ประเด็นคำถามที่ถามบ่อย (FAQ)

ลำดับ	คำถาม	คำตอบ
1. การใช้บริการ cloud computing		
1.1	กรณีที่ผู้ประกอบธุรกิจใช้บริการ cloud computing มาก่อนที่สำนักงานจะปรับปรุงหลักเกณฑ์ใหม่ แล้วพบว่าข้อกำหนดเกี่ยวกับการใช้งานยังไม่เป็นไปตามหลักเกณฑ์ดังกล่าว ต้องดำเนินการอย่างไร	ผู้ประกอบธุรกิจต้องกำหนดให้ cloud provider ติดตามหลักเกณฑ์ของสำนักงาน พร้อมทั้งจัดให้มีข้อกำหนดเกี่ยวกับการใช้งานให้เป็นไปตามหลักเกณฑ์ใหม่ของสำนักงาน ทั้งนี้ ผู้ประกอบธุรกิจมีเวลาเตรียมความพร้อม 1 ปี นับจากวันที่ประกาศกำหนด
1.2	ในการใช้บริการ cloud computing ผู้ประกอบธุรกิจต้องปฏิบัติตามหลักเกณฑ์ outsourcing ของสำนักงานหรือไม่	การใช้บริการ cloud computing ไม่จัดเป็นการใช้บริการ outsourcing ทั้งนี้ ให้ผู้ประกอบธุรกิจปฏิบัติให้เป็นไปตามแนวทางปฏิบัติของสำนักงานในส่วนของการใช้บริการ cloud computing
1.3	การใช้บริการประเภท software as a service (SAAS) บางประเภท เช่น facebook ของบริษัท หรือการ upload ข้อมูลทางธุรกิจขึ้น youtube ผู้ประกอบธุรกิจต้องปฏิบัติตามหลักเกณฑ์ของสำนักงานมากน้อยเพียงใด	หากผู้ประกอบธุรกิจใช้บริการ cloud computing โดยนำข้อมูลหรือระบบงานที่มีความสำคัญขึ้นสู่ cloud ผู้ประกอบธุรกิจต้องปฏิบัติให้เป็นไปตามแนวทางปฏิบัติของสำนักงานในส่วนของการใช้บริการ cloud computing
1.4	หากผู้ประกอบธุรกิจใช้บริการ cloud computing สำหรับระบบงานทั่วไปที่ไม่สำคัญ เช่น ระบบใบลาพนักงาน ผู้ให้บริการ cloud computing ต้องได้รับมาตรฐาน ISO27001 version ล่าสุดหรือไม่	กรณีการให้บริการระบบงานที่ไม่สำคัญ cloud provider อาจไม่จำเป็นต้องได้รับมาตรฐานการรับรองความมั่นคงปลอดภัยของระบบสารสนเทศในระดับสากลก็ได้
1.5	กรณีผู้ให้บริการภายนอกที่ผู้ประกอบธุรกิจว่าจ้าง ใช้บริการ cloud computing จากผู้ให้บริการรายอื่นอีกต่อหนึ่ง ผู้ประกอบธุรกิจต้องปฏิบัติตามหลักเกณฑ์อย่างไร	ผู้ประกอบธุรกิจต้องควบคุมดูแลให้ผู้ให้บริการภายนอกดังกล่าวจัดให้มีข้อตกลงด้านการใช้บริการกับผู้ให้บริการ cloud computing โดยให้เป็นไปตามแนวทางปฏิบัติของสำนักงานในส่วนของการใช้บริการ cloud computing

ลำดับ	คำถาม	คำตอบ
2. <u>การใช้งานอุปกรณ์คอมพิวเตอร์ประเภทพกพาและการปฏิบัติงานจากภายนอกบริษัท (mobile device and teleworking)</u>		
2.1	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> : ผู้ใช้งานนำอุปกรณ์คอมพิวเตอร์แบบพกพามาเชื่อมต่อกับระบบเครือข่ายคอมพิวเตอร์ภายในองค์กรที่มีการเชื่อมโยงกับระบบงานที่มีความสำคัญ 2. <u>teleworking</u> : ผู้ใช้งานเชื่อมต่ออุปกรณ์คอมพิวเตอร์กับระบบงานที่มีความสำคัญขององค์กรโดยไม่ผ่านการเชื่อมต่อกับระบบเครือข่ายคอมพิวเตอร์ภายในองค์กรโดยตรง
