เอกสารรับฟังความคิดเห็น

เลขที่ อกธ. 2/2558

เรื่อง

หลักการในการแก้ไขหลักเกณฑ์เกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และสัญญาซื้อขายล่วงหน้า

จัดทำโดย

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์

เผยแพร่เมื่อวันที่ 23 กุมภาพันธ์ 2558

เพื่อรับฟังความคิดเห็นจากผู้มีส่วนเกี่ยวข้อง

วันสุดท้ายของการให้ความคิดเห็น วันที่ 10 เมษายน 2558

ท่านสามารถ download เอกสารเผยแพร่ฉบับนี้ได้จาก www.sec.or.th

ฝ่ายกำกับและพัฒนาธุรกิจหลักทรัพย์

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์

เลขที่ 333/3 ถนนวิภาวดีรังสิต แขวงจอมพล เขตจตุจักร กรุงเทพฯ 10900

โทรศัพท์ 0-2695-9929 โทรสาร 0-2695-9930

<u>ส่วนที่ 1</u> : บทนำ

ตามที่สำนักงานได้ออกประกาศและแนวทางปฏิบัติเกี่ยวกับการควบคุมการปฏิบัติงานและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัทหลักทรัพย์และตัวแทนสัญญาซื้อขายล่วงหน้า[1] ("ผู้ประกอบธุรกิจ") เพื่อให้ผู้ประกอบธุรกิจกำหนดนโยบายและกระบวนการควบคุมดูแลด้านความปลอดภัยของระบบสารสนเทศให้ครอบคลุมในเรื่องการแบ่งแยกอำนาจหน้าที่ (segregation of duties) การควบคุมการเข้าออกศูนย์คอมพิวเตอร์และการป้องกันความเสียหาย (physical security) การรักษาความปลอดภัยข้อมูลระบบคอมพิวเตอร์ และระบบเครือข่าย (information and network security) การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ (change management) การสำรองข้อมูลและระบบคอมพิวเตอร์และการเตรียมความพร้อมกรณีฉุกเฉิน (backup and IT continuity plan) การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์ (computer operation) และการควบคุมการใช้บริการงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT outsourcing) นั้น

เนื่องจากหลักเกณฑ์ดังกล่าวใช้บังคับมาได้เป็นระยะเวลาหนึ่งแล้ว ขณะที่การประกอบธุรกิจของผู้ประกอบธุรกิจมีแนวโน้มพึ่งพาระบบเทคโนโลยีสารสนเทศที่ทันสมัยและมีความซับซ้อนมากขึ้นเพื่อเพิ่มประสิทธิภาพการให้บริการและความสามารถในการแข่งขัน ซึ่งทำให้ผู้ประกอบธุรกิจมีความเสี่ยงต่อภัยคุกคาม (threats) ในรูปแบบใหม่ ๆ ขณะที่หลักเกณฑ์ในปัจจุบันมีข้อกำหนดที่ยังไม่ครอบคลุมบางประเด็นซึ่งเป็นผลจากสภาพแวดล้อมที่เปลี่ยนแปลงไป รวมทั้งไม่รองรับเทคโนโลยีสารสนเทศใหม่ ๆ ที่มีความซับซ้อนมากขึ้น สำนักงานพิจารณาแล้วจึงเห็นควรทบทวนหลักเกณฑ์ดังกล่าวให้มีความเหมาะสมมากยิ่งขึ้น

สำนักงานจึงได้จัดทำเอกสารฉบับนี้ขึ้นเพื่อขอรับฟังความคิดเห็นจากผู้ประกอบธุรกิจและบุคคลทั่วไปเกี่ยวกับหลักการแก้ไขหลักเกณฑ์เกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ โดยการรับฟังความคิดเห็นนี้จะมีไปจนถึงวันที่ 10 เมษายน 2558 ผู้ที่ประสงค์จะแสดงความคิดเห็นสามารถส่งความคิดเห็นและข้อเสนอแนะต่อสำนักงานได้ทั้งในรูปแบบเอกสารหรือ e-mail ตามรายละเอียดที่ระบุด้านล่างนี้ ทั้งนี้ สำนักงานขอเสนอชื่อเจ้าหน้าที่สำหรับการสอบถามคือ นายอธิภัทร พูลถนอมสุข ฝ่ายกำกับและพัฒนาธุรกิจหลักทรัพย์ โทรศัพท์ 0-2263-6039 e-mail address: insec@sec.or.th

ที่อยู่สำหรับจัดส่งเอกสาร

ทางไปรษณีย์ : ฝ่ายกำกับและพัฒนาธุรกิจหลักทรัพย์ สำนักงานคณะกรรมการ ก.ล.ต.
ชั้น 25 เลขที่ 333/3 ถนนวิภาวดีรังสิต แขวงจอมพล เขตจตุจักร กรุงเทพฯ 10900

ทางโทรสาร : 0-2263-6299

E-mail address : insec@sec.or.th

---

[1] ประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ที่ สธ/น. 32/2552 เรื่อง การควบคุมการปฏิบัติงานและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัทหลักทรัพย์ ลงวันที่ 3 สิงหาคม พ.ศ. 2552 ประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ที่ อธ./น. 5/2547 เรื่อง แนวทางปฏิบัติในการควบคุมการปฏิบัติงานและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัทหลักทรัพย์ ลงวันที่ 20 กรกฎาคม พ.ศ. 2547 และประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ที่ สธ. 8/2548 เรื่อง การควบคุมการปฏิบัติงานและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของผู้ได้รับใบอนุญาตเป็นตัวแทนซื้อขายสัญญาซื้อขายล่วงหน้า ลงวันที่ 1 เมษายน พ.ศ. 2548

