ขอบเขตการดำเนินการ:

1. ผู้ประกอบธุรกิจที่มีความเสี่ยงระดับสูง ให้ดำเนินการตามแนวปฏิบัตินี้ครบทุกข้อ
2. ผู้ประกอบธุรกิจที่มีความเสี่ยงระดับต่ำ หรือระดับปานกลาง ให้ดำเนินการตามแนวปฏิบัตินี้ทุกข้อ ยกเว้นข้อที่ระบุว่า *"[ความเสี่ยงสูง]"*
3. ผู้ประกอบธุรกิจที่มีขนาดเล็ก ให้ดำเนินการตามแนวปฏิบัติขั้นต้น อย่างน้อยในเรื่องดังนี้

สารบัญ

หน้า

หมวดที่ 1 การกำกับดูแลและบริหารจัดการด้านเทคโนโลยีสารสนเทศ (Information Technology Governance)

ข้อกำหนดในภาคผนวก 2 แนบท้ายประกาศที่ สธ. 38/2565	แนวปฏิบัติ
1.1 บทบาทหน้าที่และความรับผิดชอบของคณะกรรมการของผู้ประกอบธุรกิจ	
ส่วนที่ 1 บทบาทหน้าที่และความรับผิดชอบของคณะกรรมการของผู้ประกอบธุรกิจ ผู้ประกอบธุรกิจต้องดำเนินการให้การควบคุมดูแลและบริหารจัดการความเสี่ยงด้าน IT ผ่านการกำกับดูแลโดยคณะกรรมการของผู้ประกอบธุรกิจ เพื่อให้สอดคล้องกับระดับความเสี่ยงที่องค์กรยอมรับได้ โดยคำนึงถึงการบริหารและจัดการความเสี่ยงขององค์กร (enterprise risk) (ถ้ามี) ซึ่งอย่างน้อยต้องครอบคลุมในเรื่องดังนี้	
1.1 การกำหนดกรอบการกำกับดูแลด้าน IT (IT governance framework) และการกำกับดูแลแผนงานด้าน IT ให้สอดคล้องกับแผนทางธุรกิจ และมีความเหมาะสมเพียงพอที่จะรองรับการเปลี่ยนแปลงด้าน IT และการเปลี่ยนแปลงการดำเนินธุรกิจในอนาคต	1. ผู้ประกอบธุรกิจควรกำหนดกรอบการกำกับดูแลด้าน IT (IT governance framework) ที่ครอบคลุมรายละเอียด ดังนี้ (1) โครงสร้างการกำกับดูแล บทบาทหน้าที่และความรับผิดชอบของคณะกรรมการของผู้ประกอบธุรกิจ ผู้บริหาร และฝ่ายงานที่เกี่ยวข้อง (2) กระบวนการที่เกี่ยวข้องกับการกำกับดูแลด้าน IT เช่น การจัดทำและขออนุมัติแผนงานด้าน IT การจัดทำแผนและและการบริหารจัดการทรัพยากรด้าน IT และการติดตามและรายงานผลการดำเนินการด้าน IT เป็นต้น 2. ผู้ประกอบธุรกิจควรจัดให้มีแผนงานด้าน IT ประจำปี เพื่อให้การใช้ IT สอดรับกับกลยุทธ์ในการดำเนินธุรกิจ
1.2 การจัดสรรทรัพยากรทางด้าน IT และทรัพยากรบุคคลที่ปฏิบัติงานด้าน IT ให้มีความเหมาะสมเพียงพอต่อการดำเนินธุรกิจ	1. ผู้ประกอบธุรกิจควรจัดสรรทรัพยากรทางด้าน IT และทรัพยากรบุคคลที่ปฏิบัติงานด้าน IT ให้สอดคล้องกับเป้าหมายตามภารกิจ กลยุทธ์ นโยบาย และแผนการดำเนินงานที่กำหนดไว้
1.3 การกำหนดนโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้าน IT ซึ่งมีการกำหนดเป็นลายลักษณ์อักษร โดยอย่างน้อยต้องครอบคลุมนโยบายตามที่กำหนดในส่วนที่ 2 ข้อ 2.2	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]
1.4 การกำหนดขั้นตอนและวิธีปฏิบัติงานในการบริหารจัดการความเสี่ยงด้าน IT และการรักษาความมั่นคงปลอดภัยด้าน IT เพื่อให้	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]

ข้อกำหนดในภาคผนวก 2 แนบท้ายประกาศที่ สธ. 38/2565	แนวปฏิบัติ
เป็นไปตามนโยบายใน 1.3 รวมถึงกำกับดูแลให้มีการนำไปปฏิบัติอย่างเหมาะสม	
1.5 การสร้างความรู้และความตระหนักด้านความเสี่ยงด้าน IT แก่กรรมการและบุคลากรอย่างต่อเนื่องและมีประสิทธิผล	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]
1.6 การติดตาม ตรวจสอบ และรายงานผลการปฏิบัติงานเพื่อให้เป็นไปตามนโยบายในข้อ 1.3 ต่อคณะกรรมการของผู้ประกอบธุรกิจ โดยมีการรายงานอย่างน้อยปีละ 1 ครั้ง และในกรณีที่มีเหตุการณ์หรือการเปลี่ยนแปลงใด ๆ ซึ่งอาจส่งผลกระทบอย่างมีนัยสำคัญต่อการปฏิบัติงานเพื่อให้เป็นไปตามนโยบายดังกล่าว ต้องมีการรายงานให้คณะกรรมการของผู้ประกอบธุรกิจทราบโดยไม่ชักช้าด้วย	1. ผู้ประกอบธุรกิจควรจัดให้มีกระบวนการติดตาม ตรวจสอบ และควบคุมการจัดทำรายงานผลการปฏิบัติงานเพื่อให้มั่นใจว่าสามารถจัดทำรายงานได้อย่างครบถ้วนถูกต้อง 2. ผู้ประกอบธุรกิจควรกำหนดให้การรายงานผลการปฏิบัติตามนโยบายที่เกี่ยวข้องกับการกำกับดูแลและบริหาร จัดการความเสี่ยงด้าน IT ต่อคณะกรรมการของผู้ประกอบธุรกิจ มีเนื้อหาครอบคลุมถึงเรื่อง ดังนี้ (1) ผลการบริหารจัดการความเสี่ยงด้าน IT โดยหน่วยงานที่ทำหน้าที่บริหารความเสี่ยงด้าน IT หรือหน่วยงานที่เกี่ยวข้อง (2) ผลการปฏิบัติตามกฎระเบียบ ข้อบังคับ หรือนโยบายการรักษาความมั่นคงปลอดภัยด้าน IT ในภาพรวมขององค์กร โดยหน่วยงานที่ทำหน้าที่กำกับดูแลการปฏิบัติงานด้าน IT หรือหน่วยงานที่เกี่ยวข้อง (3) ผลการตรวจสอบด้าน IT (IT audit) และความคืบหน้าในการดำเนินการแก้ไขข้อบกพร่อง โดยหน่วยงานที่ทำหน้าที่ตรวจสอบด้าน IT หรือหน่วยงานที่เกี่ยวข้อง (4) ผลการปฏิบัติงานด้าน IT ที่สำคัญ เช่น (ก) เหตุการณ์ผิดปกติ หรือปัญหาด้าน IT ที่สำคัญ (ข) ความเพียงพอของทรัพยากรด้าน IT (capacity and system utilization) (ค) ความคืบหน้าของโครงการด้าน IT ในภาพรวมและโครงการที่สำคัญ (ง) การปฏิบัติงานด้าน IT ของบุคคลภายนอก เช่น ผลการดำเนินการตามข้อตกลงการให้บริการ (service level agreement) เป็นต้น (จ) ผลการทดสอบการปฏิบัติตามแผนฉุกเฉินด้าน IT และการใช้งานแผน (ถ้ามี)

ข้อกำหนดในภาคผนวก 2 แนบท้ายประกาศที่ สธ. 38/2565	แนวปฏิบัติ
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 (segregation of duties) อย่างเหมาะสม ตามหลักการแบ่งแยกหน้าที่ 3 ระดับ (3 LoDs) ได้แก่ (1) การปฏิบัติงาน (first line of defense) หมายถึง หน่วยงานปฏิบัติงานด้าน IT และผู้ที่ใช้ระบบ IT ปฏิบัติงาน (ก) หน่วยงานปฏิบัติงานด้าน IT มีหน้าที่ปฏิบัติงานตามหน้าที่ความรับผิดชอบ ประเมินความเสี่ยงและควบคุมความเสี่ยงด้าน IT ติดตามและรายงานการปฏิบัติงานด้าน IT ต่อคณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมาย (ข) ผู้ที่ใช้ระบบ IT ปฏิบัติงาน มีหน้าที่ปฏิบัติตามนโยบายและระเบียบปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้าน IT รวมทั้งมีส่วนร่วมรับผิดชอบในการประเมินและจัดการความเสี่ยงด้าน IT ที่เกี่ยวข้องกับการใช้งานระบบ (2) การบริหารความเสี่ยงและกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องในการปฏิบัติงานด้าน IT (second line of defense) หมายถึง หน่วยงานบริหารความเสี่ยงด้าน IT และหน่วยงานกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ด้าน IT (ก) หน่วยงานบริหารความเสี่ยงด้าน IT (IT risk function) มีหน้าที่กำหนดกรอบนโยบาย และกระบวนการบริหารความเสี่ยงด้าน IT สนับสนุนให้มีการประเมินความเสี่ยงเป็นไปตามกรอบการบริหารความเสี่ยงที่กำหนด พร้อมทั้งให้คำปรึกษา ติดตามความเสี่ยง และทบทวนการควบคุมความเสี่ยงด้าน IT ให้อยู่ในระดับความเสี่ยงที่ยอมรับได้ โดยมีการรวบรวมและเชื่อมโยงความเสี่ยงด้าน IT กับความเสี่ยงด้านอื่น และนำเสนอผลการบริหารความเสี่ยงต่อคณะกรรมการที่ทำหน้าที่กำกับดูแลความเสี่ยง (ข) หน่วยงานกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ด้าน IT (IT compliance function) มีหน้าที่ใน

ข้อกำหนดในภาคผนวก 2 แนบท้ายประกาศที่ สธ. 38/2565	แนวปฏิบัติ
	การกำกับดูแลให้มีการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง รวมถึงติดตาม ให้คำปรึกษา และสอบทานด้านการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง (3) การตรวจสอบด้าน IT (third line of defense) หมายถึง หน่วยงานตรวจสอบด้าน IT ซึ่งมีหน้าที่ในการตรวจสอบการปฏิบัติงานของหน่วยงานที่ทำหน้าที่ first line และ second line of defense เพื่อให้มั่นใจว่ามีการปฏิบัติตามนโยบาย มาตรฐาน และกฎหมายทางด้าน IT ที่เกี่ยวข้อง หน่วยงานในระดับนี้อาจเป็นผู้ตรวจสอบภายใน หรือผู้ตรวจสอบภายนอกที่มีความเป็นอิสระจากหน่วยงานที่ทำหน้าที่ first line และ second line of defense 2. *[ความเสี่ยงสูง] ผู้ประกอบธุรกิจควรจัดให้มีกรรมการของผู้ประกอบธุรกิจ หรือที่ปรึกษาของผู้ประกอบธุรกิจ อย่างน้อย 1 ท่าน ที่มีความรู้หรือประสบการณ์ด้าน IT เพื่อให้คณะกรรมการของผู้ประกอบธุรกิจสามารถกำหนดทิศทางและกำกับดูแลให้มีการใช้ IT สอดรับกับกลยุทธ์ในการดำเนินธุรกิจ ทั้งนี้ ผู้ประกอบธุรกิจสามารถพิจารณาคุณสมบัติของกรรมการหรือที่ปรึกษาที่มีความรู้หรือประสบการณ์ด้าน IT ได้จากเรื่องดังนี้ โดยผู้ประกอบธุรกิจอาจใช้เกณฑ์ด้านอื่นในการพิจารณาตามความเหมาะสม* *(1) จบการศึกษาในสาขา IT หรือสาขาที่เกี่ยวข้อง หรือ* *(2) มีประสบการณ์ในตำแหน่งหัวหน้าหน่วยงานด้าน IT หรือมีหน้าที่รับผิดชอบเป็นผู้บริหารงานที่เกี่ยวข้องกับด้าน IT หรือมีประสบการณ์ในการให้คำปรึกษาที่เกี่ยวข้องด้าน IT หรือ* *(3) มีประสบการณ์หรือได้รับแต่งตั้งเป็นสมาชิกในคณะกรรมการหรือคณะทำงานที่เกี่ยวข้องด้าน IT* *กรณีที่คณะกรรมการของผู้ประกอบธุรกิจแต่งตั้งคณะกรรมการชุดย่อยเพื่อทำหน้าที่ให้คำปรึกษาด้าน IT แก่คณะกรรมการของผู้ประกอบธุรกิจ ผู้ประกอบธุรกิจควรกำหนดบทบาทหน้าที่คณะกรรมการชุดย่อยอย่างชัดเจนและเป็นลายลักษณ์อักษร โดยคณะกรรมการชุดย่อยควรประกอบด้วยกรรมการที่มีความรู้หรือประสบการณ์ด้าน IT อย่างน้อย 1 ท่าน* 3. *[ความเสี่ยงสูง] ผู้ประกอบธุรกิจควรจัดให้มีผู้บริหารระดับสูง (chief information security officer : CISO) หรือผู้บริหารที่รับผิดชอบในการบริหารจัดการความมั่นคงปลอดภัยด้าน IT อย่างน้อย 1 ท่าน โดยมีคุณสมบัติ ขอบเขตอำนาจ และหน้าที่อย่างน้อย ดังนี้* *(1) มีความเป็นอิสระจากหน่วยงานที่ทำหน้าที่ปฏิบัติงานด้าน IT (IT operation) และงานด้านพัฒนาระบบ IT (IT*

ข้อกำหนดในภาคผนวก 2 แนบท้ายประกาศที่ สธ. 38/2565	แนวปฏิบัติ
	development) สอดคล้องตามหลักการถ่วงดุล (check and balance) ที่ดี *(2) เป็นผู้ที่มีความรู้ความสามารถหรือมีประสบการณ์ด้าน IT และด้านการบริหารจัดการความมั่นคงปลอดภัยด้าน IT* *(3) มีอำนาจหน้าที่ (authority) เพียงพอในการปฏิบัติหน้าที่ได้อย่างมีประสิทธิภาพและประสิทธิผล โดยสามารถดำเนินการอย่างน้อย ดังนี้* *(ก) รายงานปัญหาหรือเหตุการณ์ที่มีนัยสำคัญซึ่งกระทบต่อความมั่นคงปลอดภัยด้าน IT ต่อผู้บริหารในตำแหน่งสูงสุดขององค์กร และคณะกรรมการที่เกี่ยวข้องโดยตรง* *(ข) ให้ความคิดเห็นในเรื่องภัยคุกคามทางไซเบอร์และการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยด้าน IT ต่อคณะกรรมการของผู้ประกอบธุรกิจ หรือคณะกรรมการที่เกี่ยวข้องกับการบริหารจัดการและกำกับดูแลการปฏิบัติงานด้าน IT เช่น IT steering committee หรือ IT risk committee เป็นต้น และร่วมตัดสินใจดำเนินการในเรื่องความมั่นคงปลอดภัยด้าน IT และภัยคุกคามทางไซเบอร์ที่มีผลกระทบอย่างมีนัยสำคัญ* 4. *[ความเสี่ยงสูง] คณะกรรมการของผู้ประกอบธุรกิจอาจแต่งตั้งคณะกรรมการเพื่อทำหน้าที่ที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้าน IT เช่น* *(1) คณะกรรมการกำกับดูแลและบริหารจัดการงานด้าน IT (เช่น IT steering committee หรือคณะกรรมการที่ได้รับมอบหมาย เป็นต้น) เพื่อดูแลให้มีการกำหนดกลยุทธ์ นโยบาย และแผนงานด้าน IT ที่สอดคล้องกับกลยุทธ์ของผู้ประกอบธุรกิจ* *(2) คณะกรรมการกำกับดูแลการบริหารความเสี่ยงด้าน IT (เช่น คณะกรรมการบริหารความเสี่ยง หรือคณะกรรมการที่ได้รับมอบหมาย เป็นต้น) เพื่อดูแลให้มีการกำหนดนโยบายการบริหารความเสี่ยงด้าน IT กำกับดูแลและติดตามให้เป็นไปตามนโยบายที่กำหนดไว้ รวมทั้งกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับ IT* *(3) คณะกรรมการกำกับดูแลการตรวจสอบด้าน IT (เช่น คณะกรรมการตรวจสอบ หรือคณะกรรมการที่ได้รับมอบหมาย เป็นต้น) เพื่อให้ผู้ประกอบธุรกิจมีการตรวจสอบด้าน IT อย่างเป็นอิสระ ครอบคลุมถึงการปฏิบัติงาน การบริหารความเสี่ยงด้าน IT และการกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับ IT*

