ผลการรับฟังความคิดเห็นจากผู้เกี่ยวข้อง (hearing) ร่างประกาศ

เรื่อง ร่างประกาศหลักเกณฑ์เกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และธุรกิจสัญญาซื้อขายล่วงหน้า

1. การรับฟังความคิดเห็น จำนวน 1 ครั้ง

2. เมื่อวันที่ 21 ธันวาคม 2558 - 19 กุมภาพันธ์ 2559

3. ผู้จัดส่งความคิดเห็น ชมรม IT club สมาคมบริษัทหลักทรัพย์ไทย ซึ่งประกอบไปด้วย
บริษัทหลักทรัพย์ 34 แห่ง และตัวแทนซื้อขายสัญญาซื้อขายล่วงหน้า 2 แห่ง
บริษัทหลักทรัพย์จัดการลงทุน 4 แห่ง
บริษัทหลักทรัพย์นายหน้าซื้อขายหน่วยลงทุน 1 แห่ง
อื่น ๆ 3 แห่ง

4. ที่มา

ด้วยพัฒนาการของเทคโนโลยีสารสนเทศที่เกิดขึ้นอย่างรวดเร็วและมีลักษณะที่เป็นการเปลี่ยนแปลงอย่างรุนแรง (disruptive technology) ได้เข้ามามีบทบาทสำคัญที่สามารถช่วยให้ผู้ประกอบธุรกิจลดต้นทุนการดำเนินงานและเพิ่มประสิทธิภาพการให้บริการแก่ผู้ลงทุนได้ ซึ่งสำนักงานเห็นด้วยและจะมีนโยบายส่งเสริมให้ผู้ประกอบธุรกิจมีการนำเทคโนโลยีใหม่ ๆ มาใช้ในการให้บริการเพื่อเพิ่มความสามารถในการแข่งขันของผู้ประกอบธุรกิจและยกระดับคุณภาพการให้บริการแก่ผู้ลงทุน อย่างไรก็ดี สำนักงานคาดหวังให้ผู้ประกอบธุรกิจให้ความสำคัญกับการพิจารณาความเสี่ยงที่เกี่ยวข้องก่อนที่จะนำเทคโนโลยีใด ๆ มาใช้ เช่น ความเสี่ยงในด้านการรักษาความลับของข้อมูล (confidentiality) การรักษาความครบถ้วนและความถูกต้องของข้อมูล (integrity) และการรักษาสภาพพร้อมใช้งาน (availability) รวมถึงความเสี่ยงจากการกระทำในลักษณะที่เป็นอาชญากรรมทางคอมพิวเตอร์ (cyber crime) ซึ่งอาจส่งผลกระทบเป็นวงกว้าง และกระทบต่อความเชื่อมั่นของผู้ลงทุน ด้วยเหตุผลตามที่กล่าวข้างต้น สำนักงานจึงปรับปรุงหลักเกณฑ์และแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศเพื่อให้ผู้ประกอบธุรกิจมีมาตรการด้านความปลอดภัยของระบบเทคโนโลยีสารสนเทศที่รองรับเทคโนโลยีสารสนเทศใหม่ ๆ ได้อย่างเพียงพอและมีประสิทธิภาพ

5. ประเด็นสำคัญ

ข้อกำหนดที่เกี่ยวข้อง	ความคิดเห็น / คำถาม	ความเห็นสำนักงาน
ประเด็นด้านบทนิยาม		
ผู้ให้บริการภายนอก หมายถึง บุคคลจากภายนอกองค์กรซึ่งผู้ประกอบธุรกิจว่าจ้างเพื่อใช้บริการที่เกี่ยวข้องกับระบบสารสนเทศ (ร่างประกาศแนวปฏิบัติฯ หน้า 5)	*ชมรม IT Club* 1. ผู้ให้บริการภายนอกครอบคลุมถึงหน่วยงานใดบ้าง และจากบทนิยามดังกล่าว หน่วยงานดังต่อไปนี้ถือเป็นผู้ให้บริการภายนอกด้วยหรือไม่ - ตลาดหลักทรัพย์แห่งประเทศไทย - หน่วยงานภายนอกที่บริษัท outsource งานด้าน IT เช่น ระบบ WAN, TELCO, Helpdesk เป็นต้น	ผู้ให้บริการภายนอกตามบทนิยามข้างต้น หมายถึง บุคคลที่มีลักษณะเป็นผู้รับดำเนินการ (outsourcee) ในงานที่เกี่ยวข้องกับการประกอบธุรกิจหลักทรัพย์หรือสัญญาซื้อขายล่วงหน้าของผู้ประกอบธุรกิจตามประกาศคณะกรรมการกำกับตลาดทุน ที่ ทธ. 25/2556 เรื่อง การให้บุคคลอื่นเป็นผู้รับดำเนินการในงานที่เกี่ยวข้องกับการประกอบธุรกิจ โดยผู้ให้บริการภายนอกที่เข้าข่ายเป็นผู้รับดำเนินการจะต้องได้รับว่าจ้างจากผู้ประกอบธุรกิจให้ปฏิบัติงานอย่างต่อเนื่อง มิใช่การจ้างวานเป็นครั้งคราว รวมถึงต้องใช้ดุลพินิจหรือการตัดสินใจในการปฏิบัติงานดังกล่าวแทนผู้ประกอบธุรกิจ ทั้งนี้ ลักษณะงานอื่นใดที่นอกเหนือจากขอบเขตดังกล่าว จะไม่ถือเป็นผู้รับดำเนินการตามข้างต้น เช่น งานพัฒนาซอฟแวร์ งานวางระบบเครือข่าย หรืองานซ่อมบำรุงอุปกรณ์ / ระบบสารสนเทศ เป็นต้น [ระบุเพิ่มใน FAQ] หมายเหตุ : สำนักงานจะพิจารณาปรับปรุงนิยาม “ผู้ให้บริการภายนอก” โดยเปลี่ยนเป็น “ผู้รับดำเนินการ (outsourcee)” หมายถึง บุคคลจากภายนอกองค์กรซึ่งผู้ประกอบธุรกิจว่าจ้างเพื่อให้ปฏิบัติงานอย่างต่อเนื่องและต้องใช้ดุลพินิจหรือการตัดสินใจในการปฏิบัติงานดังกล่าวแทนผู้ประกอบธุรกิจ

ข้อกำหนดที่เกี่ยวข้อง	ความคิดเห็น / คำถาม	ความเห็นสำนักงาน
	ชมรม IT Club 2. ในการบังคับใช้ในบางหัวข้อ เช่น cloud computing นั้น อาจไม่สามารถบังคับได้จริงกับบาง vendor เช่น SETTRADE ต้องทำอย่างไร แนะนำว่าควรมีข้อกำหนดที่เปิดกว้างสำหรับในกรณีลักษณะนี้ เช่น ใส่คำว่า “ถ้าเป็นไปได้” หรือ ระบุ vendor เช่น SETTRADE เป็น exception ไว้ในร่างประกาศแนวปฏิบัติฯ	SETTRADE ให้บริการ internet trading platform - ITP แก่ผู้ประกอบธุรกิจโดยจำแนกได้เป็น 2 รูปแบบ ดังนี้ 1) กรณีที่ผู้ประกอบธุรกิจใช้บริการ ITP ในลักษณะที่ผู้ประกอบธุรกิจยังคงบริหารจัดการคำสั่งซื้อขายหลักทรัพย์ (order - management) รวมถึงคัดกรองคำสั่งซื้อขายไม่เหมาะสม (order - screening) ด้วยตนเอง เช่น ระบบ one-port ในปัจจุบันซึ่งถือเป็นการเช่าใช้ software จาก vendor ตามปกติ และไม่เข้าข่ายเป็นการใช้บริการ cloud computing หรือเป็นการ outsource ระบบงาน IT แต่อย่างใด ผู้ประกอบธุรกิจจะต้องปฏิบัติตามร่างประกาศแนวปฏิบัติฯ ในเรื่อง system acquisition, development and maintenance 2) กรณีที่ผู้ประกอบธุรกิจใช้บริการ ITP ในลักษณะที่ผู้ประกอบธุรกิจได้มอบหมายงานด้านบริหารจัดการคำสั่งซื้อขายหลักทรัพย์ (order management) รวมถึงคัดกรองคำสั่งซื้อขายไม่เหมาะสม (order screening) ให้ SETTRADE เป็นผู้รับดำเนินการแทน (outsourcee) เช่น ระบบ SEOS ในปัจจุบัน ผู้ประกอบธุรกิจจะต้องปฏิบัติตามร่างประกาศแนวปฏิบัติฯ ในเรื่อง supplier relationship หมายเหตุ : สำนักงานจะพิจารณาปรับปรุงชื่อแนวปฏิบัติเรื่อง “การใช้บริการจากผู้ให้บริการภายนอก (supplier relationship)” เป็น “การใช้บริการจากผู้รับดำเนินการ (IT outsourcing)”

ข้อกำหนดที่เกี่ยวข้อง	ความคิดเห็น / คำถาม	ความเห็นสำนักงาน
	ชมรม IT Club 3. ผู้ให้บริการ cloud computing ถือเป็นผู้ให้บริการภายนอกที่ต้องปฏิบัติตามร่างประกาศแนวปฏิบัติฯ ในเรื่อง supplier relationship ด้วยหรือไม่	ผู้ให้บริการ cloud computing ถือเป็นผู้ให้เช่าใช้ software / platform / infrastructure แก่ผู้ประกอบธุรกิจผ่าน internet โดยที่ผู้ประกอบธุรกิจยังคงเป็นผู้ปฏิบัติงานหลักซึ่งต้องใช้ดุลพินิจและการตัดสินใจในระบบงานนั้น จึงไม่ต้องปฏิบัติตามร่างประกาศแนวปฏิบัติฯ ในเรื่อง supplier relationship อย่างไรก็ดี ผู้ประกอบธุรกิจยังคงมีหน้าที่ต้องปฏิบัติตามร่างประกาศแนวปฏิบัติฯ ในเรื่อง cloud computing กรณีที่มีการใช้บริการดังกล่าว [ระบุเพิ่มใน FAQ]
	ชมรม IT Club 4. อยากให้สำนักงานยืนยันและให้คำจำกัดความของคำว่า "ผู้ให้บริการภายนอก" อย่างชัดเจนมากยิ่งขึ้น ว่าในกรณีนี้จะหมายความเฉพาะ Supplier จากภายนอกเท่านั้น เพราะสำหรับโบรกต่างประเทศที่มีการใช้บริการจากทาง Global และ HUB Center ของทางบริษัทฯ เองไม่ควรถือว่าเป็นการใช้บริการจากผู้ให้บริการภายนอกซึ่งต้องปฏิบัติตามหลักเกณฑ์ของสำนักงาน	ผู้ให้บริการภายนอกตามบทนิยามข้างต้น หมายถึง บุคคลที่มีลักษณะเป็นผู้รับดำเนินการ (outsourcee) ในงานที่เกี่ยวข้องกับการประกอบธุรกิจหลักทรัพย์หรือสัญญาซื้อขายล่วงหน้าของผู้ประกอบธุรกิจตามประกาศคณะกรรมการกำกับตลาดทุน ที่ ทธ. 25/2556 ซึ่งครอบคลุมถึงผู้รับดำเนินการจากภายนอกและผู้รับดำเนินการที่เป็นบริษัทในเครือเดียวกันกับผู้ประกอบธุรกิจ และต้องปฏิบัติให้เป็นไปตามร่างประกาศแนวปฏิบัติฯ เรื่อง supplier relationship
“ระบบสารสนเทศที่มีความสำคัญ” หมายถึง ระบบสารสนเทศที่รองรับการปฏิบัติงานที่สำคัญ เช่น ระบบซื้อขาย ระบบปฏิบัติการ back office และระบบจัดการลงทุน เป็นต้น	*ชมรม IT Club* 5. ระบบจัดการลงทุน หมายถึงระบบใด	หมายถึง ระบบ IT ที่เกี่ยวข้องกับธุรกิจจัดการลงทุน (ซึ่งรวมถึง บล. / ธพ. / บ.ประกัน ที่ประกอบธุรกิจ PF) เช่น ระบบรับคำสั่งซื้อขายหน่วยลงทุน ระบบจัดการบัญชีผู้ถือหน่วยลงทุน หรือระบบจัดการลงทุนเพื่อกองทุน เป็นต้น

