ประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์
ที่ สธ. 37/2559
เรื่อง ข้อกำหนดในรายละเอียดเกี่ยวกับการจัดให้มี
ระบบเทคโนโลยีสารสนเทศ

อาศัยอำนาจตามความในข้อ 5(1) ประกอบกับข้อ 12 วรรคหนึ่ง (11) และ (12) และข้อ 14 แห่งประกาศคณะกรรมการกำกับตลาดทุน ที่ ทธ. 35/2556 เรื่อง มาตรฐานการประกอบธุรกิจ โครงสร้างการบริหารงาน ระบบงาน และการให้บริการของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสัญญาซื้อขายล่วงหน้า ลงวันที่ 6 กันยายน พ.ศ. 2556 สำนักงานออกประกาศไว้ดังต่อไปนี้

ข้อ 1 ประกาศนี้ให้ใช้บังคับตั้งแต่วันที่ 1 กันยายน พ.ศ. 2560 เป็นต้นไป

ข้อ 2 ในประกาศนี้

"ประกาศมาตรฐานการประกอบธุรกิจ" หมายความว่า ประกาศคณะกรรมการกำกับตลาดทุน ที่ ทธ. 35/2556 เรื่อง มาตรฐานการประกอบธุรกิจ โครงสร้างการบริหารงาน ระบบงาน และการให้บริการของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสัญญาซื้อขายล่วงหน้า ลงวันที่ 6 กันยายน พ.ศ. 2556

"โปรแกรมสำเร็จรูป" หมายความว่า ระบบการคำนวณที่แสดงผลเป็นการวิเคราะห์เพื่อให้คำแนะนำเกี่ยวกับคุณค่าหรือความเหมาะสมในการลงทุนในหลักทรัพย์หรือสัญญาซื้อขายล่วงหน้า

"ทรัพย์สินสารสนเทศ" หมายความว่า

(1) ทรัพย์สินสารสนเทศประเภทระบบ ได้แก่ ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

(2) ทรัพย์สินสารสนเทศประเภทอุปกรณ์ ได้แก่ ตัวเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล และอุปกรณ์อื่นใด

(3) ทรัพย์สินสารสนเทศประเภทข้อมูล ได้แก่ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์

ข้อ 3 ประกาศนี้ให้ใช้บังคับกับผู้ที่ได้รับใบอนุญาตประกอบธุรกิจหลักทรัพย์หรือธุรกิจสัญญาซื้อขายล่วงหน้าประเภทดังต่อไปนี้

(1) การเป็นนายหน้าซื้อขายหลักทรัพย์ การค้าหลักทรัพย์ หรือการจัดจำหน่ายหลักทรัพย์

(2) การเป็นที่ปรึกษาการลงทุนที่มีการวางแผนการลงทุนให้แก่ลูกค้า หรือใช้โปรแกรมสำเร็จรูปประกอบการให้บริการแก่ลูกค้า

(3) การจัดการกองทุนรวม แต่ไม่รวมถึงการจัดการกองทุนรวมเพื่อผู้ลงทุนซึ่งเป็นคนต่างด้าว

(4) การจัดการกองทุนส่วนบุคคล

(5) กิจการการยืมและให้ยืมหลักทรัพย์

(6) การให้สินเชื่อเพื่อธุรกิจหลักทรัพย์

(7) การเป็นตัวแทนซื้อขายสัญญาซื้อขายล่วงหน้า

(8) การเป็นที่ปรึกษาสัญญาซื้อขายล่วงหน้าที่มีการวางแผนการลงทุนให้แก่ลูกค้าหรือใช้โปรแกรมสำเร็จรูปประกอบการให้บริการแก่ลูกค้า

(9) การเป็นผู้จัดการเงินทุนสัญญาซื้อขายล่วงหน้า

ในกรณีที่ผู้ประกอบธุรกิจตามวรรคหนึ่งเป็นธนาคารพาณิชย์ตามกฎหมายว่าด้วยธุรกิจสถาบันการเงิน บริษัทประกันชีวิตตามกฎหมายว่าด้วยการประกันชีวิต หรือสถาบันการเงินที่จัดตั้งขึ้นตามกฎหมายอื่น ให้ปฏิบัติตามประกาศนี้เฉพาะข้อ 11 และข้อ 23(4)

ข้อ 4 ข้อกำหนดในรายละเอียดตามประกาศนี้ กำหนดขึ้นเพื่อให้ผู้ประกอบธุรกิจปฏิบัติตามประกาศมาตรฐานการประกอบธุรกิจ ในส่วนที่เกี่ยวกับระบบเทคโนโลยีสารสนเทศที่มีประสิทธิภาพในเรื่องดังต่อไปนี้ ให้เป็นไปในแนวทางเดียวกัน

(1) การกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กร ให้เป็นไปตามหมวด 1

(2) การกำหนดนโยบาย มาตรการ โครงสร้างการบริหารจัดการ เพื่อรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ให้เป็นไปตามหมวด 2

(3) การบริหารจัดการทรัพย์สินสารสนเทศและการควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ ให้เป็นไปตามหมวด 3

(4) การรักษาความมั่นคงปลอดภัยด้านการสื่อสารข้อมูลสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์และการรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ ให้เป็นไปตามหมวด 4