ข้อกำหนดในภาคผนวก 2 แนบท้ายประกาศที่ สธ. 38/2565	แนวปฏิบัติ
1.3 นโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้าน IT	
2.2 ผู้ประกอบธุรกิจต้องจัดให้มีนโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้าน IT เป็นลายลักษณ์อักษร โดยต้องได้รับความเห็นชอบจากคณะกรรมการของผู้ประกอบธุรกิจหรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบธุรกิจ ดังนี้	
2.2.1 <u>นโยบายการบริหารจัดการความเสี่ยงด้าน IT (IT risk management policy)</u> มีเรื่องที่ต้องครอบคลุม ดังนี้ (1) บทบาทหน้าที่ของผู้ที่เกี่ยวข้องในการบริหารจัดการความเสี่ยงด้าน IT (2) การจัดให้มีกระบวนการบริหารจัดการความเสี่ยงด้าน IT เพื่อให้อยู่ในระดับที่องค์กรยอมรับได้	กระบวนการบริหารจัดการความเสี่ยงด้าน IT ควรมีรายละเอียด ดังนี้ 1. เกณฑ์ความเสี่ยง (risk criteria) ควรครอบคลุมถึงโอกาสหรือความถี่ที่จะเกิดเหตุการณ์ความเสี่ยง และความมีนัยสำคัญหรือผลกระทบที่จะเกิดขึ้นเพื่อจัดลำดับความสำคัญในการบริหารจัดการความเสี่ยง 2. ระดับความเสี่ยงที่ยอมรับได้ (IT risk appetite) ควรผ่านการพิจารณาโดยคณะกรรมการบริหารความเสี่ยง (ถ้ามี) และได้รับการอนุมัติจากคณะกรรมการของผู้ประกอบธุรกิจ ทั้งนี้ ระดับความเสี่ยงที่ยอมรับได้ควรสอดคล้องกับการบริหารและจัดการความเสี่ยงขององค์กร (enterprise risk management) (ถ้ามี) 3. การประเมินความเสี่ยง (risk assessment) ควรมีการประเมินความเสี่ยงอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงระบบ IT อย่างมีนัยสำคัญ โดยมีกระบวนการครอบคลุมอย่างน้อย ดังนี้ (1) การระบุความเสี่ยง (risk identification) จัดให้มีการระบุเหตุการณ์ความเสี่ยง (risk scenario) ด้าน IT ที่อาจจะเกิดขึ้นหรือที่เคยเกิดขึ้นจริงกับผู้ประกอบธุรกิจเอง หรือเกิดกับผู้อื่นที่ใช้งานเทคโนโลยีในลักษณะเดียวกัน รวมถึงภัยคุกคามทางไซเบอร์และช่องโหว่ต่าง ๆ ที่ส่งผลกระทบต่อการดำเนินธุรกิจ โดยเหตุการณ์ความเสี่ยงดังกล่าวอาจมีสาเหตุมาจากปัจจัยภายใน (internal factor) เช่น กระบวนการปฏิบัติงาน ระบบงาน บุคลากร เป็นต้น รวมถึงปัจจัยภายนอกอื่น ๆ (external factor) เช่น การปฏิบัติตามกฎหมาย การใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก เป็นต้น (2) การวิเคราะห์ความเสี่ยง (risk analysis) จัดให้มีการวิเคราะห์ความเสี่ยงด้าน IT เพื่อหาแนวทางในการจัดการความเสี่ยงอย่างเหมาะสม โดยครอบคลุม

ข้อกำหนดในภาคผนวก 2 แนบท้ายประกาศที่ สธ. 38/2565	แนวปฏิบัติ
	การดำเนินการอย่างน้อย ดังนี้ (ก) กำหนดผู้รับผิดชอบต่อความเสี่ยง หรือเจ้าของความเสี่ยง (risk owner) (ข) ระบุการควบคุมที่มีอยู่ในปัจจุบัน (existing control) (ค) วิเคราะห์โอกาสหรือความถี่ที่จะเกิดเหตุการณ์ความเสี่ยง (likelihood) และความมีนัยสำคัญหรือผลกระทบที่จะเกิดขึ้น (potential impact) จากเหตุการณ์ดังกล่าว (3) การประเมินค่าความเสี่ยง (risk evaluation) จัดให้มีประเมินค่าความเสี่ยงด้าน IT เพื่อจัดลำดับในการบริหารความเสี่ยงอย่างเหมาะสม โดยครอบคลุมการดำเนินการอย่างน้อย ดังนี้ (ก) ประเมินผลลัพธ์ที่ได้จากการวิเคราะห์ความเสี่ยง ได้แก่ ค่าโอกาสและผลกระทบ (likelihood และ potential impact) กับเกณฑ์ความเสี่ยง (risk criteria) ที่กำหนดไว้ เพื่อระบุระดับค่าความเสี่ยงของแต่ละเหตุการณ์ความเสี่ยงด้าน IT (ข) จัดลำดับความเสี่ยงด้าน IT 4. *[ความเสี่ยงสูง] ผู้ประกอบธุรกิจควรมีการประเมินความเสี่ยงด้าน IT ให้เท่าทันต่อการเปลี่ยนแปลงความเสี่ยงขององค์กร (company risk profile) อันอาจจะเกิดจากปัจจัยทั้งภายในและภายนอกองค์กร เช่น การออกผลิตภัณฑ์ใหม่ การเปลี่ยนแปลงมาตรฐานและข้อกำหนดทางด้าน IT ในอุตสาหกรรม หรือการตรวจพบหรือมีข้อบ่งชี้ด้านความเสี่ยงทางเทคโนโลยีใหม่เกิดขึ้น เป็นต้น* 5. การจัดการความเสี่ยง (risk treatment) ควรกำหนดให้มีแนวทางในการจัดการความเสี่ยงด้าน IT อย่างเหมาะสมและสอดคล้องกับผลการประเมินความเสี่ยง (risk assessment) เพื่อให้ความเสี่ยงที่เหลืออยู่ (residual risk) อยู่ในระดับความเสี่ยงที่ยอมรับได้ (risk appetite) โดยครอบคลุมการดำเนินการอย่างน้อย ดังนี้ (1) การกำหนดแนวทางในการจัดการความเสี่ยง โดยพิจารณาถึงความคุ้มค่าและวิธีการที่เหมาะสมกับผู้ประกอบธุรกิจ เช่น การหยุดหรือหลีกเลี่ยงความเสี่ยง (risk avoidance) การลดหรือบรรเทาความเสี่ยง (risk mitigation) การโอนย้ายความเสี่ยงให้กับผู้อื่น (risk transference) และการยอมรับความเสี่ยงโดยการเสนอเหตุผลผู้บริหารเพื่อ

ข้อกำหนดในภาคผนวก 2 แนบท้ายประกาศที่ สธ. 38/2565	แนวปฏิบัติ
	ตัดสินใจ (risk acceptance) เป็นต้น (2) การระบุรายละเอียดของงานที่ต้องดำเนินการ ผู้รับผิดชอบ และระยะเวลาที่ใช้ในการดำเนินการ (3) การประเมินระดับค่าความเสี่ยงที่เหลืออยู่ (residual risk) ว่าอยู่ในระดับความเสี่ยงที่ยอมรับได้ (4) การขออนุมัติแผนการบริหารจัดการความเสี่ยงจากคณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมาย (5) การสื่อสารแผนการบริหารจัดการความเสี่ยงให้ผู้ที่เกี่ยวข้องรับทราบ 6. การจัดทำทะเบียนความเสี่ยง (risk register) ควรจัดให้มีทะเบียนความเสี่ยง (risk register) เพื่อบันทึกผลการประเมินความเสี่ยง และแนวทางในการจัดการความเสี่ยง โดยมีตัวอย่างรายละเอียด ดังนี้ (1) วันที่ประเมินความเสี่ยง (2) รายละเอียดเหตุการณ์ความเสี่ยง (3) โอกาสหรือความถี่ที่จะเกิดเหตุการณ์ความเสี่ยง (likelihood) (4) ความมีนัยสำคัญหรือผลกระทบที่จะเกิดขึ้น (potential impact) (5) ระดับค่าความเสี่ยงก่อนการควบคุม (inherent risk) (6) แนวทางจัดการความเสี่ยง (risk treatment) (7) เจ้าของความเสี่ยง (risk owner) (8) ระดับความเสี่ยงที่เหลืออยู่ (residual risk) (9) สถานะของการจัดการความเสี่ยง (status of risk treatment) 7. การติดตามและทบทวนความเสี่ยง (risk monitor and review) ควรจัดให้มีกระบวนการติดตามและทบทวนความเสี่ยงด้าน IT โดยครอบคลุมการดำเนินการ ดังนี้ (1) การกำหนดผู้รับผิดชอบในการติดตามและทบทวนความเสี่ยง (2) การกำหนดดัชนีชี้วัดความเสี่ยงด้าน IT ที่สำคัญ (IT key risk indicator) เพื่อให้สามารถติดตามแนวโน้มของความเสี่ยง และสามารถทบทวนมาตรการควบคุมความเสี่ยงได้อย่างมีประสิทธิภาพ (3) การติดตามความคืบหน้าของการดำเนินงานตามแผนการบริหารจัดการความเสี่ยงด้าน IT

ข้อกำหนดในภาคผนวก 2 แนบท้ายประกาศที่ สธ. 38/2565	แนวปฏิบัติ
	8. การรายงานความเสี่ยง (risk reporting) ควรจัดให้มีการรายงานผลการประเมินความเสี่ยงด้าน IT และผลการบริหารจัดการความเสี่ยงด้าน IT ต่อคณะกรรมการของผู้ประกอบธุรกิจอย่างน้อยปีละ 1 ครั้ง
2.2.2 นโยบายการรักษาความมั่นคงปลอดภัยด้าน IT (IT security policy) มีเรื่องที่ต้องครอบคลุม ดังนี้ (1) โครงสร้างการบริหารงานเพื่อการรักษาความมั่นคงปลอดภัยด้าน IT (organization of information technology security) (2) การบริหารจัดการบุคลากร และบุคคลภายนอก (3) การบริหารจัดการทรัพย์สินด้าน IT (IT asset management) (4) การรักษาความมั่นคงปลอดภัยของข้อมูล (data security) (5) การควบคุมการเข้าถึงข้อมูลและระบบ IT (access control) (6) การควบคุมการเข้ารหัส (cryptographic control) (7) การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (physical and environmental security) (8) การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้าน IT (IT operation security)	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]

ข้อกำหนดในภาคผนวก 2 แนบท้ายประกาศที่ สธ. 38/2565	แนวปฏิบัติ
(9) การรักษาความมั่นคงปลอดภัยเกี่ยวกับระบบเครือข่ายสื่อสาร (communication system security) (10) การบริหารจัดการโครงการด้าน IT (IT project management) การจัดหา พัฒนา และบำรุงรักษาระบบ IT (system acquisition, development and maintenance) (11) การบริหารจัดการเหตุการณ์ผิดปกติด้าน IT (IT incident management) (12) แผนฉุกเฉินด้าน IT (IT contingency plan)	
2.3 ผู้ประกอบธุรกิจต้องจัดให้มีการดำเนินการตามนโยบายใน 2.2 ดังนี้ 2.3.1 สื่อสารนโยบายตาม 2.2 ให้แก่บุคคลที่เกี่ยวข้อง[1] รับทราบตามบทบาทหน้าที่ ความรับผิดชอบ และสิทธิการเข้าถึงข้อมูล ในลักษณะที่สามารถเข้าถึงได้ง่าย เพื่อให้บุคคลที่เกี่ยวข้องดังกล่าวเข้าใจและสามารถปฏิบัติตามนโยบายได้อย่างถูกต้อง	1. ในการสื่อสารนโยบายให้กับบุคคลภายนอก ผู้ประกอบธุรกิจควรพิจารณาถึงรายละเอียดที่บุคคลภายนอกควรรู้เพื่อให้สามารถปฏิบัติงานได้สอดคล้องกับนโยบายของผู้ประกอบธุรกิจ โดยคำนึงถึงความลับของการเปิดเผยข้อมูลด้วย
2.3.2 กำหนดขั้นตอนและวิธีปฏิบัติงานให้เป็นไปตามนโยบายตามข้อ 2.2	1. ผู้ประกอบธุรกิจควรกำหนดขั้นตอนการปฏิบัติงานที่เกี่ยวข้องกับระบบ IT เป็นลายลักษณ์อักษร เพื่อให้เจ้าหน้าที่ผู้ปฏิบัติงานด้าน IT สามารถปฏิบัติงานได้อย่างถูกต้อง และเป็นไปตามนโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้าน IT 2. ผู้ประกอบธุรกิจควรกำหนดวิธีปฏิบัติสำหรับการอนุมัติยกเว้น (exception) กรณีที่มีความจำเป็นให้ไม่สามารถปฏิบัติตามขั้นตอนและวิธีปฏิบัติงานที่ผู้ประกอบธุรกิจกำหนดไว้ โดยจัดให้มีการประเมินความเสี่ยง ควบคุมความเสี่ยงอย่างเพียงพอ

[1] “บุคคลที่เกี่ยวข้อง” หมายความว่า บุคลากร กรรมการ รวมถึงบุคคลภายนอก

ข้อกำหนดในภาคผนวก 2 แนบท้ายประกาศที่ สธ. 38/2565	แนวปฏิบัติ
	เหมาะสม และขออนุมัติยกเว้นจากผู้มีอำนาจก่อนดำเนินการต่อไป พร้อมนี้ ควรจัดเก็บหลักฐานการอนุมัติยกเว้นดังกล่าวอย่างเป็นลายลักษณ์อักษร 3. ผู้ประกอบธุรกิจควรจัดให้มีการสอบทานความเหมาะสมของรายการขออนุมัติยกเว้น ตลอดจนแนวทางการควบคุมความเสี่ยงอย่างน้อยปีละ 1 ครั้ง เพื่อทบทวนแนวทางการดำเนินการให้มีความเหมาะสมต่อความเสี่ยงที่อาจมีการเปลี่ยนแปลงไปตามสภาพแวดล้อมการประกอบธุรกิจและการใช้งานเทคโนโลยีสารสนเทศในการประกอบธุรกิจ
2.3.3 ในกรณีที่มีการเปลี่ยนแปลงนโยบายตามข้อ 2.2 ต้องสื่อสารให้บุคคลที่เกี่ยวข้องได้รับทราบอย่างทั่วถึง และต้องปรับปรุงขั้นตอนและวิธีปฏิบัติงานให้สอดคล้องกับการเปลี่ยนแปลงดังกล่าว	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]
2.4 ผู้ประกอบธุรกิจต้องทบทวนหรือปรับปรุงนโยบายตามข้อ 2.2 อย่างน้อยปีละ 1 ครั้ง และโดยไม่ชักช้าเมื่อมีเหตุการณ์ใด ๆ ซึ่งอาจส่งผลกระทบต่อการกำกับดูแลและบริหารจัดการความเสี่ยงด้าน IT อย่างมีนัยสำคัญ	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]

หมวดที่ 2 การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Information Technology Security)

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. 38/2565	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 มีการสอบทานการปฏิบัติงานเพื่อป้องกันความเสี่ยงในการรักษาความมั่นคงปลอดภัยของระบบ IT ที่อาจเกิดขึ้นในการปฏิบัติงาน	1. ผู้ประกอบธุรกิจควรจัดให้มีการแบ่งแยกหน้าที่ในการปฏิบัติงานด้านต่าง ๆ ที่เกี่ยวกับความมั่นคงปลอดภัยของระบบ IT อย่างชัดเจน เพื่อให้มีการสอบทานการปฏิบัติงานระหว่างกัน เพื่อลดข้อผิดพลาดในการปฏิบัติงานและลดโอกาสการกระทำผิด (fraud) เช่น แบ่งแยกผู้พัฒนาระบบงาน (developer) ออกจากผู้มีสิทธิในการนำระบบขึ้นใช้งานจริง เป็นต้น ทั้งนี้ กรณีที่ไม่สามารถแบ่งแยกหน้าที่ความรับผิดชอบได้เนื่องจากข้อจำกัดทางด้านขนาดของธุรกิจหรือบุคลากร ผู้ประกอบธุรกิจควรจัดให้มีมาตรการควบคุมทดแทน เช่น การจัดให้มีกระบวนการติดตามและตรวจสอบการปฏิบัติงานของบุคลากรที่เกี่ยวข้องอย่างใกล้ชิดและสม่ำเสมอ เป็นต้น
2.2 การบริหารจัดการบุคลากร และบุคคลภายนอก	
ส่วนที่ 2 การบริหารจัดการบุคลากร และบุคคลภายนอก	
2.2.1 การบริหารจัดการบุคลากร	
<u>บุคลากรที่ต้องบริหารจัดการ</u> 2.1 บุคลากรที่เกี่ยวข้องหรือที่ใช้ระบบ IT ปฏิบัติงาน	

