(ร่าง)

ประกาศแนวปฏิบัติ

ที่ นป. /2565

เรื่อง แนวปฏิบัติในการจัดให้มีระบบเทคโนโลยีสารสนเทศ

ตามที่ประกาศคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ที่ กจ. 16/2561 เรื่อง หลักเกณฑ์ เงื่อนไขและวิธีการให้ความเห็นชอบผู้ให้บริการระบบเสนอขายโทเคนดิจิทัล ลงวันที่ 3 กรกฎาคม พ.ศ. 2561 และที่แก้ไขเพิ่มเติม (“ประกาศที่ กจ. 16/2561”) ประกาศคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ที่ กธ. 19/2561 เรื่อง หลักเกณฑ์ เงื่อนไข และวิธีการประกอบธุรกิจสินทรัพย์ดิจิทัล ลงวันที่ 3 กรกฎาคม พ.ศ. 2561 และที่แก้ไขเพิ่มเติม (“ประกาศที่ กธ. 19/2561”) ประกาศคณะกรรมการกำกับตลาดทุน ที่ ทธ. 35/2556 เรื่อง มาตรฐานการประกอบธุรกิจ โครงสร้างการบริหารงาน ระบบงาน และการให้บริการของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสัญญาซื้อขายล่วงหน้า ลงวันที่ 6 กันยายน พ.ศ. 2556 และที่แก้ไขเพิ่มเติม (“ประกาศที่ ทธ. 35/2556”) ประกาศคณะกรรมการกำกับตลาดทุน ที่ ทธ. 30/2559 เรื่อง หลักเกณฑ์ในการประกอบการเป็นศูนย์ซื้อขายสัญญาซื้อขายล่วงหน้า ลงวันที่ 3 สิงหาคม พ.ศ. 2559 (“ประกาศที่ ทธ. 30/2559”) ประกาศคณะกรรมการกำกับตลาดทุน ที่ ทธ. 31/2559 เรื่อง หลักเกณฑ์ในการประกอบการเป็นสำนักหักบัญชีสัญญาซื้อขายล่วงหน้า ลงวันที่ 3 สิงหาคม พ.ศ. 2559 (“ประกาศที่ ทธ. 31/2559”) ประกาศคณะกรรมการกำกับตลาดทุน ที่ ทธ. 32/2559 เรื่อง หลักเกณฑ์ เงื่อนไข และวิธีการในการประกอบการเป็นสำนักหักบัญชีหลักทรัพย์และศูนย์รับฝากหลักทรัพย์ ลงวันที่ 3 สิงหาคม พ.ศ. 2559 (“ประกาศที่ ทธ. 32/2559”) ประกาศคณะกรรมการกำกับตลาดทุน ที่ ทจ. 21/2562 เรื่อง ข้อกำหนดเกี่ยวกับการเสนอขายหลักทรัพย์ผ่านระบบคราวด์ฟันดิง ลงวันที่ 12 เมษายน พ.ศ. 2562 และที่แก้ไขเพิ่มเติม (“ประกาศที่ ทจ. 21/2562”) และประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ที่ สธ. / เรื่อง ข้อกำหนดในรายละเอียดเกี่ยวกับการจัดให้มีระบบเทคโนโลยีสารสนเทศ ลงวันที่ (“ประกาศที่ สธ. / ”) กำหนดให้ผู้ประกอบธุรกิจต้องจัดให้มีการกำกับดูแลและบริหารจัดการด้านเทคโนโลยีสารสนเทศ รักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และตรวจสอบด้านเทคโนโลยีสารสนเทศ ตลอดจนมีการทบทวนความเหมาะสมของเรื่องดังกล่าวเป็นประจำ นั้น

เพื่อประโยชน์ในการปฏิบัติตามข้อกำหนดข้างต้นของผู้ประกอบธุรกิจ สำนักงานโดยอาศัยอำนาจตามข้อ 3(2) ประกอบกับข้อ 6(7) (ฉ) ของประกาศที่ กจ. 16/2561 ข้อ 3(2) ประกอบกับข้อ 17 ข้อ 18 และข้อ 19 ของประกาศที่ กจ. 19/2561 ข้อ 5(3) ประกอบกับข้อ 12 วรรคหนึ่ง (11) และ (12) และข้อ 14 ของประกาศที่ ทธ. 35/2556 ข้อ 4(2) ประกอบกับข้อ 29 ข้อ 30 ข้อ 31 และข้อ 32 ของประกาศที่

ทธ. 30/2559 ข้อ 5(2) ประกอบกับข้อ 21 ข้อ 35 ข้อ 37 ข้อ 43 และข้อ 44 ของประกาศที่ ทธ. 31/2559 ข้อ 5(2) ประกอบกับข้อ 22 ถึงข้อ 33 และข้อ 34 วรรคสอง (2) ของประกาศที่ ทธ. 32/2559 และข้อ 5(2) ประกอบกับข้อ 31 (1) และ (4) วรรคหนึ่ง (ง) และ (10) ของประกาศที่ ทจ. 21/2562 จึงออกประกาศแนวปฏิบัติไว้ดังต่อไปนี้

ข้อ 1 ให้ยกเลิกประกาศแนวปฏิบัติ ที่ นป. 3/2559 เรื่อง แนวปฏิบัติในการจัดให้มีระบบเทคโนโลยีสารสนเทศ ลงวันที่ 12 กันยายน พ.ศ. 2559

ข้อ 2 แนวปฏิบัตินี้เป็นแนวทางเกี่ยวกับเรื่องดังต่อไปนี้

(1) การกำกับดูแลและบริหารจัดการด้านเทคโนโลยีสารสนเทศ (Information Technology Governance)

(2) การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Information Technology Security)

(3) การทบทวนความเหมาะสมของ (1) และ (2)

ข้อ 3 แนวปฏิบัติตามข้อ 2 มีรายละเอียดตามที่กำหนดในภาคผนวกแนบท้ายประกาศแนวปฏิบัตินี้

ข้อ 4 ในกรณีที่ผู้ประกอบธุรกิจได้ปฏิบัติตามแนวปฏิบัตินี้จนครบถ้วน สำนักงานจะพิจารณาว่าผู้ประกอบธุรกิจได้ปฏิบัติตามประกาศที่ กจ. 16/2561 ประกาศที่ กจ. 19/2561 ประกาศที่ ทธ. 35/2556 ประกาศที่ ทธ. 30/2559 ประกาศที่ ทธ. 31/2559 ประกาศที่ ทธ. 32/2559 ประกาศที่ ทธ. 21/2562 ในส่วนที่เกี่ยวกับระบบเทคโนโลยีสารสนเทศ และประกาศที่ สธ. / แล้ว ทั้งนี้ หากผู้ประกอบธุรกิจดำเนินการต่างจากแนวปฏิบัตินี้ ผู้ประกอบธุรกิจมีภาระที่จะต้องพิสูจน์ให้เห็นได้ว่าการดำเนินการนั้นยังคงอยู่ภายใต้หลักการและข้อกำหนดของประกาศดังกล่าว

ข้อ 5 ประกาศนี้ให้ใช้บังคับตั้งแต่วันที่ เป็นต้นไป

ประกาศ ณ วันที่

(นางสาวรื่นวดี สุวรรณมงคล)

เลขาธิการ

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์

ภาคผนวก

[แนบท้ายประกาศแนวปฏิบัติ ที่ นป. /]

<u>ขอบเขตการดำเนินการ:</u>

1. ผู้ประกอบธุรกิจระดับความเสี่ยงสูง ให้ดำเนินการตามแนวปฏิบัติทุกข้อ
2. ผู้ประกอบธุรกิจความเสี่ยงระดับกลางและระดับต่ำ ให้ดำเนินการตามแนวปฏิบัติทุกข้อ โดยได้รับยกเว้นการดำเนินการในส่วนที่ระบุว่า *"[ความเสี่ยงสูง]"*
3. ผู้ประกอบธุรกิจขนาดเล็ก ให้ดำเนินการตามแนวปฏิบัติ<u>ประกอบ</u>การดำเนินการตามหมวดที่ 2 ดังนี้

สารบัญ

หมวดที่ 1 การกำกับดูแลและบริหารจัดการด้านเทคโนโลยีสารสนเทศ (IT Governance)

ข้อกำหนดในภาคผนวก 2 แนบท้ายประกาศที่ สธ. /25	แนวปฏิบัติ
1.1 บทบาทหน้าที่และความรับผิดชอบของคณะกรรมการของผู้ประกอบธุรกิจ	
ส่วนที่ 1 บทบาทหน้าที่และความรับผิดชอบของคณะกรรมการของผู้ประกอบธุรกิจ ผู้ประกอบธุรกิจต้องดำเนินการให้การควบคุมดูแลการบริหารจัดการความเสี่ยงด้าน IT ผ่านการกำกับดูแลโดยคณะกรรมการของผู้ประกอบธุรกิจ เพื่อให้สอดคล้องกับระดับความเสี่ยง (ระดับความเสี่ยงที่ยอมรับได้ตามส่วนที่ 2 ข้อ 2.2.1(3)) โดยคำนึงถึงการบริหารและจัดการความเสี่ยงขององค์กร (enterprise risk) (ถ้ามี) ซึ่งอย่างน้อยต้องครอบคลุมในเรื่องดังนี้	
1.1 การกำหนดกรอบการกำกับดูแล (governance framework) และการกำกับดูแลแผนงานด้าน IT ให้สอดคล้องกับแผนทางธุรกิจ และมีความเหมาะสมเพียงพอที่จะรองรับการเปลี่ยนแปลงด้าน IT และการเปลี่ยนแปลงการดำเนินธุรกิจในอนาคต	1. ผู้ประกอบธุรกิจควรกำหนดกรอบการกำกับดูแลด้าน IT (governance framework) ที่ครอบคลุมรายละเอียดดังนี้ (1) โครงสร้างการกำกับดูแล: บทบาทหน้าที่และความรับผิดชอบของคณะกรรมการของผู้ประกอบธุรกิจ ผู้บริหารระดับสูง และฝ่ายงานที่เกี่ยวข้อง (2) กระบวนการที่เกี่ยวข้องกับการกำกับดูแลด้าน IT เช่น การจัดทำและขออนุมัติแผนงานด้าน IT การจัดทำและขออนุมัติทรัพยากรด้าน IT และการติดตามและรายงานผลการดำเนินการด้าน IT เป็นต้น 2. ผู้ประกอบธุรกิจควรจัดให้มีแผนงานด้านเทคโนโลยีสารสนเทศประจำปี เพื่อให้การใช้ IT สอดรับกับกลยุทธ์ในการดำเนินธุรกิจ และมีความยืดหยุ่นเพียงพอที่จะรองรับการเปลี่ยนแปลงด้านเทคโนโลยีและการเปลี่ยนแปลงการดำเนินธุรกิจ 3. *[ความเสี่ยงสูง] ผู้ประกอบธุรกิจควรจัดให้มีกลยุทธ์ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ (IT security strategy) ที่สอดคล้องกับกลยุทธ์ในการดำเนินธุรกิจ*
1.2 การจัดสรรทรัพยากรทางด้าน IT และทรัพยากรบุคคลให้มีความเหมาะสมเพียงพอต่อการดำเนินธุรกิจ	ผู้ประกอบธุรกิจควรจัดสรรทรัพยากรทางด้าน IT และทรัพยากรบุคคลให้สอดคล้องกับแผนกลยุทธ์องค์กร เพื่อให้บรรลุเป้าหมายตามภารกิจ กลยุทธ์ นโยบาย และแผนการดำเนินงานที่กำหนดไว้

ข้อกำหนดในภาคผนวก 2 แนบท้ายประกาศที่ สธ. /25	แนวปฏิบัติ
1.3 การกำหนดนโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้าน IT ซึ่งมีการกำหนดเป็นลายลักษณ์อักษร โดยอย่างน้อยต้องครอบคลุมนโยบายตามที่กำหนดในส่วนที่ 2 ข้อ 2.2	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]
1.4 การกำหนดขั้นตอนและวิธีปฏิบัติงานในการบริหารจัดการความเสี่ยงด้าน IT และการรักษาความมั่นคงปลอดภัย IT เพื่อให้เป็นไปตามนโยบายใน 1.3 รวมถึงกำกับดูแลให้มีการนำไปปฏิบัติอย่างเหมาะสม	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]
1.5 การสร้างความรู้และความตระหนักด้านความเสี่ยงด้าน IT แก่กรรมการและบุคลากรอย่างต่อเนื่องและมีประสิทธิผล	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]-
1.6 การติดตาม ตรวจสอบ และรายงานผลการปฏิบัติเพื่อให้เป็นไปตามนโยบายใน 1.3 ต่อคณะกรรมการของผู้ประกอบธุรกิจ โดยมีการรายงานอย่างน้อยปีละ 1 ครั้ง และในกรณีที่มีเหตุการณ์หรือการเปลี่ยนแปลงใด ๆ ซึ่งอาจส่งผลกระทบอย่างมีนัยสำคัญต่อการปฏิบัติเพื่อให้เป็นไปตามนโยบายดังกล่าว ต้องมีการรายงานให้คณะกรรมการของผู้ประกอบธุรกิจทราบโดยไม่ชักช้าด้วย	1. ผู้ประกอบธุรกิจควรจัดให้มีกระบวนการติดตาม ตรวจสอบ และควบคุมการจัดทำรายงานผลการปฏิบัติงานเพื่อให้มั่นใจว่าสามารถจัดทำรายงานได้อย่างครบถ้วน ถูกต้อง 2. ผู้ประกอบธุรกิจควรกำหนดให้การรายงานผลการปฏิบัติตามนโยบายที่เกี่ยวข้องกับการกำกับดูแลและบริหารจัดการความเสี่ยงด้าน IT ต่อคณะกรรมการของผู้ประกอบธุรกิจ มีเนื้อหาครอบคลุมถึงเรื่องดังนี้ (1) ผลการประเมินความเสี่ยงด้าน IT การติดตามความเสี่ยง และแนวทางการควบคุมที่เกี่ยวข้อง โดยหน่วยงานที่ทำหน้าที่บริหารความเสี่ยงด้าน IT หรือหน่วยงานที่เกี่ยวข้อง (2) ผลการปฏิบัติตามกฎระเบียบ ข้อบังคับ หรือนโยบายการรักษาความมั่นคงปลอดภัยด้าน IT ในภาพรวมขององค์กร โดยหน่วยงานที่ทำหน้าที่กำกับดูแลการปฏิบัติงานด้าน IT หรือหน่วยงานที่เกี่ยวข้อง (3) ผลการตรวจสอบด้าน IT (IT audit) และความคืบหน้าในการดำเนินการแก้ไขข้อตรวจพบ โดยหน่วยงานที่ทำหน้าที่ตรวจสอบด้าน IT หรือหน่วยงานที่เกี่ยวข้อง (4) ผลการปฏิบัติงานด้าน IT ที่สำคัญ เช่น (ก) เหตุการณ์ผิดปกติ หรือปัญหาด้าน IT ที่สำคัญ (ข) ความเพียงพอของทรัพยากรด้าน IT (capacity and system utilization)

ข้อกำหนดในภาคผนวก 2 แนบท้ายประกาศที่ สธ. /25	แนวปฏิบัติ
	(ค) ความคืบหน้าของโครงการด้าน IT ในภาพรวมและโครงการที่สำคัญ (ง) การปฏิบัติงานด้าน IT ของบุคคลภายนอก เช่น ผลการดำเนินการตามข้อตกลงการให้บริการ (service level agreement) เป็นต้น (จ) ผลการทดสอบแผนฉุกเฉินด้าน IT และการใช้งานแผน (ถ้ามี)
1.2 โครงสร้างการกำกับดูแล	
ส่วนที่ 2 การกำกับดูแลและบริหารจัดการความเสี่ยงด้าน IT ในระดับองค์กร 2.1 ผู้ประกอบธุรกิจต้องจัดให้มีโครงสร้างการกำกับดูแลและบริหารจัดการความเสี่ยงด้าน IT โดยอย่างน้อยต้องมีลักษณะดังนี้ 2.1.1 ทำให้เกิดการถ่วงดุลอย่างเป็นอิสระ 2.1.2 สอดคล้องตามหลักการแบ่งแยกหน้าที่ 3 ระดับ (3 Lines of Defense : 3 LoDs) โดยมีการแบ่งแยกหน้าที่อย่างชัดเจนระหว่างการทำหน้าที่ด้าน IT ดังนี้ ระดับที่ 1 (first line of defense) : การปฏิบัติงาน ระดับที่ 2 (second line of defense) : การบริหารความเสี่ยงและกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง ระดับที่ 3 (third line of defense) : การตรวจสอบ	1. ผู้ประกอบธุรกิจควรจัดให้มีโครงสร้างการกำกับดูแลและบริหารจัดการความเสี่ยงด้าน IT ที่มีการถ่วงดุลอำนาจ (check and balance) และมีการแบ่งแยกหน้าที่ (segratation of duties) อย่างเหมาะสม ตามหลักการแบ่งแยกหน้าที่ 3 ระดับ ได้แก่ (1) การปฏิบัติงาน (first line of defense) หมายถึง หน่วยงานปฏิบัติงานด้าน IT และผู้ใช้งานระบบ IT (ก) หน่วยงานปฏิบัติงานด้าน IT มีหน้าที่ปฏิบัติงานทางด้าน IT ในขอบเขตงานที่รับผิดชอบและตามแนวทางการควบคุมความเสี่ยง รวมถึงจัดให้มีการติดตามและรายงานการปฏิบัติงานด้าน IT ต่อคณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมาย (ข) ผู้ใช้งานระบบ IT มีหน้าที่ปฏิบัติตามนโยบายและระเบียบปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้าน IT รวมทั้งมีส่วนร่วมรับผิดชอบในการประเมินและจัดการความเสี่ยงด้าน IT ที่เกี่ยวข้องกับการใช้งานระบบ (2) การบริหารความเสี่ยงและกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องในการปฏิบัติงานด้าน IT (second line of defense) หมายถึง หน่วยงานบริหารความเสี่ยง และหน่วยงานกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ (second line of defense) (ก) หน่วยงานบริหารความเสี่ยง มีหน้าที่กำหนดกรอบและกระบวนการบริหารความเสี่ยงด้าน IT (IT risk function) สนับสนุนให้มีการประเมินความเสี่ยงเป็นไปตามกรอบการบริหารความเสี่ยงที่กำหนด พร้อมทั้งให้คำปรึกษา ติดตามความเสี่ยง และทบทวนการควบคุมความเสี่ยงด้าน IT ให้อยู่ในระดับ

ข้อกำหนดในภาคผนวก 2 แนบท้ายประกาศที่ สธ. /25	แนวปฏิบัติ
	ความเสี่ยงที่ยอมรับได้ของหน่วยงานปฏิบัติงานด้าน IT โดยมีการรวบรวมและเชื่อมโยงความเสี่ยงด้าน IT กับความเสี่ยงด้านอื่น และนำเสนอผลการบริหารความเสี่ยงต่อคณะกรรมการที่ทำหน้าที่กำกับดูแลความเสี่ยง รวมถึงมีการสื่อสารปัญหาหรือความเสี่ยงใหม่ ๆ ที่เกิดขึ้น (ข) หน่วยงานกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ (compliance function) มีหน้าที่ในการกำกับดูแลให้มีการปฏิบัติตามกฎและหลักเกณฑ์ต่าง ๆ ติดตามและสนับสนุนกระบวนการกำกับดูแลและบริหารจัดการทางด้าน IT ขององค์กรให้เป็นไปในทิศทางที่เหมาะสม รวมทั้งติดตามความเพียงพอเหมาะสมของการควบคุมและการปฏิบัติตามกฎระเบียบต่าง ๆ ขององค์กร (3) การตรวจสอบด้าน IT (third line of defense) หมายถึง หน่วยงานตรวจสอบด้าน IT ซึ่งมีหน้าที่ในการตรวจสอบการปฏิบัติงานของหน่วยงานที่ทำหน้าที่ first line และ second line of defense รวมถึงหน่วยงานอื่น ๆ ที่เกี่ยวข้อง เช่น การใช้บริการด้าน IT จากบุคคลภายนอก เป็นต้น เพื่อให้มั่นใจว่ามีการปฏิบัติตามนโยบาย มาตรฐาน และกฎหมายทางด้าน IT ที่เกี่ยวข้อง หน่วยงานในระดับนี้อาจเป็นผู้ตรวจสอบภายใน หรือผู้ตรวจสอบภายนอกที่มีความเป็นอิสระจากหน่วยงานที่ทำหน้าที่ first line และ second line of defense 2. *[ความเสี่ยงสูง] ผู้ประกอบธุรกิจควรดำเนินการดังต่อไปนี้* *(1) ผู้ประกอบธุรกิจควรจัดให้มีกรรมการของผู้ประกอบธุรกิจ หรือที่ปรึกษาของผู้ประกอบธุรกิจ อย่างน้อย 1 ท่าน ที่มีความรู้หรือประสบการณ์ด้าน IT เพื่อให้คณะกรรมการสามารถกำหนดทิศทางและกำกับดูแลให้มีการใช้ IT ให้สอดรับกับกลยุทธ์ในการดำเนินธุรกิจ และบริหารจัดการความเสี่ยงด้าน IT ได้อย่างมีประสิทธิภาพ ทั้งนี้ ผู้ประกอบธุรกิจสามารถพิจารณาคุณสมบัติของกรรมการ หรือที่ปรึกษาที่มีความรู้หรือประสบการณ์ด้าน IT ได้จากเรื่องดังนี้ โดยผู้ประกอบธุรกิจอาจใช้เกณฑ์ด้านอื่นในการพิจารณาตามความเหมาะสม* *(ก) จบการศึกษาในสาขา IT หรือสาขาที่เกี่ยวข้อง หรือ* *(ข) มีประสบการณ์ในตำแหน่งหัวหน้าหน่วยงาน หรือมีหน้าที่รับผิดชอบเป็นผู้บริหารงานหลัก หรือมีประสบการณ์ในด้านการให้คำปรึกษาที่เกี่ยวข้องด้าน IT หรือ* *(ค) มีประสบการณ์หรือได้รับแต่งตั้งเป็นสมาชิกในคณะกรรมการหรือคณะทำงานที่เกี่ยวข้องด้าน IT*

ข้อกำหนดในภาคผนวก 2 แนบท้ายประกาศที่ สธ. /25	แนวปฏิบัติ
	กรณีที่คณะกรรมการของผู้ประกอบธุรกิจแต่งตั้งคณะกรรมการชุดย่อยเพื่อทำหน้าที่ให้คำปรึกษาด้าน IT แก่คณะกรรมการของผู้ประกอบธุรกิจ ผู้ประกอบธุรกิจควรกำหนดบทบาทหน้าที่คณะกรรมการชุดย่อยอย่างชัดเจนและเป็นลายลักษณ์อักษร *(2) ผู้ประกอบธุรกิจควรจัดให้มีผู้บริหารระดับสูง (chief information security officer : CISO) หรือผู้บริหารที่รับผิดชอบในการบริหารจัดการความมั่นคงปลอดภัยด้าน IT โดยมีคุณสมบัติ ขอบเขตอำนาจ และหน้าที่อย่างน้อยดังนี้* *(ก) มีความเป็นอิสระจากหน่วยงานที่ทำหน้าที่ปฏิบัติงานด้าน IT (IT operation) และงานด้านพัฒนาระบบ IT (IT development) สอดคล้องตามหลักการถ่วงดุล (check and balance) ที่ดี* *(ข) เป็นผู้ที่มีความรู้ความสามารถหรือมีประสบการณ์ด้าน IT และด้านการบริหารจัดการความมั่นคงปลอดภัยด้าน IT* *(ค) มีอำนาจหน้าที่ (authority) เพียงพอในการปฏิบัติหน้าที่ได้อย่างมีประสิทธิภาพและประสิทธิผล โดยสามารถดำเนินการอย่างน้อย ดังนี้* *(ก) รายงานปัญหาหรือเหตุการณ์ที่มีนัยสำคัญซึ่งกระทบต่อความมั่นคงปลอดภัยด้าน IT ต่อผู้บริหารในตำแหน่งสูงสุดขององค์กร และคณะกรรมการที่เกี่ยวข้องโดยตรง* *(ข) ให้ความเห็นด้านภัยคุกคามทางไซเบอร์และการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยด้าน IT ต่อคณะกรรมการของผู้ประกอบธุรกิจ หรือ คณะกรรมการที่เกี่ยวข้องกับการบริหารจัดการและกำกับดูแลการปฏิบัติงานด้าน IT และร่วมตัดสินใจดำเนินการในเรื่องความมั่นคงปลอดภัยด้าน IT และภัยคุกคามทางไซเบอร์ที่มีผลกระทบอย่างมีนัยสำคัญ* (3) *คณะกรรมการของผู้ประกอบธุรกิจ<u>อาจ</u>แต่งตั้งคณะกรรมการเพื่อทำหน้าที่ที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้าน IT เช่น* *(ก) คณะกรรมการกำกับดูแลและบริหารจัดการด้าน IT (เช่น IT steering committee หรือคณะกรรมการที่ได้รับมอบหมาย เป็นต้น) เพื่อดูแลให้มีการใช้งาน IT ที่สอดคล้องกับกลยุทธ์ของผู้ประกอบธุรกิจ*

ข้อกำหนดในภาคผนวก 2 แนบท้ายประกาศที่ สธ. /25	แนวปฏิบัติ
	(ข) คณะกรรมการกำกับดูแลการบริหารความเสี่ยงด้าน IT (เช่น คณะกรรมการบริหารความเสี่ยง หรือคณะกรรมการที่ได้รับมอบหมาย เป็นต้น) เพื่อดูแลให้มีการกำหนดนโยบายการบริหารความเสี่ยงด้าน IT รวมทั้งกำกับดูแลและติดตามให้เป็นไปตามนโยบายที่กำหนดไว้ *(ค) คณะกรรมการกำกับดูแลการตรวจสอบด้าน IT (เช่น คณะกรรมการตรวจสอบ หรือคณะกรรมการที่ได้รับมอบหมาย เป็นต้น) เพื่อให้ผู้ประกอบธุรกิจมีการตรวจสอบด้าน IT อย่างเป็นอิสระ ครอบคลุมถึงการปฏิบัติงาน การบริหารความเสี่ยงด้าน IT และการกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับ IT*
1.3 นโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้าน IT	
2.2 ผู้ประกอบธุรกิจต้องให้มีนโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้าน IT เป็นลายลักษณ์อักษร โดยต้องได้รับความเห็นชอบจากคณะกรรมการของผู้ประกอบธุรกิจหรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบธุรกิจ ดังนี้	
2.2.1 <u>นโยบายการบริหารจัดการความเสี่ยงด้าน IT (IT risk management policy)</u> มีเรื่องที่ต้องครอบคลุม ดังนี้ (1) บทบาทหน้าที่ของผู้ที่เกี่ยวข้องในการบริหารจัดการความเสี่ยงด้าน IT (2) เกณฑ์ความเสี่ยง (risk criteria) โดยครอบคลุมถึงโอกาสหรือความถี่ที่จะเกิดเหตุการณ์ความเสี่ยงและความมีนัยสำคัญหรือผลกระทบที่จะเกิดขึ้น เพื่อจัดลำดับความสำคัญในการบริหารจัดการความเสี่ยง	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]

ข้อกำหนดในภาคผนวก 2 แนบท้ายประกาศที่ สธ. /25	แนวปฏิบัติ
(3) ระดับความเสี่ยงที่ยอมรับได้ (risk appetite)	ผู้ประกอบธุรกิจควรกำหนดให้คณะกรรมการบริหารความเสี่ยง (ถ้ามี) เป็นผู้พิจารณาระดับความเสี่ยงที่ยอมรับได้ด้าน IT และเสนอให้คณะกรรมการของผู้ประกอบธุรกิจเป็นผู้อนุมัติ โดยระดับความเสี่ยงที่ยอมรับได้ด้าน IT (IT risk appetite) ควรสอดคล้องกับการบริหารและจัดการความเสี่ยงขององค์กร (enterprise risk management) (ถ้ามี)
(4) การประเมินความเสี่ยง (risk assessment) ที่ครอบคลุมความเสี่ยงด้าน IT และความเป็นส่วนตัวจากการใช้งาน IT	1. ผู้ประกอบธุรกิจควรกำหนดให้มีการประเมินความเสี่ยง (risk assessment) ทั้งในด้าน IT และด้านความเสี่ยงด้านความเป็นส่วนตัว (privacy) จากการใช้งาน IT อย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงระบบ IT อย่างมีนัยสำคัญ โดยมีการดำเนินการ ดังนี้ (1) การระบุความเสี่ยง (risk identification) จัดให้มีการระบุเหตุการณ์ความเสี่ยง (risk scenario) ด้านความมั่นคงปลอดภัยสารสนเทศและความเสี่ยงด้านความเป็นส่วนตัว (privacy) จากการใช้งาน IT ซึ่งที่อาจจะเกิดขึ้นหรือที่เคยเกิดขึ้นจริงทั้งกับผู้ประกอบธุรกิจเองหรือเกิดกับผู้ประกอบธุรกิจอื่นที่ใช้งานเทคโนโลยีในลักษณะเดียวกัน รวมถึงภัยคุกคามทางไซเบอร์และช่องโหว่ต่าง ๆ ที่ส่งผลกระทบต่อการดำเนินธุรกิจ โดยเหตุการณ์ความเสี่ยงดังกล่าวอาจมีสาเหตุมาจากปัจจัยภายใน (internal factor) กระบวนการปฏิบัติงาน ระบบงาน บุคลากร การใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก รวมถึงปัจจัยภายนอกอื่น ๆ (external factor) เช่น การปฏิบัติตามกฎหมาย เป็นต้น (2) การวิเคราะห์ความเสี่ยง (risk analysis) จัดให้มีการวิเคราะห์ความเสี่ยงด้าน IT และความเสี่ยงด้านความเป็นส่วนตัว (privacy) จากการใช้งาน IT เพื่อหาแนวทางในการจัดการความเสี่ยงอย่างเหมาะสม โดยดำเนินการ (ก) กำหนดผู้รับผิดชอบต่อความเสี่ยงหรือเจ้าของความเสี่ยง (risk owner) (ข) ระบุการควบคุมที่มีอยู่ในปัจจุบัน (existing control) (ค) วิเคราะห์โอกาสหรือความถี่ที่จะเกิดเหตุการณ์ความเสี่ยง (likelihood) และความมีนัยสำคัญหรือผลกระทบที่จะเกิดขึ้น (potential impact) จากเหตุการณ์ดังกล่าว (3) การประเมินค่าความเสี่ยง (risk evaluation) จัดให้มีประเมินค่าความเสี่ยงด้าน IT และความเสี่ยงด้านความเป็นส่วนตัว (privacy) จากการใช้งาน IT

