สีเหลือง – ปรับปรุงเพิ่มเติมหลังจากเปิดรับฟังความเห็นในรอบเสนอหลักการ

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
2. นโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (information security policy)		
2.1	ในกรณีผู้ประกอบธุรกิจเป็นบริษัทในกลุ่มธุรกิจทางการเงิน ผู้ประกอบธุรกิจสามารถใช้นโยบายกลุ่มซึ่งได้รับอนุมัติจากคณะกรรมการบริษัทในกลุ่ม หรือคณะกรรมการที่ได้รับมอบหมาย เพื่อลดความซ้ำซ้อนในการปฏิบัติได้หรือไม่	ผู้ประกอบธุรกิจอาจดำเนินการได้ ทั้งนี้ควรปรับปรุงนโยบายดังกล่าวให้มีความสอดคล้องเหมาะสมกับลักษณะการประกอบธุรกิจของตนเองด้วย
3. การปฏิบัติงานที่มีการใช้อุปกรณ์เคลื่อนที่ (mobile device) เพื่อเข้าถึงระบบสารสนเทศภายในองค์กร และการปฏิบัติงานจากภายนอกบริษัท (teleworking)		
3.1	กรณีพนักงานทำการเชื่อมต่อ remote access จากที่บ้าน ผู้ประกอบธุรกิจอาจไม่สามารถทราบได้ว่าพนักงานทำการเชื่อมต่อโดยใช้อุปกรณ์ใด ผู้ประกอบธุรกิจต้องปฏิบัติตามหลักเกณฑ์ของสำนักงานอย่างไร	ผู้ประกอบธุรกิจต้องพิจารณาว่าการปฏิบัติงานดังกล่าวจัดเป็นการใช้งาน mobile device หรือเป็นการทำงานในลักษณะ teleworking เพื่อให้สามารถกำหนดได้ว่าการปฏิบัติงานดังกล่าวต้องเป็นไปตามแนวทางปฏิบัติของสำนักงานในส่วนของการใช้งาน mobile device หรือการทำงานในลักษณะ teleworking ทั้งนี้ การใช้งาน mobile device และการทำงานในลักษณะ teleworking มีลักษณะดังต่อไปนี้

ลำดับ	คำถาม	คำตอบ
		1. mobile device : ผู้ปฏิบัติงานนำอุปกรณ์เคลื่อนที่มาเชื่อมต่อกับระบบเครือข่ายคอมพิวเตอร์ภายในองค์กรเพื่อเข้าถึงระบบงานที่มีความสำคัญ เช่น นำ notebook ส่วนตัวมาเชื่อมต่อ Wi-Fi ของบริษัทเพื่อเข้าถึงระบบงานสำคัญ 2. teleworking : ผู้ปฏิบัติงานเข้าถึงระบบงานที่มีความสำคัญโดยไม่ผ่านการเชื่อมต่อกับระบบเครือข่ายคอมพิวเตอร์ภายในองค์กร โดยตรง เช่น ใช้งาน desktop PC ที่บ้าน เพื่อเข้าถึงระบบงานสำคัญของบริษัท โดยผ่านการเชื่อมต่ออินเตอร์เน็ตจากผู้ให้บริการอินเตอร์เน็ต (ISP)
3.2	หาก mobile device ที่เป็นอุปกรณ์ของพนักงานสูญหาย พนักงานต้องแจ้งให้ผู้ประกอบธุรกิจทราบหรือไม่	ต้องแจ้ง ในกรณีที่พนักงานเคยนำอุปกรณ์ดังกล่าวมาลงทะเบียนไว้กับผู้ประกอบธุรกิจ
3.3	จากหลักเกณฑ์ที่กำหนดให้ผู้ประกอบธุรกิจต้องจัดให้มีการป้องกันการเข้าถึงข้อมูลสารสนเทศจากบุคคลที่ไม่มีสิทธิในการใช้งานในพื้นที่ teleworking site เช่น ญาติพี่น้องและเพื่อน เป็นต้น ผู้ประกอบธุรกิจต้องดำเนินการอย่างไร เพื่อให้มั่นใจว่าได้ปฏิบัติเป็นไปตามหลักเกณฑ์ดังกล่าว	ผู้ประกอบธุรกิจอาจใช้วิธีการกำหนดนโยบายเพื่อควบคุมการเข้าถึงเครื่องคอมพิวเตอร์ที่ใช้ปฏิบัติงานจากภายนอกบริษัท เช่น จัดให้มีการควบคุมหน้าจอคอมพิวเตอร์ไม่ให้มีข้อมูลสำคัญปรากฏในขณะที่ไม่ได้ใช้งาน (clear screen) การ log-off จากระบบเมื่อใช้งานเสร็จสิ้น และการกำหนดรหัสผ่าน เป็นต้น พร้อมทั้งจัดให้มีการซักซ้อมและสร้างความตระหนักรู้แก่พนักงานเพื่อให้มีการปฏิบัติตามนโยบายดังกล่าวอย่างเคร่งครัด
