สีเหลือง – ปรับปรุงเพิ่มเติมล่าสุด

ประเด็นคำถามที่ถามบ่อย (FAQ) (ฉบับประมวล)

ลำดับ	คำถาม	คำตอบ
1. บทนิยาม		
1.1	"งานที่สำคัญ" หมายถึง งานที่เกี่ยวกับการให้บริการ การทำธุรกรรม หรืองานอื่น ๆ ของผู้ประกอบธุรกิจ ซึ่งหากมีการหยุดชะงักอาจส่งผลกระทบต่อลูกค้า การดำเนินงานธุรกิจ ชื่อเสียง ฐานะ และผลการดำเนินงานของผู้ประกอบธุรกิจอย่างมีนัยสำคัญ ขอคำอธิบายเพิ่มเติมของคำว่า "มีนัยสำคัญ"	ในการประเมินความเสี่ยงของงานที่ต้องพึ่งพาระบบสารสนเทศ กรณีที่เกิดเหตุการณ์ซึ่งส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศที่รองรับงานดังกล่าว และก่อให้เกิดความเสียหายต่อข้อมูลหรือทรัพย์สินของลูกค้า และการประกอบธุรกิจ ผลการดำเนินงานและชื่อเสียงของผู้ประกอบธุรกิจ ซึ่งเกินกว่าระดับที่ผู้ประกอบธุรกิจยอมรับได้ ให้ถือว่าผลกระทบดังกล่าวมีนัยสำคัญ และผู้ประกอบธุรกิจอาจจัดให้งานดังกล่าวเป็นงานที่สำคัญ
1.2	"ผู้รับดำเนินการ" ครอบคลุมถึงผู้ให้บริการประเภทใดบ้าง	บุคคลที่มีลักษณะเป็นผู้รับดำเนินการ (outsourcee) ในงานที่เกี่ยวข้องกับการประกอบธุรกิจหลักทรัพย์หรือสัญญาซื้อขายล่วงหน้าของผู้ประกอบธุรกิจตามประกาศคณะกรรมการกำกับตลาดทุนที่ ทธ. 25/2556 เรื่อง การให้บุคคลอื่นเป็นผู้รับดำเนินการในงานที่เกี่ยวข้องกับการประกอบธุรกิจ โดยผู้รับดำเนินการดังกล่าวจะต้องได้รับว่าจ้างจากผู้ประกอบธุรกิจให้ปฏิบัติงานอย่างต่อเนื่อง มิใช่การจ้างวานเป็นครั้งคราว รวมถึงต้องใช้ดุลพินิจหรือการตัดสินใจในการปฏิบัติงานดังกล่าวแทนผู้ประกอบธุรกิจ ทั้งนี้ ลักษณะงานอื่นใดที่นอกเหนือจากขอบเขตดังกล่าว จะไม่ถือเป็นผู้รับดำเนินการตามข้างต้น เช่น งานพัฒนาซอฟแวร์ งานวางระบบเครือข่าย หรืองานซ่อมบำรุงอุปกรณ์และระบบสารสนเทศ เป็นต้น

ลำดับ	คำถาม	คำตอบ
1.3	การใช้บริการจากผู้ให้บริการด้าน IT ตามนิยามของประกาศมีกี่ประเภท และแต่ละประเภทต้องปฏิบัติตามข้อกำหนดในส่วนใดบ้าง	การใช้บริการจากผู้ให้บริการด้าน IT เพื่อรองรับการปฏิบัติงานสำคัญที่เกี่ยวข้องกับการประกอบธุรกิจหลักทรัพย์หรือสัญญาซื้อขายล่วงหน้า สามารถจำแนกได้เป็น 3 ประเภท ดังนี้ <u>1) การใช้บริการจากผู้รับดำเนินการ (outsourcee) ตาม FAQ ข้อ 1.2 :</u> ตัวอย่างของการใช้บริการ เช่น การ outsource งานทั้งหมดของฝ่ายเทคโนโลยีสารสนเทศให้แก่บริษัทในเครือ เป็นต้น โดยผู้ประกอบธุรกิจที่ใช้บริการประเภทนี้ จะต้องปฏิบัติให้เป็นไปตามข้อกำหนดด้าน IT outsourcing ของประกาศแนวปฏิบัติที่ นป. 3/2559 (“ประกาศแนวปฏิบัติฯ”) <u>2) การใช้บริการจากผู้ให้บริการ cloud computing ตาม FAQ ข้อ 5.1 :</u> โดยผู้ประกอบธุรกิจที่ใช้บริการประเภทนี้ จะต้องปฏิบัติให้เป็นไปตามข้อกำหนดด้าน cloud computing ของประกาศแนวปฏิบัติฯ <u>3) การใช้บริการจากผู้ให้บริการด้าน IT ที่นอกเหนือจากข้อ 1) และ 2) ตามข้างต้น</u> : ตัวอย่างของการใช้บริการ เช่น บริการพัฒนาซอฟแวร์ / วางระบบเครือข่าย / ซ่อมบำรุงอุปกรณ์หรือระบบสารสนเทศ เป็นต้น โดยผู้ประกอบธุรกิจที่ใช้บริการประเภทนี้ จะต้องปฏิบัติให้เป็นไปตามข้อกำหนดด้าน system acquisition, development and maintenance ของประกาศแนวปฏิบัติฯ
1.4	นิยาม “ผู้ใช้งาน” ตามที่ปรากฏในประกาศแนวปฏิบัติฯ นั้นครอบคลุมถึงบุคคลใดบ้าง รวมถึงลูกค้าของบริษัทด้วยหรือไม่	“ผู้ใช้งาน” หมายถึง พนักงานของผู้ประกอบธุรกิจและบุคลากรภายนอก ที่มีการปฏิบัติงานโดยมีการเข้าถึงข้อมูลลับหรือระบบงานสำคัญภายในองค์กร โดยไม่รวมถึงลูกค้า

ลำดับ	คำถาม	คำตอบ
1.5	ประกาศแนวปฏิบัติฯ กำหนดขอบเขตในการ implement มากน้อยเพียงใด เช่น จัดทำเฉพาะ data center / service ที่สำคัญ / ทั้งองค์กร เนื่องจากใน ISO27001 กำหนดให้มีการระบุ scope ให้ชัดเจนก่อนทำการประเมินความเสี่ยง	ประกาศแนวปฏิบัติฯ ครอบคลุมถึง ข้อมูลสารสนเทศและทรัพย์สินสารสนเทศทั้งที่เป็น hardware / software ทั้งหมดที่เกี่ยวข้องกับระบบงานสำคัญ ดังนั้น ผู้ประกอบธุรกิจจึงควรประเมินระบบงานว่ามีระบบใดบ้างที่เข้าข่ายเป็นระบบงานสำคัญให้แล้วเสร็จก่อน จึงจะทราบว่าขอบเขตที่ต้องปฏิบัติให้เป็นไปตามประกาศแนวปฏิบัติฯ ดังกล่าวมีมากน้อยเพียงใด
1.6	ประกาศแนวปฏิบัติฯ ในแต่ละหัวข้อสามารถเลือกทำได้หรือไม่ เนื่องจากใน ISO27001 สามารถเลือกเฉพาะ control ที่ต้องการนำมาจัดการความเสี่ยงนั้น ๆ หลังจากประเมินความเสี่ยงแล้ว	กรณีที่ผู้ประกอบธุรกิจประเมินระบบงานสำคัญแล้วพบว่า มีบางหัวข้อที่ไม่เข้าข่ายต้องปฏิบัติตามประกาศแนวปฏิบัติฯ ดังกล่าว เช่น ระบบงานสำคัญของผู้ประกอบธุรกิจไม่ได้มีบุคคลอื่นเป็นผู้รับดำเนินการแทน หรือไม่มีนโยบายให้พนักงานใช้อุปกรณ์เคลื่อนที่ในการเข้าถึงระบบงานสำคัญหรือเชื่อมต่อ internet ผ่านเครือข่ายขององค์กร ผู้ประกอบธุรกิจอาจพิจารณาไม่ปฏิบัติตามในหัวข้อที่เกี่ยวข้องได้
2. <u>นโยบายและมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (information security policy)</u>		
2.1	ในกรณีผู้ประกอบธุรกิจเป็นบริษัทในกลุ่มธุรกิจทางการเงิน ผู้ประกอบธุรกิจสามารถใช้นโยบายกลุ่มซึ่งได้รับอนุมัติจาคณะกรรมการบริษัทในกลุ่ม หรือคณะกรรมการที่ได้รับมอบหมาย เพื่อลดความซ้ำซ้อนในการปฏิบัติได้หรือไม่	ผู้ประกอบธุรกิจอาจดำเนินการได้ ทั้งนี้ ควรปรับปรุงนโยบายดังกล่าวให้มีความสอดคล้องเหมาะสมกับลักษณะการประกอบธุรกิจของตนเองด้วย
3. <u>การจัดโครงสร้างภายในองค์กร (internal organization)</u>		
3.1	“ผู้บริหารระดับสูง” หมายถึงบุคลากรตั้งแต่ระดับใด	“ผู้บริหารระดับสูง” หมายถึง พนักงานของผู้ประกอบธุรกิจระดับผู้บริหารหน่วยงาน (head of department) ขึ้นไป

ลำดับ	คำถาม	คำตอบ
4. <u>การปฏิบัติงานที่มีการใช้อุปกรณ์เคลื่อนที่ (mobile device) เพื่อเข้าถึงระบบสารสนเทศภายในองค์กร และการปฏิบัติงานจากเครือข่ายภายนอกบริษัท (teleworking)</u>		
4.1	กรณีพนักงานทำการเชื่อมต่อ remote access จากที่บ้าน ผู้ประกอบธุรกิจอาจไม่สามารถทราบได้ว่าพนักงานทำการเชื่อมต่อโดยใช้อุปกรณ์ใด ผู้ประกอบธุรกิจต้องปฏิบัติตามหลักเกณฑ์ของสำนักงานอย่างไร	ผู้ประกอบธุรกิจต้องพิจารณาว่าการปฏิบัติงานดังกล่าวจัดเป็นการใช้งาน mobile device หรือเป็นการทำงานในลักษณะ teleworking เพื่อให้สามารถกำหนดได้ว่าการปฏิบัติงานดังกล่าวต้องเป็นไปตามแนวทางปฏิบัติของสำนักงานในส่วนของการใช้งาน mobile device หรือการทำงานในลักษณะ teleworking ทั้งนี้ การใช้งาน mobile device และการทำงานในลักษณะ teleworking มีลักษณะดังต่อไปนี้ 1. <u>mobile device</u> : ผู้ปฏิบัติงานนำอุปกรณ์เคลื่อนที่มาเชื่อมต่อกับระบบเครือข่ายคอมพิวเตอร์ภายในองค์กรเพื่อเข้าถึงระบบงานที่มีความสำคัญ เช่น นำ notebook ส่วนตัวมาเชื่อมต่อ Wi-Fi ของบริษัทเพื่อเข้าถึงระบบงานสำคัญ 2. <u>teleworking</u> : ผู้ปฏิบัติงานเข้าถึงระบบงานที่มีความสำคัญโดยไม่ผ่านการเชื่อมต่อกับระบบเครือข่ายคอมพิวเตอร์ภายในองค์กร โดยตรง เช่น ใช้งาน desktop PC ที่บ้าน เพื่อเข้าถึงระบบงานสำคัญของบริษัทโดยผ่านการเชื่อมต่ออินเตอร์เน็ตจากผู้ให้บริการอินเตอร์เน็ต (ISP)
4.2	หาก mobile device ที่เป็นอุปกรณ์ของพนักงานสูญหาย พนักงานต้องแจ้งให้ผู้ประกอบธุรกิจทราบหรือไม่	ต้องแจ้ง ในกรณีที่พนักงานเคยนำอุปกรณ์ดังกล่าวมาลงทะเบียนไว้กับผู้ประกอบธุรกิจ
4.3	จากหลักเกณฑ์ที่กำหนดให้ผู้ประกอบธุรกิจต้องจัดให้มีการป้องกันการเข้าถึงข้อมูลสารสนเทศจากบุคคลที่ไม่มีสิทธิในการใช้งานในพื้นที่ teleworking site เช่น ญาติพี่น้องและเพื่อน เป็นต้น ผู้ประกอบธุรกิจต้องดำเนินการ	ผู้ประกอบธุรกิจอาจใช้วิธีการกำหนดนโยบายเพื่อควบคุมการเข้าถึงเครื่องคอมพิวเตอร์ที่ใช้ปฏิบัติงานจากภายนอกบริษัท เช่น จัดให้มีการควบคุมหน้าจอคอมพิวเตอร์ไม่ให้มีข้อมูลสำคัญปรากฏในขณะที่ไม่ได้ใช้งาน (clear screen) การ log-off จากระบบเมื่อใช้งาน