2.2	หาก mobile device ที่เป็นอุปกรณ์ของพนักงานสูญหาย พนักงานต้องแจ้งให้ผู้ประกอบธุรกิจทราบหรือไม่	ต้องแจ้ง ในกรณีที่พนักงานเคยนำอุปกรณ์ดังกล่าวมาลงทะเบียนไว้กับผู้ประกอบธุรกิจ
2.3	ในการออก booth นอกพื้นที่องค์กร ผู้ประกอบธุรกิจต้องควบคุมดูแลพื้นที่ดังกล่าวอย่างไร	ในกรณีที่ผู้ประกอบธุรกิจกำหนดให้พื้นที่ดังกล่าวเป็นพื้นที่หวงห้าม ผู้ประกอบธุรกิจต้องกำหนดมาตรการรักษาความมั่นคงปลอดภัยด้านกายภาพสำหรับพื้นที่ปฏิบัติงานนอกองค์กร รวมทั้งต้องกำหนดมาตรการเพื่อป้องกันภัยคุกคามและรักษาความมั่นคงปลอดภัยต่อข้อมูลที่มีความสำคัญ และควบคุมสิทธิการใช้งานและการเข้าถึงข้อมูลและระบบงานที่มีความสำคัญโดยผู้ใช้งานอย่างเหมาะสม

ลำดับ	คำถาม	คำตอบ
3. <u>การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร (human resource security)</u>		
3.1	จากแนวทางปฏิบัติข้อ 2. ซึ่งผู้ประกอบธุรกิจต้องสื่อสารให้พนักงานละเว้นการใช้งานระบบสารสนเทศในลักษณะที่อาจก่อให้เกิดความเสียหายต่อผู้ประกอบธุรกิจ นั้น นอกเหนือจากการกำหนดนโยบายในเชิงยับยั้งดังกล่าว ผู้ประกอบธุรกิจสามารถกำหนดนโยบายในเชิงที่อนุญาตให้พนักงานใช้งานระบบสารสนเทศได้เป็นรายกรณี (case by case) ตามเงื่อนไขและข้อตกลงที่ให้พนักงานลงนามรับทราบได้หรือไม่ เช่น พนักงานสามารถตั้งค่าส่งต่อจดหมายอิเล็กทรอนิกส์แบบอัตโนมัติได้ แต่ต้องปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัยที่ระบุไว้ใน information security policy ขององค์กรและได้รับอนุมัติจากผู้มีอำนาจ เป็นต้น	ผู้ประกอบธุรกิจสามารถกำหนดนโยบายในลักษณะดังกล่าวได้
4. <u>การควบคุมการเข้ารหัสข้อมูล (cryptographic controls)</u>		
4.1	การเข้ารหัสข้อมูล นอกจากจัดทำกับข้อมูลสำคัญที่รับส่งผ่านระบบเครือข่ายคอมพิวเตอร์แล้ว ต้องจัดทำกับข้อมูลสำคัญที่ถูกจัดเก็บอยู่ในสื่อบันทึกข้อมูล (storage media) ด้วยหรือไม่ หากมีมาตรการควบคุมจาก domain อื่น ๆ เช่น มีการควบคุม access control ที่ดี เป็นต้น สามารถทดแทนการเข้ารหัสข้อมูลสำคัญที่ถูกจัดเก็บอยู่ใน storage media ได้หรือไม่	ต้องจัดทำ เว้นแต่กรณีที่ผู้ประกอบธุรกิจจัดให้มีมาตรการควบคุมการเข้าถึงข้อมูลที่เป็นความลับหรือมีความสำคัญสูงอย่างมีประสิทธิภาพ มีการจัดเก็บสื่อบันทึกข้อมูลอย่างมั่นคงปลอดภัย และมีการเข้ารหัสไฟล์ข้อมูลรหัสผ่านอย่างรัดกุม จะถือว่ามีความเพียงพอต่อการปกป้องข้อมูลที่เป็นความลับหรือมีความสำคัญสูง