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. 38/2565	แนวปฏิบัติ
<u>การบริหารจัดการ</u> ผู้ประกอบธุรกิจต้องบริหารจัดการบุคลากรตามข้อ 2.1 อย่างเหมาะสม โดยดำเนินการอย่างน้อยดังนี้ (1) มีกระบวนการคัดเลือกบุคลากรในการปฏิบัติหน้าที่ดังนี้ (1.1) คำนึงถึงความรู้ ความสามารถ และความเพียงพอในการปฏิบัติงาน (1.2) มีการตรวจสอบข้อมูลของบุคลากรก่อนการว่าจ้างอย่างเพียงพอและสอดคล้องกับความเสี่ยงของตำแหน่งงานและหน้าที่ความรับผิดชอบ	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]
(2) มีข้อกำหนดให้บุคลากรทำความเข้าใจ รับทราบ และลงนามยอมรับในเรื่องดังนี้ (2.1) บทบาทหน้าที่และความรับผิดชอบของบุคลากรดังกล่าวเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้าน IT (2.2) non-disclosure agreement	1. ผู้ประกอบธุรกิจควรให้บุคลากรที่ได้รับการว่าจ้างทำความเข้าใจ รับทราบ และลงนามยอมรับเงื่อนไขการว่าจ้างงานหรือระเบียบข้อบังคับภายในองค์กร นโยบายการรักษาความมั่นคงปลอดภัยด้าน IT และข้อตกลงการไม่เปิดเผยข้อมูล (non-disclosure agreement) ก่อนเริ่มปฏิบัติงาน 2. non-disclosure agreement ควรมีเนื้อหาขั้นต่ำ ดังนี้ (ก) ความเป็นเจ้าของข้อมูลสำคัญทางธุรกิจ ทรัพย์สินทางปัญญา และการป้องกันการรั่วไหลของข้อมูล (ข) ความรับผิดชอบในการเก็บรักษาความลับ และไม่เปิดเผยข้อมูลโดยไม่ได้รับอนุญาต (ค) การแจ้งเตือนและรายงานผู้เกี่ยวข้องหากพบการรั่วไหลหรือเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต (ง) การดำเนินการกรณีละเมิดหรือยกเลิกข้อตกลง รวมทั้งข้อกำหนดในการคืนหรือทำลายข้อมูลที่มีความสำคัญเมื่อสิ้นสุดข้อตกลง
(3) สร้างความตระหนักรู้ถึงความเสี่ยงด้าน IT ให้แก่บุคลากรที่ปฏิบัติงาน ซึ่งสามารถเข้าถึงข้อมูลหรือระบบงานภายในองค์กร เพื่อให้บุคลากรดังกล่าวสามารถใช้งานระบบ IT ได้อย่างปลอดภัย	1. ผู้ประกอบธุรกิจควรส่งเสริมและพัฒนาความรู้ด้าน IT ให้แก่บุคลากรอย่างสม่ำเสมอ เช่น การจัดการอบรมภายในองค์กร หรือการส่งบุคลากรเข้าร่วมฝึกอบรมภายนอกองค์กร เป็นต้น เพื่อให้บุคลากรมีความรู้ความเข้าใจถึงการใช้งาน IT ที่ถูกต้องปลอดภัย และลดความเสี่ยงที่อาจเกิดขึ้นจากการใช้งาน IT โดยมีเนื้อหา เช่น (ก) การรักษาความมั่นคงปลอดภัยด้าน IT

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. 38/2565	แนวปฏิบัติ
	(ข) ความเสี่ยงด้าน IT และภัยคุกคามทางไซเบอร์ (ค) หลักเกณฑ์และกฎหมายที่เกี่ยวข้องกับ IT เป็นต้น 2. ผู้ประกอบธุรกิจควรทบทวนแผนการส่งเสริมและพัฒนาความรู้ด้าน IT (training program) อย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่าเนื้อหาและรายละเอียดของแผนงานที่เกี่ยวข้องยังคงเพียงพอเหมาะสมกับแนวโน้มความเสี่ยงด้าน IT ในปัจจุบัน 3. ผู้ประกอบธุรกิจควรจัดให้มีการเสริมสร้างความตระหนักเรื่องการรักษาความมั่นคงปลอดภัยด้าน IT และความเสี่ยงด้าน IT อย่างสม่ำเสมอ ให้แก่บุคลากร (user) ที่สามารถเข้าถึงข้อมูลที่มีความสำคัญของผู้ประกอบธุรกิจหรือข้อมูลของลูกค้า เช่น การทดสอบเรื่องอีเมลหลอกลวง (phishing) การทดสอบเรื่องวิศวกรรมสังคม (social engineering) และการซักซ้อมแผนเพื่อเตรียมความพร้อมรับมือกับการโจมตีทางไซเบอร์ เป็นต้น
(4) กำหนดให้บุคลากรงดเว้นการใช้งานระบบ IT ในลักษณะที่อาจก่อให้เกิดความเสียหายแก่ผู้ประกอบธุรกิจ ตลาดทุนโดยรวม หรือที่เป็นการกระทำผิดกฎหมาย หรือข้อกำหนดและจรรยาบรรณที่ผู้ประกอบธุรกิจกำหนดไว้ (ถ้ามี)	1. ผู้ประกอบธุรกิจควรจัดให้มีนโยบายการใช้งาน IT ที่ยอมรับได้ (acceptable use policy) โดยมีรายละเอียดครอบคลุมขอบเขต ความรับผิดชอบของผู้ใช้งาน IT สิ่งที่ผู้ใช้งานพึงปฏิบัติ และสิ่งที่ผู้ใช้งานห้ามปฏิบัติ 2. ผู้ประกอบธุรกิจควรสื่อสารนโยบายการใช้งาน IT ที่ยอมรับได้ (acceptable use policy) ให้ผู้ใช้งานรับทราบ และลงนามยอมรับนโยบายดังกล่าว
(5) กำหนดมาตรการในการลงโทษบุคลากรที่มีพฤติกรรมฝ่าฝืนหรือไม่ปฏิบัติตามนโยบายและมาตรการรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้าน IT	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]
(6) กำหนดขั้นตอนปฏิบัติเมื่อสิ้นสุดการจ้างงาน หรือเมื่อมีการเปลี่ยนแปลงตำแหน่งงาน เพื่อป้องกันการละเมิดหรือความเสียหายที่อาจเกิดขึ้นต่อทรัพย์สินด้าน IT	1. ผู้ประกอบธุรกิจควรจัดให้มีกระบวนการรองรับเมื่อมีการเปลี่ยนแปลงตำแหน่งงาน หรือสิ้นสุดการจ้างงาน เช่น การคืนทรัพย์สินขององค์กร การปรับปรุงสิทธิให้เป็นปัจจุบัน การยกเลิกสิทธิเมื่อหมดหน้าที่และความรับผิดชอบ เป็นต้น รวมทั้งมีการสื่อสารให้ผู้ที่เกี่ยวข้องรับทราบถึงการเปลี่ยนแปลงสิทธิ หน้าที่ และความรับผิดชอบ
2.2.2 การบริหารจัดการบุคคลภายนอก (third-party management)	
<u>บุคลากรที่ต้องบริหารจัดการ</u>	

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. 38/2565	แนวปฏิบัติ
2.2 บุคคลภายนอก ในกรณีที่ผู้ประกอบธุรกิจมีการดำเนินการอย่างใดอย่างหนึ่งดังนี้ 2.2.1 ใช้บริการงานด้าน IT จากบุคคลภายนอก 2.2.2 เชื่อมต่อระบบ IT กับบุคคลภายนอก 2.2.3 อนุญาตให้บุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญหรือข้อมูลของลูกค้าที่ควบคุมดูแลโดยผู้ประกอบธุรกิจได้	
<u>การบริหารจัดการ</u> ผู้ประกอบธุรกิจต้องบริหารจัดการบุคคลภายนอกตามข้อ 2.2.1 , 2.2.2 หรือ 2.2.3 ดังนี้ (1) ประเมินความเสี่ยงจากการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก รวมถึงผู้รับดำเนินการช่วง (subcontract) จากบุคคลภายนอก (ถ้ามี)	1. ผู้ประกอบธุรกิจควรประเมินความเสี่ยงและผลกระทบก่อน (1) การใช้บริการงานด้าน IT จากบุคคลภายนอก (2) การเชื่อมต่อระบบ IT กับบุคคลภายนอก และ (3) การอนุญาตให้บุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญหรือข้อมูลของลูกค้าที่ควบคุมดูแลโดยผู้ประกอบธุรกิจได้ โดยคำนึงถึงความเสี่ยง ดังนี้ (1) ความเสี่ยงด้านกฎหมาย และกฎเกณฑ์ที่เกี่ยวข้องทั้งในประเทศและต่างประเทศ เช่น กฎหมายเกี่ยวกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ กฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล กฎหมายเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ และ The EU General Data Protection Regulation (GDPR) เป็นต้น (2) ความเสี่ยงจากการกำกับดูแลและบริหารจัดการบุคคลภายนอกที่ไม่รัดกุมเพียงพอ เช่น การไม่สามารถตรวจสอบการดำเนินงานของบุคคลภายนอกได้ด้วยตนเอง เป็นต้น (3) ความเสี่ยงจากการกระจุกตัว (concentration risk) เช่น ผู้ประกอบธุรกิจและบริษัทในกลุ่มธุรกิจเดียวกันใช้บริการจากบุคคลภายนอกเพียงรายเดียว เป็นต้น (4) ความเสี่ยงจากการพึ่งพาบุคคลภายนอกรายใดรายหนึ่งเป็นหลัก (third party/vendor locked-in) ซึ่งทำให้มีข้อจำกัดในการเปลี่ยนแปลงเทคโนโลยี ผู้ให้บริการ หรือข้อจำกัดในการนำระบบหรือข้อมูลกลับมาดำเนินการเอง

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. 38/2565	แนวปฏิบัติ
	(5) ความเสี่ยงด้าน IT และภัยทางไซเบอร์ เช่น ระบบที่ให้บริการโดยบุคคลภายนอกเกิดขัดข้อง ระบบของบุคคลภายนอกมีช่องโหว่ทำให้ข้อมูลเกิดการสูญหายหรือรั่วไหล เป็นต้น (6) ความเสี่ยงกรณีบุคคลภายนอกให้ผู้อื่นดำเนินการแทน (sub-contracting) เช่น subcontractor ปฏิบัติงานบกพร่อง เป็นต้น 2. ผู้ประกอบธุรกิจควรจัดให้มีการกำหนดระดับความมีนัยสำคัญของบุคคลภายนอกแต่ละราย
(2) กำหนดวิธีปฏิบัติและหลักเกณฑ์ในการคัดเลือกบุคคลภายนอก	1. ผู้ประกอบธุรกิจควรกำหนดกระบวนการและหลักเกณฑ์ในการคัดเลือกบุคคลภายนอกอย่างชัดเจน และเป็นลายลักษณ์อักษร เพื่อให้มั่นใจว่าผู้ให้บริการภายนอกจะสามารถให้บริการได้ตรงตามความต้องการของผู้ประกอบธุรกิจ ทั้งนี้ การตัดสินใจในการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอกที่มีความเสี่ยงหรือมีนัยสำคัญ ควรได้รับความเห็นชอบจากคณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมาย 2. ผู้ประกอบธุรกิจควรประเมินศักยภาพบุคคลภายนอก (due diligence) ให้สอดคล้องกับระดับความเสี่ยง และความมีนัยสำคัญของบุคคลภายนอก โดยคำนึงถึงเรื่องดังต่อไปนี้ (1) ฐานะทางการเงิน ชื่อเสียง ความรู้ความเชี่ยวชาญ ประสบการณ์ และความสามารถในการให้บริการในช่วงที่ผ่านมา (2) การบริหารจัดการความเสี่ยง การควบคุมภายใน การตรวจสอบภายใน และการติดตามผลการปฏิบัติงาน (3) การรักษาความมั่นคงปลอดภัยด้าน IT (4) การบริหารจัดการความต่อเนื่องทางธุรกิจ และความพร้อมรับมือภัยหรือเหตุการณ์ต่าง ๆ (5) การปฏิบัติตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้อง เช่น การขอตรวจสอบเอกสารหลักฐานหรือใบรับรองจากบุคคลภายนอกในการดำเนินการตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้อง หรือการตรวจสอบประวัติด้านการกระทำความผิด เป็นต้น (6) การปฏิบัติตามมาตรฐานสากลด้าน IT เช่น การตรวจสอบเอกสารหลักฐานการได้รับการรองรับตามมาตรฐาน ISO 27001 เป็นต้น โดยการรับรองการปฏิบัติตามมาตรฐานสากล ผู้ประกอบธุรกิจควรพิจารณาว่า บุคคลภายนอกได้รับการรับรองในส่วนระบบที่สำคัญ หรือระบบที่ผู้ประกอบธุรกิจใช้บริการ เชื่อมต่อ หรือเข้าถึงข้อมูล หรือได้รับการรับรองครอบคลุมทั้งองค์กร (7) การใช้เทคโนโลยีแบบเปิด (open technology) เพื่อให้สามารถนำระบบหรือข้อมูลไปใช้งานหรือเชื่อมโยงกับระบบอื่นได้

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. 38/2565	แนวปฏิบัติ
	(interoperability) และลดข้อจำกัดในการย้ายหรือเปลี่ยนแปลงเทคโนโลยี ผู้ให้บริการ หรือพันธมิตร รวมถึงข้อจำกัดในการนำระบบหรือข้อมูลกลับมาดำเนินการเอง (8) กรณีที่บุคคลภายนอกมอบหมายการปฏิบัติงานที่สำคัญให้กับบุคคลอื่นต่อ (sub-contracting to another supplier) ผู้ประกอบธุรกิจควรพิจารณารายละเอียดด้านความมั่นคงปลอดภัยสารสนเทศของบุคคลดังกล่าวด้วย (9) *[ความเสี่ยงสูง] ผู้ประกอบธุรกิจควรจัดให้มีการประเมินด้านคุณภาพและความน่าเชื่อถือของบุคคลภายนอก โดยพิจารณาจากประสบการณ์ คุณภาพของบริการและผลงานที่ส่งมอบ ตลอดจนมาตรฐานด้านความปลอดภัย IT ที่เกี่ยวข้องกับสินค้าและบริการ และจัดทำเป็นรายชื่อบุคคลภายนอกที่เชื่อถือได้ (trusted third-party/trusted vendor) เพื่อใช้เป็นส่วนหนึ่งของเกณฑ์การคัดเลือกผู้ให้บริการในอนาคต*
(3) กำหนดบทบาท หน้าที่ และความรับผิดชอบของผู้ประกอบธุรกิจและบุคคลภายนอกอย่างชัดเจนและเป็นลายลักษณ์อักษร	1. ผู้ประกอบธุรกิจควรจัดทำสัญญาหรือข้อตกลงการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอกเป็นลายลักษณ์อักษร โดยมีการลงนามร่วมกันระหว่างผู้ประกอบธุรกิจและบุคคลภายนอก เพื่อให้มั่นใจได้ว่าบุคคลภายนอกมีหน้าที่รับผิดชอบในการรักษาความมั่นคงปลอดภัยของระบบ IT ในระดับที่เหมาะสม โดยมีรายละเอียดสอดคล้องกับความเสี่ยง และความมีนัยสำคัญของบุคคลภายนอก ดังนี้ (1) ขอบเขตการให้บริการ การเชื่อมต่อ และการเข้าถึงข้อมูลจากบุคคลภายนอก (2) บทบาท หน้าที่ และความรับผิดชอบของบุคคลภายนอกและผู้ประกอบธุรกิจ (3) มาตรฐานขั้นต่ำในการปฏิบัติงานของบุคคลภายนอก เช่น การรักษาความปลอดภัยของระบบ IT การรักษาความลับของข้อมูล และการไม่นำข้อมูลไปใช้นอกเหนือจากที่ระบุไว้ในสัญญาหรือข้อตกลงการให้บริการ เป็นต้น (4) ข้อตกลงระดับการให้บริการด้าน IT (service level agreement : SLA) สำหรับการใช้บริการจากบุคคลภายนอก (5) การติดตามและรายงานผลการปฏิบัติงานของบุคคลภายนอก ซึ่งครอบคลุมถึงการแจ้งการเปลี่ยนแปลงหรือปัญหาที่สำคัญและการรายงานเหตุการณ์ผิดปกติอย่างทันการณ์ (6) รายชื่อ และช่องทางการติดต่อในกรณีเกิดปัญหาเกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบ IT (7) การทำลายข้อมูลเมื่อสิ้นสุดหรือยกเลิกการใช้บริการ การเชื่อมต่อ และการเข้าถึงข้อมูลจากบุคคลภายนอก (8) เงื่อนไขหรือสิทธิของผู้ประกอบธุรกิจในการเปลี่ยนแปลง ยุติ หรือยกเลิกสัญญาหรือข้อตกลงกับบุคคลภายนอก เช่น กรณีที่