ลำดับ	คำถาม	คำตอบ
	อย่างไร เพื่อให้มั่นใจว่าได้ปฏิบัติเป็นไปตามหลักเกณฑ์ดังกล่าว	เสร็จสิ้น และการกำหนดรหัสผ่าน เป็นต้น พร้อมทั้งจัดให้มีการซักซ้อมและสร้างความตระหนักรู้แก่พนักงานเพื่อให้มีการปฏิบัติตามนโยบายดังกล่าวอย่างเคร่งครัด
4.4	การตรวจสอบความมั่นคงปลอดภัยของอุปกรณ์คอมพิวเตอร์ส่วนตัวของพนักงานในพื้นที่ teleworking site อาจทำได้ยากในทางปฏิบัติ จึงขอให้ใช้วิธีการกำหนดสิทธิและตรวจสอบการเข้าถึงของพนักงานที่ได้รับอนุญาตให้ปฏิบัติงานที่ teleworking site พร้อมทั้งควบคุมความมั่นคงปลอดภัยของเครื่องคอมพิวเตอร์ในองค์กร และช่องทางการเชื่อมต่อ remote access ได้หรือไม่	เพื่อป้องกันการบุกรุกหรือเข้าถึงข้อมูลหรือระบบงานที่สำคัญในองค์กรอย่างไม่เหมาะสมจากการปฏิบัติงาน teleworking โดยเชื่อมต่อ remote access มายังองค์กร ผู้ประกอบธุรกิจอาจใช้วิธีกำหนดและตรวจสอบสิทธิการเข้าถึงของพนักงานที่ teleworking site แทนได้ หากมีการรักษาความปลอดภัยกับระบบคอมพิวเตอร์ในองค์กร และช่องทางการเชื่อมต่อแล้ว เช่น ติดตั้ง firewall update โปรแกรม anti-virus กำหนดสิทธิการเข้าถึง และกำหนดให้มีการเข้ารหัส network เป็นต้น
4.5	ในการออก booth นอกพื้นที่องค์กร ผู้ประกอบธุรกิจต้องควบคุมดูแลพื้นที่ดังกล่าวอย่างไร	ในกรณีที่ผู้ประกอบธุรกิจกำหนดให้พื้นที่ดังกล่าวเป็นพื้นที่หวงห้าม ผู้ประกอบธุรกิจต้องกำหนดมาตรการรักษาความมั่นคงปลอดภัยด้านกายภาพสำหรับพื้นที่ปฏิบัติงานนอกองค์กร รวมทั้งต้องกำหนดมาตรการเพื่อป้องกันภัยคุกคามและรักษาความมั่นคงปลอดภัยต่อข้อมูลที่มีความสำคัญ และควบคุมสิทธิการใช้งานและการเข้าถึงข้อมูลและระบบงานที่มีความสำคัญโดยผู้ใช้งานอย่างเหมาะสม
4.6	การควบคุมให้มีความปลอดภัยด้านกายภาพสำหรับพื้นที่ปฏิบัติงานนอกองค์กรเป็นเรื่องยาก โดยเฉพาะกรณีพนักงานหรือ vendor ทำการ remote เข้ามาเพื่อแก้ไขปัญหา บริษัทไม่สามารถรู้ได้ว่าเจ้าหน้าที่ดังกล่าวดำเนินการจากสถานที่ใด	ผู้ประกอบธุรกิจอาจกำหนดมาตรการดังกล่าวให้มีความยืดหยุ่นและเหมาะสมโดยคำนึงถึงขอบเขตการปฏิบัติงานเป็นสำคัญ เช่น การปฏิบัติงานที่ศูนย์สำรองต้องมีมาตรการการรักษาความมั่นคงปลอดภัยเทียบเท่าการทำงานที่บริษัทตามปกติ ขณะที่การปฏิบัติงานที่บ้าน (work from home) อาจกำหนดให้

ลำดับ	คำถาม	คำตอบ
		มีการป้องกันการเข้าถึงข้อมูลสารสนเทศจากบุคคลที่ไม่มีสิทธิ์ในการใช้งานก็เพียงพอ สำหรับกรณีที่พนักงานหรือ vendor ทำการ remote เข้ามาเพื่อปฏิบัติงานหรือแก้ไขปัญหาด้านระบบ IT นั้น หากผู้ประกอบธุรกิจมีการสื่อสารนโยบายและแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยของระบบ IT ให้แก่บุคลากรดังกล่าวทราบ เช่น การสื่อสารผ่าน e-mail หรือแสดงข้อความ pop-up เมื่อเข้าใช้งานระบบ รวมถึงจัดให้มีการตรวจสอบการใช้งานระบบ / การเข้าถึงข้อมูลของบุคลากรดังกล่าวขณะที่มีการเชื่อมต่อผ่านเครือข่ายของผู้ประกอบธุรกิจอย่างเหมาะสมรัดกุม จะถือว่า ผู้ประกอบธุรกิจปฏิบัติตามหลักเกณฑ์ของข้อกำหนดในส่วนนี้แล้ว
4.7	หัวข้อ mobile device และ teleworking ครอบคลุมเฉพาะพนักงานของบริษัทอย่างเดียวหรือ vendor ด้วย เพราะบริษัทอาจไม่สามารถปฏิบัติได้ทุกข้อ เช่น การลงเฉพาะ software ที่มีลิขสิทธิ์หรือการ update patch ซึ่งในการที่ vendor เข้ามา support ผ่าน teleworking บริษัทอาจไม่สามารถตรวจสอบได้ว่า เครื่องมือหรืออุปกรณ์ที่เชื่อมต่อนั้นมีความปลอดภัยเพียงใด	หัวข้อดังกล่าวครอบคลุมถึงบุคลากรของผู้ให้บริการภายนอก (vendor) ที่มีการปฏิบัติงานโดยมีการเข้าถึงข้อมูลลับหรือระบบงานสำคัญภายในองค์กรด้วย อย่างไรก็ดี หากผู้ประกอบธุรกิจมีการสื่อสารนโยบายและแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยของระบบ IT ให้แก่บุคลากรดังกล่าวทราบ เช่น การสื่อสารผ่าน e-mail หรือแสดงข้อความ pop-up เมื่อใช้งานระบบ รวมถึงจัดให้มีการตรวจสอบการใช้งานระบบและการเข้าถึงข้อมูลของบุคลากรดังกล่าวขณะที่มีการเชื่อมต่อผ่านเครือข่ายของผู้ประกอบธุรกิจอย่างเหมาะสมรัดกุมแล้ว ให้ถือว่าผู้ประกอบธุรกิจได้ปฏิบัติให้เป็นไปตามหลักเกณฑ์ของข้อกำหนดในส่วนนี้แล้ว

ลำดับ	คำถาม	คำตอบ
4.8	ในการปฏิบัติงานที่มีการใช้ mobile device จะต้องกำหนดให้มีการลงทะเบียนอุปกรณ์ เช่น ยี่ห้อ รุ่น , OS , serial number , MAC address ขอสอบถามเพิ่มเติมว่า การลงทะเบียนนั้นใช้เฉพาะกับพนักงานของบริษัทที่นำอุปกรณ์มาใช้ หรือว่ารวมไปถึงลูกค้าและ supplier ด้วย	การลงทะเบียนอุปกรณ์นั้นให้รวมถึงเฉพาะพนักงานของผู้ประกอบธุรกิจและบุคลากรภายนอก ที่มีการปฏิบัติงานโดยมีการเข้าถึงข้อมูลลับหรือระบบงานสำคัญภายในองค์กรโดยผ่านการเชื่อมต่อกับเครือข่ายคอมพิวเตอร์ภายในองค์กรเท่านั้น สำหรับในส่วนของลูกค้า ผู้ประกอบธุรกิจควรจัดให้มีการลงทะเบียนผู้ใช้งาน internet ทุกรายที่เชื่อมต่อผ่านเครือข่ายของผู้ประกอบธุรกิจด้วยวิธีการที่เหมาะสมและสอดคล้องกับวัตถุประสงค์ของการปฏิบัติให้เป็นไปตามประกาศแนวปฏิบัติฯ 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 ผ่านเครือข่ายของผู้ประกอบธุรกิจได้อย่างถูกต้องและเป็นประโยชน์ในการติดตามตรวจสอบและป้องกันการใช้งานระบบสารสนเทศที่มีความผิดปกติหรือไม่เป็นไปตามกฎหมายหรือกฎเกณฑ์ที่เกี่ยวข้องต่อไป
4.9	กรณีอุปกรณ์สูญหาย เป็นการยากหากต้องดำเนินการลบข้อมูลจากระยะไกล (remote wipe-out) หากบริษัทมีการควบคุมเรื่องของรหัสผ่านในการเข้าเครื่องและการ lock screen จะสามารถทดแทนการลบข้อมูลได้หรือไม่	เพื่อป้องกันข้อมูลที่เป็นความลับหรือมีความสำคัญสูงซึ่งถูกจัดเก็บในอุปกรณ์เคลื่อนที่จากการถูกเข้าถึงโดยไม่ได้รับอนุญาต ผู้ประกอบธุรกิจควรจัดให้มีการเข้ารหัสข้อมูล (data encryption) หรือเข้ารหัสไดรฟ์ข้อมูลเพิ่มเติมสำหรับกรณีที่ไม่สามารถทำ remote wipe-out ได้