4.2	การรับส่งจดหมายอิเล็กทรอนิกส์ (email) ผ่านระบบเครือข่ายคอมพิวเตอร์ จำเป็นต้องเข้ารหัส email ด้วยหรือไม่	หากผู้ประกอบธุรกิจจัดให้มีระบบการใส่รหัสผ่านสำหรับไฟล์ข้อมูลแนบ (attached file) ที่มีความสำคัญอย่างมั่นคงปลอดภัย ก็ถือว่าเพียงพอแล้ว

ลำดับ	คำถาม	คำตอบ
4.3	กรณีที่ผู้ประกอบธุรกิจจัดให้มีระบบการให้บริการเรียกข้อมูลส่วนตัวของลูกค้าในรูปแบบไฟล์ pdf ผ่านเครือข่ายอินเทอร์เน็ต จำเป็นต้องเข้ารหัสไฟล์ข้อมูล pdf ดังกล่าวหรือไม่	หากผู้ประกอบธุรกิจกำหนดให้ลูกค้าต้อง login เข้าสู่ระบบการให้บริการดังกล่าวด้วยรหัสผ่านที่มีความปลอดภัยก่อนใช้บริการเรียกข้อมูลดังกล่าว ก็ถือว่าเพียงพอแล้ว
5. <u>การจัดทำ penetration test</u>		
5.1	ผู้จัดทำ penetration test เป็นบุคลากรภายในองค์กร ได้หรือไม่	ได้ ทั้งนี้ บุคลากรดังกล่าวต้องมีความรู้ความสามารถเป็นที่น่าเชื่อถือได้และมีความเป็นอิสระจากฝ่ายเทคโนโลยีสารสนเทศ
5.2	ในกรณีที่ระบบซื้อขายของบริษัทหลักทรัพย์เชื่อมโยงกับระบบของ settrade ถ้า settrade เป็นผู้จัดทำ penetration test แล้ว บริษัทหลักทรัพย์ยังต้องจัดทำหรือไม่	บริษัทหลักทรัพย์อาจไม่ต้องจัดทำก็ได้ หากมั่นใจได้ว่า settrade มีการจัดทำ penetration test แล้ว อย่างไรก็ดี บริษัทหลักทรัพย์ยังคงต้องจัดทำ penetration test กับระบบงานที่มีความสำคัญอื่น ๆ ซึ่งไม่ได้เชื่อมต่อกับระบบของ settrade
6. การบันทึก จัดเก็บหลักฐานและติดตาม (logging and monitoring)		
6.1	กรณีเกิดเหตุฉุกเฉิน การใช้จดหมายอิเล็กทรอนิกส์จากผู้ให้บริการโดยไม่เสียค่าบริการ (free email) โดยส่งสำเนา (carbon copy : cc) ไปที่องค์กร การ cc กลับไปที่องค์กรสามารถทดแทนการจัดเก็บหลักฐาน email ทั้งฉบับได้หรือไม่	ในกรณีที่เกิดเหตุฉุกเฉินซึ่งส่งผลกระทบต่อการใช้งานระบบ email ผู้ประกอบธุรกิจสามารถจัดเก็บหลักฐานข้อความใน email ในลักษณะดังกล่าวได้
6.2	กรณีที่ระบบ instant messaging บางระบบ เช่น ระบบ chat ใน Lotus Note หรือ Bloomberg ไม่สามารถบันทึกและจัดเก็บหลักฐานการสนทนาได้ ผู้ประกอบธุรกิจสามารถใช้ระบบงานดังกล่าวได้หรือไม่	สามารถใช้ได้เฉพาะกรณีที่บุคคลผู้ใช้งานไม่จัดเป็น access person ตามที่ระบุในประกาศว่าด้วยแนวทางปฏิบัติเกี่ยวกับระบบงานในการป้องกันมิให้เกิดการกระทำที่อาจมีความขัดหรือแย้งกับประโยชน์ของลูกค้า

ลำดับ	คำถาม	คำตอบ
6.3	ผู้ประกอบธุรกิจต้องวิเคราะห์ log ทุกประเภทตามที่สำนักงานกำหนดให้จัดเก็บหรือไม่ ผู้ประกอบธุรกิจต้องใช้เครื่องมือที่ซับซ้อนสำหรับการวิเคราะห์ log เพื่อประมวลหาความสัมพันธ์ (correlation) หรือรูปแบบ (pattern) ของข้อมูล log หรือไม่	ผู้ประกอบธุรกิจต้องวิเคราะห์ log ทุกประเภทอย่างสม่ำเสมอ เพื่อให้สามารถติดตามความเสี่ยงที่อาจเกิดขึ้นกับระบบสารสนเทศในเชิงรุก (proactive) เช่น ความพยายามเข้าถึงหรือใช้งานระบบสารสนเทศที่ผิดปกติ ซึ่งจะช่วยให้สามารถเตรียมความพร้อมรองรับความเสี่ยงดังกล่าวได้อย่างทันต่อเหตุการณ์ ทั้งนี้ ผู้ประกอบธุรกิจอาจใช้เครื่องมือหรือวิธีการวิเคราะห์ที่ไม่ซับซ้อนก็ได้ หากวิธีการดังกล่าวช่วยให้ติดตามความเสี่ยงได้อย่างเพียงพอและมีประสิทธิภาพ