3.4	การตรวจสอบความมั่นคงปลอดภัยของอุปกรณ์คอมพิวเตอร์ส่วนตัวของพนักงานในพื้นที่ teleworking site อาจทำได้ยาก ในทางปฏิบัติ จึงขอให้ใช้วิธีการกำหนดสิทธิและตรวจสอบการเข้าถึงของพนักงานที่ได้รับอนุญาตให้ปฏิบัติงานที่ teleworking site พร้อมทั้งควบคุมความมั่นคงปลอดภัยของ	เพื่อป้องกันการบุกรุกหรือเข้าถึงข้อมูลหรือระบบงานที่สำคัญในองค์กรอย่างไม่เหมาะสมจากการปฏิบัติงาน teleworking โดยเชื่อมต่อ remote access มายังองค์กร ผู้ประกอบธุรกิจอาจใช้วิธีกำหนดและตรวจสอบสิทธิการเข้าถึงของพนักงานที่ teleworking site แทนได้ หากมีการรักษาความปลอดภัยกับระบบคอมพิวเตอร์

ลำดับ	คำถาม	คำตอบ
	เครื่องคอมพิวเตอร์ในองค์กร และช่องทางการเชื่อมต่อ remote access ได้หรือไม่	ในองค์กร และช่องทางการเชื่อมต่อแล้ว เช่น ติดตั้ง firewall update โปรแกรม anti-virus กำหนดสิทธิการเข้าถึง และกำหนดให้มีการเข้ารหัส network เป็นต้น
3.5	ในการออก booth นอกพื้นที่องค์กร ผู้ประกอบธุรกิจต้องควบคุมดูแลพื้นที่ดังกล่าวอย่างไร	ในกรณีที่ผู้ประกอบธุรกิจกำหนดให้พื้นที่ดังกล่าวเป็นพื้นที่หวงห้าม ผู้ประกอบธุรกิจต้องกำหนดมาตรการรักษาความมั่นคงปลอดภัยด้านกายภาพสำหรับพื้นที่ปฏิบัติงานนอกองค์กร รวมทั้งต้องกำหนดมาตรการเพื่อป้องกันภัยคุกคามและรักษาความมั่นคงปลอดภัยต่อข้อมูลที่มีความสำคัญ และควบคุมสิทธิการใช้งานและการเข้าถึงข้อมูลและระบบงานที่มีความสำคัญโดยผู้ใช้งานอย่างเหมาะสม
3.6	การควบคุมให้มีความปลอดภัยด้านกายภาพสำหรับพื้นที่ปฏิบัติงานนอกองค์กรเป็นเรื่องยาก	ผู้ประกอบธุรกิจอาจกำหนดมาตรการดังกล่าวให้มีความยืดหยุ่นและเหมาะสมโดยคำนึงถึงขอบเขตการปฏิบัติงานเป็นสำคัญ เช่น การปฏิบัติงานที่ศูนย์สำรองต้องมีมาตรการการรักษาความมั่นคงปลอดภัยเทียบเท่าการทำงานที่บริษัทตามปกติ ขณะที่การปฏิบัติงานที่บ้าน (work from home) อาจกำหนดให้มีการป้องกันการเข้าถึงข้อมูลสารสนเทศจากบุคคลที่ไม่มีสิทธิ์ในการใช้งานก็เพียงพอ
4. <u>การใช้บริการ cloud computing</u>		
4.1	ขอให้ระบุนิยามของ cloud computing เพิ่มเติม เพื่อความเข้าใจในคำจำกัดความที่ตรงกัน	ผู้ประกอบธุรกิจสามารถประเมินลักษณะการให้บริการว่าเป็น cloud computing หรือไม่ โดยพิจารณาจากนิยามของหน่วยงาน National Institute of Standards and Technology (NIST)[1] (ต้องมีลักษณะครบทั้ง 5 จึงจะเข้าองค์ประกอบ)

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

ลำดับ	คำถาม	คำตอบ