ข้อกำหนดที่เกี่ยวข้อง	ความคิดเห็น / คำถาม	ความเห็นสำนักงาน
นิยาม “ผู้ใช้งาน”	*ชมรม IT Club* 6. เสนอแนะให้เพิ่มบทนิยามของคำว่า “ผู้ใช้งาน” ให้ชัดเจนว่าหมายรวมถึงลูกค้าหรือไม่ เพื่ออ้างอิงกับหลักเกณฑ์และแนวทางปฏิบัติทั้งฉบับ	“ผู้ใช้งาน” ตามที่ปรากฏในร่างประกาศแนวปฏิบัติฯ หมายถึง พนักงานของผู้ประกอบธุรกิจและบุคลากรภายนอก ที่มีการปฏิบัติงานโดยมีการเข้าถึงข้อมูลลับหรือระบบงานสำคัญภายในองค์กรโดยไม่รวมถึงลูกค้า หมายเหตุ : เพิ่มนิยามดังกล่าวในร่างประกาศแนวปฏิบัติฯ และ FAQ ตามที่เสนอ
ขอบเขตของระบบงานที่ต้องปฏิบัติให้เป็นไปตามร่างประกาศแนวปฏิบัติฯ	*บลน. เวลธ์ เมจิค / ISV* 7. ร่างประกาศแนวปฏิบัติฯ กำหนดขอบเขตในการ implement มากน้อยเพียงใด เช่น จัดทำเฉพาะ data center / service ที่สำคัญ / ทั้งองค์กร เนื่องจากใน ISO27001 กำหนดให้มีการระบุ scope ให้ชัดเจน ก่อนทำการประเมินความเสี่ยง *บลน. เวลธ์ เมจิค* 8. ร่างประกาศแนวปฏิบัติฯ ในแต่ละหัวข้อสามารถเลือกทำได้หรือไม่ เนื่องจากใน ISO27001 สามารถเลือกเฉพาะ control ที่ต้องการนำมาจัดการความเสี่ยงนั้น ๆ หลังจากประเมินความเสี่ยงแล้ว	ร่างประกาศแนวปฏิบัติฯ ครอบคลุมถึง ข้อมูลสารสนเทศและทรัพย์สินสารสนเทศทั้งที่เป็น hardware / software ทั้งหมดที่เกี่ยวข้องกับระบบงานสำคัญ ดังนั้น ผู้ประกอบธุรกิจจึงควรประเมินระบบงานว่ามีระบบใดบ้างที่เข้าข่ายเป็นระบบงานสำคัญให้แล้วเสร็จก่อน จึงจะทราบว่าขอบเขตที่ต้องปฏิบัติให้เป็นไปตามร่างประกาศแนวปฏิบัติฯ ดังกล่าวมีมากน้อยเพียงใด *ระบบงานสำคัญ หมายถึง ระบบงานที่เกี่ยวกับการให้บริการ การทำธุรกรรม หรืองานอื่น ๆ ของผู้ประกอบธุรกิจ ซึ่งหากมีการหยุดชะงักอาจส่งผลกระทบต่อลูกค้า การดำเนินงาน ธุรกิจ ชื่อเสียง ฐานะ และผลการดำเนินงานของผู้ประกอบธุรกิจอย่างมีนัยสำคัญ* [ระบุเพิ่มใน FAQ] กรณีที่ผู้ประกอบธุรกิจประเมินระบบงานสำคัญแล้วพบว่าไม่มีระบบงานที่เกี่ยวข้องตามที่กำหนดในร่างประกาศดังกล่าว เช่น ระบบงานสำคัญของผู้ประกอบธุรกิจไม่ได้มีบุคคลอื่น

ข้อกำหนดที่เกี่ยวข้อง	ความคิดเห็น / คำถาม	ความเห็นสำนักงาน
		เป็นผู้รับดำเนินการ (outsourcee) แทน หรือไม่มีนโยบายให้พนักงานใช้อุปกรณ์เคลื่อนที่ในการเข้าถึงระบบงานสำคัญ หรือเชื่อมต่อ internet ผ่านเครือข่ายขององค์กร ผู้ประกอบธุรกิจอาจพิจารณาไม่ปฏิบัติตามในหัวข้อที่เกี่ยวข้องได้ [ระบุเพิ่มใน FAQ]
1. นโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (information security policy) และการควบคุมการปฏิบัติงานให้เป็นไปตามข้อกำหนด (compliance)		
1.2 การควบคุมการปฏิบัติงานให้เป็นไปตามข้อกำหนด (compliance)		
แนวทางปฏิบัติเพิ่มเติม ข้อ 1 ในการปฏิบัติให้เป็นไปตามข้อกำหนด 7(5) ผู้ประกอบธุรกิจอาจจัดให้มีการตรวจสอบขั้นตอนและการปฏิบัติงานโดยผู้ตรวจสอบที่เป็นหน่วยงานตรวจสอบภายในของผู้ประกอบธุรกิจเองซึ่งเป็นอิสระจากการบริหารจัดการความมั่นคงปลอดภัยของระบบสารสนเทศ หรือผู้ตรวจสอบจากภายนอกก็ได้	*บล. เครดิต สวิส* 9. ในข้อกำหนด 7(5) ทางบริษัทใช้เจ้าหน้าที่ IT จากหน่วยงาน IT Risk ที่อยู่ต่างประเทศซึ่งเป็นอิสระจากหน่วยงานของบริษัทในการตรวจสอบ ขอเสนอให้พิจารณาปรับข้อความในแนวทางปฏิบัติของกรณีดังกล่าว	ผู้ประกอบธุรกิจสามารถกำหนดให้เจ้าหน้าที่จากหน่วยงานดังกล่าวเป็นผู้ตรวจสอบขั้นตอนและการปฏิบัติงานได้ โดยไม่ขัดกับข้อกำหนดในปัจจุบันแต่อย่างใด เนื่องจากหน่วยงานดังกล่าวมีความเป็นอิสระจากหน่วยงาน IT ของผู้ประกอบธุรกิจ
2. การจัดโครงสร้างความมั่นคงปลอดภัยของระบบสารสนเทศ (organization of information security)		
	ชมรม IT Club / บลจ. ทหารไทย 10. แนวทางปฏิบัติลงรายละเอียดที่ต้องลงทุนในระบบจำนวนมาก ควรมีแนวทางที่ใช้การควบคุมทางนโยบายประกอบเป็นทางเลือก	ผู้ประกอบธุรกิจสามารถดำเนินการต่างจากแนวปฏิบัติที่สำนักงานกำหนดได้ หากสามารถพิสูจน์ได้ว่าการดำเนินการดังกล่าวนั้นยังคงอยู่ในหลักการและข้อกำหนดของประกาศที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

ข้อกำหนดที่เกี่ยวข้อง	ความคิดเห็น / คำถาม	ความเห็นสำนักงาน
2.1 การจัดโครงสร้างภายในองค์กร (internal organization)		
แนวทางปฏิบัติเพิ่มเติม ข้อ 1 ผู้ประกอบธุรกิจควรกำหนดให้ผู้บริหารระดับสูงเป็นผู้รับผิดชอบในการปฏิบัติให้เป็นไปตามข้อกำหนด 8(1) และ (2) (หน้า 9)	*ชมรม IT Club / บล. ทรีนีตี้* 11. ขอความชัดเจนเพิ่มเติมของคำว่า “ผู้บริหารระดับสูง”	“ผู้บริหารระดับสูง” ตามที่ปรากฏในร่างประกาศแนวปฏิบัติฯ หมายถึง พนักงานของผู้ประกอบธุรกิจระดับผู้บริหารหน่วยงาน (head of department) ขึ้นไป [ระบุเพิ่มใน FAQ]
2.2 การปฏิบัติงานที่มีการใช้อุปกรณ์เคลื่อนที่ (mobile device) เพื่อเข้าถึงระบบสารสนเทศภายในองค์กร และการปฏิบัติงานจากภายนอกบริษัท (teleworking)		
	ชมรม IT Club / บล. ทรีนีตี้ 12. Mobile Device ควรอยู่ในหัวข้อ Access Control (หากเทียบการจัดหมวดหมู่ของ ISO)	สำนักงานจัดหมวดเรื่องการใช้งาน mobile device และ teleworking ให้อยู่ภายใต้หัวข้อการจัดโครงสร้างความมั่นคงปลอดภัยของระบบ IT ตามมาตรฐานสากล (ISO27001 v.2013) เนื่องจากหัวข้อดังกล่าวมุ่งเน้นให้ผู้ประกอบธุรกิจมีการกำหนดมาตรการควบคุมการปฏิบัติหน้าที่ด้าน IT security สำหรับส่วนงานต่าง ๆ ภายในองค์กร โดยรวมถึงการปฏิบัติงานจากภายนอกองค์กร (teleworking) และการใช้อุปกรณ์เคลื่อนที่ (mobile device) เชื่อมต่อกับระบบงานสำคัญภายในองค์กร หมายเหตุ : สำนักงานจะพิจารณาปรับปรุงคำนิยามของ teleworking ในร่างประกาศและร่างประกาศแนวปฏิบัติฯ เป็น “การปฏิบัติงานโดยเชื่อมต่อกับเครือข่ายภายนอกบริษัท”
	ชมรม IT Club / บล. ทรีนีตี้ 13. ในหัวข้อ mobile device และ teleworking ครอบคลุมเฉพาะพนักงานของบริษัทฯ อย่างเดียวหรือผู้ให้บริการภายนอก (vendor) ด้วย เพราะหากครอบคลุมถึงผู้ให้บริการภายนอก (vendor) บริษัทอาจไม่สามารถปฏิบัติได้ทุกข้อ เช่น การลงเฉพาะ software ที่มีลิขสิทธิ์	หัวข้อดังกล่าวครอบคลุมถึงบุคลากรของผู้ให้บริการภายนอก (vendor) ที่มีการปฏิบัติงานโดยมีการเข้าถึงข้อมูลลับหรือระบบงานสำคัญภายในองค์กรด้วย อย่างไรก็ดี หากผู้ประกอบธุรกิจมีการสื่อสารนโยบายและแนวทางปฏิบัติด้านการรักษาความมั่นคง

ข้อกำหนดที่เกี่ยวข้อง	ความคิดเห็น / คำถาม	ความเห็นสำนักงาน
	การ update patch เป็นต้น หรือในการที่ vendor เข้ามา support ผ่าน teleworking บริษัทอาจไม่สามารถไปตรวจสอบได้ว่าเครื่องมือหรืออุปกรณ์ที่เชื่อมต่อนั้นมีความปลอดภัยเพียงใด	ปลอดภัยของระบบ IT ให้แก่บุคลากรดังกล่าวทราบ เช่น การสื่อสารผ่าน e-mail หรือแสดงข้อความ pop-up เมื่อใช้งานระบบ รวมถึงจัดให้มีการติดตามตรวจสอบการใช้งานระบบ / การเข้าถึงข้อมูลของบุคลากรดังกล่าวขณะที่มีการเชื่อมต่อผ่านเครือข่ายของผู้ประกอบธุรกิจอย่างเหมาะสมรัดกุมแล้ว ให้ถือว่าผู้ประกอบธุรกิจได้ปฏิบัติให้เป็นไปตามหลักเกณฑ์ของข้อกำหนดในส่วนนี้แล้ว [ระบุเพิ่มใน FAQ]
	ชมรม IT Club / ISV 14. ในการปฏิบัติงานที่มีการใช้ mobile device จะต้องกำหนดให้มีการลงทะเบียนอุปกรณ์ เช่น ยี่ห้อ, รุ่น , OS , Serial Number , MAC Address ขอสอบถามเพิ่มเติมว่า การลงทะเบียนนั้นใช้เฉพาะกับพนักงานของบริษัทที่นำอุปกรณ์มาใช้ หรือว่ารวมไปถึงลูกค้าและ Supplier ด้วย	ในการลงทะเบียนอุปกรณ์นั้นให้รวมถึงเฉพาะพนักงานของผู้ประกอบธุรกิจและบุคลากรภายนอกที่มีการปฏิบัติงานโดยมีการเข้าถึงข้อมูลลับหรือระบบงานสำคัญภายในองค์กรโดยผ่านการเชื่อมต่อกับเครือข่ายคอมพิวเตอร์ภายในองค์กรเท่านั้น สำหรับในส่วนของลูกค้า ผู้ประกอบธุรกิจควรจัดให้มีการลงทะเบียนผู้ใช้งาน internet ทุกรายที่เชื่อมต่อผ่านเครือข่ายของผู้ประกอบธุรกิจด้วยวิธีการที่เหมาะสมและสอดคล้องกับวัตถุประสงค์ของการปฏิบัติให้เป็นไปตามร่างประกาศแนวปฏิบัติฯ ในหัวข้อ 8.4 เรื่อง logging and monitoring ซึ่งกำหนดให้ผู้ประกอบธุรกิจจัดเก็บ internet access log โดยมีรายละเอียดขั้นต่ำคือ บัญชีผู้ใช้งาน / หมายเลขประจำเครื่องที่ใช้งาน (IP address) / หมายเลข internet ของผู้ประกอบธุรกิจ (organization IP address) / วันเวลาที่มีการใช้งาน / ที่อยู่ของเว็บไซต์ปลายทาง (full URL) เพื่อให้ผู้ประกอบธุรกิจสามารถยืนยันตัวตนของบุคคลผู้ใช้งาน internet ผ่านเครือข่ายของผู้ประกอบธุรกิจได้อย่างถูกต้องและเป็นประโยชน์ในการติดตามตรวจสอบและป้องกันการใช้งาน

