10 สิงหาคม 2547

เรียน ผู้จัดการ

บริษัทหลักทรัพย์จัดการกองทุนรวมทุกบริษัท

ที่ น.(ว) 26/2547 เรื่อง นำส่งสำเนาประกาศและสรุปข้อเสนอแนะ

ด้วยสำนักงานได้ออกประกาศสำนักงานคณะกรรมการ ก.ล.ต. เกี่ยวกับการควบคุมการปฏิบัติงานและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัทหลักทรัพย์ ซึ่งได้ลงประกาศในราชกิจจานุเบกษา เล่ม 121 ตอนพิเศษ 86ง ลงวันที่ 30 กรกฎาคม 2547 จำนวน 2 ฉบับ ดังนี้

1. ประกาศสำนักงานคณะกรรมการ ก.ล.ต. ที่ สธ./น. 34/2547 เรื่อง การควบคุมการปฏิบัติงานและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัทหลักทรัพย์ ลงวันที่ 20 กรกฎาคม พ.ศ. 2547

2. ประกาศสำนักงานคณะกรรมการ ก.ล.ต. ที่ อธ./น. 5/2547 เรื่อง แนวทางปฏิบัติในการควบคุมการปฏิบัติงานและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัทหลักทรัพย์ ลงวันที่ 20 กรกฎาคม พ.ศ. 2547

จึงขอนำส่งสำเนาประกาศ พร้อมสรุปรายละเอียดข้อเสนอแนะและความเห็นเกี่ยวกับประกาศทั้ง 2 ฉบับมาเพื่อโปรดทราบและถือปฏิบัติ

ขอแสดงความนับถือ

(นางสาวดวงมน ธีระวิคาวี)
ผู้อำนวยการฝ่ายกำกับธุรกิจจัดการลงทุน
เลขาธิการแทน

สิ่งที่ส่งมาด้วย 1. ประกาศสำนักงานคณะกรรมการ ก.ล.ต. ที่ สธ./น. 34/2547 เรื่อง การควบคุมการปฏิบัติงานและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัทหลักทรัพย์ ลงวันที่ 20 กรกฎาคม พ.ศ. 2547
2. ประกาศสำนักงานคณะกรรมการ ก.ล.ต. ที่ อธ./น. 5/2547 เรื่อง แนวทางปฏิบัติในการควบคุมการปฏิบัติงานและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัทหลักทรัพย์ ลงวันที่ 20 กรกฎาคม พ.ศ. 2547
3. สรุปรายละเอียดข้อเสนอแนะและความเห็นฯ

ฝ่ายกำกับธุรกิจจัดการลงทุน
โทร. 0-2252-3223 ต่อ 2734, 2754

สรุปรายละเอียดข้อเสนอแนะและความเห็นจากการ public hearing เกี่ยวกับข้อบังคับและแนวทางปฏิบัติด้านเทคโนโลยีสารสนเทศ				
ข้อบังคับเดิมที่เสนอ		**ข้อเสนอแนะ/คำถาม**	**จากบริษัท**	**ความเห็นสำนักงาน**
	มีผลบังคับใช้ 6 เดือนหลังจากวันที่ออกประกาศ	ขอให้มีผลบังคับใช้ 1 ปี หลังจากวันที่ออกประกาศ	บลจ.อเบอร์ดีน ,บลจ.พรีมา เวสท์, บลจ. ธนชาติ	ระยะเวลา 6 เดือนน่าจะเพียงพอต่อการเตรียมพร้อม จึงเห็นควรให้ข้อบังคับมีผลบังคับใช้ 6 เดือนนับจากวันที่ออกประกาศ