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. 38/2565	แนวปฏิบัติ
	บุคคลภายนอกมีการละเมิดสัญญาหรือข้อตกลง เป็นต้น (9) การจัดให้มีแผนฉุกเฉินด้าน IT (IT contingency plan) ที่สอดคล้องกับแผนฉุกเฉินด้าน IT ของผู้ประกอบธุรกิจ (10) ความรับผิดชอบต่อความเสียหายที่เกิดจากบุคคลภายนอก เช่น กรณีการให้บริการไม่เป็นไปตาม SLA ที่กำหนดไว้ เป็นต้น หากมีข้อจำกัดในการระบุรายละเอียดและกำหนดเงื่อนไขที่สำคัญลงในข้อตกลงหรือสัญญาที่ทำกับบุคคลภายนอก ผู้ประกอบธุรกิจควรมีการประเมินความเสี่ยงและพิจารณาแนวทางควบคุมความเสี่ยงที่เพียงพอเหมาะสม พร้อมทั้งขออนุมัติยกเว้น (exception) จากผู้มีอำนาจ
(4) กรณีบุคคลภายนอกซึ่งเป็นผู้ให้บริการงานด้าน IT รายที่มีนัยสำคัญตามผลการประเมินความเสี่ยงในข้อ 2.2 (1) ข้อตกลงหรือสัญญาการให้บริการต้องระบุสิทธิให้ผู้ประกอบธุรกิจ สำนักงาน และผู้ตรวจสอบภายนอกที่ได้รับการแต่งตั้งจากผู้ประกอบธุรกิจหรือสำนักงาน สามารถเข้าตรวจสอบการดำเนินงานและการควบคุมภายในของบุคคลภายนอกดังกล่าวได้ หากมีเหตุจำเป็นทำให้ผู้ประกอบธุรกิจไม่สามารถระบุสิทธิในการเข้าตรวจสอบตามวรรคหนึ่งไว้ในข้อตกลงหรือสัญญา ผู้ประกอบธุรกิจต้องมีมาตรการประเมินหรือติดตามการดำเนินงานและการควบคุมภายในของบุคคลภายนอกให้รัดกุมเพียงพอสอดคล้องกับความเสี่ยงและความมีนัยสำคัญของการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูล	1. ผู้ประกอบธุรกิจควรกำหนดสิทธิให้ผู้ประกอบธุรกิจ สำนักงาน และผู้ตรวจสอบภายนอกที่ได้รับการแต่งตั้งจากผู้ประกอบธุรกิจหรือสำนักงาน สามารถเข้าตรวจสอบการดำเนินงานด้าน IT และการควบคุมภายในของบุคคลภายนอกที่ให้บริการงานด้าน IT รายที่มีนัยสำคัญ โดยระบุไว้เป็นส่วนหนึ่งของข้อตกลงหรือสัญญาการให้บริการ 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. 38/2565	แนวปฏิบัติ
(5) มี non-disclosure agreement สำหรับบุคคลภายนอกหรือผู้รับดำเนินการช่วงของบุคคลภายนอก ในกรณีที่บุคคลดังกล่าวสามารถเข้าถึงข้อมูลสำคัญของผู้ประกอบธุรกิจหรือข้อมูลของลูกค้า	1. non-disclosure agreement ควรมีรายละเอียดครอบคลุมขอบเขตความรับผิดชอบในการเก็บรักษาความลับ การไม่เปิดเผยข้อมูลโดยไม่ได้รับอนุญาต การรายงานผู้ประกอบธุรกิจเมื่อพบการรั่วไหลหรือเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต และการทำลายข้อมูลที่มีความสำคัญเมื่อสิ้นสุดข้อตกลงหรือสัญญา
(6) กำกับดูแล ติดตาม และบริหารจัดการความเสี่ยงจากการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก โดยต้องสอดคล้องกับระดับความเสี่ยงและระดับความมีนัยสำคัญของบุคคลภายนอก	1. ผู้ประกอบธุรกิจควรกำกับดูแล ติดตาม และบริหารจัดการความเสี่ยงจากการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอกให้สอดคล้องกับความเสี่ยง และความมีนัยสำคัญของบุคคลภายนอก โดยครอบคลุมการดำเนินการอย่างน้อย ดังนี้ (1) กำหนดผู้รับผิดชอบในการติดตามผลการปฏิบัติงานของบุคคลภายนอกอย่างต่อเนื่อง โดยพิจารณาตามขอบเขต ระดับความเสี่ยงและความมีนัยสำคัญของการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก (2) จัดให้มีทะเบียนบุคคลภายนอก เพื่อให้สามารถใช้ในการบริหารจัดการความเสี่ยง ติดตาม และตรวจสอบการปฏิบัติงานของบุคคลภายนอกได้อย่างครบถ้วนต่อเนื่อง โดยมีรายละเอียดครอบคลุม (ก) ชื่อบุคคลภายนอก (ข) รายละเอียดของการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก (ค) ระดับความเสี่ยงและระดับความมีนัยสำคัญ (ง) วันเริ่มต้นและสิ้นสุดสัญญาหรือข้อตกลง (3) จัดให้มีมาตรการควบคุมและติดตามสิทธิการเข้าถึงข้อมูลสารสนเทศของบุคคลภายนอกอย่างสม่ำเสมอ เพื่อให้สิทธิดังกล่าวเป็นไปตามหลักความจำเป็นต้องรู้ (need-to-know basis) (4) กำหนดให้บุคคลภายนอกรายงานเหตุการณ์ผิดปกติที่เกิดขึ้นระหว่างการดำเนินงานที่เกี่ยวข้องให้ผู้ประกอบธุรกิจได้รับทราบอย่างทันการณ์ (5) ประเมินผลการปฏิบัติงานหรือผลการให้บริการของบุคคลภายนอก ทั้งในด้านประสิทธิภาพของบริการ การรักษาความมั่นคงปลอดภัยด้าน IT และการปฏิบัติตามกฎหมายที่เกี่ยวข้อง เมื่อจะต่อสัญญาหรือเมื่อถึงรอบระยะเวลาที่ผู้ประกอบธุรกิจกำหนด (6) ทบทวนคุณสมบัติบุคคลภายนอกอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าบุคคลภายนอกยังคงมีคุณสมบัติที่เหมาะสม

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. 38/2565	แนวปฏิบัติ
(7) รักษาความมั่นคงปลอดภัยด้าน IT จากการใช้บริการการเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอกที่สอดคล้องกับมาตรฐานการรักษาความมั่นคงปลอดภัยด้าน IT ของผู้ประกอบธุรกิจ	1. ผู้ประกอบธุรกิจควรมีแนวทางการดูแลให้มั่นใจว่าการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอกมีการรักษาความมั่นคงปลอดภัยด้าน IT ตามกรอบหลักการที่สำคัญ 3 ประการ คือ การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของระบบและข้อมูล และสอดคล้องกับนโยบายและมาตรการรักษาความมั่นคงปลอดภัยด้าน IT ของผู้ประกอบธุรกิจ หรือมาตรฐานสากลที่เกี่ยวข้อง เช่น ISO/IEC 27001 เป็นต้น โดยพิจารณาให้สอดคล้องกับระดับความเสี่ยง และความมีนัยสำคัญของบุคคลภายนอก
(8) เตรียมความพร้อมรับมือต่อเหตุการณ์ผิดปกติด้าน IT ที่อาจเกิดขึ้นและมีผลกระทบอย่างมีนัยสำคัญเพื่อให้สามารถให้บริการหรือดำเนินธุรกิจได้อย่างต่อเนื่อง	1. ผู้ประกอบธุรกิจควรจัดให้มีแผนรองรับในกรณีที่บุคคลภายนอกเกิดเหตุการณ์ผิดปกติด้าน IT (incident response plan) ซึ่งมีผลกระทบกับการดำเนินการของผู้ประกอบธุรกิจ โดยครอบคลุมเหตุการณ์ที่เกี่ยวข้องกับเหตุการณ์ความปลอดภัยทางไซเบอร์และเหตุการณ์การละเมิดต่อข้อมูลส่วนบุคคล
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 ครอบคลุมการจัดทำทะเบียนรายการทรัพย์สิน การปรับปรุงทะเบียนรายการทรัพย์สิน การยกเลิกและเรียกคืนทรัพย์สิน 2. ผู้ประกอบธุรกิจควรจัดทำทะเบียนรายการทรัพย์สินด้าน IT ประเภทอุปกรณ์ (hardware) รวมถึง virtual machine ให้ครบถ้วนและเป็นปัจจุบัน โดยมีตัวอย่างของรายละเอียด ดังนี้ (1) เลขทะเบียนทรัพย์สิน (2) ประเภทฮาร์ดแวร์ (3) รายละเอียดทางเทคนิค ยี่ห้อ รุ่น

<table>
<tr><th>ข้อกำหนดในภาคผนวก 3
แนบท้ายประกาศที่ สธ. 38/2565</th><th>แนวปฏิบัติ</th></tr>
<tr><td></td><td>
(4) ระบบปฏิบัติการและเวอร์ชัน
(5) เจ้าของทรัพย์สิน
(6) ผู้ดูแลทรัพย์สิน
(7) สถานที่ตั้ง
(8) วันที่เริ่มใช้งาน/วันที่ติดตั้ง
(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 ประเภทซอฟต์แวร์ (software) ให้ครบถ้วนและเป็นปัจจุบัน โดยมีตัวอย่างของรายละเอียด ดังนี้
(1) เลขทะเบียนทรัพย์สิน
(2) ชื่อซอฟต์แวร์
</td></tr>
</table>

<table>
<tr><th>ข้อกำหนดในภาคผนวก 3
แนบท้ายประกาศที่ สธ. 38/2565</th><th>แนวปฏิบัติ</th></tr>
<tr><td></td><td>(3) รายละเอียดทางเทคนิค/การใช้งาน
(4) ระบบปฏิบัติการและเวอร์ชัน
(5) หน่วยงานภายในผู้เป็นเจ้าของซอฟต์แวร์
(6) วันที่ลงทะเบียนซอฟต์แวร์
(7) วันที่สิ้นสุดการใช้บริการ
(8) เลขทะเบียนทรัพย์สินฮาร์ดแวร์ที่อ้างอิง
<u>ตัวอย่างเช่น</u>
<table>
<tr><th>เลขทะเบียนทรัพย์สิน</th><th>ชื่อซอฟต์แวร์</th><th>รายละเอียดทางเทคนิค/การใช้งาน</th><th>ระบบปฏิบัติการและเวอร์ชัน</th><th>หน่วยงานภายในผู้เป็นเจ้าของซอฟต์แวร์</th><th>วันที่ลงทะเบียนซอฟต์แวร์</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 และทุกครั้งที่มีการเปลี่ยนแปลงระบบ IT อย่างมีนัยสำคัญ</td></tr>
<tr><td>3.2 กำหนดบุคคลหรือหน่วยงานซึ่งรับผิดชอบทรัพย์สินด้าน IT แต่ละรายการ</td><td>1. ผู้ประกอบธุรกิจควรกำหนดบุคคลหรือหน่วยงานที่รับผิดชอบในการจัดทำและปรับปรุงทะเบียนรายการทรัพย์สินด้าน IT รวมถึงบำรุงรักษาทรัพย์สินด้าน IT อย่างสม่ำเสมอตลอดอายุการใช้งานของทรัพย์สินดังกล่าว</td></tr>
<tr><td>3.3 จัดให้มีการบำรุงรักษาทรัพย์สินด้าน IT อย่างสม่ำเสมอ</td><td>1. ผู้ประกอบธุรกิจควรบำรุงรักษาทรัพย์สินด้าน IT ให้มีสภาพพร้อมใช้งานและรองรับการดำเนินธุรกิจอย่างต่อเนื่อง พร้อมทั้งวางแผน</td></tr>
</table>

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. 38/2565	แนวปฏิบัติ
	รองรับทรัพย์สินด้าน IT ที่ใกล้จะสิ้นสุดอายุการใช้งาน (end of life) หรือสิ้นสุดการสนับสนุนหรือให้บริการจากผู้ผลิต (end of support) ได้อย่างเหมาะสมทันการณ์ ทั้งนี้ ในกรณีที่มีความจำเป็นต้องใช้ทรัพย์สินที่สิ้นสุดอายุการใช้งานหรือสิ้นสุดการสนับสนุนหรือให้บริการจากผู้ผลิต ผู้ประกอบธุรกิจควรประเมินความเสี่ยงและจัดให้มีมาตรการควบคุมความเสี่ยงอย่างเหมาะสม
2.4 การรักษาความมั่นคงปลอดภัยของข้อมูล (data security)	
ส่วนที่ 4 การรักษาความมั่นคงปลอดภัยของข้อมูล (data security) ผู้ประกอบธุรกิจต้องจัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลเพื่อให้ข้อมูลมีความถูกต้องครบถ้วน และมีสภาพพร้อมใช้งาน รวมถึงสามารถรักษาความลับของข้อมูลได้อย่างเหมาะสม ดังนี้	
4.1 การกำหนดบุคคลหรือหน่วยงานซึ่งเป็นเจ้าของข้อมูล	1. ผู้ประกอบธุรกิจควรกำหนดบุคคลหรือหน่วยงานซึ่งเป็นเจ้าของข้อมูล (data owner) เพื่อรับผิดชอบในการกำหนดผู้ใช้งาน สิทธิการเข้าถึงและแก้ไขเปลี่ยนแปลงข้อมูล และวิธีปฏิบัติในการใช้งานข้อมูลอย่างปลอดภัย