(5) หลักเกณฑ์เพิ่มเติมอื่น ๆ ให้เป็นไปตามหมวด 5

หมวด 1
การกำกับดูแลและบริหารจัดการเทคโนโลยี
สารสนเทศระดับองค์กร

ข้อ 5 ผู้ประกอบธุรกิจต้องจัดให้มีนโยบายเป็นลายลักษณ์อักษรในการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศอย่างน้อยในเรื่องดังต่อไปนี้ ทั้งนี้ นโยบายดังกล่าวต้องได้รับความเห็นชอบจากคณะกรรมการของผู้ประกอบธุรกิจหรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบธุรกิจ

(1) การบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ซึ่งครอบคลุมถึงการระบุความเสี่ยง การประเมินความเสี่ยง และการควบคุมความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้

(2) การจัดสรรและบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศ ซึ่งครอบคลุมถึงการจัดสรรทรัพยากรให้เพียงพอต่อการดำเนินธุรกิจ และการกำหนดแนวทางเพื่อรองรับในกรณีที่ไม่สามารถจัดสรรทรัพยากรได้เพียงพอตามที่กำหนดไว้

(3) การจัดให้มีนโยบายและมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามข้อ 8 และข้อ 9

ข้อ 6 ผู้ประกอบธุรกิจต้องจัดให้มีการกำกับดูแลและบริหารจัดการด้านเทคโนโลยีสารสนเทศตามหลักเกณฑ์ดังต่อไปนี้ ทั้งนี้ เพื่อให้เป็นไปตามนโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจที่กำหนดไว้ตามข้อ 5

(1) สื่อสารนโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศให้แก่บุคลากรของผู้ประกอบธุรกิจที่เกี่ยวข้องอย่างทั่วถึงในลักษณะที่สามารถเข้าถึงได้ง่าย เพื่อให้บุคลากรดังกล่าวเข้าใจและสามารถปฏิบัติตามนโยบายดังกล่าวได้อย่างถูกต้อง

(2) กำหนดขั้นตอนและวิธีปฏิบัติงานให้เป็นไปตามนโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศ

(3) ทบทวนหรือปรับปรุงนโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศอย่างน้อยปีละ 1 ครั้ง โดยต้องทบทวนโดยไม่ชักช้าเมื่อมีเหตุการณ์ใด ๆ ซึ่งอาจส่งผลกระทบต่อการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศอย่างมีนัยสำคัญ และต้องปรับปรุงขั้นตอนและวิธีปฏิบัติงานให้สอดคล้องกับนโยบายที่มีการเปลี่ยนแปลงด้วย

(4) จัดให้มีการรายงานการปฏิบัติตามนโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศ ให้คณะกรรมการของผู้ประกอบธุรกิจทราบอย่างน้อยปีละ 1 ครั้ง และในกรณีที่มีเหตุการณ์ใด ๆ ซึ่งอาจส่งผลกระทบต่อการปฏิบัติตามนโยบายดังกล่าวอย่างมีนัยสำคัญ ต้องรายงานให้คณะกรรมการของผู้ประกอบธุรกิจทราบโดยไม่ชักช้าด้วย

(5) จัดให้มีระบบการควบคุมภายในสำหรับการปฏิบัติงานให้เป็นไปตามนโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศ อย่างน้อยดังนี้

(ก) มีการตรวจสอบภายในและการสอบทานการปฏิบัติงานให้เป็นไปตามนโยบายดังกล่าวอย่างเป็นระบบ

(ข) มีการปรับปรุงแก้ไขข้อบกพร่อง และติดตามการปรับปรุงแก้ไขดังกล่าวอย่างเป็นระบบ

หมวด 2
การกำหนดนโยบาย มาตรการ โครงสร้างการบริหารจัดการ เพื่อรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

ข้อ 7 ในหมวดนี้

“การปฏิบัติงานจากเครือข่ายภายนอกบริษัท” (teleworking) หมายความว่า การปฏิบัติงานที่มีการเข้าถึงระบบสารสนเทศที่มีความสำคัญโดยไม่ผ่านการเชื่อมต่อกับระบบเครือข่ายคอมพิวเตอร์ภายในของผู้ประกอบธุรกิจโดยตรง

“การใช้งานอุปกรณ์เคลื่อนที่” หมายความว่า การปฏิบัติงานที่มีการใช้อุปกรณ์เคลื่อนที่ (mobile device) เพื่อเข้าถึงระบบสารสนเทศที่มีความสำคัญโดยผ่านการเชื่อมต่อกับระบบเครือข่ายคอมพิวเตอร์ภายในของผู้ประกอบธุรกิจโดยตรง

ข้อ 8 ผู้ประกอบธุรกิจต้องจัดให้มีการกำหนดนโยบายอย่างน้อยในเรื่องดังต่อไปนี้ไว้เป็นลายลักษณ์อักษร เพื่อรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (information security policy)

(1) นโยบายการใช้งานระบบสารสนเทศร่วมกันบนระบบเครือข่ายคอมพิวเตอร์เพื่อการประมวลผลตามความต้องการของผู้ใช้งาน (cloud computing) ซึ่งครอบคลุมถึงวิธีการคัดเลือกและประเมินผู้ให้บริการ การทบทวนคุณสมบัติของผู้ให้บริการ ข้อกำหนดเกี่ยวกับการใช้บริการและการตรวจสอบบันทึกหลักฐานต่าง ๆ ที่อาจส่งผลกระทบต่อการใช้บริการ