แนวทางปฏิบัติเดิมที่เสนอ		ข้อเสนอแนะ/คำถาม	จากบริษัท	ความเห็นสำนักงาน
นโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ				
<u>การจัดทำนโยบาย</u>	o ต้องจัดทำนโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ ที่เป็นลายลักษณ์อักษร และผู้บริหาร เจ้าหน้าที่ฝ่ายคอมพิวเตอร์และผู้ใช้งานของแต่ละฝ่ายงานต้องมีส่วนร่วมในการจัดทำนโยบาย และอย่างน้อยต้องได้รับอนุมัติจากคณะกรรมการของบริษัท	สามารถใช้นโยบายจากบริษัทแม่ได้หรือไม่	บลจ. อเบอร์ดีน	เพิ่มเติมในแนวทางปฏิบัติว่า “ในกรณีที่บริษัทหลักทรัพย์เป็นบริษัทในเครือของสถาบันการเงินอื่น บริษัทหลักทรัพย์ก็อาจใช้นโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของสถาบันการเงินนั้นได้” และเปลี่ยนข้อความจาก “.....อย่างน้อยต้องได้รับอนุมัติจากคณะกรรมการของบริษัท” เป็น “....อย่างน้อยต้องได้รับอนุมัติจากผู้บริหารบริษัท” โดยขยายความเพิ่ม ว่า “ผู้บริหารบริษัทให้หมายความรวมถึง ผู้บริหารของสถาบันการเงินอื่นที่เป็นบริษัทในเครือด้วย”

แนวทางปฏิบัติเดิมที่เสนอ		ข้อเสนอแนะ/คำถาม	จากบริษัท	ความเห็นสำนักงาน
การปฏิบัติตามนโยบาย	o ต้องมีการตรวจสอบ รวมทั้งประเมินความเพียงพอของนโยบายและระบบควบคุมภายในด้านเทคโนโลยีสารสนเทศโดยหน่วยงานที่เป็นอิสระอย่างน้อยปีละครั้งซึ่งอาจเป็นหน่วยงานตรวจสอบภายในของบริษัทหลักทรัพย์เอง หรือผู้ตรวจสอบภายนอก	ขอแก้ไขจาก mandatory เป็น accredit	IT Club	การตรวจสอบจากหน่วยงานอิสระเป็นสาระสำคัญสำหรับการควบคุมความเสี่ยงของบริษัทและเพื่อให้เป็นไปตามมาตรฐานสากล จึงเห็นควรให้การตรวจสอบโดยหน่วยงานอิสระยังคงเป็น mandatory ตามเดิม
	o ต้องแจ้งสำนักงานทันที เมื่อมีกรณีที่ส่งผลกระทบต่อการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศที่มีนัยสำคัญ	ขอให้ขยายความคำว่า ผลกระทบที่มีนัยสำคัญ	บลจ. ทหารไทย	เพื่อให้เกิดความเข้าใจที่ตรงกัน สำนักงานจึงได้ขยายความคำว่า “ผลกระทบที่มีนัยสำคัญ”ดังนี้ “ผลกระทบต่อการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศที่มีนัยสำคัญ หมายถึง ผลกระทบที่ส่งผลให้บริษัทหลักทรัพย์ไม่สามารถดำเนินงานได้อย่างต่อเนื่อง เช่น ระบบซื้อขายหลักทรัพย์เสียหายไม่สามารถส่งคำสั่งได้ตามปกติ เป็นต้น หรือผลกระทบที่ก่อให้เกิดความเสียหายต่อข้อมูลหรือทรัพย์สินของลูกค้า เช่น ข้อมูลลูกค้าหรือข้อมูลหน่วยลงทุนไม่ถูกต้องเนื่องจากการประมวลผลของระบบคอมพิวเตอร์หรือเนื่องจากการแก้ไขโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง เป็นต้น”
		ขอให้ตัดข้อนี้ออกเนื่องจาก "ผลกระทบที่มีนัยสำคัญ" ยากแก่การตีความ หรือแก้เป็นต้องรายงานให้ผู้บริหารทราบ	IT Club	

