอมพิวเตอร์ในส่วนที่ต้องมีการรักษาความปลอดภัยโดยไม่ได้รับอนุญาต รวมถึงการป้องกันการก่อให้เกิดความเสียหาย ก่อกวนหรือแทรกแซงต่อทรัพย์สินขององค์กร

- มีการแบ่งแยกบริเวณที่เป็นสัดส่วนโดยเฉพาะ
- มีการควบคุมการเข้า-ออกได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น
- มีการบันทึกข้อมูลบุคคลเข้า-ออก และเหตุผลในการเข้าใช้งานทุกครั้ง
- มีการติดตั้งระบบการรักษาความปลอดภัยที่ได้มาตรฐาน เช่น การเข้า/ออกห้องคอมพิวเตอร์ต้องมีการใช้บัตรผ่าน (Access Control) หรือมีเจ้าหน้าที่ควบคุมการเข้า-ออกสถานที่ตลอด 24 ชั่วโมง เป็นต้น
- มีการวางแนวทางการบำรุงรักษา การป้องกันภัยและการเตือนภัยต่อภัยคุกคามต่างๆ เช่น เหตุขัดข้อง ไฟไหม้ น้ำท่วม แผ่นดินไหว การระเบิด ความไม่สงบของบ้านเมือง หรือหายนะอื่นๆ ทั้งที่เกิดจากมนุษย์และธรรมชาติ เป็นต้น

1.2 ความปลอดภัยของอุปกรณ์ (Equipment Security)

อุปกรณ์คอมพิวเตอร์และเครือข่ายที่ใช้งานจะต้องติดตั้งในบริเวณที่มีการรักษาความปลอดภัยอย่างเพียงพอ รวมทั้งมีการป้องกันการสูญหาย การเกิดความเสียหาย การถูกขโมย หรือการถูกเปิดเผยโดยไม่ได้รับอนุญาต และการกระทำการใดๆ ที่ทำให้การดำเนินงานต่างๆ เกิดการติดขัดหรือหยุดชะงัก

- มีกลไกการป้องกันความล้มเหลวของระบบ และอุปกรณ์สนับสนุนต่างๆ เช่น ระบบกระแสไฟฟ้าสำรอง ระบบควบคุมเพลิง ระบบควบคุมอุณหภูมิ ระบบสายสื่อสารสำรอง เป็นต้น
- มีการกำหนดให้มีการบำรุงรักษาอุปกรณ์อย่างสม่ำเสมอ เพื่อให้อุปกรณ์ทำงานได้อย่างต่อเนื่องและอยู่ในสภาพที่มีความสมบูรณ์ต่อการใช้งาน

2. การบริหารจัดการด้านการดำเนินงาน (Operations Management)

เพื่อกำหนดนโยบาย หน้าที่ความรับผิดชอบ การรักษาความลับ และขั้นตอนการปฏิบัติงานให้เป็นไปอย่างถูกต้องและมีความปลอดภัยเพียงพอ รวมทั้งจะต้องมีการตรวจยืนยันตัวผู้ใช้งานว่าเป็นบุคคลที่ได้รับอนุญาตจริง (User Authentication) และสามารถเข้าถึงเฉพาะส่วนที่ได้รับอนุญาตเท่านั้น (User Authorization) นอกจากนี้จะต้องมีการบันทึกและตรวจสอบ Log การดำเนินงานย้อนหลังได้ในระยะเวลาที่เหมาะสม โดยมีข้อมูลที่สามารถระบุรายละเอียดแหล่งที่มา ปลายทาง วันที่เวลา ผู้ใช้งาน และข้อมูลการดำเนินการหรือข้อมูลอื่นใดที่มีนัยสำคัญ ทั้งนี้หากเป็นระบบซื้อขายหรือระบบชำระราคา จะต้องมีรายละเอียดการซื้อขายหรือการชำระราคาที่ชัดเจนตรวจสอบได้

2.1 ความปลอดภัยของระบบเครือข่าย (Network Security)

- ต้องระบุและกำหนดประเภทบริการ (Service) รวมถึงเวลาใช้งานของอุปกรณ์รักษาความปลอดภัย และอุปกรณ์เครือข่ายทุกชนิดที่ต่อเชื่อมกันตามการใช้งานจริงเท่านั้น
- ต้องมีมาตรการป้องกันการเข้าถึงเครือข่ายระบบให้มีความปลอดภัย เช่น Firewall, Anti-virus, Anti-Spyware, ระบบป้องกันการดักจับ หรือขโมยข้อมูล, การบริหารจัดการเรื่อง Patch เป็นต้น
- ต้องมีการเข้ารหัสข้อมูล (Encryption) บนเส้นทางการต่อเชื่อมระบบอย่างเหมาะสม

2.2 ความปลอดภัยของระบบ (System Security)

- ต้องมีขั้นตอนการปฏิบัติที่มีความปลอดภัยสำหรับการเข้าถึงหรือการเข้าใช้งานระบบ
- ทุกระบบจะต้องเปิด Service เท่าที่จำเป็นต่อการใช้งานเท่านั้น
- ต้องมีมาตรการป้องกันระบบให้มีความปลอดภัย เช่น Anti-virus, Anti-Spyware, ระบบป้องกันการดักจับ หรือขโมยข้อมูล, การบริหารจัดการเรื่อง Patch เป็นต้น
- ต้องมีการบันทึกการใช้งาน และ Event Log ของระบบ เพื่อตรวจสอบการดำเนินงานย้อนหลังได้ และเก็บไว้ในระยะเวลาที่เหมาะสม เช่น การบันทึกการเข้าออกของผู้ใช้ระบบ, การใช้งานของ Server และ Database เป็นต้น