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. 38/2565	แนวปฏิบัติ
4.2 การจัดชั้นความลับของข้อมูล (data classification) และแนวทางการรักษาความปลอดภัยของข้อมูลที่สอดคล้องตามชั้นความลับ โดยครอบคลุมข้อมูลดังนี้ 4.2.1 ข้อมูลที่อยู่บนอุปกรณ์ที่ใช้ปฏิบัติงาน (data at endpoint) 4.2.2 ข้อมูลที่อยู่ระหว่างการรับส่งผ่านเครือข่าย (data in transit) 4.2.3 ข้อมูลที่อยู่บนระบบงานและสื่อบันทึกข้อมูล (data at rest)	1. ผู้ประกอบธุรกิจควรกำหนดหลักเกณฑ์การจัดชั้นความลับของข้อมูล (data classification) และวิธีการจัดการข้อมูล (data handling) ตามชั้นความลับ ให้ครอบคลุมตลอดวงจรชีวิตของข้อมูล (data life cycle) ตั้งแต่การสร้างหรือการได้มาซึ่งข้อมูล การประมวลผล การจัดเก็บ การใช้งาน ไปจนถึงการทำลายข้อมูล รวมทั้งระบุชั้นความลับของข้อมูล (labeling) อย่างชัดเจน 2. ผู้ประกอบธุรกิจควรกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลที่สอดคล้องกับชั้นความลับ โดยครอบคลุม (1) ข้อมูลที่อยู่บนอุปกรณ์ที่ใช้ปฏิบัติงาน (data at endpoint) (2) ข้อมูลที่อยู่ระหว่างการรับส่งผ่านเครือข่าย (data in transit) (3) ข้อมูลที่อยู่บนระบบงานและสื่อบันทึกข้อมูล (data at rest) 3. ผู้ประกอบธุรกิจควรจัดให้มีการรักษาความปลอดภัยของข้อมูลที่อยู่บนสื่อบันทึกข้อมูล โดยดำเนินการ ดังนี้ (1) คำนึงถึงความเสี่ยงที่สื่อบันทึกข้อมูลอาจเสื่อมสภาพ รวมทั้งวิธีการนำข้อมูลกลับมาใช้งานใหม่ ในกรณีที่จัดเก็บข้อมูลเป็นระยะเวลานาน (2) จัดเก็บสื่อบันทึกข้อมูลในพื้นที่ที่มีความมั่นคงปลอดภัย และเป็นไปตามคำแนะนำของผู้ผลิต (ถ้ามี) (3) จัดให้มีมาตรการรักษาความปลอดภัยของการขนส่งสื่อบันทึกข้อมูล (physical media transfer)
4.3 การจัดให้มีแนวทางในการนำเข้า ประมวลผล และทำลายข้อมูลอย่างปลอดภัย	1. ผู้ประกอบธุรกิจควรกำหนดระเบียบปฏิบัติในการทำลายข้อมูล (data disposal) ซึ่งครอบคลุมหน้าที่ความรับผิดชอบของเจ้าของข้อมูล หน่วยงานที่เกี่ยวข้อง และวิธีการทำลายข้อมูลที่เหมาะสมกับชั้นความลับของข้อมูล 2. ผู้ประกอบธุรกิจควรจัดให้มีกระบวนการควบคุมการทำลายข้อมูลที่ครอบคลุมการขออนุมัติจากเจ้าของข้อมูลก่อนดำเนินการ การควบคุมและสอบทานการปฏิบัติงาน และการจัดทำทะเบียนการทำลายข้อมูลสำคัญ
4.4 การจัดทำทะเบียนทรัพย์สินด้าน IT ประเภทข้อมูล (data Inventory) ให้ครบถ้วนและเป็นปัจจุบัน	1. ผู้ประกอบธุรกิจควรจัดทำทะเบียนทรัพย์สินประเภทข้อมูล (data inventory) ให้ครบถ้วนและเป็นปัจจุบัน โดยมีตัวอย่างของรายละเอียด ดังนี้ (1) เลขทะเบียนข้อมูล (2) ชื่อข้อมูลหรือชุดข้อมูล (3) รายละเอียดลักษณะและประเภทของข้อมูล (4) ระดับชั้นความลับและระดับความสำคัญของข้อมูล

<table>
<tr><th>ข้อกำหนดในภาคผนวก 3
แนบท้ายประกาศที่ สธ. 38/2565</th><th>แนวปฏิบัติ</th></tr>
<tr><td></td><td>(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>ระบบ Intranet</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>
<tr><td colspan="2">2.5 การควบคุมการเข้าถึงข้อมูลและระบบ IT (access control)</td></tr>
<tr><td>ส่วนที่ 5 การควบคุมการเข้าถึงข้อมูลและระบบ IT (access control)
ผู้ประกอบธุรกิจต้องจัดให้มีการควบคุมการเข้าถึงข้อมูลและระบบ IT อย่างมีประสิทธิภาพ เพื่อให้สามารถป้องกันการเข้าถึง และเปลี่ยนแปลงแก้ไขโดยผู้ไม่มีสิทธิหรือไม่ได้รับอนุญาต ดังนี้</td><td></td></tr>
<tr><td>5.1 จัดให้มีแนวทางการบริหารจัดการบัญชีผู้ใช้งานและสิทธิการเข้าถึง โดยมีการทบทวนปรับปรุงสิทธิให้เหมาะสมอย่าง</td><td>1. แนวทางการบริหารจัดการบัญชีผู้ใช้งาน ควรครอบคลุมอย่างน้อย ดังนี้
(1) หน่วยงานที่รับผิดชอบในการบริหารจัดการบัญชีผู้ใช้งาน
(2) ขั้นตอนการสร้างบัญชีผู้ใช้งาน โดยบัญชีผู้ใช้งาน (user ID) ควรระบุตัวตนผู้ใช้งานได้ และหลีกเลี่ยงการใช้บัญชีผู้ใช้งานที่มี</td></tr>
</table>

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. 38/2565	แนวปฏิบัติ
สม่ำเสมอ สอดคล้องกับหน้าที่ความรับผิดชอบ รวมถึงมีกระบวนการเพิกถอนสิทธิเมื่อสิ้นสุดความจำเป็นต้องใช้งาน	ผู้ใช้งานมากกว่า 1 ราย (shared ID) (3) การจำกัดหรือหลีกเลี่ยงการใช้งานบัญชีผู้ใช้งานที่มาพร้อมกับระบบ (default user account) (4) การทบทวนบัญชีผู้ใช้งานอย่างน้อยปีละ 1 ครั้ง (5) การระงับหรือลบบัญชีผู้ใช้งานเมื่อ (1) ผู้ใช้งานสิ้นสุดสภาพการเป็นพนักงาน และ (2) ไม่มีความจำเป็นต้องใช้งาน 2. แนวทางการบริหารจัดการสิทธิการเข้าถึงข้อมูลและระบบ IT ควรครอบคลุมอย่างน้อย ดังนี้ (1) หน่วยงานที่รับผิดชอบในการบริหารจัดการสิทธิการเข้าถึงข้อมูลและระบบ IT (2) ขั้นตอนการขออนุมัติสิทธิในการเข้าถึงข้อมูลและระบบ IT จากผู้มีอำนาจ เช่น เจ้าของระบบ หรือเจ้าของข้อมูล เป็นต้น (3) ขั้นตอนการปรับปรุงสิทธิของผู้ใช้งานเมื่อมีการเปลี่ยนแปลงหน้าที่ความรับผิดชอบหรือตำแหน่งงาน (4) ขั้นตอนการเพิกถอนสิทธิของผู้ใช้งาน โดยเพิกถอนสิทธิทันทีเมื่อผู้ใช้งานสิ้นสุดสภาพการเป็นพนักงาน และเมื่อไม่มีความจำเป็นต้องใช้งาน (5) การแบ่งแยกบทบาทหน้าที่ของบุคคลที่เกี่ยวข้องในการจัดสรรสิทธิ เช่น ผู้ร้องขอ (access request) ผู้มีอำนาจอนุมัติ (access authorization) และผู้ดูแลสิทธิการเข้าถึง (access administration) เป็นต้น เพื่อให้สอดคล้องตามหลักการถ่วงดุล (check and balance) ที่ดี (6) กำหนดสิทธิของผู้ใช้งานโดยคำนึงถึงความจำเป็นต้องรู้ (need-to-know) ความจำเป็นต้องใช้งาน (need-to-use) และหลักการแบ่งแยกหน้าที่ความรับผิดชอบ (segregation of duties) (7) จัดทำตารางควบคุมการให้สิทธิ (authorization matrix) ของผู้ใช้งานที่สอดคล้องกับตำแหน่งหน้าที่และความรับผิดชอบ เพื่อใช้เป็นแนวทางการกำหนดสิทธิอย่างถูกต้องเหมาะสม (8) ทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง โดยกำหนดรอบระยะเวลาในการทบทวนสิทธิให้สอดคล้องกับความเสี่ยงและความสำคัญของสิทธิ
5.2 จัดให้มีกระบวนการยืนยันตัวตนผู้ใช้งาน (authentication) ที่เหมาะสมกับความเสี่ยง และป้องกันการปฏิเสธความรับผิด	1. ผู้ประกอบธุรกิจควรจัดให้มีกระบวนการยืนยันตัวตนผู้ใช้งาน (authentication) ที่มีประสิทธิภาพเหมาะสมกับความเสี่ยงของการเข้าถึงระบบโดยไม่ได้รับอนุญาตและความเสี่ยงจากการปฏิเสธความรับผิด โดยครอบคลุมอย่างน้อย ดังนี้ (1) กำหนดวิธีการยืนยันตัวตนผู้ใช้งานที่เหมาะสมกับความเสี่ยง

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. 38/2565	แนวปฏิบัติ
	(2) กรณีที่มีการสร้างรหัสผ่านครั้งแรกสำหรับผู้ใช้งาน ให้มีการจัดส่งรหัสผ่านให้แก่ผู้ใช้งานด้วยวิธีการที่รัดกุมและปลอดภัย และให้ผู้ใช้งานเปลี่ยนแปลงรหัสผ่านทันทีที่ได้รับรหัสดังกล่าว (3) กำหนดให้ผู้ใช้งานตั้งรหัสผ่านที่ซับซ้อนและยากต่อการคาดเดา โดยมีความยาวขั้นต่ำ 8 อักขระ (8 characters) และประกอบด้วยตัวเลขและตัวอักษร ทั้งนี้ ผู้ประกอบธุรกิจอาจพิจารณาเพิ่มความซับซ้อนโดยกำหนดให้รหัสผ่านประกอบด้วยตัวเลข ตัวอักษรพิมพ์ใหญ่ ตัวอักษรพิมพ์เล็ก และอักขระพิเศษ (เช่น “#”) (4) กำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดพลาดติดต่อกัน ก่อนระงับการเข้าสู่ระบบชั่วคราวหรือวิธีการอื่น ๆ ที่เทียบเท่า เพื่อป้องกันการเข้าใช้งานโดยวิธีเดาสุ่ม (brute force) ทั้งนี้ ในทางปฏิบัติไม่ควรยอมให้ผู้ใช้งานยืนยันตัวตนผิดพลาดติดต่อกันเกิน 10 ครั้ง (5) กำหนดให้ใช้รหัสผ่านที่ไม่ซ้ำกับรหัสที่เคยใช้งานอย่างน้อย 4 ครั้งล่าสุด หรือไม่ซ้ำกับรหัสผ่านที่เคยใช้งานในช่วง 1 ปีที่ผ่านมา (6) กำหนดการตั้งค่าปกติ (default) ให้ไม่แสดงรหัสผ่านบนหน้าจอ ระหว่างที่ผู้ใช้งานใส่รหัสผ่าน (7) มีวิธีจัดเก็บข้อมูลรหัสผ่านที่ปลอดภัย เพื่อป้องกันการล่วงรู้หรือแก้ไขเปลี่ยนแปลง รวมทั้งไม่จัดเก็บข้อมูลรหัสผ่านใน folder เดียวกันกับ folder ที่จัดเก็บข้อมูลของแอปพลิเคชัน (8) กำหนดให้ผู้ใช้งานรับผิดชอบการใช้งานบัญชีผู้ใช้งาน (user ID) และการรักษาความปลอดภัยสิ่งที่ใช้ยืนยันตัวตน (authenticator) เช่น รหัสผ่าน รหัสที่ใช้ครั้งเดียว (one-time password) เป็นต้น รวมทั้งข้อมูลส่วนบุคคลที่อาจนำมาใช้เพื่อขอเปลี่ยนแปลงข้อมูลบัญชีผู้ใช้งาน เพื่อป้องกันการใช้งานจากผู้ไม่หวังดี 2. *[ความเสี่ยงสูง] ผู้ประกอบธุรกิจควรมีระบบอัตโนมัติในการตรวจสอบและแจ้งเตือนพฤติกรรมการยืนยันตัวตนที่ผิดปกติหรือต้องสงสัย เช่น การเข้าสู่ระบบจากเครื่องคอมพิวเตอร์ต้นทางพร้อมกันหลายเครื่อง หรือการเข้าสู่ระบบจากเครื่องคอมพิวเตอร์ต้นทางที่มีความแตกต่างกันด้านสถานที่ทางภูมิศาสตร์ภายในระยะเวลาอันสั้น เป็นต้น*

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. 38/2565	แนวปฏิบัติ
5.3 กำหนดมาตรการควบคุม จำกัด และติดตามการใช้งานบัญชี privileged user (privileged user management) ดังนี้ 5.3.1 มี MFA เมื่อเข้าใช้งานและเปลี่ยนรหัสผ่านสำหรับระบบปฏิบัติการและระบบฐานข้อมูลที่เกี่ยวข้องกับระบบ IT ที่มีนัยสำคัญ 5.3.2 กรณีผู้ประกอบธุรกิจมีข้อจำกัดสำหรับ MFA สามารถใช้วิธีการอื่นใดที่เทียบเท่าทดแทน และจัดให้มีการประเมินความเสี่ยงและพิจารณาแนวทางควบคุมความเสี่ยงก่อนดำเนินการเพื่อขออนุมัติยกเว้น (exception)	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]
5.3.3 มีการควบคุมและติดตามตรวจสอบการใช้งานบัญชี privileged user อย่างเข้มงวด	1. ผู้ประกอบธุรกิจควรจัดให้มีการควบคุมและติดตามการใช้งานบัญชี privileged user ดังนี้ (1) ควบคุมดูแลการให้สิทธิโดยจำกัดตามบทบาทหน้าที่ และความจำเป็นในการใช้งาน (2) จำกัดจำนวนบัญชี privileged user ให้มีจำนวนน้อยที่สุดหรือเท่าที่จำเป็น (3) มีกระบวนการขอใช้งานบัญชี privileged user และการอนุมัติโดยผู้มีอำนาจ (4) ทบทวนบัญชีผู้ใช้งาน privileged user อย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง (5) กำหนดนโยบายหรือมาตรการยืนยันตัวตนของบัญชี privileged user ที่เข้มงวดกว่าบัญชีผู้ใช้งานทั่วไป (6) จัดเก็บบันทึกการยืนยันตัวตนและการเข้าถึง (authentication log และ access log) และการดำเนินงาน (activity log) ของบัญชี privileged user อย่างเหมาะสม (7) สอบทานบันทึกการยืนยันตัวตนและการเข้าถึง (authentication log และ access log) และการดำเนินงาน (activity log) ของบัญชี privileged user หลังเสร็จสิ้นการใช้งาน หรือสอบทานอย่างสม่ำเสมอตามรอบระยะเวลาที่เหมาะสมกับความเสี่ยง โดยควรสอบทานอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าการใช้งานสิทธิเป็นไปอย่างเหมาะสม

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. 38/2565	แนวปฏิบัติ
	(8) มีเครื่องมือหรือกระบวนการป้องกันการเข้าใช้งานบัญชี 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	1. ในการกำหนดวิธีการเข้ารหัสที่ปลอดภัย ผู้ประกอบธุรกิจควรดำเนินการอย่างน้อย ดังนี้ (1) กำหนดความรับผิดชอบของหน่วยงานหรือบุคลากรที่เกี่ยวข้อง (2) กำหนดมาตรฐานวิธีการเข้ารหัสข้อมูล (cryptographic algorithm) ให้เป็นไปตามมาตรฐานสากล และมีความมั่นคงปลอดภัยเหมาะสมกับระดับความสำคัญของข้อมูล (3) การกำหนดรอบระยะเวลาในการทบทวนมาตรฐานวิธีการเข้ารหัสข้อมูล เพื่อให้มั่นใจว่าวิธีการเข้ารหัสข้อมูลที่ใช้งานอยู่ยังมีความมั่นคงเพียงพอในการรักษาความปลอดภัยของข้อมูล
6.2 กำหนดการบริหารจัดการกุญแจเข้ารหัส โดยจัดให้มีมาตรการการควบคุมตั้งแต่การสร้างและติดตั้งกุญแจเข้ารหัส	1. การสร้างและติดตั้งกุญแจเข้ารหัส ผู้ประกอบธุรกิจควรดำเนินการอย่างน้อย ดังนี้ (1) ควบคุมสภาพแวดล้อมและกระบวนการในการสร้างกุญแจเข้ารหัสที่รัดกุมปลอดภัย เช่น เลือกใช้ผู้ให้บริการออก