ข้อกำหนดในภาคผนวก 2 แนบท้ายประกาศที่ สธ. /25	แนวปฏิบัติ
	เพื่อจัดลำดับในการบริหารความเสี่ยงอย่างเหมาะสม โดยดำเนินการ (ก) เปรียบเทียบและประเมินผลลัพธ์ที่ได้จากการวิเคราะห์ความเสี่ยง ได้แก่ ค่าโอกาสและผลกระทบ (likelihood และ potential impact) กับเกณฑ์ความเสี่ยง (risk criteria) ที่กำหนดไว้ เพื่อระบุระดับค่าความเสี่ยงของแต่ละเหตุการณ์ความเสี่ยงด้าน IT (ข) จัดลำดับความเสี่ยงด้าน IT 2. *[ความเสี่ยงสูง] ผู้ประกอบธุรกิจควรมีการประเมินความเสี่ยงด้าน IT และความเสี่ยงด้านความเป็นส่วนตัว (privacy) จากการใช้งาน IT ให้เท่าทันต่อการเปลี่ยนแปลงความเสี่ยงของบริษัท (company risk profile) อันอาจจะเกิดจากปัจจัยทางเทคโนโลยี ทั้งภายในและภายนอกองค์กร เช่น การออกหรือเปลี่ยนแปลงมาตรฐานและข้อกำหนดทางเทคโนโลยีในอุตสาหกรรม หรือการตรวจพบหรือมีข้อบ่งชี้ด้านความเสี่ยงทางเทคโนโลยีใหม่เกิดขึ้น เป็นต้น*
(5) การจัดการความเสี่ยง (risk treatment) ให้ความเสี่ยงที่เหลืออยู่ (residual risk) อยู่ในระดับความเสี่ยงที่ยอมรับได้	ผู้ประกอบธุรกิจควรกำหนดให้มีแนวทางในการจัดการความเสี่ยง (risk treatment) ด้าน IT และความเสี่ยงด้านความเป็นส่วนตัว (privacy) จากการใช้งาน IT อย่างเหมาะสมและสอดคล้องกับผลการประเมินความเสี่ยง (risk assessment) เพื่อให้ความเสี่ยงที่เหลืออยู่ (residual risk) อยู่ในระดับความเสี่ยงที่ยอมรับได้ (risk appetite) โดยควรครอบคลุมอย่างน้อย ดังนี้ 1. การกำหนดแนวทางในการจัดการความเสี่ยง และวิธีการที่เหมาะสมกับผู้ประกอบธุรกิจ เช่น การหยุดหรือหลีกเลี่ยงความเสี่ยง (risk avoidance) การลดหรือบรรเทาความเสี่ยง (risk mitigation) การโอนย้ายความเสี่ยง (risk transference) และการยอมรับความเสี่ยง (risk acceptance) เป็นต้น 2. การระบุรายละเอียดของงานที่ต้องดำเนินการ ผู้รับผิดชอบ และระยะเวลาที่ใช้ในการดำเนินการ 3. การประเมินระดับค่าความเสี่ยงที่เหลืออยู่ (residual risk) ว่าอยู่ในระดับความเสี่ยงที่ยอมรับได้ 4. การขออนุมัติแผนการจัดการความเสี่ยงจากคณะกรรมการหรือผู้บริหารที่ได้รับมอบหมาย 5. การสื่อสารแผนการบริหารจัดการความเสี่ยงให้ผู้ที่เกี่ยวข้องรับทราบ
(6) การจัดทำทะเบียนความเสี่ยง (risk register)	ผู้ประกอบธุรกิจควรจัดให้มีทะเบียนความเสี่ยง (risk register) เพื่อบันทึกผลการประเมินความเสี่ยง และแนวทางในการจัดการความเสี่ยง โดยทะเบียนความเสี่ยงควรมีรายละเอียดอย่างน้อย ดังนี้ 1. วันที่ประเมินความเสี่ยง

ข้อกำหนดในภาคผนวก 2 แนบท้ายประกาศที่ สธ. /25	แนวปฏิบัติ
	2. คำอธิบายรายละเอียดเหตุการณ์ความเสี่ยง 3. โอกาสหรือความถี่ที่จะเกิดเหตุการณ์ความเสี่ยง (likelihood) 4. ความมีนัยสำคัญหรือผลกระทบที่จะเกิดขึ้น (potential impact) 5. ระดับค่าความเสี่ยง 6. แนวทางจัดการความเสี่ยง (risk treatment) 7. เจ้าของความเสี่ยง (risk owner) 8. ระดับความเสี่ยงที่เหลืออยู่ (residual risk) 9. สถานะของการจัดการความเสี่ยง (status of risk treatment)
(7) การติดตามและทบทวนความเสี่ยง (risk monitor and review)	ผู้ประกอบธุรกิจควรให้มีกระบวนการในการติดตามความเสี่ยงด้าน IT โดยครอบคลุมการดำเนินการดังนี้ 1. กำหนดผู้รับผิดชอบในการติดตามและทบทวนความเสี่ยง 2. การกำหนดดัชนีชี้วัดความเสี่ยงด้าน IT (IT key risk indicator) เพื่อให้สามารถติดตามแนวโน้มของความเสี่ยง และสามารถทบทวนมาตรการควบคุมความเสี่ยงได้อย่างมีประสิทธิภาพ 3. การติดตามความคืบหน้าของการดำเนินงานตามแผนการบริหารจัดการความเสี่ยงด้าน IT
(8) การรายงานความเสี่ยง (risk reporting) และผลการบริหารจัดการความเสี่ยงด้าน IT ต่อคณะกรรมการของผู้ประกอบธุรกิจหรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบธุรกิจ อย่างน้อยปีละ 1 ครั้ง	ผู้ประกอบธุรกิจควรจัดให้มีการรายงานระดับความเสี่ยง (risk reporting) และผลการบริหารจัดการความเสี่ยงด้าน IT ต่อคณะกรรมการของผู้ประกอบธุรกิจหรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบธุรกิจอย่างน้อยปีละ 1 ครั้ง โดยการรายงานระดับความเสี่ยงและผลการบริหารจัดการความเสี่ยงด้าน IT ควรครอบคลุมรายละเอียดอย่างน้อย ดังนี้ 1. ผลการประเมินความเสี่ยงและจัดการความเสี่ยงด้าน IT และความเสี่ยงด้านความเป็นส่วนตัว (privacy) จากการใช้งาน IT 2. แนวโน้มความเสี่ยงด้าน IT ที่อาจเกิดขึ้นกับผู้ประกอบธุรกิจ 3. ความคืบหน้าของการดำเนินงานตามแผนการบริหารจัดการความเสี่ยงด้าน IT

ข้อกำหนดในภาคผนวก 2 แนบท้ายประกาศที่ สธ. /25	แนวปฏิบัติ
2.2.2 นโยบายการรักษาความมั่นคงปลอดภัยด้าน IT (IT security policy) มีเรื่องที่ต้องครอบคลุม ดังนี้ (1) โครงสร้างการบริหารงานเพื่อการรักษาความมั่นคงปลอดภัยด้าน IT (2) การบริหารจัดการบุคลากรที่ปฏิบัติงานด้าน IT หรือบุคคลภายนอก (3) การบริหารจัดการทรัพย์สินด้าน IT (4) การรักษาความมั่นคงปลอดภัยของข้อมูล (5) การควบคุมการเข้าถึงและระบบ IT (6) การควบคุมการเข้ารหัส (7) การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (8) มาตรการรักษาความมั่งคงปลอดภัยในการปฏิบัติงานด้าน IT (9) มาตรการรักษาความมั่นคงปลอดภัยเกี่ยวกับระบบเครือข่ายสื่อสาร (10) การบริหารจัดการโครงการด้าน IT และการจัดหาพัฒนาและบำรุงรักษาระบบ IT) (11) การบริหารจัดการเหตุการณ์ผิดปกติด้าน IT และปัญหาด้าน IT (12) การจัดทำแผนฉุกเฉินด้าน IT	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]

ข้อกำหนดในภาคผนวก 2 แนบท้ายประกาศที่ สธ. /25	แนวปฏิบัติ
2.3 ผู้ประกอบธุรกิจต้องจัดให้มีการดำเนินการตามนโยบายใน 2.2 ดังนี้ 2.3.1 เปิดเผยนโยบายตาม 2.2 ในลักษณะที่สามารถเข้าถึงได้ง่าย และสื่อสารให้แก่บุคคลที่เกี่ยวข้อง[1] รับทราบอย่างทั่วถึง เพื่อให้บุคคลดังกล่าวเข้าใจและสามารถปฏิบัติตามได้อย่างถูกต้อง	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]
2.3.2 กำหนดขั้นตอนและวิธีปฏิบัติงานให้เป็นไปตามนโยบายตาม 2.2	ผู้ประกอบธุรกิจควรกำหนดขั้นตอนการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศเป็นลายลักษณ์อักษร เพื่อให้เจ้าหน้าที่ผู้ปฏิบัติงานด้าน IT สามารถปฏิบัติงานได้อย่างถูกต้องและเป็นไปตามนโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้าน IT นอกจากนี้ ผู้ประกอบธุรกิจควรกำหนดวิธีปฏิบัติสำหรับกรณีที่มีความจำเป็นให้ไม่สามารถปฏิบัติตามขั้นตอนและวิธีปฏิบัติงานที่ผู้ประกอบธุรกิจกำหนดไว้ โดยจัดให้มีการประเมินความเสี่ยง กำหนดแนวทางการควบคุมความเสี่ยงอย่างเพียงพอเหมาะสม และขออนุมัติจากผู้มีอำนาจก่อนดำเนินการต่อไป นอกจากนี้ ควรจัดเก็บหลักฐานการอนุมัติยกเว้นดังกล่าวอย่างเป็นลายลักษณ์อักษร และจัดให้มีกระบวนการสอบทานความเหมาะสมของรายการขออนุมัติยกเว้น ตลอดจนแนวทางการควบคุมความเสี่ยงอย่างน้อยปีละ 1 ครั้ง
2.3.3 ในกรณีที่มีการเปลี่ยนแปลงนโยบายดังกล่าว ต้องสื่อสารให้บุคคลที่เกี่ยวข้องได้รับทราบอย่างทั่วถึง และต้องปรับปรุงขั้นตอนและวิธีปฏิบัติงานให้สอดคล้องการเปลี่ยนแปลงดังกล่าว	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]
2.4 ผู้ประกอบธุรกิจต้องทบทวนหรือปรับปรุงนโยบายตาม 2.2 อย่างน้อยปีละ 1 ครั้ง หรือโดยไม่ชักช้าเมื่อมีเหตุการณ์ใด ๆ ซึ่งอาจส่งผลกระทบต่อการกำกับดูแลและบริหารจัดการความเสี่ยงด้าน IT อย่างมีนัยสำคัญ	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]

[1] บุคคลที่เกี่ยวข้อง หมายความว่า บุคลากร กรรมการ รวมถึงบุคคลภายนอก

หมวด 2 การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Information Technology Security)

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. /25	แนวปฏิบัติ
2.1 โครงสร้างการบริหารงานเพื่อการรักษาความมั่นคงปลอดภัยด้าน IT (organization of information technology security)	
ส่วนที่ 1 โครงสร้างการบริหารงานเพื่อการรักษาความมั่นคงปลอดภัยด้าน IT (organization of information technology security) ผู้ประกอบธุรกิจต้องดำเนินการจัดให้มีโครงสร้างดังกล่าว โดยมีลักษณะอย่างน้อยดังนี้	
1.1 กำหนดโครงสร้างภายในองค์กร (organizational structure) ในการปฏิบัติงานด้าน IT โดยมีรายละเอียดหน้าที่และความรับผิดชอบของบุคลากรเป็นลายลักษณ์อักษร	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]
1.2 แบ่งแยกหน้าที่ในการปฏิบัติงานที่เกี่ยวกับความมั่นคงปลอดภัยของระบบ IT เพื่อให้มีการสอบทานการปฏิบัติงาน และลดโอกาสในการแก้ไขเปลี่ยนแปลงหรือใช้งานทรัพย์สินด้าน IT โดยมิชอบหรือไม่ได้รับอนุญาต	ผู้ประกอบธุรกิจควรจัดให้มีการแบ่งแยกหน้าที่ในการปฏิบัติงานด้านต่าง ๆ ที่เกี่ยวกับความมั่นคงปลอดภัยของระบบ IT อย่างชัดเจน เพื่อให้มีการสอบทานการปฏิบัติงานระหว่างกันเพื่อป้องกันความเสี่ยงในการแก้ไขเปลี่ยนแปลงหรือใช้งานทรัพย์สินด้าน IT โดยมิชอบหรือไม่ได้รับอนุญาต เช่น 1. แบ่งแยกผู้พัฒนาระบบงาน (developer) ออกจากผู้ดูแลระบบ (system administrator) 2. แบ่งแยกผู้พัฒนาระบบงาน (developer) ออกจากผู้มีสิทธิในการนำระบบขึ้นใช้งานจริง 3. แบ่งแยกผู้ทำหน้าที่ปฏิบัติงานด้าน IT อื่น ๆ ออกจากผู้ดูแลระบบฐานข้อมูล (database administrator) เพื่อป้องกันการนำข้อมูลไปใช้ เปลี่ยนแปลงแก้ไขข้อมูล และลบข้อมูลโดยไม่ได้รับอนุญาต เป็นต้น
2.2 การบริหารจัดการบุคลากรที่ปฏิบัติงานด้าน IT หรือบุคคลภายนอก	
2.2.1 การบริหารจัดการบุคลากรที่ปฏิบัติงานด้าน IT	
ส่วนที่ 2 การบริหารจัดการบุคลากรที่ปฏิบัติงานด้าน IT หรือบุคคลภายนอก <u>บุคลากรที่ต้องบริหารจัดการ</u>	

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. /25	แนวปฏิบัติ
2.1 บุคลากรที่มีหน้าที่ดังนี้ 2.1.1 การปฏิบัติงานด้าน IT 2.1.2 การบริหารความเสี่ยงและกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง 2.1.3 การตรวจสอบด้าน IT 2.2 บุคลากรอื่นนอกจาก 2.1 ที่ใช้ระบบ IT ในการปฏิบัติงาน	
<u>การบริหารจัดการ</u> ผู้ประกอบธุรกิจต้องบริหารจัดการบุคลากรตาม 2.1 หรือ 2.2 อย่างเหมาะสม โดยดำเนินการอย่างน้อยดังนี้ (1) มีกระบวนการคัดเลือกบุคลากรในการปฏิบัติหน้าที่ดังนี้ (1.1) คำนึงถึงความรู้ ความสามารถ และความเพียงพอในการปฏิบัติงาน (1.2) มีการตรวจสอบข้อมูลของบุคลากรก่อนการว่าจ้างอย่างเพียงพอและสอดคล้องกับความเสี่ยงของตำแหน่งงานและหน้าที่ความรับผิดชอบ	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]
(2) มีการกำหนดเรื่องดังนี้ไว้ในข้อตกลงการจ้างงานเพื่อป้องกันการละเมิดหรือความเสียหายที่อาจเกิดขึ้นต่อทรัพย์สินด้าน IT ของผู้ประกอบธุรกิจ (2.1) บทบาทหน้าที่และความรับผิดชอบของบุคลากรดังกล่าวเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้าน IT	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. /25	แนวปฏิบัติ
(2.2) non-disclosure agreement	non-disclosure agreement ควรมีเนื้อหาขั้นต่ำ ดังนี้ 1. ความเป็นเจ้าของข้อมูลสำคัญทางธุรกิจ ทรัพย์สินทางปัญญา และวิธีป้องกันการรั่วไหลของข้อมูล 2. ขอบเขตความรับผิดชอบในการเก็บรักษาความลับ และไม่เปิดเผยข้อมูลโดยไม่ได้รับอนุญาต 3. กระบวนการแจ้งเตือนและรายงานผู้เกี่ยวข้องหากพบการรั่วไหลหรือเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต 4. มาตรการดำเนินการกรณีละเมิดหรือยกเลิกข้อตกลง รวมทั้งข้อกำหนดในการคืนหรือทำลายข้อมูลที่มีความสำคัญเมื่อสิ้นสุดข้อตกลง
(3) สร้างความตระหนักรู้เกี่ยวกับนโยบายและมาตรการรักษาความมั่นคงปลอดภัยของระบบ IT ให้แก่บุคลากรที่ปฏิบัติงานโดยมีการเข้าถึงข้อมูลหรือระบบงานภายในองค์กร เพื่อให้บุคลากรดังกล่าวสามารถปฏิบัติหน้าที่ได้ตามนโยบายและมาตรการที่กำหนด	1. ผู้ประกอบธุรกิจควรส่งเสริมและพัฒนาความรู้ด้าน IT (training program) ให้แก่บุคลากรของผู้ประกอบธุรกิจอย่างสม่ำเสมอ เช่น การจัดการอบรมภายในองค์กร หรือส่งบุคลากรเข้าร่วมฝึกอบรมภายนอกองค์กร เป็นต้น เพื่อให้บุคลากรมีความรู้ความเข้าใจถึงการใช้ IT ที่ถูกต้องปลอดภัย และลดความเสี่ยงที่อาจเกิดขึ้น โดยมีเนื้อหาครอบคลุม ดังนี้ (ก) ตระหนักถึงความเสี่ยงและการรักษาความมั่นคงปลอดภัยด้าน IT (ข) ความเสี่ยงด้าน IT และความเสี่ยงด้านความเป็นส่วนตัว (privacy) จากการใช้งาน IT (ค) หลักเกณฑ์และกฎหมายที่เกี่ยวข้องกับ IT 2. ผู้ประกอบธุรกิจควรจัดให้มีการเสริมสร้างความตระหนักเรื่องการรักษาความมั่นคงปลอดภัยด้าน IT ความเสี่ยงด้าน IT และความเสี่ยงด้านความเป็นส่วนตัว (privacy) จากการใช้งาน IT อย่างสม่ำเสมอ ให้แก่บุคลากร (user) ที่สามารถเข้าถึงข้อมูลที่มีความสำคัญของผู้ประกอบธุรกิจหรือข้อมูลของผู้ใช้บริการ เช่น การทดสอบเรื่องอีเมลหลอกลวง (phishing) การทดสอบเรื่องวิศวกรรมสังคม (social engineering) และการซักซ้อมแผนเพื่อเตรียมความพร้อมรับมือกับการโจมตีทางไซเบอร์ เป็นต้น 3. ผู้ประกอบธุรกิจควรทบทวนแผนการส่งเสริมและพัฒนาความรู้ด้าน IT (training program) อย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่าเนื้อหาและรายละเอียดของแผนงานที่เกี่ยวข้องยังคงเพียงพอเหมาะสมกับแนวโน้มความเสี่ยงด้าน IT ในปัจจุบัน
(4) กำหนดให้บุคลากรดังกล่าวงดเว้นการใช้งานระบบ IT ในลักษณะที่อาจก่อให้เกิดความเสียหายแก่ผู้ประกอบธุรกิจ ตลาดทุนโดยรวม หรือที่เป็นการกระทำผิดกฎหมาย หรือข้อกำหนดและจรรยาบรรณที่ผู้ประกอบธุรกิจกำหนดไว้ (ถ้ามี)	ผู้ประกอบธุรกิจควรจัดให้มีเอกสารข้อกำหนดในการใช้งานทรัพย์สินด้าน IT (acceptable use policy) โดยครอบคลุมขอบเขตความรับผิดชอบของผู้ใช้งาน สิ่งที่ผู้ใช้งานพึงปฏิบัติ และสิ่งที่ผู้ใช้งานห้ามปฏิบัติ

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. /25	แนวปฏิบัติ
(5) กำหนดมาตรการในการลงโทษบุคลากรที่มีพฤติกรรมฝ่าฝืนหรือไม่ปฏิบัติตามนโยบายและมาตรการรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้าน IT	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]
(6) กำหนดขั้นตอนปฏิบัติเมื่อสิ้นสุดการจ้างงาน หรือยกเลิกข้อตกลงการจ้างบุคลากร เพื่อป้องกันการละเมิดหรือความเสียหายที่อาจเกิดขึ้นต่อทรัพย์สินด้าน IT	ผู้ประกอบธุรกิจควรจัดให้มีกระบวนการรองรับเมื่อมีการเปลี่ยนแปลงตำแหน่งงานหรือสิ้นสุดการจ้างงาน เช่น การคืนทรัพย์สินขององค์กร การปรับปรุงสิทธิให้เป็นปัจจุบัน และยกเลิกสิทธิเมื่อสิ้นสุดการจ้างงาน เป็นต้น รวมทั้งมีการสื่อสารให้ผู้ที่เกี่ยวข้องรับทราบถึงการเปลี่ยนแปลงสิทธิ หน้าที่ และความรับผิดชอบ เป็นต้น
2.2.2 การบริหารจัดการบุคคลภายนอก (third-party management)	
<u>บุคลากรที่ต้องบริหารจัดการ</u> 2.3 บุคคลภายนอก ในกรณีที่ผู้ประกอบธุรกิจมีการดำเนินการอย่างใดอย่างหนึ่งดังนี้ 2.3.1 ใช้บริการงานด้าน IT จากบุคคลภายนอก 2.3.2 เชื่อมต่อกับระบบ IT ของบุคคลภายนอก 2.3.3 อนุญาตให้บุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญหรือข้อมูลของลูกค้าที่ควบคุมดูแลโดยผู้ประกอบธุรกิจได้	

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. /25	แนวปฏิบัติ
<u>การบริหารจัดการ</u> ผู้ประกอบธุรกิจต้องบริหารจัดการบุคคลภายนอกตาม 2.3.1 , 2.3.2 หรือ 2.3.3 ดังนี้ (1) ประเมินความเสี่ยงจากการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก รวมถึงผู้รับดำเนินการช่วง (subcontract) จากบุคคลภายนอก (ถ้ามี)	ผู้ประกอบธุรกิจควรประเมินความเสี่ยงและผลกระทบก่อน (1) การใช้บริการงานด้าน IT จากบุคคลภายนอก (2) การเชื่อมต่อระบบ IT กับบุคคลภายนอก และ (3) การอนุญาตให้บุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญหรือข้อมูลของลูกค้าที่ควบคุมดูแลโดยผู้ประกอบธุรกิจได้ โดยคำนึงถึงความเสี่ยงดังนี้ 1. ความเสี่ยงด้านกฎหมาย และกฎเกณฑ์ที่เกี่ยวข้องทั้งในประเทศและต่างประเทศ เช่น กฎหมายเกี่ยวกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ กฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล และกฎหมายเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ เป็นต้น 2. ความเสี่ยงจากการกำกับดูแลและบริหารจัดการบุคคลภายนอกที่ไม่รัดกุมเพียงพอ (operational risk) 3. ความเสี่ยงจากการกระจุกตัว (concentration risk) เช่น ผู้ประกอบธุรกิจและบริษัทในกลุ่มธุรกิจเดียวกันใช้บริการจากบุคคลภายนอกเพียงรายเดียว เป็นต้น 4. ความเสี่ยงจากการพึ่งพาบุคคลภายนอกรายใดรายหนึ่งเป็นหลัก (third party/vendor locked-in) ซึ่งทำให้มีข้อจำกัดในการเปลี่ยนแปลงเทคโนโลยี ผู้ให้บริการ หรือข้อจำกัดในการนำระบบหรือข้อมูลกลับมาดำเนินการเอง 5. ความเสี่ยงด้าน IT และภัยทางไซเบอร์ เช่น ระบบที่ให้บริการโดยบุคคลภายนอกเกิดขัดข้อง ระบบของบุคคลภายนอกมีช่องโหว่ทำให้ข้อมูลเกิดการสูญหายหรือรั่วไหล เป็นต้น 6. ความเสี่ยงกรณีบุคคลภายนอกให้ผู้อื่นดำเนินการแทน (sub-contracting) เช่น subcontractor ปฏิบัติงานบกพร่อง เป็นต้น นอกจากนี้ ควรทบทวนความเสี่ยงเป็นประจำตามรอบระยะเวลาที่สอดคล้องกับระดับความเสี่ยงและความสำคัญของบุคคลภายนอก

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. /25	แนวปฏิบัติ
(2) กำหนดวิธีปฏิบัติและหลักเกณฑ์ในการคัดเลือกบุคคลภายนอก	ผู้ประกอบธุรกิจควรกำหนดกระบวนการ และหลักเกณฑ์การคัดเลือกบุคคลภายนอก (due diligence) โดยให้ความสำคัญในการพิจารณาความมั่นคงปลอดภัยของบุคคลภายนอกและศักยภาพในการให้บริการ เพื่อให้มั่นใจว่าบุคคลภายนอกสามารถให้บริการได้อย่างต่อเนื่อง และสามารถตอบสนองความต้องการของบริษัทได้ โดยในกรณีบุคคลภายนอกรายที่มีนัยสำคัญ (critical third party) ตามผลการประเมินความเสี่ยงในข้อ (1) ผู้ประกอบธุรกิจควรคำนึงถึงเรื่องดังนี้ 1. ฐานะทางการเงิน ชื่อเสียง ความรู้ความเชี่ยวชาญ ประสบการณ์ และความสามารถในการให้บริการในช่วงที่ผ่านมา และระบบการบริหารงานภายใน 2. การบริหารจัดการความเสี่ยง การควบคุมภายใน การตรวจสอบภายใน และการติดตามผลการปฏิบัติงาน 3. การรักษาความมั่นคงปลอดภัยด้าน IT 4. การบริหารจัดการความต่อเนื่องทางธุรกิจ และความพร้อมรับมือภัยหรือเหตุการณ์ต่าง ๆ 5. การปฏิบัติตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้อง เช่น การขอตรวจสอบเอกสารหลักฐานหรือใบรับรองจากบุคคลภายนอกในการดำเนินการตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้อง เป็นต้น 6. การปฏิบัติตามมาตรฐานสากลด้าน IT เช่น การขอตรวจสอบ หรือสามารถแสดงเอกสารหลักฐานการได้รับการรองรับตามมาตรฐาน ISO 27001 เป็นต้น โดยการรับรองการปฏิบัติตามมาตรฐานสากล ผู้ประกอบธุรกิจควรพิจารณาว่าบุคคลภายนอกได้รับการรับรองการให้บริการในส่วนที่ผู้ประกอบธุรกิจใช้บริการ เชื่อมต่อ หรือเข้าถึงข้อมูล หรือได้รับการรับรองครอบคลุมทั้งองค์กร 7. การใช้เทคโนโลยีแบบเปิด (open technology) เพื่อให้สามารถนำระบบไปใช้งานหรือเชื่อมโยงกับระบบอื่นได้ (interoperability) และลดข้อจำกัดในการย้ายหรือเปลี่ยนแปลงเทคโนโลยีผู้ให้บริการหรือพันธมิตร รวมถึงข้อจำกัดในการนำระบบหรือข้อมูลกลับมาดำเนินการเอง เช่น การใช้รูปแบบการรับส่งข้อมูลกับบุคคลภายนอกที่เป็นมาตรฐานแบบเปิด (open standard หรือ open source) เป็นต้น 8. กรณีที่บุคคลภายนอกมอบหมายการปฏิบัติงานที่สำคัญให้กับบุคคลอื่นต่อ (sub-contracting to another supplier) ผู้ประกอบธุรกิจควรพิจารณารายละเอียดด้านความมั่นคงปลอดภัยสารสนเทศของบุคคลดังกล่าวด้วย

