ประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์
ที่ สธ./น. 34/2547
เรื่อง การควบคุมการปฏิบัติงานและการรักษาความปลอดภัย
ด้านเทคโนโลยีสารสนเทศของบริษัทหลักทรัพย์

---

เนื่องจากในปัจจุบันบริษัทหลักทรัพย์มีการใช้เทคโนโลยีสารสนเทศเป็นเครื่องมือในการประกอบธุรกิจหลักทรัพย์อย่างแพร่หลาย ซึ่งการใช้เทคโนโลยีสารสนเทศดังกล่าวอาจก่อให้เกิดความเสี่ยงในการดำเนินงานของบริษัทหลักทรัพย์หลายประการ โดยความเสี่ยงที่สำนักงานให้ความสำคัญ ได้แก่ ความเสี่ยงเกี่ยวกับการเข้าถึงข้อมูลและระบบคอมพิวเตอร์โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง หรือการที่บุคคลที่มีอำนาจหน้าที่ไม่สามารถเข้าถึงข้อมูลในระบบคอมพิวเตอร์ในส่วนที่เกี่ยวข้องกับงานที่รับผิดชอบ หรือความไม่ถูกต้องครบถ้วนของข้อมูลและการทำงานของระบบคอมพิวเตอร์ หรือการที่ไม่สามารถใช้ข้อมูลหรือระบบคอมพิวเตอร์ได้อย่างต่อเนื่องหรือในเวลาที่ต้องการ ตลอดจนการที่บริษัทหลักทรัพย์มิได้จัดให้มีการบริหารจัดการ ระบบคอมพิวเตอร์ และบุคลากรด้านคอมพิวเตอร์ ให้เหมาะสมและเพียงพอแก่การสนับสนุนการประกอบธุรกิจ ซึ่งความเสี่ยงตามที่กล่าวมาข้างต้นอาจก่อให้เกิดความเสียหายต่อการประกอบธุรกิจหลักทรัพย์ของบริษัทหลักทรัพย์และลูกค้าได้

ดังนั้น เพื่อเป็นการป้องกันความเสี่ยงเกี่ยวกับการใช้เทคโนโลยีสารสนเทศในการดำเนินงานของบริษัทหลักทรัพย์ และเพื่อประโยชน์ในการสั่งการของสำนักงาน อาศัยอำนาจตามมาตรา 141(2) แห่งพระราชบัญญัติหลักทรัพย์และตลาดหลักทรัพย์ พ.ศ. 2535 สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์โดยความเห็นชอบของคณะกรรมการ ก.ล.ต. ออกข้อกำหนดไว้ดังต่อไปนี้

ข้อ 1 ในประกาศนี้

“บริษัทหลักทรัพย์” หมายความว่า บริษัทที่ได้รับใบอนุญาตประกอบธุรกิจหลักทรัพย์ประเภทการเป็นนายหน้าซื้อขายหลักทรัพย์ การค้าหลักทรัพย์ การจัดจำหน่ายหลักทรัพย์ หรือการจัดการกองทุนรวม แต่ไม่รวมถึงสถาบันการเงินที่จัดตั้งตามกฎหมายอื่นและได้รับใบอนุญาตประกอบธุรกิจหลักทรัพย์

“สำนักงาน” หมายความว่า สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์

ข้อ 2 บริษัทหลักทรัพย์ต้องจัดให้มีนโยบายและระเบียบปฏิบัติเกี่ยวกับการควบคุมการปฏิบัติงานและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัทหลักทรัพย์ที่เป็นลายลักษณ์อักษรและได้รับความเห็นชอบจากคณะกรรมการบริหารหรือคณะกรรมการของบริษัทหลักทรัพย์

ข้อ 3 บริษัทหลักทรัพย์ต้องจัดให้มีการตรวจสอบการปฏิบัติงานด้านเทคโนโลยีสารสนเทศโดยหน่วยงานภายในบริษัทหลักทรัพย์เองหรือโดยผู้ตรวจสอบที่เป็นบุคคลภายนอกเพื่อทำหน้าที่ตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศทุกประเภทที่อาจเกิดขึ้นได้ ทั้งนี้ ในกรณีที่การตรวจสอบดังกล่าวดำเนินการโดยหน่วยงานภายในของบริษัทหลักทรัพย์ หน่วยงานดังกล่าวต้องมีความเป็นอิสระจากฝ่ายงานคอมพิวเตอร์ของบริษัทด้วย

ข้อ 4 บริษัทหลักทรัพย์ต้องแบ่งแยกหน่วยงานและบุคลากรที่ปฏิบัติหน้าที่ในส่วนการพัฒนาระบบงาน (development) ออกจากหน่วยงานและบุคลากรที่ปฏิบัติหน้าที่ในส่วนการบริหารระบบ (system administration) ออกจากกัน และต้องจัดให้มีระบบการสอบยันการปฏิบัติงานระหว่างบุคลากรในหน่วยงานดังกล่าว โดยอย่างน้อยต้องไม่มอบหมายให้บุคลากรคนหนึ่งคนใดรับผิดชอบการปฏิบัติงานตลอดกระบวนการในลักษณะที่อาจเป็นช่องทางให้มีการแก้ไขหรือเปลี่ยนแปลงข้อมูลหรือการทำงานของระบบคอมพิวเตอร์โดยมิชอบ