ข้อกำหนดที่เกี่ยวข้อง	ความคิดเห็น / คำถาม	ความเห็นสำนักงาน
		ระบบสารสนเทศที่มีความผิดปกติหรือไม่เป็นไปตามกฎหมายหรือกฎเกณฑ์ที่เกี่ยวข้องต่อไป [ระบุเพิ่มใน FAQ]
<u>แนวทางปฏิบัติเพิ่มเติม</u> ข้อ 1 ในการปฏิบัติงานที่มีการใช้อุปกรณ์เคลื่อนที่เพื่อเข้าถึงระบบงานภายในองค์กร (ไม่รวมถึงระบบ mail service) ผู้ประกอบธุรกิจควรจัดให้มีมาตรการป้องกันข้อมูลสารสนเทศที่สำคัญตามข้อกำหนด 7(6) โดยพิจารณาถึงแนวทางดังต่อไปนี้	*ชมรม IT Club* 15. กรณีอุปกรณ์สูญหาย เป็นการยากหากต้องดำเนินการลบข้อมูลจากระยะไกล หากบริษัทมีการควบคุมเรื่องของรหัสผ่านในการเข้าเครื่องและการ Lock Screen จะสามารถทดแทนการลบข้อมูลได้หรือไม่	เพื่อป้องกันข้อมูลที่เป็นความลับหรือมีความสำคัญสูงซึ่งถูกจัดเก็บในอุปกรณ์เคลื่อนที่จากการถูกเข้าถึงโดยไม่ได้รับอนุญาต ผู้ประกอบธุรกิจควรจัดให้มีการเข้ารหัสข้อมูล (data encryption) หรือเข้ารหัสไดรฟ์ข้อมูลเพิ่มเติมสำหรับกรณีที่ไม่สามารถทำ remote wipe-out ได้ [ระบุเพิ่มใน FAQ]
(2) มีมาตรการป้องกันข้อมูลที่เป็นความลับหรือมีความสำคัญ (sensitive data) กรณีที่อุปกรณ์เคลื่อนที่สูญหาย เช่น การกำหนดให้ใส่รหัสผ่านก่อนใช้งานอุปกรณ์ (lock screen) หรือการลบข้อมูลจากระยะไกล (remote wipe-out) เป็นต้น (หน้า 10)	*ชมรม IT Club* 16. ในส่วนนี้ไม่จำเป็นสำหรับเครื่อง PC ใช่หรือไม่	ข้อกำหนดในส่วนนี้ใช้บังคับเฉพาะกับอุปกรณ์เคลื่อนที่เท่านั้น อย่างไรก็ดี ผู้ประกอบธุรกิจยังคงมีหน้าที่จัดให้มีการเข้ารหัสข้อมูลสำคัญซึ่งถูกจัดเก็บในเครื่อง PC ตามที่กำหนดในร่างประกาศแนวปฏิบัติฯ เรื่อง cryptographic control
(4) จัดให้มีการเข้ารหัสข้อมูลสารสนเทศที่สำคัญทั้งที่จัดเก็บในอุปกรณ์เคลื่อนที่และที่รับส่งผ่านระบบเครือข่ายคอมพิวเตอร์ (หน้า 11)	*บลจ. อเบอร์ดีน* 17. หากบริษัทใช้งาน secure mobile platform เช่น Good Dynamics ซึ่งสามารถควบคุมความเสี่ยงที่อาจเกิดขึ้นจากการใช้งาน mobile device ได้อย่างเหมาะสมมากกว่า สามารถปฏิบัติได้หรือไม่	ข้อกำหนดดังกล่าวเป็นเพียงมาตรการขั้นต่ำเพื่อป้องกันข้อมูลที่มีความสำคัญหรือเป็นความลับจากความเสียหายหรือถูกบุกรุก หากผู้ประกอบธุรกิจมีกระบวนการอื่นใดที่มีประสิทธิภาพดีกว่าในการป้องกันความเสี่ยงตามข้างต้น ก็สามารถปฏิบัติได้
(6) ควบคุมให้มีการติดตั้งเฉพาะซอฟต์แวร์ที่ถูกต้องตามลิขสิทธิ์ และโปรแกรมเพื่อปิดช่องโหว่ (patches) ที่เหมาะสม และกำหนดมาตรการป้องกันโปรแกรมไม่ประสงค์ดี (malware) ทั้งนี้ เพื่อป้องกันการบุกรุกหรือก่อให้เกิดความเสียหายต่อข้อมูลที่เป็นความลับและมีความสำคัญที่จัดเก็บในอุปกรณ์เคลื่อนที่ (หน้า 11)		

ข้อกำหนดที่เกี่ยวข้อง	ความคิดเห็น / คำถาม	ความเห็นสำนักงาน
ข้อ 2 ในกรณีที่มีการปฏิบัติงานจากภายนอกบริษัท (teleworking) ผู้ประกอบธุรกิจควรกำหนดมาตรการรักษาความมั่นคงปลอดภัยที่รัดกุมเพียงพอสำหรับข้อมูลสารสนเทศที่ถูกเข้าถึง ประมวลผล และจัดเก็บในพื้นที่ปฏิบัติงานตามข้อกำหนด 7(6) โดยพิจารณาถึง		
(1) การกำหนดมาตรการรักษาความมั่นคงปลอดภัยด้านกายภาพที่เหมาะสมรัดกุมเพียงพอกับขอบเขตการปฏิบัติงานสำหรับพื้นที่ปฏิบัติงานนอกองค์กร (หน้า 11)	*ชมรม IT Club* 18. เป็นเรื่องที่ตรวจสอบได้ยาก เช่น กรณีพนักงานหรือ vendor ทำการ remote เข้ามาเพื่อแก้ไขปัญหา บริษัทไม่สามารถรู้ได้ว่าพนักงานดำเนินการจากสถานที่ใด	หากผู้ประกอบธุรกิจมีการสื่อสารนโยบายและแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยของระบบ IT ให้แก่บุคลากรดังกล่าวทราบ เช่น การสื่อสารผ่าน e-mail หรือแสดงข้อความ pop-up เมื่อเข้าใช้งานระบบ รวมถึงจัดให้มีการตรวจสอบการใช้งานระบบ / การเข้าถึงข้อมูลของบุคลากรดังกล่าวขณะที่มีการเชื่อมต่อผ่านเครือข่ายของผู้ประกอบธุรกิจอย่างเหมาะสมรัดกุมแล้ว จะถือว่าผู้ประกอบธุรกิจได้ปฏิบัติตามหลักเกณฑ์ของข้อกำหนดในส่วนนี้แล้ว ทั้งนี้ รายละเอียดเกี่ยวกับข้อกำหนดดังกล่าวสามารถศึกษาเพิ่มเติมได้จาก FAQ ข้อ 3.6 [ระบุเพิ่มใน FAQ]
(2) การควบคุมสิทธิการใช้งานและการเข้าถึงข้อมูลสารสนเทศของผู้ใช้งานอย่างเหมาะสม (หน้า 11)	*ชมรม IT Club* 19. “ผู้ใช้งาน” ในที่นี้หมายถึงพนักงาน หรือ vendor	อ้างอิงคำตอบตามข้อ 6
(5) การป้องกันการเข้าถึงข้อมูลสารสนเทศจากบุคคลที่ไม่มีสิทธิในการใช้งาน เช่น ญาติพี่น้องและเพื่อน เป็นต้น (หน้า 11)	*ชมรม IT Club* 20. ขอความชัดเจนเพิ่มเติมถึงข้อกำหนดนี้ เนื่องจากอาจไม่สามารถทำได้ในทางปฏิบัติ เนื่องจากบริษัทไม่สามารถควบคุมบุคคลภายนอกได้	อ้างอิงคำตอบตามข้อ 18 และ FAQ ข้อ 3.3

ข้อกำหนดที่เกี่ยวข้อง	ความคิดเห็น / คำถาม	ความเห็นสำนักงาน
2.3 การใช้บริการ cloud computing		
	ชมรม IT Club 21. ในการใช้บริการ cloud computing ให้เป็นไปตามหลักเกณฑ์ที่สำนักงานกำหนดนั้น บริษัทจะต้องมีการจัดทำนโยบายและมาตรการในการรักษาความมั่นคงปลอดภัย ข้อกำหนดเกี่ยวกับการใช้งาน รวมถึงต้องปรับปรุงแก้ไขการปฏิบัติงานและการติดตามควบคุมดูแลการใช้บริการ cloud computing ซึ่งต้องใช้ระยะเวลาในการดำเนินการเพื่อให้ครอบคลุมและสอดคล้องตามหลักเกณฑ์ให้ครบถ้วน จึงขอให้สำนักงานโปรดพิจารณาทบทวนขยายระยะเวลาจากการบังคับใช้ออกไปอีก	อ้างอิงคำตอบในหมวด “การมีผลใช้บังคับ”
ข้อ 3 ในกรณีที่ใช้บริการ cloud computing กับระบบสารสนเทศที่มีความสำคัญ ผู้ประกอบธุรกิจควรจัดให้มีข้อกำหนดเกี่ยวกับการใช้งาน โดยขั้นต่ำควรมีรายละเอียดดังนี้ (5) กำหนดการทบทวนคุณสมบัติของผู้ให้บริการอย่างสม่ำเสมอ เช่น ฐานะทางการเงิน ความเพียงพอของการให้บริการ (capacity planning) เพื่อให้มั่นใจว่าผู้ให้บริการยังคงมีความพร้อมในการให้บริการที่เพียงพอต่อความต้องการของผู้ประกอบธุรกิจอย่างต่อเนื่อง (หน้า 13)	*ชมรม IT Club / บลจ. โซลาริส* 22. ในการตรวจสอบผู้ให้บริการ cloud computing นั้น ข้อมูลบางอย่างที่กำหนดไว้ เช่น ฐานะทางการเงิน, มาตรฐานความปลอดภัยด้านเครือข่าย, ISO, Capacity หรืออื่น ๆ ถ้าผู้ให้บริการไม่ได้เปิดเผยหรือบริษัทไม่สามารถที่จะตรวจสอบได้ เช่น SETTRADE / Microsoft ต้องทำอย่างไร	ผู้ประกอบธุรกิจอาจใช้ข้อมูลจากแหล่งอื่นทดแทน เช่น ข้อมูลรายชื่อบริษัทที่ผ่านการรับรองมาตรฐาน ISO จากเว็บไซต์ของผู้ให้บริการรับรองมาตรฐานดังกล่าว หรือข้อมูลฐานะทางการเงินจากผู้ให้บริการข้อมูลด้านธุรกิจ เป็นต้น นอกจากนี้ ผู้ประกอบธุรกิจอาจใช้กระบวนการอื่นร่วมกับข้อมูลที่มีอยู่ประกอบการพิจารณาทบทวนคุณสมบัติของผู้ให้บริการ เพื่อให้มั่นใจได้ว่าผู้ให้บริการของตนมีระบบการรักษาความมั่นคงปลอดภัยของข้อมูลอย่างเพียงพอ รวมถึงมีศักยภาพและความพร้อมในการให้บริการได้อย่างต่อเนื่อง [ระบุเพิ่มใน FAQ]