(2) นโยบายการใช้งานระบบการเข้ารหัสข้อมูลและการบริหารกุญแจเข้ารหัสข้อมูลที่สามารถป้องกันการเข้าถึงหรือเปลี่ยนแปลงแก้ไขข้อมูลที่เป็นความลับหรือมีความสำคัญ

(3) นโยบายการรับส่งข้อมูลสารสนเทศผ่านระบบเครือข่ายภายในองค์กร และระหว่างเครือข่ายภายในองค์กรกับระบบเครือข่ายภายนอกองค์กร ให้มีความมั่นคงปลอดภัย

(4) นโยบายควบคุมการเข้าถึงข้อมูลและสิ่งอำนวยความสะดวกในการประมวลผลข้อมูลต่าง ๆ (information processing facilities) ให้สอดคล้องกับข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

(5) นโยบายเพื่อรองรับในกรณีที่ผู้ประกอบธุรกิจแต่งตั้งบุคคลอื่นเป็นผู้รับดำเนินการในงานที่เกี่ยวกับระบบสารสนเทศของผู้ประกอบธุรกิจ ซึ่งครอบคลุมถึงวิธีการคัดเลือกและประเมินผู้รับดำเนินการ การทบทวนคุณสมบัติของผู้รับดำเนินการ และการมีข้อกำหนดเกี่ยวกับการใช้บริการเพื่อลดความเสี่ยงจากการเข้าถึงทรัพย์สินสารสนเทศอย่างไม่เหมาะสม

เพื่อประโยชน์ตามวรรคหนึ่ง (4) คำว่า “สิ่งอำนวยความสะดวกในการประมวลผลข้อมูล” หมายความว่า อุปกรณ์ ระบบงาน หรือสภาพแวดล้อม ที่จำเป็นหรือมีส่วนช่วยให้การประมวลผลข้อมูลเป็นไปอย่างครบถ้วน ถูกต้อง และมีประสิทธิภาพ เช่น อุปกรณ์หรือโปรแกรมประมวลผลข้อมูล ระบบเครือข่ายคอมพิวเตอร์ ขั้นตอน หรือสถานที่ประมวลผลข้อมูล

ข้อ 9 ผู้ประกอบธุรกิจต้องจัดให้มีมาตรการอย่างน้อยในเรื่องดังต่อไปนี้ เพื่อรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

(1) มาตรการรักษาความปลอดภัยที่รัดกุมเพียงพอสำหรับข้อมูลที่เป็นความลับหรือมีความสำคัญ ในกรณีที่มีการปฏิบัติงานจากเครือข่ายภายนอกบริษัทหรือมีการใช้งานอุปกรณ์เคลื่อนที่ โดยกรณีที่เป็นการใช้งานอุปกรณ์เคลื่อนที่ ต้องจัดให้มีการลงทะเบียนอุปกรณ์เคลื่อนที่ก่อนการใช้งานและทบทวนทะเบียนดังกล่าวอย่างน้อยปีละ 1 ครั้งและเมื่อมีการเปลี่ยนอุปกรณ์เคลื่อนที่

(2) มาตรการในการใช้งานระบบสารสนเทศร่วมกันบนระบบเครือข่ายคอมพิวเตอร์เพื่อการประมวลผลตามความต้องการของผู้ใช้งานตามนโยบายที่กำหนดไว้ในข้อ 8(1) ที่ครอบคลุมเรื่องดังนี้

(ก) ข้อตกลงร่วมกันระหว่างผู้ให้บริการและผู้ใช้บริการซึ่งมีรายละเอียดในเรื่องดังต่อไปนี้เป็นอย่างน้อย

1. หน้าที่และความรับผิดชอบของผู้ให้บริการ รวมถึงความรับผิดต่อผู้ประกอบธุรกิจในกรณีที่ผู้ให้บริการไม่สามารถปฏิบัติตามข้อตกลงได้

2. ขั้นตอนการปฏิบัติงานที่เป็นไปตามมาตรฐานการรับรองความมั่นคงปลอดภัยด้านสารสนเทศในระดับสากล

3. มาตรการการรักษาความมั่นคงปลอดภัย การควบคุมการเข้าถึง และการเปิดเผยข้อมูลสารสนเทศ

4. การตรวจสอบการปฏิบัติงานจากผู้ตรวจสอบที่เป็นอิสระ

5. เงื่อนไขในกรณีที่ผู้ให้บริการจะให้ผู้ให้บริการรายอื่นรับดำเนินการช่วง (subcontract of the cloud provider) และข้อกำหนดความรับผิดต่อความเสียหายที่อาจเกิดขึ้นจากการดำเนินการของผู้ให้บริการรายอื่น

(ข) คุณสมบัติด้านความปลอดภัยของผู้ให้บริการรายอื่นที่รับดำเนินการช่วงซึ่งเทียบเท่ากับผู้ให้บริการหรือเป็นไปตามมาตรฐานสากล

(ค) การติดตาม ประเมิน และทบทวนการให้บริการของผู้ให้บริการ

(ง) ขั้นตอนในการโอนย้ายข้อมูลไปยังผู้ให้บริการรายใหม่ ในกรณีที่มีการเปลี่ยนตัวผู้ให้บริการ

ข้อ 10 ผู้ประกอบธุรกิจต้องจัดให้มีโครงสร้างการบริหารงานเพื่อรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (organization of information security) ตามหลักเกณฑ์ดังต่อไปนี้