แนวทางปฏิบัติเดิมที่เสนอ		ข้อเสนอแนะ/คำถาม	จากบริษัท	ความเห็นสำนักงาน
การควบคุมการเข้าออกศูนย์คอมพิวเตอร์และการป้องกันความเสียหาย (Physical Security)				
การป้องกันความเสียหาย	o ในกรณีที่มีการยกระดับพื้นของศูนย์คอมพิวเตอร์ เพื่อติดตั้งระบบปรับอากาศรวมทั้งเดินสายไฟและสายเครือข่ายด้านล่าง ก็ควรติดตั้งระบบเตือนภัยน้ำรั่วบริเวณที่มีท่อน้ำเพื่อป้องกันหรือระงับเหตุน้ำรั่วได้ทันเวลา นอกจากนี้ หากศูนย์คอมพิวเตอร์ตั้งอยู่ในสถานที่ที่มีความเสี่ยงต่อภัยน้ำรั่ว ก็ควรหมั่นสังเกตว่ามีน้ำรั่วหรือไม่อย่างสม่ำเสมอ	ขอแก้ไขจาก mandatory เป็น accredit	IT Club	เห็นควรตามข้อเสนอจากบริษัท
การรักษาความปลอดภัยข้อมูล ระบบคอมพิวเตอร์ และระบบเครือข่าย				
การบริหารจัดการข้อมูล	o การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (encryption) ที่เป็นมาตรฐานสากล เช่น การใช้ SSL การใช้ VPN เป็นต้น	เสนอทางเลือกให้มีการกำหนดรหัสผ่าน (password) ก่อนส่งข้อมูลเพื่อทดแทนการเข้ารหัส (encryption)	IT Club	การเข้ารหัส (encryption) สำหรับการรับส่งข้อมูลผ่านเครือข่ายสาธารณะนั้น เป็นการแปลงข้อมูลเพื่อป้องกันความลับของข้อมูลรั่วไหลในกรณีที่อาจถูกเข้าถึงระหว่างการรับส่งโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง ซึ่งการกำหนดรหัสผ่าน (password) ก่อนส่งข้อมูลเป็นเพียงการระบุตัวตนของผู้ส่งข้อมูล จึงไม่สามารถป้องกันกรณีดังกล่าวได้ จึงเห็นควรให้คงแนวทางเดิม

แนวทางปฏิบัติเดิมที่เสนอ		ข้อเสนอแนะ/คำถาม	จากบริษัท	ความเห็นสำนักงาน
<u>การควบคุมการใช้งานบัญชีรายชื่อผู้ใช้งาน (user account) และรหัสผ่าน (password)</u>	o ต้องมีระบบตรวจสอบตัวตนจริงและสิทธิการเข้าใช้งานของผู้ใช้งาน (identification and authentication) ก่อนเข้าสู่ระบบงานคอมพิวเตอร์ที่รัดกุมเพียงพอ เช่น กำหนดรหัสผ่านให้ยาก แก่การคาดเดา เป็นต้น และต้องกำหนดให้ผู้ใช้งานแต่ละรายมี user account เป็นของตนเอง ทั้งนี้ การพิจารณาว่าการกำหนดรหัสผ่านมีความยากแก่การคาดเดาและการควบคุมการใช้รหัสผ่านมีความรัดกุมหรือไม่นั้น สำนักงานจะใช้ปัจจัยดังต่อไปนี้ประกอบการพิจารณาในภาพรวม	ระบบมีข้อจำกัดที่ไม่สามารถกำหนดรหัสผ่านได้ตามแนวทางของสำนักงาน จึงควรระบุเพิ่มเติมว่า ให้กำหนดรหัสผ่านตามแนวทางของสำนักงานในข้อที่ระบบสามารถรองรับได้	บลจ. ทหารไทย	สำนักงานเห็นว่าการจะกำหนดให้รหัสผ่านมีความยากแก่การคาดเดาได้อย่างมีประสิทธิภาพนั้น ควรเป็นการกำหนดจากระบบ อย่างไรก็ดี หากระบบมีข้อจำกัดที่ไม่สามารถกำหนดรหัสผ่านได้ตามแนวทางที่สำนักงานกำหนดได้ครบทุกข้อ บริษัทก็อาจกำหนดเป็นนโยบายเพิ่มเติมและควบคุมให้ผู้ใช้งานปฏิบัติตามอย่างเคร่งครัด ทั้งนี้ การพิจารณาการกำหนดรหัสผ่านว่ามีความรอบคอบและ รัดกุมเพียงพอหรือไม่นั้น สำนักงานจะพิจารณาในภาพรวมโดยมิได้พิจารณาเป็นรายข้อ ดังนั้นจึงเห็นควรให้คงแนวทางเดิม
		ระบบมีข้อจำกัดที่ไม่สามารถกำหนดรหัสผ่านได้ตามแนวทางของสำนักงาน จึงขอเสนอให้กำหนดเป็นนโยบายและขอความร่วมมือจากผู้ใช้งาน	บลจ. อเบอร์ดีน	
		เสนอให้แนวทางการกำหนดรหัสผ่านของสำนักงานเป็นเพียงตัวอย่างเท่านั้น	IT Club	