		1. On-demand self-service : ผู้ใช้บริการสามารถกำหนด computing capabilities เช่น server time หรือ network storage ได้เองโดยไม่จำเป็นต้องพึ่งพาผู้ให้บริการ 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
4.2	กรณีที่ผู้ประกอบธุรกิจใช้บริการ cloud computing มาก่อนที่สำนักงานจะปรับปรุงหลักเกณฑ์ใหม่ แล้วพบว่าข้อกำหนดเกี่ยวกับการใช้งานยังไม่เป็นไปตามหลักเกณฑ์ดังกล่าว ต้องดำเนินการอย่างไร	ผู้ประกอบธุรกิจต้องกำหนดให้ cloud provider ติดตามหลักเกณฑ์ของสำนักงาน พร้อมทั้งจัดให้มีข้อกำหนดเกี่ยวกับการใช้งานให้เป็นไปตามหลักเกณฑ์ใหม่ของสำนักงาน ทั้งนี้ ผู้ประกอบธุรกิจมีเวลาเตรียมความพร้อม 1 ปีนับจากวันที่ประกาศกำหนด
4.3	ในการใช้บริการ cloud computing ผู้ประกอบธุรกิจต้องปฏิบัติตามหลักเกณฑ์ outsourcing ของสำนักงานหรือไม่	การใช้บริการ cloud computing ไม่จัดเป็นการใช้บริการ outsourcing ทั้งนี้ ให้ผู้ประกอบธุรกิจปฏิบัติให้เป็นไปตามแนวทางปฏิบัติของสำนักงานในส่วนของการใช้บริการ cloud computing
4.4	การใช้บริการประเภท software as a service (SAAS) บางประเภท เช่น facebook ของบริษัท หรือการ upload ข้อมูลทางธุรกิจขึ้น youtube ผู้ประกอบธุรกิจต้องปฏิบัติตามหลักเกณฑ์ของสำนักงานมากน้อยเพียงใด	หากผู้ประกอบธุรกิจใช้บริการ cloud computing โดยนำข้อมูลหรือระบบงานที่มีความสำคัญขึ้นสู่ cloud ผู้ประกอบธุรกิจต้องปฏิบัติให้เป็นไปตามแนวทางปฏิบัติของสำนักงานในส่วนของการใช้บริการ cloud computing

ลำดับ	คำถาม	คำตอบ
4.5	หากผู้ประกอบธุรกิจใช้บริการ cloud computing สำหรับระบบงานทั่วไปที่ไม่สำคัญ เช่น ระบบใบลาพนักงาน ผู้ให้บริการ cloud computing ต้องได้รับมาตรฐาน ISO27001 version ล่าสุดหรือไม่	กรณีการให้บริการระบบงานที่ไม่สำคัญ cloud provider อาจไม่จำเป็นต้องได้รับมาตรฐานการรับรองความมั่นคงปลอดภัยของระบบสารสนเทศในระดับสากลก็ได้
4.6	กรณีผู้ให้บริการ cloud computing จัดให้ผู้ให้บริการรายอื่นรับดำเนินการช่วง (subcontract of cloud provider) ผู้ประกอบธุรกิจต้องปฏิบัติตามหลักเกณฑ์อย่างไร	ผู้ประกอบธุรกิจต้องควบคุมดูแลให้ผู้ให้บริการดังกล่าวจัดให้มีข้อกำหนดในการใช้บริการ cloud computing ต่อจากผู้ให้บริการรายอื่น (sub cloud) อย่างชัดเจน โดยอย่างน้อยควรมีเงื่อนไขให้ผู้ให้บริการต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้นจากการกระทำหรือการดำเนินการใด ๆ ของผู้ให้บริการรายอื่นเสมือนเป็นส่วนหนึ่งของผู้ให้บริการ ทั้งนี้ คุณสมบัติด้านความปลอดภัยของผู้ให้บริการรายอื่นจะต้องเทียบเท่าผู้ให้บริการหรือเป็นไปตามมาตรฐานสากล