ลำดับ	คำถาม	คำตอบ
5. <u>การใช้บริการ cloud computing</u>		
5.1	ขอให้ระบุนิยามของ cloud computing เพิ่มเติม เพื่อความเข้าใจในคำจำกัดความที่ตรงกัน	ผู้ประกอบธุรกิจสามารถประเมินลักษณะการให้บริการว่าเป็น cloud computing หรือไม่ โดยพิจารณาจากนิยามของหน่วยงาน National Institute of Standards and Technology (NIST)[1] (ต้องมีลักษณะครบทั้ง 5 จึงจะเข้าองค์ประกอบ) 1. On-demand self-service : ผู้ใช้บริการสามารถกำหนด computing capabilities เช่น server time หรือ network storage ได้เอง โดยไม่จำเป็นต้องพึ่งพาผู้ให้บริการ 2. Broad network access : สามารถเข้าถึงระบบได้หลายช่องทาง เช่น smartphone tablet หรือ personal computer 3. Resource pooling : ผู้ใช้บริการหลายรายใช้งาน computing resource เดียวกัน 4. Rapid elasticity : ผู้ใช้บริการสามารถปรับแต่ง computing capabilities ให้เหมาะสมกับ scale ทางธุรกิจได้ด้วยตนเอง 5. Measured service : การใช้บริการ (resource usage) ต้องสามารถวัด / ควบคุม / รายงานผลการใช้งานแก่ผู้ใช้บริการได้
5.2	กรณีที่ผู้ประกอบธุรกิจใช้บริการ cloud computing มาก่อนที่สำนักงานจะปรับปรุงหลักเกณฑ์ใหม่ แล้วพบว่าข้อกำหนดเกี่ยวกับการใช้งานยังไม่เป็นไปตามหลักเกณฑ์ดังกล่าว ต้องดำเนินการอย่างไร	ผู้ประกอบธุรกิจต้องกำหนดให้ cloud provider ติดตามหลักเกณฑ์ของสำนักงาน พร้อมทั้งจัดให้มีข้อกำหนดเกี่ยวกับการใช้งานให้เป็นไปตามหลักเกณฑ์ใหม่ของสำนักงาน ทั้งนี้ ผู้ประกอบธุรกิจมีเวลาเตรียมความพร้อม 1 ปีนับจากวันที่ประกาศกำหนด

[1] http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

ลำดับ	คำถาม	คำตอบ
5.3	ในการใช้บริการ cloud computing ผู้ประกอบธุรกิจต้องปฏิบัติตามหลักเกณฑ์ outsourcing ของสำนักงานหรือไม่	การใช้บริการ cloud computing ไม่จัดเป็นการใช้บริการ outsourcing ทั้งนี้ ให้ผู้ประกอบธุรกิจปฏิบัติให้เป็นไปตามแนวทางปฏิบัติของสำนักงานในส่วนของการใช้บริการ cloud computing
5.4	การใช้บริการประเภท software as a service (SAAS) บางประเภท เช่น facebook ของบริษัท หรือการ upload ข้อมูลทางธุรกิจขึ้น youtube ผู้ประกอบธุรกิจต้องปฏิบัติตามหลักเกณฑ์ของสำนักงานมากน้อยเพียงใด	หากผู้ประกอบธุรกิจใช้บริการ cloud computing โดยนำข้อมูลหรือระบบงานที่มีความสำคัญขึ้นสู่ cloud ผู้ประกอบธุรกิจต้องปฏิบัติให้เป็นไปตามแนวทางปฏิบัติของสำนักงานในส่วนของการใช้บริการ cloud computing
5.5	หากผู้ประกอบธุรกิจใช้บริการ cloud computing สำหรับระบบงานทั่วไปที่ไม่สำคัญ เช่น ระบบใบลาพนักงาน ผู้ให้บริการ cloud computing ต้องได้รับมาตรฐาน ISO27001 version ล่าสุดหรือไม่	กรณีการให้บริการระบบงานที่ไม่สำคัญ cloud provider อาจไม่จำเป็นต้องได้รับมาตรฐานการรับรองความมั่นคงปลอดภัยของระบบสารสนเทศในระดับสากลก็ได้
5.6	กรณีผู้ให้บริการ cloud computing จัดให้ผู้ให้บริการรายอื่นรับดำเนินการช่วง (subcontract of cloud provider) ผู้ประกอบธุรกิจต้องปฏิบัติตามหลักเกณฑ์อย่างไร	ผู้ประกอบธุรกิจต้องควบคุมดูแลให้ผู้ให้บริการดังกล่าวจัดให้มีข้อกำหนดในการใช้บริการ cloud computing ต่อจากผู้ให้บริการรายอื่น (sub cloud) อย่างชัดเจน โดยอย่างน้อยควรมีเงื่อนไขให้ผู้ให้บริการต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้นจากการกระทำหรือการดำเนินการใด ๆ ของผู้ให้บริการรายอื่นเสมือนเป็นส่วนหนึ่งของผู้ให้บริการ ทั้งนี้ คุณสมบัติด้านความปลอดภัยของผู้ให้บริการรายอื่นจะต้องเทียบเท่าผู้ให้บริการหรือเป็นไปตามมาตรฐานสากล
5.7	กรณีที่ผู้ประกอบธุรกิจใช้บริการผ่านตัวแทนจัดจำหน่าย (cloud distributor) ของผู้ให้บริการ cloud computing (cloud provider) ถือเป็นการ sub cloud หรือไม่ และ	กรณีดังกล่าว cloud distributor เป็นเพียงผู้จัดหาระบบ cloud computing จึงไม่จัดเป็นการ sub cloud ดังนั้น cloud distributor จึงไม่ต้องได้รับมาตรฐานการรับรองความปลอดภัย

ลำดับ	คำถาม	คำตอบ
	cloud distributor ต้องได้รับมาตรฐานการรับรองความปลอดภัยด้านสารสนเทศในระดับสากล (เช่น ISO27001) ด้วยหรือไม่	ด้านสารสนเทศในระดับสากล อย่างไรก็ดี cloud provider ที่ cloud distributor จัดหาให้ยังคงต้องได้รับมาตรฐานการรับรองความปลอดภัยด้านสารสนเทศดังกล่าว
5.8	การใช้บริการ cloud computing แบบ private cloud[2] เข้าข่ายต้องปฏิบัติตาม guideline ซึ่งว่าด้วยข้อกำหนดกรณีที่ผู้ประกอบธุรกิจใช้บริการ cloud computing ด้วยหรือไม่	เฉพาะกรณีที่ cloud computing นั้นเป็น private cloud ซึ่งผู้ประกอบธุรกิจเป็นเจ้าของและบริหารจัดการระบบทั้งหมดแต่เพียงผู้เดียว ให้งดเว้นการปฏิบัติตาม guideline ในหัวข้อดังกล่าวได้
5.9	ผู้ให้บริการ cloud computing ถือเป็นผู้รับดำเนินการที่ต้องปฏิบัติตามประกาศแนวปฏิบัติฯ ในเรื่อง IT outsourcing ด้วยหรือไม่	ผู้ให้บริการ cloud computing ถือเป็นผู้ให้เช่าใช้ software / platform / infrastructure แก่ผู้ประกอบธุรกิจผ่าน internet โดยที่ผู้ประกอบธุรกิจยังคงเป็นผู้ปฏิบัติงานหลักซึ่งต้องใช้ดุลพินิจและการตัดสินใจในระบบงานนั้น จึงไม่ต้องปฏิบัติตามประกาศแนวปฏิบัติฯ ในเรื่อง IT outsourcing อย่างไรก็ดี ผู้ประกอบธุรกิจยังคงมีหน้าที่ต้องปฏิบัติตามประกาศแนวปฏิบัติฯ ในเรื่อง cloud computing กรณีที่มีการใช้บริการดังกล่าว
5.10	ในการตรวจสอบผู้ให้บริการ cloud computing นั้น ข้อมูลบางอย่างที่กำหนดไว้ เช่น ฐานะทางการเงิน, มาตรฐานความปลอดภัยด้านเครือข่าย, ISO, capacity หรืออื่น ๆ ถ้าผู้ให้บริการไม่ได้เปิดเผย หรือบริษัทไม่สามารถที่จะตรวจสอบได้ เช่น SETTRADE หรือ Microsoft ต้องทำอย่างไร	ผู้ประกอบธุรกิจอาจใช้กระบวนการหรือข้อมูลอื่นทดแทนเพื่อให้สามารถมั่นใจได้ว่าผู้ให้บริการของตนมีระบบการรักษาความมั่นคงปลอดภัยของข้อมูลอย่างเพียงพอ รวมถึงมีศักยภาพและความพร้อมในการให้บริการได้อย่างต่อเนื่อง
5.11	ข้อกำหนดในเรื่องให้ทบทวนคุณสมบัติของผู้ให้บริการอย่างสม่ำเสมอตามที่กำหนดในประกาศแนวปฏิบัติฯ นั้น เฉพาะขั้นตอน	ผู้ประกอบธุรกิจควรกำหนดให้นโยบายการใช้งาน cloud computing ครอบคลุมถึงขั้นตอนและระยะเวลาในการทบทวนคุณสมบัติ

[2] นิยาม private cloud จากหน่วยงาน National Institute of Standards and Technology (NIST) หมายถึง “The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.”

ลำดับ	คำถาม	คำตอบ
	การจัดซื้อจัดจ้าง หรือขั้นตอนการประเมิน vendor เพียงพอแล้วหรือไม่ ถ้าไม่เพียงพอ ความถี่ในการตรวจสอบต้องเป็นอย่างไร	ของผู้ให้บริการตามที่เห็นสมควรและเหมาะสมกับลักษณะการประกอบธุรกิจของตน เพื่อให้มั่นใจได้ว่าผู้ให้บริการของตนยังคงมีคุณสมบัติตามที่ผู้ประกอบธุรกิจได้ประเมินไว้ตั้งแต่ต้น และยังคงมีศักยภาพที่จะให้บริการได้อย่างต่อเนื่อง
5.12	ขอคำแนะนำเกี่ยวกับการตรวจสอบฐานะทางการเงินที่เพียงพอของผู้ให้บริการ	ผู้ประกอบธุรกิจอาจพิจารณาได้จากมูลค่าส่วนของผู้ถือหุ้น กำไรสุทธิจากการดำเนินงาน หรือความสามารถในการชำระหนี้ของผู้ให้บริการ เป็นต้น ทั้งนี้ ความเพียงพอในด้านฐานะทางการเงินของผู้ให้บริการนั้น ให้เป็นตามที่ผู้ประกอบธุรกิจเห็นสมควร
5.13	การเลือกผู้ให้บริการ cloud computing ควรใช้หลักเกณฑ์อย่างไร	ผู้ประกอบธุรกิจอาจจัดทำ due diligence โดยประเมินจากการที่ผู้ให้บริการได้รับมาตรฐานการรับรองความมั่นคงปลอดภัยด้านสารสนเทศหรือมาตรฐานที่เกี่ยวข้องกับ cloud computing ในระดับสากล เช่น ISO27017 / 27018 CSA STAR รวมถึงมาตรฐานอื่นๆ ซึ่งเป็นที่ยอมรับโดยสากล เพื่อให้มั่นใจได้ว่าผู้ให้บริการได้จัดให้มีกระบวนการรักษาความมั่นคงปลอดภัยด้านระบบสารสนเทศที่ครบถ้วนถูกต้อง และได้รับการตรวจสอบจาก independent auditor อย่างเหมาะสม
5.14	ข้อกำหนดว่าด้วยการทำข้อตกลง / สัญญาระหว่างบริษัทกับผู้ให้บริการ cloud computing ให้ใช้บังคับกับข้อตกลง / สัญญาเฉพาะที่ทำหลังประกาศ IT ใหม่มีผลใช้บังคับเท่านั้นใช่หรือไม่	ผู้ประกอบธุรกิจที่ใช้บริการ cloud computing ภายหลังประกาศ IT ใหม่มีผลใช้บังคับ จะต้องจัดทำข้อตกลง / สัญญา ให้เป็นไปตามที่ประกาศกำหนด สำหรับผู้ประกอบธุรกิจที่ใช้บริการ cloud computing ก่อนประกาศมีผลใช้บังคับ ให้พิจารณาปรับปรุงข้อตกลง / สัญญา ให้เป็นไปตามที่ประกาศกำหนดภายใน 1 ปีนับจากวันที่