(1) กำหนดรายละเอียดเกี่ยวกับหน้าที่และความรับผิดชอบในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศเป็นลายลักษณ์อักษร และแนวทางในการปฏิบัติหน้าที่ ให้กับบุคลากรของผู้ประกอบธุรกิจ

(2) สอบทานการปฏิบัติงานเพื่อป้องกันความเสี่ยงในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศที่อาจเกิดขึ้นในการปฏิบัติหน้าที่

(3) จัดให้มีช่องทางในการติดต่อสำนักงาน หน่วยงานกำกับดูแลด้านเทคโนโลยีสารสนเทศ และหน่วยงานของผู้ให้บริการที่สนับสนุนการทำงานระบบสารสนเทศของผู้ประกอบธุรกิจ โดยต้องปรับปรุงรายชื่อและช่องทางสำหรับติดต่อดังกล่าวให้เป็นปัจจุบัน

ข้อ 11 ผู้ประกอบธุรกิจต้องมีการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (information security incident management) ให้เป็นไปตามหลักเกณฑ์ดังต่อไปนี้

(1) กำหนดขั้นตอนและกระบวนการในการบริหารจัดการเหตุการณ์ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ

(2) กำหนดผู้มีหน้าที่รับผิดชอบในการบริหารจัดการเหตุการณ์ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ

(3) รายงานต่อผู้มีหน้าที่รับผิดชอบในการบริหารจัดการเหตุการณ์ตาม (2) และสำนักงานโดยไม่ชักช้าเมื่อเกิดเหตุการณ์ดังกล่าว

(4) ทดสอบขั้นตอนและกระบวนการในการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศตาม (1) อย่างน้อยปีละ 1 ครั้ง โดยอย่างน้อยต้องครอบคลุมถึงการบริหารจัดการความเสี่ยงไซเบอร์ (cyber security drill)

(5) พิจารณาทบทวนขั้นตอนและกระบวนการในการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ หลังจากที่มีการทดสอบตาม (4) แล้วอย่างน้อยปีละ 1 ครั้ง

(6) จัดให้มีการประเมินผลการทดสอบตาม (4) และประเมินผลพิจารณาทบทวนตาม (5) โดยต้องรายงานผลต่อคณะกรรมการของผู้ประกอบธุรกิจหรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบธุรกิจอย่างน้อยปีละ 1 ครั้ง ทั้งนี้ การดำเนินการดังกล่าวต้องกระทำโดยบุคคลที่เป็นอิสระจากผู้มีหน้าที่รับผิดชอบในการบริหารจัดการเหตุการณ์ตาม (2)

(7) จัดเก็บเอกสารหลักฐานที่เกี่ยวข้องกับการดำเนินการในการบริหารจัดการเหตุการณ์ดังกล่าวเป็นระยะเวลาไม่น้อยกว่า 2 ปีนับแต่วันที่จัดทำเอกสารนั้น โดยต้องเก็บรักษาไว้ในลักษณะที่พร้อมให้สำนักงานสามารถเรียกดูและตรวจสอบได้โดยไม่ชักช้า

เพื่อประโยชน์ตามวรรคหนึ่ง (4) ให้คำว่า “ความเสี่ยงไซเบอร์” หมายความว่า ภัยคุกคามที่ส่งผลกระทบ หรือสร้างความเสียหาย หรือก่อให้เกิดความเสี่ยงต่อการประกอบธุรกิจของผู้ประกอบธุรกิจ ซึ่งเกิดจากการใช้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ อินเทอร์เน็ต โครงข่ายโทรคมนาคม หรือการให้บริการโดยปกติของดาวเทียม

ข้อ 12 ผู้ประกอบธุรกิจต้องมีการบริหารความต่อเนื่องทางธุรกิจในด้านความมั่นคงปลอดภัยของระบบสารสนเทศ (information security of business continuity management) ให้เป็นไปตามหลักเกณฑ์ดังต่อไปนี้

(1) กำหนดมาตรการรองรับสำหรับกรณีที่อาจเกิดเหตุการณ์ไม่พึงประสงค์

(2) กำหนดขั้นตอน กระบวนการดำเนินการ และการควบคุม เกี่ยวกับความมั่นคงปลอดภัยของระบบสารสนเทศให้สอดคล้องกับแผนบริหารความต่อเนื่องทางธุรกิจ

(3) กำหนดระยะเวลาในการกลับคืนสู่สภาพการดำเนินงานปกติของระบบสารสนเทศ และจัดลำดับการกู้คืนระบบงานสารสนเทศที่มีความสำคัญให้สอดคล้องกับผลกระทบที่อาจเกิดขึ้น

(4) มีระบบสารสนเทศสำรองที่อยู่ในสภาพพร้อมใช้งาน ซึ่งต้องสอดคล้องกับระยะเวลาในการกลับคืนสู่สภาพการดำเนินงานตามปกติของระบบสารสนเทศตาม (3)

ข้อ 13 ผู้ประกอบธุรกิจต้องสร้างความตระหนักรู้เกี่ยวกับนโยบายและมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศให้แก่บุคลากรของผู้ประกอบธุรกิจและบุคคลภายนอก (human resource security) ที่มีการปฏิบัติงานโดยมีการเข้าถึงข้อมูลหรือระบบงานภายในองค์กร และดำเนินการให้บุคลากรดังกล่าวสามารถปฏิบัติหน้าที่ได้ตามนโยบายและมาตรการที่กำหนด ทั้งนี้ ตามหลักเกณฑ์ดังต่อไปนี้