4.7	กรณีที่ผู้ประกอบธุรกิจใช้บริการผ่านตัวแทนจัดจำหน่าย (cloud distributor) ของผู้ให้บริการ cloud computing (cloud provider) ถือเป็นการ sub cloud หรือไม่ และ cloud distributor ต้องได้รับมาตรฐานการรับรองความปลอดภัยด้านสารสนเทศในระดับสากล (เช่น ISO27001) ด้วยหรือไม่	กรณีดังกล่าว cloud distributor เป็นเพียงผู้จัดหาระบบ cloud computing จึงไม่จัดเป็นการ sub cloud ดังนั้น cloud distributor จึงไม่ต้องได้รับมาตรฐานการรับรองความปลอดภัยด้านสารสนเทศในระดับสากล อย่างไรก็ดี cloud provider ที่ cloud distributor จัดหาให้ยังคงต้องได้รับมาตรฐานการรับรองความปลอดภัยด้านสารสนเทศดังกล่าว
4.8	การใช้บริการ cloud computing แบบ private cloud[2] เข้าข่ายต้องปฏิบัติตาม guideline ซึ่งว่าด้วยข้อกำหนดกรณีที่ผู้ประกอบธุรกิจใช้บริการ cloud computing ด้วยหรือไม่	เฉพาะกรณีที่ cloud computing นั้นเป็น private cloud ซึ่งผู้ประกอบธุรกิจเป็นเจ้าของและบริหารจัดการระบบทั้งหมดแต่เพียงผู้เดียว ให้งดเว้นการปฏิบัติตาม guideline ในหัวข้อดังกล่าวได้

[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
5. <u>การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร (human resource security)</u>		
5.1	บุคคลภายนอกที่ปฏิบัติงานโดยมีการเข้าถึงข้อมูลหรือระบบงานภายในองค์กร หมายความรวมถึงผู้ให้บริการที่เข้ามา on-site เป็นครั้งคราวด้วยหรือไม่	หมายความรวมถึงผู้ให้บริการที่เข้ามา on-site เป็นครั้งคราวด้วย หากมีการเข้าถึงข้อมูลหรือระบบงานภายในองค์กร
5.2	ในการสร้างความตระหนักรู้แก่บุคคลภายนอกที่ปฏิบัติงานโดยมีการเข้าถึงข้อมูลหรือระบบงานภายในองค์กร ผู้ประกอบธุรกิจสามารถใช้วิธีการส่ง email เพื่อแจ้ง policy แทนได้หรือไม่	ผู้ประกอบธุรกิจอาจสื่อสารให้บุคคลภายนอกซึ่งปฏิบัติงานที่ต้องเข้าถึงข้อมูลหรือระบบงานภายในองค์กรโดยวิธีการแจ้งนโยบายและแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของผู้ประกอบธุรกิจผ่านช่องทางสื่อสารด้านอิเล็กทรอนิกส์ เช่น email หรือแสดงข้อความ pop-up เมื่อใช้งานระบบก็ได้ โดยกำหนดวิธีให้บุคคลภายนอกดังกล่าวลงนามรับทราบนโยบายและแนวทางปฏิบัติด้วย
5.3	จากแนวทางปฏิบัติที่กำหนดให้ผู้ประกอบธุรกิจต้องสื่อสารให้พนักงานละเว้นการใช้งานระบบสารสนเทศในลักษณะที่อาจก่อให้เกิดความเสียหายต่อผู้ประกอบธุรกิจ นั้น นอกเหนือจากการกำหนดนโยบายในเชิงยับยั้งดังกล่าว ผู้ประกอบธุรกิจสามารถกำหนดนโยบายในเชิงที่อนุญาตให้พนักงานใช้งานระบบสารสนเทศได้เป็นรายกรณี (case by case) ตามเงื่อนไขและข้อตกลงที่ให้พนักงานลงนามรับทราบได้หรือไม่ เช่น พนักงานสามารถตั้งค่าส่งต่อจดหมายอิเล็กทรอนิกส์แบบอัตโนมัติได้ แต่ต้องปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัยที่ระบุไว้ใน information security policy ขององค์กรและได้รับอนุมัติจากผู้มีอำนาจ เป็นต้น	ผู้ประกอบธุรกิจสามารถกำหนดนโยบายในลักษณะดังกล่าวได้

ลำดับ	คำถาม	คำตอบ
6. <u>การควบคุมการเข้ารหัสข้อมูล (cryptographic controls)</u>		
6.1	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