ลำดับ	คำถาม	คำตอบ
		ประกาศ IT ใหม่มีผลใช้บังคับ (คือภายในวันที่ 1 กันยายน 2561)
6. การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร (human resource security)		
6.1	บุคคลภายนอกที่ปฏิบัติงาน โดยมีการเข้าถึงข้อมูลหรือระบบงานภายในองค์กร หมายความรวมถึงผู้ให้บริการที่เข้ามา on-site เป็นครั้งคราวด้วยหรือไม่	หมายความรวมถึงผู้ให้บริการที่เข้ามา on-site เป็นครั้งคราวด้วย หากมีการเข้าถึงข้อมูลหรือระบบงานภายในองค์กร
6.2	ในการสร้างความตระหนักรู้แก่บุคคลภายนอกที่ปฏิบัติงานโดยมีการเข้าถึงข้อมูลหรือระบบงานภายในองค์กร ผู้ประกอบธุรกิจสามารถใช้วิธีการส่ง e-mail เพื่อแจ้ง policy แทนได้หรือไม่	ผู้ประกอบธุรกิจอาจสื่อสารให้บุคคลภายนอกซึ่งปฏิบัติงานที่ต้องเข้าถึงข้อมูลหรือระบบงานภายในองค์กร โดยวิธีการแจ้งนโยบายและแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของผู้ประกอบธุรกิจผ่านช่องทางสื่อสารด้านอิเล็กทรอนิกส์ เช่น e-mail หรือแสดงข้อความ pop-up เมื่อใช้งานระบบก็ได้ โดยกำหนดวิธีให้บุคคลภายนอกดังกล่าวลงนามรับทราบนโยบายและแนวทางปฏิบัติด้วย
6.3	จากแนวทางปฏิบัติที่กำหนดให้ผู้ประกอบธุรกิจต้องสื่อสารให้พนักงานละเว้นการใช้งานระบบสารสนเทศในลักษณะที่อาจก่อให้เกิดความเสียหายต่อผู้ประกอบธุรกิจ นั้น นอกเหนือจากการกำหนดนโยบายในเชิงยับยั้งดังกล่าว ผู้ประกอบธุรกิจสามารถกำหนดนโยบายในเชิงที่อนุญาตให้พนักงานใช้งานระบบสารสนเทศได้เป็นรายกรณี (case by case) ตามเงื่อนไขและข้อตกลงที่ให้พนักงานลงนามรับทราบได้หรือไม่ เช่น พนักงานสามารถตั้งค่าส่งต่อจดหมายอิเล็กทรอนิกส์แบบอัตโนมัติได้ แต่ต้องปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัยที่ระบุไว้ใน information security policy ขององค์กรและได้รับอนุมัติจากผู้มีอำนาจ เป็นต้น	ผู้ประกอบธุรกิจสามารถกำหนดนโยบายในลักษณะดังกล่าวได้

ลำดับ	คำถาม	คำตอบ
7. <u>การควบคุมการเข้ารหัสข้อมูล (cryptographic control)</u>		
7.1	การเข้ารหัสข้อมูล นอกจากจัดทำกับข้อมูลสำคัญที่รับส่งผ่านระบบเครือข่ายคอมพิวเตอร์แล้ว ต้องจัดทำกับข้อมูลสำคัญที่ถูกจัดเก็บอยู่ในสื่อบันทึกข้อมูล (storage media) ด้วยหรือไม่ หากมีมาตรการควบคุมจาก domain อื่น ๆ เช่น มีการควบคุม access control ที่ดี เป็นต้น สามารถทดแทนการเข้ารหัสข้อมูลสำคัญที่ถูกจัดเก็บอยู่ใน storage media ได้หรือไม่	ผู้ประกอบธุรกิจยังคงต้องจัดทำ เว้นแต่กรณีที่ผู้ประกอบธุรกิจจัดให้มีมาตรการควบคุมการเข้าถึงข้อมูลที่เป็นความลับหรือมีความสำคัญสูงอย่างมีประสิทธิภาพ มีการจัดเก็บสื่อบันทึกข้อมูลอย่างมั่นคงปลอดภัย และมีการเข้ารหัสไฟล์ข้อมูลรหัสผ่านอย่างรัดกุม ให้ถือว่ามีความเพียงพอต่อการปกป้องข้อมูลที่เป็นความลับหรือมีความสำคัญสูงแล้ว
7.2	การรับส่งจดหมายอิเล็กทรอนิกส์ (e-mail) ผ่านระบบเครือข่ายคอมพิวเตอร์ จำเป็นต้องเข้ารหัส e-mail ด้วยหรือไม่	หากผู้ประกอบธุรกิจจัดให้มีระบบการใส่รหัสผ่านสำหรับไฟล์ข้อมูลแนบ (attached file) ที่มีความสำคัญอย่างมั่นคงปลอดภัย ให้ถือว่าเพียงพอแล้ว
7.3	กรณีที่ผู้ประกอบธุรกิจจัดให้มีระบบการให้บริการเรียกข้อมูลส่วนตัวของลูกค้าในรูปแบบไฟล์ pdf ผ่านเครือข่ายอินเทอร์เน็ต จำเป็นต้องเข้ารหัสไฟล์ข้อมูล pdf ดังกล่าวหรือไม่	หากผู้ประกอบธุรกิจกำหนดให้ลูกค้าต้อง login เข้าสู่ระบบการให้บริการดังกล่าวด้วยรหัสผ่านที่มีความปลอดภัยก่อนใช้บริการเรียกข้อมูลดังกล่าว ให้ถือว่าเพียงพอแล้ว
7.4	ขอให้กำหนดความชัดเจนของประเภทข้อมูลที่เป็นความลับหรือมีความสำคัญเฉพาะข้อมูลในระดับที่มีความสำคัญสูง พร้อมยกตัวอย่างประเภทของข้อมูลที่ควรมีการควบคุมโดยการเข้ารหัสข้อมูล เพื่อให้เป็นมาตรฐานเดียวกัน	ผู้ประกอบธุรกิจควรดำเนินการจัดชั้นความลับของข้อมูลตามที่กำหนดในประกาศแนวปฏิบัติฯ หัวข้อ 4.2 เรื่อง asset classification ให้แล้วเสร็จก่อน จึงจะทราบว่าข้อมูลใดบ้างที่ควรได้รับการปกป้องด้วยการเข้ารหัสข้อมูล ทั้งนี้ การจัดชั้นความลับของข้อมูลควรยึดหลักผลกระทบที่เกิดขึ้นต่อลูกค้า การดำเนินธุรกิจ ชื่อเสียง ฐานะและผลการดำเนินงานของผู้ประกอบธุรกิจ หากข้อมูลดังกล่าวมีการรั่วไหล เช่น ข้อมูลการซื้อขาย / ข้อมูลการถือครองหลักทรัพย์ของลูกค้า
7.5	ขอให้ระบุขอบเขตของการ encrypt data ทั้งนี้ ต้องทำในระดับ database ด้วยหรือไม่	ประกาศแนวปฏิบัติฯ ไม่มีข้อกำหนดให้ผู้ประกอบธุรกิจต้องเข้ารหัสในระดับ database

ลำดับ	คำถาม	คำตอบ
		อย่างไรก็ดี เพื่อเป็นการป้องกันการเข้าถึงข้อมูลที่ถูกจัดเก็บใน database โดยไม่ได้รับอนุญาต ผู้ประกอบธุรกิจควรดำเนินการดังนี้ 1.) เข้ารหัสข้อมูลที่เกี่ยวกับบัญชีผู้ใช้งานและรหัสผ่านของผู้บริหารระบบฐานข้อมูล (database admin) 2.) เข้ารหัสฮาร์ดดิสก์ (full disk encryption) หรือพิจารณาใช้เทคโนโลยีอื่นใดที่ทำให้ไม่สามารถเรียกดูข้อมูลจากฮาร์ดดิสก์นั้นได้เมื่อนำไปต่อพ่วงกับเครื่องคอมพิวเตอร์อื่น
7.6	การ encrypt data รวมถึงการสื่อสารภายในองค์กรด้วยหรือไม่ และขอบเขตของการทำอยู่ในระดับใด เช่น client to server, server to server เป็นต้น ซึ่งหากรวมถึงภายในองค์กรอาจจะส่งผลกระทบถึง performance ของระบบได้	ประกาศแนวปฏิบัติฯ ไม่มีข้อกำหนดให้ผู้ประกอบธุรกิจต้องเข้ารหัสข้อมูลการสื่อสารภายในองค์กรทั้งหมด อย่างไรก็ดี ในกรณีที่เป็นการสื่อสารข้อมูลที่เป็นความลับหรือมีความสำคัญ ผู้ประกอบธุรกิจควรกำหนดให้มีการเข้ารหัสข้อมูลหรือมีมาตรการอื่นใดเพื่อป้องกันการเข้าถึงข้อมูลดังกล่าวโดยไม่ได้รับอนุญาต เช่น กำหนดให้มีการเข้ารหัสผ่านสำหรับไฟล์ข้อมูลแนบ (attached file) ซึ่งเป็นความลับหรือมีความสำคัญทุกครั้งก่อนจัดส่งผ่าน e-mail เป็นต้น
7.7	ขอทราบกรอบมาตรฐานการ encrypt data ขั้นต่ำของสำนักงาน	ผู้ประกอบธุรกิจควรจัดให้มีการเข้ารหัสข้อมูลด้วยวิธีการ (encryption algorithm) ที่สอดคล้องเหมาะสมกับระดับความเสี่ยงที่อาจเกิดขึ้นกับข้อมูลที่เป็นความลับหรือมีความสำคัญ รวมถึงเป็นไปตามมาตรฐานหรือ best practice ในปัจจุบัน
8. <u>การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม (physical and environmental security)</u>		
8.1	การจัดการอุปกรณ์บันทึกข้อมูล เช่น thumb drive และ external hard disk ไม่ให้วางไว้บนโต๊ะทำงานขณะที่ไม่ได้ใช้งาน	ผู้ประกอบธุรกิจอาจใช้วิธีสื่อสารนโยบายและแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยของระบบ IT ให้แก่พนักงาน