2.3 ความปลอดภัยของแอพพลิเคชั่น (Application Security)

- ต้องมีการจำกัดการเข้าถึงข้อมูลและฟังก์ชันต่างๆ ของแอพพลิเคชั่นเฉพาะผู้ที่ได้รับอนุญาตเท่านั้น และการเข้าถึงจะต้องแยกตามประเภทของผู้ใช้งาน
- ต้องมีวิธีการหรือเทคโนโลยีใดๆ ที่สามารถตรวจสอบและยืนยันความเป็นตัวตนว่าเป็นบุคคลที่ได้รับอนุญาตจริง ไม่ใช่เป็นผู้อื่นปลอมแปลง เช่น การระบุรหัสผู้ใช้งานและรหัสผ่าน เป็นต้น
- ต้องมีวิธีการหรือเทคโนโลยีใดๆ ในการระบุความเป็นตัวตนของผู้ส่งคำสั่งได้อย่างชัดเจนและเหมาะสม เช่น PIN ID เป็นต้น
- มีข้อความแจ้งเตือนผู้ใช้งานระบบเกี่ยวกับความเสี่ยงที่เกิดจากการกระทำของผู้ใช้งานระบบอย่างชัดเจนและครบถ้วน

3. การบริหารจัดการรหัสผู้ใช้งานและรหัสผ่าน (User ID and Password Management)

รหัสผู้ใช้งาน (User ID) และรหัสผ่าน (Password) หมายรวมถึงเทคโนโลยีอื่นใดที่ใช้ในการระบุความเป็นตัวตน เช่น PIN ID เป็นต้น ซึ่งถือว่ามีความสำคัญในการควบคุมการเข้าถึงระบบ เครือข่าย หรือแอพพลิเคชั่นต่างๆ ดังนั้นจึงต้องจัดทำระบบหรือมีระบบบริหารจัดการที่มีความปลอดภัยเพียงพอ ดังนี้

- สามารถใช้ User Login เพียง 1 ชื่อ เพื่อ Login ในเวลาใดเวลาหนึ่งเท่านั้น (User Login / Session) หรือตามที่ตลาดสัญญาซื้อขายล่วงหน้าเห็นสมควร
- รหัสผ่านต้องมีความยาวและการผสมอักษรที่มีความปลอดภัยเพียงพอ (หากมีการใช้งาน PIN ID จะต้องมีความยาวที่ปลอดภัยเพียงพอ) รวมทั้งไม่มีการแสดงผลรหัสผ่านในลักษณะที่สามารถอ่านได้ (Clear Text)
- ต้องกำหนดนโยบายการเปลี่ยนรหัสผ่านในช่วงเวลาที่เหมาะสม
- การเก็บรหัสผ่านที่ระบบหรืออุปกรณ์จะต้องมีการเข้ารหัส (Encryption)
- ต้องมีการ Lock การ Login หรือรหัสผ่านของผู้ใช้นั้นทันที เมื่อมีการใช้รหัสผ่านใดๆ ผิดเกินกว่าจำนวนครั้งที่กำหนดไว้ (Invalid Logon Attempt)
- มีขั้นตอนการส่งมอบรหัสผู้ใช้งานและรหัสผ่านที่มีความปลอดภัยเพียงพอ และมีการให้ความรู้กับผู้ใช้งานในการเก็บรักษารหัสผ่านของตนไว้เป็นความลับ เพื่อให้มีความตระหนักถึงประเด็นของความปลอดภัย เช่น การแนะนำให้ใช้รหัสผ่านที่ซับซ้อนหรือเดาได้ยาก, การแนะนำไม่ให้เปิดเผยรหัสผ่านใดๆ ให้บุคคลอื่นทราบ, การแนะนำให้มีการ Logout ออกจากระบบทุกครั้งที่ไม่ได้ใช้งานทั้งแบบชั่วคราวและเมื่อเลิกใช้งาน, การแนะนำความเสี่ยงในการบันทึกรหัสผ่านไว้บนเครื่องหรือระบบ เป็นต้น

4. ความต่อเนื่องในการดำเนินงาน (Business Continuity Management)

เพื่อป้องกันการติดขัดหรือการหยุดชะงักของการดำเนินงานต่างๆ ทางธุรกิจ อันเป็นผลมาจากความล้มเหลวหรือหายนะที่มีต่อความปลอดภัยและการทำงานของระบบสารสนเทศ อีกทั้งเพื่อให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาอันเหมาะสม

- ต้องมีการประเมินความเสี่ยงเกี่ยวกับเหตุการณ์ พร้อมกำหนดให้มีกระบวนการในการสร้างความต่อเนื่องให้กับการดำเนินงานอย่างเพียงพอ อีกทั้งต้องมีการบริหารจัดการ ปรับปรุงและทดสอบกระบวนการดังกล่าวอย่างสม่ำเสมอ โดยต้องมีการระบุข้อกำหนดที่เกี่ยวข้องกับความปลอดภัยที่จำเป็นไว้ด้วย
- ต้องมีการสำรองและเก็บรักษา (Backup) ข้อมูลและระบบ ตลอดจนโปรแกรมใช้งานในระยะเวลาที่เหมาะสมและสามารถนำข้อมูลกลับมาใช้งานได้อย่างทันทีเมื่อมีเหตุขัดข้อง โดยต้องมีการจัดเก็บไว้นอกที่ทำการหลักขององค์กร