6.2	การรับส่งจดหมายอิเล็กทรอนิกส์ (email) ผ่านระบบเครือข่ายคอมพิวเตอร์ จำเป็นต้องเข้ารหัส email ด้วยหรือไม่	หากผู้ประกอบธุรกิจจัดให้มีระบบการใส่รหัสผ่านสำหรับไฟล์ข้อมูลแนบ (attached file) ที่มีความสำคัญอย่างมั่นคงปลอดภัย ให้ถือว่าเพียงพอแล้ว
6.3	กรณีที่ผู้ประกอบธุรกิจจัดให้มีระบบการให้บริการเรียกข้อมูลส่วนตัวของลูกค้าในรูปแบบไฟล์ pdf ผ่านเครือข่ายอินเทอร์เน็ต จำเป็นต้องเข้ารหัสไฟล์ข้อมูล pdf ดังกล่าวหรือไม่	หากผู้ประกอบธุรกิจกำหนดให้ลูกค้าต้อง login เข้าสู่ระบบการให้บริการดังกล่าวด้วยรหัสผ่านที่มีความปลอดภัยก่อนใช้บริการเรียกข้อมูลดังกล่าว ให้ถือว่าเพียงพอแล้ว
7. <u>การจัดทำ penetration test</u>		
7.1	ควรกำหนดขอบเขตการจัดทำ penetration test อย่างไร	ผู้ประกอบธุรกิจต้องประเมินความเสี่ยงของระบบงานที่สำคัญ โดยอาจพิจารณาจากการวิเคราะห์ผลกระทบทางธุรกิจ (business impact analysis) ทั้งนี้ กรณีระบบงานที่มีผลกระทบสูง ผู้ประกอบธุรกิจต้องจัดให้มีการทดสอบอย่างเข้มงวด เพื่อทราบถึงช่องโหว่ของระบบ (vulnerability scanning) และการใช้ประโยชน์จากช่องโหว่ (exploitation test) ทั้งนี้ ผู้ประกอบธุรกิจต้องจัดให้มีมาตรการควบคุมเพื่อให้กระบวนการทดสอบส่งผลกระทบต่อการปฏิบัติงานน้อยที่สุด

ลำดับ	คำถาม	คำตอบ
7.2	ผู้จัดทำ penetration test เป็นบุคลากรภายในองค์กร ได้หรือไม่	สามารถกระทำได้ ทั้งนี้ บุคลากรดังกล่าวต้องมีความรู้ความสามารถเป็นที่น่าเชื่อถือได้ และมีความเป็นอิสระจากฝ่ายเทคโนโลยีสารสนเทศ
7.3	ในกรณีที่ระบบซื้อขายของบริษัทหลักทรัพย์เชื่อมโยงกับระบบของ settrade ใครเป็นผู้จัดทำ penetration test	settrade เป็นผู้จัดทำ ทั้งนี้ ผู้ประกอบธุรกิจอาจกำหนดให้เป็นข้อกำหนดในสัญญากับ settrade ได้
8. <u>การจัดเก็บข้อมูล electronic messaging</u>		
8.1	electronic messaging ครอบคลุมถึงอะไรบ้าง ต้องจัดเก็บเนื้อหาอะไร และจัดเก็บเฉพาะกรณีผู้ติดต่อกับลูกค้าได้หรือไม่	electronic messaging คือ การรับส่งข้อมูลสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์ เช่น การสนทนาโดยใช้จดหมายอิเล็กทรอนิกส์ (e-mail) โปรแกรมสนทนาผ่านระบบอิเล็กทรอนิกส์ (instant messaging) และระบบเครือข่ายสังคมออนไลน์ (social networking) เป็นต้น โดยต้องจัดเก็บทั้งเนื้อหาการสนทนาและการรับส่งข้อมูลสารสนเทศทั้งหมดสำหรับบุคคลที่เป็น access person ตามประกาศสำนักงานคณะกรรมการ ก.ล.ต. ที่ นป. 1/2558 เรื่อง แนวทางปฏิบัติสำหรับการกำหนดนโยบาย มาตรการ และระบบงานที่เกี่ยวกับการกระทำที่อาจมีความขัดแย้งทางผลประโยชน์กับลูกค้า