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. 38/2565	แนวปฏิบัติ
การจัดเก็บและสำรองกุญแจเข้ารหัส ไปจนถึงการเพิกถอนหรือทำลายกุญแจเข้ารหัส	ใบรับรอง (certification authority) ที่น่าเชื่อถือ และมีการทำลายข้อมูลที่อาจหลงเหลือภายหลังการสร้างกุญแจเข้ารหัสแล้วเสร็จ เพื่อป้องกันการเข้าถึงหรือกู้คืนกุญแจเข้ารหัสข้อมูลโดยไม่ได้รับอนุญาต เป็นต้น (2) กำหนดสิทธิการเข้าถึงกุญแจเข้ารหัสให้สามารถเข้าถึงได้โดยผู้ที่ได้รับอนุญาตเท่านั้น (3) กำหนดความยาวของกุญแจเข้ารหัสที่เพียงพอในการป้องกันการถูกถอดรหัส (decrypt) โดยผู้ไม่หวังดี เช่น การโจมตีแบบ brute force เป็นต้น (4) แลกเปลี่ยนกุญแจเข้ารหัส (key exchange) ผ่านกระบวนการและช่องทางที่ปลอดภัย 2. การจัดเก็บและการสำรองกุญแจเข้ารหัส ผู้ประกอบธุรกิจควรดำเนินการอย่างน้อย ดังนี้ (1) มีการรักษาความปลอดภัยในการจัดเก็บกุญแจเข้ารหัสทั้งด้าน physical และ logical เช่น การใช้อุปกรณ์ Hardware Security Module (HSM) หรืออุปกรณ์ที่ทำหน้าที่ในลักษณะเดียวกัน เป็นต้น (2) มีการสำรองข้อมูลกุญแจเข้ารหัส โดยวิธีการเก็บรักษาข้อมูลกุญแจเข้ารหัสชุดสำรองต้องมีการรักษาความปลอดภัยในระดับเดียวกับกุญแจเข้ารหัสชุดหลัก 3. การเพิกถอนหรือทำลายกุญแจเข้ารหัส ผู้ประกอบธุรกิจควรดำเนินการอย่างน้อย ดังนี้ (1) กำหนดเกณฑ์และแนวทางในการเปลี่ยนและเพิกถอนกุญแจเข้ารหัส เช่น กรณีกุญแจเข้ารหัสหมดอายุการใช้งาน หรือไม่ปลอดภัย เป็นต้น (2) กำหนดกระบวนการทำลายกุญแจ เพื่อให้มั่นใจว่าจะไม่สามารถนำกุญแจนั้นมาใช้งานได้อีก 4. ผู้ประกอบธุรกิจควรจัดเก็บข้อมูลบันทึกเหตุการณ์กิจกรรมสำคัญที่เกี่ยวกับกุญแจเข้ารหัส เช่น การสร้างกุญแจ การสำรองกุญแจ การเข้าถึงหรือใช้งานกุญแจ และการเพิกถอนกุญแจ เป็นต้น
6.3 กำหนดมาตรการการควบคุมกุญแจเข้ารหัสที่ให้บริการโดยบุคคลภายนอก ซึ่งต้องตรวจสอบเพื่อให้มั่นใจได้ว่ากุญแจการเข้ารหัสที่สร้างขึ้นไม่มีการนำมาใช้ร่วมกับบุคคลอื่น	1. กรณีที่ผู้ประกอบธุรกิจไม่สามารถสร้างกุญแจเข้ารหัสด้วยตนเองได้ หรือมีความจำเป็นต้องใช้กุญแจเข้ารหัสที่ให้บริการโดยบุคคลภายนอก ผู้ประกอบธุรกิจควรดำเนินการเพื่อให้มั่นใจได้ว่ากุญแจเข้ารหัสที่ให้บริการโดยบุคคลภายนอกไม่มีการนำมาใช้งานร่วมกับผู้ใช้บริการรายอื่นและมีความมั่นคงปลอดภัย โดยพิจารณาเงื่อนไขหรือรายละเอียดของการให้บริการ ดังนี้ (1) ประเภทของกุญแจเข้ารหัส (2) รายละเอียดของระบบ และกระบวนการบริหารจัดการกุญแจเข้ารหัส

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. 38/2565	แนวปฏิบัติ
	(3) ข้อแนะนำการใช้งานและการควบคุมการเข้ารหัสข้อมูล
6.4 กำหนดกระบวนการรองรับกรณีเกิดการรั่วไหลของกุญแจเข้ารหัส	1. ผู้ประกอบธุรกิจควรกำหนดกิจกรรมที่ต้องดำเนินการเมื่อเกิดการรั่วไหลของกุญแจเข้ารหัส เช่น การติดต่อหน่วยงานและผู้ที่เกี่ยวข้องกับชุดข้อมูลที่ใช้กุญแจเข้ารหัสชุดดังกล่าว การตรวจสอบชุดข้อมูลที่มีความเสี่ยงในการรั่วไหล การเปลี่ยนหรือเพิกถอนกุญแจการเข้ารหัสข้อมูล เป็นต้น
2.7 การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (physical and environmental security)	
ส่วนที่ 7 การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (physical and environmental security) ผู้ประกอบธุรกิจต้องจัดให้มีการรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อมของทรัพย์สินด้าน IT พร้อมทั้งมีระบบการป้องกัน และกระบวนการบำรุงรักษาฮาร์ดแวร์และระบบสาธารณูปโภค (facilities) ที่เกี่ยวข้องกับ IT เพื่อให้สามารถป้องกันความเสียหายต่อทรัพย์สินด้าน IT ที่จัดเก็บอยู่ในศูนย์คอมพิวเตอร์หลัก ศูนย์คอมพิวเตอร์สำรอง และศูนย์คอมพิวเตอร์จากบุคคลภายนอก (co-location)	1. ผู้ประกอบธุรกิจควรออกแบบศูนย์คอมพิวเตอร์ และพื้นที่ที่เกี่ยวข้องกับระบบ IT ที่มีนัยสำคัญ โดยคำนึงถึงความเสี่ยงจากภัยธรรมชาติและภัยคุกคามจากมนุษย์ เช่น มีกำแพงหรือรั้วที่มั่นคง และมีระยะห่างของศูนย์คอมพิวเตอร์สำรองและศูนย์คอมพิวเตอร์หลักที่เพียงพอ เป็นต้น 2. ผู้ประกอบธุรกิจควรมีการบริหารจัดการสิทธิการเข้าถึงศูนย์คอมพิวเตอร์ และพื้นที่ที่เกี่ยวข้องกับระบบ IT ที่มีนัยสำคัญ โดยครอบคลุมการดำเนินการอย่างน้อย ดังนี้ (1) ให้สิทธิการเข้าถึงตามหลักความจำเป็น (2) อนุมัติสิทธิการเข้าถึงโดยผู้มีอำนาจ (3) ปรับปรุง/ยกเลิกสิทธิการเข้าถึง ทันทีที่พนักงานลาออกหรือเปลี่ยนหน้าที่ความรับผิดชอบ (4) ทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง 3. ผู้ประกอบธุรกิจควรจัดให้มีวิธีการยืนยันตัวตนผู้เข้า-ออกศูนย์คอมพิวเตอร์ และพื้นที่ที่เกี่ยวข้องกับระบบ IT ที่มีนัยสำคัญ เช่น การใช้ access card door เป็นต้น พร้อมทั้งบันทึกเหตุการณ์การเข้า-ออก ทั้งนี้ สำหรับพื้นที่ที่มีความเสี่ยงสูง ผู้ประกอบธุรกิจอาจพิจารณาใช้วิธีการยันตัวตนแบบ MFA เช่น ใช้ access card door ร่วมกับรหัสผ่านส่วนตัว (PIN) เป็นต้น 4. ผู้ประกอบธุรกิจควรมีมาตรการควบคุมการเข้า-ออกศูนย์คอมพิวเตอร์ และพื้นที่ที่เกี่ยวข้องกับระบบ IT ที่มีนัยสำคัญ สำหรับพนักงานที่ไม่ได้มีหน้าที่ปฏิบัติงานประจำหรือผู้ที่เข้าถึงแบบชั่วคราว โดยจัดให้มีการอนุมัติจากผู้มีอำนาจ การบันทึกเหตุการณ์เข้า-ออก และมีการติดตามและควบคุม (escort) อย่างใกล้ชิด ตลอดระยะเวลาปฏิบัติงานในพื้นที่ดังกล่าว 5. ผู้ประกอบธุรกิจควรจัดให้มีระบบรักษาความมั่นคงปลอดภัยให้กับศูนย์คอมพิวเตอร์ เช่น ระบบกล้องวงจรปิด ระบบแจ้งเตือนและ

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. 38/2565	แนวปฏิบัติ
	ระงับอัคคีภัย ระบบควบคุมแรงดันและกระแสไฟฟ้า ระบบสำรองไฟฟ้า (uninterrupted power supply) และระบบควบคุมอุณหภูมิและความชื้น เป็นต้น พร้อมทั้งมีการบำรุงรักษาอย่างสม่ำเสมอ 6. ผู้ประกอบธุรกิจควรจัดให้มีมาตรการรองรับการทำงานผิดพลาดของระบบสาธารณูปโภคของศูนย์คอมพิวเตอร์ เช่น ระบบไฟฟ้า ระบบโทรคมนาคมและระบบปรับอากาศ เป็นต้น 7. ผู้ประกอบธุรกิจควรจัดเก็บอุปกรณ์คอมพิวเตอร์ที่สำคัญ เช่น เครื่องแม่ข่าย และอุปกรณ์เครือข่าย เป็นต้น ไว้ในพื้นที่ที่มีการควบคุมอย่างปลอดภัย 8. ผู้ประกอบธุรกิจควรจัดให้มีมาตรการป้องกันสายเคเบิลและสายไฟของศูนย์คอมพิวเตอร์จากการขัดขวางการทำงาน หรือการทำให้เสียหาย และบำรุงรักษาอย่างสม่ำเสมอ 9. ผู้ประกอบธุรกิจควรจัดให้มีการดูแลและบำรุงรักษาทรัพย์สินด้าน IT ประเภทฮาร์ดแวร์อย่างถูกวิธี เพื่อให้อยู่ในสภาพครบถ้วนสมบูรณ์และพร้อมใช้งาน 10. ผู้ประกอบธุรกิจควรแยกพื้นที่จุดรับส่งของ (delivery and loading area) ซึ่งเป็นพื้นที่ส่วนที่ต้องมีการเข้าถึงโดยบุคคลภายนอกออกจากพื้นที่ที่มีการประมวลผลข้อมูล 11. ผู้ประกอบธุรกิจควรควบคุมมิให้มีการนำทรัพย์สินด้าน IT ประเภทฮาร์ดแวร์ออกนอกพื้นที่โดยมิได้รับอนุญาต 12. ก่อนการยกเลิกการใช้งานหรือจำหน่ายทรัพย์สินด้าน IT ประเภทฮาร์ดแวร์ เช่น hard disk, switch, firewall และ router เป็นต้น ผู้ประกอบธุรกิจควรจัดเก็บทรัพย์สินในพื้นที่ปลอดภัย และตรวจสอบให้มั่นใจว่าได้มีการลบ ย้าย ทำลายข้อมูลสำคัญและข้อมูลการปรับแต่ง (configuration) หรือปรับค่าดังกล่าวกลับไปสู่ค่าตั้งต้น (factory reset) ด้วยวิธีการที่ไม่สามารถกู้คืนได้อีก
2.8 การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้าน IT (IT operations security)	
ส่วนที่ 8 การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้าน IT (IT operations security) ผู้ประกอบธุรกิจต้องมีมาตรการรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้าน IT เพื่อให้การปฏิบัติงานเกี่ยวกับการประมวลผลข้อมูลมีความถูกต้องและมั่นคงปลอดภัย	

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. 38/2565	แนวปฏิบัติ
โดยต้องครอบคลุมการบริหารจัดการอย่างน้อยในเรื่องดังนี้	
2.8.1 การบริหารจัดการการตั้งค่าระบบ (system configuration management)	
8.1 การบริหารจัดการการตั้งค่าระบบ (system configuration management) โดยมีกระบวนการในการควบคุมการตั้งค่าระบบ และสอบทานการตั้งค่าระบบอย่างสม่ำเสมอ เพื่อให้การตั้งค่าระบบเป็นไปอย่างถูกต้องและปลอดภัย	1. ผู้ประกอบธุรกิจควรกำหนดมาตรฐานการตั้งค่าด้านความมั่นคงปลอดภัย (security configuration standard) หรือ security basedline อย่างเป็นลายลักษณ์อักษร เพื่อใช้ในการตั้งค่าระบบปฏิบัติการ ระบบฐานข้อมูล และอุปกรณ์เครือข่าย โดยคำนึงถึงเรื่อง ดังนี้ (1) การลบบัญชีผู้ใช้งานตั้งต้น (default user) หรือการเปลี่ยนแปลงรหัสผ่านตั้งต้น (default password) (2) การใช้วิธีการยืนยันตัวตนที่มีความรัดกุมปลอดภัย (3) การกำหนดบริการ แอปพลิเคชัน และพอร์ตการเชื่อมต่อเท่าที่จำเป็น (4) การจัดเก็บข้อมูลบันทึกเหตุการณ์ (log) (5) การปรับปรุงเวอร์ชันของซอฟต์แวร์หรือ firmware ให้เป็นปัจจุบัน 2. ผู้ประกอบธุรกิจควรทบทวนและปรับปรุงมาตรฐานการตั้งค่าด้านความมั่นคงปลอดภัย (security configuration standard) หรือ security basedline ให้เป็นปัจจุบันอย่างสม่ำเสมอ 3. ผู้ประกอบธุรกิจควรตั้งค่าด้านความมั่นคงปลอดภัยของระบบปฏิบัติการ ระบบฐานข้อมูล และอุปกรณ์เครือข่ายตามมาตรฐานที่กำหนดไว้ ก่อนการนำไปใช้งาน 4. ผู้ประกอบธุรกิจควรสอบทานการตั้งค่าด้านความมั่นคงปลอดภัยของระบบปฏิบัติการ ระบบฐานข้อมูล และอุปกรณ์เครือข่ายอย่างสม่ำเสมอ และทุกครั้งที่มีการเปลี่ยนแปลงระบบและอุปกรณ์ดังกล่าวอย่างมีนัยสำคัญ เพื่อให้สอดคล้องกับมาตรฐานที่กำหนดไว้
2.8.2 การบริหารจัดการการเปลี่ยนแปลง (change management)	
8.2 การบริหารจัดการการเปลี่ยนแปลง(change management) อย่างรัดกุมเพียงพอเพื่อให้การเปลี่ยนแปลงเป็นไปตามวัตถุประสงค์ที่กำหนดไว้อย่างถูกต้องครบถ้วน และป้องกันการเปลี่ยนแปลงโดยที่ไม่ได้รับอนุญาต	1. ผู้ประกอบธุรกิจควรกำหนดกระบวนการบริหารจัดการการเปลี่ยนแปลงอย่างเป็นลายลักษณ์อักษรเพื่อควบคุมการเปลี่ยนแปลงโครงสร้างพื้นฐานด้าน IT ระบบ IT และขั้นตอนการปฏิบัติงานที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัย 2. ผู้ประกอบธุรกิจควรกำหนดหลักเกณฑ์การจัดประเภทการเปลี่ยนแปลงตามระดับความสำคัญหรือความจำเป็นเร่งด่วน และกำหนดขั้นตอนสำหรับการเปลี่ยนแปลงแต่ละประเภท เช่น (1) การเปลี่ยนแปลงมาตรฐานที่ได้รับอนุมัติเป็นการทั่วไป (standard change)