<u>ส่วนที่ 2</u> : หลักการในการแก้ไขหลักเกณฑ์

2.1 วัตถุประสงค์

เพื่อให้ผู้ประกอบธุรกิจสามารถให้บริการลูกค้าได้อย่างต่อเนื่องโดยมีมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศอย่างเพียงพอ สามารถปิดความเสี่ยงด้านเทคโนโลยีสารสนเทศได้อย่างมีประสิทธิภาพ

2.2 ขอบเขตการใช้บังคับ

ผู้ประกอบธุรกิจที่ได้รับใบอนุญาตประกอบธุรกิจหลักทรัพย์และธุรกิจสัญญาซื้อขายล่วงหน้าประเภทดังต่อไปนี้

(1) การเป็นนายหน้าซื้อขายหลักทรัพย์ การค้าหลักทรัพย์ หรือการจัดจำหน่ายหลักทรัพย์

(2) การจัดการกองทุนรวมหรือกองทุนส่วนบุคคล

(3) กิจการยืมและให้ยืมหลักทรัพย์

(4) การให้สินเชื่อเพื่อธุรกิจหลักทรัพย์

(5) การเป็นตัวแทนสัญญาซื้อขายล่วงหน้า

(6) การเป็นผู้ค้าสัญญาซื้อขายล่วงหน้า

(7) การเป็นผู้จัดการเงินทุนสัญญาซื้อขายล่วงหน้า

ทั้งนี้ ไม่รวมถึง

(1) การเป็นที่ปรึกษาการลงทุนและ/หรือการเป็นที่ปรึกษาสัญญาซื้อขายล่วงหน้า เว้นแต่เป็นผู้ประกอบธุรกิจที่ประกอบธุรกิจดังกล่าวโดยทราบความเคลื่อนไหวของพอร์ตการลงทุนของลูกค้า

(2) การจัดการเงินร่วมลงทุน

(3) การเป็นนายหน้าระหว่างผู้ค้าหลักทรัพย์

(4) ผู้ประกอบธุรกิจที่อยู่ภายใต้การกำกับดูแลของหน่วยงานกำกับอื่น ๆ เช่น ธนาคารพาณิชย์ และบริษัทประกัน เว้นแต่กรณีที่หลักเกณฑ์กำกับดูแลของหน่วยงานดังกล่าวมีความครอบคลุมน้อยกว่าของสำนักงาน

2.3 หลักการและเหตุผลความจำเป็นในการแก้ไขหลักเกณฑ์

เพื่อปรับปรุงเนื้อหาของหลักเกณฑ์ให้มีความเป็นปัจจุบันสอดคล้องกับมาตรฐานสากล เพื่อให้ผู้ประกอบธุรกิจมีมาตรการด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศอย่างเพียงพอในการป้องกันและบริหารความเสี่ยงด้านระบบสารสนเทศที่อาจส่งผลกระทบต่อการรักษาความลับของข้อมูล (confidentiality) ความครบถ้วนถูกต้องน่าเชื่อถือของข้อมูล (integrity) และสภาพพร้อมใช้งานของข้อมูลและระบบสารสนเทศ (availability) ได้อย่างมีประสิทธิภาพ

2.4 หลักเกณฑ์ที่ปรับปรุง

เพื่อให้ผู้ประกอบธุรกิจมีมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศได้อย่างเพียงพอและมีประสิทธิภาพ สำนักงานจึงเห็นควรปรับปรุงหลักเกณฑ์ดังต่อไปนี้ (ส่วนที่ปรับปรุงเพิ่มเติม แสดงด้วยตัวอักษรหนา)

2.4.1 ปรับปรุงโครงสร้างของประกาศและแนวทางปฏิบัติ โดยแบ่งเป็น 14 หัวข้อ (domain) เพื่อขยายขอบเขตให้เป็นไปตามมาตรฐานสากลโดยครอบคลุมการป้องกันความเสี่ยงด้านสารสนเทศในด้านต่าง ๆ รวมทั้งเพิ่มเติมข้อกำหนดเพื่อให้รองรับเทคโนโลยีใหม่ ๆ ดังนี้

บทนิยาม

"ทรัพย์สินสารสนเทศที่มีความสำคัญ" หมายถึง ทรัพย์สินสารสนเทศที่เกี่ยวข้อง หรือจำเป็นต้องใช้ประกอบกับงานที่มีความสำคัญ

"ระบบสารสนเทศที่มีความสำคัญ" หมายถึง ระบบสารสนเทศที่รองรับการปฏิบัติงานที่สำคัญ

"งานที่สำคัญ" หมายถึง งานที่เกี่ยวกับการให้บริการ การทำธุรกรรม หรืองานอื่น ๆ ของผู้ประกอบธุรกิจ ซึ่งหากมีการหยุดชะงักอาจส่งผลกระทบต่อลูกค้า การดำเนินงาน ธุรกิจ ชื่อเสียง ฐานะ และผลการดำเนินงานของผู้ประกอบธุรกิจอย่างมีนัยสำคัญ

"ผู้ให้บริการภายนอก" หมายถึง บุคคลจากภายนอกองค์กรซึ่งผู้ประกอบธุรกิจว่าจ้างเพื่อใช้บริการที่เกี่ยวข้องกับระบบสารสนเทศ

(1) นโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Policy)

เพื่อให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องได้ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ และได้รับทราบถึงหน้าที่ความรับผิดชอบและแนวทางปฏิบัติในการควบคุมความเสี่ยงต่าง ๆ ให้ผู้ประกอบธุรกิจดำเนินการดังต่อไปนี้