8.2	กรณีเกิดเหตุฉุกเฉิน การใช้จดหมายอิเล็กทรอนิกส์จากผู้ให้บริการโดยไม่เสียค่าบริการ (free e-mail) โดยส่งสำเนา (carbon copy : cc) ไปที่องค์กร การ cc กลับไปที่องค์กรสามารถทดแทนการจัดเก็บหลักฐาน email ทั้งฉบับได้หรือไม่	ในกรณีที่เกิดเหตุฉุกเฉินซึ่งส่งผลกระทบต่อการใช้งานระบบ e-mail ผู้ประกอบธุรกิจสามารถจัดเก็บหลักฐาน e-mail ในลักษณะดังกล่าวได้
8.3	กรณี e-mail ให้จัดเก็บเฉพาะของผู้ที่ทำหน้าที่ติดต่อกับลูกค้าเท่านั้นใช่หรือไม่ และบริษัทต้องจัดเก็บ content ด้วยหรือไม่ หากต้องจัดเก็บทั้งองค์กรจะทำให้บริษัทต้องมีการลงทุนเพิ่ม หรือกำหนดให้บริษัทจัดเก็บเฉพาะ	เพื่อให้มีบันทึกหลักฐานเพียงพอต่อการตรวจสอบ ให้ผู้ประกอบธุรกิจจัดเก็บ e-mail ทั้งฉบับ โดยอาจจัดเก็บเฉพาะ access person ก็ได้ ทั้งนี้ ขอบเขตของ access person ให้พิจารณาจากประกาศสำนักงานคณะกรรมการ ก.ล.ต. ที่

ลำดับ	คำถาม	คำตอบ
	e-mail ของบุคคลที่บริษัทพิจารณาแล้วเห็นว่าสามารถเข้าถึงข้อมูลภายในในแต่ละด้าน (“access person”) เท่านั้น	นป. 1/2558 เรื่อง แนวทางปฏิบัติสำหรับการกำหนดนโยบาย มาตรการ และระบบงานที่เกี่ยวกับการกระทำที่อาจมีความขัดแย้งทางผลประโยชน์กับลูกค้า
8.4	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
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	ผู้ประกอบธุรกิจต้องจัดเก็บและติดตามวิเคราะห์ log การเข้าถึงระบบฐานข้อมูลดังกล่าว เว้นแต่กรณีที่ผู้ประกอบธุรกิจได้จัดให้มีข้อกำหนดที่ทำให้มั่นใจว่าผู้ให้บริการภายนอกได้

ลำดับ	คำถาม	คำตอบ
	server) อยู่ที่ผู้ให้บริการภายนอก และผู้ให้บริการภายนอกมีการว่าจ้างผู้ตรวจสอบภายนอก (external auditor) ให้ตรวจสอบการเข้าถึงระบบฐานข้อมูลของผู้ประกอบธุรกิจแล้ว ผู้ประกอบธุรกิจไม่ต้องจัดเก็บและติดตามวิเคราะห์ log ดังกล่าวได้หรือไม่	ให้ผู้ตรวจสอบภายนอกตรวจสอบ log การเข้าถึงระบบฐานข้อมูลของผู้ประกอบธุรกิจ และจัดให้มีการเปิดเผยผลการตรวจสอบให้ผู้ประกอบธุรกิจรับทราบ โดยผลการตรวจสอบดังกล่าวต้องมีรายละเอียดขั้นต่ำเกี่ยวกับบัญชีผู้ใช้งาน วันเวลาที่เข้าใช้งาน และความพยายามในการเข้าใช้งาน
9.4	traffic log หากหมายความถึง payload ในทางปฏิบัติอาจทำได้ยาก และกระทบ performance ของระบบอย่างมาก ขอให้ระบุขอบเขตของอุปกรณ์เครือข่ายที่สำคัญ และประเภทของอุปกรณ์เครือข่าย เช่น รวมถึง switch และ router ด้วยหรือไม่	ในการจัดเก็บหลักฐานบันทึกข้อมูลจราจรคอมพิวเตอร์ ผู้ประกอบธุรกิจอาจจัดเก็บเฉพาะข้อมูลการเชื่อมต่ออุปกรณ์เครือข่ายที่สำคัญก็ได้ ทั้งนี้ อุปกรณ์เครือข่ายที่สำคัญ ได้แก่ อุปกรณ์เครือข่ายที่เกี่ยวข้องกับการเชื่อมต่อผ่านระบบงานที่สำคัญ เช่น switch, router และ firewall เป็นต้น
9.5	system operator log หมายถึง log ของผู้ใช้งานในหน่วยงาน หรือเรียกอีกอย่างหนึ่งว่า application log ใช่หรือไม่	system operator log ใน guideline หมายถึง log การจัดการระบบ ซึ่งมีความหมายใกล้เคียงกับ system administrator log