ข้อกำหนดที่เกี่ยวข้อง	ความคิดเห็น / คำถาม	ความเห็นสำนักงาน
	ชมรม IT Club 23. คำว่าสม่ำเสมอตามที่กำหนดในร่างประกาศแนวปฏิบัติฯ นั้น เฉพาะในขั้นตอนการจัดซื้อจัดจ้าง หรือขั้นตอนการประเมิน vendor เพียงพอแล้วหรือไม่ ถ้าไม่เพียงพอ ความถี่ในการตรวจสอบต้องเป็นอย่างไร	ผู้ประกอบธุรกิจควรกำหนดให้นโยบายการใช้งาน cloud computing ครอบคลุมถึงขั้นตอนและระยะเวลาในการทบทวนคุณสมบัติของผู้ให้บริการตามที่เห็นสมควรและเหมาะสมกับลักษณะการประกอบธุรกิจของตน เพื่อให้มั่นใจได้ว่าผู้ให้บริการของตนยังคงมีคุณสมบัติตามที่ผู้ประกอบธุรกิจได้ประเมินไว้ตั้งแต่ต้น และยังคงมีศักยภาพที่จะให้บริการได้อย่างต่อเนื่อง [ระบุเพิ่มใน FAQ]
	ชมรม IT Club 24. ขอคำแนะนำเกี่ยวกับการตรวจสอบฐานะทางการเงินที่เพียงพอของผู้ให้บริการ	ผู้ประกอบธุรกิจอาจพิจารณาได้จากมูลค่าส่วนของผู้ถือหุ้น กำไรสุทธิจากการดำเนินงาน หรือความสามารถในการชำระหนี้ของผู้ให้บริการ เป็นต้น ทั้งนี้ ความเพียงพอในด้านฐานะทางการเงินของผู้ให้บริการนั้น ให้เป็นตามที่ผู้ประกอบธุรกิจเห็นสมควร [ระบุเพิ่มใน FAQ]
3. การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร (human resource security)		
ข้อกำหนดในประกาศที่ สธ. xx/2559 ข้อ 11 ผู้ประกอบธุรกิจต้องสร้างความตระหนักรู้เกี่ยวกับนโยบายและมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศให้แก่บุคลากรของผู้ประกอบธุรกิจและบุคคลภายนอก (human resource security) ที่มีการปฏิบัติงานโดยมีการเข้าถึงข้อมูลหรือระบบงานภายในองค์กร และดำเนินการให้บุคลากรดังกล่าวสามารถปฏิบัติหน้าที่ได้ตามนโยบายและมาตรการที่กำหนด ทั้งนี้ ตามหลักเกณฑ์ดังต่อไปนี้		

ข้อกำหนดที่เกี่ยวข้อง	ความคิดเห็น / คำถาม	ความเห็นสำนักงาน
(1) ให้ความรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศที่เกี่ยวข้องกับการปฏิบัติหน้าที่แก่บุคลากรของผู้ประกอบธุรกิจและบุคคลภายนอกที่ปฏิบัติงานดังกล่าว (2) สื่อสารให้บุคลากรของผู้ประกอบธุรกิจและบุคคลภายนอกที่ปฏิบัติงานดังกล่าว ระมัดระวังและงดเว้นการใช้งานระบบสารสนเทศในลักษณะที่อาจก่อให้เกิดความเสียหายแก่ผู้ประกอบธุรกิจหรือตลาดทุนโดยรวม หรือกระทบต่อความมั่นคงของประเทศ และต้องรายงานผู้มีหน้าที่รับผิดชอบในการบริหารจัดการเหตุการณ์ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศโดยไม่ชักช้าเมื่อพบความผิดปกติใด ๆ อย่างมีนัยสำคัญ (หน้า 16)	*ชมรม IT Club* 25. ติดประเด็นเรื่องบุคคลภายนอกซึ่งเป็นการยากที่พนักงาน outsource จะมีความตระหนักเรื่องของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ซึ่งในกรณีนี้ ทางบริษัททำได้เพียงการติดตามกับบริษัทต้นสังกัดของเจ้าหน้าที่ภายนอกที่มาดำเนินการเท่านั้น การดำเนินการดังกล่าวถือว่าได้มีการครอบคลุมตามเกณฑ์ข้อนี้หรือไม่	หากผู้ประกอบธุรกิจมีการสื่อสารนโยบายและแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยของระบบ IT ให้แก่บุคลากรดังกล่าวทราบ เช่น การสื่อสารผ่าน e-mail หรือแสดงข้อความ pop-up เมื่อเข้าใช้งานระบบ โดยกำหนดวิธีให้บุคคลภายนอกดังกล่าวลงนามรับทราบนโยบายและแนวทางปฏิบัติด้วย จะถือว่า ผู้ประกอบธุรกิจได้ปฏิบัติตามหลักเกณฑ์ของข้อกำหนดในส่วนนี้แล้ว [อ้างอิง FAQ ข้อ 5.2]
5. การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ (access control)		
5.4 การควบคุมการเข้าถึงระบบสารสนเทศและโปรแกรมประยุกต์ (system and application access control)		
แนวทางปฏิบัติเพิ่มเติม ข้อ 1 ตัวอย่างของการควบคุมการเข้าใช้งานระบบสารสนเทศและโปรแกรมประยุกต์ตามข้อกำหนด 18(3)(ข) เช่น มีการป้องกันการเข้าใช้งานโดยวิธีเดาสุ่ม (brute force) แจ้งเตือนกรณีที่มีความพยายามเข้าใช้งานอย่างไม่เหมาะสม (breach of log-on control) และจัดเก็บหลักฐานดังกล่าว เป็นต้น (หน้า 21)	*ชมรม IT Club / บล. ทรีนีตี้* 26. ตัวอย่างตามข้อ 1 นี้ ถือเป็นการกำหนดให้ดำเนินการหรือไม่ และหากบริษัทมีการตรวจสอบเรื่องความพยายามในการเข้าใช้งานทุกสิ้นวันเป็นประจำ ไม่ต้องจัดให้มีระบบแจ้งเตือนแบบ real-time ได้หรือไม่	ผู้ประกอบธุรกิจควรดำเนินการขั้นต่ำในส่วนนี้โดยจัดให้มีการป้องกันการเข้าใช้งานโดยวิธีเดาสุ่ม (brute force) รวมถึงมีการจัดเก็บและตรวจสอบ log-in attempt log อย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่าระบบสารเทศและโปรแกรมประยุกต์จะไม่ถูกเข้าถึงโดยไม่ได้รับอนุญาต ทั้งนี้ สำนักงานรับไปปรับปรุงแนวทางปฏิบัติข้อดังกล่าวเพื่อป้องกันความสับสนในประเด็นการแจ้งเตือนกรณีที่มีความพยายามเข้าใช้งานอย่างไม่เหมาะสมแบบ real-time

ข้อกำหนดที่เกี่ยวข้อง	ความคิดเห็น / คำถาม	ความเห็นสำนักงาน
		หมายเหตุ : สำนักงานจะพิจารณาปรับปรุงเนื้อหาแนวทางปฏิบัติเพิ่มเติมข้อ 1 เป็นดังนี้ “ตัวอย่างของการควบคุมการเข้าใช้งานระบบสารสนเทศและโปรแกรมประยุกต์ตามข้อกำหนด 18(3)(ข) เช่น มีการป้องกันการเข้าใช้งานโดยวิธีเดาสุ่ม (brute force) ~~แจ้งเตือนกรณีที่มีความพยายามเข้าใช้งานอย่างไม่เหมาะสม (breach of log-on control) และจัดเก็บหลักฐานดังกล่าว~~ จัดเก็บและตรวจสอบ log-in attempt log อย่างสม่ำเสมอ เป็นต้น”
ข้อ 2 การปฏิบัติให้เป็นไปตามข้อกำหนด 18(3)(ค) ผู้ประกอบธุรกิจควรพิจารณากำหนดกระบวนการที่จำเป็นดังนี้ (4) กำหนดให้ผู้ใช้งานเปลี่ยนแปลงรหัสผ่านทันทีที่ได้รับรหัสผ่านครั้งแรก และควรเปลี่ยนรหัสผ่านอย่างน้อยทุก 6 เดือน (หน้า 21) (9) ควรมีวิธีการจัดส่งรหัสผ่านให้แก่ผู้ใช้งานอย่างรัดกุมและปลอดภัย เช่น การใส่ซองปิดผนึก เป็นต้น (หน้า 22)	*ชมรม IT Club* 27. ข้อกำหนดนี้หมายรวมถึงผู้ใช้งานที่เป็นลูกค้าหรือไม่ *บลจ. อเบอร์ดีน* 28. บริษัทสามารถใช้วิธีการแจ้งรหัสผ่านให้แก่ผู้ใช้งานทางวาจา / e-mail / ช่องทางอื่น ๆ ที่นอกเหนือจากการใส่ซองปิดผนึกได้หรือไม่ เนื่องจากบริษัทกำหนดให้มีการสร้างรหัสผ่านแบบสุ่มในทุกบัญชี / พนักงานทุกคนต้องเปลี่ยนรหัสผ่านในการ log-in ครั้งแรก / รหัสที่กำหนดขึ้นมาใหม่มีความยากในการคาดเดาสูง	ข้อกำหนดนี้ไม่รวมถึงลูกค้า ผู้ประกอบธุรกิจควรเลือกใช้วิธีจัดส่งรหัสผ่านที่มีเพียงผู้ใช้งานเท่านั้นที่จะทราบ เช่น การจัดส่งด้วย e-mail พร้อมแนบไฟล์ข้อมูลรหัสผ่านของผู้ใช้งานซึ่งถูกเข้ารหัสที่มีความยากในการคาดเดา เป็นต้น อย่างไรก็ดี การแจ้งรหัสผ่านด้วยวาจาต่อผู้ใช้งานโดยตรง ผู้ประกอบธุรกิจควรระมัดระวังมิให้ผู้อื่นล่วงรู้ข้อมูลดังกล่าว

ข้อกำหนดที่เกี่ยวข้อง	ความคิดเห็น / คำถาม	ความเห็นสำนักงาน
6. การควบคุมการเข้ารหัสข้อมูล (cryptographic control) (หน้า 23)		
	ชมรม IT Club 29. ขอให้สำนักงานพิจารณากำหนดความชัดเจนของประเภทข้อมูลที่เป็นความลับหรือมีความสำคัญเฉพาะข้อมูลในระดับที่มีความสำคัญสูง พร้อมยกตัวอย่างประเภทของข้อมูลที่ควรมีการควบคุมโดยการเข้ารหัสข้อมูล เพื่อเป็นแนวทางปฏิบัติที่เป็นมาตรฐานเดียวกัน	ผู้ประกอบธุรกิจควรดำเนินการจัดชั้นความลับของข้อมูลตามที่กำหนดในร่างประกาศแนวปฏิบัติฯ หัวข้อ 4.2 เรื่อง asset classification ให้แล้วเสร็จก่อน จึงจะทราบว่าข้อมูลใดบ้างที่ควรได้รับการปกป้องด้วยการเข้ารหัสข้อมูล ทั้งนี้ การจัดชั้นความลับของข้อมูลควรยึดหลักผลกระทบที่เกิดขึ้นต่อลูกค้า การดำเนินธุรกิจ ชื่อเสียง ฐานะและผลการดำเนินงานของผู้ประกอบธุรกิจ หากข้อมูลดังกล่าวมีการรั่วไหล เช่น ข้อมูลการซื้อขาย / ข้อมูลการถือครองหลักทรัพย์ของลูกค้า [ระบุเพิ่มใน FAQ]
	ชมรม IT Club 30. ขอให้ระบุขอบเขตของการ encrypt data ทั้งนี้ ต้องทำในระดับ database ด้วยหรือไม่	ร่างประกาศแนวปฏิบัติฯ ไม่มีข้อกำหนดให้ผู้ประกอบธุรกิจต้องเข้ารหัสในระดับ database อย่างไรก็ดี เพื่อเป็นการป้องกันการเข้าถึงข้อมูลที่ถูกจัดเก็บใน database โดยไม่ได้รับอนุญาต ผู้ประกอบธุรกิจควรดำเนินการดังนี้ 1) เข้ารหัสข้อมูลที่เกี่ยวกับบัญชีผู้ใช้งานและรหัสผ่านของผู้บริหารระบบฐานข้อมูล (database admin) 2) เข้ารหัสฮาร์ดดิสก์ (full disk encryption) หรือพิจารณาใช้เทคโนโลยีอื่นใดที่ทำให้ไม่สามารถเรียกดูข้อมูลจากฮาร์ดดิสก์นั้นได้เมื่อนำไปต่อพ่วงกับเครื่องคอมพิวเตอร์อื่น [ระบุเพิ่มใน FAQ]