(1) ให้ความรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศที่เกี่ยวข้องกับการปฏิบัติหน้าที่แก่บุคลากรของผู้ประกอบธุรกิจและบุคคลภายนอกที่ปฏิบัติงานดังกล่าว

(2) สื่อสารให้บุคลากรของผู้ประกอบธุรกิจและบุคคลภายนอกที่ปฏิบัติงานดังกล่าวระมัดระวังและงดเว้นการใช้งานระบบสารสนเทศในลักษณะที่อาจก่อให้เกิดความเสียหายแก่ผู้ประกอบธุรกิจหรือตลาดทุนโดยรวม หรือกระทบต่อความมั่นคงของประเทศ และต้องรายงานผู้มีหน้าที่รับผิดชอบในการบริหารจัดการเหตุการณ์ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศโดยไม่ชักช้าเมื่อพบความผิดปกติใด ๆ อย่างมีนัยสำคัญ

(3) กำหนดมาตรการในการลงโทษบุคลากรที่มีพฤติกรรมฝ่าฝืนหรือไม่ปฏิบัติตามนโยบายหรือหลักเกณฑ์เกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

หมวด 3
การบริหารจัดการทรัพย์สินสารสนเทศและการควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ

ข้อ 14 ในการบริหารจัดการทรัพย์สินสารสนเทศและการควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ ให้ผู้ประกอบธุรกิจปฏิบัติตามหลักเกณฑ์ดังต่อไปนี้

(1) มีการบริหารจัดการทรัพย์สินสารสนเทศ ตามข้อ 15 ถึงข้อ 17

(2) มีมาตรการเพื่อสร้างความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อมของทรัพย์สินสารสนเทศ ตามข้อ 18

(3) มีมาตรการเพื่อสร้างความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อมของทรัพย์สินสารสนเทศประเภทอุปกรณ์ ตามข้อ 19

(4) มีการควบคุมการเข้าถึงระบบและข้อมูลสารสนเทศ ตามข้อ 20

ข้อ 15 ผู้ประกอบธุรกิจต้องมีการบริหารจัดการทรัพย์สินสารสนเทศ (asset management) ให้เป็นไปตามหลักเกณฑ์ดังต่อไปนี้

(1) กำหนดบุคคลหรือหน่วยงานที่มีหน้าที่ดูแลรับผิดชอบทรัพย์สินสารสนเทศแต่ละประเภทตลอดอายุการใช้งานของทรัพย์สินดังกล่าว

(2) มีข้อกำหนดการใช้งานทรัพย์สินสารสนเทศที่เหมาะสม

(3) มีการทบทวนหน้าที่ความรับผิดชอบที่มีต่อทรัพย์สินสารสนเทศให้สอดคล้องกับหน้าที่ของผู้ปฏิบัติงานเมื่อมีการเปลี่ยนแปลงหน้าที่และความรับผิดชอบ

ข้อ 16 ในการบริหารจัดการทรัพย์สินสารสนเทศที่เป็นทรัพย์สินสารสนเทศประเภทระบบหรืออุปกรณ์ ผู้ประกอบธุรกิจต้องมีการจัดทำและจัดเก็บทะเบียนทรัพย์สินดังกล่าวตลอดจนทบทวนทะเบียนดังกล่าวอย่างน้อยปีละ 1 ครั้งหรือเมื่อมีการเปลี่ยนแปลงทรัพย์สินสารสนเทศอย่างมีนัยสำคัญด้วย

ข้อ 17 ในการบริหารจัดการทรัพย์สินสารสนเทศที่เป็นทรัพย์สินสารสนเทศประเภทข้อมูล ผู้ประกอบธุรกิจต้องดำเนินการจัดประเภทข้อมูลดังกล่าวตามระดับชั้นความลับและจัดประเภททรัพย์สินสารสนเทศอื่น ๆ ตามระดับความสำคัญ เพื่อให้ทรัพย์สินสารสนเทศได้รับการปกป้องในระดับที่เหมาะสมตามระดับชั้นความลับหรือระดับความสำคัญ แล้วแต่กรณีด้วย และในกรณีที่เป็นข้อมูลสารสนเทศ ผู้ประกอบธุรกิจต้องมีกระบวนการป้องกันการเปิดเผย เปลี่ยนแปลงแก้ไขหรือสร้างความเสียหายต่อข้อมูลสารสนเทศที่สำคัญ ที่ถูกจัดเก็บในสื่อบันทึกข้อมูลด้วย

ข้อ 18 ผู้ประกอบธุรกิจต้องมีมาตรการเพื่อสร้างความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (physical and environmental security) ของทรัพย์สินสารสนเทศตามหลักเกณฑ์ดังต่อไปนี้

(1) ประเมินความเสี่ยงและความสำคัญของทรัพย์สินสารสนเทศ

(2) กำหนดพื้นที่หวงห้ามและพื้นที่สำหรับจัดวางทรัพย์สินสารสนเทศที่มีความสำคัญให้มีความมั่นคงปลอดภัยและป้องกันมิให้บุคคลที่ไม่เกี่ยวข้องเข้าถึงพื้นที่ดังกล่าว