(ก) จัดให้มีนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศอย่างเป็นลายลักษณ์อักษร โดยคำนึงถึงลักษณะ ขนาด และความซับซ้อนของการประกอบธุรกิจ รวมทั้งกฎเกณฑ์ต่าง ๆ ที่เกี่ยวข้อง

(ข) นโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศต้องได้รับการพิจารณาอนุมัติจากคณะกรรมการบริษัทหรือคณะกรรมการอื่นที่คณะกรรมการบริษัทมอบหมาย

(ค) จัดให้มีการเผยแพร่นโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศต่อบุคลากรที่เกี่ยวข้องโดยจัดให้เข้าถึงได้ง่าย เพื่อให้บุคลากรที่เกี่ยวข้องรับทราบและถือปฏิบัติ

(ง) จัดให้มีการทบทวนหรือปรับปรุงนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงของสภาพแวดล้อมต่าง ๆ ที่มีนัยสำคัญ

(2) การจัดโครงสร้างความมั่นคงปลอดภัยของระบบสารสนเทศ (Organization of Information Security)

(2.1) เพื่อกำหนดมาตรการควบคุมการปฏิบัติหน้าที่ด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศสำหรับส่วนงานต่าง ๆ ภายในองค์กร ให้ผู้ประกอบธุรกิจดำเนินการจัดการโครงสร้างภายในองค์กรดังต่อไปนี้

(ก) กำหนดรายละเอียดหน้าที่ความรับผิดชอบด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ พร้อมทั้งจัดสรรหน้าที่ความรับผิดชอบและกำหนดแนวทางในการปฏิบัติหน้าที่ดังกล่าวให้กับพนักงานให้ครบถ้วน

(ข) กำหนดให้มีการแบ่งแยกหน้าที่ในการปฏิบัติงานด้านต่าง ๆ ที่เกี่ยวกับความมั่นคงปลอดภัยของระบบสารสนเทศออกจากกันอย่างชัดเจน เพื่อให้มีการสอบทานระหว่างกัน และป้องกันความเสี่ยงในการปฏิบัติงานที่อาจเกิดขึ้น

(ค) จัดให้มีรายชื่อและช่องทางสำหรับติดต่อ (contact person) ของหน่วยงานกำกับดูแลและหน่วยงานผู้ให้บริการที่สนับสนุนการทำงานระบบสารสนเทศของบริษัท พร้อมทั้งปรับปรุงรายชื่อและช่องทางสำหรับติดต่อดังกล่าวให้เป็นปัจจุบัน

(2.2) ผู้ประกอบธุรกิจต้องมีมาตรการรักษาความมั่นคงปลอดภัยที่รัดกุมเพียงพอสำหรับข้อมูลสารสนเทศที่เป็นความลับหรือมีความสำคัญ ในกรณีที่มีการปฏิบัติงานขององค์กรจากระยะไกล หรือมีการใช้งานอุปกรณ์คอมพิวเตอร์ประเภทพกพา

(2.3) ในกรณีที่มีการใช้บริการ cloud computing ผู้ประกอบธุรกิจต้องจัดให้มีข้อกำหนดเกี่ยวกับการใช้งาน เพื่อควบคุมการให้บริการและการเข้าถึงข้อมูลสารสนเทศของผู้ให้บริการอย่างเหมาะสม โดยครอบคลุมในเรื่องดังต่อไปนี้

(ก) นโยบายการใช้งาน cloud computing

(ข) ข้อตกลงระหว่างผู้ให้บริการและผู้ใช้บริการ

(ค) ข้อกำหนดในกรณีที่ผู้ให้บริการมีการใช้บริการ cloud computing ต่อจากผู้ให้บริการรายอื่น

(ง) การติดตาม ประเมิน และทบทวนการให้บริการของผู้ให้บริการ

(จ) ขั้นตอนการโอนย้ายข้อมูลไปยังผู้ให้บริการรายใหม่ในกรณีที่มีการเปลี่ยนแปลงผู้ให้บริการ

(3) การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร (Human Resource Security)

เพื่อให้พนักงานและผู้ให้บริการภายนอกที่ปฏิบัติงานภายในองค์กรมีความตระหนักรู้และปฏิบัติงานโดยคำนึงถึงการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ให้ผู้ประกอบธุรกิจดำเนินการดังต่อไปนี้

(ก) จัดให้มีการสร้างความตระหนักรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศแก่พนักงานและผู้ให้บริการภายนอกที่ปฏิบัติงานภายในองค์กร

(ข) สื่อสารให้พนักงานและผู้ให้บริการภายนอกที่ปฏิบัติงานภายในองค์กรระมัดระวังและละเว้นการใช้งานระบบสารสนเทศในลักษณะที่อาจก่อให้เกิดความเสียหายกับผู้ประกอบธุรกิจ ตลาดทุนโดยรวม หรือความมั่นคงของประเทศ รวมทั้งให้ตระหนักรู้ และสังเกตถึงความผิดปกติใด ๆ ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ พร้อมทั้งรายงานทันทีเมื่อพบความผิดปกติดังกล่าวทุกครั้ง

(ค) จัดให้มีมาตรการดำเนินการทางวินัยต่อผู้ฝ่าฝืนนโยบายและหลักปฏิบัติเกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

(4) การบริหารจัดการทรัพย์สินสารสนเทศ (Asset Management)

(4.1) เพื่อให้ทรัพย์สินสารสนเทศที่มีความสำคัญได้รับการป้องกันอย่างเหมาะสม ผู้ประกอบธุรกิจต้องระบุและกำหนดหน้าที่ความรับผิดชอบในการรักษาความมั่นคงปลอดภัยของทรัพย์สินสารสนเทศโดยดำเนินการดังต่อไปนี้