ข้อกำหนดที่เกี่ยวข้อง	ความคิดเห็น / คำถาม	ความเห็นสำนักงาน
	ชมรม IT Club 31. การ encrypt data รวมถึงการสื่อสารภายในองค์กรด้วยหรือไม่ และขอบเขตของการทำอยู่ในระดับใด เช่น client to server, server to server เป็นต้น ซึ่งหากรวมถึงภายในองค์กรด้วย อาจจะส่งผลกระทบถึง performance ของระบบ	ร่างประกาศแนวปฏิบัติฯ ไม่มีข้อกำหนดให้ผู้ประกอบธุรกิจต้องเข้ารหัสข้อมูลการสื่อสารภายในองค์กรทั้งหมด อย่างไรก็ดี ในกรณีที่เป็นการสื่อสารข้อมูลที่เป็นความลับหรือมีความสำคัญ ผู้ประกอบธุรกิจควรกำหนดให้มีการเข้ารหัสข้อมูลหรือมีมาตรการอื่นใดเพื่อป้องกันการเข้าถึงข้อมูลดังกล่าวโดยไม่ได้รับอนุญาต เช่น กำหนดให้มีการเข้ารหัสผ่านสำหรับไฟล์ข้อมูลแนบ (attached file) ซึ่งเป็นความลับหรือมีความสำคัญทุกครั้งก่อนจัดส่งผ่าน e-mail เป็นต้น [ระบุเพิ่มใน FAQ]
	ISV 32. ขอทราบกรอบมาตรฐานการ encryption data ขั้นต่ำของสำนักงาน	ผู้ประกอบธุรกิจควรจัดให้มีการเข้ารหัสข้อมูลด้วยวิธีการ (encryption algorithm) ที่สอดคล้องเหมาะสมกับระดับความเสี่ยงที่อาจเกิดขึ้นกับข้อมูลที่เป็นความลับหรือมีความสำคัญ รวมถึงเป็นไปตามมาตรฐานหรือ best practice ในปัจจุบัน [ระบุเพิ่มใน FAQ]
7. การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม (physical and environmental security)		
7.1 พื้นที่หวงห้าม (secure areas)		
<u>แนวทางปฏิบัติเพิ่มเติม</u> ข้อ 2 ผู้ประกอบธุรกิจควรกำหนดสิทธิการเข้าออกพื้นที่หวงห้ามให้เฉพาะบุคคลที่มีหน้าที่เกี่ยวข้องภายใต้หลักความจำเป็นในการรู้ข้อมูล (need-to-know basis) รวมทั้งควรจัดให้มีระบบการควบคุมการเข้าออกอย่างรัดกุม และทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ	*ชมรม IT Club* 33. กรณีพนักงานจากฝ่ายอื่นซึ่งมีหน้าที่ร่วมดูแลรับผิดชอบศูนย์คอมพิวเตอร์ เช่น ระบบไฟฟ้า ระบบเครื่องปรับอากาศ ควรอนุญาตให้เข้าถึงศูนย์คอมพิวเตอร์ได้	หลักการในร่างประกาศแนวปฏิบัติฯ เรื่อง secure areas ถือว่าบุคลากรซึ่งมีหน้าที่ดูแลรักษาอุปกรณ์ให้อยู่ในสภาพที่พร้อมใช้เป็นบุคลากรที่เกี่ยวข้องและสามารถเข้าออกศูนย์คอมพิวเตอร์ได้ตามความจำเป็น ทั้งนี้ ผู้ประกอบธุรกิจควรมีการติดตามและควบคุมบุคลากรดังกล่าวที่เข้าปฏิบัติงานภายในพื้นที่หวงห้ามอย่างรัดกุมเหมาะสม

ข้อกำหนดที่เกี่ยวข้อง	ความคิดเห็น / คำถาม	ความเห็นสำนักงาน
		หมายเหตุ : สำนักงานจะพิจารณาปรับปรุงเนื้อหาแนวทางปฏิบัติเพิ่มเติม ข้อ 2 เป็นดังนี้ “ผู้ประกอบธุรกิจควรกำหนดสิทธิการเข้าออกพื้นที่หวงห้ามให้เฉพาะบุคคลที่มีหน้าที่เกี่ยวข้อง~~ภายใต้หลักความจำเป็นในการรู้ข้อมูล (need-to-know basis)~~ รวมทั้งควรจัดให้มีระบบการควบคุมการเข้าออกอย่างรัดกุม และทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ”
แนวทางปฏิบัติเพิ่มเติม ข้อ 5 ผู้ประกอบธุรกิจควรแยกพื้นที่จุดรับส่งของ (delivery and loading area) ซึ่งเป็นพื้นที่ส่วนที่ต้องมีการเข้าถึงโดยพนักงานฝ่ายอื่น เช่น ส่วนที่ใช้เก็บรายงานที่ฝ่ายคอมพิวเตอร์ได้จัดพิมพ์ให้หน่วยงานต่าง ๆ และส่วนที่ใช้เป็นที่ตั้งเครื่องบันทึกเทปการสนทนา เป็นต้น ออกจากศูนย์คอมพิวเตอร์ (หน้า 25)	*ชมรม IT Club / บลจ. กสิกรไทย / บล. เครดิต สวิส* 34. การกำหนดในลักษณะนี้อาจก่อให้เกิดประเด็นปัญหาในทางปฏิบัติ เนื่องจากในปัจจุบัน ฐานข้อมูลเทปการสนทนาของบริษัทถูกจัดเก็บอยู่ในศูนย์คอมพิวเตอร์และสามารถเรียกฟังได้เมื่อต้องการ โดยไม่จำเป็นต้องเข้าไปในบริเวณดังกล่าว	สำนักงานเห็นด้วยตามที่เสนอ และรับไปปรับปรุงร่างประกาศแนวปฏิบัติฯ เพื่อให้เป็นไปตามความเห็นของผู้ประกอบธุรกิจ หมายเหตุ : สำนักงานจะพิจารณาปรับปรุงเนื้อหาแนวทางปฏิบัติเพิ่มเติม ข้อ 5 เป็นดังนี้ “ผู้ประกอบธุรกิจควรแยกพื้นที่จุดรับส่งของ (delivery and loading area) ซึ่งเป็นพื้นที่ส่วนที่ต้องมีการเข้าถึงโดยพนักงานฝ่ายอื่น เช่น ส่วนที่ใช้เก็บรายงานที่ฝ่ายคอมพิวเตอร์ได้จัดพิมพ์ให้หน่วยงานต่าง ๆ ~~และส่วนที่ใช้เป็นที่ตั้งเครื่องบันทึกเทปการสนทนา เป็นต้น~~ ออกจากศูนย์คอมพิวเตอร์”
7.2 ทรัพย์สินสารสนเทศประเภทอุปกรณ์ (equipment)		
แนวทางปฏิบัติเพิ่มเติม (6) ผู้ประกอบธุรกิจควรจัดให้มีการควบคุมป้องกันทรัพย์สินสารสนเทศประเภทอุปกรณ์ระหว่างที่ไม่มีผู้ใช้งาน (unattended user equipment) ให้มีความปลอดภัย รวมทั้งควรกำหนดการควบคุมเอกสารข้อมูลหรือสื่อบันทึก	*ชมรม IT Club* 35. การจัดการอุปกรณ์บันทึกข้อมูล เช่น thumb drive และ external hard disk ไม่ให้วางไว้บนโต๊ะทำงานขณะที่ไม่ได้ใช้งาน เป็นเรื่องที่ควบคุมด้วยเทคนิคได้ยาก จะใช้การกำหนดเป็นข้อบังคับหรือประกาศให้พนักงานรับทราบและเป็นแนวทางปฏิบัติได้หรือไม่	ผู้ประกอบธุรกิจอาจใช้วิธีสื่อสารนโยบายและแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยของระบบ IT ให้แก่พนักงาน เพื่อลงนามรับทราบ รวมถึงกำหนดบทลงโทษกรณีที่พนักงานไม่ปฏิบัติตามให้มีความเหมาะสมชัดเจน [ระบุเพิ่มใน FAQ]

ข้อกำหนดที่เกี่ยวข้อง	ความคิดเห็น / คำถาม	ความเห็นสำนักงาน
ข้อมูลต่าง ๆ เช่น thumb drive และ external hard disk ที่มีข้อมูลสารสนเทศที่จัดเก็บหรือบันทึกอยู่ ไม่ให้วางทิ้งไว้บนโต๊ะทำงานหรือสถานที่ไม่ปลอดภัยในขณะที่ไม่ได้ใช้งาน (clear desk) ตลอดจนการควบคุมหน้าจอคอมพิวเตอร์ไม่ให้มีข้อมูลสำคัญปรากฏในขณะที่ไม่ได้ใช้งาน (clear screen) เช่น การตัดออกจากระบบ (session time out) และการล็อคหน้าจอ (lock screen) อัตโนมัติ เป็นต้น (หน้า 26)		
8. การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ (operations security)		
8.4 การบันทึก จัดเก็บหลักฐานและติดตาม (logging and monitoring)		
ตารางแสดงรายละเอียดการจัดเก็บหลักฐาน (หน้า 30 – 31)	*ชมรม IT Club* 36. ขอรายละเอียดเพิ่มเติมเกี่ยวกับข้อมูลที่แสดงในตาราง เช่น หลักฐานการใช้งานแฟ้มข้อมูล (audit log) หมายถึง แฟ้มข้อมูลทุกแฟ้ม แฟ้มข้อมูลสำคัญ หรือ file server หากกำหนดในลักษณะ policy control (ไม่ใช่ system control) จะมีความเป็นไปได้ในทางปฏิบัติมากกว่า เช่น ให้บริษัทออกเกณฑ์ภายในให้พนักงานเก็บ file สำคัญไว้ใน server เป็นต้น นอกจากนี้ การจัดเก็บ audit log ในส่วนที่เรียกใช้ผ่านเครื่องคอมพิวเตอร์ส่วนบุคคลจะเป็นภาระมาก เนื่องจากต้องจัดเก็บนานถึง 6 เดือน *ชมรม IT Club* 37. เหตุใด internet access log จึงระบุให้จัดเก็บ 1 ปี ขณะที่ พ.ร.บ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ กำหนดให้จัดเก็บ log เพียง 90 วัน	ผู้ประกอบธุรกิจต้องจัดเก็บหลักฐานการใช้งานแฟ้มข้อมูล (audit log) เฉพาะที่เป็นแฟ้มข้อมูลสำคัญของบุคลากรที่เป็น access person ตามประกาศแนวปฏิบัติว่าด้วยแนวทางปฏิบัติสำหรับการกำหนดนโยบาย มาตรการ และระบบงานที่เกี่ยวข้องกับการกระทำที่อาจมีความขัดแย้งทางผลประโยชน์กับลูกค้า ทั้งนี้ เพื่อให้สะดวกในการจัดเก็บ audit log ผู้ประกอบธุรกิจอาจกำหนดให้บุคลากรของตนจัดเก็บข้อมูลสำคัญไว้ใน server เท่านั้นก็ได้ [ระบุเพิ่มใน FAQ] การจัดเก็บ internet access log ตามระยะเวลาดังกล่าวนั้น เพื่อประโยชน์ในการตรวจสอบและป้องกันการใช้งานระบบสารสนเทศที่มีความผิดปกติหรือไม่เป็นไปตามกฎหมายหรือกฎเกณฑ์ที่เกี่ยวข้องตาม พ.ร.บ. หลักทรัพย์และตลาด

ข้อกำหนดที่เกี่ยวข้อง	ความคิดเห็น / คำถาม	ความเห็นสำนักงาน
		หลักทรัพย์ พ.ศ. 2535 รวมทั้งเพื่อเป็นประโยชน์ต่อผู้ประกอบธุรกิจในการติดตามตรวจสอบตามวัตถุประสงค์ดังกล่าวด้วย
	ชมรม IT Club 38. traffic log จะทำได้ยาก หากเป็น internal network ที่ไม่มี firewall มากั้น (เพื่อป้องกันปัญหาการรับส่ง package ช้า)	สำนักงานพิจารณาทบทวนในประเด็นดังกล่าวแล้วเห็นว่าควรกำหนดให้ผู้ประกอบธุรกิจจัดเก็บ network firewall log ทดแทนการจัดเก็บ traffic log เพื่อเป็นการลดภาระแก่ผู้ประกอบธุรกิจและยังสามารถบรรลุวัตถุประสงค์ในการจัดเก็บหลักฐานได้ตามเดิม ทั้งนี้ สำนักงานรับไปปรับปรุงข้อกำหนดที่เกี่ยวข้องเพื่อให้เป็นไปตามแนวทางดังกล่าว หมายเหตุ : สำนักงานจะพิจารณาปรับปรุงเนื้อหาร่างประกาศข้อกำหนดเกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รวมถึงร่างประกาศแนวปฏิบัติฯ โดยกำหนดให้จัดเก็บ network firewall log ทดแทนการจัดเก็บ traffic log และมีรายละเอียดขั้นต่ำในการจัดเก็บคือ IP address ต้นทาง / IP address ปลายทาง / firewall action / port ที่ใช้ติดต่อ / วันและเวลา
	ชมรม IT Club / ISV 39. database log ควรระบุขอบเขตว่าต้องจัดเก็บถึง level ไหน เพื่อป้องกัน log มีขนาดใหญ่จนเกินไปซึ่งอาจกระทบกับ performance ของระบบงานได้	วัตถุประสงค์ในการจัดเก็บ database log เพื่อให้ผู้ประกอบธุรกิจมีข้อมูลเพียงพอในการติดตามตรวจสอบและป้องกันการเข้าถึงฐานข้อมูลของบริษัทโดยไม่ได้รับอนุญาต ดังนั้น ข้อกำหนดในส่วนนี้จึงระบุเพียงให้ผู้ประกอบธุรกิจจัดเก็บ log การเข้าใช้งานของผู้บริหารระบบฐานข้อมูล (database admin) ซึ่งมีรายละเอียดขั้นต่ำเกี่ยวกับชื่อบัญชีผู้ใช้งาน วันและเวลาที่เข้าใช้งาน เท่านั้น [ระบุเพิ่มใน FAQ]