ลำดับ	คำถาม	คำตอบ
	เป็นเรื่องที่ควบคุมทางเทคนิคได้ยาก จะใช้การกำหนดเป็นข้อบังคับหรือประกาศให้พนักงานรับทราบและเป็นแนวทางปฏิบัติได้หรือไม่	เพื่อลงนามรับทราบ รวมถึงกำหนดบทลงโทษกรณีที่พนักงานไม่ปฏิบัติตามให้มีความเหมาะสมชัดเจน
8.2	การตรวจสอบหรือบำรุงรักษาสายเคเบิ้ลที่อยู่ในตึกเช่าหรือตึกเก่าควรทำอย่างไร จะต้องมีการ shield สายทั้งหมดหรือไม่ วัตถุประสงค์ของประกาศข้อ 7.2 นี้คืออะไร	วัตถุประสงค์ของข้อกำหนดในประกาศแนวปฏิบัติฯ ข้อ 7.2 มีไว้เพื่อป้องกันทรัพย์สินสารสนเทศประเภทอุปกรณ์ที่ใช้ประกอบการปฏิบัติงานสำคัญจากการสูญหาย เสียหาย ถูกโจรกรรม หรือเข้าถึงโดยไม่ได้รับอนุญาต ทั้งนี้เพื่อให้ระบบงานสำคัญสามารถดำเนินไปได้อย่างต่อเนื่องโดยในส่วนของมาตรการป้องกันสายเคเบิลที่เหมาะสมนั้น สำนักงานขอให้พิจารณาแนวทางในการดำเนินการดังต่อไปนี้ 1. สำหรับสายเคเบิลที่เดินผ่านพื้นที่ที่บริษัทไม่สามารถเข้าถึงอันเนื่องมาจากพื้นที่ดังกล่าวเป็นของผู้ให้เช่า ผู้ประกอบธุรกิจควรดำเนินการตามที่เห็นสมควรเพื่อป้องกันความเสียหายหรือการเสื่อมสภาพของสายเคเบิล เช่น ระบุในสัญญาเช่าพื้นที่โดยกำหนดว่า ผู้ให้เช่าต้องบำรุงรักษาพื้นที่ให้เช่าซึ่งรวมถึงสาธารณูปโภคที่เกี่ยวข้อง หรืออนุญาตให้ผู้เช่าดำเนินการแทนได้ตามรอบระยะเวลาที่เหมาะสม เป็นต้น 2. สำหรับสายเคเบิลที่อยู่ในพื้นที่ของบริษัทซึ่งผู้ประกอบธุรกิจสามารถเข้าถึง / บำรุงรักษาได้ ผู้ประกอบธุรกิจควรพิจารณาดำเนินการให้สายเคเบิลดังกล่าวอยู่ในพื้นที่มิดชิด ยากต่อการเข้าถึงโดยง่าย เช่น การเดินสายเคเบิลใต้พื้นที่ทำการของบริษัท (raised floor) การเดินสายเคเบิลบนฝ้าเพดานของอาคาร การปกป้องสายเคเบิลด้วยวิธีการร้อยท่อ flex / เดินราง

ลำดับ	คำถาม	คำตอบ
		สายเคเบิล หรือกำหนดให้บริเวณที่มีการเดินสายเคเบิลเป็นพื้นที่ควบคุม เป็นต้น
9. <u>การบันทึก จัดเก็บหลักฐานและติดตาม (logging and monitoring)</u>		
9.1	ผู้ประกอบธุรกิจต้องวิเคราะห์ log ทุกประเภทตามที่สำนักงานกำหนดให้จัดเก็บหรือไม่ ผู้ประกอบธุรกิจต้องใช้เครื่องมือที่ซับซ้อนสำหรับการวิเคราะห์ log เพื่อประมวลหาความสัมพันธ์ (correlation) หรือรูปแบบ (pattern) ของข้อมูล log หรือไม่	ผู้ประกอบธุรกิจต้องวิเคราะห์ log ทุกประเภทอย่างสม่ำเสมอ เพื่อให้สามารถติดตามความเสี่ยงที่อาจเกิดขึ้นกับระบบสารสนเทศในเชิงรุก (proactive) เช่น ความพยายามเข้าถึงหรือใช้งานระบบสารสนเทศที่ผิดปกติ ซึ่งจะช่วยให้สามารถเตรียมพร้อมรองรับความเสี่ยงดังกล่าวได้อย่างทันต่อเหตุการณ์ ทั้งนี้ ผู้ประกอบธุรกิจอาจใช้เครื่องมือหรือวิธีการวิเคราะห์ที่ไม่ซับซ้อนก็ได้ หากวิธีการดังกล่าวช่วยให้ติดตามความเสี่ยงได้อย่างเพียงพอและมีประสิทธิภาพ
9.2	กรณีที่ผู้ตรวจสอบ (auditor) เป็นผู้รวบรวม log ของผู้ประกอบธุรกิจไปวิเคราะห์ จะถือว่าผู้ประกอบธุรกิจได้จัดให้มีการวิเคราะห์ log แล้วหรือไม่	หากการตรวจสอบโดยผู้ตรวจสอบดังกล่าวสามารถติดตามความเสี่ยงที่อาจเกิดขึ้นกับระบบสารสนเทศในเชิงรุก (proactive) ได้อย่างเพียงพอและมีประสิทธิภาพ ให้ถือว่าผู้ประกอบธุรกิจมีการวิเคราะห์ log แล้ว
9.3	ในการจัดเก็บหลักฐานการเข้าถึงระบบฐานข้อมูล (authentication log) หากผู้ประกอบธุรกิจใช้บริการจากผู้ให้บริการภายนอก โดยมีเครื่องแม่ข่ายของระบบฐานข้อมูล (database server) อยู่ที่ผู้ให้บริการภายนอก และผู้ให้บริการภายนอกมีการว่าจ้างผู้ตรวจสอบภายนอก (external auditor) ให้ตรวจสอบการเข้าถึงระบบฐานข้อมูลของผู้ประกอบธุรกิจแล้ว ผู้ประกอบธุรกิจไม่ต้องจัดเก็บและติดตามวิเคราะห์ log ดังกล่าวได้หรือไม่	ผู้ประกอบธุรกิจต้องจัดเก็บและติดตามวิเคราะห์ log การเข้าถึงระบบฐานข้อมูลดังกล่าว เว้นแต่กรณีที่ผู้ประกอบธุรกิจได้จัดให้มีข้อกำหนดที่ทำให้มั่นใจว่าผู้ให้บริการภายนอกได้ให้ผู้ตรวจสอบภายนอกตรวจสอบ log การเข้าถึงระบบฐานข้อมูลของผู้ประกอบธุรกิจ และจัดให้มีการเปิดเผยผลการตรวจสอบให้ผู้ประกอบธุรกิจรับทราบ โดยผลการตรวจสอบดังกล่าวต้องมีรายละเอียดขั้นต่ำเกี่ยวกับบัญชีผู้ใช้งาน วันเวลาที่เข้าใช้งาน และความพยายามในการเข้าใช้งาน
9.4	traffic log หากหมายความถึง payload ในทางปฏิบัติอาจทำได้ยาก และกระทบ	ในการจัดเก็บหลักฐานบันทึกข้อมูลจราจรคอมพิวเตอร์ ผู้ประกอบธุรกิจอาจจัดเก็บเฉพาะ

ลำดับ	คำถาม	คำตอบ
	performance ของระบบอย่างมาก ขอให้ระบุขอบเขตของอุปกรณ์เครือข่ายที่สำคัญ และประเภทของอุปกรณ์เครือข่าย เช่น รวมถึง switch และ router ด้วยหรือไม่	ข้อมูลการเชื่อมต่ออุปกรณ์เครือข่ายที่สำคัญก็ได้ ทั้งนี้ อุปกรณ์เครือข่ายที่สำคัญ ได้แก่ อุปกรณ์เครือข่ายที่เกี่ยวข้องกับการเชื่อมต่อผ่านระบบงานที่สำคัญ เช่น switch, router หรือfirewall เป็นต้น
9.5	ผู้ประกอบธุรกิจยังคงต้องวิเคราะห์ log ในระบบงานที่กำหนดกฎ (rule) การใช้งานหรือกำหนดสิทธิการเข้าถึงระบบไว้อย่างชัดเจนแล้ว หรือไม่	ในกรณีที่ระบบงานกำหนดกฎการใช้งานหรือสิทธิการเข้าถึงระบบไว้อย่างชัดเจน ผู้ประกอบธุรกิจยังคงต้องจัดให้มีการวิเคราะห์ log ทั้งนี้ เพื่อให้มั่นใจได้ว่ากฎหรือสิทธิการเข้าถึงดังกล่าวยังสามารถควบคุมผู้ใช้งานได้อย่างปลอดภัยและมีประสิทธิภาพ
9.6	ขอรายละเอียดเพิ่มเติมเกี่ยวกับหลักฐานการใช้งานแฟ้มข้อมูล (audit log) หมายถึงแฟ้มข้อมูลทุกแฟ้ม แฟ้มข้อมูลสำคัญหรือ file server หากกำหนดในลักษณะ policy control (ไม่ใช่ system control) จะมีความเป็นไปได้ในทางปฏิบัติมากกว่า เช่น ให้บริษัทออกเกณฑ์ภายในให้พนักงานเก็บ file สำคัญไว้ใน server เป็นต้น นอกจากนี้ การจัดเก็บ audit log ในส่วนที่เรียกใช้ผ่านเครื่องคอมพิวเตอร์ส่วนบุคคลจะเป็นภาระมาก เนื่องจากต้องจัดเก็บนานถึง 6 เดือน	ผู้ประกอบธุรกิจต้องจัดเก็บหลักฐานการใช้งานแฟ้มข้อมูล (audit log) <u>เฉพาะที่เป็นแฟ้มข้อมูลสำคัญ</u>ของบุคลากรที่เป็น access person ตามประกาศสำนักงานคณะกรรมการ ก.ล.ต. ที่ นป. 1/2558 เรื่อง แนวทางปฏิบัติสำหรับการกำหนดนโยบาย มาตรการ และระบบงานที่เกี่ยวข้องกับการกระทำที่อาจมีความขัดแย้งทางผลประโยชน์กับลูกค้า ทั้งนี้ เพื่อให้สะดวกในการจัดเก็บ audit log ผู้ประกอบธุรกิจอาจกำหนดให้บุคลากรของตนจัดเก็บข้อมูลสำคัญไว้ใน server เท่านั้นก็ได้
9.7	database log ควรระบุขอบเขตว่าต้องจัดเก็บถึง level ใด เพื่อป้องกัน log มีขนาดใหญ่จนเกินไปซึ่งอาจกระทบกับ performance ของระบบงานได้	กรณีที่ผู้ประกอบธุรกิจจัดเก็บ log การเข้าใช้งานของผู้บริหารระบบฐานข้อมูล (database admin) ซึ่งมีรายละเอียดเกี่ยวกับชื่อบัญชีผู้ใช้งาน วันและเวลาที่เข้าใช้งาน จะถือว่าผู้ประกอบธุรกิจได้ปฏิบัติตามหลักเกณฑ์ของข้อกำหนดในส่วนนี้แล้ว
9.8	หลักฐานการใช้งาน internet ผ่านระบบเครือข่ายคอมพิวเตอร์ภายในของผู้ประกอบธุรกิจ (internet access log) ในกรณีที่เป็นการใช้งาน internet เพื่อเข้าถึงระบบซื้อขายภายนอก เช่น	ผู้ประกอบธุรกิจอาจพิจารณางดเว้นการจัดเก็บหลักฐาน full URL ได้ หากผู้ประกอบธุรกิจสามารถเรียกขอหลักฐานดังกล่าวจากผู้ให้บริการเมื่อมีความต้องการใช้งานมาใช้ร่วมกับข้อมูล