ข้อ 5 บริษัทหลักทรัพย์ต้องจัดให้มีระบบการรักษาความปลอดภัยทางกายภาพที่เพียงพอแก่การป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องได้เข้าถึงอุปกรณ์คอมพิวเตอร์ที่สำคัญซึ่งจัดเก็บอยู่ในศูนย์คอมพิวเตอร์ และต้องจัดให้มีระบบป้องกันความเสียหายจากสภาวะแวดล้อมหรือภัยพิบัติต่างๆ ให้แก่อุปกรณ์คอมพิวเตอร์ที่สำคัญภายในศูนย์คอมพิวเตอร์ด้วย

ข้อ 6 บริษัทหลักทรัพย์ต้องจัดให้มีระบบการรักษาความปลอดภัยของข้อมูลระบบคอมพิวเตอร์และระบบเครือข่าย ที่เพียงพอแก่การป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องได้เข้าถึง ล่วงรู้ ใช้ประโยชน์ หรือแก้ไขเปลี่ยนแปลงข้อมูลหรือระบบดังกล่าวได้

ข้อ 7 บริษัทหลักทรัพย์ต้องจัดให้มีมาตรการควบคุมที่เพียงพอเพื่อให้ระบบงานคอมพิวเตอร์ (application software) ที่ได้รับการพัฒนาหรือแก้ไขเปลี่ยนแปลงมีการประมวลผลที่ถูกต้องครบถ้วนและเป็นไปตามความต้องการของผู้ใช้งาน รวมทั้งต้องสื่อสารการพัฒนาหรือการเปลี่ยนแปลงให้ผู้ที่เกี่ยวข้องได้รับทราบอย่างทั่วถึงเพื่อให้สามารถใช้งานได้อย่างถูกต้อง

ข้อ 8 บริษัทหลักทรัพย์ต้องจัดให้มีการสำรองข้อมูลและระบบคอมพิวเตอร์ของบริษัทหลักทรัพย์เพื่อให้สามารถรองรับการประกอบธุรกิจได้อย่างต่อเนื่อง มีประสิทธิภาพและทันต่อเหตุการณ์

ข้อ 9 บริษัทหลักทรัพย์ต้องจัดให้มีมาตรการในการควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์อย่างเพียงพอเพื่อให้ระบบคอมพิวเตอร์และการประมวลผลข้อมูลสามารถทำงานได้อย่างต่อเนื่องและถูกต้องครบถ้วน

ข้อ 10 ในกรณีที่บริษัทหลักทรัพย์ใช้บริการงานเทคโนโลยีสารสนเทศของผู้ให้บริการที่เป็นบุคคลภายนอก บริษัทหลักทรัพย์ต้องจัดให้มีหลักเกณฑ์ในการคัดเลือกและพิจารณาความเหมาะสมของผู้ให้บริการ รวมทั้งต้องควบคุมและตรวจสอบการปฏิบัติงานของผู้ให้บริการอย่างเข้มงวด เพื่อให้มั่นใจว่าผู้ให้บริการสามารถปฏิบัติงานตามข้อกำหนดในประกาศนี้ได้

ข้อ 11 เพื่อให้บริษัทหลักทรัพย์สามารถปฏิบัติตามข้อกำหนดในประกาศนี้อย่างมีประสิทธิภาพและมีมาตรฐานในระดับเดียวกัน ให้บริษัทหลักทรัพย์ปฏิบัติตามแนวทางปฏิบัติเกี่ยวกับการควบคุมการปฏิบัติงานและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัทหลักทรัพย์ตามที่สำนักงานกำหนด (guideline)

ในกรณีที่บริษัทหลักทรัพย์ดำเนินการในแนวทางปฏิบัติอื่นที่แตกต่างจากแนวทางที่สำนักงานกำหนด สำนักงานจะพิจารณาว่าบริษัทหลักทรัพย์ได้ปฏิบัติให้เป็นไปตามข้อกำหนดในประกาศนี้ ต่อเมื่อบริษัทหลักทรัพย์สามารถแสดงต่อสำนักงานได้ว่าแนวทางอื่นนั้นสามารถป้องกันความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัทหลักทรัพย์ได้และมีประสิทธิภาพเพียงพอ ตลอดจนอยู่ในมาตรฐานที่ยอมรับได้สำหรับการควบคุมการปฏิบัติงานและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัทหลักทรัพย์

ข้อ 12 ประกาศนี้ให้ใช้บังคับตั้งแต่วันที่ 1 กุมภาพันธ์ พ.ศ. 2548 เป็นต้นไป

ประกาศ ณ วันที่ 20 กรกฎาคม พ.ศ. 2547

(นายธีระชัย ภูวนาถนรานุบาล)
เลขาธิการ
สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์