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. 38/2565	แนวปฏิบัติ
	(2) การเปลี่ยนแปลงที่ต้องขออนุมัติตามกระบวนการปกติ (normal change) (3) การเปลี่ยนแปลงที่ต้องดำเนินการอย่างเร่งด่วน (emergency change) เป็นต้น 3. ผู้ประกอบธุรกิจควรกำหนดคณะกรรมการหรือผู้บริหารที่ทำหน้าที่อนุมัติการเปลี่ยนแปลงแต่ละประเภท 4. ผู้ประกอบธุรกิจควรแบ่งแยกหน้าที่ (segregation of duties) ผู้ที่เกี่ยวข้องในกระบวนการการเปลี่ยนแปลง เพื่อไม่ให้บุคคลใดบุคคลหนึ่งสามารถปฏิบัติงานได้ตั้งแต่เริ่มต้นจนจบกระบวนการการเปลี่ยนแปลง เช่น ผู้มีสิทธิร้องขอ ผู้ที่มีอำนาจในการอนุมัติการเปลี่ยนแปลง ผู้ที่สามารถดำเนินการเปลี่ยนแปลงระบบ เป็นต้น 5. ผู้ประกอบธุรกิจควรจัดให้มีคำขอการเปลี่ยนแปลง (change request) และการอนุมัติการเปลี่ยนแปลง เป็นลายลักษณ์อักษร เพื่อเป็นหลักฐานแสดงให้เห็นว่าการเปลี่ยนแปลงได้ผ่านการพิจารณาจากเจ้าของข้อมูล เจ้าของระบบ หรือผู้มีอำนาจตามสิทธิที่กำหนดไว้ โดยคำขอการเปลี่ยนแปลงควรระบุเหตุผลความจำเป็นและผลกระทบที่อาจเกิดขึ้นจากการเปลี่ยนแปลง 6. ผู้ประกอบธุรกิจควรจัดให้มีระบบหรือทะเบียนในการจัดเก็บคำขอเปลี่ยนแปลงและเอกสารรายละเอียดที่เกี่ยวข้อง เพื่อใช้ควบคุมการปฏิบัติงานตั้งแต่ต้นจนจบกระบวนการ และสามารถใช้ในการติดตามและสอบทานการปฏิบัติงาน 7. กรณีที่การเปลี่ยนแปลงมีผลกระทบต่อการปฏิบัติงาน ผู้ประกอบธุรกิจควรสื่อสารให้ผู้เกี่ยวข้องรับทราบการเปลี่ยนแปลงเพื่อให้สามารถปฏิบัติงานได้อย่างถูกต้อง 8. ผู้ประกอบธุรกิจควรจัดให้มีแผนการถอยกลับสู่สภาพเดิม (fallback procedure) หากเกิดข้อผิดพลาดจากการเปลี่ยนแปลง เช่น การจัดเก็บเวอร์ชันของระบบก่อนการเปลี่ยนแปลงไว้ เป็นต้น 9. กรณีการเปลี่ยนแปลงที่ต้องดำเนินการอย่างเร่งด่วน (emergency change) ควรมีกระบวนการพิจารณาความเสี่ยงและผลกระทบรวมถึงขออนุมัติจากผู้บริหารที่ได้รับมอบหมายให้สามารถตัดสินใจได้กรณีเร่งด่วน โดยภายหลังดำเนินการ ให้มีการรายงานผู้บริหารที่เกี่ยวข้อง และคณะกรรมการบริหารจัดการการเปลี่ยนแปลง (change advisory board : CAB) (ถ้ามี) รับทราบโดยเร็ว 10. *[ความเสี่ยงสูง] ผู้ประกอบธุรกิจควรกำหนดบทบาทหน้าที่และความรับผิดชอบของคณะกรรมการบริหารจัดการการเปลี่ยนแปลง (change advisory board : CAB) ซึ่งควรประกอบด้วยผู้บริหารจากหน่วยงาน IT หน่วยงานธุรกิจ และหน่วยงานผู้ใช้งานที่เกี่ยวข้อง เพื่อทำหน้าที่พิจารณาเหตุผลความจำเป็นและประเมินผลกระทบก่อนอนุมัติให้ดำเนินการเปลี่ยนแปลง เพื่อป้องกันการแก้ไขเปลี่ยนแปลงโดยไม่ได้รับอนุญาตและไม่ให้เกิดผลกระทบที่อาจเกิดกับระบบที่เกี่ยวข้อง*

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. 38/2565	แนวปฏิบัติ
	นอกจากนี้ CAB ควรมีการติดตามผลหลังการเปลี่ยนแปลงระบบ (post implementation review) เพื่อให้มั่นใจได้ว่าการเปลี่ยนแปลงนั้นเป็นไปตามวัตถุประสงค์ที่กำหนด
2.8.3 การบริหารจัดการขีดความสามารถของระบบ IT (capacity management)	
8.3 การบริหารจัดการขีดความสามารถของระบบ 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. ผู้ประกอบธุรกิจควรมีกระบวนการหรือเครื่องมือติดตามตัวชี้วัดการใช้ทรัพยากรด้าน IT (threshold and trigger) เช่น ประสิทธิภาพการทำงาน (performance) ความหน่วง (latency) ขีดความสามารถ (capacity) และปริมาณทรัพยากรที่ใช้งาน (utilization) เป็นต้น เพื่อให้เจ้าหน้าที่ที่เกี่ยวข้องสามารถรับทราบปัญหาอย่างทันท่วงที และดำเนินการรับมืออย่างเหมาะสม 4. ผู้ประกอบธุรกิจควรจัดทำรายงานความเพียงพอของทรัพยากรด้าน IT นำเสนอต่อคณะกรรมการที่ได้รับมอบหมาย หรือผู้บริหารระดับสูงที่เกี่ยวข้องรับทราบอย่างสม่ำเสมอ เพื่อให้มีการกำกับดูแลความพร้อมใช้และความเพียงพอของระบบในการรองรับการให้บริการทางธุรกิจได้อย่างต่อเนื่อง และสามารถพิจารณาแนวทางลดความเสี่ยงได้อย่างทันการณ์
2.8.4 การรักษาความมั่นคงปลอดภัยของเครื่องแม่ข่าย (server) และอุปกรณ์ที่ใช้ปฏิบัติงาน (endpoint)	
8.4 การรักษาความมั่นคงปลอดภัยของเครื่องแม่ข่าย (server) และอุปกรณ์ที่ใช้ปฏิบัติงาน (endpoint) เพื่อไม่ให้ถูกใช้เป็นช่องทางที่ทำให้ข้อมูลสำคัญรั่วไหล หรือมีการเข้าใช้งานระบบ IT โดยไม่ได้รับอนุญาต	1. ผู้ประกอบธุรกิจควรกำหนดมาตรการรักษาความปลอดภัยของเครื่องแม่ข่าย และอุปกรณ์ที่ใช้ในการปฏิบัติงาน เพื่อให้สามารถป้องกันและตรวจจับโปรแกรมไม่ประสงค์ดี (malware) และภัยคุกคามทางไซเบอร์ โดยครอบคลุมการดำเนินการอย่างน้อย ดังนี้ (1) มีกระบวนการหรือเครื่องมือในการควบคุมและติดตามไม่ให้มีการติดตั้งซอฟต์แวร์ที่ไม่ได้รับอนุญาต (2) ติดตั้งเครื่องมือในการป้องกันและตรวจจับโปรแกรมไม่ประสงค์ดี เช่น anti-virus, anti-malware และ intrusion prevention system เป็นต้น โดยปรับปรุง (update) เครื่องมือที่ใช้งานให้เป็นปัจจุบันอย่างสม่ำเสมอ เพื่อให้เท่าทันในการป้องกันภัยคุกคามใหม่ ๆ

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. 38/2565	แนวปฏิบัติ
	(3) ควบคุมการใช้งานหรือการเชื่อมต่อสื่อบันทึกข้อมูลพกพา (removable media) เช่น กำหนดแนวทางการควบคุมการใช้งาน universal serial bus (USB) หรือ external hard disk เป็นต้น 2. ผู้ประกอบธุรกิจควรจัดให้มีการควบคุมป้องกันทรัพย์สินด้าน IT ประเภทฮาร์ดแวร์ระหว่างที่ไม่มีผู้ใช้งาน (unattended user equipment) ให้มีความปลอดภัย โดยครอบคลุมการดำเนินการอย่างน้อย ดังนี้ (1) ควบคุมเอกสาร อุปกรณ์ที่ใช้ปฏิบัติงาน หรือสื่อบันทึกข้อมูลต่าง ๆ ที่มีการจัดเก็บข้อมูลสำคัญหรือข้อมูลลับ ไม่ให้วางทิ้งไว้บนโต๊ะทำงานหรือสถานที่ไม่ปลอดภัยในขณะที่ไม่ได้ใช้งาน (clear desk) (2) ควบคุมหน้าจอคอมพิวเตอร์ไม่ให้มีข้อมูลสำคัญปรากฏในขณะที่ไม่ได้ใช้งาน (clear screen) เช่น การตัดออกจากระบบ (session time out) หรือการล็อคหน้าจอ (lock screen) อัตโนมัติ เมื่อไม่มีการใช้งานถึงระยะเวลาที่กำหนด เป็นต้น 3. ผู้ประกอบธุรกิจควรกำหนดมาตรการรักษาความมั่นคงปลอดภัยในการใช้งานเทคโนโลยี virtualization โดยครอบคลุม hypervisor, host operating system และ guest operating system พร้อมทั้งมีการรักษาความปลอดภัยของข้อมูลที่เกิดจากการใช้เทคโนโลยี virtualization เช่น virtual machine image และ snapshot เป็นต้น อย่างเหมาะสม 4. *[ความเสี่ยงสูง] ผู้ประกอบธุรกิจควรติดตั้งระบบหรือเครื่องมือตรวจจับภัยคุกคามซึ่งสามารถวิเคราะห์พฤติกรรมผิดปกติ ตรวจจับภัยคุกคาม และจัดเก็บข้อมูลหลักฐาน เพื่อช่วยให้สามารถตอบสนองต่อภัยคุกคามทางไซเบอร์ได้อย่างทันการณ์ เช่น การติดตั้งระบบ endpoint detection & response (EDR) หรือระบบ host-based intrusion prevention system (HIPS) เป็นต้น* 5. *[ความเสี่ยงสูง] ผู้ประกอบธุรกิจควรกำหนดกระบวนการหรือเครื่องมือป้องกันข้อมูลสำคัญรั่วไหล (data leak prevention) จากการส่งข้อมูลออกโดยไม่ได้รับอนุญาตผ่านช่องทางต่าง ๆ เช่น อุปกรณ์พกพาและสื่อบันทึกข้อมูล อีเมล และโปรแกรมการประชุมและสื่อสารผ่านสื่ออิเล็กทรอนิกส์ (online communication tool) เป็นต้น* 6. *[ความเสี่ยงสูง] กรณีที่มีฟังก์ชันให้ปิดการใช้งานพอร์ตการเชื่อมต่อของเครื่องแม่ข่าย และอุปกรณ์ที่ใช้ในการปฏิบัติงาน ให้ปิดพอร์ตการเชื่อมต่อภายนอกทั้งหมด (เช่น พอร์ต USB เป็นต้น) ที่รองรับการเชื่อมต่อกับสื่อบันทึกข้อมูลพกพา (removable media) โดยให้เปิดใช้งานตามความจำเป็นและได้รับอนุมัติโดยผู้มีอำนาจเท่านั้น*

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. 38/2565	แนวปฏิบัติ
2.8.5 การกำหนดนโยบายและมาตรการรักษาความปลอดภัยสำหรับการปฏิบัติงานจากเครือข่ายภายนอก (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) เพื่อเข้าถึงระบบ IT ที่มีนัยสำคัญ ผู้ประกอบธุรกิจควรจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่รัดกุมเพียงพอเหมาะสมกับระบบ IT และข้อมูลที่ถูกเข้าถึง โดยครอบคลุมอย่างน้อยดังนี้ (1) มาตรการรักษาความมั่นคงปลอดภัยด้านกายภาพที่เหมาะสม รัดกุมเพียงพอกับขอบเขตการปฏิบัติงาน สำหรับพื้นที่ปฏิบัติงานนอกองค์กร (2) การอนุมัติการปฏิบัติงานจากเครือข่ายภายนอกโดยผู้มีอำนาจหรือผู้บริหารที่เกี่ยวข้อง (3) การกำหนดสิทธิการเข้าถึงข้อมูลและระบบ IT จากเครือข่ายภายนอกเท่าที่จำเป็น พร้อมทั้งมีการทบทวนสิทธิอย่างสม่ำเสมอ (4) การยืนยันตัวตน (authencitation) ของพนักงานที่ปฏิบัติงานจากเครือข่ายภายนอกด้วยวิธีการที่รัดกุมปลอดภัย เช่น การใช้วิธียืนยันตัวตนแบบหลายปัจจัย (multi-factor authentication : MFA) และการเข้าใช้งานผ่านอุปกรณ์ที่อนุญาตเท่านั้น เป็นต้น (5) มาตรการป้องกันความเสี่ยงจากการใช้อุปกรณ์ที่ใช้ในการปฏิบัติงานจากเครือข่ายภายนอก เป็นช่องทางในการแพร่กระจายของโปรแกรมไม่ประสงค์ดี (malware) และการรั่วไหลของข้อมูลสำคัญ (6) มาตรการป้องกันข้อมูลที่เป็นความลับหรือมีความสำคัญ (sensitive data) เช่น การยืนยันตัวตนก่อนใช้งานอุปกรณ์ (lock screen) การเข้ารหัสข้อมูลบนอุปกรณ์ที่ใช้ในการปฏิบัติงาน หรือการลบข้อมูลจากระยะไกล (remote wipe-out) เป็นต้น 2. ในการปฏิบัติงานที่มีการใช้อุปกรณ์เคลื่อนที่ (mobile device) เพื่อเข้าถึงระบบ IT ที่มีนัยสำคัญ ผู้ประกอบธุรกิจควรจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่รัดกุมเพียงพอเหมาะสมกับระบบ IT และข้อมูลที่ถูกเข้าถึง โดยครอบคลุมอย่างน้อยดังนี้ (1) การลงทะเบียนอุปกรณ์เคลื่อนที่ก่อนการใช้งาน โดยมีการทบทวนทะเบียนดังกล่าวอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนอุปกรณ์ เพื่อให้มั่นใจได้ว่าอุปกรณ์เคลื่อนที่ดังกล่าวมีความความมั่นคงปลอดภัยเพียงพอ ทั้งนี้ ผู้ประกอบธุรกิจอาจใช้ระบบหรือเทคโนโลยีการลงทะเบียนอื่นทดแทนได้ หากพิจารณาแล้วเห็นว่าเหมาะสม (2) มาตรการป้องกันข้อมูลที่เป็นความลับหรือมีความสำคัญ (sensitive data) เช่น การยืนยันตัวตนก่อนใช้งานอุปกรณ์ (lock

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. 38/2565	แนวปฏิบัติ
	screen) การเข้ารหัสข้อมูลบนอุปกรณ์ที่ใช้ปฏิบัติงาน หรือการลบข้อมูลจากระยะไกล (remote wipe-out) เป็นต้น (3) *[ความเสี่ยงสูง] การจัดให้มีเครื่องมือในการบริหารจัดการอุปกรณ์เคลื่อนที่ที่มีความสามารถในการบริหารจัดการชุดโปรแกรมแก้ไขช่องโหว่ด้านความมั่นคงปลอดภัย (security patch) การตั้งค่าอุปกรณ์ (configuration) และการบริหารจัดการด้านการป้องกันไวรัสและโปรแกรมไม่พึงประสงค์* 3. กรณีที่อนุญาตให้พนักงานสามารถใช้อุปกรณ์ส่วนตัวของพนักงาน (bring your own device : BYOD) ผู้ประกอบธุรกิจควรพิจารณาความเสี่ยงที่เกี่ยวข้อง และจัดให้มีมาตรการควบคุมความเสี่ยงอย่างเหมาะสม โดยครอบคลุมอย่างน้อยดังนี้ (1) การกำหนดหลักเกณฑ์การอนุญาตให้ใช้งาน BYOD (2) การควบคุมการใช้ BYOD ให้สามารถเข้าถึงเครือข่ายสื่อสาร ข้อมูล และระบบ IT เท่าที่จำเป็น (3) การยืนยันตัวตนเพื่อปลดล็อคในการเข้าถึง BYOD เช่น การใช้รหัสผ่าน และการสแกนลายนิ้วมือ เป็นต้น (4) ในกรณีที่เครื่องคอมพิวเตอร์ส่วนตัวของพนักงาน (personal computer, notebook) สามารถเชื่อมต่อเข้าสู่ระบบเครือข่ายภายในหรือข้อมูลสำคัญ ควรจัดให้มีการติดตั้งซอฟต์แวร์ป้องกันโปรแกรมไม่ประสงค์ดี (anti-virus/ anti-malware) และปรับปรุงให้ทันสมัย (update) อยู่เสมอ (5) การห้ามใช้อุปกรณ์เคลื่อนที่ (tablet, smartphone) ที่ถูกปรับแต่ง (rooted หรือ jailbroken) เข้าถึงระบบ IT 4. *[ความเสี่ยงสูง] กรณีที่อนุญาตให้พนักงานสามารถใช้อุปกรณ์ส่วนตัวของพนักงาน (bring your own device : BYOD) ผู้ประกอบธุรกิจควรจัดให้มีกระบวนการหรือเครื่องมือตรวจสอบ วิเคราะห์ และติดตามความเสี่ยงของอุปกรณ์ที่นำมาใช้งาน เช่น ระบบบริหารจัดการอุปกรณ์เคลื่อนที่ (mobile device management : MDM) เป็นต้น*
2.8.6 การสำรองข้อมูล (data backup)	
8.6 การสำรองข้อมูล (data backup) ที่สำคัญด้วยวิธีการและความถี่ที่เหมาะสม เพื่อให้ข้อมูลสำรองมีสภาพพร้อมใช้งานสอดคล้องกับเป้าหมายการกู้คืนระบบ IT ในกรณีที่ระบบ IT และข้อมูลหลักเกิดเหตุขัดข้องหรือได้รับความเสียหาย โดยต้องมีการทดสอบข้อมูลสำรองและกระบวนการกู้คืน	1. ผู้ประกอบธุรกิจควรกำหนดมาตรฐานหรือวิธีปฏิบัติในการสำรองข้อมูลที่สอดคล้องกับระยะเวลาเป้าหมายในการกู้คืนระบบ IT (Recovery Time Objective : RTO) และระยะเวลาเป้าหมายสูงสุดที่ยอมให้ข้อมูลเสียหาย (Recovery Point Objective : RPO) โดยอย่างน้อยควรมีรายละเอียดครอบคลุม (1) ข้อมูลที่ต้องสำรอง (2) ความถี่หรือรอบเวลาในการสำรองข้อมูล