(ก) ระบุประเภททรัพย์สินสารสนเทศ พร้อมทั้งบันทึกและทบทวนรายการทรัพย์สินดังกล่าวอย่างสม่ำเสมอ

(ข) กำหนดผู้รับผิดชอบทรัพย์สินสารสนเทศแต่ละประเภทตลอดอายุการใช้งานของทรัพย์สิน

(ค) จัดให้มีข้อกำหนดในการใช้งานทรัพย์สินสารสนเทศอย่างเหมาะสม

(ง) ควบคุมให้พนักงานและผู้ให้บริการภายนอก คืนทรัพย์สินสารสนเทศในกรณีที่มีการลาออก เลิกสัญญาว่าจ้าง หรือเปลี่ยนแปลงหน้าที่ปฏิบัติงาน

(4.2) ผู้ประกอบธุรกิจต้องจำแนกประเภททรัพย์สินสารสนเทศที่มีความสำคัญ เพื่อให้ทรัพย์สินสารสนเทศดังกล่าวได้รับการปกป้องในระดับที่เหมาะสมตามระดับความสำคัญ

(4.3) เพื่อป้องกันการเปิดเผย เปลี่ยนแปลงแก้ไข หรือสร้างความเสียหายต่อข้อมูลสารสนเทศที่ถูกจัดเก็บในสื่อบันทึกข้อมูล ให้ผู้ประกอบธุรกิจดำเนินการดังต่อไปนี้

(ก) จัดให้มีกระบวนการทำลายข้อมูลและสื่อบันทึกข้อมูลในกรณีที่ไม่มีความจำเป็นต้องใช้ข้อมูลหรือสื่อบันทึกข้อมูลดังกล่าว

(ข) กรณีที่จัดเก็บข้อมูลเป็นระยะเวลานาน ต้องคำนึงถึงความเสี่ยงที่สื่อบันทึกข้อมูลอาจเสื่อมสภาพ รวมทั้งวิธีการนำข้อมูลกลับมาใช้งานใหม่

(ค) จัดเก็บสื่อบันทึกข้อมูลในพื้นที่ที่มีความมั่นคงปลอดภัย และเป็นไปตามคำแนะนำของผู้ผลิต

(ง) มีกระบวนการดูแลรักษาความปลอดภัย กรณีมีการเคลื่อนย้ายสื่อบันทึกข้อมูลออกจากพื้นที่ทำการ

(5) การควบคุมการเข้าถึง (Access Control)

(5.1) ผู้ประกอบธุรกิจต้องจัดให้มีนโยบายควบคุมการเข้าถึงข้อมูลและ information processing facilities ต่าง ๆ เช่น อุปกรณ์หรือโปรแกรมประมวลผลข้อมูล ระบบเครือข่ายคอมพิวเตอร์ ขั้นตอนหรือสถานที่ประมวลผลข้อมูลตามที่ผู้ประกอบธุรกิจกำหนด เป็นต้น โดยจัดทำเป็นลายลักษณ์อักษรและทบทวนนโยบายดังกล่าวอย่างสม่ำเสมอ

(5.2) ผู้ประกอบธุรกิจต้องจัดให้มีการบริหารจัดการบัญชีผู้ใช้งานเพื่อจำกัดการเข้าถึงข้อมูลสารสนเทศเฉพาะบุคคลที่ได้รับสิทธิการเข้าถึง โดยให้ดำเนินการดังต่อไปนี้

(ก) จัดให้มีการลงทะเบียนบัญชีผู้ใช้งานระบบสารสนเทศอย่างเป็นทางการ

(ข) จัดสรรและควบคุมสิทธิการเข้าถึงระดับสูงอย่างเคร่งครัด

(ค) มีขั้นตอนการบริหารจัดการเรื่องการกำหนดรหัสผ่านอย่างเหมาะสม

(ง) มีการติดตามทบทวนระดับสิทธิการเข้าถึงอย่างสม่ำเสมอ

(5.3) ผู้ประกอบธุรกิจต้องจัดให้มีข้อบังคับให้ผู้ใช้งานปฏิบัติตามขั้นตอนการใช้งานและดูแลรับผิดชอบรหัสผ่านอย่างมั่นคงปลอดภัยตามนโยบายการควบคุมการเข้าถึงที่ได้กำหนดไว้

(5.4) ผู้ประกอบธุรกิจต้องป้องกันมิให้มีการเข้าถึงระบบสารสนเทศและแอพพลิเคชั่นโดยไม่ได้รับอนุญาต โดยให้ดำเนินการดังต่อไปนี้

(ก) ควบคุมการเข้าถึงข้อมูลสารสนเทศและฟังก์ชั่นต่าง ๆ ในแอพพลิเคชั่นของผู้ใช้งานและผู้ดูแลระบบสารสนเทศ โดยให้สอดคล้องกับสิทธิที่ได้รับและนโยบายควบคุมการเข้าถึงที่ได้กำหนดไว้

(ข) ควบคุมการเข้าใช้งานระบบสารสนเทศและแอพพลิเคชั่นด้วยวิธีการแบบปลอดภัย

(ค) จัดให้มีระบบการบริหารจัดการรหัสผ่านที่มีความมั่นคงปลอดภัย

(ง) จำกัดการใช้งานโปรแกรมอรรถประโยชน์ต่าง ๆ และจำกัดการเข้าถึงชุดคำสั่งควบคุมการทำงานของโปรแกรมอย่างเข้มงวด

(6) การควบคุมการเข้ารหัสข้อมูล (Cryptographic Controls)

ผู้ประกอบธุรกิจต้องจัดให้มีนโยบายการใช้งานระบบการเข้ารหัสข้อมูลและการบริหารกุญแจเข้ารหัสข้อมูล เพื่อให้การใช้งานระบบการเข้ารหัสข้อมูลมีความเหมาะสมและมีประสิทธิภาพ สามารถป้องกันการเข้าถึงหรือเปลี่ยนแปลงแก้ไขข้อมูลที่เป็นความลับหรือมีความสำคัญ