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. /25	แนวปฏิบัติ
	9. [ความเสี่ยงสูง] ผู้ประกอบธุรกิจควรจัดให้มีการประเมินด้านคุณภาพและความน่าเชื่อถือของบุคคลภายนอก โดยพิจารณาจากประสบการณ์ คุณภาพของบริการและผลงานที่ส่งมอบ ตลอดจนมาตรฐานด้านความปลอดภัย IT ที่เกี่ยวข้องกับสินค้าและบริการ และจัดทำเป็นรายชื่อบุคคลภายนอกที่เชื่อถือได้ (trusted third-party/trusted vendor) เพื่อใช้เป็นส่วนหนึ่งของเกณฑ์การคัดเลือกผู้ให้บริการในอนาคต
(3) กำหนดบทบาท หน้าที่ และความรับผิดชอบของผู้ประกอบธุรกิจและบุคคลภายนอกอย่างชัดเจนและเป็นลายลักษณ์อักษร	ผู้ประกอบธุรกิจควรจัดทำสัญญาหรือข้อตกลงการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอกเป็นลายลักษณ์อักษร โดยมีการลงนามร่วมกันระหว่างผู้ประกอบธุรกิจและบุคคลภายนอก เพื่อให้มั่นใจได้ว่าบุคคลภายนอกมีหน้าที่รับผิดชอบในการรักษาความมั่นคงปลอดภัยของระบบ IT ในระดับที่เหมาะสม โดยควรพิจารณาการกำหนดรายละเอียด ดังนี้ 1. ขอบเขตการให้บริการ การเชื่อมต่อ และการเข้าถึงข้อมูลจากบุคคลภายนอก 2. บทบาท หน้าที่ และความรับผิดชอบของบุคคลภายนอกและผู้ประกอบธุรกิจ 3. การรักษาความปลอดภัยของระบบ IT 4. ข้อตกลงระดับการให้บริการด้าน IT (service level agreement: SLA) สำหรับการใช้บริการจากบุคคลภายนอก 5. การรักษาความปลอดภัยและการคุ้มครองข้อมูลลับหรือข้อมูลสำคัญ ทรัพย์สินทางปัญญา และลิขสิทธิ์ของผู้ประกอบธุรกิจตามกฎหมายและหลักเกณฑ์ของทางการที่เกี่ยวข้อง 6. รายละเอียดของข้อมูลที่จำเป็นต้องใช้หรือเข้าถึงโดยบุคคลภายนอก รวมทั้งวิธีการเข้าถึงข้อมูลดังกล่าว 7. การติดตามและรายงานผลการปฏิบัติงานของบุคคลภายนอก ซึ่งครอบคลุมถึงการแจ้งการเปลี่ยนแปลงหรือเหตุการณ์ที่สำคัญและการรายงานปัญหาผิดปกติอย่างทันการณ์ 8. รายชื่อและช่องทางสำหรับติดต่อบุคคลหรือหน่วยงานที่เกี่ยวข้อง โดยเฉพาะช่องการติดต่อในเรื่องการรักษาความมั่นคงปลอดภัยของระบบ IT 9. การทำลายข้อมูลเมื่อสิ้นสุดหรือยกเลิกการใช้บริการ การเชื่อมต่อ และการเข้าถึงข้อมูลจากบุคคลภายนอก 10. ในกรณีเป็นการใช้บริการงานด้าน IT จากบุคคลภายนอกรายที่มีนัยสำคัญตามผลการประเมินความเสี่ยง ผู้ประกอบธุรกิจควรระบุสิทธิในการพิจารณาอนุมัติกรณีบุคคลภายนอกว่าจ้าง subcontract และข้อกำหนดให้บุคคลภายนอกต้องรับผิดชอบต่อผลการปฏิบัติงานของ subcontract

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. /25	แนวปฏิบัติ
	11. เงื่อนไขหรือสิทธิของผู้ประกอบธุรกิจในการเปลี่ยนแปลง ยุติ หรือยกเลิกสัญญาหรือข้อตกลงกับบุคคลภายนอก 12. การจัดให้มีแผนบริหารจัดการเหตุการณ์ผิดปกติและปัญหาด้าน IT (incident response plan) หรือแผนฉุกเฉินด้าน IT (IT contingency plan) 13. ความรับผิดชอบต่อความเสียหายที่เกิดจากบุคคลภายนอก เช่น กรณีการให้บริการไม่เป็นไปตาม SLA ที่กำหนดไว้ เป็นต้น 14. หากมีข้อจำกัดในการระบุรายละเอียดและกำหนดเงื่อนไขที่สำคัญลงในข้อตกลงหรือสัญญาที่ทำกับบุคคลภายนอก ผู้ประกอบธุรกิจควรมีการประเมินความเสี่ยงและพิจารณาแนวทางควบคุมความเสี่ยงที่เพียงพอเหมาะสม พร้อมทั้งขออนุมัติยกเว้น (exception) จากผู้มีอำนาจ
(4) กรณีเป็นบุคคลภายนอกรายที่มีนัยสำคัญตามผลการประเมินความเสี่ยงใน 2.3 (1) ข้อตกลงหรือสัญญาการให้บริการต้องระบุสิทธิให้ผู้ประกอบธุรกิจ สำนักงาน และผู้ตรวจสอบภายนอกที่ได้รับการแต่งตั้งจากผู้ประกอบธุรกิจหรือสำนักงาน สามารถเข้าตรวจสอบการดำเนินงานและการควบคุมภายในของบุคคลภายนอกดังกล่าว ในส่วนที่เกี่ยวข้องการกับใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลของผู้ประกอบธุรกิจจากบุคคลภายนอก หากมีเหตุจำเป็นทำให้ผู้ประกอบธุรกิจไม่สามารถระบุสิทธิในการเข้าตรวจสอบตามวรรคหนึ่งไว้ในข้อตกลงหรือสัญญา ผู้ประกอบธุรกิจต้องมีมาตรการประเมินหรือติดตามการดำเนินงานและการควบคุมภายในของบุคคลภายนอกให้รัดกุมเพียงพอสอดคล้องกับความเสี่ยงและความมีนัยสำคัญของการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูล	ผู้ประกอบธุรกิจควรกำหนดสิทธิการเข้าตรวจสอบการดำเนินการและการควบคุมภายในของบุคคลภายนอกเป็นส่วนหนึ่งของข้อตกลงหรือสัญญาการให้บริการ ในกรณีที่ไม่สามารถระบุสิทธิดังกล่าวได้ ผู้ประกอบธุรกิจควรพิจารณาเลือกใช้บุคคลภายนอกที่มีการดำเนินการตรวจสอบด้าน IT โดยผู้ตรวจสอบภายนอกที่มีความเป็นอิสระและได้มาตรฐานสากล เช่น ผลการตรวจสอบตามมาตรฐาน SSAE 18 (SOC 2 Type 2 Report) หรือ PCI-DSS Attestation of Compliance (AOC) เป็นต้น นอกจากนี้ ผู้ประกอบธุรกิจควรพิจารณารายละเอียดของผลการตรวจสอบที่จัดทำโดยผู้ตรวจสอบภายนอกอย่างเหมาะสม

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. /25	แนวปฏิบัติ
(5) มี non-disclosure agreement สำหรับบุคคลภายนอกหรือผู้รับดำเนินการช่วงของบุคคลภายนอก ในกรณีที่บุคคลดังกล่าวสามารถเข้าถึงข้อมูลสำคัญของผู้ประกอบธุรกิจหรือข้อมูลของลูกค้า	1. non-disclosure agreement ควรมีรายละเอียดครอบคลุมขอบเขตความรับผิดชอบในการเก็บรักษาความลับ การไม่เปิดเผยข้อมูลโดยไม่ได้รับอนุญาต การรายงานผู้ประกอบธุรกิจเมื่อพบการรั่วไหลหรือเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต และการทำลายข้อมูลที่มีความสำคัญเมื่อสิ้นสุดข้อตกลงหรือสัญญา 2. ในกรณีต้องมีการเปิดเผยข้อมูลชั้นความลับจากเหตุทางกฎหมายหรือความจำเป็นตามสัญญา ผู้ประกอบธุรกิจควรกำหนดให้บุคคลภายนอก และผู้รับดำเนินการช่วง (sub-contract) มีการแจ้งและขอความยินยอมจากผู้ประกอบธุรกิจก่อนเปิดเผยต่อบุคคลอื่น
(6) กำกับดูแล ติดตาม และบริหารจัดการความเสี่ยงจากการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก โดยต้องสอดคล้องกับระดับความเสี่ยงและระดับความมีนัยสำคัญของบุคคลภายนอก	ผู้ประกอบธุรกิจควรกำกับดูแล ติดตาม และบริหารจัดการความเสี่ยงจากการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก โดยดำเนินการดังนี้ 1. กำหนดผู้รับผิดชอบและจัดการติดตามผลการปฏิบัติงานของบุคคลภายนอกอย่างต่อเนื่อง โดยพิจารณาตามขอบเขต ระดับความเสี่ยงและความมีนัยสำคัญของการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก 2. จัดให้มีมาตรการควบคุมและติดตามสิทธิการเข้าถึงข้อมูลสารสนเทศของบุคคลภายนอกอย่างสม่ำเสมอ เพื่อให้สิทธิดังกล่าวเป็นไปตามหลักความจำเป็นในการรู้ข้อมูล (need-to-know basis) 3. ประเมินผลการปฏิบัติงานหรือการใช้บริการ ทั้งในด้านประสิทธิภาพของบริการ การรักษาความมั่นคงปลอดภัย การรักษาความเสี่ยงส่วนตัว (privacy) และการปฏิบัติตามกฎหมายที่เกี่ยวข้อง เมื่อจะต่อสัญญาหรือเมื่อถึงรอบระยะเวลาที่ผู้ประกอบธุรกิจกำหนด 4. ทบทวนคุณสมบัติบุคคลภายนอกอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าบุคคลภายนอกยังคงมีคุณสมบัติที่เหมาะสม
(7) รักษาความมั่นคงปลอดภัยด้าน IT จากการใช้บริการการเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอกที่สอดคล้องกับมาตรฐานการรักษาความมั่นคงปลอดภัยด้าน IT ของผู้ประกอบธุรกิจ	1. ผู้ประกอบธุรกิจควรจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยในการเคลื่อนย้ายหรือถ่ายโอนข้อมูลสารสนเทศระหว่างผู้ประกอบธุรกิจกับบุคคลภายนอก 2. ผู้ประกอบธุรกิจควรมีมาตรการควบคุมความถูกต้องครบถ้วนของข้อมูลและการประมวลผลข้อมูลที่ได้รับจากบุคคลภายนอก

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. /25	แนวปฏิบัติ
(8) เตรียมความพร้อมรับมือต่อเหตุการณ์ผิดปกติด้าน IT และปัญหาด้าน IT ที่อาจเกิดขึ้นและมีผลกระทบอย่างมีนัยสำคัญ เพื่อให้สามารถให้บริการหรือดำเนินธุรกิจได้อย่างต่อเนื่อง	ผู้ประกอบธุรกิจควรจัดให้มีแผนรองรับในกรณีที่บุคคลภายนอกเกิดเหตุการณ์ผิดปกติด้าน IT (incident response policy) และปัญหาด้าน IT ซึ่งมีผลกระทบกับการดำเนินการของผู้ประกอบธุรกิจ โดยครอบคลุมเหตุการณ์ที่เกี่ยวข้องกับเหตุการณ์ความปลอดภัยทางไซเบอร์ และเหตุการณ์การละเมิดต่อข้อมูลส่วนบุคคล
2.3 การบริหารจัดการทรัพย์สินด้าน IT (IT asset management)	
ส่วนที่ 3 การบริหารจัดการทรัพย์สินด้าน IT (IT asset management) ผู้ประกอบธุรกิจต้องจัดให้มีการบริหารจัดการทรัพย์สินด้าน IT เพื่อนำไปใช้ดำเนินการเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้าน IT ได้อย่างเหมาะสม ครบถ้วนและเป็นปัจจุบัน ดังนี้	
3.1 จัดทำทะเบียนรายการทรัพย์สินด้าน IT ประเภทฮาร์ดแวร์ ซอฟต์แวร์ รวมถึงสิทธิในการใช้งานฮาร์ดแวร์และซอฟต์แวร์	1. ผู้ประกอบธุรกิจควรกำหนดระเบียบปฏิบัติเกี่ยวกับการบริหารจัดการทรัพย์สินด้าน IT เพื่อให้ทะเบียนทรัพย์สินมีความครบถ้วนและเป็นปัจจุบัน ได้แก่ การจัดทำทะเบียนรายการทรัพย์สิน การปรับปรุงทะเบียนรายการทรัพย์สิน การยกเลิกและเรียกคืนทรัพย์สิน โดยครอบคลุมทั้งทรัพย์สินที่บริหารจัดการโดยผู้ประกอบธุรกิจเอง และทรัพย์สินที่บริหารจัดการโดยบุคคลภายนอก 2. ผู้ประกอบธุรกิจควรจัดทำทะเบียนรายการทรัพย์สินด้าน IT ประเภทอุปกรณ์ (hardware) รวมถึง virtual machine ให้ครบถ้วนและเป็นปัจจุบัน โดยครอบคลุมรายละเอียด ตัวอย่างเช่น (1) เลขทะเบียนทรัพย์สิน (2) ประเภทฮาร์ดแวร์ (3) รายละเอียดทางเทคนิค ยี่ห้อ รุ่น (4) ระบบปฏิบัติการและเวอร์ชัน (5) เจ้าของทรัพย์สิน (6) ผู้ดูแลทรัพย์สิน (7) สถานที่ตั้ง (8) วันที่เริ่มใช้งาน/วันที่ติดตั้ง

<table>
<tr><th>ข้อกำหนดในภาคผนวก 3
แนบท้ายประกาศที่ สธ. /25</th><th>แนวปฏิบัติ</th></tr>
<tr><td></td><td>
(9) วันที่สิ้นสุดการรับประกัน หรือสิ้นสุดการใช้งานตามสัญญา
(10) ประเภทการครอบครอง (ซื้อ หรือเช่า)
<u>ตัวอย่างเช่น</u>
<table>
<tr><th>เลขทะเบียนทรัพย์สิน</th><th>ประเภท</th><th>รายละเอียด</th><th>ระบบปฏิบัติการ/เวอร์ชัน</th><th>เจ้าของทรัพย์สิน</th><th>ผู้ดูแลทรัพย์สิน</th><th>สถานที่ตั้ง</th><th>วันที่เริ่มใช้งาน</th><th>วันที่สิ้นสุดประกัน</th><th>การครอบครอง</th></tr>
<tr><td>RT123456</td><td>Switch</td><td>ยี่ห้อ CC รุ่น 1000 48 ports</td><td>A-OS 1.0.2</td><td>ฝ่าย IT</td><td>บริษัท A</td><td>สำนักงาน</td><td>1 มี.ค. 64</td><td>1 มี.ค. 67</td><td>ซื้อ</td></tr>
<tr><td>SV212224</td><td>Router</td><td>ยี่ห้อ JP รุ่น 3700 8 ports</td><td>13.2B</td><td>ฝ่าย IT</td><td>ฝ่าย IT</td><td>สำนักงาน</td><td>5 พ.ค. 64</td><td>5 พ.ค. 66</td><td>เช่า</td></tr>
</table>
3. ผู้ประกอบธุรกิจควรจัดทำทะเบียนรายการทรัพย์สินด้าน IT ประเภทระบบ (software) ให้ครบถ้วนและเป็นปัจจุบัน โดยครอบคลุมรายละเอียด ตัวอย่างเช่น
(1) เลขทะเบียนทรัพย์สิน
(2) ชื่อซอฟต์แวร์
(3) รายละเอียดทางเทคนิค / การใช้งาน
(4) ระบบปฏิบัติการและเวอร์ชัน
(5) หน่วยงานภายในผู้เป็นเจ้าของซอฟต์แวร์
(6) วันลงทะเบียนซอฟต์แวร์
(7) วันที่สิ้นสุดการใช้บริการ
</td></tr>
</table>

<table>
<tr><th>ข้อกำหนดในภาคผนวก 3
แนบท้ายประกาศที่ สธ. /25</th><th>แนวปฏิบัติ</th></tr>
<tr><td></td><td>(8) เลขทะเบียนทรัพย์สินฮาร์ดแวร์ที่อ้างอิง
<u>ตัวอย่างเช่น</u>
<table>
<tr><th>เลขทะเบียนทรัพย์สิน</th><th>ชื่อซอฟต์แวร์</th><th>รายละเอียดทางเทคนิค / การใช้งาน</th><th>ระบบปฏิบัติการและเวอร์ชัน</th><th>หน่วยงานภายในผู้เป็นเจ้าของซอฟต์แวร์</th><th>วันลงทะเบียนซอฟต์แวร์</th><th>วันที่สิ้นสุดการใช้บริการ</th><th>เลขทะเบียนทรัพย์สินฮาร์ดแวร์ (เพื่อใช้อ้างอิง)</th></tr>
<tr><td>SP123456</td><td>Sheet processor pro</td><td>Software ประมวลผล sheet/excel</td><td>10.2.3A</td><td>IT</td><td>1 พ.ค. 64</td><td>1 ธ.ค. 69</td><td>SV123456</td></tr>
</table>
4. ผู้ประกอบธุรกิจควรปรับปรุงทะเบียนทรัพย์สินสารสนเทศต่าง ๆ ให้ครบถ้วนและเป็นปัจจุบันอยู่อย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ</td></tr>
<tr><td>3.2 กำหนดบุคคลหรือหน่วยงานซึ่งรับผิดชอบทรัพย์สินด้าน IT แต่ละรายการ</td><td>ผู้ประกอบธุรกิจควรกำหนดบุคคลหรือหน่วยงานที่รับผิดชอบในการจัดทำ ปรับปรุงทะเบียนรายการทรัพย์สิน และบำรุงรักษาทรัพย์สินด้าน IT อย่างสม่ำเสมอตลอดอายุการใช้งานของทรัพย์สินดังกล่าว</td></tr>
<tr><td>3.3 จัดให้มีการบำรุงรักษาทรัพย์สินด้าน IT อย่างสม่ำเสมอ</td><td>ผู้ประกอบธุรกิจควรบำรุงรักษาทรัพย์สินด้าน IT ให้มีสภาพพร้อมใช้งานและรองรับการดำเนินธุรกิจอย่างต่อเนื่อง พร้อมทั้งวางแผนรองรับทรัพย์สินด้าน IT ที่ใกล้จะสิ้นสุดอายุการใช้งาน (end of life) หรือสิ้นสุดการสนับสนุนหรือให้บริการจากผู้ผลิต (end of support) ได้อย่างเหมาะสมทันการณ์ ทั้งนี้ ในกรณีที่มีความจำเป็นต้องใช้ทรัพย์สินที่สิ้นสุดอายุการใช้งานหรือสิ้นสุดการสนับสนุนหรือให้บริการจากผู้ผลิต ผู้ประกอบธุรกิจควรประเมินความเสี่ยงและจัดให้มีมาตรการควบคุมความเสี่ยงอย่างเหมาะสม</td></tr>
</table>

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. /25	แนวปฏิบัติ
2.4 การรักษาความมั่นคงปลอดภัยของข้อมูล (data security)	
ส่วนที่ 4 การรักษาความมั่นคงปลอดภัยของข้อมูล (Data Security) ผู้ประกอบธุรกิจต้องจัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลอย่างถูกต้องครบถ้วน มีสภาพพร้อมใช้งาน รวมถึงสามารถรักษาความลับและคุ้มครองข้อมูลส่วนบุคคลได้อย่างเหมาะสม ดังนี้	
4.1 การกำหนดบุคคลหรือหน่วยงานซึ่งเป็นเจ้าของข้อมูล	ผู้ประกอบธุรกิจควรกำหนดบุคคลหรือหน่วยงานเป็นเจ้าของข้อมูล (data owner) เพื่อรับผิดชอบในการกำหนดผู้ใช้งาน สิทธิการเข้าถึง วิธีปฏิบัติในการใช้งานข้อมูลอย่างปลอดภัย และการอนุมัติแก้ไขเปลี่ยนแปลงข้อมูล
4.2 การจัดชั้นความลับของข้อมูล (data classification) และแนวทางการรักษาความปลอดภัยของข้อมูลที่สอดคล้องตามชั้นความลับ โดยครอบคลุมข้อมูลดังนี้ 4.2.1 ข้อมูลที่อยู่บนอุปกรณ์ที่ใช้ปฏิบัติงาน (data at endpoint) 4.2.2 ข้อมูลที่อยู่ระหว่างการรับส่งผ่านเครือข่าย (data in transit)	1. ผู้ประกอบธุรกิจควรกำหนดหลักเกณฑ์การจัดชั้นความลับของข้อมูล (data classification) และวิธีการจัดการข้อมูล (data handling) ตามชั้นความลับให้ครอบคลุมตลอดวงจรชีวิตของข้อมูล (data life cycle) ตั้งแต่การสร้างหรือการได้มาซึ่งข้อมูล การประมวลผล การจัดเก็บ การใช้งาน ไปจนถึงการทำลายข้อมูล รวมทั้งระบุชั้นความลับของข้อมูล (labeling) อย่างชัดเจน 2. ผู้ประกอบธุรกิจควรกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล ตลอดจนความเป็นส่วนตัวที่สอดคล้องตามชั้นความลับ ครอบคลุม (1) ข้อมูลที่อยู่บนอุปกรณ์ที่ใช้ปฏิบัติงาน (data at endpoint) (2) ข้อมูลที่อยู่ระหว่างการรับส่งผ่านเครือข่าย (data in transit) (3) ข้อมูลที่อยู่บนระบบงานและสื่อบันทึกข้อมูล (data at rest)
4.2.3 ข้อมูลที่อยู่บนระบบงานและสื่อบันทึกข้อมูล (data at rest)	ผู้ประกอบธุรกิจควรจัดให้มีการรักษาความปลอดภัยของข้อมูลที่อยู่บนสื่อบันทึกข้อมูล โดยดำเนินการดังนี้ 1. คำนึงถึงความเสี่ยงที่สื่อบันทึกข้อมูลอาจเสื่อมสภาพ รวมทั้งวิธีการนำข้อมูลกลับมาใช้งานใหม่ ในกรณีที่จัดเก็บข้อมูลเป็นระยะเวลานาน 2. จัดเก็บสื่อบันทึกข้อมูลในพื้นที่ที่มีความมั่นคงปลอดภัย และเป็นไปตามคำแนะนำของผู้ผลิต (ถ้ามี) 3. จัดให้มีมาตรการรักษาความปลอดภัยของสื่อบันทึกข้อมูลระหว่างการขนส่ง (physical media transfer)

<table>
<tr><th>ข้อกำหนดในภาคผนวก 3
แนบท้ายประกาศที่ สธ. /25</th><th>แนวปฏิบัติ</th></tr>
<tr><td>4.3 การจัดให้มีแนวทางในการนำเข้า ประมวลผล และทำลายข้อมูลอย่างปลอดภัย</td><td>ผู้ประกอบธุรกิจควรกำหนดระเบียบปฏิบัติในการทำลายข้อมูล (data disposal) ซึ่งครอบคลุมหน้าที่ความรับผิดชอบของหน่วยงานที่เกี่ยวข้อง และวิธีการทำลายข้อมูลให้สอดคล้องกับระดับชั้นความลับ นอกจากนี้ควรมีกระบวนการควบคุมการทำลายข้อมูลที่ครอบคลุมการขออนุมัติจากเจ้าของข้อมูล (data owner) ก่อนดำเนินการ การสอบทานการปฏิบัติงาน และการทำทะเบียนการทำลายข้อมูลสำคัญ</td></tr>
<tr><td>4.4 การจัดทำทะเบียนทรัพย์สินด้าน IT ประเภทข้อมูล (data Inventory) ให้ครบถ้วนและเป็นปัจจุบัน</td><td>ผู้ประกอบธุรกิจควรจัดทำทะเบียนทรัพย์สินประเภทข้อมูล (data inventory) ให้ครบถ้วนและเป็นปัจจุบัน โดยครอบคลุมรายละเอียด ตัวอย่างเช่น
1. เลขทะเบียนข้อมูล
2. ชื่อข้อมูลหรือชุดข้อมูล
3. รายละเอียดลักษณะ และประเภทของข้อมูล
4. ระดับชั้นความลับและระดับความสำคัญของข้อมูล
5. เจ้าของข้อมูลและผู้ดูแลข้อมูล (data owner)
6. สถานที่ หรือเครื่องแม่ข่ายที่จัดเก็บ
<u>ตัวอย่างเช่น</u>
<table>
<tr><th>เลขทะเบียนข้อมูล</th><th>ชื่อข้อมูล/ชุดข้อมูล</th><th>รายละเอียด</th><th>ระดับชั้นความลับ</th><th>เจ้าของข้อมูล</th><th>ผู้ดูแลข้อมูล</th><th>สถานที่จัดเก็บ</th></tr>
<tr><td>ABC-IT-001</td><td>IT security policy</td><td>นโยบายด้าน IT</td><td>Internal</td><td>ฝ่าย IT</td><td>ฝ่าย IT</td><td>- ฝ่าย IT</td></tr>
<tr><td>ABC-Data-002</td><td>Customer information</td><td>ข้อมูลของลูกค้า ได้แก่ ชื่อ สกุล วัน เดือนปีเกิด</td><td>Confidential</td><td>ฝ่ายปฏิบัติการหลักทรัพย์</td><td>ฝ่าย IT</td><td>- DB server 015
- DB backup 012</td></tr>
</table>
</td></tr>
</table>

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. /25	แนวปฏิบัติ
2.5 การควบคุมการเข้าถึงข้อมูลและระบบ IT (access control)	
ส่วนที่ 5 การควบคุมการเข้าถึงข้อมูลและระบบ IT (access control) ผู้ประกอบธุรกิจต้องจัดให้มีการควบคุมการเข้าถึงข้อมูลและระบบ IT อย่างมีประสิทธิภาพ เพื่อให้สามารถป้องกันการเข้าถึง และเปลี่ยนแปลงแก้ไขโดยผู้ไม่มีสิทธิหรือไม่ได้รับอนุญาต ดังนี้	
5.1 จัดให้มีแนวทางการบริหารจัดการบัญชีผู้ใช้งานและสิทธิการเข้าถึง โดยมีการทบทวนปรับปรุงสิทธิให้เหมาะสมอย่างสม่ำเสมอ สอดคล้องกับหน้าที่ความรับผิดชอบ รวมถึงมีกระบวนการเพิกถอนสิทธิเมื่อสิ้นสุดความจำเป็นต้องใช้งาน	1. แนวทางการบริหารจัดการบัญชีผู้ใช้งาน ควรครอบคลุมในเรื่องดังนี้ (1) การกำหนดหน่วยงานที่รับผิดชอบในการบริหารจัดการบัญชีผู้ใช้งาน (2) ขั้นตอนการสร้างบัญชีผู้ใช้งาน โดยบัญชีผู้ใช้งาน (user ID) ควรระบุตัวตนผู้ใช้งานได้ หลีกเลี่ยงการใช้บัญชีผู้ใช้งานที่มีผู้ใช้งานมากกว่า 1 ราย (shared ID) (3) ขั้นตอนการทบทวนบัญชีผู้ใช้งาน โดยกำหนดให้มีการทบทวนบัญชีผู้ใช้งาน อย่างน้อยปีละ 1 ครั้ง (4) ขั้นตอนการยกเลิกบัญชีผู้ใช้งาน โดยระงับหรือลบบัญชีผู้ใช้งานเมื่อ (1) ผู้ใช้งานสิ้นสุดสภาพการเป็นพนักงาน (2) ไม่มีความจำเป็นต้องใช้งาน และ (3) ไม่มีการใช้งานในรอบ 90 วันที่ผ่านมา 2. แนวทางการบริหารจัดการสิทธิการเข้าถึงข้อมูลและระบบ IT ควรครอบคลุมในเรื่องดังนี้ (1) การกำหนดหน่วยงานที่รับผิดชอบในการบริหารจัดการสิทธิการเข้าถึงข้อมูลและระบบ IT (2) ขั้นตอนการขออนุมัติสิทธิในการเข้าถึงข้อมูลและระบบ IT จากผู้มีอำนาจ เช่น เจ้าของระบบ หรือเจ้าของข้อมูล (3) ขั้นตอนการปรับปรุงสิทธิของผู้ใช้งานเมื่อมีการเปลี่ยนแปลงหน้าที่ความรับผิดชอบหรือตำแหน่งงาน (4) ขั้นตอนการเพิกถอนสิทธิของผู้ใช้งาน โดยเพิกถอนสิทธิทันทีเมื่อผู้ใช้งานสิ้นสุดสภาพการเป็นพนักงาน และเมื่อไม่มีความจำเป็นต้องใช้งาน (5) การแบ่งแยกบทบาทหน้าที่ของบุคคลที่เกี่ยวข้องในการจัดสรรสิทธิ เช่น ผู้ร้องขอ (access request) ผู้มีอำนาจอนุมัติ (access authorization) และผู้ดูแลสิทธิการเข้าถึง (access administration) เป็นต้น เพื่อให้สอดคล้องตามหลัก