6.4	กรณีที่ผู้ตรวจสอบ (auditor) เป็นผู้รวบรวม log ของผู้ประกอบธุรกิจไปวิเคราะห์ จะถือว่าผู้ประกอบธุรกิจได้จัดให้มีการวิเคราะห์ log แล้วหรือไม่	หากการตรวจสอบโดยผู้ตรวจสอบดังกล่าวสามารถติดตามความเสี่ยงที่อาจเกิดขึ้นกับระบบสารสนเทศในเชิงรุก (proactive) ได้อย่างเพียงพอและมีประสิทธิภาพ ถือว่าผู้ประกอบธุรกิจมีการวิเคราะห์ log แล้ว
6.5	ผู้ประกอบธุรกิจยังคงต้องวิเคราะห์ log ในระบบงานที่กำหนดกฎ (rule) การใช้งานหรือกำหนดสิทธิการเข้าถึงระบบไว้อย่างชัดเจนแล้ว หรือไม่	ในกรณีที่ระบบงานกำหนดกฎการใช้งานหรือสิทธิการเข้าถึงระบบไว้อย่างชัดเจน ผู้ประกอบธุรกิจยังคงต้องจัดให้มีการวิเคราะห์ log ทั้งนี้ เพื่อให้มั่นใจได้ว่ากฎหรือสิทธิการเข้าถึงดังกล่าวยังสามารถควบคุมผู้ใช้งานได้อย่างปลอดภัยและมีประสิทธิภาพ
7. <u>การรักษาความมั่นคงปลอดภัยด้านการสื่อสารและระบบเครือข่ายคอมพิวเตอร์ (communication security)</u>		
7.1	ผู้ประกอบธุรกิจต้องดำเนินการอย่างไรในกรณีที่มีบุคลากรไม่เพียงพอที่จะแบ่งแยกหน้าที่ความรับผิดชอบระหว่าง network administrator และ computer administrator ได้	ผู้ประกอบธุรกิจอาจจัดให้มีมาตรการหรือวิธีการควบคุมอื่นใดที่แสดงให้เห็นได้ว่าสามารถแบ่งแยกหน้าที่ความรับผิดชอบดังกล่าวได้อย่างมีประสิทธิภาพ

ลำดับ	คำถาม	คำตอบ
8. <u>การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ</u> <u>(information Security incident management)</u>		
8.1	กรณีระบบหยุดชะงัก แต่ไม่มีนัยสำคัญ เช่น การปิดระบบซื้อขายเพื่อเตรียมความพร้อมก่อนเปิดตลาด ผู้ประกอบธุรกิจต้องรายงานสำนักงานหรือไม่	ให้ผู้ประกอบธุรกิจรายงานสำนักงานเมื่อระบบสารสนเทศที่มีความสำคัญหยุดชะงัก <u>เฉพาะ</u> ในกรณีที่อาจส่งผลกระทบต่อลูกค้า การดำเนินงาน ธุรกิจ ชื่อเสียง ฐานะ และผลการดำเนินงานของผู้ประกอบธุรกิจอย่างมีนัยสำคัญ เท่านั้น
8.2	กรณีที่พบ virus คอมพิวเตอร์ ผู้ประกอบธุรกิจต้องรายงานสำนักงานหรือไม่	ให้รายงานเฉพาะกรณีที่พบการบุกรุกระบบสารสนเทศที่มีความสำคัญ หรือเครื่อง server ที่มีความสำคัญ
8.3	กรณีที่พบการโจมตีแบบ distributed denial of service (DDoS) ต้องรายงานสำนักงานหรือไม่	ต้องรายงานทุกกรณีที่พบการโจมตีในลักษณะดังกล่าว หากเกิดขึ้นกับระบบสารสนเทศที่มีความสำคัญ