ข้อกำหนดที่เกี่ยวข้อง	ความคิดเห็น / คำถาม	ความเห็นสำนักงาน
	ชมรม IT Club / นักวิชาการ 40. electronic messaging log ที่ให้เก็บนั้น เฉพาะการสื่อสารกับภายนอกองค์กรเท่านั้นหรือไม่ และเหตุใดสำนักงานจึงกำหนดให้เฉพาะผู้ประกอบธุรกิจจัดการกองทุนรวม / กองทุนส่วนบุคคล จัดเก็บหลักฐานดังกล่าวเท่านั้น	เนื่องจากประกาศแนวปฏิบัติว่าด้วยแนวทางปฏิบัติสำหรับการกำหนดนโยบาย มาตรการ และระบบงานที่เกี่ยวข้องกับการกระทำที่อาจมีความขัดแย้งทางผลประโยชน์กับลูกค้า กำหนดให้ผู้ประกอบธุรกิจจัดการลงทุนจัดเก็บหลักฐานการติดต่อสนทนาผ่านช่องทางอิเล็กทรอนิกส์ (electronic messaging) ของบุคลากรที่เป็น access person โดยให้จัดเก็บข้อมูลการสื่อสารกับบุคคลอื่นทั้งภายในและภายนอกองค์กร อย่างไรก็ดี สำนักงานได้พิจารณาความเสี่ยงเกี่ยวกับการใช้ประโยชน์จากข้อมูลภายในที่ยังมิได้เปิดเผยต่อประชาชนหรือข้อมูลที่เกี่ยวข้องกับลูกค้าที่มิพึงเปิดเผยซึ่งผู้ประกอบธุรกิจล่วงรู้มาเนื่องจากการประกอบธุรกิจแล้ว จึงเห็นควรขยายขอบเขตการจัดเก็บหลักฐานดังกล่าวให้ครอบคลุมถึงผู้ประกอบธุรกิจนายหน้าซื้อขายหลักทรัพย์ การค้าหลักทรัพย์ หรือการจัดจำหน่ายหลักทรัพย์ซึ่งมิได้จำกัดเฉพาะหลักทรัพย์อันเป็นตราสารแห่งหนี้หรือหน่วยลงทุน และตัวแทนซื้อขายสัญญาซื้อขายล่วงหน้าด้วย [ระบุเพิ่มใน FAQ] หมายเหตุ : สำนักงานจะพิจารณาปรับปรุงเนื้อหาร่างประกาศข้อกำหนดเกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รวมถึงร่างประกาศแนวปฏิบัติฯ โดยขยายขอบเขตการจัดเก็บหลักฐานการติดต่อสนทนาผ่านช่องทางอิเล็กทรอนิกส์ (electronic messaging) ให้ครอบคลุมถึงผู้ที่ได้รับใบอนุญาตให้ประกอบธุรกิจหลักทรัพย์หรือธุรกิจสัญญาซื้อขายล่วงหน้าประเภทดังต่อไปนี้

ข้อกำหนดที่เกี่ยวข้อง	ความคิดเห็น / คำถาม	ความเห็นสำนักงาน
		1) การเป็นนายหน้า ค้า จัดจำหน่ายหลักทรัพย์ ซึ่งมิได้จำกัดเฉพาะหลักทรัพย์อันเป็นตราสารแห่งหนี้หรือหน่วยลงทุน 2) การเป็นตัวแทนซื้อขายสัญญาซื้อขายล่วงหน้า
	ชมรม IT Club / บล. ทรีนีตี้ 41. เห็นด้วยกับการจัดเก็บ audit log ระยะเวลาไม่น้อยกว่า 6 เดือน แต่มีความเห็นเพิ่มเติม ดังนี้ 1) แฟ้มข้อมูลที่ทำการเก็บหลักฐานดังกล่าวควรขึ้นอยู่กับความสำคัญ ความเสี่ยง ความสามารถของระบบในการเก็บหลักฐานและผลกระทบต่อความรวดเร็วในการให้บริการเมื่อต้องทำการจัดเก็บรายละเอียดดังกล่าว	เนื่องจากร่างประกาศแนวปฏิบัติฯ กำหนดให้จัดเก็บหลักฐานการใช้งานแฟ้มข้อมูล (audit log) เฉพาะที่เป็นแฟ้มข้อมูลสำคัญของบุคลากรที่ล่วงรู้ / เข้าถึงข้อมูลลับ (access person) และมีความเสี่ยงที่จะนำข้อมูลดังกล่าวไปใช้เพื่อประโยชน์ส่วนตนหรือบุคคลอื่นซึ่งเป็นประเด็นที่สำนักงานให้ความสำคัญเป็นอย่างมาก ด้วยเหตุนั้น สำนักงานจึงเห็นว่าหลักการดังกล่าวสอดคล้องกับความเห็นของผู้ประกอบธุรกิจแล้ว
	2) การจัดเก็บหลักฐานดังกล่าวควรเป็นการเก็บเฉพาะกรณีเข้าถึงแฟ้มข้อมูลที่อยู่บนเครื่องแม่ข่าย (server) เท่านั้น	อ้างอิงคำตอบตามข้อ 34
	ชมรม IT Club 42. หลักฐานการใช้งาน internet ผ่านระบบเครือข่ายคอมพิวเตอร์ภายในของผู้ประกอบธุรกิจ ในกรณีที่เป็นการใช้งาน internet เพื่อเข้าถึงระบบซื้อขายภายนอก เช่น ระบบ SETTRADE ในการจัดเก็บหลักฐานการใช้งานดังกล่าวควรสามารถยกเว้นการจัดเก็บข้อมูล “ที่อยู่ของเว็บไซต์ปลายทาง (full URL)” เนื่องจากผู้ให้บริการจะมีหน้าที่ในการจัดเก็บหลักฐานดังกล่าวอยู่แล้ว อีกทั้งหลักฐานการใช้งานส่วนอื่นที่ยังคงจัดเก็บอยู่ก็น่าจะเพียงพอต่อการตรวจสอบ ทั้งนี้เพื่อให้การเข้าถึงบริการมีความรวดเร็ว สำหรับการเข้าถึงเว็บไซต์อื่น ๆ ที่ไม่เกี่ยวกับการซื้อขาย เห็นด้วยที่จะต้องจัดเก็บ full URL	ผู้ประกอบธุรกิจอาจจัดเก็บข้อมูลหลักฐานที่เกิดจากการสื่อสารไปยังภายนอกองค์กรผ่าน firewall ของบริษัทร่วมกับข้อมูลหลักฐานประเภทอื่น ๆ เพื่อให้ได้มาซึ่งหลักฐานตามที่ร่างประกาศแนวปฏิบัติฯ กำหนดอย่างครบถ้วนได้ [ระบุเพิ่มใน FAQ]

ข้อกำหนดที่เกี่ยวข้อง	ความคิดเห็น / คำถาม	ความเห็นสำนักงาน
	ชมรม IT Club 43. หัวข้อการบันทึก จัดเก็บหลักฐานและการติดตามในส่วนของหลักฐานการใช้งานข้อมูล มีข้อกำหนดเจาะจงทางเทคนิคเกินไป ควรมีข้อกำหนดทางนโยบายควบคู่ไป *ชมรม IT Club* 44. การเก็บ log ตามเกณฑ์ของ ก.ล.ต. จะทำให้เกิดต้นทุนจำนวนมาก เช่น payload อาจทำให้บริษัทไม่มีงบประมาณเพียงพอในการดำเนินการ	ผู้ประกอบธุรกิจควรจัดให้มีข้อกำหนดทางนโยบายควบคู่กันไป เพื่อเป็นการลดภาระในการจัดเก็บหลักฐาน โดยที่ยังคงปฏิบัติได้อย่างถูกต้องตามข้อกำหนดในส่วนนี้ อ้างอิงคำตอบตามข้อ 38
<u>แนวทางปฏิบัติเพิ่มเติม</u> ข้อ 3 ผู้ประกอบธุรกิจที่เป็นสมาชิกของตลาดหลักทรัพย์ควรกำหนด ระบบเวลาของอุปกรณ์และระบบสารสนเทศที่เกี่ยวกับการซื้อขายหลักทรัพย์และการชำระราคาให้ตรงกับเวลาอ้างอิงของระบบซื้อขายหลักทรัพย์ของตลาดหลักทรัพย์ สำหรับผู้ประกอบธุรกิจอื่นที่ไม่ได้เป็นสมาชิกของตลาดหลักทรัพย์ ควรกำหนดระบบเวลาให้ตรงกับเวลาอ้างอิงของกรมอุทกศาสตร์กองทัพเรือ ทั้งนี้ เพื่อให้การตรวจสอบธุรกรรมที่ไม่เหมาะสมทั้งหมดเป็นไปอย่างถูกต้องและมีประสิทธิภาพ (หน้า 32)	*ชมรม IT Club* 45. ในส่วนของผู้ประกอบธุรกิจอื่นที่ไม่ได้เป็นสมาชิกของตลาดหลักทรัพย์ การกำหนดระบบเวลาให้ตรงกับเวลาอ้างอิงของกรมอุทกศาสตร์กองทัพเรือเพียงอย่างเดียว อาจไม่มีความยืดหยุ่นเพียงพอในการปฏิบัติ (กรณีโบรกเกอร์ลูกแบงค์ อาจต้องใช้ระบบต่าง ๆ ร่วมกับแบงค์)	สำนักงานเห็นด้วยตามที่เสนอ และรับไปปรับปรุงร่างประกาศแนวปฏิบัติฯ เพื่อให้เป็นไปตามความเห็นของผู้ประกอบธุรกิจ <u>หมายเหตุ :</u> สำนักงานจะพิจารณาปรับปรุงเนื้อหาแนวทางปฏิบัติเพิ่มเติม ข้อ 3 เป็นดังนี้ “ผู้ประกอบธุรกิจที่เป็นสมาชิกของตลาดหลักทรัพย์ควรกำหนดระบบเวลาของอุปกรณ์และระบบสารสนเทศที่เกี่ยวกับการซื้อขายหลักทรัพย์และการชำระราคาให้ตรงกับเวลาอ้างอิงของระบบซื้อขายหลักทรัพย์ของตลาดหลักทรัพย์ ~~สำหรับผู้ประกอบธุรกิจอื่นที่ไม่ได้เป็นสมาชิกของตลาดหลักทรัพย์ ควรกำหนดระบบเวลาให้ตรงกับเวลาอ้างอิงของกรมอุทกศาสตร์กองทัพเรือ~~ <u>หรือเวลาอ้างอิงของบริษัทที่อยู่ในกลุ่มธุรกิจเดียวกัน</u> ทั้งนี้ เพื่อให้การตรวจสอบธุรกรรมที่ไม่เหมาะสมทั้งหมดเป็นไปอย่างถูกต้องและมีประสิทธิภาพ”