ลำดับ	คำถาม	คำตอบ
	ระบบ SETTRADE ในการจัดเก็บหลักฐานการใช้งานดังกล่าวควรยกเว้นการจัดเก็บข้อมูล “ที่อยู่ของเว็บไซต์ปลายทาง (full URL)” เนื่องจากผู้ให้บริการจะมีหน้าที่ในการจัดเก็บหลักฐานดังกล่าวอยู่แล้ว อีกทั้งหลักฐานการใช้งานส่วนอื่นที่ยังคงจัดเก็บอยู่น่าจะเพียงพอต่อการตรวจสอบ ทั้งนี้เพื่อให้การเข้าถึงบริการมีความรวดเร็ว อนึ่ง การเข้าถึงเว็บไซต์อื่น ๆ ที่ไม่เกี่ยวกับการซื้อขาย เห็นด้วยที่จะต้องจัดเก็บ full URL	หลักฐานประเภทอื่นๆ ที่ผู้ประกอบธุรกิจจัดเก็บจากการสื่อสารไปยังภายนอกองค์กรผ่าน firewall ของผู้ประกอบธุรกิจ เพื่อให้ได้มาซึ่งหลักฐานตามที่ประกาศแนวปฏิบัติฯ กำหนดอย่างครบถ้วนได้
9.9	กรณีที่เว็บไซต์ปลายทางใช้โปรโตคอลแบบ secure http (HTTPS) อาจทำให้เกิดต้นทุนในการจัดเก็บหลักฐานที่อยู่ของเว็บไซต์ปลายทาง (full URL) ตามที่สำนักงานกำหนดในส่วนของ internet access log	หากผู้ประกอบธุรกิจจัดให้มีแนวปฏิบัติในการจัดเก็บ internet access log ที่เป็นไปตามกฎหมาย พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์แล้ว ให้ถือว่าผู้ประกอบธุรกิจได้ปฏิบัติให้เป็นไปตามที่ประกาศแนวปฏิบัติฯ กำหนดอย่างครบถ้วน
9.10	ควรมีการกำหนดรายละเอียดระบบที่ต้องอ้างอิงเวลากับตลาดหลักทรัพย์ เพราะบริษัทมี server ระบบซื้อ/ขายมากกว่า 1 เครื่อง และไม่สามารถนำทุก server ไปอ้างอิงเวลาจากตลาดหลักทรัพย์ได้ทั้งหมด	ผู้ประกอบธุรกิจสามารถกำหนดให้ server ตัวอื่น ๆ ใช้เวลาอ้างอิงของ master server ที่เทียบเวลาโดยตรงกับตลาดหลักทรัพย์ทดแทนการกำหนดให้ server ทุกตัวใช้เวลาอ้างอิงของตลาดหลักทรัพย์ได้
9.11	บริษัทจะต้องจัดเก็บ application log ของ source IP และ destination IP รวมถึง full URL อย่างไรสำหรับระบบ trading system จึงจะเป็นไปตามความคาดหวังของสำนักงาน	ให้ผู้ประกอบธุรกิจจัดเก็บ source IP และ destination IP โดยจำแนกตามลักษณะการใช้งานของลูกค้าดังนี้ (พิจารณาประกอบกับรูปตามแผนภาพที่ 1 ในเอกสารแนบท้าย FAQ) 1. กรณีลูกค้าซื้อขายหลักทรัพย์ผ่านอุปกรณ์ที่ผู้ประกอบธุรกิจจัดไว้ภายในที่ทำการของผู้ประกอบธุรกิจ (เช่น desktop ในห้องค้า) 1.1 หากส่งคำสั่งผ่าน trading application ที่ผู้ประกอบธุรกิจพัฒนาขึ้น / จ้างพัฒนาหรือเช่าระบบของ vendor โดยที่ application ดังกล่าว

ลำดับ	คำถาม	คำตอบ
		host อยู่ในที่ทำการของผู้ประกอบธุรกิจ รวมถึงกรณีลูกค้าส่งคำสั่งผ่านพนักงาน IC ให้ผู้ประกอบธุรกิจจัดเก็บ private IP address ตามคู่ A-A' และ full URL ให้ครบถ้วน (ยกเว้นกรณี non web-based application ไม่ต้องจัดเก็บ full URL) 1.2 หากส่งคำสั่งผ่าน SETTRADE application หรือ application อื่นที่มิได้ host อยู่ในที่ทำการของผู้ประกอบธุรกิจ (โดยการเชื่อมต่อ internet) ผู้ประกอบธุรกิจต้องจัดเก็บ private IP address (source) ของเครื่องที่ทำการส่งคำสั่ง พร้อมกับจัดให้ผู้ให้บริการ application ดำเนินการจัดเก็บ public IP address ตามคู่ B-B' และ full URL ให้ครบถ้วน ทั้งนี้ เพื่อให้ผู้ประกอบธุรกิจมีข้อมูลเพียงพอยืนยันตัวตนของลูกค้าที่ส่งคำสั่งได้ 2. กรณีลูกค้าซื้อขายหลักทรัพย์ผ่านอุปกรณ์ที่มิใช่ทรัพย์สินของผู้ประกอบธุรกิจผ่าน internet (เช่น mobile phone / internet café / personal laptop เป็นต้น) 2.1 หากส่งคำสั่งผ่าน trading application ที่ผู้ประกอบธุรกิจพัฒนาขึ้น / จ้างพัฒนาหรือเช่าระบบของ vendor โดยที่ application ดังกล่าว host อยู่ในที่ทำการของผู้ประกอบธุรกิจ ให้ผู้ประกอบธุรกิจจัดเก็บ IP address ตามคู่ C-C' และ full URL (ยกเว้นกรณี mobile application หรือ non-web-based application ไม่ต้องจัดเก็บ full URL) ทั้งนี้ ผู้ประกอบธุรกิจควรจัดให้มีระบบงานที่จะช่วย correlate log ที่เกิดจาก trading application และ log จากคู่ C-C' เพื่อประโยชน์ในการยืนยันตัวตนลูกค้าผู้ส่งคำสั่ง (ดูตัวอย่าง log ได้จากตารางที่ 1 ในเอกสารแนบท้าย FAQ)

ลำดับ	คำถาม	คำตอบ
		2.2 หากส่งคำสั่งผ่าน SETTRADE application หรือ application อื่นที่มิได้ host อยู่ในที่ทำการของผู้ประกอบธุรกิจ ให้ดำเนินการเช่นเดียวกับข้อ 1.2 (ยกเว้นกรณี mobile application ไม่ต้องจัดเก็บ full URL)
9.12	บริษัทสามารถจัดเก็บ log ในส่วนของ order number ที่บริษัทสร้างขึ้นมาเองแทนการเก็บ SET order number ได้หรือไม่	ผู้ประกอบธุรกิจไม่สามารถจัดเก็บ order number ที่สร้างขึ้นเองได้ เนื่องจากการตรวจสอบตัวตนของลูกค้าผู้ส่งคำสั่ง สำนักงานจำเป็นต้องใช้ SET order number ประกอบการพิจารณาเพื่อให้สามารถตรวจสอบ log เทียบกับข้อมูลซื้อขายที่ได้จากระบบของ SET ซึ่งการใช้ข้อมูลแวดล้อมอื่น ๆ ในการพิจารณา เช่น order time หรือข้อมูล login / logout time อาจทำให้การตรวจสอบมีความคลาดเคลื่อนได้
9.13	ข้อมูล log ตามประกาศ อาจไม่สามารถจัดเก็บทั้งหมดให้อยู่ใน log เดียวกันได้ เนื่องจากในทางปฏิบัติ log ของแต่ละอุปกรณ์จะจัดเก็บแยกกัน เช่น firewall, load balancer, proxy server, web server และ application server	ผู้ประกอบธุรกิจสามารถจัดเก็บ log แยกกันในแต่ละอุปกรณ์ได้ โดยควรจัดให้มีระบบงานที่ช่วยให้ correlate log ระหว่างอุปกรณ์เพื่อประโยชน์ในการจัดส่งข้อมูลประกอบการพิจารณาตรวจสอบตัวตนของลูกค้าผู้ส่งคำสั่งเมื่อสำนักงานร้องขอ
9.14	Internet access log หมายถึงหลักฐานการใช้งานอินเตอร์เน็ตสำหรับพนักงานหรือบุคคลภายนอก (ลูกค้า) ที่เข้ามาใช้งานอินเตอร์เน็ตของบริษัท	Internet access log หมายถึงหลักฐานที่เกิดจากการใช้งาน internet ผ่านอุปกรณ์และโครงสร้างพื้นฐานของผู้ประกอบธุรกิจ ซึ่งรวมถึงการใช้งานทั้งหมดจากพนักงานและบุคคลภายนอก
10. <u>การจัดเก็บหลักฐานการติดต่อสนทนาผ่านช่องทางอิเล็กทรอนิกส์ (electronic messaging)</u>		
10.1	electronic messaging ครอบคลุมถึงอะไรบ้าง ต้องจัดเก็บเนื้อหาอะไร และจัดเก็บเฉพาะกรณีผู้ติดต่อกับลูกค้าได้หรือไม่	electronic messaging คือ การรับส่งข้อมูลสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์ เช่น การสนทนาโดยใช้จดหมายอิเล็กทรอนิกส์ (e-mail) โปรแกรมสนทนาผ่านระบบอิเล็กทรอนิกส์ (instant messaging) และระบบเครือข่ายสังคมออนไลน์ (social networking)