(7) การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม (Physical and Environmental Security)

(7.1) ผู้ประกอบธุรกิจต้องกำหนดพื้นที่หวงห้าม เช่น ศูนย์คอมพิวเตอร์ ศูนย์สำรอง และพื้นที่ที่ตั้งอุปกรณ์ระบบเครือข่ายคอมพิวเตอร์ พร้อมทั้งป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าถึงพื้นที่ดังกล่าว ซึ่งอาจก่อให้เกิดความเสียหายต่ออุปกรณ์สารสนเทศหรือมีผลกระทบต่อข้อมูลที่เป็นความลับหรือมีความสำคัญ

(7.2) ผู้ประกอบธุรกิจต้องจัดให้มีการป้องกันอุปกรณ์สารสนเทศมิให้เกิดความเสียหาย และสามารถทำงานได้อย่างต่อเนื่อง

(8) การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ (Operations Security)

(8.1) ผู้ประกอบธุรกิจต้องกำหนดหน้าที่ความรับผิดชอบ และขั้นตอนการปฏิบัติงานสารสนเทศ ทั้งนี้ เพื่อให้มั่นใจว่าขั้นตอนและกระบวนการปฏิบัติงานด้านระบบสารสนเทศเป็นไปอย่างถูกต้องและมั่นคงปลอดภัย

(8.2) ผู้ประกอบธุรกิจต้องจัดให้มีมาตรการป้องกันและตรวจสอบโปรแกรมไม่ประสงค์ดี รวมทั้งแก้ไขเพื่อให้ระบบกลับมาใช้งานได้ตามปกติ

(8.3) ผู้ประกอบธุรกิจต้องจัดให้มีนโยบายสำรองข้อมูลสำคัญทางธุรกิจ ระบบปฏิบัติการ แอพพลิเคชั่นระบบงานคอมพิวเตอร์ และชุดคำสั่งที่ใช้ทำงานให้ครบถ้วนและสามารถพร้อมใช้งานได้อย่างต่อเนื่อง

(8.4) ผู้ประกอบธุรกิจต้องจัดเก็บและบันทึกหลักฐาน (logs) ต่าง ๆ อย่างครบถ้วนและเพียงพอ รวมทั้งมีการติดตามและวิเคราะห์หลักฐานที่จัดเก็บดังกล่าว ทั้งนี้ เพื่อการตรวจสอบการล่วงรู้ข้อมูลภายในระหว่างหน่วยงาน และบุคลากร การสอบทานการใช้งานข้อมูลและระบบสารสนเทศตามหน้าที่ที่ผู้ปฏิบัติงานได้รับมอบหมาย การตรวจสอบการเข้าใช้งานระบบสารสนเทศโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง การตรวจสอบและป้องกันการใช้งานระบบสารสนเทศที่มีความผิดปกติหรือไม่เป็นไปตามกฎหมายหรือหลักเกณฑ์ของทางการ และการตรวจสอบตัวตนของลูกค้าที่ทำรายการซื้อขายผ่านระบบอินเทอร์เน็ต

(8.5) ผู้ประกอบธุรกิจต้องจัดให้มีขั้นตอนควบคุมการติดตั้งซอฟต์แวร์บนระบบงาน รวมทั้งจัดให้มีมาตรการเพื่อจำกัดการติดตั้งซอฟต์แวร์โดยผู้ใช้งาน เพื่อให้ระบบปฏิบัติงานต่าง ๆ มีความครบถ้วนถูกต้องและน่าเชื่อถือ

(8.6) ประกอบธุรกิจต้องจัดให้มีระบบในการบริหารจัดการช่องโหว่ทางเทคนิคอย่างเหมาะสมเพียงพอ ทั้งนี้ เพื่อป้องกันภัยคุกคามจากช่องโหว่ดังกล่าว

(8.7) ผู้ประกอบธุรกิจต้องจัดให้มีการวางแผนการตรวจสอบระบบสารสนเทศอย่างเพียงพอเหมาะสม โดยให้ดำเนินการ ดังต่อไปนี้

(ก) จัดให้มีการวางแผนการตรวจสอบระบบสารสนเทศให้สอดคล้องกับความเสี่ยงที่ได้ประเมินไว้

(ข) กำหนดขอบเขตการตรวจสอบทางเทคนิคให้ครอบคลุมจุดเสี่ยงที่สำคัญ และต้องควบคุมการตรวจสอบดังกล่าวไม่ให้กระทบต่อการปฏิบัติงานตามปกติ

(ค) จัดให้มีการทดสอบนอกเวลาทำการ ในกรณีที่การตรวจสอบระบบสารสนเทศดังกล่าวมีโอกาสกระทบต่อความพร้อมใช้งานของระบบ

(9) การรักษาความมั่นคงปลอดภัยด้านการสื่อสารและระบบเครือข่ายคอมพิวเตอร์ (Communications Security)

(9.1) เพื่อป้องกันการกระทำที่มีความเสี่ยงต่อข้อมูลสารสนเทศในระบบเครือข่ายคอมพิวเตอร์ และป้องกันโครงสร้างพื้นฐานที่สนับสนุนระบบเครือข่ายคอมพิวเตอร์ ให้ผู้ประกอบธุรกิจดำเนินการดังต่อไปนี้