ข้อ 19 ในกรณีที่เป็นทรัพย์สินสารสนเทศประเภทอุปกรณ์ นอกจากมาตรการเพื่อสร้างความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อมของทรัพย์สินสารสนเทศตามข้อ 18 แล้ว ผู้ประกอบธุรกิจต้องป้องกันทรัพย์สินดังกล่าวมิให้เกิดความเสียหาย สูญหาย ถูกโจรกรรม เข้าถึงหรือถูกใช้งานโดยบุคคลที่ไม่เกี่ยวข้อง เพื่อให้สามารถปฏิบัติงานได้อย่างต่อเนื่อง

ข้อ 20 ผู้ประกอบธุรกิจต้องมีการควบคุมการเข้าถึงระบบและข้อมูลสารสนเทศ (access control) ให้เป็นไปตามหลักเกณฑ์ดังต่อไปนี้

(1) มีการบริหารจัดการบัญชีผู้ใช้งานโดยจำกัดการเข้าถึงข้อมูลสารสนเทศ ให้สามารถเข้าถึงได้เฉพาะบุคคลที่ได้รับสิทธิการเข้าถึงดังนี้

(ก) มีการลงทะเบียนบัญชีผู้ใช้งานระบบสารสนเทศ

(ข) มีการจัดสรรสิทธิการเข้าถึงระดับสูงอย่างจำกัดและมีการควบคุมการเข้าถึงสิทธิดังกล่าวอย่างเคร่งครัด

(ค) มีขั้นตอนการบริหารจัดการในการกำหนดรหัสผ่านอย่างเหมาะสม

(ง) มีการติดตามและทบทวนระดับสิทธิการเข้าถึงอย่างสม่ำเสมอ

(2) มีข้อกำหนดให้ผู้ใช้งานปฏิบัติตามขั้นตอนการใช้งานและดูแลรับผิดชอบรหัสผ่านอย่างมั่นคงปลอดภัย

(3) มีการป้องกันมิให้มีการเข้าถึงระบบสารสนเทศและโปรแกรมประยุกต์ (application software) โดยไม่ได้รับอนุญาต ดังนี้

(ก) ควบคุมการเข้าถึงข้อมูลสารสนเทศและฟังก์ชั่นต่าง ๆ ในโปรแกรมประยุกต์ของผู้ใช้งานและผู้ดูแลระบบสารสนเทศ ให้สอดคล้องกับสิทธิที่ได้รับ

(ข) ควบคุมการเข้าใช้งานระบบสารสนเทศและโปรแกรมประยุกต์

(ค) จัดให้มีระบบการบริหารจัดการรหัสผ่านที่มีความมั่นคงปลอดภัย

(ง) จำกัดการใช้งานโปรแกรมอรรถประโยชน์ต่าง ๆ (utility program) และจำกัดการเข้าถึงชุดคำสั่งควบคุมการทำงานของโปรแกรมอย่างเข้มงวด

หมวด 4
การรักษาความมั่นคงปลอดภัยด้านการสื่อสารข้อมูลสารสนเทศ ผ่านระบบเครือข่ายคอมพิวเตอร์และการรักษาความมั่นคงปลอดภัยในการปฏิบัติงาน ที่เกี่ยวข้องกับระบบสารสนเทศ

ข้อ 21 ผู้ประกอบธุรกิจต้องมีมาตรการรักษาความมั่นคงปลอดภัยในการสื่อสารข้อมูลและการปฏิบัติงานในเรื่องดังต่อไปนี้

(1) การสื่อสารข้อมูลสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์ตามข้อ 22

(2) การปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ ตามข้อ 23

ข้อ 22 ผู้ประกอบธุรกิจต้องมีมาตรการรักษาความมั่นคงปลอดภัยด้านการสื่อสารข้อมูลสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์ (communications security) ให้เป็นไปตามหลักเกณฑ์ดังต่อไปนี้

(1) มีการบริหารจัดการและควบคุมระบบเครือข่ายคอมพิวเตอร์อย่างมั่นคงและปลอดภัย โดยต้องสามารถป้องกันมิให้เกิดการกระทำที่มีความเสี่ยงต่อข้อมูลสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์

(2) จัดทำข้อตกลงการใช้บริการผ่านระบบเครือข่ายคอมพิวเตอร์ที่เกี่ยวกับวิธีการบริหารจัดการ คุณภาพการให้บริการ และกระบวนการรักษาความมั่นคงปลอดภัยของระบบเครือข่ายคอมพิวเตอร์กับผู้รับดำเนินการ

(3) แบ่งแยกระบบเครือข่ายคอมพิวเตอร์ตามความเหมาะสม โดยระบุขอบเขตของระบบเครือข่ายย่อยอย่างชัดเจน และมีกระบวนการควบคุมการเข้าถึงขอบเขตดังกล่าวอย่างเหมาะสม

(4) กำหนดมาตรการในการรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศที่มีการรับส่งผ่านระบบเครือข่ายคอมพิวเตอร์

(5) ดำเนินการให้บุคลากรของผู้ประกอบธุรกิจและผู้รับดำเนินการ (ถ้ามี) มีข้อตกลงเกี่ยวกับการรักษาความลับหรือไม่เปิดเผยข้อมูลที่มีความสำคัญ