ลำดับ	คำถาม	คำตอบ
		เป็นต้น โดยต้องจัดเก็บทั้งเนื้อหาการสนทนาและการรับส่งข้อมูลสารสนเทศทั้งหมดสำหรับบุคคลที่เป็น access person ตามประกาศสำนักงานคณะกรรมการ ก.ล.ต. ที่ นป. 1/2558 เรื่อง แนวทางปฏิบัติสำหรับการกำหนดนโยบาย มาตรการ และระบบงานที่เกี่ยวกับการกระทำที่อาจมีความขัดแย้งทางผลประโยชน์กับลูกค้า
10.2	กรณีเกิดเหตุฉุกเฉิน การใช้จดหมายอิเล็กทรอนิกส์จากผู้ให้บริการโดยไม่เสียค่าบริการ (free e-mail) โดยส่งสำเนา (carbon copy : cc) ไปที่องค์กร การ cc กลับไปที่องค์กรสามารถทดแทนการจัดเก็บหลักฐาน e-mail ทั้งฉบับได้หรือไม่	ในกรณีที่เกิดเหตุฉุกเฉินซึ่งส่งผลกระทบต่อการใช้งานระบบ e-mail ผู้ประกอบธุรกิจสามารถจัดเก็บหลักฐาน e-mail ในลักษณะดังกล่าวได้
10.3	กรณี e-mail ให้จัดเก็บเฉพาะของผู้ที่ทำหน้าที่ติดต่อกับลูกค้าเท่านั้นใช่หรือไม่ และบริษัทต้องจัดเก็บ content ด้วยหรือไม่ หากต้องจัดเก็บทั้งองค์กรจะทำให้บริษัทต้องมีการลงทุนเพิ่ม หรือกำหนดให้บริษัทจัดเก็บเฉพาะ e-mail ของบุคคลที่บริษัทพิจารณาแล้วเห็นว่าสามารถเข้าถึงข้อมูลภายในในแต่ละด้าน (“access person”) เท่านั้น	เพื่อให้มีบันทึกหลักฐานเพียงพอต่อการตรวจสอบ ให้ผู้ประกอบธุรกิจจัดเก็บ e-mail ทั้งฉบับ โดยอาจจัดเก็บเฉพาะ access person ก็ได้ ทั้งนี้ ขอบเขตของ access person ให้พิจารณาจากประกาศสำนักงานคณะกรรมการ ก.ล.ต. ที่ นป. 1/2558 เรื่อง แนวทางปฏิบัติสำหรับการกำหนดนโยบาย มาตรการ และระบบงานที่เกี่ยวกับการกระทำที่อาจมีความขัดแย้งทางผลประโยชน์กับลูกค้า
10.4	กรณีที่ระบบ instant messaging บางระบบ เช่น ระบบ chat ใน Lotus Note หรือ Bloomberg ไม่สามารถบันทึกและจัดเก็บหลักฐานการสนทนาได้ ผู้ประกอบธุรกิจสามารถใช้ระบบงานดังกล่าวได้หรือไม่	สามารถใช้ได้เฉพาะกรณีที่บุคคลผู้ใช้งานไม่จัดเป็น access person ตามที่ระบุในประกาศสำนักงานคณะกรรมการ ก.ล.ต. ที่ นป. 1/2558 เรื่อง แนวทางปฏิบัติสำหรับการกำหนดนโยบาย มาตรการ และระบบงานที่เกี่ยวกับการกระทำที่อาจมีความขัดแย้งทางผลประโยชน์กับลูกค้า
10.5	electronic messaging log ที่ให้เก็บนั้นเฉพาะการสื่อสารกับภายนอกองค์กรเท่านั้นหรือไม่	ผู้ประกอบธุรกิจต้องจัดเก็บหลักฐานการรับส่งข้อมูลสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์ (electronic messaging) ของ

ลำดับ	คำถาม	คำตอบ
		บุคลากรที่เป็น access person ตามประกาศแนวปฏิบัติว่าด้วยแนวทางปฏิบัติสำหรับการกำหนดนโยบาย มาตรการ และระบบงานที่เกี่ยวข้องกับการกระทำที่อาจมีความขัดแย้งทางผลประโยชน์กับลูกค้า โดยให้จัดเก็บทั้งการสื่อสารภายในและภายนอกองค์กร
11. การบริหารจัดการช่องโหว่ทางเทคนิค (technical vulnerability management)		
11.1	การกำหนดให้ผู้ประกอบธุรกิจควรมีการประเมินความเสี่ยงของโปรแกรมเพื่อปิดช่องโหว่ (patches) ก่อนดำเนินการติดตั้งเพื่อทดสอบและประเมินผลกระทบที่อาจเกิดจากโปรแกรมดังกล่าว อาจทำให้ขัดแย้งกับแนวปฏิบัติที่ว่า ผู้ประกอบธุรกิจควรจัดให้มีการปิดช่องโหว่ที่พบโดยไม่ชักช้า หากการประเมินและทดสอบดังกล่าวใช้ระยะเวลาในการดำเนินการที่ค่อนข้างนาน	หากผู้ประกอบธุรกิจได้ทำการประเมินความเสี่ยงหลังจากที่พบช่องโหว่ในระบบแล้วว่าการติดตั้ง patches ทันทีอาจก่อให้เกิดความผิดพลาดต่อระบบได้ ให้ผู้ประกอบธุรกิจดำเนินการทดสอบโปรแกรมดังกล่าวโดยใช้ระยะเวลาตามที่จำเป็นเพื่อให้มั่นใจได้ว่าโปรแกรมที่จะดำเนินการติดตั้งนั้นไม่สร้างความเสียหายต่อระบบเพิ่มเติม โดยหาก patches ดังกล่าวผ่านการทดสอบแล้ว ให้ผู้ประกอบธุรกิจติดตั้ง patches โดยไม่ชักช้า นอกจากนี้ เพื่อเป็นการปิดความเสี่ยงที่อาจเกิดขึ้นจากช่องโหว่ในระหว่างที่ patches ดังกล่าวยังไม่ผ่านการทดสอบ ผู้ประกอบธุรกิจอาจใช้วิธีการอื่นในการปิดความเสี่ยงได้ เช่น การติดตั้ง firewall เป็นต้น
12. การทดสอบการเจาะระบบ (penetration test)		
12.1	ควรกำหนดขอบเขตการจัดทำ penetration test อย่างไร	ผู้ประกอบธุรกิจต้องประเมินความเสี่ยงของระบบงานที่สำคัญ โดยอาจพิจารณาจากการวิเคราะห์ผลกระทบทางธุรกิจ (business impact analysis) ทั้งนี้ กรณีระบบงานที่มีผลกระทบสูง ผู้ประกอบธุรกิจต้องจัดให้มีการทดสอบอย่างเข้มงวด เพื่อทราบถึงช่องโหว่ของระบบ (vulnerability scanning) และการใช้ประโยชน์จากช่องโหว่ (exploitation test) ทั้งนี้ ผู้ประกอบธุรกิจต้องจัดให้มีมาตรการ

ลำดับ	คำถาม	คำตอบ
		ควบคุมเพื่อให้กระบวนการทดสอบ ส่งผลกระทบต่อการปฏิบัติงานน้อยที่สุด
12.2	ผู้จัดทำ penetration test เป็นบุคลากรภายในองค์กร ได้หรือไม่	สามารถกระทำได้ ทั้งนี้ บุคลากรดังกล่าวต้องมีความรู้ความสามารถ และมีความเป็นอิสระจากฝ่ายเทคโนโลยีสารสนเทศ เช่น บุคลากรด้าน IT จากบริษัทแม่ของผู้ประกอบธุรกิจ / ผู้เชี่ยวชาญด้านการเจาะระบบจากภายนอก
12.3	ในกรณีที่ระบบซื้อขายของบริษัทหลักทรัพย์เชื่อมโยงกับระบบของ SETTRADE ใครเป็นผู้จัดทำ penetration test	SETTRADE เป็นผู้จัดทำ ทั้งนี้ ผู้ประกอบธุรกิจอาจกำหนดให้เป็นข้อกำหนดในสัญญากับ SETTRADE ได้
12.4	ผู้ทดสอบเจาะระบบ (penetration test) ต้องมีคุณสมบัติอย่างไร	ผู้ทดสอบดังกล่าวต้องมีความเป็นอิสระจากฝ่ายเทคโนโลยีสารสนเทศ รวมถึงสามารถดำเนินการทดสอบเจาะระบบโดยครอบคลุมจุดเสี่ยงที่สำคัญ 10 อันดับล่าสุดตามการจัดอันดับความเสี่ยงของ web application จากองค์กร OWASP (The Open Web Application Security Project) สำหรับคุณสมบัติในส่วนอื่นของผู้ทดสอบ ให้เป็นตามที่ผู้ประกอบธุรกิจเห็นสมควร
12.5	ในกรณีที่บริษัทใช้บริการระบบ / โปรแกรมจากผู้ให้บริการ (vendor) บริษัทสามารถให้ vendor จัดทำ penetration test ระบบดังกล่าว และนำส่งผลต่อสำนักงานได้หรือไม่	ผู้ประกอบธุรกิจสามารถใช้ผลการจัดทำ penetration test ของ vendor ได้ในกรณีที่ผู้ประกอบธุรกิจนำระบบ / โปรแกรมที่เป็นผลิตภัณฑ์สำเร็จรูปแบบ physical / virtual appliance มาใช้งาน โดยที่ไม่สามารถดัดแปลงหรือแก้ไขผลิตภัณฑ์ได้เอง และต้องปฏิบัติตามเงื่อนไขการใช้งานของผลิตภัณฑ์นั้นเพื่อป้องกันผลกระทบที่อาจเกิดต่อระบบการรักษาความปลอดภัยของผลิตภัณฑ์ดังกล่าว รวมถึงเมื่อนำผลิตภัณฑ์มาเชื่อมต่อกับระบบและเครือข่ายของผู้ประกอบธุรกิจแล้ว จะไม่ก่อให้เกิดช่องโหว่เพิ่มเติมจาก environment หรือ operation ของ