9.6	ผู้ประกอบธุรกิจยังคงต้องวิเคราะห์ log ในระบบงานที่กำหนดกฎ (rule) การใช้งานหรือกำหนดสิทธิการเข้าถึงระบบไว้อย่างชัดเจนแล้ว หรือไม่	ในกรณีที่ระบบงานกำหนดกฎการใช้งานหรือสิทธิการเข้าถึงระบบไว้อย่างชัดเจน ผู้ประกอบธุรกิจยังคงต้องจัดให้มีการวิเคราะห์ log ทั้งนี้ เพื่อให้มั่นใจได้ว่ากฎหรือสิทธิการเข้าถึงดังกล่าวยังสามารถควบคุมผู้ใช้งานได้อย่างปลอดภัยและมีประสิทธิภาพ
10. <u>การบริหารจัดการช่องโหว่ทางเทคนิค (technical vulnerability management)</u>		
10.1	การกำหนดให้ผู้ประกอบธุรกิจควรมีการประเมินความเสี่ยงของโปรแกรมเพื่อปิดช่องโหว่ (patches) ก่อนดำเนินการติดตั้งเพื่อทดสอบและประเมินผลกระทบที่อาจเกิดจากโปรแกรมดังกล่าว อาจทำให้ขัดแย้งกับแนวปฏิบัติที่ว่า ผู้ประกอบธุรกิจควรจัดให้มีการปิดช่องโหว่ที่พบ<u>โดยไม่ชักช้า</u> หากการประเมินและทดสอบดังกล่าวใช้ระยะเวลา	หากผู้ประกอบธุรกิจได้ทำการประเมินความเสี่ยงหลังจากที่พบช่องโหว่ในระบบแล้วว่าการติดตั้ง patches ทันทีอาจก่อให้เกิดความผิดพลาดต่อระบบได้ ให้ผู้ประกอบธุรกิจดำเนินการทดสอบโปรแกรมดังกล่าวโดยใช้ระยะเวลาตามที่จำเป็นเพื่อให้มั่นใจได้ว่าโปรแกรมที่จะดำเนินการติดตั้งนั้นไม่สร้างความเสียหายต่อระบบเพิ่มเติม โดยหาก patches ดังกล่าวผ่านการทดสอบแล้ว

ลำดับ	คำถาม	คำตอบ
	ในการดำเนินการที่ค่อนข้างนาน	ให้ผู้ประกอบธุรกิจติดตั้ง patches โดยไม่ชักช้า นอกจากนี้ เพื่อเป็นการปิดความเสี่ยงที่อาจเกิดขึ้นจากช่องโหว่ในระหว่างที่ patches ดังกล่าวยังไม่ผ่านการทดสอบ ผู้ประกอบธุรกิจอาจใช้วิธีการอื่นในการปิดความเสี่ยงได้ เช่น การติดตั้ง firewall เป็นต้น
11. การตรวจสอบระบบสารสนเทศ (information systems audit)		
11.1	จากแนวทางปฏิบัติที่กำหนดให้ผู้ประกอบธุรกิจกำหนดขอบเขตการตรวจสอบทางเทคนิค (technical audit test) ให้ครอบคลุมจุดเสี่ยงที่สำคัญและต้องควบคุมการตรวจสอบดังกล่าวไม่ให้กระทบต่อการปฏิบัติงานตามปกติ หากผู้ประกอบธุรกิจจัดให้มีการทำ pre-test ก่อนการวางระบบ จะถือว่าเพียงพอแล้วหรือไม่	ในการจัดทำ technical audit test ผู้ประกอบธุรกิจอาจใช้วิธีการทำ pre-test ก่อนการวางระบบได้ ทั้งนี้ ต้องเป็นการจัดทำ pre-test ทางเทคนิคบนเครื่องทดสอบเท่านั้น
12. การรักษาความมั่นคงปลอดภัยด้านการสื่อสารข้อมูลสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์ (communication security)		
12.1	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

ลำดับ	คำถาม	คำตอบ