(ก) จัดให้มีการบริหารจัดการและควบคุมระบบเครือข่ายคอมพิวเตอร์อย่างมั่นคงปลอดภัย

(ข) จัดทำข้อตกลงการใช้บริการระบบเครือข่ายคอมพิวเตอร์กับผู้ให้บริการภายนอก ทั้งในด้านวิธีการบริหารจัดการ คุณภาพการให้บริการ รวมทั้งกระบวนการรักษาความมั่นคงปลอดภัยของระบบเครือข่ายคอมพิวเตอร์

(ค) จัดให้มีการแบ่งแยกระบบเครือข่ายคอมพิวเตอร์ตามความเหมาะสม โดยระบุขอบเขตของระบบเครือข่ายย่อยอย่างชัดเจน และจัดให้มีกระบวนการควบคุมการเข้าถึงขอบเขตดังกล่าวอย่างเหมาะสม

(9.2) เพื่อรักษาความมั่นคงปลอดภัยในการรับส่งข้อมูลสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์ ให้ผู้ประกอบธุรกิจดำเนินการดังต่อไปนี้

(ก) จัดให้มีนโยบายและหลักปฏิบัติเพื่อปกป้องข้อมูลสารสนเทศที่รับส่งผ่านระบบและอุปกรณ์ในการสื่อสารทุกประเภท

(ข) ต้องคำนึงถึงความมั่นคงปลอดภัยของข้อมูลสารสนเทศที่รับส่งผ่านระบบ กรณีที่มีการใช้งานระบบรับส่งข้อความผ่านทางอิเล็กทรอนิกส์

(ค) จัดให้พนักงานและผู้ให้บริการภายนอก มีการทำสัญญารักษาความลับหรือไม่เปิดเผยข้อมูลที่มีความสำคัญ

(10) การจัดหาหรือจัดให้มีการพัฒนาและดูแลรักษาระบบสารสนเทศ (System Acquisition, Development and Maintenance)

(10.1) เพื่อให้กระบวนการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเป็นส่วนหนึ่งของระบบสารสนเทศของทั้งภายในองค์กรและที่เกี่ยวข้องกับการให้บริการภายนอกผ่านเครือข่ายสาธารณะ ตลอดช่วงอายุการใช้งานระบบสารสนเทศ ให้ผู้ประกอบธุรกิจดำเนินการ ดังต่อไปนี้

(ก) ระบุข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศไว้เป็นส่วนหนึ่งเมื่อจัดให้มีระบบสารสนเทศใหม่หรือเมื่อปรับปรุงระบบเก่า

(ข) จัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศที่ผ่านระบบให้บริการการใช้งาน ทั้งในกรณีทั่วไป และกรณีที่ผ่านเครือข่ายสาธารณะ

(10.2) ผู้ประกอบธุรกิจต้องจัดให้มีการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตลอดช่วงการพัฒนาระบบสารสนเทศ โดยให้มีการดำเนินการดังต่อไปนี้

(ก) จัดให้มีการควบคุมการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบสารสนเทศตลอดทุกขั้นตอนตามการควบคุมที่ได้กำหนดไว้

(ข) จัดให้มีการทดสอบระบบสารสนเทศที่ได้รับการพัฒนาหรือแก้ไขเปลี่ยนแปลง เพื่อให้มั่นใจว่าการทำงานมีประสิทธิภาพ การประมวลผลถูกต้องครบถ้วนและเป็นไปตามความต้องการของผู้ใช้งาน พร้อมทั้งปรับปรุงแผนบริหารความต่อเนื่องทางธุรกิจให้สอดคล้องกับการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบสารสนเทศดังกล่าว

(ค) มีการควบคุมสภาพแวดล้อมของการพัฒนาระบบสารสนเทศให้มีความมั่นคงปลอดภัยตลอดขั้นตอนการพัฒนาระบบ

(ง) จัดให้มีการดูแล ติดตาม และควบคุมการปฏิบัติงานของผู้ให้บริการพัฒนาระบบงานสารสนเทศจากภายนอกให้เป็นไปตามนโยบายการพัฒนาระบบงานสารสนเทศของบริษัท ภายใต้ข้อตกลงที่ให้สิทธิผู้ประกอบธุรกิจสามารถเข้าตรวจสอบการปฏิบัติงานดังกล่าวได้

(จ) จัดให้มีการทดสอบการทำงานของระบบที่ได้รับการพัฒนาโดยผู้ใช้งานหรือผู้ทดสอบอื่นที่เป็นอิสระจากผู้พัฒนาระบบสารสนเทศดังกล่าว

(11) การควบคุมดูแลผู้ให้บริการภายนอก (Supplier Relationships)

(11.1) เพื่อป้องกันทรัพย์สินสารสนเทศของผู้ประกอบธุรกิจจากการเข้าถึงโดยผู้ให้บริการภายนอกอย่างไม่เหมาะสม ให้ผู้ประกอบธุรกิจดำเนินการดังต่อไปนี้

(ก) จัดให้มีนโยบายในการควบคุมดูแลผู้ให้บริการภายนอกอย่างเป็นลายลักษณ์อักษร

(ข) จัดให้มีข้อตกลงเกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและกระบวนการควบคุมอย่างเป็นลายลักษณ์อักษร และมีการลงนามร่วมกันระหว่างผู้ประกอบธุรกิจและผู้ให้บริการภายนอก

(11.2) ผู้ประกอบธุรกิจต้องควบคุมผู้ให้บริการภายนอกส่งมอบงานให้เป็นไปตามข้อตกลงที่จัดทำไว้กับผู้ประกอบธุรกิจ โดยให้ดำเนินการดังต่อไปนี้

(ก) จัดให้มีการติดตาม ทบทวน และตรวจสอบผู้ให้บริการภายนอกอย่างสม่ำเสมอ ทั้งในด้านฐานะทางการเงิน กระบวนการปฏิบัติงาน และประสิทธิภาพการปฏิบัติงาน