ข้อกำหนดที่เกี่ยวข้อง	ความคิดเห็น / คำถาม	ความเห็นสำนักงาน
	ชมรม IT Club 46. หากระบบงานของผู้ประกอบธุรกิจกำหนดเวลาอ้างอิงกับ NTP server (Stratum 1) ซึ่งอ้างอิงเวลากับดาวเทียม (ซึ่งเป็น Stratum 0) อยู่แล้ว จะเทียบเท่ากับการไปอ้างอิงเวลากับกรมอุทกศาสตร์กองทัพเรือได้หรือไม่ ขอให้ระบุให้ชัดเจน	ผู้ประกอบธุรกิจที่มิใช่สมาชิกของตลาดหลักทรัพย์สามารถกำหนดเวลาอ้างอิงได้ตามที่เห็นสมควร
	ชมรม IT Club 47. ควรมีการกำหนดรายละเอียดระบบที่ต้องอ้างอิงเวลากับตลาดหลักทรัพย์ เพราะบริษัทมี server ระบบซื้อ/ขายมากกว่า 1 เครื่อง และไม่สามารถนำทุก server ไปอ้างอิงเวลาจากตลาดหลักทรัพย์ได้ทั้งหมด	ผู้ประกอบธุรกิจสามารถกำหนดให้ server ตัวอื่น ๆ ใช้เวลาอ้างอิงของ master server ที่เทียบเวลาโดยตรงกับตลาดหลักทรัพย์ทดแทนการกำหนดให้ server ทุกตัวใช้เวลาอ้างอิงของตลาดหลักทรัพย์ได้ [ระบุเพิ่มใน FAQ]
8.6 การบริหารจัดการช่องโหว่ทางเทคนิค (technical vulnerability management)		
	ชมรม IT Club 48. บริษัทเห็นว่าการกำหนดให้การทดสอบเจาะระบบ (penetration test) ต้องกระทำโดยบุคคลที่เป็นอิสระจากฝ่าย IT เป็นเรื่องที่ปฏิบัติได้ยาก เห็นควรมีข้อยกเว้น	วัตถุประสงค์ในการกำหนดให้การทดสอบดังกล่าวต้องกระทำโดยบุคคลที่เป็นอิสระจากฝ่าย IT เท่านั้น ก็เพื่อให้ผู้ประกอบธุรกิจได้รับทราบถึงข้อมูลเกี่ยวกับความเสี่ยงที่อาจเกิดขึ้นจากการถูกบุกรุกผ่านช่องโหว่ของระบบเครือข่ายได้อย่างถูกต้อง เที่ยงตรงจากบุคคลที่ไม่มีส่วนได้เสียกับการดำเนินการดังกล่าว อย่างไรก็ดี ผู้ประกอบธุรกิจสามารถจัดให้บุคคลอื่นดำเนินการทดสอบดังกล่าวแทนบุคลากรของผู้ประกอบธุรกิจได้ เช่น บุคลากรด้าน IT จากบริษัทแม่ของผู้ประกอบธุรกิจเอง หรือผู้เชี่ยวชาญด้านการเจาะระบบจากภายนอก เป็นต้น [อ้างอิง FAQ ข้อ 8.2] หมายเหตุ : สำนักงานจะพิจารณาปรับปรุงเนื้อหาร่างประกาศข้อกำหนดเกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยี

ข้อกำหนดที่เกี่ยวข้อง	ความคิดเห็น / คำถาม	ความเห็นสำนักงาน
		สารสนเทศ รวมถึงร่างประกาศแนวปฏิบัติฯ ในส่วนของข้อกำหนดดังกล่าว โดยกำหนดให้ 1) มีการทดสอบเจาะระบบ (penetration test) โดยบุคคลที่เป็นอิสระจากฝ่ายเทคโนโลยีสารสนเทศ 2) มีการรายงานผลการประเมินช่องโหว่ของระบบ (vulnerability assessment) ไปยังหน่วยงานกำกับการปฏิบัติงาน หรือหน่วยงานตรวจสอบภายใน
	ISV 49. ผู้ทดสอบเจาะระบบ (penetration test) ต้องมีความรู้ความสามารถเป็นที่น่าเชื่อถือได้นั้นควรมีคุณสมบัติอย่างไร	ผู้ทดสอบดังกล่าวต้องมีความเป็นอิสระจากฝ่าย IT รวมถึงสามารถดำเนินการทดสอบเจาะระบบโดยครอบคลุมจุดเสี่ยงที่สำคัญ 10 อันดับล่าสุดตามการจัดอันดับความเสี่ยงของ web application จากองค์กร OWASP (The Open Web Application Security Project) สำหรับคุณสมบัติในส่วนอื่นของผู้ทดสอบ ให้เป็นตามที่ผู้ประกอบธุรกิจเห็นสมควร [ระบุเพิ่มใน FAQ]
9. การรักษาความมั่นคงปลอดภัยด้านการสื่อสารข้อมูลสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์ (Communications Security)		
9.2 การควบคุมการรับส่งข้อมูลสารสนเทศ (information transfer)		
วัตถุประสงค์ เพื่อรักษาความมั่นคงปลอดภัยในการรับส่งข้อมูลสารสนเทศผ่านระบบเครือข่ายภายในองค์กร และระหว่างระบบเครือข่ายภายในองค์กรกับระบบเครือข่ายภายนอก (หน้า 36)	*ชมรม IT Club* 50. การ Encrypt Data รวมถึงการสื่อสารภายในองค์กร ด้วยหรือไม่ (ระบุอยู่ในข้อ 6 แล้ว)	อ้างอิงคำตอบตามข้อ 29
10. การจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศ (system acquisition, development and maintenance)		
	ชมรม IT Club 51. จะเป็นการกีดกันการเลือกใช้งานผู้พัฒนาขนาดกลางและขนาดเล็กในการนำเสนอบริการไปโดยปริยาย	ข้อกำหนดในหัวข้อดังกล่าวมีวัตถุประสงค์เพียงเพื่อให้กระบวนการจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศของ

ข้อกำหนดที่เกี่ยวข้อง	ความคิดเห็น / คำถาม	ความเห็นสำนักงาน
		ผู้ประกอบธุรกิจมีความมั่นคงปลอดภัยตลอดช่วงอายุการใช้งาน ซึ่งปกติเป็นมาตรฐานที่ผู้พัฒนาทุกรายพึงมีอยู่แล้ว นอกจากนี้ ไม่มีข้อกำหนดใดในส่วนนี้ที่ระบุถึงคุณสมบัติขั้นต่ำเกี่ยวกับการคัดเลือกผู้พัฒนาระบบสารสนเทศ
	ISV 52. บริษัทผู้พัฒนาระบบควรต้องผ่าน ISO27001 หรือไม่	อ้างอิงคำตอบตามข้อ 51
11. การใช้บริการจากผู้ให้บริการภายนอก (supplier relationship)		
	ชมรม IT Club 53. ข้อกำหนดในหัวข้อนี้ ใช้กับ vendor ที่บริษัทเคยใช้บริการในอดีตด้วยหรือไม่ ทั้งนี้ หากปัจจุบัน vendor รายดังกล่าวเลิกกิจการไปแล้ว จะต้องดำเนินการอย่างไร	ข้อกำหนดในส่วนนี้ใช้บังคับเฉพาะกรณีที่ผู้ประกอบธุรกิจใช้บริการจากผู้รับดำเนินการ (outsourcee) รายปัจจุบันเท่านั้น
11.1 การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศจากผู้ให้บริการภายนอก (information security in supplier relationships)		
	ชมรม IT Club 54. หลักเกณฑ์และแนวปฏิบัติสามารถใช้บังคับเฉพาะกับการเริ่มทำสัญญากับผู้ให้บริการภายนอกรายใหม่ได้หรือไม่ เนื่องจากผู้ให้บริการรายเดิมซึ่งมีความชำนาญหรือมีความต่อเนื่องในการดูแลระบบงาน อาจมีข้อขัดข้องหรือไม่สามารถปฏิบัติตามหลักเกณฑ์ได้ และอาจส่งผลให้เกิดปัญหาในการปฏิบัติงานของบริษัท	ผู้ประกอบธุรกิจควรกำหนดให้ผู้รับดำเนินการ (outsourcee) ของตน ติดตามหลักเกณฑ์และแนวปฏิบัติที่เกี่ยวข้องของสำนักงาน รวมถึงเตรียมความพร้อมเพื่อให้สามารถดำเนินการให้เป็นไปตามหลักเกณฑ์ใหม่ของสำนักงานได้อย่างถูกต้อง ครบถ้วน ทั้งนี้ ผู้ประกอบธุรกิจมีเวลาเตรียมความพร้อมจนถึงก่อนวันที่ประกาศมีผลใช้บังคับ 1 กรกฎาคม 2560

ข้อกำหนดที่เกี่ยวข้อง	ความคิดเห็น / คำถาม	ความเห็นสำนักงาน
<u>ข้อกำหนดในประกาศที่ สธ. xx/2559</u> ข้อ 23 ในกรณีที่ผู้ประกอบธุรกิจแต่งตั้งบุคคลอื่นเป็นผู้รับดำเนินการในงานที่เกี่ยวกับระบบสารสนเทศของผู้ประกอบธุรกิจ ผู้ประกอบธุรกิจต้องดำเนินการให้เป็นไปตามหลักเกณฑ์ดังต่อไปนี้ (6) กำหนดสิทธิในการเข้าตรวจสอบกระบวนการปฏิบัติงานของผู้รับดำเนินการและควบคุมให้การปฏิบัติงานเป็นไปตามข้อตกลงที่กำหนดไว้ เว้นแต่ในกรณีที่ผู้รับดำเนินการมีข้อจำกัดในการเข้าตรวจสอบการปฏิบัติงานดังกล่าว ผู้ประกอบธุรกิจต้องมีมาตรการเพื่อให้มั่นใจได้ว่าสามารถควบคุมการปฏิบัติงานของผู้รับดำเนินการให้เป็นไปตามข้อตกลงที่กำหนดไว้ได้ (หน้า 41)	*ชมรม IT Club* 55. บริษัทมีข้อจำกัดในการดำเนินการดังกล่าวกับผู้ให้บริการบางราย เช่น SETTRADE สำนักงาน ก.ล.ต. อาจต้องกำหนดเป็นข้อยกเว้นสำหรับผู้ให้บริการรายนั้น ๆ	กรณีที่ผู้ประกอบธุรกิจมีข้อจำกัดในการเข้าตรวจสอบการปฏิบัติงานของผู้รับดำเนินการ (outsourcee) ผู้ประกอบธุรกิจอาจกำหนดมาตรการอื่นทดแทนเพื่อให้มั่นใจได้ว่าสามารถควบคุมการปฏิบัติงานของผู้รับดำเนินการให้เป็นไปตามข้อตกลงที่กำหนดไว้ เช่น กำหนดให้ผู้รับดำเนินการจัดให้มีการตรวจสอบการปฏิบัติงานโดยผู้ตรวจสอบอิสระ และรายงานผลการตรวจสอบดังกล่าวแก่ผู้ประกอบธุรกิจตามรอบระยะเวลาที่กำหนด เป็นต้น
<u>แนวทางปฏิบัติเพิ่มเติม</u> ข้อ 1 นโยบายเกี่ยวกับการให้บุคคลอื่นเป็นผู้รับดำเนินการในงานที่เกี่ยวกับระบบสารสนเทศของผู้ประกอบธุรกิจตามข้อกำหนด 7(12) ควรมีเนื้อหาขั้นต่ำครอบคลุมประเด็นดังต่อไปนี้ (5) ระบุประเภทข้อมูลสารสนเทศที่อนุญาตให้ผู้รับดำเนินการเข้าถึง เพื่อให้การกำหนดมาตรการควบคุมและติดตามการเข้าถึงข้อมูลเป็นไปอย่างเหมาะสมภายใต้หลักความจำเป็นในการรู้ข้อมูล (need-to-know basis) (6) จัดให้มีขั้นตอนและกระบวนการติดตามควบคุมการเข้าถึงสารสนเทศอย่างเหมาะสม (หน้า 42)	*ชมรม IT Club* 56. ขอคำอธิบายเพิ่มเติม ของ (5) และ (6)	ผู้ประกอบธุรกิจควรประเมินขอบเขตและประเภทของข้อมูลที่ผู้รับดำเนินการจำเป็นต้องใช้หรือเข้าถึงเพื่อให้สามารถปฏิบัติงานได้อย่างเพียงพอเหมาะสมและเป็นไปตามที่ผู้ประกอบธุรกิจกำหนดให้แล้วเสร็จก่อน จากนั้นจึงพิจารณากำหนดมาตรการในการควบคุมให้ผู้รับดำเนินการสามารถเข้าถึงข้อมูลได้เฉพาะที่จำเป็น รวมทั้งปฏิบัติให้เป็นไปตามมาตรการที่ผู้ประกอบธุรกิจกำหนด