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. /25	แนวปฏิบัติ
	การถ่วงดุล (check and balance) (6) การกำหนดสิทธิของผู้ใช้งานโดยคำนึงถึงความจำเป็นต้องรู้ (need-to-know) ความจำเป็นต้องใช้งาน (need-to-use) และหลักการแบ่งแยกหน้าที่ความรับผิดชอบ (segregation of duties) (7) การจัดทำตารางควบคุมการให้สิทธิ (authorization matrix) ของบัญชีผู้ใช้งานที่สอดคล้องกับตำแหน่งหน้าที่และความรับผิดชอบ เพื่อใช้เป็นแนวทางการกำหนดสิทธิอย่างถูกต้องเหมาะสม (8) ติดตามและทบทวนสิทธิการเข้าถึงให้สอดคล้องกับความเสี่ยงและความสำคัญของสิทธิอย่างสม่ำเสมอ โดยกำหนดรอบระยะเวลาในการทบทวนสิทธิทุกประเภทอย่างน้อยปีละ 1 ครั้ง
5.2 จัดให้มีกระบวนการยืนยันตัวตนผู้ใช้งาน (authentication) ที่เหมาะสมกับความเสี่ยง และป้องกันการปฏิเสธความรับผิด	1. ผู้ประกอบธุรกิจควรจัดให้มีกระบวนการยืนยันตัวตนผู้ใช้งาน (authentication) ที่มีประสิทธิภาพเหมาะสมกับความเสี่ยง และป้องกันการปฏิเสธความรับผิด โดยพิจารณากำหนดกระบวนการที่จำเป็น ดังนี้ (1) กำหนดวิธีการยืนยันตัวตนผู้ใช้งานที่เหมาะสมกับความเสี่ยง เพื่อควบคุมการเข้าถึงข้อมูล และระบบ IT (2) กรณีที่มีรหัสผ่านครั้งแรกสำหรับผู้ใช้งาน กำหนดให้มีการจัดส่งรหัสผ่านให้แก่ผู้ใช้งานอย่างรัดกุมและปลอดภัย และให้ผู้ใช้งานเปลี่ยนแปลงรหัสผ่านทันทีที่ได้รับรหัสดังกล่าว (3) กำหนดให้ผู้ใช้งานตั้งรหัสผ่านที่ซับซ้อนและยากต่อการคาดเดา เช่น มีความยาวขั้นต่ำอย่างน้อย 8 ตัวอักษร โดยอาจประกอบด้วยอักขระพิเศษ (เช่น “#”) เป็นต้น (4) กำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดพลาดติดต่อกัน ก่อนระงับการเข้าสู่ระบบชั่วคราวหรือวิธีการอื่น ๆ ที่เทียบเท่า เพื่อป้องกันการเข้าใช้งานโดยวิธีเดาสุ่ม (brute force) ทั้งนี้ ในทางปฏิบัติไม่ควรยอมให้ผู้ใช้งานยืนยันตัวตนผิดพลาดติดต่อกันเกิน 6-8 ครั้ง (5) กำหนดให้การเปลี่ยนรหัสผ่านใหม่ไม่ซ้ำกับรหัสที่ใช้งานอย่างน้อย 12 ครั้งล่าสุด ทั้งนี้ หากระบบมีข้อจำกัดควรประเมินความเสี่ยงที่เกี่ยวข้องและกำหนดให้การเปลี่ยนรหัสผ่านใหม่ไม่ซ้ำกับรหัสที่ใช้งานอย่างน้อย 4 ครั้งล่าสุด (6) ระหว่างที่ผู้ใช้งานใส่รหัสผ่าน ระบบไม่ควรแสดงให้เห็นค่ารหัสผ่านบนหน้าจอ (7) มีวิธีจัดเก็บข้อมูลรหัสผ่านที่ปลอดภัย เพื่อป้องกันการล่วงรู้หรือแก้ไขเปลี่ยนแปลง รวมทั้งไม่จัดเก็บข้อมูลรหัสผ่านใน folder เดียวกันกับ folder ที่จัดเก็บข้อมูลของแอปพลิเคชัน

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. /25	แนวปฏิบัติ
	(8) กำหนดให้ผู้ใช้งานรับผิดชอบการใช้งานบัญชีผู้ใช้งาน (user ID) และการรักษาความปลอดภัยสิ่งที่ใช้ยืนยันตัวตน (authenticator) เช่น รหัสผ่าน รหัสที่ใช้ครั้งเดียว (one-time password) เป็นต้น รวมทั้งข้อมูลส่วนบุคคลที่อาจนำมาใช้เพื่อขอเปลี่ยนแปลงข้อมูลบัญชีผู้ใช้งาน เพื่อป้องกันการใช้งานจากผู้ไม่หวังดี 2. *[ความเสี่ยงสูง] ผู้ประกอบธุรกิจควรมีระบบอัตโนมัติในการตรวจสอบและแจ้งเตือนพฤติกรรมการยืนยันตัวตนที่ผิดปกติหรือต้องสงสัย เช่น การเข้าสู่ระบบจากเครื่องคอมพิวเตอร์ต้นทางพร้อมกันหลายเครื่อง หรือการเข้าสู่ระบบจากเครื่องคอมพิวเตอร์ต้นทางที่มีความแตกต่างกันด้านสถานที่ทางภูมิศาสตร์ภายในระยะเวลาอันสั้น เป็นต้น*
5.3 กำหนดมาตรการควบคุม จำกัด และติดตามการใช้งานบัญชี privileged user (privileged user management) ดังนี้ 5.3.1 มี MFA เมื่อเข้าใช้งานและเปลี่ยนรหัสผ่าน สำหรับระบบปฏิบัติการและระบบฐานข้อมูลที่เกี่ยวข้องกับระบบ IT ที่มีนัยสำคัญ 5.3.2 กรณีผู้ประกอบธุรกิจมีข้อจำกัดสำหรับ MFA สามารถใช้วิธีการอื่นใดที่เทียบเท่าทดแทน และจัดให้มีการประเมินความเสี่ยงและพิจารณาแนวทางควบคุมความเสี่ยงก่อนดำเนินการเพื่อขออนุมัติยกเว้น (exception)	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]
5.3.3 มีการควบคุมและติดตามตรวจสอบการใช้งานบัญชี privileged user อย่างเข้มงวด	ผู้ประกอบธุรกิจควรพิจารณากำหนดกระบวนที่จำเป็นในการควบคุมและติดตามการใช้บัญชี privileged user ดังนี้ 1. กำหนดให้ใช้งานบัญชี privileged user เมื่อมีความจำเป็นเท่านั้น 2. กำหนดกระบวนการร้องขอเพื่อเข้าใช้งานบัญชี privileged user โดยมีการขออนุมัติจากผู้มีอำนาจ และกำหนดระยะเวลาการใช้งานที่ชัดเจน 3. ห้ามใช้งานบัญชี privileged user ร่วมกัน (shared account) 4. จำกัดจำนวนบัญชี privileged user ให้มีจำนวนน้อยที่สุด หรือเท่าที่จำเป็นเท่านั้น

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. /25	แนวปฏิบัติ
	5. กำหนดนโยบายการยืนยันตัวตนของบัญชี privileged user ที่เข้มงวดกว่าบัญชีผู้ใช้งานทั่วไป 6. ระงับหรือยกเลิกบัญชี privileged user เมื่อสิ้นสุดการใช้งาน 7. จัดเก็บข้อมูลประวัติการยืนยันตัวตนและการเข้าถึง (access log) และกิจกรรม (activity log) เกี่ยวกับบัญชี privileged user อย่างเหมาะสม 8. สอบทานการใช้งานบัญชี privileged user ทั้งจากการใช้งานบัญชี privileged user โดยตรง หรือกิจกรรมการยกระดับสิทธิการใช้งาน เช่น switch user อย่างสม่ำเสมอ 9. มีกระบวนการควบคุมเพื่อป้องกันการเข้าใช้งานบัญชี privileged user และยกระดับสิทธิการใช้งานโดยผู้ที่ไม่ได้รับอนุญาต เช่น การใช้เครื่องมือบริหารจัดการบัญชี privileged user (privilege access management: PAM) และการใช้ระบบติดตามแจ้งเตือนเมื่อมีการใช้งานสิทธิระดับสูง เป็นต้น
2.6 การควบคุมการเข้ารหัส (cryptographic control)	
ส่วนที่ 6 การควบคุมการเข้ารหัส (cryptographic control) ผู้ประกอบธุรกิจต้องจัดให้มีการควบคุมการเข้ารหัสที่เชื่อถือได้และเป็นไปตามมาตรฐานสากลโดยกำหนดวิธีการเข้ารหัสข้อมูล (encryption) และการบริหารจัดการกุญแจเข้ารหัส (key management) อย่างปลอดภัยเพื่อให้มั่นใจได้ว่า การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และความถูกต้องแท้จริง (authenticity) ของข้อมูลมีความเหมาะสมและมีประสิทธิภาพ ดังนี้	
6.1 กำหนดวิธีการเข้ารหัสที่ปลอดภัย	ในการกำหนดวิธีการเข้ารหัสที่ปลอดภัย ผู้ประกอบธุรกิจควรดำเนินการอย่างน้อย ดังนี้ 1. กำหนดหน่วยงานหรือบุคลากรที่รับผิดชอบของในการดำเนินการตามนโยบายและบริหารจัดการกุญแจเข้ารหัสข้อมูล 2. กำหนดมาตรฐานวิธีการเข้ารหัสข้อมูล (algorithm และ cipher suite) ขององค์กรที่เป็นไปตามมาตรฐานสากล โดยมี

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. /25	แนวปฏิบัติ
	ความมั่นคงปลอดภัยเหมาะสมกับระดับความสำคัญหรือความเสี่ยงของข้อมูล 3. การกำหนดรอบระยะเวลาในการทบทวนมาตรฐานวิธีการเข้ารหัสข้อมูล เพื่อให้มั่นใจว่าวิธีการเข้ารหัสข้อมูลที่ใช้งานอยู่ ยังมีความมั่นคงเพียงพอในการรักษาความปลอดภัยของข้อมูล
6.2 กำหนดการบริหารจัดการกุญแจเข้ารหัสโดยกำหนดให้มีมาตรการการควบคุมตั้งแต่การสร้างและติดตั้งกุญแจเข้ารหัส การจัดเก็บและสำรอง ไปจนถึงการเพิกถอนหรือทำลายกุญแจเข้ารหัส	ผู้ประกอบธุรกิจควรกำหนดกระบวนการบริหารจัดการกุญแจเข้ารหัสที่ครอบคลุมอย่างน้อยในเรื่อง ดังนี้ 1. การสร้างและติดตั้งกุญแจเข้ารหัส (1) มีการควบคุมสภาพแวดล้อมและกระบวนการในการสร้างกุญแจเข้ารหัสที่รัดกุมปลอดภัย เช่น เลือกใช้ผู้ให้บริการออกใบรับรอง (certification authority) ที่น่าเชื่อถือ และทำลายข้อมูลที่ใช้ในกระบวนการเข้ารหัสเพื่อควบคุมความเสี่ยงจากการเข้าถึงหรือกู้คืนกุญแจเข้ารหัสข้อมูลโดยไม่ได้รับอนุญาต เป็นต้น (2) กำหนดสิทธิการเข้าถึงกุญแจเข้ารหัสและระบบบริหารจัดการกุญแจเข้ารหัส ให้สามารถเข้าถึงได้โดยผู้ที่ได้รับอนุญาตเท่านั้น (3) กำหนดความยาวของกุญแจเข้ารหัสที่เพียงพอในการป้องกันการถูกถอดรหัส (decrypt) โดยผู้ไม่หวังดี เช่น การโจมตีแบบ brute force เป็นต้น (4) แลกเปลี่ยนกุญแจผ่านกระบวนการและช่องทางที่ปลอดภัย (5) กำหนดไม่ให้ใช้กุญแจเข้ารหัสข้อมูลเดียวกันกับหลายระบบงาน 2. การจัดเก็บและการสำรองกุญแจเข้ารหัส (1) มีการรักษาความปลอดภัยในการจัดเก็บกุญแจเข้ารหัสทั้งด้าน physical และ logical เช่น การใช้อุปกรณ์รักษาความปลอดภัย HSM หรืออุปกรณ์ที่ทำหน้าที่ในลักษณะเดียวกัน เป็นต้น (2) มีการสำรองข้อมูลกุญแจเข้ารหัส โดยวิธีการเก็บรักษาข้อมูลกุญแจเข้ารหัสชุดสำรองต้องมีการรักษาความปลอดภัยในระดับเดียวกับกุญแจเข้ารหัสชุดหลัก 3. การเพิกถอนหรือทำลายกุญแจเข้ารหัส (1) กำหนดเกณฑ์และแนวทางในการเปลี่ยนและเพิกถอนกุญแจเข้ารหัส เช่น กรณีกุญแจเข้ารหัสหมดอายุการใช้งาน หรือไม่ปลอดภัย เป็นต้น

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. /25	แนวปฏิบัติ
	(2) กำหนดกระบวนการทำลายกุญแจ เพื่อให้มั่นใจว่าจะไม่สามารถนำกุญแจนั้นมาใช้งานได้อีก 4. การจัดเก็บข้อมูลบันทึกเหตุการณ์กิจกรรมสำคัญที่เกี่ยวกับการบริหารจัดการกุญแจเข้ารหัส ได้แก่ การสร้างกุญแจ การสำรองกุญแจ และการเพิกถอนกุญแจ
6.3 กำหนดมาตรการการควบคุมกุญแจเข้ารหัสที่ให้บริการโดยบุคคลภายนอก ซึ่งต้องตรวจสอบเพื่อให้มั่นใจได้ว่ากุญแจการเข้ารหัสที่สร้างขึ้นไม่มีการนำมาใช้ร่วมกับบุคคลอื่น	กรณีที่ผู้ประกอบธุรกิจไม่สามารถสร้างกุญแจเข้ารหัสด้วยตนเองได้หรือมีความจำเป็นต้องใช้กุญแจเข้ารหัสที่ให้บริการโดยบุคคลภายนอก ผู้ประกอบธุรกิจควรมีการดำเนินการเพื่อให้มั่นใจได้ว่ากุญแจเข้ารหัสที่ให้บริการโดยบุคคลภายนอกไม่มีการนำมาใช้งานร่วมกับผู้ใช้บริการรายอื่น โดยตรวจสอบรายละเอียดด้านความมั่นคงปลอดภัยของระบบการบริหารจัดการกุญแจเข้ารหัสของบุคคลภายนอก ได้แก่ 1. ประเภทของกุญแจเข้ารหัสที่ให้บริการ 2. รายละเอียดของระบบหรือเครื่องมือเข้ารหัส รวมถึงกระบวนการควบคุมการเข้ารหัสในแต่ละขั้นตอน ตลอดวงจรการบริหารจัดการกุญแจเข้ารหัส 3. ข้อแนะนำการใช้งานและการควบคุมการเข้ารหัสข้อมูล
6.4 กำหนดกระบวนการรองรับกรณีเกิดการรั่วไหลของกุญแจเข้ารหัส	ผู้ประกอบธุรกิจควรกำหนดรายการกิจกรรมที่ต้องปฏิบัติเมื่อเกิดการรั่วไหลของกุญแจเข้ารหัส เช่น การติดต่อหน่วยงานและผู้ที่เกี่ยวข้องกับชุดข้อมูลที่ใช้กุญแจเข้ารหัสชุดดังกล่าว การตรวจสอบชุดข้อมูลที่มีความเสี่ยงในการรั่วไหล การเปลี่ยนหรือเพิกถอนกุญแจการเข้ารหัสข้อมูล เป็นต้น
2.7 การสร้างความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (physical and environmental security)	
ส่วนที่ 7 การสร้างความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (physical and environmental security) ผู้ประกอบธุรกิจต้องจัดให้มีการสร้างความมั่นคงปลอดภัย รวมทั้งมีระบบการป้องกันและกระบวนการในการบำรุงรักษาฮาร์ดแวร์ และระบบสาธารณูปโภค (facilities) ทางกายภาพและสภาพแวดล้อมที่เกี่ยวข้อง	1. ผู้ประกอบธุรกิจควรจัดให้มีมาตรการรักษาความปลอดภัย และมาตรการควบคุมการเข้าถึงศูนย์คอมพิวเตอร์ และพื้นที่ที่เกี่ยวข้องกับระบบ IT ที่มีนัยสำคัญ โดยคำนึงถึงความเสี่ยงจากภัยธรรมชาติ และภัยคุกคามจากมนุษย์ 2. ผู้ประกอบธุรกิจควรกำหนดสิทธิการเข้าออกศูนย์คอมพิวเตอร์ และพื้นที่ที่เกี่ยวข้องกับระบบ IT ที่มีนัยสำคัญ ตามหลักความจำเป็น ถูกต้อง และเป็นปัจจุบัน โดยทบทวนสิทธิการเข้าออกพื้นที่อย่างสม่ำเสมอ 3. ผู้ประกอบธุรกิจควรมีมาตรการควบคุมการเข้า-ออกศูนย์คอมพิวเตอร์ และพื้นที่ที่เกี่ยวข้องกับระบบ IT ที่มีนัยสำคัญ สำหรับพนักงานที่ไม่ได้มีหน้าที่ปฏิบัติงานประจำหรือผู้ที่เข้าถึงแบบชั่วคราว โดยจัดให้มีการอนุมัติจากผู้มีอำนาจ มีการลงบันทึกเข้า-ออก และมีการติดตามและควบคุม (escort) อย่างใกล้ชิด ตลอดระยะเวลาปฏิบัติงานในพื้นที่ดังกล่าว

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. /25	แนวปฏิบัติ
กับ IT อย่างเหมาะสม เพื่อให้สามารถป้องกันการเข้าถึงและป้องกันการสร้างความเสียหายต่อทรัพย์สินด้าน IT ที่จัดเก็บอยู่ในศูนย์คอมพิวเตอร์หลัก ศูนย์คอมพิวเตอร์สำรอง และศูนย์คอมพิวเตอร์จากบุคคลภายนอก (co-location) ตลอดจนมีการป้องกันความปลอดภัยทางกายภาพของอุปกรณ์ IT อื่น ๆ	4. ผู้ประกอบธุรกิจควรจัดให้มีการรักษาความมั่นคงปลอดภัยให้กับศูนย์คอมพิวเตอร์ เช่น ระบบกล้องวงจรปิด อุปกรณ์เตือนไฟไหม้ ถังดับเพลิงหรือระบบดับเพลิงแบบอัตโนมัติ อุปกรณ์ปรับแรงดันและสำรองไฟฟ้า (uninterrupted power supply) และระบบควบคุมอุณหภูมิและความชื้นที่เหมาะสม เป็นต้น พร้อมทั้งมีการบำรุงรักษาอย่างสม่ำเสมอ 5. ผู้ประกอบธุรกิจควรแยกพื้นที่จุดรับส่งของ (delivery and loading area) ซึ่งเป็นพื้นที่ส่วนที่ต้องมีการเข้าถึงโดยบุคคลภายนอกออกจากพื้นที่ที่มีการประมวลผลข้อมูล เช่น พื้นที่ใช้เก็บรายงานที่ฝ่ายคอมพิวเตอร์ได้จัดพิมพ์ให้หน่วยงานต่าง ๆ เป็นต้น ออกจากศูนย์คอมพิวเตอร์ 6. ผู้ประกอบธุรกิจควรจัดเก็บอุปกรณ์คอมพิวเตอร์ที่สำคัญ เช่น เครื่องแม่ข่าย อุปกรณ์เครือข่าย เป็นต้น ไว้ในพื้นที่ที่มีมาตรการควบคุมอย่างปลอดภัย 7. ผู้ประกอบธุรกิจควรจัดให้มีการป้องกันทรัพย์สินด้าน IT ประเภทฮาร์ดแวร์ที่อาจหยุดชะงักจากการทำงานผิดพลาดของระบบสาธารณูปโภค เช่น ระบบไฟฟ้า และระบบปรับอากาศ เป็นต้น 8. ผู้ประกอบธุรกิจควรจัดให้มีมาตรการป้องกันสายเคเบิลและสายไฟของศูนย์คอมพิวเตอร์จากการขัดขวางการทำงาน หรือการทำให้เสียหาย และบำรุงรักษาอย่างสม่ำเสมอ 9. ผู้ประกอบธุรกิจควรจัดให้มีการดูแลและบำรุงรักษาทรัพย์สินด้าน IT ประเภทฮาร์ดแวร์อย่างถูกวิธี มีการทดสอบการใช้งานระบบสาธารณูปโภคอย่างสม่ำเสมอ เพื่อให้อยู่ในสภาพครบถ้วนสมบูรณ์และพร้อมใช้งาน 10. ผู้ประกอบธุรกิจควรควบคุมมิให้มีการนำทรัพย์สินด้าน IT ประเภทฮาร์ดแวร์ออกนอกพื้นที่โดยมิได้รับอนุญาต 11. ก่อนการยกเลิกการใช้งานหรือจำหน่ายทรัพย์สินด้าน IT ประเภทฮาร์ดแวร์ เช่น hard disk, switch, firewall และ router เป็นต้น ผู้ประกอบธุรกิจควรจัดเก็บทรัพย์สินในพื้นที่ปลอดภัย และตรวจสอบให้มั่นใจว่าได้มีการลบ ย้าย ทำลายข้อมูลสำคัญและข้อมูลการปรับแต่ง (configuration) หรือปรับค่าดังกล่าวกลับไปสู่ค่าตั้งต้น (factory reset) ด้วยวิธีการที่ไม่สามารถกู้คืนได้อีก

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. /25	แนวปฏิบัติ
2.8 มาตรการรักษาความมั่งคงปลอดภัยในการปฏิบัติงานด้าน IT (IT operations security)	
ส่วนที่ 8 มาตรการรักษาความมั่งคงปลอดภัยในการปฏิบัติงานด้าน IT (IT operations security) ผู้ประกอบธุรกิจต้องมีมาตรการรักษาความมั่งคงปลอดภัยในการปฏิบัติงานด้าน IT เพื่อให้การปฏิบัติงานเกี่ยวกับการประมวลผลข้อมูลมีความถูกต้องและมั่นคงปลอดภัย โดยต้องครอบคลุมการบริหารจัดการอย่างน้อยในเรื่องดังนี้	
2.8.1 การตั้งค่าระบบ (system configuration management)	
8.1 การตั้งค่าระบบ (system configuration management) โดยมีกระบวนการในการควบคุมการตั้งค่าของระบบที่ใช้งานจริง และมีการสอบทานการตั้งค่าเพื่อให้การตั้งค่าระบบ IT เป็นไปอย่างถูกต้อง และปลอดภัย	1. ผู้ประกอบธุรกิจควรกำหนดมาตรฐานการตั้งค่าด้านความมั่นคงปลอดภัย (security configuration standard) สำหรับระบบปฏิบัติการ ระบบฐานข้อมูล แอปพลิเคชัน อุปกรณ์รักษาความปลอดภัย และอุปกรณ์เครือข่าย อย่างเป็นลายลักษณ์อักษร โดยคำนึงถึงเรื่องดังนี้ (1) การลบบัญชีผู้ใช้งานตั้งต้น หรือเปลี่ยนแปลงรหัสผ่านเมื่อเข้าใช้งานครั้งแรก (2) การใช้วิธีการยืนยันตัวตนที่มีความรัดกุมปลอดภัย (3) การกำหนดบริการ แอปพลิเคชัน และพอร์ตการเชื่อมต่อตามความจำเป็น (4) การเก็บข้อมูลเหตุการณ์ของอุปกรณ์ที่สำคัญ เพื่อใช้ในการตรวจสอบย้อนหลัง 2. ผู้ประกอบธุรกิจควรตั้งค่าด้านความมั่นคงปลอดภัยของระบบและอุปกรณ์ตามมาตรฐานที่กำหนดไว้ (security hardening) ก่อนการนำระบบและอุปกรณ์ไปใช้งาน 3. ผู้ประกอบธุรกิจควรสอบทานการตั้งค่าด้านความมั่นคงปลอดภัยของระบบและอุปกรณ์อย่างสม่ำเสมอ และทุกครั้งที่มีการเปลี่ยนแปลงระบบและอุปกรณ์อย่างมีนัยสำคัญ เพื่อให้สอดคล้องกับมาตรฐานที่กำหนดไว้
2.8.2 การเปลี่ยนแปลงด้าน IT (change management)	
8.2 การเปลี่ยนแปลงด้าน IT (change management) อย่างรัดกุมเพียงพอเพื่อให้การเปลี่ยนแปลงเป็นไปตาม	1. ผู้ประกอบธุรกิจควรกำหนดขั้นตอนปฏิบัติในการบริหารจัดการการเปลี่ยนแปลงอย่างเป็นลายลักษณ์อักษรเพื่อควบคุมการเปลี่ยนแปลงโครงสร้างพื้นฐานด้าน IT ระบบ IT และขั้นตอนการปฏิบัติงาน ที่อาจกระทบต่อความมั่นคงปลอดภัย

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. /25	แนวปฏิบัติ
วัตถุประสงค์ที่กำหนดไว้อย่างถูกต้องครบถ้วน และป้องกันการเปลี่ยนแปลงโดยที่ไม่ได้รับอนุญาต	2. ผู้ประกอบธุรกิจควรกำหนดหลักเกณฑ์การจัดประเภทการเปลี่ยนแปลงตามระดับความสำคัญหรือความจำเป็นเร่งด่วน และกำหนดขั้นตอนในการเปลี่ยนแปลงแต่ละประเภท เช่น (1) การเปลี่ยนแปลงมาตรฐานที่ได้รับอนุมัติเป็นการทั่วไป (standard change) (2) การเปลี่ยนแปลงที่ต้องขออนุมัติตามกระบวนการปกติ (normal change) (3) การเปลี่ยนแปลงที่ต้องดำเนินการอย่างเร่งด่วน (emergency change) เป็นต้น 3. ผู้ประกอบธุรกิจควรแบ่งแยกหน้าที่ (segregation of duties) ผู้ที่เกี่ยวข้องในกระบวนการการเปลี่ยนแปลง เพื่อไม่ให้บุคคลใดบุคคลหนึ่งสามารถปฏิบัติงานได้ตั้งแต่เริ่มต้นจนจบกระบวนการการเปลี่ยนแปลง เช่น ผู้มีสิทธิร้องขอ ผู้ที่มีอำนาจในการอนุมัติการเปลี่ยนแปลง ผู้ที่สามารถดำเนินการเปลี่ยนแปลงระบบ เป็นต้น 4. ผู้ประกอบธุรกิจควรจัดให้มีคำขอการเปลี่ยนแปลง (change request) และการอนุมัติการเปลี่ยนแปลงเป็นลายลักษณ์อักษร เพื่อเป็นหลักฐานแสดงให้เห็นว่าการเปลี่ยนแปลงได้ผ่านการพิจารณาจากเจ้าของระบบหรือผู้มีอำนาจตามสิทธิที่กำหนดไว้ โดยคำขอการเปลี่ยนแปลงควรระบุเหตุผลความจำเป็น และผลกระทบที่อาจเกิดขึ้นจากการเปลี่ยนแปลง 5. ผู้ประกอบธุรกิจควรจัดให้มีระบบหรือทะเบียนในการจัดเก็บคำขอเปลี่ยนแปลงและเอกสารรายละเอียดที่เกี่ยวข้อง เพื่อใช้ควบคุมการปฏิบัติงานตั้งแต่ต้นจนจบกระบวนการและสามารถใช้ในการติดตามและสอบทานการปฏิบัติงานได้ 6. กรณีที่การเปลี่ยนแปลงมีผลกระทบต่อการปฏิบัติงาน ผู้ประกอบธุรกิจควรสื่อสารให้ผู้เกี่ยวข้องรับทราบการเปลี่ยนแปลงเพื่อให้สามารถปฏิบัติงานได้อย่างถูกต้อง 7. ผู้ประกอบธุรกิจควรจัดให้มีแผนการถอยกลับสู่สภาพเดิม (fallback procedure) หากเกิดข้อผิดพลาดจากการเปลี่ยนแปลง เช่น การจัดเก็บเวอร์ชันของระบบก่อนการเปลี่ยนแปลงไว้ เป็นต้น 8. กรณีการเปลี่ยนแปลงที่ต้องดำเนินการอย่างเร่งด่วน (emergency change) ควรมีกระบวนการในการพิจารณาความเสี่ยงและผลกระทบ รวมถึงขออนุมัติจากผู้บริหารที่ได้รับมอบหมายให้สามารถตัดสินใจได้กรณีเร่งด่วน โดยภายหลังดำเนินการให้มีการรายงานผู้บริหารที่เกี่ยวข้อง และคณะกรรมการบริหารจัดการการเปลี่ยนแปลง (change advisory board : CAB) (ถ้ามี) รับทราบโดยเร็ว 9. *[ความเสี่ยงสูง] ผู้ประกอบธุรกิจควรกำหนดบทบาทหน้าที่และความรับผิดชอบของผู้บริหารที่ได้รับมอบหมายหรือ*