(ข) จัดให้มีการประเมินความเสี่ยงและกำหนดกระบวนการบริหารจัดการความเสี่ยง ในกรณีที่ผู้ให้บริการภายนอกมีการเปลี่ยนแปลงกระบวนการ ขั้นตอน วิธีการปฏิบัติงาน การรักษาความมั่นคงปลอดภัยในการปฏิบัติงาน รวมถึงการเปลี่ยนแปลงผู้ให้บริการภายนอก

(12) การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Incident Management)

ผู้ประกอบธุรกิจต้องจัดให้มีการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศได้อย่างถูกต้องและมีประสิทธิภาพในช่วงระยะเวลาที่เหมาะสม โดยครอบคลุมถึงกรณี

(ก) การรายงานเหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัย

(ข) การวิเคราะห์ภายหลังเหตุการณ์ยุติแล้ว เพื่อระบุถึงสาเหตุของเหตุการณ์ และเพื่อใช้ประโยชน์จากผลการวิเคราะห์ในการเตรียมความพร้อมรองรับเหตุการณ์ที่อาจเกิดขึ้นได้อีกในอนาคต

(13) การบริหารความต่อเนื่องทางธุรกิจในด้านความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Aspects of Business Continuity Management)

เพื่อให้มาตรการด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่อง ให้ผู้ประกอบธุรกิจดำเนินการดังต่อไปนี้

(ก) ต้องคำนึงถึงความมั่นคงปลอดภัยของระบบสารสนเทศเมื่อเกิดสถานการณ์ที่ไม่พึงประสงค์หรือไม่คาดคิด

(ข) จัดให้มีขั้นตอน กระบวนการดำเนินการ และการควบคุมด้านความมั่นคงปลอดภัยของระบบสารสนเทศ เพื่อให้มั่นใจได้ว่ามีความสอดคล้องกับแผนบริหารความต่อเนื่องทางธุรกิจ

(ค) กำหนดระยะเวลาในการกลับคืนสู่สภาพการดำเนินงานปกติของระบบสารสนเทศ พร้อมทั้งจัดลำดับการกู้คืนระบบงานสารสนเทศที่มีความสำคัญทุกระบบให้เหมาะสมกับผลกระทบที่อาจเกิดขึ้น

(ง) จัดให้มีการสำรองระบบสารสนเทศ เพื่อให้อยู่ในสภาพพร้อมใช้งานหรือสอดคล้องกับระยะเวลาในการกลับคืนสู่สภาพการดำเนินงานปกติของระบบสารสนเทศที่กำหนด

(14) การควบคุมกระบวนการทำงานให้เป็นไปตามข้อกำหนด (Compliance)

(14.1) เพื่อป้องกันการละเมิดกฎหมาย หลักเกณฑ์ของทางการและข้อกำหนดตามสัญญาต่าง ๆ ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ให้ผู้ประกอบธุรกิจดำเนินการดังต่อไปนี้

(ก) จัดให้มีการระบุกฎหมาย หลักเกณฑ์ของทางการ และข้อกำหนดตามสัญญาต่าง ๆ ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ โดยจัดทำเป็นเอกสารและปรับปรุงให้เป็นปัจจุบันอย่างสม่ำเสมอ

(ข) กำหนดขั้นตอนปฏิบัติงานเพื่อให้มั่นใจว่าในการใช้งานข้อมูลสารสนเทศที่อาจถือเป็นทรัพย์สินทางปัญญา หรือการใช้งานซอฟต์แวร์ที่พัฒนาโดยผู้ประกอบธุรกิจมีความสอดคล้องกับกฎหมายและข้อกำหนดตามสัญญาต่าง ๆ

(ค) ป้องกันมิให้ข้อมูลบันทึกหลักฐานต่าง ๆ เกิดความเสียหาย สูญหาย เปลี่ยนแปลงแก้ไข เข้าถึงหรือเผยแพร่โดยไม่ได้รับอนุญาต โดยให้สอดคล้องกับกฎหมาย ข้อกำหนดตามสัญญาต่าง ๆ และความต้องการทางธุรกิจ

(ง) จัดให้มีการคุ้มครองข้อมูลส่วนบุคคลโดยให้สอดคล้องกับกฎหมาย หลักเกณฑ์ของทางการ และข้อกำหนดตามสัญญาต่าง ๆ

(จ) ควบคุมการเข้ารหัสข้อมูลให้สอดคล้องกับกฎหมาย หลักเกณฑ์ของทางการ และข้อกำหนดตามสัญญาต่าง ๆ

(14.2) เพื่อให้การบริหารจัดการความมั่นคงปลอดภัยของระบบสารสนเทศให้เป็นไปตามนโยบายและหลักปฏิบัติของผู้ประกอบธุรกิจ รวมทั้งมาตรฐานสากลด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ให้ผู้ประกอบธุรกิจดำเนินการดังต่อไปนี้

(ก) จัดให้มีการตรวจสอบขั้นตอนและการปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศให้เป็นไปตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศอย่างน้อยปีละ 1 ครั้ง และเมื่อมีเหตุการณ์ที่มีนัยสำคัญ

(ข) จัดให้มีการทบทวนและปรับปรุงขั้นตอนและการปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศให้เป็นไปตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ และสอดคล้องกับมาตรฐานสากลด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

(ค) จัดให้มีการทบทวนตรวจสอบระบบสารสนเทศในด้านเทคนิคอย่างสม่ำเสมอ เพื่อให้สอดคล้องกับนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ และมาตรฐานสากลด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

2.4.2 ปรับปรุงแนวทางปฏิบัติให้สอดคล้องกับหลักการตามข้อ 2.4.1 โดยมีรายละเอียดตามเอกสารแนบ