ข้อกำหนดที่เกี่ยวข้อง	ความคิดเห็น / คำถาม	ความเห็นสำนักงาน
	ชมรม IT Club 57. กรณีบริษัทมี audit เข้าดำเนินการตรวจสอบ vendor และมีรายงานการตรวจสอบอยู่แล้ว จะถือว่าบริษัทดำเนินการตามข้อกำหนดของ ก.ล.ต. แล้วหรือไม่	การดำเนินการดังกล่าวเป็นไปตามข้อกำหนดในส่วนนี้แล้ว
12. การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Incident Management)		
	ชมรม IT Club 58. ขอเสนอเพิ่มเติมเกี่ยวกับเงื่อนไขในการพิจารณารายงาน incident ต่อคณะกรรมการกำกับฯ เช่น ผลกระทบเป็นจำนวนเงินตั้งแต่เท่าใด หรือจำนวนลูกค้าเคลมตั้งแต่เท่าใด หรือระยะเวลาที่เกิดปัญหาจึงจะต้องเริ่มรายงาน	วัตถุประสงค์ของข้อกำหนดในส่วนนี้มีเพื่อให้สำนักงานรับทราบข้อมูลที่เกี่ยวกับการหยุดชะงักของระบบหรือการถูก cyber attack ได้อย่างทันท่วงที เพื่อประโยชน์ในการพิจารณาแจ้งเตือนผู้ประกอบธุรกิจรายอื่น รวมถึงพิจารณาดำเนินการอื่นใดเพื่อช่วยเหลือผู้ประกอบธุรกิจได้อย่างเหมาะสม ดังนั้น เงื่อนไขในการรายงานตามที่ผู้ประกอบธุรกิจเสนอนั้นอาจใช้ระยะเวลาในการประเมินผลกระทบค่อนข้างนานจึงขัดกับวัตถุประสงค์ตามข้างต้น
13. การบริหารความต่อเนื่องทางธุรกิจในด้านความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Aspects of Business Continuity Management)		
แนวทางปฏิบัติเพิ่มเติม ในการกำหนดขั้นตอน กระบวนการดำเนินการและการควบคุมด้านความมั่นคงปลอดภัยของระบบสารสนเทศตามข้อกำหนด 10(2) ควรมีรายละเอียดขั้นต่ำดังต่อไปนี้ (4) ระบุรายละเอียดเกี่ยวกับศูนย์คอมพิวเตอร์สำรองให้ชัดเจน เช่น สถานที่ตั้ง แผนที่ เป็นต้น	*ชมรม IT Club / บล. CLSA / บล. เครดิต สวิส* 59. แนวทางข้อ 4 ในข้อกำหนดข้อ 10 ที่ให้ระบุรายละเอียดเกี่ยวกับศูนย์คอมพิวเตอร์สำรองให้ชัดเจน ขอให้สำนักงานพิจารณาข้อความดังกล่าว เนื่องจากบางบริษัทอาจไม่มีศูนย์คอมพิวเตอร์สำรอง	สำนักงานเห็นด้วยตามที่เสนอ และรับไปปรับปรุงร่างประกาศแนวปฏิบัติฯ เพื่อให้เป็นไปตามความเห็นของผู้ประกอบธุรกิจ หมายเหตุ : สำนักงานจะพิจารณาปรับปรุงเนื้อหาแนวทางปฏิบัติเพิ่มเติมข้อ 1(4) เป็นดังนี้ “ระบุรายละเอียดเกี่ยวกับศูนย์คอมพิวเตอร์สำรอง (ถ้ามี) ให้ชัดเจน เช่น สถานที่ตั้ง แผนที่ เป็นต้น”

ข้อกำหนดที่เกี่ยวข้อง	ความคิดเห็น / คำถาม	ความเห็นสำนักงาน
การมีผลใช้บังคับ		
1 เมษายน 2560	*ชมรม IT Club (9 เดือน - 2 ปี) / บล. ทรีนีตี้ (2 ปี) / บลจ. กสิกรไทย (n/a) / บลจ. โซลาริส (2 ปี) / บล. เครดิต สวิส (2 ปี) / บลจ. ทหารไทย (1 ปี)* 60. ขอเลื่อนระยะเวลามีผลใช้บังคับ เนื่องจากมีข้อจำกัดในการเตรียมความพร้อมเพื่อให้สามารถปฏิบัติได้ตามที่ประกาศกำหนด *ชมรม IT Club* 61. เนื่องจากเกณฑ์ของ ก.ล.ต. บังคับใช้กับผู้ประกอบธุรกิจ หาก ISV ไม่สามารถดำเนินการตามเกณฑ์ จะมีผลกับบริษัท ISV อย่างไร	สำนักงานพิจารณาแล้วจะกำหนดให้ผู้ประกอบธุรกิจปฏิบัติให้เป็นไปตามที่ประกาศกำหนดตั้งแต่วันที่ 1 กรกฎาคม 2560 เป็นต้นไป อ้างอิงคำตอบตามข้อ 52
ข้อคิดเห็นอื่น ๆ		
	ชมรม IT Club 62. หลังจากมีการบังคับใช้ประกาศแล้วนั้น ขอให้ทางสำนักงานแปลประกาศฉบับดังกล่าวเป็นภาษาอังกฤษเพื่อประโยชน์ในการสื่อสารกับต่างประเทศ *สมาคมผู้ตรวจสอบและควบคุมระบบสารสนเทศ (ISACA)* 63. เพื่อให้กระบวนการในการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศมีประสิทธิภาพและเป็นไปตามกรอบนโยบายที่คณะกรรมการบริษัทและผู้บริหารระดับสูงได้กำหนดไว้ รวมถึงยกระดับในการกำกับดูแลกิจการด้าน IT ให้ดียิ่งขึ้น สำนักงานควรกำหนดให้ IT governance เป็นส่วนหนึ่งของหลักเกณฑ์ในการกำกับดูแลด้าน IT สำหรับบริษัทหลักทรัพย์ที่มีการใช้เทคโนโลยีสารสนเทศเป็น key driver ในการดำเนินธุรกิจ	สำนักงานเห็นด้วย และรับไปดำเนินการตามที่เสนอ สำนักงานเห็นด้วย และรับไปดำเนินการตามที่เสนอ <u>หมายเหตุ :</u> สำนักงานจะพิจารณาปรับปรุงเนื้อหาร่างประกาศข้อกำหนดเกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รวมถึงร่างประกาศแนวปฏิบัติฯ โดยแบ่งออกเป็น 2 ส่วน ดังนี้ 1) การกำกับดูแลกิจการด้าน IT ที่ดี (IT governance) 2) การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยี

ข้อกำหนดที่เกี่ยวข้อง	ความคิดเห็น / คำถาม	ความเห็นสำนักงาน
		สารสนเทศ (IT security) ซึ่งมีเนื้อหาเป็นไปตามที่ได้รับฟังความคิดเห็น
	นักวิชาการ 64. สำนักงานมีแนวทางในการกำกับดูแลผู้ประกอบธุรกิจที่ปรึกษาการลงทุนซึ่งมีการใช้ fintech เพื่อให้คำแนะนำแก่ผู้ลงทุน หรือผู้พัฒนาซอฟแวร์ประเภท program trading เพื่อขายแก่ผู้ลงทุน / ผู้ประกอบธุรกิจ รวมถึงธนาคารพาณิชย์และบริษัทประกันภัยที่ได้รับอนุญาตให้ประกอบธุรกิจหลักทรัพย์ เช่น ธุรกิจค้าตราสารหนี้และค้าสัญญาซื้อขายล่วงหน้า หรือไม่อย่างไร	สำนักงานพิจารณาแล้วเห็นควรขยายขอบเขตการใช้บังคับให้ครอบคลุมถึงผู้ประกอบธุรกิจประเภทดังกล่าว เนื่องจากเป็นกลุ่มธุรกิจที่ใช้เทคโนโลยีสารเทศเป็นหัวใจสำคัญในการขับเคลื่อนธุรกิจเพื่อตอบสนองความต้องการของผู้ลงทุน โดยผู้ประกอบธุรกิจประเภทดังกล่าวจะปฏิบัติตามเฉพาะส่วนที่มีระบบงานสำคัญเกี่ยวข้องเท่านั้น ซึ่งโดยสรุปแล้วร่างประกาศข้อกำหนดเกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รวมถึงร่างประกาศแนวปฏิบัติฯ จะมีผลใช้บังคับกับผู้ที่ได้รับใบอนุญาตหรือได้รับจดทะเบียนให้ประกอบธุรกิจหลักทรัพย์หรือธุรกิจสัญญาซื้อขายล่วงหน้าประเภทดังต่อไปนี้ 1) การเป็นนายหน้า ค้า จัดจำหน่ายหลักทรัพย์ 2) การเป็นที่ปรึกษาการลงทุนหรือสัญญาซื้อขายล่วงหน้าที่ให้บริการประเภทดังต่อไปนี้ แต่ไม่รวมถึงการให้บริการจัดทำบทวิเคราะห์การลงทุน - พัฒนาโปรแกรมการลงทุน (program trading) หรือมีการใช้โปรแกรมดังกล่าวประกอบการให้บริการแก่ลูกค้า - ให้บริการวางแผนการลงทุนแก่ลูกค้า 3) การจัดการกองทุนรวม 4) การจัดการกองทุนส่วนบุคคล 5) กิจการการยืมและให้ยืมหลักทรัพย์ 6) การให้สินเชื่อเพื่อธุรกิจหลักทรัพย์ 7) การเป็นตัวแทนซื้อขายสัญญาซื้อขายล่วงหน้า

ข้อกำหนดที่เกี่ยวข้อง	ความคิดเห็น / คำถาม	ความเห็นสำนักงาน
		8) การค้าสัญญาซื้อขายล่วงหน้า 9) การเป็นผู้จัดการเงินทุนสัญญาซื้อขายล่วงหน้า ทั้งนี้ ในกรณีเป็นผู้ประกอบธุรกิจที่มีการกำกับดูแลโดยหน่วยงานกำกับดูแลอื่น ให้ปฏิบัติตามประกาศและแนวทางปฏิบัติเฉพาะในเรื่องการบันทึกจัดเก็บหลักฐานและติดตาม (logging and monitoring) และการบริหารจัดการเหตุการณ์ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ (information security incident management) หมายเหตุ : สำนักงานจะพิจารณาปรับปรุงเนื้อหาร่างประกาศข้อกำหนดเกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ โดยขยายขอบเขตใช้บังคับให้ครอบคลุมผู้ที่ได้รับใบอนุญาตหรือได้รับจดทะเบียนให้ประกอบธุรกิจหลักทรัพย์หรือธุรกิจสัญญาซื้อขายล่วงหน้าประเภทดังต่อไปนี้ 1) การเป็นนายหน้า ค้า จัดจำหน่ายหลักทรัพย์อันเป็นตราสารแห่งหนี้ 2) การค้าสัญญาซื้อขายล่วงหน้า 3) การเป็นที่ปรึกษาการลงทุนหรือสัญญาซื้อขายล่วงหน้าที่ให้บริการประเภทดังต่อไปนี้ แต่ไม่รวมถึงการให้บริการจัดทำบทวิเคราะห์การลงทุน - พัฒนาโปรแกรมการลงทุน (program trading) หรือมีการใช้โปรแกรมดังกล่าวประกอบการให้บริการแก่ลูกค้า - ให้บริการวางแผนการลงทุนแก่ลูกค้า

ข้อกำหนดที่เกี่ยวข้อง	ความคิดเห็น / คำถาม	ความเห็นสำนักงาน
	นักวิชาการ 65. สำนักงานควรกำหนดให้ผู้ประกอบธุรกิจต้องจัดให้มีการซักซ้อมรับมือภัยคุกคามด้านเทคโนโลยีสารสนเทศ (cybersecurity drill) เพื่อเป็นการเสริมสร้าง risk awareness และความคุ้นเคยในการรับมือภัยดังกล่าวแก่พนักงานของผู้ประกอบธุรกิจ	สำนักงานเห็นด้วย และรับไปดำเนินการตามที่เสนอ หมายเหตุ : สำนักงานจะพิจารณาปรับปรุงเนื้อหาร่างประกาศข้อกำหนดเกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รวมถึงร่างประกาศแนวปฏิบัติฯ ในส่วนของข้อกำหนดเกี่ยวกับ information security incident management โดยกำหนดเพิ่มให้ผู้ประกอบธุรกิจต้องจัดให้มี cybersecurity drill อย่างน้อยปีละ 1 ครั้ง