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. /25	แนวปฏิบัติ
	คณะกรรมการบริหารจัดการการเปลี่ยนแปลง (change advisory board : CAB) ซึ่งควรประกอบด้วยผู้บริหารจากหน่วยงาน IT หน่วยงานธุรกิจ และหน่วยงานผู้ใช้งานที่เกี่ยวข้องเพื่อทำหน้าที่พิจารณาเหตุผลความจำเป็นและประเมินผลกระทบก่อนอนุมัติให้ดำเนินการเปลี่ยนแปลง เพื่อป้องกันการแก้ไขเปลี่ยนแปลงโดยไม่ได้รับอนุญาตและไม่ให้เกิดผลกระทบที่อาจเกิดกับระบบที่เกี่ยวข้อง นอกจากนี้ ผู้บริหารที่ได้รับมอบหมายหรือ CAB ควรมีการติดตามผลหลังการเปลี่ยนแปลงระบบ (post implementation review) เพื่อให้มั่นใจได้ว่าการเปลี่ยนแปลงนั้นเป็นไปตามวัตถุประสงค์ที่กำหนด
2.8.3 การคำนึงถึงขีดความสามารถของระบบ IT (capacity management)	
8.3 การคำนึงถึงขีดความสามารถของระบบ IT (capacity management) โดยจัดให้มีมาตรฐานและวิธีปฏิบัติเรื่องการจัดการขีดความสามารถ การติดตามประสิทธิภาพการทำงานของระบบ และการประเมินแนวโน้มการใช้ทรัพยากรด้าน IT เพื่อให้สามารถรองรับการดำเนินธุรกิจในปัจจุบัน และสามารถวางแผนการจัดสรรทรัพยากรให้รองรับการใช้งานในอนาคตได้อย่างมีประสิทธิภาพ	1. ผู้ประกอบธุรกิจควรกำหนดมาตรฐานและระเบียบวิธีปฏิบัติในการบริหารจัดการขีดความสามารถของระบบ เพื่อประเมินและติดตามดูแลความเพียงพอของโครงสร้างพื้นฐานด้าน IT ที่ครอบคลุมถึงระบบคอมพิวเตอร์ ระบบฐานข้อมูล ระบบเครือข่ายสื่อสาร และระบบสาธารณูปโภคที่เกี่ยวข้องกับงานด้าน IT 2. ผู้ประกอบธุรกิจควรประเมินแนวโน้มการใช้ทรัพยากรด้าน IT (forecasting) โดยคำนึงถึงปริมาณธุรกรรมและปริมาณลูกค้าในภาวะปกติและภาวะวิกฤตที่อาจจะเกิดขึ้น เพื่อวางแผนรองรับการใช้งานในอนาคต (capacity planning) โดยครอบคลุมทั้งระบบหลักและระบบสำรอง 3. ผู้ประกอบธุรกิจควรมีเครื่องมือติดตามตัวชี้วัดการใช้ทรัพยากรด้าน IT (threshold and trigger) เช่น ประสิทธิภาพการทำงาน (performance) ความหน่วง (latency) ขีดความสามารถ (capacity) และปริมาณทรัพยากรที่ถูกใช้งาน (utilization) เป็นต้น ที่มีการแจ้งเตือนผู้เกี่ยวข้องอย่างทันท่วงที และสามารถวิเคราะห์ปัญหาและแนวทางรับมือที่เหมาะสม 4. ผู้ประกอบธุรกิจควรจัดทำรายงานความเพียงพอของทรัพยากรด้าน IT นำเสนอต่อคณะกรรมการหรือผู้บริหารระดับสูงที่เกี่ยวข้อง รับทราบอย่างสม่ำเสมอ เพื่อให้มีการกำกับดูแลความพร้อมใช้และความเพียงพอของระบบในการรองรับการให้บริการทางธุรกิจได้อย่างต่อเนื่อง และสามารถพิจารณาแนวทางลดความเสี่ยงได้อย่างทันการณ์
2.8.4 การรักษาความมั่นคงปลอดภัยของเครื่องแม่ข่าย (server) และอุปกรณ์ที่ใช้ปฏิบัติงาน (endpoint)	
8.4 การรักษาความมั่นคงปลอดภัยของเครื่องแม่ข่าย (server) และอุปกรณ์ที่ใช้ปฏิบัติงาน (endpoint) เพื่อไม่ให้ถูกใช้เป็นช่องทางที่ทำให้ข้อมูลสำคัญรั่วไหล หรือมีการเข้าใช้งานระบบ	1. ผู้ประกอบธุรกิจควรกำหนดมาตรการรักษาความปลอดภัยของเครื่องแม่ข่าย และอุปกรณ์ที่ใช้ในการปฏิบัติงาน เพื่อให้สามารถป้องกันและตรวจจับโปรแกรมไม่ประสงค์ดี (malware) และภัยคุกคามทางไซเบอร์ โดยอย่างน้อยครอบคลุม ดังนี้ (1) มีกระบวนการ หรือเครื่องมือในการควบคุมและติดตามไม่ให้มีการติดตั้งซอฟต์แวร์ที่ไม่ได้รับอนุญาต

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. /25	แนวปฏิบัติ
IT โดยไม่ได้รับอนุญาต	(2) ติดตั้งเครื่องมือในการป้องกันและตรวจจับโปรแกรมไม่ประสงค์ดี เช่น anti-virus, anti-malware และ intrusion prevention system เป็นต้น โดยปรับปรุงเครื่องมือที่ใช้งานให้เป็นปัจจุบัน (update) และเท่าทันภัยคุกคามใหม่อย่างสม่ำเสมอ (3) ควบคุมการใช้สื่อบันทึกข้อมูลพกพา (removable media) เช่น กำหนดแนวทางการอนุญาตให้ใช้งาน universal serial bus (USB) หรือ external hard disk เป็นต้น 2. ผู้ประกอบธุรกิจควรจัดให้มีการควบคุมป้องกันทรัพย์สินด้าน IT ประเภทฮาร์ดแวร์ระหว่างที่ไม่มีผู้ใช้งาน (unattended user equipment) ให้มีความปลอดภัย รวมทั้งควรกำหนดการควบคุมเอกสาร ข้อมูลหรือสื่อบันทึกข้อมูลต่าง ๆ เช่น thumb drive และ external hard disk ที่มีข้อมูลสารสนเทศที่จัดเก็บ หรือบันทึกอยู่ ไม่ให้วางทิ้งไว้บนโต๊ะทำงานหรือสถานที่ไม่ปลอดภัย ในขณะที่ไม่ได้ใช้งาน (clear desk) ตลอดจนการควบคุมหน้าจอคอมพิวเตอร์ไม่ให้มีข้อมูลสำคัญปรากฏในขณะที่ไม่ได้ใช้งาน (clear screen) เช่น การตัดออกจากระบบ (session time out) หรือการล็อคหน้าจอ (lock screen) อัตโนมัติ เป็นต้น 3. ผู้ประกอบธุรกิจควรกำหนดมาตรฐานและระเบียบปฏิบัติในการบริหารจัดการระบบเสมือนจริง (virtualization) โดยครอบคลุมการควบคุมสิทธิการเข้าถึง และการรักษาความปลอดภัยของระบบ ตลอดจนการควบคุมข้อมูลที่เกิดจากระบบเสมือนจริง เช่น ข้อมูลระบบปฏิบัติการ (VM image) และข้อมูลสำรองระบบ (VM snapshot) เพื่อป้องกันการเข้าถึงและเปลี่ยนแปลงระบบโดยผู้ไม่มีสิทธิหรือไม่รับอนุญาต 4. *[ความเสี่ยงสูง] ผู้ประกอบธุรกิจควรติดตั้งระบบตรวจสอบภัยคุกคามขั้นสูง (endpoint detection & response) บนเครื่องแม่ข่าย และอุปกรณ์ที่ใช้ปฏิบัติงาน สำหรับตรวจจับ เก็บหลักฐาน และตอบสนองต่อภัยคุกคามทางไซเบอร์ได้อย่างทันการณ์* 5. *[ความเสี่ยงสูง] ผู้ประกอบธุรกิจควรกำหนดมาตรการทางเทคนิคหรือเครื่องมือป้องกันข้อมูลสำคัญรั่วไหล (data leak prevention) จากการส่งข้อมูลออกโดยไม่ได้รับอนุญาตผ่านช่องทางต่าง ๆ เช่น อุปกรณ์พกพาและสื่อบันทึกข้อมูล จดหมายอิเล็กทรอนิกส์ และโปรแกรมการประชุมและสื่อสารผ่านสื่ออิเล็กทรอนิกส์ (online communication tool) เป็นต้น* 6. *[ความเสี่ยงสูง] กรณีที่มีฟังก์ชันเปิดการใช้งานพอร์ตการเชื่อมต่อ ให้ปิดพอร์ตการเชื่อมต่อภายนอกทั้งหมด (เช่น พอร์ต USB) ที่รองรับการเชื่อมต่อกับสื่อบันทึกข้อมูลพกพา (removable media) และอุปกรณ์คอมพิวเตอร์แบบพกพา โดยให้เปิดใช้งานเมื่อจำเป็นและได้รับอนุมัติโดยผู้มีอำนาจเท่านั้น*

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. /25	แนวปฏิบัติ
2.8.5 การรักษาความปลอดภัยสำหรับการปฏิบัติงานจากเครือข่ายภายนอก (teleworking) การใช้งานอุปกรณ์เคลื่อนที่ (mobile device) และการใช้งานอุปกรณ์ส่วนตัว (bring your own device : BYOD)	
8.5 การกำหนดนโยบายและมาตรการรักษาความปลอดภัยสำหรับการปฏิบัติงานจากเครือข่ายภายนอก (teleworking) การใช้งานอุปกรณ์เคลื่อนที่ (mobile device) และรวมถึงการใช้งานอุปกรณ์ส่วนตัว (bring your own device : BYOD) โดยพิจารณาความเสี่ยงที่เกี่ยวข้อง และจัดให้มีมาตรการควบคุมอย่างเหมาะสม	1. ในกรณีที่มีการปฏิบัติงานจากเครือข่ายภายนอก (teleworking) ผู้ประกอบธุรกิจควรกำหนดมาตรการรักษาความมั่นคงปลอดภัยที่รัดกุมเพียงพอเหมาะสมกับระดับความสำคัญของข้อมูล และระบบ IT ที่ถูกเข้าถึง โดยพิจารณาถึง (1) การกำหนดมาตรการรักษาความมั่นคงปลอดภัยด้านกายภาพสำหรับพื้นที่ปฏิบัติงานนอกองค์กรที่เหมาะสมรัดกุมเพียงพอกับขอบเขตการปฏิบัติงาน (2) การลงทะเบียน และขออนุมัติการปฏิบัติงานจากเครือข่ายภายนอกบริษัทจากผู้มีอำนาจหรือผู้บริหารที่เกี่ยวข้อง (3) การกำหนดสิทธิการเข้าถึงข้อมูลและระบบ IT จากเครือข่ายภายนอกบริษัทเท่าที่จำเป็น พร้อมทั้งมีการทบทวนสิทธิอย่างสม่ำเสมอ (4) การยืนยันตัวตนพนักงานที่ได้รับอนุญาตให้ปฏิบัติงานจากภายนอกบริษัทด้วยวิธีการที่รัดกุมปลอดภัย เช่น การใช้วิธียืนยันตัวตนแบบหลายปัจจัย (multi-factor authentication) และการเข้าใช้งานผ่านอุปกรณ์ที่อนุญาตเท่านั้น เป็นต้น (5) การจัดให้มีมาตรการป้องกันความเสี่ยงจากอุปกรณ์ที่ใช้ในการปฏิบัติงานจากเครือข่ายภายนอกถูกใช้เป็นช่องทางในการแพร่กระจายของโปรแกรมไม่ประสงค์ดี (malware) และการรั่วไหลของข้อมูลสำคัญ 2. ในการปฏิบัติงานที่มีการใช้อุปกรณ์เคลื่อนที่ (mobile device) เพื่อเข้าถึงข้อมูลและระบบ IT ขององค์กร ผู้ประกอบธุรกิจควรจัดให้มาตรการป้องกันข้อมูลและระบบ IT ที่มีความสำคัญ โดยพิจารณาถึงแนวทางดังนี้ (1) มีการลงทะเบียนอุปกรณ์เคลื่อนที่ทั้งของพนักงานและบุคคลภายนอกก่อนการใช้งาน และมีการอนุมัติโดยผู้บริหารที่เกี่ยวข้อง ที่รวมถึงจัดให้มีการทบทวนทะเบียนดังกล่าวอย่างน้อยปีละ 1 ครั้งหรือเมื่อมีการเปลี่ยนอุปกรณ์ พร้อมทั้งยกเลิกสิทธิการใช้งานของอุปกรณ์เดิม เพื่อให้มั่นใจได้ว่าการใช้งานอุปกรณ์ดังกล่าวมีความความมั่นคงปลอดภัยเพียงพอ ทั้งนี้ ผู้ประกอบธุรกิจอาจใช้ระบบการลงทะเบียนอื่นทดแทนได้ หากพิจารณาแล้วเห็นว่าเหมาะสม (2) มีมาตรการป้องกันข้อมูลที่เป็นความลับหรือมีความสำคัญ (sensitive data) กรณีที่อุปกรณ์เคลื่อนที่สูญหาย เช่น การเข้ารหัสอุปกรณ์บันทึกข้อมูล หรือการลบข้อมูลจากระยะไกล (remote wipe-out) เป็นต้น (3) จัดให้มีการเข้ารหัสข้อมูลสำคัญทั้งที่จัดเก็บในอุปกรณ์เคลื่อนที่ และข้อมูลที่รับส่งผ่านระบบเครือข่ายสื่อสาร

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. /25	แนวปฏิบัติ
	(4) [ความเสี่ยงสูง] จัดหาเครื่องมือในการบริหารจัดการอุปกรณ์เคลื่อนที่ที่มีความสามารถในการบริหารจัดการชุดโปรแกรมแก้ไขช่องโหว่ด้านความมั่นคงปลอดภัยสารสนเทศ (security patch) การบริหารและติดตั้งค่า configuration ของอุปกรณ์ รวมถึงการบริหารจัดการด้านการป้องกันไวรัสและโปรแกรมไม่พึงประสงค์ 3. กรณีที่อนุญาตให้พนักงานสามารถใช้อุปกรณ์ส่วนตัวของพนักงาน (bring your own device : BYOD) เพื่อเข้าถึงข้อมูลและระบบ IT ผู้ประกอบธุรกิจควรพิจารณาความเสี่ยงที่เกี่ยวข้อง และจัดให้มีมาตรการควบคุมความเสี่ยงอย่างเหมาะสม โดยพิจารณาถึงแนวทางดังนี้ (1) กำหนดหลักเกณฑ์การอนุญาตให้ใช้งาน BYOD (2) ใช้งานระบบบริหารจัดการอุปกรณ์เคลื่อนที่ (mobile device management: MDM) หรือวิธีการที่มีประสิทธิผลในการตรวจสอบ วิเคราะห์และติดตามความเสี่ยงของอุปกรณ์ที่นำมาใช้งาน (3) ควบคุมการใช้ BYOD ในการเข้าถึงระบบเครือข่ายสื่อสาร ข้อมูลและระบบ IT เท่าที่จำเป็น (4) กำหนดรหัสผ่านเพื่อใช้ในการล็อคหรือปลดล็อคในการเข้าถึงอุปกรณ์ส่วนตัว (5) ในกรณีเครื่องคอมพิวเตอร์ (personal computer, notebook) ให้มีการติดตั้งซอฟต์แวร์ตรวจสอบโปรแกรมไม่ประสงค์ดี (anti-virus/anti-malware) และปรับปรุงให้ทันสมัยอยู่เสมอ (6) ไม่อนุญาตให้ใช้โทรศัพท์เคลื่อนที่ที่ถูกปรับแต่ง (rooted หรือ jailbroken) เพื่อเข้าถึงข้อมูลและระบบ IT
2.8.6 การสำรองข้อมูล (data backup)	
8.6 การสำรองข้อมูล (data backup) ที่สำคัญด้วยวิธีการและความถี่ที่เหมาะสม เพื่อให้ข้อมูลสำรองมีสภาพพร้อมใช้งานสอดคล้องกับเป้าหมายการกู้คืนระบบ IT ในกรณีที่ระบบ IT และข้อมูลหลักเกิดเหตุขัดข้องหรือได้รับความเสียหาย โดยต้องมีการทดสอบข้อมูลสำรองและกระบวนการกู้คืนข้อมูลอย่างน้อยปีละ 1 ครั้ง	1. ผู้ประกอบธุรกิจควรกำหนดมาตรฐานหรือวิธีปฏิบัติในการสำรองข้อมูลที่สอดคล้องกับระยะเวลาเป้าหมายในการกู้คืนระบบ IT (Recovery Time Objective : RTO) และระยะเวลาเป้าหมายสูงสุดที่ยอมให้ข้อมูลเสียหาย (Recovery Point Objective : RPO) โดยอย่างน้อยควรมีรายละเอียดครอบคลุม (1) ข้อมูลที่ต้องสำรอง (2) ความถี่หรือรอบเวลาในการสำรองข้อมูล (3) ขั้นตอนและวิธีการสำรองข้อมูล (4) ขั้นตอนและวิธีการกู้คืนข้อมูล

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. /25	แนวปฏิบัติ
	(5) สถานที่และวิธีการเก็บรักษาสื่อบันทึกข้อมูล 2. ผู้ประกอบธุรกิจควรจัดเก็บสื่อบันทึกข้อมูลสำรอง พร้อมทั้งสำเนาขั้นตอนหรือวิธีปฏิบัติต่าง ๆ ไว้นอกศูนย์คอมพิวเตอร์หลักหรือนอกสถานที่ปฏิบัติงานหลัก โดยสถานที่ดังกล่าวควรจัดให้มีมาตรการรักษาความปลอดภัยเทียบเคียงกับศูนย์คอมพิวเตอร์หลักหรือสถานที่ปฏิบัติงานหลัก 3. ผู้ประกอบธุรกิจควรจัดให้มีการสอบทานการสำรองข้อมูล และทดสอบข้อมูลสำรองอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่ามีการสำรองข้อมูลมีความครบถ้วนถูกต้อง พร้อมใช้งาน และปลอดภัย 4. ในกรณีที่จำเป็นต้องจัดเก็บข้อมูลเป็นระยะเวลานาน ผู้ประกอบธุรกิจควรคำนึงถึงวิธีการนำข้อมูลกลับมาใช้งานในอนาคตด้วย หากมีความจำเป็น เช่น เมื่อมีการจัดเก็บข้อมูลลงในสื่อบันทึกข้อมูลใด ให้มีการจัดเก็บอุปกรณ์และโปรแกรมที่ใช้อ่านสื่อบันทึกข้อมูลนั้นด้วย เป็นต้น
2.8.7 การจัดเก็บข้อมูลบันทึกเหตุการณ์การใช้งานเกี่ยวกับระบบ IT (log)	
8.7 การจัดเก็บข้อมูลบันทึกเหตุการณ์การใช้งานเกี่ยวกับระบบ IT (log) อย่างครบถ้วนและเพียงพอ เพื่อให้สามารถใช้เป็นหลักฐานการทำธุรกรรมทางอิเล็กทรอนิกส์ และสามารถติดตามและตรวจสอบการเข้าถึงและใช้งานข้อมูลและระบบ IT ตามที่กฎหมายกำหนด	1. ผู้ประกอบธุรกิจควรจัดเก็บข้อมูลบันทึกเหตุการณ์ (log) ด้วยวิธีการที่ปลอดภัย โดยมีรายละเอียดครบถ้วนเพียงพอที่จะใช้เป็นหลักฐานในการตรวจสอบที่สามารถระบุตัวผู้กระทำได้ และจัดเก็บเป็นระยะเวลาอย่างน้อย 90 วัน หรือตามกฎหมายที่เกี่ยวข้องกำหนด ประกอบด้วยรายการหลักฐานอย่างน้อย ดังนี้ (1) บันทึกเหตุการณ์การเข้า-ออกพื้นที่ตั้งของทรัพย์สินด้าน IT และพื้นที่ปฏิบัติงานด้าน IT ที่สำคัญ (physical access log) (2) บันทึกการยืนยันตัวตนและการเข้าถึง (authentication log และ access log) ของเครื่องแม่ข่าย ระบบงาน อุปกรณ์เครือข่าย และข้อมูลสำคัญ โดยรวมถึงความพยายามในการเข้าถึง (log-in attempt) (3) บันทึกการดำเนินงาน (activity log) ที่สำคัญ โดยอย่างน้อยครอบคลุม (ก) การเปลี่ยนแปลงแก้ไขโครงสร้างข้อมูล และการเปลี่ยนแปลงแก้ไขข้อมูลในฐานข้อมูล (ข) การเปลี่ยนแปลงการตั้งค่าของระบบ (system configuration) (ค) การเข้าถึง เปลี่ยนแปลง ลบ หรือถ่ายโอนข้อมูลสำคัญหรือข้อมูลส่วนบุคคล (ง) การเปลี่ยนแปลงแก้ไขบัญชี และสิทธิของผู้ใช้งาน (จ) การใช้งานอินเทอร์เน็ตผ่านระบบเครือข่ายภายในของผู้ประกอบธุรกิจ

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. /25	แนวปฏิบัติ
	(ฉ) การทำงานของ firewall (network firewall log) (ช) หลักฐานการติดต่อสนทนาผ่านช่องทางอิเล็กทรอนิกส์ (electronic messaging) ของบุคคลที่สามารถเข้าถึงข้อมูลภายใน (access person)[2] (4) บันทึกการทำธุรกรรม (transaction log) ให้จัดเก็บเป็นระยะเวลาอย่างน้อย 1 ปี โดยในกรณีที่เป็นระบบ IT เพื่อการซื้อขายหลักทรัพย์ (trading system) ให้บันทึกบัญชีผู้ใช้งาน / ข้อมูลรายละเอียดชื่อย่อหลักทรัพย์ (securities symbol) / หมายเลขบริษัทสมาชิก (broker No. 4 หลัก : xxxx) / เลขที่คำสั่งซื้อขายหลักทรัพย์ (SET order ID) / เลขที่บัญชีซื้อขายหลักทรัพย์ (account ID) / วันและเวลาในการส่งคำสั่งซื้อขายหลักทรัพย์ (yyyy/mm/dd - hh:mm:ss:sss) / หมายเลข public และ local IP address ต้นทาง (source) / หมายเลข IP address ปลายทาง (destination) / ที่อยู่ของเว็บไซต์ปลายทาง (full URL) / terminal type (ถ้ามี) เช่น iPad, iPhone เป็นต้น 2. ผู้ประกอบธุรกิจควรมีการใช้ระบบในการควบคุมค่าเวลาของเครื่องแม่ข่าย ระบบงาน และอุปกรณ์เครือข่ายให้ตรงกับเครื่องแม่ข่าย network time protocol : NTP (clock synchronization) เพื่อให้ค่าเวลาในการบันทึกเหตุการณ์มีความถูกต้องในลักษณะ real-time ซึ่งเครื่อง NTP ควรรับสัญญาณให้ตรงกับเวลาอ้างอิงตามมาตรฐานสากล (stratum 1) เช่น สถาบันมาตรวิทยาแห่งชาติ และกรมอุทกศาสตร์กองทัพเรือ เป็นต้น ทั้งนี้ ในกรณีผู้ประกอบธุรกิจที่เป็นสมาชิกของตลาดหลักทรัพย์ ควรกำหนดระบบเวลาของอุปกรณ์และระบบ IT ที่เกี่ยวกับการซื้อขายหลักทรัพย์และการชำระราคาให้ตรงกับเวลาอ้างอิงของระบบซื้อขายหลักทรัพย์ของตลาดหลักทรัพย์ เพื่อให้การตรวจสอบธุรกรรมที่ไม่เหมาะสมทั้งหมดเป็นไปอย่างถูกต้องและมีประสิทธิภาพ 3. ผู้ประกอบธุรกิจควรจัดเก็บ log ที่เกี่ยวข้องกับข้อมูลส่วนบุคคล เพื่อใช้ระบุและตรวจสอบกิจกรรมของผู้ใช้งานและใช้เป็นหลักฐานหากเกิดเหตุการณ์การเข้าถึง ใช้งาน แก้ไขเปลี่ยนแปลง หรือเปิดเผยข้อมูลส่วนบุคคลที่ไม่เหมาะสม โดยสอดคล้องกับหลักเกณฑ์และมาตรฐานที่เกี่ยวข้อง เช่น พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) เป็นต้น

[2] นิยามว่าด้วย access person ให้เป็นไปตามประกาศแนวปฏิบัติว่าด้วยการกำหนดนโยบาย มาตรการ และระบบงานที่เกี่ยวกับการกระทำที่อาจมีความขัดแย้งทางผลประโยชน์กับลูกค้า

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. /25	แนวปฏิบัติ
	4. ผู้ประกอบธุรกิจควรจัดเก็บ log ของอุปกรณ์สำคัญไว้ที่เครื่องแม่ข่ายที่ใช้จัดเก็บ log (logging server) ที่แยกเฉพาะ หรือใช้วิธีการที่เทียบเคียงซึ่งสามารถป้องกันการเปลี่ยนแปลง แก้ไข หรือทำลาย log ได้ โดยมีมาตรการรักษาความปลอดภัยอย่างน้อยดังนี้ (1) กำหนดหน้าที่และความรับผิดชอบผู้ที่สามารถเข้าถึง log ตามความจำเป็น (2) มีกระบวนการยืนยันตัวตนและตรวจสอบสิทธิในการเข้าถึง log ที่เข้มงวด (3) ติดตั้งเครื่องแม่ข่าย หรืออุปกรณ์ที่ใช้จัดเก็บ log ให้อยู่ในโซนเครือข่ายที่มีความมั่นคงปลอดภัย 5. ผู้ประกอบธุรกิจควรสอบทานบันทึกการเข้าถึง (access log) และบันทึกการดำเนินงาน (activity log) ของผู้ใช้งานสิทธิสูงอย่างสม่ำเสมอ เช่น system administrator หรือ system operator เป็นต้น เพื่อให้มั่นใจได้ว่าผู้ปฏิบัติงานเข้าถึงและปฏิบัติงานตามขอบเขตหน้าที่ที่ได้รับมอบหมาย
2.8.8 การติดตามดูแลระบบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (security monitoring)	
8.8 การติดตามดูแลระบบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (security monitoring) โดยมีกระบวนการหรือเครื่องมือป้องกันและตรวจจับเหตุการณ์ผิดปกติด้าน IT โปรแกรมไม่ประสงค์ดี (malware) หรือภัยคุกคามทางไซเบอร์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยต่อระบบ IT ที่มีนัยสำคัญ	1. ผู้ประกอบธุรกิจควรมีกระบวนการหรือเครื่องมือในการตรวจจับเหตุการณ์ผิดปกติที่กระทบต่อความปลอดภัยของระบบ IT ที่สำคัญอย่างทันท่วงที เพื่อให้รับทราบความผิดปกติหรือภัยคุกคาม และสามารถดำเนินการป้องกันหรือรับมือได้อย่างเหมาะสม 2. ผู้ประกอบธุรกิจควรสอบทาน และวิเคราะห์ log อย่างสม่ำเสมอ เพื่อให้สามารถตรวจสอบพฤติกรรมการใช้งานระบบ IT ที่ผิดปกติ พร้อมทั้งจัดทำรายงานความผิดที่พบให้ผู้บริหารที่เกี่ยวข้องทราบ 3. ผู้ประกอบธุรกิจควรติดตามและกลั่นกรองข่าวสารเกี่ยวกับภัยคุกคาม (cyber threat intelligence) เพื่อให้สามารถติดตามและวิเคราะห์ภัยคุกคามทางไซเบอร์ที่เกิดขึ้นใหม่ และสามารถเตรียมความพร้อมในการรับมือกับเหตุการณ์ทางไซเบอร์อย่างทันการณ์ 4. *[ความเสี่ยงสูง] ผู้ประกอบธุรกิจควรมีหน่วยงานที่รับผิดชอบในการเฝ้าระวัง ติดตาม วิเคราะห์ ประสานงาน และเป็นศูนย์กลางในการจัดการเหตุภัยคุกคาม เช่น หน่วยงาน security operations center (SOC) เป็นต้น* 5. *[ความเสี่ยงสูง] ผู้ประกอบธุรกิจควรมีระบบรวบรวมข้อมูลเหตุการณ์จากแหล่งข้อมูลต่าง ๆ เช่น อุปกรณ์เครือข่าย ระบบงาน และระบบรักษาความปลอดภัยเครือข่าย เป็นต้น เพื่อใช้ในกระบวนการเชื่อมโยงข้อมูล (log correlation) และวิเคราะห์เหตุการณ์ผิดปกติด้านความมั่นคงปลอดภัยสารสนเทศ* 6. *[ความเสี่ยงสูง] ผู้ประกอบธุรกิจควรมีมาตรการในการควบคุมและป้องกันความเสี่ยงจากการบุกรุกโจมตีประเภท zero-day*