แนวทางปฏิบัติเดิมที่เสนอ		ข้อเสนอแนะ/คำถาม	จากบริษัท	ความเห็นสำนักงาน
	- ควรกำหนดให้รหัสผ่านมีความยาวพอสมควร ซึ่งมาตรฐานสากลโดยส่วนใหญ่แนะนำให้มีความยาวขั้นต่ำ 6 ตัวอักษร	เสนอให้กำหนดความยาวขั้นต่ำเพียง 4ตัวอักษร	บล.กรุงศรีอยุธยา	การกำหนดความยาวขั้นต่ำของรหัสผ่านไว้ 6 ตัวอักษร เป็นไปมาตรฐานสากล จึงเห็นควรให้คงแนวทางเดิม
	- ในการเปลี่ยนรหัสผ่านแต่ละครั้งไม่ควรกำหนดรหัสผ่านใหม่ให้ซ้ำของเดิม	เสนอให้การกำหนดรหัสผ่านไม่ซ้ำกับของเดิมย้อนหลัง 1 ครั้ง	IT Club	เห็นด้วยตามข้อเสนอจากบริษัท
	- ควรกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิด ซึ่งในทางปฏิบัติโดยทั่วไปไม่ควรเกิน 3 ครั้ง	เสนอให้จำนวนครั้งที่ยอมให้ผู้ใช้งาน ใส่รหัสผ่านผิดไม่ควรเกิน 5 ครั้ง	บล.กรุงศรีอยุธยา , IT Club	เห็นด้วยตามข้อเสนอจากบริษัท
<u>การรักษาความปลอดภัยระบบคอมพิวเตอร์แม่ข่าย (Server)</u>	o ต้องดำเนินการติดตั้ง patch ของโปรแกรมระบบ (system software) เช่น ระบบปฏิบัติการ DBMS และ web server เป็นต้น เพื่ออุดช่องโหว่ต่าง ๆ อย่างสม่ำเสมอ	เสนอให้ติดตั้ง patch เฉพาะที่กระทบกับระบบงาน	บลจ.ทหารไทย	เห็นด้วยตามข้อเสนอจากบริษัท

แนวทางปฏิบัติเดิมที่เสนอ		ข้อเสนอแนะ/คำถาม	จากบริษัท	ความเห็นสำนักงาน
การบริหารจัดการและการตรวจสอบระบบเครือข่าย (Network)	o ต้องมีระบบตรวจสอบการบุกรุกและการใช้งานในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยอย่างน้อยต้องมีการตรวจสอบในเรื่องดังต่อไปนี้อย่างสม่ำเสมอ	ขอแก้ไขจาก mandatory เป็น accredit	IT Club	การตรวจสอบการบุกรุกผ่านเครือข่ายเป็นสาระสำคัญในการป้องกันความเสี่ยงด้าน access risk จึงเห็นควรให้เป็น mandatory ตามเดิม
การป้องกันไวรัส และ malicious code	o เครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ของผู้ใช้งานที่เชื่อมต่อกับระบบเครือข่ายทุกเครื่อง ต้องติดตั้งซอฟต์แวร์ป้องกัน ไวรัสที่มีประสิทธิภาพ และปรับปรุงให้เป็นปัจจุบันอยู่เสมอ	เสนอให้แก้ไขเป็น "ต้องมีมาตรการในการป้องกันไวรัส" เนื่องจากการติดตั้งซอฟต์แวร์ป้องกันไวรัสมิได้เป็นวิธีการเดียวในการป้องกันไวรัส	บลจ. ทหารไทย, IT Club	เห็นด้วยตามข้อเสนอจากบริษัท