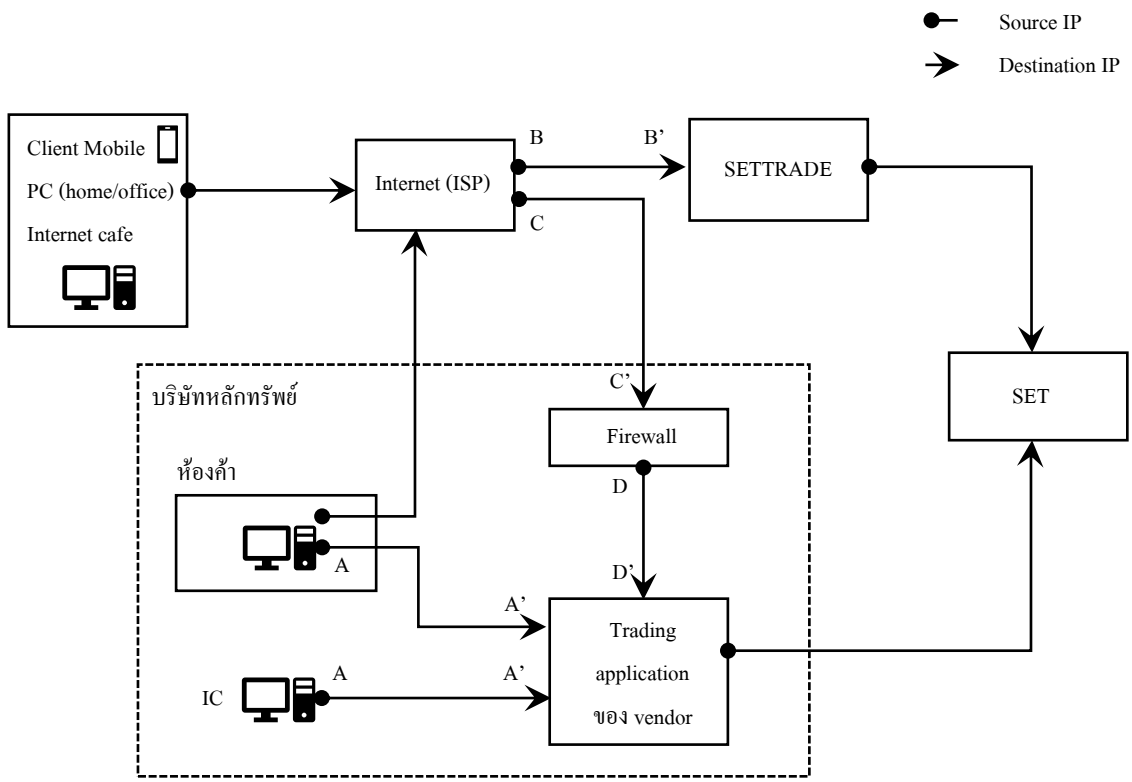
ลำดับ	คำถาม	คำตอบ
		ผู้ประกอบธุรกิจ ซึ่งจะส่งผลให้การทำ penetration test นั้นไม่ถูกต้อง
13. การตรวจสอบระบบสารสนเทศ (information systems audit)		
13.1	จากแนวทางปฏิบัติที่กำหนดให้ผู้ประกอบธุรกิจกำหนดขอบเขตการตรวจสอบทางเทคนิค (technical audit test) ให้ครอบคลุมจุดเสี่ยงที่สำคัญและต้องควบคุมการตรวจสอบดังกล่าวไม่ให้กระทบต่อการปฏิบัติงานตามปกติ หากผู้ประกอบธุรกิจจัดให้มีการทำ pre-test ก่อนการวางระบบ จะถือว่าเพียงพอแล้วหรือไม่	ในการจัดทำ technical audit test ผู้ประกอบธุรกิจอาจใช้วิธีการทำ pre-test ก่อนการวางระบบได้ ทั้งนี้ ต้องเป็นการจัดทำ pre-test ทางเทคนิคบนเครื่องทดสอบเท่านั้น
14. การรักษาความมั่นคงปลอดภัยด้านการสื่อสารข้อมูลสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์ (communications security)		
14.1	ผู้ประกอบธุรกิจต้องดำเนินการอย่างไรในกรณีที่มีบุคลากรไม่เพียงพอที่จะแบ่งแยกหน้าที่ความรับผิดชอบระหว่าง network administrator และ computer administrator ได้	ในระยะแรกผู้ประกอบธุรกิจอาจจัดให้มีมาตรการหรือวิธีการควบคุมอื่นใดที่แสดงให้เห็นได้ว่าสามารถแบ่งแยกหน้าที่ความรับผิดชอบดังกล่าวได้อย่างมีประสิทธิภาพ เช่น จัดให้มีการบันทึก จัดเก็บหลักฐาน (log) การปฏิบัติงานของบุคลากรผู้ปฏิบัติหน้าที่ network administrator และ computer administrator รวมทั้งจัดให้มีการติดตามวิเคราะห์หลักฐานดังกล่าวอย่างสม่ำเสมอโดยบุคคลที่เป็นอิสระจากผู้ปฏิบัติหน้าที่ network administrator และ computer administrator เป็นต้น
14.2	ในการจัดให้พนักงานและผู้ให้บริการภายนอกทำสัญญารักษาความลับหรือไม่เปิดเผยข้อมูลที่มีความสำคัญ ผู้ประกอบธุรกิจสามารถกำหนดให้ผู้ให้บริการภายนอกลงนามในสัญญาโดยผู้มีอำนาจลงนาม ขณะที่	ในการลงนามในสัญญารักษาความลับหรือไม่เปิดเผยข้อมูลที่มีความสำคัญ ผู้ประกอบธุรกิจอาจดำเนินการดังนี้ 1. กรณีพนักงาน อาจลงนามในเอกสารรักษาความลับก่อนเริ่มปฏิบัติงานได้

ลำดับ	คำถาม	คำตอบ
	พนักงานลงนามในเอกสารการรักษาความลับเมื่อแรกเข้า ได้หรือไม่ นอกจากนี้ ในการขออนุญาตเข้าถึงข้อมูลหรือกำหนดสิทธิการเข้าถึงข้อมูล สามารถใช้วิธีการอนุมัติทางอิเล็กทรอนิกส์ผ่านระบบได้หรือไม่	2. กรณีผู้ให้บริการภายนอก อาจจัดให้ผู้มีอำนาจลงนามเป็นผู้ลงนามได้ ผู้ประกอบธุรกิจสามารถทำได้ หากจัดให้มีกระบวนการที่สามารถพิสูจน์ตัวตนของผู้ขออนุญาต
14.3	การควบคุมป้องกัน network port (outlet) ควรทำในพื้นที่ใดบ้าง และควรใช้การป้องกันในรูปแบบใด	ผู้ประกอบธุรกิจควรจัดให้มีการควบคุมป้องกัน network port (outlet) ด้วยวิธีการและรูปแบบที่เหมาะสมกับสภาพความเสี่ยงของพื้นที่นั้น ๆ (risk-based approach) โดยในกรณีที่ผู้ประกอบธุรกิจพิจารณาแล้วว่าพื้นที่ดังกล่าวมีความเสี่ยงสูง เช่น พื้นที่ที่บุคคลภายนอกสามารถเข้าถึงได้และผู้ประกอบธุรกิจไม่มีมาตรการอื่นใดทดแทนที่จะช่วยป้องกันการเชื่อมต่อ network port (outlet) จากผู้ไม่ประสงค์ดี ผู้ประกอบธุรกิจอาจพิจารณาจำกัดการเชื่อมต่อหรือเปิดให้เชื่อมต่อเท่าที่จำเป็นเท่านั้น
15. <u>การใช้บริการระบบสารสนเทศจากผู้รับดำเนินการ (IT outsourcing)</u>		
15.1	จากแนวปฏิบัติที่กำหนดให้ผู้ให้บริการภายนอกต้องกำหนดแผนรองรับกรณีเกิดเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (<u>incident response policy</u>) ให้สอดคล้องกับแผนของผู้ประกอบธุรกิจ รวมทั้งกำหนดหน้าที่ความรับผิดชอบของผู้ให้บริการภายนอกในการกู้คืนระบบงานให้เป็นไปตามข้อตกลงที่ได้กำหนดไว้ ผู้ประกอบธุรกิจสามารถจัดให้มีกลไกอื่นเพื่อลดความเสี่ยงดังกล่าวได้หรือไม่ เช่น จัดให้มีการ due diligence ผู้ให้บริการโดยประเมินว่า	ผู้ประกอบธุรกิจสามารถกำหนดวิธีการดังกล่าวเป็นการทดแทนได้

ลำดับ	คำถาม	คำตอบ
	incident response policy ของผู้ให้บริการเป็นที่ยอมรับได้หรือไม่ หรือกำหนดกระบวนการจัดการของผู้ประกอบธุรกิจเองเพื่อลดผลกระทบที่เกิดขึ้นให้น้อยที่สุด เป็นต้น	
16. <u>การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (information Security incident management)</u>		
16.1	กรณีระบบหยุดชะงักแต่ไม่มีนัยสำคัญ เช่น การปิดระบบซื้อขายเพื่อเตรียมความพร้อมก่อนเปิดตลาด ผู้ประกอบธุรกิจต้องรายงานสำนักงานหรือไม่	ให้ผู้ประกอบธุรกิจรายงานสำนักงานเมื่อระบบสารสนเทศที่มีความสำคัญหยุดชะงัก <u>เฉพาะ</u>ในกรณีที่อาจส่งผลกระทบต่อลูกค้า การดำเนินงาน ธุรกิจ ชื่อเสียง ฐานะและผลการดำเนินงานของผู้ประกอบธุรกิจอย่างมีนัยสำคัญเท่านั้น
16.2	กรณีที่ระบบ SETTRADE หยุดชะงัก ผู้ประกอบธุรกิจที่เป็นบริษัทหลักทรัพย์ทุกแห่งต้องรายงานสำนักงานให้ทราบหรือไม่	ผู้ประกอบธุรกิจแต่ละรายต้องรายงานสำนักงานเมื่อระบบ SETTRADE หยุดชะงัก เฉพาะในกรณีที่ส่งผลกระทบต่อลูกค้า การดำเนินงาน ธุรกิจ ชื่อเสียง ฐานะ และผลการดำเนินงานของผู้ประกอบธุรกิจอย่างมีนัยสำคัญเท่านั้น เพื่อให้สำนักงานรับทราบถึงผลกระทบและแนวทางดำเนินการรองรับเหตุการณ์ดังกล่าว
16.3	กรณีที่พบ virus คอมพิวเตอร์ ผู้ประกอบธุรกิจต้องรายงานสำนักงานหรือไม่	ให้รายงานเฉพาะกรณีที่พบการบุกรุกระบบสารสนเทศที่มีความสำคัญ หรือเครื่อง server ที่มีความสำคัญ
16.4	กรณีที่พบการโจมตีแบบ distributed denial of service (DDoS) ต้องรายงานสำนักงานหรือไม่	ต้องรายงานทุกกรณีที่พบการโจมตีในลักษณะดังกล่าว หากเกิดขึ้นกับระบบสารสนเทศที่มีความสำคัญ
16.5	การจัดทำ cyber security drill ต้องจัดทำถึงระดับใด และกรณีที่เป็นบริษัทในเครือหรือใช้ infrastructure เดียวกันกับธนาคารพาณิชย์ จะสามารถใช้ผลทดสอบร่วมกันได้หรือไม่	ผู้ประกอบธุรกิจสามารถพิจารณาจัดทำได้ทั้งรูปแบบ tabletop exercise หรือ full live ตามที่เห็นสมควร ตัวอย่างเช่น การทดสอบ cyber security awareness ของพนักงานโดยการส่งเมล์เพื่อทำ social engineering เป็นต้น

ลำดับ	คำถาม	คำตอบ
		สำหรับกรณีการใช้ผลทดสอบร่วมกับบริษัทในเครือ ผู้ประกอบธุรกิจสามารถดำเนินการได้หากการทดสอบดังกล่าวครอบคลุมถึงพนักงานของผู้ประกอบธุรกิจแล้ว
16.6	การรายงาน incident ต่อสำนักงานควรรายงานผ่านช่องทางใด	ปัจจุบันสำนักงานจัดให้มีช่องทางการรายงานดังต่อไปนี้ 1. จัดส่งรายงานผ่าน TCM-CERT portal : สำหรับผู้ประกอบธุรกิจที่เป็นสมาชิก TCM-CERT (ผู้สนใจสมัครสมาชิกสามารถดาวน์โหลดแบบฟอร์มได้ที่เว็บไซต์สำนักงาน http://www.sec.or.th/TH/Pages/Online-Download.aspx และสอบถามรายละเอียดเพิ่มเติมได้ที่ helpdesk : 02-033-9111) 2. จัดส่งรายงานผ่านอีเมล์ tcm-cert@sec.or.th สำหรับผู้ประกอบธุรกิจที่ไม่ได้เป็นสมาชิก TCM-CERT

แผนภาพที่ 1 : แสดงการเก็บ application log (ขยายความ FAQ ข้อ 9.11)



ตารางที่ 1 : ตัวอย่างการเก็บ application log (ขยายความ FAQ ข้อ 9.11)

1. Authentication part	User ID	Date/time	IP address (Source)		
2. Trading part	Broker ID/No.	Symbol	SET order ID	Account ID	Date & order time
3. Source - IP part	IP address (Source)	IP address (Destination)	Full URL		

การ corelate log ระหว่างอุปกรณ์

กรณี 1.1 (1) + (2) + (3) (1),(3) Private IP
Trading app

กรณี 2.1 (1) + (2) + (3) (1),(3) public IP
Trading app Network Firewall

กรณี 1.2 (1) (2) + (3) (1) Private IP (3) Public IP
เครื่องของ บล. SETTRADE

กรณี 2.2 (1) + (2) + (3) (1),(3) public IP
SETTRADE