ข้อ 23 ผู้ประกอบธุรกิจต้องมีมาตรการรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ (operations security) ตามหลักเกณฑ์ดังต่อไปนี้

(1) กำหนดขั้นตอนการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศเพื่อให้การปฏิบัติงานนั้นเป็นไปอย่างถูกต้องและมั่นคงปลอดภัย

(2) มีมาตรการป้องกันและตรวจสอบโปรแกรมไม่ประสงค์ดี (malware) และมาตรการในการแก้ไขระบบสารสนเทศให้สามารถกลับมาใช้งานได้ตามปกติ

(3) มีการสำรองข้อมูลสำคัญทางธุรกิจ ระบบปฏิบัติการ โปรแกรมประยุกต์ ระบบงานคอมพิวเตอร์ และชุดคำสั่งที่ใช้ทำงาน ไว้อย่างครบถ้วน และต้องมีการทดสอบข้อมูลสำรองและกระบวนการกู้คืนข้อมูลอย่างน้อยปีละ 1 ครั้ง

(4) จัดเก็บและบันทึกหลักฐาน (logs) ต่าง ๆ ให้ครบถ้วนและเพียงพอสำหรับการตรวจสอบการล่วงรู้ข้อมูลภายในระหว่างหน่วยงานและบุคลากร การสอบทานการใช้งานข้อมูลและระบบสารสนเทศตามหน้าที่ที่ผู้ปฏิบัติงานได้รับมอบหมาย การตรวจสอบการเข้าใช้งานระบบสารสนเทศโดยบุคคลที่ไม่มีหน้าที่เกี่ยวข้อง การตรวจสอบและป้องกันการใช้งานระบบสารสนเทศที่มีความผิดปกติหรือไม่เป็นไปตามกฎหมายหรือกฎเกณฑ์ที่เกี่ยวข้อง และการตรวจสอบตัวตนของลูกค้าที่ทำรายการซื้อขายผ่านระบบอิเล็กทรอนิกส์ ทั้งนี้ ตามตารางแสดงรายละเอียดการจัดเก็บหลักฐาน

ที่แนบท้ายประกาศนี้โดยต้องมีการติดตามและวิเคราะห์หลักฐานที่จัดเก็บสำหรับการใช้งานสารสนเทศที่มีความสำคัญให้สอดคล้องกับการประเมินความเสี่ยงขององค์กร

(5) มีขั้นตอนควบคุมการติดตั้งซอฟท์แวร์บนระบบงาน และมีมาตรการจำกัดการติดตั้งซอฟท์แวร์โดยผู้ใช้งาน เพื่อให้ระบบปฏิบัติงานต่าง ๆ มีความถูกต้องครบถ้วนและน่าเชื่อถือ

(6) มีระบบในการบริหารจัดการกรณีช่องโหว่ทางเทคนิค (technical vulnerability management) ที่อาจเกิดขึ้นอย่างเพียงพอและเหมาะสมดังนี้

(ก) มีการทดสอบการเจาะระบบ (penetration test) กับระบบงานที่มีความสำคัญที่เชื่อมต่อกับระบบเครือข่ายภายนอก (untrusted network) โดยบุคคลที่เป็นอิสระจากหน่วยงานที่รับผิดชอบด้านเทคโนโลยีสารสนเทศ และเป็นไปตามการวิเคราะห์ความเสี่ยงและผลกระทบทางธุรกิจ (risk and business impact analysis) ดังนี้

1. กรณีที่เป็นระบบงานสำคัญที่ประเมินแล้วมีความสำคัญสูง ต้องทดสอบอย่างน้อยทุก 3 ปีและเมื่อมีการเปลี่ยนแปลงระบบงานดังกล่าวอย่างมีนัยสำคัญ

2. กรณีที่เป็นระบบงานที่มีความสำคัญอื่น ๆ ต้องทดสอบอย่างน้อยทุก 6 ปี

(ข) มีการประเมินช่องโหว่ของระบบ (vulnerability assessment) กับระบบงานที่มีความสำคัญทุกระบบอย่างน้อยปีละ 1 ครั้งและเมื่อมีการเปลี่ยนแปลงระบบงานดังกล่าวอย่างมีนัยสำคัญ และรายงานผลไปยังหน่วยงานกำกับดูแลการปฏิบัติงานหรือหน่วยงานตรวจสอบภายในโดยไม่ชักช้า

(7) มีการตรวจสอบระบบสารสนเทศดังนี้

(ก) วางแผนการตรวจสอบระบบสารสนเทศให้สอดคล้องกับความเสี่ยงที่ได้ประเมินไว้

(ข) กำหนดขอบเขตในการตรวจสอบระบบสารสนเทศทางเทคนิคให้ครอบคลุมถึงจุดเสี่ยงที่สำคัญ โดยการตรวจสอบดังกล่าวต้องไม่กระทบต่อการปฏิบัติงาน

(ค) ตรวจสอบระบบสารสนเทศนอกเวลาทำงาน ในกรณีที่การตรวจสอบนั้นอาจส่งผลกระทบต่อความพร้อมในการใช้งานระบบดังกล่าว

หมวด 5
หลักเกณฑ์เพิ่มเติมอื่น ๆ

ข้อ 24 ผู้ประกอบธุรกิจต้องจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศ (system acquisition, development and maintenance) ตามหลักเกณฑ์ดังต่อไปนี้