แนวทางปฏิบัติเดิมที่เสนอ		ข้อเสนอแนะ/คำถาม	จากบริษัท	ความเห็นสำนักงาน
บันทึกเพื่อการตรวจสอบ (audit logs)	o ต้องกำหนดให้มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่าย บันทึกการปฏิบัติงานของผู้ใช้งาน (application logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้าออกระบบ (login-logout logs) บันทึกการพยายามเข้าสู่ระบบ (login attempts) บันทึกการใช้ command line และ firewall log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบ และต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย 6 เดือน	เสนอให้เก็บ log ของระบบ front office ไว้ 5 วัน	บล.กรุงศรีอยุธยา	เพื่อประโยชน์ในการกำกับดูแลของสำนักงาน และเพื่อลดภาระของบริษัท เห็นควรให้บริษัทเก็บบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่าย บันทึกการปฏิบัติงานของผู้ใช้งาน (application logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุกไว้อย่างน้อย 3 เดือน
		เสนอให้เก็บ log ของระบบ back office ไว้ 30 วัน	บล.กรุงศรีอยุธยา	
		เสนอให้เก็บ log ของระบบ (system log) ไว้ 30 วัน	บล.กรุงศรีอยุธยา	
		เสนอให้เก็บ logs ทั้งหมดไว้อย่างน้อย 1 เดือน	IT Club	
		เสนอให้เพิ่มเรื่องการตรวจสอบ log อย่างสม่ำเสมอด้วย	บลจ.ทหารไทย	เห็นด้วยตามข้อเสนอจากบริษัท โดยกำหนดให้เป็น accredit

แนวทางปฏิบัติเดิมที่เสนอ		ข้อเสนอแนะ/คำถาม	จากบริษัท	ความเห็นสำนักงาน
	o ต้องมีระบบป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิการเข้าถึงบันทึกต่างๆ ให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น	ขอเปลี่ยนคำว่า "ระบบ" เป็น "วิธีการ"	IT Club	เห็นด้วยตามข้อเสนอจากบริษัท
		ขอเปลี่ยนจาก mandatory เป็น accredit	IT Club	ระบบป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ เป็นสาระสำคัญในการติดตามและตรวจสอบการปฏิบัติงาน จึงเห็นควรให้เป็น mandatory ตามเดิม

แนวทางปฏิบัติเดิมที่เสนอ		ข้อเสนอแนะ/คำถาม	จากบริษัท	ความเห็นสำนักงาน
การสำรองข้อมูลและระบบคอมพิวเตอร์ และการเตรียมพร้อมกรณีฉุกเฉิน (Backup and IT Continuity Plan)				
การเตรียมพร้อมกรณีฉุกเฉิน	o ต้องมีรายละเอียดของอุปกรณ์ที่จำเป็นต้องใช้ในกรณีฉุกเฉินของแต่ละระบบงาน เช่น รุ่นของเครื่องคอมพิวเตอร์ คุณลักษณะของเครื่องคอมพิวเตอร์ (specification) ค่า configuration และอุปกรณ์เครือข่าย เป็นต้น	ขอแก้ไข เป็น "คุณลักษณะของเครื่องคอมพิวเตอร์ (specification) ขั้นต่ำ"	IT Club	เห็นด้วยตามข้อเสนอจากบริษัท
	o ควรสื่อสารแผนฉุกเฉินให้บุคคลที่เกี่ยวข้องทราบเท่าที่จำเป็น และป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องได้รับทราบ	ขอให้ตัดคำว่า "ป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องได้รับทราบ" ออก	IT Club	เห็นด้วยตามข้อเสนอจากบริษัท