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. /25	แนวปฏิบัติ
	attack และแจ้งเตือนไปยังคณะทำงานในการรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (incident response team) เมื่อมีการตรวจพบเหตุการณ์ 7. *[ความเสี่ยงสูง] ผู้ประกอบธุรกิจควรกำหนดกระบวนการตรวจจับเพื่อป้องกันการเปลี่ยนแปลงแก้ไขการตั้งค่าอุปกรณ์คอมพิวเตอร์ โปรแกรม และระบบงานโดยไม่ได้รับอนุญาต โดยอาจพิจารณาใช้เทคโนโลยีที่สนับสนุนกระบวนการข้างต้น เช่น การใช้งานซอฟต์แวร์ file integrity monitoring (FIM) เป็นต้น รวมถึงความพยายามในการเข้าถึงและแก้ไขเปลี่ยนแปลงการตั้งค่าอุปกรณ์รักษาความปลอดภัย เช่น อุปกรณ์ไฟร์วอลล์ อุปกรณ์ตรวจจับและป้องกันผู้บุกรุก หรือ ระบบรักษาความปลอดภัยอื่น ๆ เป็นต้น* 8. *[ความเสี่ยงสูง] ผู้ประกอบธุรกิจควรกำหนดกระบวนการในการติดตามและวิเคราะห์เพื่อใช้แจ้งเตือนพฤติกรรมต้องสงสัยของผู้ใช้งานตามระดับความเสี่ยง ได้แก่ พฤติกรรมการใช้งานเครือข่ายที่ผิดปกติ การถ่ายโอนข้อมูลเป็นจำนวนมาก การเข้าใช้งานในระบบงานในช่วงเวลาผิดปกติ หรือ การเข้าใช้งานจากเครื่องคอมพิวเตอร์ที่ไม่เคยมีการใช้งาน หรืออาจพิจารณาใช้เทคโนโลยีที่สนับสนุนกระบวนการข้างต้น อาทิ ระบบ security analytics*
2.8.9 การประเมินช่องโหว่ทางเทคนิค (technical vulnerability assessment)	
8.9 การประเมินช่องโหว่ทางเทคนิค (technical vulnerability assessment) ของระบบ IT ที่เหมาะสมกับระดับความเสี่ยงเพื่อให้ทราบถึงช่องโหว่ และสามารถดำเนินการแก้ไขและป้องกันภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นได้อย่างทันท่วงที โดยการประเมินช่องโหว่ทางเทคนิคครอบคลุมระบบ IT ที่มีนัยสำคัญ และระบบ IT ที่เชื่อมต่อกับเครือข่ายสาธารณะ (internet facing) ทุกระบบอย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญของระบบดังกล่าว เช่น การเปลี่ยนแปลงโครงสร้างพื้นฐานของระบบ IT หรือการเพิ่มเติมฟังก์ชันสำคัญของระบบ IT เป็นต้น	ในการประเมินช่องโหว่ทางเทคนิค (technical vulnerability assessment) ผู้ประกอบธุรกิจควรดำเนินการ ดังนี้ 1. กำหนดขอบเขตของการประเมินช่องโหว่ทางเทคนิคให้ครอบคลุมทุกระบบงานตามระดับความเสี่ยง สำหรับระบบ IT ที่มีความสำคัญและระบบ IT ที่เชื่อมต่อกับเครือข่ายสาธารณะทุกระบบต้องได้รับการประเมินช่องโหว่อย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ 2. วิเคราะห์และจัดระดับความรุนแรงของช่องโหว่ (severity) ที่ตรวจพบเพื่อประเมินความเสี่ยงและกำหนดระยะเวลาแก้ไขที่เหมาะสมกับความเสี่ยง 3. รายงานผลการประเมินช่องโหว่ไปยังผู้รับผิดชอบ รวมถึงการติดตามให้มีการแก้ไขช่อง

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. /25	แนวปฏิบัติ
2.8.10 การทดสอบเจาะระบบงาน (penetration test)	
8.10 การทดสอบเจาะระบบงาน (penetration test) 8.10.1 ต้องจัดให้มีการทดสอบการเจาะระบบงานดังนี้ <u>(1) ระบบงาน (application system) และระบบเครือข่ายที่มีการเชื่อมต่อกับเครือข่ายสาธารณะ (internet facing)</u> (1.1) อย่างน้อยปีละ 1 ครั้ง และ (1.2) ทุกครั้งที่มีการเปลี่ยนแปลงระบบงานดังกล่าวอย่างมีนัยสำคัญ <u>(2) ระบบงานอื่น ๆ นอกจาก (1)</u> จัดให้มีการประเมินความเสี่ยงจากการบุกรุกผ่านระบบเครือข่ายคอมพิวเตอร์ที่ใช้สื่อสารภายในองค์กร เพื่อกำหนดขอบเขตการทดสอบเจาะระบบและทดสอบเจาะระบบตามความเหมาะสม	ในการทดสอบการเจาะระบบ (penetration test) ผู้ประกอบธุรกิจควรดำเนินการ ดังนี้ 1. กำหนดขอบเขตของการทดสอบการเจาะระบบให้ครอบคลุม application system และระบบเครือข่ายที่มีช่องทางเชื่อมต่อกับเครือข่ายสาธารณะ (internet facing) อย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงระบบงานดังกล่าวอย่างมีนัยสำคัญ โดยระบบงานอื่น ๆ ควรจัดให้มีการประเมินความเสี่ยงจากการบุกรุกผ่านระบบเครือข่ายสื่อสารที่ใช้สื่อสารภายในองค์กร เพื่อกำหนดขอบเขตการทดสอบเจาะระบบและทดสอบเจาะระบบตามความเหมาะสม 2. วิเคราะห์และจัดระดับความรุนแรงของช่องโหว่ (severity) ที่ตรวจพบเพื่อประเมินความเสี่ยงและกำหนดระยะเวลาในการแก้ไขที่เหมาะสมกับความเสี่ยง 3. รายงานสรุปผลการทดสอบการเจาะระบบไปยังเฉพาะผู้รับผิดชอบที่เกี่ยวข้อง เช่น หน่วยงานกำกับการปฏิบัติงาน หรือหน่วยงานตรวจสอบภายใน เป็นต้น รวมถึงการติดตามให้มีการแก้ไขช่องโหว่ที่ตรวจพบภายในระยะเวลาที่กำหนดไว้ โดยมีการรายงานความคืบหน้าของการดำเนินการต่อคณะกรรมการหรือผู้บริหารที่ได้รับมอบหมาย 4. รวบรวมและวิเคราะห์ช่องโหว่ทางเทคนิคที่ตรวจพบ เพื่อช่วยในการกำหนดมาตรการรักษาความมั่นคงปลอดภัยของระบบ IT ที่จะมีการพัฒนาในอนาคต
8.10.2 การทดสอบการเจาะระบบงานข้างต้น ต้องดำเนินการโดยผู้เชี่ยวชาญภายในหรือภายนอกที่เป็นอิสระจากเจ้าของระบบ	1. ผู้ประกอบธุรกิจควรกำหนดให้ผู้ที่ทดสอบการเจาะระบบ เป็นผู้มีความรู้ความสามารถและเชี่ยวชาญในการทดสอบเจาะระบบ โดยเป็นอิสระจากหน่วยงานเจ้าของระบบ และเป็นอิสระจากการพัฒนาระบบดังกล่าว 2. *[ความเสี่ยงสูง] ผู้ประกอบธุรกิจควรกำหนดคุณสมบัติให้ผู้ทดสอบเจาะระบบ (penetration tester) ที่ทำการทดสอบการเจาะระบบ IT ที่มีนัยสำคัญได้รับการรับรองและมีประกาศนียบัตร (accreditations and certifications) ที่เป็นที่ยอมรับในอุตสาหกรรมเช่น OSCP, OSWP, OSCE, OSEE และ OSWE เป็นต้น*
8.10.3 ในกรณีที่มีการตรวจพบช่องโหว่ ผู้ประกอบธุรกิจต้องดำเนินการแก้ไข และป้องกันภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นอย่างทันท่วงที เพื่อขจัดความเสี่ยงจากช่องโหว่ดังกล่าว	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. /25	แนวปฏิบัติ
8.10.4 จัดเก็บรายงานการดำเนินการตาม 8.10 เป็นระยะเวลาไม่น้อยกว่า 2 ปีนับแต่วันที่จัดทำเอกสารนั้น โดยต้องจัดเก็บไว้ในลักษณะที่พร้อมให้สำนักงานสามารถเรียกดูและตรวจสอบได้โดยไม่ชักช้า	ผู้ประกอบธุรกิจควรกำหนดให้รายงานผลการเจาะระบบควรครอบคลุมรายละเอียดที่สำคัญ เช่น ขอบเขตการทดสอบ ช่วงเวลาที่ทดสอบ ผู้ทำการทดสอบ วิธีการและขั้นตอนดำเนินการทดสอบเจาะระบบ และช่องโหว่ที่ตรวจพบ รวมถึงแผนการปรับปรุงแก้ไขช่องโหว่ตามระดับความเสี่ยง เป็นต้น
8.10.5 นำส่งรายงานผลการเจาะระบบโดยไม่ชักช้าเมื่อได้รับการแจ้งจากสำนักงาน ตามวิธีการที่กำหนดไว้บนเว็บไซต์ของสำนักงาน	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]
2.8.11 การบริหารจัดการโปรแกรมแก้ไขช่องโหว่ (patch management)	
8.11 การบริหารจัดการโปรแกรมแก้ไขช่องโหว่ (patch management) โดยจัดให้มีกระบวนการควบคุมการติดตั้งโปรแกรมแก้ไขช่องโหว่บนระบบที่ใช้งานจริง เพื่อลดความเสี่ยงที่ระบบ IT อาจถูกโจมตีในอนาคต	1. ผู้ประกอบธุรกิจควรมีการกำหนดมาตรฐานและระเบียบวิธีปฏิบัติในการบริหารจัดการโปรแกรมแก้ไขช่องโหว่ (patch) ที่ครอบคลุมอย่างน้อยดังนี้ (1) การประเมินความเสี่ยงและความจำเป็นในการติดตั้ง patch (2) การกำหนดกรอบระยะเวลาการติดตั้ง patch โดยคำนึงถึงความจำเป็นและความเสี่ยงจากการถูกโจมตีจากช่องโหว่ (3) การตรวจสอบความถูกต้องและการทดสอบ patch ก่อนการดำเนินการติดตั้งบนระบบที่ให้บริการจริง เพื่อป้องกันผลกระทบที่ไม่พึงประสงค์จากการติดตั้ง patch ทั้งนี้ ในกรณีที่มีข้อจำกัดในการทดสอบ patch ผู้ประกอบธุรกิจอาจพิจารณาการควบคุมทดแทน เช่น กำหนดลำดับการติดตั้ง (patch sequence) อย่างเหมาะสม เป็นต้น 2. ผู้ประกอบธุรกิจควรติดตามข้อมูลข่าวสารเกี่ยวกับ patch ที่อาจมีความเสี่ยงต่อระบบ IT ของผู้ประกอบธุรกิจอย่างทันต่อเหตุการณ์ รวมทั้งจัดให้มีการตรวจสอบช่องโหว่ที่เกี่ยวข้องบนระบบ 3. กรณีที่ยังไม่มี patch เพื่อปิดช่องโหว่ ผู้ประกอบธุรกิจควรปฏิบัติตามคำแนะนำของผู้พัฒนาระบบ เจ้าของผลิตภัณฑ์ หรือผู้เชี่ยวชาญด้านความมั่นคงปลอดภัย เพื่อจัดให้มีมาตรการควบคุมความเสี่ยงอย่างเหมาะสม 4. การติดตั้ง patch บนระบบงานจริง ควรดำเนินการตามกระบวนการบริหารจัดการการเปลี่ยนแปลง (change management) ที่กำหนดไว้ เพื่อป้องกันความเสี่ยงและข้อผิดพลาดจากการปฏิบัติงาน 5. *[ความเสี่ยงสูง] ผู้ประกอบธุรกิจควรมีการติดตั้งเครื่องมือที่ใช้ติดตาม patch ด้านการรักษาความปลอดภัย (patch monitoring*

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. /25	แนวปฏิบัติ
	software) ที่ยังไม่มีการติดตั้งบนระบบปฏิบัติการ (operation system) และระบบฐานข้อมูล (database system) ที่สำคัญของผู้ประกอบธุรกิจ
2.9 มาตรการรักษาความมั่นคงปลอดภัยเกี่ยวกับระบบเครือข่ายสื่อสาร (communication system security)	
ส่วนที่ 9 มาตรการรักษาความมั่นคงปลอดภัยเกี่ยวกับระบบเครือข่ายสื่อสาร (communication system security) ผู้ประกอบธุรกิจต้องมีมาตรการรักษาความมั่นคงปลอดภัยเกี่ยวกับระบบเครือข่ายสื่อสารอย่างเหมาะสม เพื่อรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสารและข้อมูลที่รับส่งผ่านระบบเครือข่ายสื่อสาร	1. ผู้ประกอบธุรกิจควรจัดให้มีการรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร โดยมีการดำเนินการอย่างน้อย ดังนี้ (1) ออกแบบเครือข่ายคอมพิวเตอร์ที่มีการแบ่งแยกเครือข่ายอย่างเหมาะสม โดยคำนึงถึงระดับความสำคัญของระบบงาน (application system) ระดับความสำคัญของข้อมูล รวมถึงความจำเป็นในการเชื่อมต่อกับระบบงานซึ่งอยู่ต่างเครือข่าย และการเชื่อมต่อจากภายนอกองค์กร (2) จัดให้มีการควบคุมการเชื่อมต่อของ application system มีความสำคัญอย่างเข้มงวด (3) การแบ่งแยกเครือข่ายให้มีความรัดกุมปลอดภัย ควรดำเนินการ ดังนี้ (ก) แบ่งแยกเครือข่ายภายใน (private network) และเครือข่ายภายนอก (public network) ออกจากกัน (ข) แบ่งแยกเครือข่ายของระบบ IT ที่มีความสำคัญ เครือข่ายสำหรับการปฏิบัติงานของพนักงานทั่วไป และเครือข่ายสำหรับการใช้งานทั่วไป/เครือข่ายสำหรับบุคคลภายนอก (guest network) ออกจากกัน (ค) จุดที่มีการแบ่งแยกเครือข่ายที่มีความสำคัญและมีความเสี่ยง ควรติดตั้งอุปกรณ์รักษาความปลอดภัยเครือข่ายที่มีความสามารถในการควบคุมและคัดกรองข้อมูล (traffic) ที่รับส่งผ่านเครือข่าย เพื่อป้องกันและตรวจจับการบุกรุก ไวรัส หรือมัลแวร์ต่าง ๆ (ง) กรณีที่มีการแบ่งแยกเครือข่ายเป็นหลายชั้น ควรกำหนดมาตรการควบคุมทางเทคนิคที่แตกต่างกันในแต่ละจุด เช่น ใช้ access control list (ACL) หรือใช้อุปกรณ์รักษาความปลอดภัยเครือข่ายที่แตกต่างยี่ห้อกัน เป็นต้น เพื่อเพิ่มประสิทธิภาพในการคัดกรอง traffic และลดความเสี่ยงที่แต่ละจุดการเชื่อมต่ออาจมีช่องโหว่เดียวกัน (4) จำกัดให้เฉพาะอุปกรณ์ที่ได้รับอนุญาตเท่านั้นที่สามารถเชื่อมต่อกับระบบเครือข่ายภายในบริษัท เช่น จำกัดการใช้งานจุดเชื่อมต่อระบบเครือข่าย (port outlet) หรือจำกัดอุปกรณ์ที่มาเชื่อมต่อกับระบบเครือข่าย (network port security) เป็นต้น (5) เปิดใช้งานช่องทางเชื่อมต่อ (port) ตามความจำเป็นเท่านั้น ในกรณีที่ต้องใช้งาน port ที่ถูกปิดไว้ ควรกำหนด

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. /25	แนวปฏิบัติ
	กระบวนการในการขออนุมัติจากผู้มีอำนาจ และจัดให้มีการควบคุมอย่างเหมาะสม (6) บริหารระบบเครือข่ายสื่อสาร และติดตามสถานะความพร้อมใช้งานให้อยู่ในระดับการให้บริการที่กำหนดไว้ (service level agreement : SLA) (7) สอบทานกฎของอุปกรณ์ firewall อย่างสม่ำเสมอ หรืออย่างน้อยปีละ 1 ครั้งพร้อมจัดทำรายงานการสอบทานอย่างเป็นลายลักษณ์อักษร รวมถึงกำหนดให้มีการรายงานต่อผู้บริหารที่เกี่ยวข้อง (8) จัดให้มีระบบหรือมาตรการรป้องกันการถูกโจมตีจากเครือข่ายสาธารณะที่เหมาะสมตามความเสี่ยง เช่น การใช้อุปกรณ์การรักษาความปลอดภัย intrusion prevention system (IPS) web application firewall (WAF) และมาตรการป้องกันการโจมตีแบบ DDoS (DDoS protection) เป็นต้น *(9) [ความเสี่ยงสูง] ผู้ประกอบธุรกิจควรมีการติดตั้งอุปกรณ์รักษาความปลอดภัยเครือข่ายเพื่อคัดกรอง traffic ในระดับ application ในจุดที่มีการเชื่อมต่อกับเครือข่ายสาธารณะ เช่น การใช้ web application firewall (WAF) เป็นต้น* *(10) [ความเสี่ยงสูง] การเข้าถึงอุปกรณ์เครือข่าย และอุปกรณ์รักษาความปลอดภัยเพื่อบริหารจัดการค่าต่าง ๆ ควรทำผ่านเครือข่ายเฉพาะที่แยกออกจากเครือข่ายปกติ เพื่อลดความเสี่ยงในการเปลี่ยนแปลงอุปกรณ์เครือข่ายและอุปกรณ์รักษาความปลอดภัยเครือข่ายโดยบุคคลที่ไม่ได้รับอนุญาต* 2. ผู้ประกอบธุรกิจควรจัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศที่รับส่งผ่านระบบเครือข่ายสื่อสาร โดยมีการดำเนินการอย่างน้อย ดังนี้ (1) กำหนดแนวปฏิบัติที่ดีในการรับส่งข้อมูลสารสนเทศผ่านช่องทางการสื่อสารอิเล็กทรอนิกส์ประเภทต่าง ๆ (2) นำเทคนิคการเข้ารหัสข้อมูลมาใช้ในการรับส่งข้อมูลสารสนเทศที่เป็นความลับและมีความสำคัญ (3) ป้องกันข้อมูลที่เป็นความลับหรือมีความสำคัญที่รับส่งในรูปแบบของไฟล์แนบ (attachment files) และการส่งต่อจดหมายอิเล็กทรอนิกส์แบบอัตโนมัติออกสู่ภายนอกองค์กร 3. ผู้ประกอบธุรกิจควรจัดให้มีการรักษาความมั่นคงปลอดภัยสำหรับการใช้งานระบบรับส่งข้อมูลสารสนเทศผ่านระบบเครือข่ายสื่อสาร (electronic messaging) โดยมีการดำเนินการอย่างน้อย ดังนี้ (1) จัดให้มีมาตรการป้องกันการเปลี่ยนแปลงแก้ไข ทำความเสียหาย หรือเข้าถึงข้อมูล โดยไม่ได้รับอนุญาต

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. /25	แนวปฏิบัติ
	(2) มีกระบวนการยืนยันตัวตนผู้ใช้งานที่เหมาะสม โดยใช้วิธีการที่เข้มงวดในกรณีที่ใช้งานผ่านเครือข่ายสาธารณะ (3) กรณีที่มีการใช้งานระบบรับส่งข้อมูลสารสนเทศผ่านระบบเครือข่ายสื่อสารที่ให้บริการโดยบุคคลภายนอก เช่น โปรแกรมสนทนาผ่านระบบอิเล็กทรอนิกส์ (instant messaging) ระบบเครือข่ายสังคมออนไลน์ (social networking) หรือโปรแกรมเรียกใช้แฟ้มข้อมูลร่วมกัน (file sharing) ผู้ประกอบธุรกิจควรจัดให้มีการควบคุมดูแลอย่างเหมาะสมเพียงพอและคำนึงถึงการปฏิบัติตามกฎหมายและหลักเกณฑ์ของทางการอย่างเคร่งครัด (4) จัดให้มีมาตรการคัดกรอง (filter) จดหมายอิเล็กทรอนิกส์ที่มีความเสี่ยงต่อการเกิดภัยคุกคามทางไซเบอร์ เช่น จดหมายอิเล็กทรอนิกส์ที่มีไฟล์แนบชนิด .exe เป็นต้น (5) *[ความเสี่ยงสูง] ผู้ประกอบธุรกิจควรมีเครื่องมือในการวิเคราะห์พฤติกรรมการใช้งาน และเอกสารไฟล์แนบจากจดหมายอิเล็กทรอนิกส์ของผู้ใช้งาน ในสภาพแวดล้อมเสมือน เช่น การใช้งานเครื่องมือประเภท sandbox และระบบ advanced threat protection (ATP) เป็นต้น เพื่อตรวจสอบพฤติกรรมเสี่ยง และป้องกันความเสียหายจากการเข้าถึงข้อมูลและระบบงานสำคัญของบริษัท เป็นต้น*
2.10 การบริหารจัดการโครงการด้าน IT (IT project management) และมาตรการการจัดหา พัฒนา รวมถึงบำรุงรักษาระบบ IT (system acquisition, development and maintenance)	
ส่วนที่ 10 การบริหารจัดการโครงการด้าน IT (IT project management) มาตรการการจัดหา พัฒนา และบำรุงรักษาระบบ IT (system acquisition, development and maintenance) ผู้ประกอบธุรกิจต้องมีการบริหารจัดการโครงการด้าน IT และมีมาตรการการจัดหา พัฒนา และบำรุงรักษาระบบ IT เพื่อให้มั่นใจว่ามีการรักษาความมั่นคงปลอดภัยตลอดวงจรชีวิตของระบบ IT (entire life cycle) ดังนี้	

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. /25	แนวปฏิบัติ
2.10.1 การบริหารจัดการโครงการด้าน IT (IT project management)	
10.1 บริหารจัดการโครงการด้าน IT (IT project management) กำหนดกรอบการบริหารจัดการโครงการ (project management framework) เพื่อให้การบริหารจัดการโครงการที่มีนัยสำคัญเป็นไปอย่างมีประสิทธิภาพ สามารถส่งมอบโครงการได้อย่างถูกต้อง ครบถ้วนตามแผนงานและบรรลุวัตถุประสงค์ตามเป้าหมายที่กำหนดไว้	1. ผู้ประกอบธุรกิจควรกำหนดกรอบการบริหารจัดการโครงการ (project management framework) เป็นลายลักษณ์อักษร โดยมีรายละเอียดขั้นต่ำดังนี้ (1) โครงสร้างการควบคุมและกำกับดูแลโครงการ (project governance) ที่ชัดเจน เพื่อให้มีการควบคุมดูแลโครงการให้สำเร็จเป็นไปตามแผนงานที่กำหนด โดยพิจารณาการจัดให้มีผู้รับผิดชอบในบทบาทหน้าที่ตามความจำเป็นและความเหมาะสม เช่น (ก) คณะกรรมการกำกับดูแลโครงการ (project steering committee) มีบทบาทหน้าที่และความรับผิดชอบในการกำกับดูแลให้โครงการสำเร็จเป็นไปตามเป้าหมายที่กำหนด มีการติดตามความคืบหน้า ปัญหาและอุปสรรคของโครงการ เพื่อให้คำแนะนำและพิจารณาตัดสินใจการดำเนินงานที่สำคัญ โดยควรประกอบด้วยผู้บริหารจากหน่วยงานต่าง ๆ ที่เกี่ยวข้อง และเจ้าของโครงการหรือผู้สนับสนุนโครงการ (project owner/project sponsor) มีส่วนร่วมในการตัดสินใจ รวมทั้งคณะกรรมการกำกับดูแลโครงการควรมีการประชุมอย่างสม่ำเสมอเพื่อควบคุมดูแลโครงการที่สำคัญให้เป็นไปตามแผนงานที่กำหนด (ข) เจ้าของโครงการหรือผู้สนับสนุนโครงการ (project owner/ project sponsor) มีบทบาทหน้าที่ในการอนุมัติทรัพยากรในการดำเนินโครงการตั้งแต่ช่วงเริ่มต้นจนถึงช่วงจบโครงการ และพิจารณาการเปลี่ยนแปลงที่มีความสำคัญต่อโครงการ ประเมินผลการปฏิบัติงานของโครงการเมื่อจบแต่ละระยะของโครงการ รวมถึงกำหนดทิศทางในการตัดสินใจที่สำคัญต่าง ๆ ที่มีความเสี่ยงสูงในโครงการ (go/no-go decisions) และบริหารจัดการให้มั่นใจว่าโครงการจะสามารถส่งมอบตามที่คาดหวังได้ (ค) หน่วยงานหรือทีมงานดูแลภาพรวมโครงการ (project management office) มีบทบาทหน้าที่และความรับผิดชอบในการกำหนดรูปแบบ กระบวนการและเครื่องมือที่เป็นมาตรฐานในการบริหารจัดการและติดตามโครงการ รวมทั้งติดตาม รายงานภาพรวมโครงการสำคัญของผู้ประกอบธุรกิจ ให้กับคณะกรรมการของผู้ประกอบธุรกิจ และผู้บริหารระดับสูงที่เกี่ยวข้องได้รับทราบ เพื่อติดตามและสนับสนุนให้บริหารจัดการโครงการสำเร็จลุล่วงสอดคล้องกับเป้าหมายในระดับกลยุทธ์ของผู้ประกอบธุรกิจตามแผนงานที่กำหนด

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. /25	แนวปฏิบัติ
	(ง) ผู้จัดการโครงการ (project manager) มีบทบาทหน้าที่และความรับผิดชอบในการบริหารจัดการโครงการครอบคลุม กำหนดแผนงานโครงการ วิเคราะห์ผลกระทบ และจัดให้มีแนวทางรองรับหรือแผนสำรองกรณีโครงการประสบปัญหาหรือล่าช้า รวมทั้งรายงานให้คณะกรรมการกำกับดูแลโครงการพิจารณาตัดสินใจแก้ไขปัญหาได้ทันการณ์ เพื่อให้โครงการสามารถส่งมอบได้อย่างถูกต้องครบถ้วนสำเร็จตามแผนงานที่กำหนด โดยผู้จัดการโครงการ ต้องมีความรู้ความสามารถและประสบการณ์ในการบริหารโครงการที่เพียงพอ (2) แนวทางการบริหารจัดการโครงการ โดยมีรายละเอียดขั้นต่ำดังนี้ (ก) ระเบียบขั้นตอนการบริหารจัดการโครงการ ครอบคลุมตั้งแต่ก่อนเริ่มโครงการ การดำเนินการและควบคุมโครงการ การปิดโครงการ และการสอบทานโครงการ (ข) ปัจจัยและเกณฑ์ในการประเมินหรือจัดระดับความสำคัญของโครงการที่ชัดเจน รวมถึงขอบเขตอำนาจหน้าที่ในการอนุมัติและกำกับดูแลโครงการตามระดับความสำคัญของโครงการ (ค) เอกสารหรือสิ่งส่งมอบในแต่ละขั้นตอนอย่างชัดเจน เช่น แผนการดำเนินโครงการ รายงานความคืบหน้า รายงานการปิดโครงการ เป็นต้น 2. การเริ่มโครงการ ผู้ประกอบธุรกิจควรดำเนินการ ดังนี้ (1) ประเมินความจำเป็นและประโยชน์ที่คาดว่าจะได้รับ ประเมินความเสี่ยงและผลกระทบที่อาจเกิดขึ้นต่อฝ่ายงานอื่นและระบบที่เกี่ยวข้อง รวมทั้งเลือกใช้เทคโนโลยีที่เหมาะสม ทั้งนี้ โครงการต้องมีเป้าหมายที่ชัดเจน (project objective) สอดคล้องกับกลยุทธ์ขององค์กรและคำนึงถึงการรักษาความมั่นคงปลอดภัย (2) จัดทำแผนการดำเนินโครงการที่มีรายละเอียดครบถ้วนเพียงพอต่อการบริหารจัดการโครงการอย่างน้อยครอบคลุม (ก) เป้าหมายโครงการ (ข) ทรัพยากรที่ใช้ (ค) บทบาทหน้าที่ ความรับผิดชอบของทีมงานในการดำเนินโครงการ โดยทีมงานจะต้องมีประสิทธิภาพและมีความรู้ความเชี่ยวชาญเพียงพอในการดำเนินโครงการ (ง) ขอบเขตและระยะเวลาของการดำเนินโครงการในแต่ละขั้นตอน