(1) มีข้อกำหนดในการจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศให้มีความมั่นคงปลอดภัย เมื่อมีระบบสารสนเทศใหม่หรือมีการปรับปรุงระบบเดิม

(2) จัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศ ในกรณีที่มีการเข้าถึงระบบการให้บริการการใช้งาน (application service)

(3) มีการควบคุมการพัฒนาหรือการแก้ไขเปลี่ยนแปลงระบบสารสนเทศในทุกขั้นตอนให้เป็นไปตามขั้นตอนการควบคุมความมั่นคงปลอดภัยด้านสารสนเทศที่กำหนดไว้

(4) มีการทดสอบระบบสารสนเทศที่ได้รับการพัฒนาหรือแก้ไขเปลี่ยนแปลง เพื่อให้มั่นใจได้ว่าระบบสารสนเทศดังกล่าวทำงานได้อย่างมีประสิทธิภาพ สามารถประมวลผลได้อย่างถูกต้องครบถ้วนและเป็นไปตามความต้องการของผู้ใช้งาน

(5) ปรับปรุงแผนบริหารความต่อเนื่องทางธุรกิจให้สอดคล้องกับการพัฒนาหรือการแก้ไขเปลี่ยนแปลงระบบสารสนเทศ

(6) มีการควบคุมบุคลากร ขั้นตอน และเทคโนโลยีสำหรับการพัฒนาระบบสารสนเทศให้มีความมั่นคงปลอดภัยตลอดขั้นตอนการพัฒนาระบบ

(7) มีการดูแล ติดตาม และควบคุมการพัฒนาระบบสารสนเทศของผู้รับดำเนินการให้เป็นไปตามข้อตกลงการใช้บริการ

(8) มีการทดสอบการทำงานของระบบสารสนเทศที่ได้รับการพัฒนา โดยผู้ใช้งานหรือผู้ทดสอบที่เป็นอิสระจากผู้พัฒนาระบบสารสนเทศดังกล่าว

ข้อ 25 ในกรณีที่ผู้ประกอบธุรกิจแต่งตั้งบุคคลอื่นเป็นผู้รับดำเนินการในงานที่เกี่ยวกับระบบสารสนเทศของผู้ประกอบธุรกิจ ผู้ประกอบธุรกิจต้องดำเนินการให้เป็นไปตามหลักเกณฑ์ดังต่อไปนี้

(1) มีข้อตกลงและกระบวนการควบคุมเกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศอย่างเป็นลายลักษณ์อักษรในการใช้บริการจากผู้รับดำเนินการ โดยผู้ประกอบธุรกิจและผู้รับดำเนินการ ต้องมีการลงนามร่วมกันในข้อตกลงและกระบวนการดังกล่าว

(2) มีการติดตาม ประเมิน ทบทวน และตรวจสอบผู้รับดำเนินการอย่างสม่ำเสมอ

(3) มีการประเมินความเสี่ยงและกำหนดกระบวนการบริหารจัดการความเสี่ยงในกรณีที่ผู้รับดำเนินการมีการเปลี่ยนแปลงกระบวนการ ขั้นตอน หรือวิธีการปฏิบัติงานในการรักษาความมั่นคงปลอดภัยในการปฏิบัติงาน หรือเปลี่ยนตัวผู้รับดำเนินการ

(4) มีมาตรการตรวจสอบดูแลให้ผู้รับดำเนินการปฏิบัติตามหลักเกณฑ์การปฏิบัติงานที่คณะกรรมการ ก.ล.ต. คณะกรรมการกำกับตลาดทุน หรือสำนักงาน กำหนดเกี่ยวกับงานที่รับดำเนินการ รวมทั้งระเบียบวิธีปฏิบัติที่ผู้ประกอบธุรกิจกำหนดขึ้นเพื่อให้เป็นไปตามหลักเกณฑ์ดังกล่าว โดยอย่างน้อยมาตรการดังกล่าวต้องสามารถควบคุมให้ผู้รับดำเนินการไม่มีลักษณะที่จะทำให้มีเหตุอันควรเชื่อได้ว่ามีข้อบกพร่องหรือมีความไม่เหมาะสมเกี่ยวกับการควบคุมและการปฏิบัติงานอันดีของธุรกิจ

(5) มีแผนรองรับในกรณีที่เกิดเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (incident response policy)

(6) กำหนดสิทธิในการเข้าตรวจสอบกระบวนการปฏิบัติงานของผู้รับดำเนินการและควบคุมให้การปฏิบัติงานเป็นไปตามข้อตกลงที่กำหนดไว้ เว้นแต่ในกรณีที่ผู้รับดำเนินการมีข้อจำกัดในการเข้าตรวจสอบการปฏิบัติงานดังกล่าว ผู้ประกอบธุรกิจต้องมีมาตรการเพื่อให้มั่นใจได้ว่าสามารถควบคุมการปฏิบัติงานของผู้รับดำเนินการให้เป็นไปตามข้อตกลงที่กำหนดไว้ได้

(7) มีข้อกำหนดให้ผู้รับดำเนินการยินยอมให้สำนักงานเรียกดู ตรวจสอบเอกสารหลักฐานที่เกี่ยวข้อง หรือสามารถเข้าตรวจสอบการปฏิบัติงานของผู้รับดำเนินการ

ประกาศ ณ วันที่ 12 กันยายน พ.ศ. 2559

(นายรพี สุจริตกุล)

เลขาธิการ

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์