12.2	ในการจัดให้พนักงานและผู้ให้บริการภายนอกทำสัญญารักษาความลับหรือไม่เปิดเผยข้อมูลที่มีความสำคัญ ผู้ประกอบธุรกิจสามารถกำหนดให้ผู้ให้บริการภายนอกลงนามในสัญญาโดยผู้มีอำนาจลงนาม ขณะที่พนักงานลงนามในเอกสารการรักษาความลับเมื่อแรกเข้า ได้หรือไม่ นอกจากนี้ ในการขออนุญาตเข้าถึงข้อมูลหรือกำหนดสิทธิการเข้าถึงข้อมูล สามารถใช้วิธีการอนุมัติทางอิเล็กทรอนิกส์ผ่านระบบได้หรือไม่	ในการลงนามในสัญญารักษาความลับหรือไม่เปิดเผยข้อมูลที่มีความสำคัญ ผู้ประกอบธุรกิจอาจดำเนินการดังนี้ 1. กรณีพนักงาน อาจลงนามในเอกสารรักษาความลับก่อนเริ่มปฏิบัติงานได้ 2. กรณีผู้ให้บริการภายนอก อาจจัดให้ผู้มีอำนาจลงนามเป็นผู้ลงนามได้ ผู้ประกอบธุรกิจสามารถทำได้ หากจัดให้มีกระบวนการที่สามารถพิสูจน์ตัวตนของผู้ขออนุญาต
13. <u>การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ</u> <u>(information Security incident management)</u>		
13.1	กรณีระบบหยุดชะงักแต่ไม่มีนัยสำคัญ เช่น การปิดระบบซื้อขายเพื่อเตรียมความพร้อมก่อนเปิดตลาด ผู้ประกอบธุรกิจต้องรายงานสำนักงานหรือไม่	ให้ผู้ประกอบธุรกิจรายงานสำนักงานเมื่อระบบสารสนเทศที่มีความสำคัญหยุดชะงัก <u>เฉพาะ</u>ในกรณีที่อาจส่งผลกระทบต่อลูกค้า การดำเนินงาน ธุรกิจ ชื่อเสียง ฐานะและผลการดำเนินงานของผู้ประกอบธุรกิจอย่างมีนัยสำคัญเท่านั้น
13.2	กรณีที่ระบบ settrade หยุดชะงัก ผู้ประกอบธุรกิจที่เป็นบริษัทหลักทรัพย์ทุกแห่งต้องรายงานสำนักงานให้ทราบหรือไม่	ผู้ประกอบธุรกิจแต่ละรายต้องรายงานสำนักงานเมื่อระบบ settrade หยุดชะงัก เฉพาะในกรณีที่ส่งผลกระทบต่อลูกค้า การดำเนินงาน ธุรกิจ ชื่อเสียง ฐานะ และผลการดำเนินงานของผู้ประกอบธุรกิจอย่างมีนัยสำคัญเท่านั้น เพื่อให้สำนักงานรับทราบถึงผลกระทบและแนวทางดำเนินการรองรับเหตุการณ์ดังกล่าว
13.3	กรณีที่พบ virus คอมพิวเตอร์ ผู้ประกอบธุรกิจต้องรายงานสำนักงานหรือไม่	ให้รายงานเฉพาะกรณีที่พบการบุกรุกระบบสารสนเทศที่มีความสำคัญ หรือเครื่อง server ที่มีความสำคัญ

ลำดับ	คำถาม	คำตอบ
13.4	กรณีที่พบการโจมตีแบบ distributed denial of service (DDoS) ต้องรายงานสำนักงานหรือไม่	ต้องรายงานทุกกรณีที่พบการโจมตีในลักษณะดังกล่าว หากเกิดขึ้นกับระบบสารสนเทศที่มีความสำคัญ
14. <u>การใช้บริการจากผู้ให้บริการภายนอก (Supplier Relationship)</u>		
14.1	จากแนวปฏิบัติที่กำหนดให้ผู้ให้บริการภายนอกต้องกำหนดแผนรองรับกรณีเกิดเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (<u>incident response policy</u>) ให้สอดคล้องกับแผนของผู้ประกอบธุรกิจ รวมทั้งกำหนดหน้าที่ความรับผิดชอบของผู้ให้บริการภายนอกในการกู้คืนระบบงานให้เป็นไปตามข้อตกลงที่ได้กำหนดไว้ ผู้ประกอบธุรกิจสามารถจัดให้มีกลไกอื่นเพื่อลดความเสี่ยงดังกล่าวได้หรือไม่ เช่น จัดให้มีการ due diligence ผู้ให้บริการโดยประเมินว่า incident response policy ของผู้ให้บริการเป็นที่ยอมรับได้หรือไม่ หรือ กำหนดกระบวนการจัดการของผู้ประกอบธุรกิจเอง เพื่อลดผลกระทบที่เกิดขึ้นให้น้อยที่สุด เป็นต้น	ผู้ประกอบธุรกิจสามารถกำหนดวิธีการดังกล่าวเป็นการทดแทนได้