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. /25	แนวปฏิบัติ
	(จ) ผลงานที่จะส่งมอบในแต่ละขั้นตอน (ฉ) ข้อกำหนดเงื่อนไขที่เกี่ยวข้องกับโครงการ เช่น ข้อกำหนดของผู้ว่าจ้าง ภาระผูกพัน ข้อจำกัด เป็นต้น (3) มีการนำเสนอแผนการดำเนินโครงการ เพื่อขออนุมัติโครงการต่อคณะกรรมการหรือผู้บริหารของผู้ประกอบธุรกิจที่ได้รับมอบหมายตามขอบเขตในการอนุมัติที่กำหนดไว้ 3. การดำเนินงานและควบคุมโครงการ ผู้ประกอบธุรกิจควรดำเนินการ ดังนี้ (1) ประเมินและติดตามการดำเนินโครงการอย่างต่อเนื่องและครอบคลุมขอบเขต ระยะเวลา และทรัพยากรที่วางแผน (2) ในกรณีที่มีการเปลี่ยนแปลงขอบเขต ระยะเวลาและหรือทรัพยากร หรือยกเลิกโครงการ ควรมีการนำเสนอเพื่อขออนุมัติการเปลี่ยนแปลงหรือยกเลิกโครงการ (3) รายงานความคืบหน้า ปัญหา อุปสรรคและข้อจำกัดในการดำเนินโครงการ ต่อคณะกรรมการกำกับดูแลโครงการหรือผู้บริหารที่ได้รับมอบหมายอย่างสม่ำเสมอ (4) โครงการที่ส่งผลกระทบต่อธุรกิจของผู้ประกอบธุรกิจอย่างมีนัยสำคัญ ควรได้รับการนำเสนอแก่คณะกรรมการของผู้ประกอบธุรกิจด้วย 4. การปิดโครงการ ผู้ประกอบธุรกิจควรดำเนินการ ดังนี้ (1) มีการสรุปประโยชน์ที่ได้รับจากโครงการเปรียบเทียบกับเป้าหมายที่กำหนด (2) มีการรวบรวมปัญหา อุปสรรคจากการบริหารจัดการโครงการ เพื่อนำมาเป็นสิ่งที่ได้เรียนรู้ (lesson learned) ใช้สำหรับวิเคราะห์ ปรับปรุง และพัฒนา 5. ผู้ประกอบธุรกิจควรสอบทานโครงการที่สำคัญ เพื่อให้มั่นใจได้ว่าโครงการสอดคล้องกับเป้าหมายของโครงการ นโยบาย มาตรฐาน ระเบียบและวิธีปฏิบัติของผู้ประกอบธุรกิจ รวมทั้งกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง 6. *[ความเสี่ยงสูง] ผู้ประกอบธุรกิจควรกำหนดให้ผู้สอบทานโครงการที่สำคัญมีความเป็นอิสระจากผู้ดำเนินโครงการ เช่น หน่วยงาน project quality* assurance *เป็นต้น*

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. /25	แนวปฏิบัติ
2.10.2 การจัดหาระบบ IT (system acquisition)	
10.2 จัดหาระบบ IT (system acquisition) จัดให้มีหลักเกณฑ์ในการจัดหาระบบ IT และผู้ให้บริการ เพื่อมั่นใจว่าระบบที่จัดหาสามารถตอบสนองความต้องการทางธุรกิจและความต้องการด้านความมั่นคงปลอดภัย IT โดยคำนึงถึงความยืดหยุ่นในการเปลี่ยนแปลงผู้ให้บริการ การเปลี่ยนแปลงเทคโนโลยี รวมถึงการเปลี่ยนแปลงต่าง ๆ ที่เกี่ยวข้องกับการดำเนินธุรกิจอย่างมีนัยสำคัญ	ผู้ประกอบธุรกิจควรจัดให้มีหลักเกณฑ์ในการคัดเลือกระบบ IT และผู้ให้บริการ เพื่อมั่นใจว่าระบบที่จัดหาสามารถตอบสนองความต้องการทางธุรกิจและความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ ซึ่งควรคำนึงถึงเรื่องดังนี้ 1. รายละเอียดทั่วไป เช่น เทคโนโลยีที่ใช้ สิทธิการใช้งานซอฟต์แวร์ (software license) ฟังก์ชันการทำงานของระบบ เป็นต้น 2. ความมั่นคงปลอดภัยของระบบ 3. ฐานะการเงิน ชื่อเสียง และความสามารถด้านเทคนิค 4. การได้รับการรับรองตามมาตรฐานสากลหรือมาตรฐานด้าน IT ที่เกี่ยวข้องที่ได้รับการยอมรับโดยทั่วไป (certificate) 5. การสนับสนุนและการบำรุงรักษาระบบ 6. ความน่าเชื่อถือของระบบและผู้ให้บริการ 7. การทดสอบการทำงานขั้นต้น (proof of concept) ในกรณีที่เป็นระบบ IT ที่มีนัยสำคัญ 8. ข้อตกลงการรับฝากโค้ดต้นฉบับ (source code escrow agreement) เพื่อให้มั่นใจว่าในกรณีที่ผู้พัฒนาระบบหรือผู้ให้บริการซอฟต์แวร์ไม่ปฏิบัติตามข้อตกลงในการบำรุงรักษาระบบหรือให้การสนับสนุนการดำเนินงานตามที่ตกลงไว้ ผู้ประกอบธุรกิจจะมีสิทธิในการเข้าถึง source code ของระบบหรือซอฟต์แวร์ดังกล่าว ทั้งนี้ กรณีที่มีข้อจำกัดทำให้ไม่สามารถกำหนดข้อตกลงข้างต้นได้ ผู้ประกอบธุรกิจควรพิจารณาวิธีการบริหารจัดการความเสี่ยงดังกล่าวอย่างเหมาะสม 9. ความยืดหยุ่นในการเปลี่ยนแปลงผู้ให้บริการ การเปลี่ยนแปลงเทคโนโลยี และการเปลี่ยนแปลงกลยุทธ์ในการดำเนินธุรกิจ
2.10.3 การพัฒนาระบบ IT (system development))	
10.3 พัฒนาระบบ IT (system development) จัดให้มีมาตรการควบคุมเกี่ยวกับการพัฒนาระบบ IT ในการออกแบบ พัฒนา ทดสอบระบบ และนำระบบขึ้นใช้งานจริง เพื่อให้มั่นใจว่าระบบมีความถูกต้อง มั่นคงปลอดภัย เชื่อถือได้ พร้อมใช้งาน และมีความยืดหยุ่นเพียงพอจะรองรับการใช้งานได้ สอดคล้องกับแผนการดำเนินธุรกิจ โดยต้อง	ผู้ประกอบธุรกิจควรจัดให้มีการควบคุมด้านความมั่นคงปลอดภัยด้านสารสนเทศในการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบ IT เพื่อให้มั่นใจว่าระบบมีความถูกต้อง มั่นคงปลอดภัย เชื่อถือได้ พร้อมใช้งาน และมีความยืดหยุ่นเพียงพอที่จะรองรับการปรับปรุงเปลี่ยนแปลง ทั้งนี้ รวมถึงกรณีการพัฒนาระบบ IT ที่มีการกำหนดรอบการพัฒนาย่อย ๆ (sprint) เช่น การพัฒนาระบบ IT แบบ agile เป็นต้น

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. /25	แนวปฏิบัติ
ดำเนินการอย่างน้อยดังนี้	
(1) มีการกำหนดรายละเอียดความต้องการของระบบ (requirement) และคุณสมบัติทางเทคนิค (technical specification) ของระบบที่พัฒนา ดังนี้ (1.1) ความมั่นคงปลอดภัย (security) (1.2) ความเป็นส่วนตัว (privacy) (1.3) สภาพพร้อมใช้งาน (availability) (1.4) ขีดความสามารถที่รองรับ (capacity)	<u>การออกแบบระบบ</u> ผู้ประกอบธุรกิจควรกำหนดกระบวนการขั้นต่ำในการกำหนดรายละเอียดความต้องการของระบบ (requirement) และคุณสมบัติทางเทคนิค (technical specification) ของระบบที่พัฒนา ดังนี้ 1. กำหนดให้หน่วยงานธุรกิจที่เกี่ยวข้องมีส่วนร่วมในการกำหนดรายละเอียดความต้องการทางธุรกิจ (business requirement) ก่อนเริ่มออกแบบระบบ 2. จัดทำเอกสารความต้องการของระบบ (system requirement) ทั้งในด้านความต้องการที่เป็นหน้าที่หลักของระบบ (functional requirement) และความต้องการที่ไม่ใช่หน้าที่หลัก (non-functional requirement) 3. จัดทำเอกสารรายละเอียดคุณสมบัติทางเทคนิค (technical specification) ของระบบที่พัฒนาที่ครอบคลุมเรื่อง ดังนี้ (1) ความมั่นคงปลอดภัย (security) (2) ความเป็นส่วนตัว (privacy) (3) ความพร้อมใช้ (availability) เช่น การออกแบบให้มีระบบทดแทน high availability หรือ redundancy รวมถึงมีระบบสำรอง (DR strategy) เพื่อให้ระบบสามารถให้บริการได้อย่างต่อเนื่อง และลดความเสี่ยงที่จุดใดจุดหนึ่งทำให้ระบบเกิดปัญหาหรือล้มเหลวทั้งหมด (single point of failure) (4) ขีดความสามารถที่รองรับ (capacity) ทั้งนี้ เอกสารรายละเอียดคุณสมบัติทางเทคนิคควรผ่านการสอบทานความถูกต้องครบถ้วนและได้รับอนุมัติจากผู้เกี่ยวข้องก่อนเริ่มพัฒนาระบบ
(2) มีการแบ่งแยกบทบาทหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องในการพัฒนาระบบ เพื่อให้มีการสอบทานก่อนนำระบบขึ้นไปให้บริการจริง	<u>การพัฒนาระบบ</u> ผู้ประกอบธุรกิจควรกำหนดกระบวนการขั้นต่ำในการการพัฒนาระบบ ดังนี้ 1. แบ่งแยกบทบาทหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องในการพัฒนาระบบ (segregation of duty) เพื่อให้มีการสอบทานก่อนนำระบบขึ้นไปให้บริการจริง เช่น แยกผู้พัฒนาระบบ ออกจากผู้นำระบบขึ้นใช้งานจริง เป็นต้น

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. /25	แนวปฏิบัติ
(3) มีการแบ่งแยกสภาพแวดล้อมของระบบงานที่ใช้สำหรับการพัฒนา (development) และการทดสอบ (testing) ออกจากระบบงานที่ให้บริการจริง (production)	2. แบ่งแยกสภาพแวดล้อมของระบบงานที่ใช้สำหรับการพัฒนา (development) และการทดสอบ (testing) ออกจากระบบงานที่ให้บริการจริง (production) โดยควบคุมให้มีการเข้าถึงเฉพาะผู้ที่เกี่ยวข้องในแต่ละส่วนเท่านั้น 3. จัดให้มีการรักษาความมั่นคงปลอดภัยของเครื่องที่ไม่ได้อยู่บนระบบที่ให้บริการจริง (non-production) ให้เพียงพอกับระดับความเสี่ยงของการเข้าถึงโดยไม่ได้รับอนุญาต และการรั่วไหลของข้อมูลที่ใช้ทดสอบ 4. จัดให้มีการควบคุมไม่ให้มีการติดตั้งเครื่องมือการพัฒนาระบบ (development tools) และเครื่องมือแปลโปรแกรม (compilers) ไว้บนระบบที่ให้บริการจริง เพื่อป้องกันความเสี่ยงที่อาจถูกปรับเปลี่ยนหรือติดตั้งโปรแกรมโดยไม่ได้รับอนุญาต
(4) มีกระบวนการหรือเครื่องมือควบคุมการพัฒนาชุดคำสั่งคอมพิวเตอร์ให้มีความปลอดภัย	5. กำหนดมาตรฐานและระเบียบวิธีปฏิบัติในการออกแบบและพัฒนาระบบอย่างปลอดภัย (secure coding) สอดคล้องกับมาตรฐานสากล รวมทั้งควบคุมให้ผู้พัฒนาระบบปฏิบัติตามมาตรฐานและระเบียบวิธีปฏิบัติดังกล่าว 6. สอบทานคำสั่งในการเขียนโปรแกรม (source code review) โดยใช้ระบบอัตโนมัติ (automated review) หรือแบบ manual ซึ่งดำเนินการโดยบุคคลที่ไม่ใช่ผู้พัฒนาโปรแกรม เมื่อมีการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบ IT ที่มีความสำคัญ ซึ่งมีความเสี่ยงด้านความมั่นคงปลอดภัย เพื่อให้สามารถระบุช่องโหว่ด้านความมั่นคงปลอดภัย และปิดช่องโหว่ที่พบก่อนนำระบบไปใช้งานจริง 7. [ความเสี่ยงสูง] สอบทานคำสั่งในการเขียนโปรแกรมแบบ manual (manual source code review) โดยผู้เชี่ยวชาญที่มีความเป็นอิสระจากผู้พัฒนาโปรแกรม เมื่อมีการพัฒนาระบบ IT ที่มีความสำคัญ หรือมีการเปลี่ยนแปลงที่มีความเสี่ยงด้านความมั่นคงปลอดภัยของระบบ IT ที่มีความสำคัญ 8. มีกระบวนการหรือเครื่องมือควบคุมเวอร์ชันของชุดคำสั่งคอมพิวเตอร์ (source code version control)
(5) มีการทดสอบระบบ IT ที่ได้รับการพัฒนาหรือแก้ไขเปลี่ยนแปลง เพื่อให้มั่นใจได้ว่าระบบดังกล่าวสามารถประมวลผลได้อย่างถูกต้องครบถ้วน และเป็นไปตามความต้องการของผู้ใช้งาน	<u>การทดสอบระบบ</u> ผู้ประกอบธุรกิจควรกำหนดกระบวนการขั้นต่ำในการการทดสอบระบบ IT ที่ได้รับการพัฒนาหรือแก้ไขเปลี่ยนแปลง เพื่อให้มั่นใจว่า

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. /25	แนวปฏิบัติ
	การทำงานของระบบมีประสิทธิภาพ การประมวลผลถูกต้องครบถ้วน และเป็นไปตามความต้องการของผู้ใช้งานดังนี้ 1. ทดสอบระบบ IT โดยผู้ทดสอบที่เป็นอิสระจากผู้พัฒนาระบบ เพื่อให้มั่นใจได้ว่าระบบที่ได้รับการพัฒนาดังกล่าวสามารถทำงานได้อย่างถูกต้องตรงความต้องการของผู้ใช้งาน และเป็นไปตามนโยบายด้านความมั่นคงปลอดภัยของระบบ IT 2. ทดสอบระบบ IT ก่อนนำไปใช้งานหรือให้บริการจริง โดยครอบคลุมการทดสอบ ดังนี้ (1) ทดสอบการทำงานของแต่ละหน่วย (unit test) (2) ทดสอบการทำงานของระบบและการเชื่อมต่อ (system and integration test) (3) ทดสอบความต้องการของผู้ใช้งาน (user acceptance test) (4) ทดสอบการรักษาความปลอดภัย (security test) ได้แก่ การประเมินช่องโหว่ (vulnerabilities assessment) และการทดสอบเจาะระบบ (penetration test) ตามความจำเป็น สำหรับระบบใหม่ใด ๆ ที่มีการเชื่อมต่อกับระบบ IT ที่มีความสำคัญ เพื่อให้สามารถตรวจพบช่องโหว่และดำเนินการปรับปรุงแก้ไขได้ก่อนเริ่มให้บริการจริง 3. กำหนดสถานการณ์ที่ใช้ทดสอบ (test scenario) หรือกรณีที่ใช้ทดสอบ (test case) แบบ end-to-end และมีกระบวนการสอบทาน test scenario หรือ test case เพื่อให้มั่นใจว่ามีความครอบคลุมเพียงพอและตรงกับความต้องการของหน่วยงานธุรกิจ (business requirement) 4. ทดสอบระบบบนสภาพแวดล้อม (test environment) ที่ใกล้เคียงระบบที่ให้บริการจริง เพื่อลดความเสี่ยงที่อาจเกิดขึ้นจากการเปลี่ยนแปลงบนระบบที่ให้บริการจริง 5. จัดการข้อบกพร่อง (defect) ของระบบที่พบในการทดสอบ โดยพิจารณาแนวทางปรับปรุง หรือลดความเสี่ยงหรือผลกระทบของข้อบกพร่องดังกล่าว 6. มีการขออนุมัติผลการทดสอบจากฝ่ายงานที่เกี่ยวข้อง ก่อนนำระบบขึ้นใช้งานจริง
(6) มีมาตรการควบคุมความถูกต้องครบถ้วนของการแปลงข้อมูล (data conversion)	มาตรการควบคุมความถูกต้องครบถ้วนของการแปลงข้อมูล (data conversion) ควรครอบคลุมกรณีที่มีการโอนย้ายข้อมูลจากระบบเดิมไปยังระบบใหม่ (data migration) เช่น การทำ storage migration cloud migration หรือ application migration เป็นต้น
(7) มีมาตรการรักษาความมั่นคงปลอดภัย และความลับของข้อมูลสำคัญที่นำไปใช้ในการทดสอบ	กรณีที่มีการนำข้อมูลสำคัญจากระบบจริงมาใช้เพื่อทดสอบระบบ ผู้ประกอบธุรกิจควรจัดให้มีแนวทางการรักษาความปลอดภัยและความลับของข้อมูลดังกล่าว เช่น การทำ data masking เป็นต้น เพื่อป้องกันความเสี่ยงในการรั่วไหลของข้อมูล

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. /25	แนวปฏิบัติ
(8) มีการทดสอบประสิทธิภาพ (performance test) ของระบบที่เกี่ยวข้องกับการให้บริการหรือการทำธุรกรรมทางอิเล็กทรอนิกส์ เมื่อมีการพัฒนาหรือเปลี่ยนแปลงอย่างมีนัยสำคัญ เพื่อให้มั่นใจว่าระบบดังกล่าวสามารถรองรับปริมาณการใช้งานได้สอดคล้องกับความต้องการทางธุรกิจ	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]
(9) ในกรณีที่มีการมอบให้มอบหมายให้บุคคลภายนอกเป็นผู้พัฒนาหรือแก้ไขเปลี่ยนแปลงระบบ IT ผู้ประกอบธุรกิจต้องจัดให้มีการติดตาม และควบคุมการดำเนินการให้ไปตามข้อตกลงในการมอบหมายงาน	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]
(10) มีกระบวนการขออนุมัติจากผู้บริหารหรือคณะกรรมการที่ได้รับมอบหมายจากผู้ประกอบธุรกิจ ก่อนนำระบบขึ้นใช้งานจริง	<u>การนำระบบขึ้นใช้งานจริง</u> ผู้ประกอบธุรกิจควรจัดให้มีขั้นตอนการประเมินความพร้อมและมาตรการป้องกันความเสี่ยงในการนำระบบขึ้นใช้งานจริง เช่น 1. การพิจารณาผลการทดสอบระบบ การจัดการข้อบกพร่อง และความเสี่ยงของข้อบกพร่องคงค้าง (outstanding issue) ว่าอยู่ในระดับที่ยอมรับได้ 2. การเตรียมความพร้อมในการนำระบบขึ้นใช้งานจริง และเตรียมระบบเวอร์ชันก่อนการเปลี่ยนแปลงให้พร้อมนำกลับมาใช้งานได้ 3. การเตรียมเงื่อนไขการนำระบบใหม่เข้าไปทดแทน (cutover หรือ go-live technique) ที่เหมาะสมกับระดับความเสี่ยง เช่น parallel changeover, phased changeover หรือ abrupt changeover เป็นต้น 4. การตรวจสอบความครบถ้วนของการดำเนินการตามมาตรการรักษาความมั่นคงปลอดภัยด้าน IT เช่น จัดทำรายการ operational clearance และ security check เป็นต้น ก่อนที่จะขออนุมัติการนำระบบขึ้นใช้งานจริงควรได้รับการเห็นชอบจากผู้บริหารหรือคณะกรรมการที่ได้รับมอบหมายจากผู้ประกอบธุรกิจ ตามขั้นตอนปฏิบัติในการบริหารจัดการการเปลี่ยนแปลง (change management)

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. /25	แนวปฏิบัติ
2.10.4 การแก้ไขเปลี่ยนแปลงระบบ IT (system change)	
10.4 แก้ไขเปลี่ยนแปลงระบบ IT (system change)	การแก้ไขเปลี่ยนแปลงระบบ IT (system change) ควรพิจารณาดำเนินการตามแนวปฏิบัติเรื่องการบริหารจัดการการเปลี่ยนแปลง (change management) และแนวปฏิบัติเรื่องการพัฒนาระบบ
(1) มีการประเมินผลกระทบ และจัดลำดับความสำคัญของการเปลี่ยนแปลง	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]
(2) มีกระบวนการอนุมัติการเปลี่ยนแปลง (change request) โดยต้องได้รับการอนุมัติจากหน่วยงานเจ้าของระบบ (system owner) เป็นลายลักษณ์อักษร เพื่อให้มั่นใจได้ว่าการขอเปลี่ยนแปลงได้รับการพิจารณาความจำเป็นอย่างเหมาะสมแล้ว	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]
(3) มีการทดสอบระบบภายหลังจากการเปลี่ยนแปลง	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]
(4) มีกระบวนการขออนุมัติจากผู้บริหารหรือคณะกรรมการที่ได้รับมอบหมายจากผู้ประกอบธุรกิจก่อนนำระบบขึ้นใช้งานจริง	ปรับปรุงขั้นตอนการปฏิบัติงาน และแผนบริหารความต่อเนื่องทางธุรกิจ (business continuity plan) หลังจากที่ได้มีการแก้ไขเปลี่ยนแปลงระบบ IT เพื่อให้ทันสมัยอยู่เสมอ นอกจากนี้ ควรสื่อสารให้กับบุคคลที่เกี่ยวข้องได้รับทราบเพื่อให้สามารถปฏิบัติงานได้อย่างถูกต้อง
(5) มีกระบวนการหรือเครื่องมือควบคุมการเปลี่ยนแปลงรุ่น (version) ของชุดคำสั่งคอมพิวเตอร์ (source code version control) และรองรับการถอยกลับสู่สภาพเดิม (fallback)	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]
(6) ปรับปรุงรายละเอียดประกอบระบบงานที่ได้มีการแก้ไขเปลี่ยนแปลง เพื่อให้เป็นปัจจุบัน	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. /25	แนวปฏิบัติ
2.11 การบริหารจัดการเหตุการณ์ผิดปกติด้าน IT และปัญหาด้าน IT (IT incident management)	
ส่วนที่ 11 การบริหารจัดการเหตุการณ์ผิดปกติด้าน IT และปัญหาด้าน IT (IT incident management) ผู้ประกอบธุรกิจต้องมีการบริหารจัดการเหตุการณ์ผิดปกติด้าน IT และปัญหาด้าน IT อย่างเหมาะสมและทันท่วงที ดังนี้	
11.1 จัดให้มีช่องทางรับแจ้งเหตุการณ์ผิดปกติด้าน IT จากบุคลากร ผู้ใช้บริการ และผู้ที่เกี่ยวข้อง	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]
11.2 กำหนดแผน หรือขั้นตอนการบริหารจัดการเหตุการณ์ผิดปกติด้าน IT และปัญหาด้าน IT	ผู้ประกอบธุรกิจควรกำหนดแผนหรือขั้นตอนการบริหารจัดการเหตุการณ์ผิดปกติและปัญหาด้าน IT ที่ครอบคลุมรายละเอียดอย่างน้อย ดังนี้ 1. การรับแจ้งเหตุการณ์ (1) หน่วยงาน หรือบุคลากรที่มีหน้าที่รับแจ้งเหตุการณ์ (point of contact) (2) ช่องทางการรับแจ้งเหตุการณ์จากผู้พบเห็นหรือสงสัยว่ามีเหตุการณ์ผิดปกติและปัญหาด้าน IT เกิดขึ้น เช่น อีเมล โทรศัพท์ แบบฟอร์มติดต่อทางเว็บไซต์ และสื่อสังคมออนไลน์ เป็นต้น ตามข้อกำหนด 11.1 (3) การบันทึกข้อมูลเหตุการณ์ที่ได้รับแจ้ง เพื่อใช้ในการติดตามการดำเนินงาน 2. การตรวจสอบและประเมินเหตุการณ์ (1) การตรวจสอบความถูกต้องข้อมูลที่ได้รับแจ้ง (2) การจัดประเภท และความเร่งด่วนของเหตุการณ์ เพื่อดำเนินการแก้ไขปัญหาภายในระยะเวลาที่เหมาะสม 3. การสื่อสารเหตุการณ์ (1) หลักเกณฑ์การส่งต่อเหตุการณ์ผิดปกติ (incident escalation) และรายงานความคืบหน้าเหตุการณ์ให้ผู้ที่เกี่ยวข้อง ผู้บริหารระดับสูง และคณะกรรมการของผู้ประกอบธุรกิจได้ทราบ ให้สอดคล้องกับระดับความรุนแรงของเหตุการณ์ (2) การแจ้งบุคคลที่เกี่ยวข้อง เช่น ลูกค้า หรือหน่วยงานที่เกี่ยวข้อง เป็นต้น รับทราบโดยไม่ชักช้า ในกรณีที่เหตุการณ์ส่งผล

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. /25	แนวปฏิบัติ
	กระทบต่อบุคคลดังกล่าว (3) การจัดให้มีการรายงานความคืบหน้าในการบริหารจัดการสถานการณ์และผลการบริหารจัดการให้ผู้ที่เกี่ยวข้องรับทราบเป็นระยะตามความเหมาะสม และแจ้งเมื่อเหตุการณ์ยุติแล้ว 4. การแก้ไขเหตุการณ์ (1) ขั้นตอนการตอบสนองต่อเหตุการณ์ (incident response plan) ตามประเภทหรือความเร่งด่วนของเหตุการณ์ เพื่อทำให้เหตุการณ์คลี่คลายหรือกลับสู่ภาวะปกติอย่างรวดเร็ว โดยอย่างน้อยควรระบุกระบวนการรับมือ และช่องทางประสานงานเพื่อรับการสนับสนุนจากผู้เชี่ยวชาญ (2) การวิเคราะห์ข้อมูล (analysis) การจำกัดความเสียหาย (containment) การจัดเก็บหลักฐานอย่างปลอดภัย (evidence gathering) และการแก้ไขปัญหาและฟื้นฟูระบบ (eradication and recovery) ในกรณีของภัยคุกคามทางไซเบอร์ (3) การตรวจพิสูจน์พยานหลักฐานทางดิจิทัล (digital forensic) โดยผู้ที่มีความเชี่ยวชาญเพื่อให้ทราบสาเหตุหรือช่องโหว่ของระบบ และสามารถดำเนินการปิดช่องโหว่ได้อย่างปลอดภัย ในกรณีภัยคุกคามทางไซเบอร์ซึ่งส่งผลกระทบอย่างมีนัยสำคัญต่อทรัพย์สินและข้อมูลของลูกค้า 5. การสิ้นสุดการแก้ไขเหตุการณ์ (1) การทบทวนหลังการดำเนินการ (after-action review process) เพื่อวิเคราะห์สาเหตุที่แท้จริง (root cause analysis) ของเหตุการณ์ และเพื่อหาแนวทางการแก้ไขทั้งในระยะสั้นและระยะยาว และป้องกันเหตุการณ์ที่อาจเกิดขึ้นซ้ำในอนาคต ตามข้อกำหนด 11.4 (2) การจัดเก็บข้อมูลบันทึกเหตุการณ์ที่เกิดขึ้นในรูปแบบที่เป็นมาตรฐาน โดยมีเนื้อหาขั้นต่ำประกอบด้วย วันเวลาที่เกิดเหตุการณ์ รายละเอียดเหตุการณ์ ผลกระทบ วิธีการแก้ไข วันเวลาที่สิ้นสุดเหตุการณ์ สาเหตุที่เกิดปัญหา และแนวทางการป้องกันในอนาคต ตามข้อกำหนด 11.5 (3) *[ความเสี่ยงสูง] การถอดบทเรียน (lesson learned) จากเหตุการณ์การโจมตีทางไซเบอร์ที่เกิดขึ้นจริง เพื่อทบทวนหรือปรับปรุงความสามารถในการลดความเสี่ยง ป้องกันการเกิดเหตุการณ์ซ้ำ และปรับปรุงแผนรับมือภัยคุกคามทางไซเบอร์*