2.5 การมีผลใช้บังคับ

ให้ประกาศมีผลใช้บังคับในอีก 12 เดือนข้างหน้านับแต่วันที่กำหนดในประกาศ

แบบสำรวจรับฟังความคิดเห็น

เรื่อง หลักการในการแก้ไขหลักเกณฑ์เกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และสัญญาซื้อขายล่วงหน้า

ข้อมูลทั่วไป

ชื่อผู้ตอบ_____ตำแหน่ง_____

ชื่อบริษัท/ องค์กร_____

อาชีพ/ ประเภทธุรกิจ_____

เบอร์โทรศัพท์_____เบอร์โทรสาร_____

e-mail address_____

สถานะของผู้ให้ความคิดเห็น

- ☐ บริษัทหลักทรัพย์
- ☐ ผู้ประกอบธุรกิจสัญญาซื้อขายล่วงหน้า
- ☐ ธนาคารพาณิชย์
- ☐ บริษัทประกันชีวิต
- ☐ อื่น ๆ (ระบุ)_____

ความเห็นและข้อเสนอแนะ

1. วัตถุประสงค์

   ☐ เห็นด้วย ☐ ไม่เห็นด้วย

   ความเห็นและข้อเสนอแนะ_____

2. ขอบเขตการใช้บังคับ

   ☐ เห็นด้วย ☐ ไม่เห็นด้วย

   ความเห็นและข้อเสนอแนะ_____

3. หลักเกณฑ์ที่ปรับปรุง

(3.1) นโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Policy)

☐ เห็นด้วย ☐ ไม่เห็นด้วย

ความเห็นและข้อเสนอแนะ_____

_____

_____

(3.2) การจัดโครงสร้างความมั่นคงปลอดภัยของระบบสารสนเทศ (Organization of Information Security)

☐ เห็นด้วย ☐ ไม่เห็นด้วย

ความเห็นและข้อเสนอแนะ_____

_____

_____

(3.3) การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร (Human Resource Security)

☐ เห็นด้วย ☐ ไม่เห็นด้วย

ความเห็นและข้อเสนอแนะ_____

_____

_____

(3.4) การบริหารจัดการทรัพย์สินสารสนเทศ (Asset Management)

☐ เห็นด้วย ☐ ไม่เห็นด้วย

ความเห็นและข้อเสนอแนะ_____

_____

_____

(3.5) การควบคุมการเข้าถึง (Access Control)

☐ เห็นด้วย ☐ ไม่เห็นด้วย

ความเห็นและข้อเสนอแนะ_____

_____

_____

(3.6) การควบคุมการเข้ารหัสข้อมูล (Cryptographic Controls)

☐ เห็นด้วย ☐ ไม่เห็นด้วย

ความเห็นและข้อเสนอแนะ_____

_____

_____

(3.7) การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม (Physical and Environmental Security)

☐ เห็นด้วย ☐ ไม่เห็นด้วย

ความเห็นและข้อเสนอแนะ_____

_____

_____

(3.8) การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ (Operations Security)

☐ เห็นด้วย ☐ ไม่เห็นด้วย

ความเห็นและข้อเสนอแนะ_____

_____

_____

(3.9) การรักษาความมั่นคงปลอดภัยด้านการสื่อสารและระบบเครือข่ายคอมพิวเตอร์ (Communications Security)

☐ เห็นด้วย ☐ ไม่เห็นด้วย

ความเห็นและข้อเสนอแนะ_____

_____

_____

(3.10) การจัดหาหรือจัดให้มีการพัฒนาและดูแลรักษาระบบสารสนเทศ (System Acquisition, Development and Maintenance)

☐ เห็นด้วย ☐ ไม่เห็นด้วย

ความเห็นและข้อเสนอแนะ_____

_____

_____

(3.11) การควบคุมดูแลผู้ให้บริการภายนอก (Supplier Relationships)

☐ เห็นด้วย ☐ ไม่เห็นด้วย

ความเห็นและข้อเสนอแนะ_____

_____

_____

(3.12) การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Incident Management)

☐ เห็นด้วย ☐ ไม่เห็นด้วย

ความเห็นและข้อเสนอแนะ_____

_____

_____

(3.13) การบริหารความต่อเนื่องทางธุรกิจในด้านความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Aspects of Business Continuity Management)

☐ เห็นด้วย ☐ ไม่เห็นด้วย

ความเห็นและข้อเสนอแนะ_____

_____

_____

(3.14) การควบคุมกระบวนการทำงานให้เป็นไปตามข้อกำหนด (Compliance)

☐ เห็นด้วย ☐ ไม่เห็นด้วย

ความเห็นและข้อเสนอแนะ_____

_____

_____

4. การมีผลใช้บังคับ

☐ เห็นด้วย ☐ ไม่เห็นด้วย

ความเห็นและข้อเสนอแนะ_____

_____

_____

5. ความเห็นและข้อเสนอแนะอื่น ๆ_____

_____

_____

กรุณาส่งแบบสำรวจความคิดเห็นกลับไปที่
ฝ่ายกำกับและพัฒนาธุรกิจหลักทรัพย์
สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์
ชั้น 25 เลขที่ 333/3 ถนนวิภาวดีรังสิต
แขวงจอมพล เขตจตุจักร กรุงเทพฯ 10900
หรือ โทรสาร 0-2263-6229 หรือ e-mail: insec@sec.or.th

วันสุดท้ายของการแสดงความคิดเห็น วันที่ 10 เมษายน 2558

***** สำนักงานขอขอบคุณท่านที่ได้ให้ความร่วมมือในการแสดงความคิดเห็นในครั้งนี้ *****