<table>
<tr><th>ข้อกำหนดในภาคผนวก 3
แนบท้ายประกาศที่ สธ. /25</th><th>แนวปฏิบัติ</th></tr>
<tr><td>11.3 รายงานเหตุการณ์ผิดปกติด้าน IT เหตุการณ์การละเมิดต่อข้อมูลส่วนบุคคล และเหตุการณ์ที่ส่งผลให้ทรัพย์สินด้าน IT ของผู้ใช้งานเสียหายอันเกิดจากเหตุการณ์ด้านความมั่นคงปลอดภัยระบบ IT ต่อผู้มีหน้าที่รับผิดชอบเหตุการณ์ และสำนักงานโดยไม่ชักช้าเมื่อทราบเหตุการณ์ดังกล่าว</td><td>1. ผู้ประกอบธุรกิจควรรายงานเหตุการณ์ที่มีการละเมิดกฎหมาย กฎ และระเบียบที่เกี่ยวข้องกับผู้ประกอบธุรกิจ กับหน่วยงานที่เกี่ยวข้องโดยไม่ชักช้า และภายในระยะเวลาที่กฎหมายกำหนดไว้ เช่น รายงานเหตุการณ์ที่ส่งผลกระทบต่อลูกค้าในวงกว้างต่อสำนักงานภายใน 3 ชั่วโมง และรายงานเหตุการณ์ข้อมูลของลูกค้ารั่วไหลต่อสำนักงานคณะกรรมความเป็นส่วนตัวภายใน 72 ชั่วโมง เป็นต้น
2. ผู้ประกอบธุรกิจควรรายงานสำนักงานในกรณีที่มีเหตุการณ์ผิดปกติด้าน IT เหตุการณ์การละเมิดต่อข้อมูลส่วนบุคคล และเหตุการณ์ที่ส่งผลให้ทรัพย์สินด้าน IT ของผู้ใช้งานเสียหาย ซึ่งมีผลกระทบต่อลูกค้าในวงกว้าง โดยครอบคลุมเหตุการณ์ ดังนี้
(1) การละเมิดต่อข้อมูลส่วนบุคคลที่เกิดจากเหตุการณ์ผิดปกติด้าน IT
(2) ทรัพย์สินของผู้ใช้งานสูญหาย หรือเสียหาย
(3) การบุกรุก เข้าถึง หรือใช้งานระบบโดยไม่ได้รับอนุญาต (system compromised)
(4) ส่งผลกระทบต่อชื่อเสียงของผู้ประกอบธุรกิจ (harm to reputation) เช่น ถูกปลอมแปลงหน้าเว็บไซต์ของบริษัท (website defacement) เป็นต้น
(5) การหยุดชะงักของระบบงาน (system disruption) ในช่วงเวลาทำการซื้อขายระหว่างวันทำการ เป็นระยะเวลาถึงระดับที่ต้องรายงานสำนักงาน ดังนี้
<table>
<tr><th>ระบบงาน</th><th>ระยะเวลาหยุดชะงัก
ก่อนที่จะรายงานสำนักงาน</th></tr>
<tr><td>ระบบจับคู่คำสั่งซื้อขาย (trading system)</td><td>การหยุดชะงักทุกกรณี</td></tr>
<tr><td>ระบบจัดการคำสั่งซื้อขาย (order management system)</td><td>15 นาที</td></tr>
<tr><td>ระบบอื่น ๆ เช่น หน้าเว็บไซต์หลัก ระบบฝากและถอนทรัพย์สิน เป็นต้น</td><td>60 นาที</td></tr>
</table>
ทั้งนี้ ไม่รวมถึงกรณีที่ปิดปรับปรุงระบบ (system maintenance) ซึ่งมีการแจ้งให้ลูกค้าทราบล่วงหน้า
3. ผู้ประกอบธุรกิจควรรายงานเหตุการณ์ต่อสำนักงานภายในกรอบระยะเวลา ดังนี้
(1) รายงานโดยไม่ชักช้าภายใน 3 ชั่วโมงนับแต่ทราบเหตุการณ์ โดยมีเนื้อหาครอบคลุมถึงวันเวลา ประเภทเหตุการณ์ เหตุการณ์ และผลกระทบที่คาดว่าจะเกิดขึ้น ทั้งนี้ สามารถแจ้งโดยวาจาหรือรายงานผ่านช่องทางอิเล็กทรอนิกส์ตามที่</td></tr>
</table>

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. /25	แนวปฏิบัติ
	สำนักงานกำหนดตามความเหมาะสม (2) รายงานความคืบหน้าเป็นลายลักษณ์อักษรอย่างน้อยทุกวันทำการภายในเวลา 16:00 น. เริ่มจากวันทำการถัดไปหลังทราบเหตุการณ์ หรือตามที่สำนักงานร้องขอ จนกว่าระบบ IT จะกลับสู่การให้บริการได้อย่างเป็นปกติ โดยมีเนื้อหาครอบคลุมถึงวันเวลา ประเภทเหตุการณ์ เหตุการณ์ ผลกระทบที่เกิดขึ้น และความคืบหน้าในการแก้ไขปัญหา ทั้งนี้ ให้รายงานผ่านช่องทางอิเล็กทรอนิกส์ที่สำนักงานกำหนด (3) รายงานเมื่อเหตุการณ์ยุติหรือแก้ไขปัญหาแล้วเสร็จ โดยมีเนื้อหาครอบคลุมถึงวันเวลา ประเภทเหตุการณ์ เหตุการณ์ ผลกระทบที่เกิดขึ้น การดำเนินการแก้ไขปัญหา ผลการแก้ไขปัญหา ระยะเวลาในการแก้ไข สาเหตุที่เกิดปัญหา และแนวทางป้องกันในอนาคต ทั้งนี้ ให้รายงานผ่านช่องทางอิเล็กทรอนิกส์ที่สำนักงานกำหนด 4. กรณีของหน่วยงานโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศ (critical information infrastructure organization หรือ CII organization) ให้รายงานสำนักงานภายในกรอบระยะเวลา ดังนี้ (1) รายงานโดยไม่ชักช้าภายใน 1 ชั่วโมงนับแต่ทราบเหตุการณ์ โดยมีเนื้อหาครอบคลุมถึงวันเวลา ประเภทเหตุการณ์ เหตุการณ์ และผลกระทบที่คาดว่าจะเกิดขึ้น ทั้งนี้ สามารถแจ้งโดยวาจาหรือรายงานผ่านช่องทางอิเล็กทรอนิกส์ตามที่สำนักงานกำหนดตามความเหมาะสม (2) รายงานความคืบหน้าเป็นลายลักษณ์อักษรครั้งแรก ภายใน 2 ชั่วโมงนับแต่ทราบเหตุการณ์ และรายงานครั้งต่อไปอย่างน้อยทุกวันทำการภายในเวลา 16:00 น. เริ่มจากวันทำการถัดไปหลังทราบเหตุการณ์ หรือตามที่สำนักงานร้องขอ จนกว่าระบบ IT จะกลับสู่การให้บริการได้อย่างเป็นปกติ โดยมีเนื้อหาครอบคลุมถึงวันเวลา ประเภทเหตุการณ์ เหตุการณ์ ผลกระทบที่เกิดขึ้น และความคืบหน้าในการแก้ไขปัญหา ทั้งนี้ ให้รายงานผ่านช่องทางอิเล็กทรอนิกส์ที่สำนักงานกำหนด (3) รายงานเมื่อเหตุการณ์ยุติหรือแก้ไขปัญหาแล้วเสร็จ โดยมีเนื้อหาครอบคลุมถึงวันเวลา ประเภทเหตุการณ์ เหตุการณ์ ผลกระทบที่เกิดขึ้น การดำเนินการแก้ไขปัญหา ผลการแก้ไขปัญหา ระยะเวลาในการแก้ไข สาเหตุที่เกิดปัญหา และแนวทางป้องกันในอนาคต ทั้งนี้ ให้รายงานผ่านช่องทางอิเล็กทรอนิกส์ที่สำนักงานกำหนด
11.4 วิเคราะห์สาเหตุที่แท้จริง (root cause) ของเหตุการณ์ผิดปกติด้าน IT เพื่อหาแนวทางการแก้ไขจากสาเหตุที่แท้จริง	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. /25	แนวปฏิบัติ
และป้องกันไม่ให้เกิดเหตุการณ์ซ้ำในอนาคต	
11.5 บันทึกข้อมูลที่เกี่ยวข้องกับการบริหารจัดการเหตุการณ์ผิดปกติด้าน IT และปัญหาด้าน IT และจัดเก็บข้อมูลดังกล่าวเป็นระยะเวลาไม่น้อยกว่า 2 ปีนับแต่วันที่เกิดเหตุการณ์นั้น โดยต้องจัดเก็บไว้ในลักษณะที่พร้อมให้สำนักงานสามารถเรียกดูและตรวจสอบได้โดยไม่ชักช้า	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]
11.6 ทดสอบและทบทวนขั้นตอนปฏิบัติหรือแผนการบริหารจัดการเหตุการณ์ผิดปกติด้าน IT และปัญหาด้าน IT อย่างน้อยปีละ 1 ครั้ง โดยต้องครอบคลุมถึงการทดสอบการบริหารจัดการเหตุการณ์ด้านภัยคุกคามทางไซเบอร์ (cyber security drill) และจัดให้มีการรายงานผลการทดสอบและทบทวนต่อคณะกรรมการของผู้ประกอบธุรกิจหรือผู้ที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบธุรกิจ	ผู้ประกอบธุรกิจควรทดสอบและทบทวนขั้นตอนการบริหารจัดการเหตุการณ์ผิดปกติและปัญหาด้าน IT อย่างน้อยปีละ 1 ครั้ง เพื่อให้สามารถจัดการแก้ไขปัญหาให้กลับสู่สภาพปกติได้อย่างรวดเร็วและจำกัดความเสียหายที่ส่งผลกระทบต่อธุรกิจ โดยดำเนินการ ดังนี้ 1. จัดให้มีการจำลองสถานการณ์เสี่ยง (risk scenario) ด้านเหตุการณ์ภัยคุกคามทางไซเบอร์ที่มีความเป็นไปได้ที่จะเกิดขึ้น สอดคล้องกับลักษณะ ขอบเขต และความซับซ้อนในการประกอบธุรกิจ สอดคล้องกับแนวโน้มภัยคุกคามไซเบอร์ที่อาจเกิดขึ้นกับผู้ประกอบธุรกิจ โดยสถานการณ์ดังกล่าวควรเป็นสถานการณ์ที่เกิดขึ้นแล้วส่งผลกระทบต่อระบบ IT หรือทำให้เกิดการละเมิดความเป็นส่วนตัว (privacy) อย่างมีนัยสำคัญ 2. จัดเก็บเอกสารที่เกี่ยวข้องกับการทดสอบให้ครบถ้วนและเป็นปัจจุบัน ดังนี้ (1) สถานการณ์ความเสี่ยง (risk scenario) รูปแบบการทดสอบ วัน เวลา สถานที่ในการทดสอบ บทบาทหน้าที่ของผู้ที่เกี่ยวข้องที่ใช้ในการทดสอบ (2) สรุปผลการทดสอบ และผลการทบทวนขั้นตอนการบริหารจัดการเหตุการณ์ 3. จัดให้มีการรายงานผลการทดสอบและทบทวนต่อคณะกรรมการของผู้ประกอบธุรกิจหรือผู้ที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบธุรกิจ

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. /25	แนวปฏิบัติ
2.12 แผนฉุกเฉินด้าน IT (IT contingency plan)	
ส่วนที่ 12 แผนฉุกเฉินด้าน IT (IT contingency plan) ผู้ประกอบธุรกิจต้องจัดให้มีแผนฉุกเฉินด้าน IT อย่างเป็นลายลักษณ์อักษร โดยต้องได้รับความเห็นชอบจากคณะกรรมการของผู้ประกอบธุรกิจหรือผู้ที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบธุรกิจ เพื่อรองรับเหตุการณ์ผิดปกติด้าน IT ในกรณีที่ระบบ IT หยุดชะงัก ไม่สามารถให้บริการได้ตามปกติ หรือไม่สามารถดำเนินธุรกิจอย่างต่อเนื่อง โดยต้องกู้คืนระบบให้กลับคืนสู่สภาพปกติภายในระยะเวลาที่เหมาะสมได้ โดยแผนฉุกเฉินด้าน IT ต้องมีลักษณะดังนี้	
12.1 จัดให้มีคณะทำงานหรือหน่วยงานที่รับผิดชอบในการจัดทำแผนฉุกเฉินด้าน IT	ผู้ประกอบธุรกิจควรจัดให้มีคณะทำงานหรือหน่วยงานที่รับผิดชอบในการจัดทำแผนฉุกเฉินด้าน IT โดยมีผู้บริหารและบุคลากรของหน่วยงานด้านต่าง ๆ ที่เกี่ยวข้องเข้าร่วมด้วย เช่น ด้าน IT ด้านธุรกิจ และด้านสื่อสารองค์กร เป็นต้น
12.2 ประเมินความเสี่ยง (risk analysis) เพื่อให้สามารถระบุเหตุการณ์ความเสี่ยงที่อาจทำให้กระบวนการและระบบ IT หยุดชะงัก ไม่สามารถให้บริการได้ตามปกติ หรือไม่สามารถดำเนินธุรกิจอย่างต่อเนื่อง	กระบวนการจัดทำแผนฉุกเฉินด้าน IT ควรครอบคลุมการดำเนินการ ดังนี้ 1. การประเมินความเสี่ยง (risk analysis) เพื่อให้สามารถระบุเหตุการณ์ความเสี่ยงซึ่งส่งผลกระทบต่อการหยุดชะงักของกระบวนการและระบบ IT โดยมีแนวทางดำเนินการดังนี้ (1) ระบุเหตุการณ์ความเสี่ยง (risk scenarios) ที่อาจทำให้กระบวนการและระบบ IT หยุดชะงักทั้งจากภายในและภายนอก เช่น การโจมตีด้านไซเบอร์ ไฟไหม้ เป็นต้น (2) ประเมินความเสี่ยงโดยพิจารณาการควบคุมที่มีอยู่ รวมถึงผลกระทบและโอกาสที่จะเกิดขึ้น พร้อมทั้งกำหนดกระบวนการและทรัพยากรที่จะใช้ในการควบคุมความเสี่ยง (3) จัดทำแผนในการจัดการความเสี่ยง เพื่อปรับปรุงกระบวนการและจัดเตรียมทรัพยากรที่จำเป็นในการควบคุมความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ 2. การวิเคราะห์ผลกระทบทางธุรกิจ (business impact analysis) เพื่อให้ทราบถึงความสำคัญของระบบ IT ที่มีผลต่อการดำเนิน
12.3 วิเคราะห์ผลกระทบทางธุรกิจ (business impact analysis) จากเหตุการณ์ความเสี่ยงตาม 12.2 เพื่อกำหนดระยะเวลาเป้าหมายในการกู้คืนระบบ IT (Recovery Time Objective : RTO)ระยะเวลาเป้าหมายสูงสุดที่ยอมให้ข้อมูลเสียหาย (Recovery Point Objective : RPO) และระยะเวลาสูงสุดที่ยอมให้กระบวนการทางธุรกิจหยุดชะงัก (Maximum	

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. /25	แนวปฏิบัติ
Tolerable Downtime : MTD) อย่างเหมาะสม 12.4 จัดให้มีระบบ IT สำรอง และทรัพยากรที่จำเป็น เพื่อให้สามารถกู้คืนระบบได้ตามระยะเวลาเป้าหมายที่กำหนดไว้	ธุรกิจ โดยมีแนวทางการดำเนินการ ดังนี้ (1) ระบุรายการกระบวนการทางธุรกิจ (business process) ซึ่งพึ่งพาการใช้งานระบบ IT (2) วิเคราะห์ผลกระทบที่เกิดจากการหยุดชะงักของระบบ IT เพื่อกำหนดระยะเวลา RTO, RPO และ MTD ทั้งนี้ (ก) RTO ไม่ควรเกิน 2 ชั่วโมง สำหรับระบบ IT ที่สนับสนุนกระบวนการทางธุรกิจที่สำคัญของศูนย์ซื้อขายสัญญาซื้อขายล่วงหน้า สำนักหักบัญชีสัญญาซื้อขายล่วงหน้า สำนักหักบัญชีหลักทรัพย์ และศูนย์รับฝากหลักทรัพย์ (ข) RTO ไม่ควรเกิน 4 ชั่วโมง สำหรับระบบ IT ที่สนับสนุนกระบวนการทางธุรกิจที่สำคัญของผู้ประกอบธุรกิจอื่น ๆ กรณีที่ผู้ประกอบธุรกิจไม่สามารถกำหนด RTO ของระบบ IT ได้ตามที่กำหนดข้างต้น ผู้ประกอบธุรกิจสามารถใช้วิธีการให้บริการแบบ manual ทดแทนได้ โดยวิธีการดังกล่าวต้องไม่ส่งผลต่อประสิทธิภาพการให้บริการอย่างมีนัยสำคัญ (3) ระบุระบบ IT และทรัพยากรที่จำเป็นต่อกระบวนทางธุรกิจที่สำคัญ (ฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูล และทรัพยากรอื่น ๆ) พร้อมทั้งรายละเอียดคุณสมบัติ (specification) ขั้นต่ำของระบบ IT และทรัพยากรดังกล่าว (3) จัดลำดับความสำคัญของระบบ IT เพื่อให้ระบบ IT ที่สนับสนุนกระบวนการทางธุรกิจที่สำคัญสูงได้รับการกู้คืนเป็นลำดับแรก 3. จัดทำแผนฉุกเฉินด้าน IT ที่ระบุกระบวนการหรือขั้นตอนการปฏิบัติงานที่ชัดเจน เพื่อให้สามาถดำเนินการได้อย่างรวดเร็วและง่ายต่อการปฏิบัติอย่างน้อยครอบคลุม (1) หน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องในการดำเนินการตามแผน (2) รายละเอียดของระบบ IT เช่น โครงสร้างสถาปัตยกรรม แผนภาพแสดงระบบเครือข่ายสื่อสาร เป็นต้น (3) เงื่อนไขและขั้นตอนในการประกาศใช้แผนฉุกเฉินด้าน IT และการสื่อสารให้ผู้ที่เกี่ยวข้องรับทราบ (4) ขั้นตอนการกู้คืนระบบ IT และข้อมูลอย่างละเอียด ชัดเจนและเพียงพอที่ผู้ปฏิบัติงานสามารถใช้เป็นขั้นตอนปฏิบัติได้อย่างถูกต้อง และเป็นไปตามเป้าหมายเวลาที่กำหนดไว้ โดยอาจจัดทำในรูปแบบรายการตรวจสอบขั้นตอนปฏิบัติ (checklist) (5) ขั้นตอนการตรวจสอบความถูกต้องครบถ้วนของระบบ IT และข้อมูลที่กู้คืน ก่อนกลับสู่การดำเนินกระบวนการทางธุรกิจอย่างปกติ (return to normal) (6) ขั้นตอนในการประกาศยกเลิกแผนฉุกเฉินด้าน IT

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. /25	แนวปฏิบัติ
	(7) การจัดเก็บแผนฉุกเฉินด้าน IT ไว้ในสถานที่ปลอดภัยและมีความพร้อมใช้งานในสถานที่ปฏิบัติงานหลักและสถานที่สำรอง 4. จัดให้มีระบบ IT สำรอง และทรัพยากรที่จำเป็นเพื่อให้สามารถกู้คืนระบบ IT ได้ตามระยะเวลาเป้าหมายที่กำหนดไว้ กรณีที่ผู้ประกอบธุรกิจมีศูนย์คอมพิวเตอร์สำรอง ควรระบุรายละเอียดเกี่ยวกับศูนย์คอมพิวเตอร์สำรองให้ชัดเจน เช่น สถานที่ตั้ง แผนที่ เป็นต้น
12.5 สื่อสารให้บุคลากรที่เกี่ยวข้องมีความเข้าใจและสามารถปฏิบัติตามแผนฉุกเฉินด้าน IT อย่างเหมาะสม	ผู้ประกอบธุรกิจควรสื่อสารแผนฉุกเฉินด้าน IT ให้พนักงานทุกคนที่มีส่วนเกี่ยวข้องกับการปฏิบัติตามแผนฉุกเฉินด้าน IT มีความเข้าใจและสามารถปฏิบัติตามแผนได้อย่างถูกต้อง
12.6 ทบทวนและทดสอบการปฏิบัติตามแผนฉุกเฉินด้าน IT อย่างน้อยปีละ 1 ครั้ง และเมื่อมีเหตุจำเป็นที่ควรได้รับการทบทวนและทดสอบดังกล่าว โดยรายงานผลการทบทวนและทดสอบต่อคณะกรรมการของผู้ประกอบธุรกิจหรือผู้ที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบธุรกิจ	1. ผู้ประกอบธุรกิจควรทดสอบและทบทวนการปฏิบัติตามแผนฉุกเฉินด้าน IT อย่างน้อยปีละ 1 ครั้ง และเมื่อมีเหตุจำเป็นที่ควรได้รับการทดสอบและทบทวนดังกล่าว เพื่อให้แน่ใจว่าแผนยังคงมีประสิทธิภาพเมื่อต้องรับมือกับเหตุการณ์ผิดปกติ 2. ผู้ประกอบธุรกิจควรกำหนดเหตุการณ์ที่ใช้ในการทดสอบประจำปี (test scenario) โดยเป็นเหตุการณ์ที่มีโอกาสที่จะเกิดขึ้นและอาจส่งผลกระทบให้กระบวนการทางธุรกิจที่สำคัญหยุดชะงัก เช่น การหยุดชะงักของระบบ IT ที่สนับสนุนกระบวนการทางธุรกิจที่สำคัญ การหยุดชะงักของผู้ให้บริการภายนอกที่สำคัญ (รวมถึงผู้ให้บริการคลาวด์) และการโจมตีทางไซเบอร์ เป็นต้น 3. ผู้ประกอบธุรกิจควรรายงานผลการทดสอบแผนฉุกเฉินด้าน IT ต่อคณะกรรมการของผู้ประกอบธุรกิจหรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบธุรกิจ โดยมีรายละเอียดอย่างน้อยครอบคลุมถึง วัตถุประสงค์ ขอบเขตการทดสอบ สถานการณ์จำลอง ระยะเวลาที่ใช้ในการกู้คืนระบบเทียบกับเป้าหมายที่กำหนด ข้อผิดพลาดและปัญหาหรืออุปสรรคที่พบ พร้อมทั้งแนวทางปรับปรุงแก้ไข 4. *[ความเสี่ยงสูง] ผู้ประกอบธุรกิจควรมีการทดสอบแผนการรับมือเหตุการณ์ โดยครอบคลุมการทดสอบการโอนย้ายกระบวนการทางธุรกิจ หรือ การโอนย้ายการประมวลผลไปยังศูนย์ประมวลผลสำรอง โดยจำกัดความเสียหายหรือการหยุดชะงักของระบบให้บริการ และการสูญหายของข้อมูล*
12.7 กำหนดกระบวนการดำเนินงาน เพื่อรับมือเหตุการณ์การใช้ทรัพยากรด้าน IT หรือการใช้ประสิทธิภาพของระบบงานเกินขีดจำกัดของตัวชี้วัดที่กำหนดไว้ เช่น การจำกัดการให้บริการบางช่องทาง หรือตัดการเชื่อมต่อกับผู้ให้บริการ	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. /25	แนวปฏิบัติ
หรือบุคคลภายนอกที่มีผลกระทบต่อระบบ IT เป็นต้น	
12.8 จัดให้มีรายละเอียดในการติดต่อดังนี้ เพื่อให้สามารถประสานงานในการรายงานเหตุการณ์ผิดปกติด้าน IT หรือขอความช่วยเหลือจากหน่วยงานภายนอกที่เกี่ยวข้องได้อย่างมีประสิทธิภาพ โดยต้องปรับปรุงข้อมูลดังกล่าวให้เป็นปัจจุบันอยู่เสมอ 12.8.1 รายชื่อหน่วยงานกำกับดูแลและบุคคลภายนอกที่ให้บริการหรือที่มีการเชื่อมต่อกับระบบ IT ของผู้ประกอบธุรกิจ 12.8.2 ช่องทางในการติดต่อ และรายชื่อผู้ที่เกี่ยวข้องของหน่วยงานกำกับดูแลหรือบุคคลภายนอกตาม 12.8.1	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]

หมวด 3 การตรวจสอบด้านเทคโนโลยีสารสนเทศ (Information Technology Audit)

การตรวจสอบด้านเทคโนโลยีสารสนเทศ (Information Technology Audit) ให้ผู้ประกอบธุรกิจดำเนินการตามที่กำหนดในภาคผนวกนี้

ข้อกำหนดในภาคผนวก 3 **แนบท้ายประกาศที่ สธ. /25**	**แนวปฏิบัติ**
1. <u>การจัดให้มีผู้ตรวจสอบ</u> ผู้ตรวจสอบตาม 1. ต้องมีลักษณะดังนี้ 1.1 ผ่านการรับรองและมีวุฒิบัตรอย่างหนึ่งอย่างใดดังนี้ 1.1.1 Certified Information Systems Auditor (CISA) 1.1.2 Certified Information Security Manager (CISM) 1.1.3 Certified Information Systems Security Professional (CISSP) 1.1.4 ISO/IEC 27001 Lead Auditor 1.1.5 ใบรับรองอื่นตามที่กำหนดเพิ่มเติมบนเว็บไซต์ของสำนักงาน 1.2 มีความเป็นอิสระจากผู้ทำหน้าที่ด้าน IT ในระดับ ดังนี้ 1.2.1 ระดับที่ 1 (first line of defense) : การปฏิบัติงาน 1.2.2 ระดับที่ 2 (second line of defense) : การบริหารความเสี่ยงและกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]
2. <u>การวางแผนและกำหนดขอบเขตการตรวจสอบ</u> ทบทวนแผนงานและขอบเขตการตรวจสอบให้สอดคล้องกับความเสี่ยงด้าน IT และประกาศที่ สธ..... โดยต้องดำเนินการอย่างน้อยปีละ 1 ครั้ง และเมื่อมีเหตุจำเป็นที่ควรได้รับการทบทวนดังกล่าว	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]
3. <u>การตรวจสอบด้าน IT ตามแผนงานและขอบเขตที่กำหนด</u> จัดให้มีการตรวจสอบและรายงานผลการตรวจสอบด้าน IT อย่างน้อยปีละ 1 ครั้ง โดยมีรายละเอียดดังนี้ 3.1 กรณีเป็นผู้ประกอบธุรกิจที่มีความเสี่ยงระดับต่ำ ต้องจัดให้มีการตรวจสอบด้าน IT อย่างน้อยปีละ 1 ครั้ง โดยเป็นการตรวจสอบแบบเต็มรูปแบบ (full scope) ที่ครอบคลุมหลักเกณฑ์ครบถ้วนทุกหัวข้อการควบคุมอย่างน้อยทุก 2 ปี 3.2 กรณีเป็นผู้ประกอบธุรกิจที่มีความเสี่ยงระดับปานกลางหรือหรือระดับสูง ต้องจัดให้มีการตรวจสอบด้าน IT แบบเต็มรูปแบบ (full scope) ที่ครอบคลุมหลักเกณฑ์ครบถ้วนทุกหัวข้อการควบคุม อย่างน้อยปีละ 1 ครั้ง	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. /25	แนวปฏิบัติ
3.3 กรณีเป็นผู้ประกอบธุรกิจขนาดเล็ก ต้องจัดให้มีการตรวจสอบด้าน IT อย่างน้อยปีละ 1 ครั้ง โดยเป็นการตรวจสอบตามการรักษาความมั่นคงปลอดภัยของระบบ IT ขั้นต้นที่จำเป็นที่ครอบคลุมหลักเกณฑ์ครบถ้วนทุกหัวข้อการควบคุมอย่างน้อยทุก 2 ปี	
4. <u>จัดให้มีแผนการปรับปรุง แก้ไขข้อบกพร่องจากการตรวจสอบ และการติดตามความคืบหน้า</u> จัดให้มีแผนการปรับปรุงแก้ไขข้อบกพร่องที่พบจากการตรวจสอบด้าน IT ตาม 3. และติดตามความคืบหน้าในการดำเนินการตามแผนดังกล่าวโดยไม่ชักช้า	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]
5. <u>การจัดทำและรายงานผลการตรวจสอบ</u> 5.1 เสนอรายงานผลการตรวจสอบตาม 3. และแผนการปรับปรุงแก้ไขข้อบกพร่องต่อจากคณะกรรมการของผู้ประกอบธุรกิจหรือคณะกรรมการตรวจสอบของผู้ประกอบธุรกิจโดยไม่ชักช้า 5.2 รายงานผลการตรวจสอบและแผนการปรับปรุงแก้ไขข้อบกพร่อง ที่ผ่านการพิจารณาจากคณะกรรมการของผู้ประกอบธุรกิจหรือคณะกรรมการตรวจสอบของผู้ประกอบธุรกิจตาม 5.1 พร้อมทั้งเอกสารรับรองผลการพิจารณาดังกล่าว ต่อสำนักงานตามรูปแบบและวิธีการที่กำหนดไว้บนเว็บไซต์ของสำนักงาน ภายใน 30 วันนับแต่วันที่เสนอรายงานและแผนดังกล่าวต่อคณะกรรมการของผู้ประกอบธุรกิจหรือคณะกรรมการตรวจสอบของผู้ประกอบธุรกิจ แต่ต้องไม่เกินกว่าระยะเวลาดังนี้ แล้วแต่ระยะเวลาใดจะครบกำหนดก่อน 5.2.1 90 วันนับแต่วันที่สิ้นสุดการตรวจสอบตาม 3. 5.2.2 3 เดือนนับแต่วันสิ้นปีปฏิทินของปีที่เริ่มตรวจสอบตาม 3. กรณีที่ไม่สามารถจัดทำรายงานผลการตรวจสอบให้เสร็จสิ้นภายในปีที่เริ่มการ 5.3 จัดเก็บรายงานผลการตรวจสอบและแผนการปรับปรุงแก้ไขข้อบกพร่องเป็นระยะเวลาไม่น้อยกว่า 2 ปีนับแต่วันที่จัดทำรายงานและแผนดังกล่าว โดยต้องจัดเก็บไว้ในลักษณะที่พร้อมให้สำนักงานสามารถเรียกดูและตรวจสอบได้โดยไม่ชักช้า	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]