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. 38/2565	แนวปฏิบัติ
ข้อมูลอย่างน้อยปีละ 1 ครั้ง	(3) ขั้นตอนและวิธีการสำรองข้อมูล (4) ขั้นตอนและวิธีการกู้คืนข้อมูล (5) สถานที่และวิธีการเก็บรักษาสื่อบันทึกข้อมูล 2. ผู้ประกอบธุรกิจควรจัดเก็บสื่อบันทึกข้อมูลสำรอง พร้อมทั้งสำเนาขั้นตอนหรือวิธีปฏิบัติงานต่าง ๆ ไว้นอกศูนย์คอมพิวเตอร์หลักหรือนอกสถานที่ปฏิบัติงานหลัก โดยสถานที่ดังกล่าวควรจัดให้มีมาตรการรักษาความปลอดภัยเทียบเคียงกับศูนย์คอมพิวเตอร์หลักหรือสถานที่ปฏิบัติงานหลัก 3. ผู้ประกอบธุรกิจควรจัดให้มีการสอบทานการสำรองข้อมูล และทดสอบข้อมูลสำรองอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่าการสำรองข้อมูลมีความครบถ้วนถูกต้อง พร้อมใช้งาน และปลอดภัย 4. ในกรณีที่จำเป็นต้องจัดเก็บข้อมูลเป็นระยะเวลานาน ผู้ประกอบธุรกิจควรคำนึงถึงวิธีการนำข้อมูลกลับมาใช้งานในอนาคตด้วยหากมีความจำเป็น เช่น เมื่อมีการจัดเก็บข้อมูลลงในสื่อบันทึกข้อมูลใด ให้มีการจัดเก็บอุปกรณ์และโปรแกรมที่ใช้อ่านสื่อบันทึกข้อมูลนั้นด้วย เป็นต้น
2.8.7 การจัดเก็บข้อมูลบันทึกเหตุการณ์การใช้งานเกี่ยวกับระบบ IT (log)	
8.7 การจัดเก็บข้อมูลบันทึกเหตุการณ์การใช้งานเกี่ยวกับระบบ IT (log) อย่างครบถ้วนและเพียงพอ เพื่อให้สามารถใช้เป็นหลักฐานการทำธุรกรรมทางอิเล็กทรอนิกส์ และสามารถติดตามและตรวจสอบการเข้าถึงและใช้งานข้อมูลและระบบ IT ย้อนหลังได้ ตามที่กฎหมายกำหนด	1. ผู้ประกอบธุรกิจควรจัดเก็บข้อมูลบันทึกเหตุการณ์ (log) ด้วยวิธีการที่ปลอดภัย โดยมีรายละเอียดครบถ้วนเพียงพอที่จะใช้เป็นหลักฐานในการตรวจสอบที่สามารถระบุตัวบุคคลผู้กระทำได้ และจัดเก็บเป็นระยะเวลาอย่างน้อย 90 วัน หรือจัดเก็บตามกฎหมายที่เกี่ยวข้องกำหนด ประกอบด้วยรายการหลักฐานอย่างน้อย ดังนี้ (1) บันทึกเหตุการณ์การเข้า-ออกศูนย์คอมพิวเตอร์ และพื้นที่ที่เกี่ยวข้องกับระบบ IT ที่มีนัยสำคัญ (physical access log) (2) บันทึกการยืนยันตัวตนและการเข้าถึง (authentication log และ access log) ของเครื่องแม่ข่าย ระบบงาน อุปกรณ์เครือข่าย และข้อมูลที่มีความสำคัญ โดยรวมถึงความพยายามในการเข้าถึง (log-in attempt) (3) บันทึกการดำเนินงาน (activity log) ที่สำคัญ โดยอย่างน้อยครอบคลุม (ก) การเปลี่ยนแปลงแก้ไขโครงสร้างข้อมูล (ข) การเปลี่ยนแปลงแก้ไข และลบข้อมูลสำคัญ (ค) การเปลี่ยนแปลงแก้ไขการตั้งค่าของระบบ (system configuration)

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. 38/2565	แนวปฏิบัติ
	(ง) การเปลี่ยนแปลงแก้ไขบัญชี และสิทธิของผู้ใช้งาน (จ) การใช้งานอินเทอร์เน็ตผ่านระบบเครือข่ายของผู้ประกอบธุรกิจ (ฉ) การทำงานของ firewall (network firewall log) (4)[2] หลักฐานการติดต่อสนทนาผ่านช่องทางอิเล็กทรอนิกส์ (electronic messaging) ของบุคคลที่สามารถเข้าถึงข้อมูลภายใน (access person) โดยมีรายละเอียดขั้นต่ำประกอบด้วยบัญชีผู้ใช้งาน / วันเวลาที่เข้าใช้งาน / ข้อมูลการติดต่อตลอดระยะเวลาการสนทนา และจัดเก็บเป็นระยะเวลาอย่างน้อย 6 เดือน (5) บันทึกการทำธุรกรรม (transaction log) ควรมีระยะเวลาจัดเก็บขั้นต่ำ 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. ผู้ประกอบธุรกิจควรมีการควบคุมค่าเวลาของเครื่องแม่ข่าย ระบบงาน และอุปกรณ์เครือข่ายให้ตรงกับเครื่องแม่ข่าย network time protocol : NTP (clock synchronization) เพื่อให้ค่าเวลาในการบันทึกเหตุการณ์มีความถูกต้องในลักษณะ real-time ซึ่งเครื่อง NTP ควรรับสัญญาณให้ตรงกับสัญญาณนาฬิกาจากแหล่งที่มีความน่าเชื่อถือ (เช่น Stratum 1 จากสถาบันมาตรวิทยาแห่งชาติ และกรมอุทกศาสตร์ กองทัพเรือ เป็นต้น) ทั้งนี้ ในกรณีผู้ประกอบธุรกิจที่เป็นสมาชิกของตลาดหลักทรัพย์ ควรกำหนดระบบเวลาของอุปกรณ์และระบบ IT ที่เกี่ยวกับการซื้อขายหลักทรัพย์และการชำระราคาให้ตรงกับเวลาอ้างอิงของระบบซื้อขายหลักทรัพย์ของตลาดหลักทรัพย์ เพื่อให้

[2] จัดเก็บเฉพาะบุคคลที่สามารถเข้าถึงข้อมูลภายใน (access person) ของผู้ประกอบธุรกิจนายหน้าซื้อขายหลักทรัพย์ การค้าหลักทรัพย์ หรือการจัดจำหน่ายหลักทรัพย์ ซึ่งมิได้จำกัดเฉพาะหลักทรัพย์อันเป็นตราสารแห่งหนี้หรือหน่วยลงทุน ตัวแทนซื้อขายสัญญาซื้อขายล่วงหน้าและผู้ประกอบธุรกิจจัดการกองทุนรวมหรือกองทุนส่วนบุคคล เท่านั้น
ทั้งนี้ นิยามว่าด้วย access person ให้เป็นไปตามประกาศแนวปฏิบัติว่าด้วยการกำหนดนโยบาย มาตรการ และระบบงานที่เกี่ยวกับการกระทำที่อาจมีความขัดแย้งทางผลประโยชน์กับลูกค้า

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. 38/2565	แนวปฏิบัติ
	การตรวจสอบธุรกรรมที่ไม่เหมาะสมทั้งหมดเป็นไปอย่างถูกต้องและมีประสิทธิภาพ 3. ผู้ประกอบธุรกิจควรจัดเก็บ log ที่เกี่ยวข้องกับข้อมูลส่วนบุคคล เพื่อใช้ตรวจสอบกิจกรรมของผู้ใช้งานและใช้เป็นหลักฐานหากเกิดเหตุการณ์การเข้าถึง ใช้งาน แก้ไขเปลี่ยนแปลง หรือเปิดเผยข้อมูลส่วนบุคคลที่ไม่เหมาะสม โดยสอดคล้องกับ กฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง เช่น กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล เป็นต้น 4. ผู้ประกอบธุรกิจควรจัดเก็บ log ของอุปกรณ์สำคัญไว้ที่เครื่องแม่ข่ายที่ใช้จัดเก็บ log (logging server) ที่แยกเฉพาะ หรือใช้วิธีการที่เทียบเคียงซึ่งสามารถป้องกันการเปลี่ยนแปลง แก้ไข หรือทำลาย log ได้ โดยมีมาตรการรักษาความปลอดภัยอย่างน้อย ดังนี้ (1) กำหนดหน้าที่และความรับผิดชอบผู้ที่สามารถเข้าถึง log ตามความจำเป็น (2) มีกระบวนการยืนยันตัวตนและตรวจสอบสิทธิในการเข้าถึง log ที่เข้มงวด (3) ติดตั้งเครื่องแม่ข่าย หรืออุปกรณ์ที่ใช้จัดเก็บ log ให้อยู่ในโซนเครือข่ายที่มีความมั่นคงปลอดภัย
2.8.8 การติดตามดูแลระบบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (security monitoring)	
8.8 การติดตามดูแลระบบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (security monitoring) โดยมีกระบวนการหรือเครื่องมือป้องกันและตรวจจับเหตุการณ์ผิดปกติด้าน IT โปรแกรมไม่ประสงค์ดี (malware) หรือภัยคุกคามทางไซเบอร์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยต่อระบบ IT ที่มีนัยสำคัญ	1. ผู้ประกอบธุรกิจควรจัดให้มีกระบวนการหรือเครื่องมือในการตรวจจับเหตุการณ์ผิดปกติที่อาจส่งผลกระทบต่อความปลอดภัยของระบบ IT ที่มีนัยสำคัญอย่างทันท่วงที เช่น กระบวนการหรือเครื่องมือในการสอบทาน log เป็นต้น เพื่อให้รับทราบความผิดปกติหรือภัยคุกคาม และสามารถดำเนินการป้องกันหรือรับมือได้อย่างเหมาะสม 2. ผู้ประกอบธุรกิจควรจัดให้มีกระบวนการหรือเครื่องมือในการรับข้อมูลข่าวสารเกี่ยวกับภัยคุกคาม (cyber threat intelligence) เพื่อให้สามารถติดตามและวิเคราะห์ภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น และสามารถดำเนินการป้องกันหรือรับมือได้อย่างเหมาะสม 3. *[ความเสี่ยงสูง] ผู้ประกอบธุรกิจควรมีหน่วยงานที่รับผิดชอบในการเฝ้าระวัง ติดตาม วิเคราะห์ ประสานงาน และเป็นศูนย์กลางในการจัดการเหตุภัยคุกคาม เช่น หน่วยงาน security operations center (SOC) เป็นต้น* 4. *[ความเสี่ยงสูง] ผู้ประกอบธุรกิจควรมีระบบรวบรวมข้อมูลเหตุการณ์จากแหล่งข้อมูลต่าง ๆ เช่น อุปกรณ์เครือข่าย ระบบงาน และระบบรักษาความปลอดภัยเครือข่าย เป็นต้น เพื่อใช้ในกระบวนการเชื่อมโยงข้อมูล (log correlation) และวิเคราะห์เหตุการณ์ผิดปกติด้านความมั่นคงปลอดภัยสารสนเทศ* 5. *[ความเสี่ยงสูง] ผู้ประกอบธุรกิจควรจัดให้มีกระบวนการหรือเครื่องมือตรวจจับการแก้ไขเปลี่ยนแปลงไฟล์หรือการตั้งค่า*

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. 38/2565	แนวปฏิบัติ
	(configuration) บนระบบ IT หรืออุปกรณ์ที่มีนัยสำคัญ เช่น การทำ file integrity monitoring (FIM) / file integrity check บนเครื่องแม่ข่ายที่เชื่อมต่ออินเทอร์เน็ต และการตรวจจับการเปลี่ยนแปลงแก้ไขการตั้งค่าอุปกรณ์เครือข่ายที่สำคัญ (เช่น firewall) เป็นต้น 6. *[ความเสี่ยงสูง] ผู้ประกอบธุรกิจควรจัดให้มีกระบวนการหรือเครื่องมือติดตามและแจ้งเตือนพฤติกรรมต้องสงสัยของผู้ใช้งาน เช่น พฤติกรรมการใช้งานเครือข่ายที่ผิดปกติ การถ่ายโอนข้อมูลเป็นจำนวนมาก การเข้าใช้งานในระบบงานในช่วงเวลาผิดปกติ หรือการเข้าใช้งานจากเครื่องคอมพิวเตอร์ที่ไม่เคยมีการใช้งาน เป็นต้น*
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	1. ผู้ประกอบธุรกิจควรกำหนดขอบเขตและความถี่ของการประเมินช่องโหว่ทางเทคนิคให้ครอบคลุมทุกระบบงานตามระดับความเสี่ยง ทั้งนี้ สำหรับระบบ IT ที่มีนัยสำคัญและระบบ IT ที่เชื่อมต่อกับเครือข่ายสาธารณะทุกระบบต้องได้รับการประเมินช่องโหว่อย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงระบบดังกล่าวอย่างมีนัยสำคัญ 2. ผู้ประกอบธุรกิจควรประเมินความเสี่ยงของช่องโหว่ที่ตรวจพบและกำหนดระยะเวลาแก้ไขที่เหมาะสมกับความเสี่ยง 3. ผู้ประกอบธุรกิจควรรายงานผลการประเมินช่องโหว่ไปยังผู้รับผิดชอบ รวมถึงติดตามให้มีการแก้ไขช่องโหว่ภายในระยะเวลาที่กำหนดไว้ โดยนำเสนอความคืบหน้าของการดำเนินการต่อคณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมาย
2.8.10 การทดสอบการเจาะระบบ (penetration test)	
8.10 การทดสอบการเจาะระบบ (penetration test) 8.10.1 ผู้ประกอบธุรกิจต้องจัดให้มีการทดสอบการเจาะระบบดังนี้	1. ผู้ประกอบธุรกิจควรจัดให้มีการทดสอบการเจาะระบบที่ครอบคลุมระบบงาน (application system) และระบบเครือข่ายที่มีช่องทางเชื่อมต่อกับเครือข่ายสาธารณะ (internet facing) อย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงระบบดังกล่าว

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. 38/2565	แนวปฏิบัติ
(1) ระบบงาน (application system) และระบบเครือข่ายที่มีการเชื่อมต่อกับเครือข่ายสาธารณะ (internet facing) (1.1) อย่างน้อยปีละ 1 ครั้ง และ (1.2) ทุกครั้งที่มีการเปลี่ยนแปลงระบบดังกล่าวอย่างมีนัยสำคัญ (2) ระบบอื่น ๆ นอกจาก (1) จัดให้มีการประเมินความเสี่ยงจากการบุกรุกผ่านระบบเครือข่ายคอมพิวเตอร์ที่ใช้สื่อสารภายในองค์กร เพื่อกำหนดขอบเขตการทดสอบการเจาะระบบและทดสอบการเจาะระบบตามความเหมาะสม	อย่างมีนัยสำคัญ โดยระบบอื่น ๆ ควรจัดให้มีการประเมินความเสี่ยงจากการบุกรุกผ่านระบบเครือข่ายคอมพิวเตอร์ที่ใช้สื่อสารภายในองค์กร เพื่อกำหนดขอบเขตการทดสอบการเจาะระบบตามความเหมาะสม 2. ผู้ประกอบธุรกิจควรประเมินความเสี่ยงของช่องโหว่ที่ตรวจพบและกำหนดระยะเวลาแก้ไขที่เหมาะสมกับความเสี่ยง 3. ผู้ประกอบธุรกิจควรรายงานสรุปผลการทดสอบการเจาะระบบไปยังผู้รับผิดชอบที่เกี่ยวข้อง เช่น หน่วยงานเจ้าของระบบ หน่วยงานกำกับการปฏิบัติงาน หรือหน่วยงานตรวจสอบภายใน เป็นต้น รวมถึงติดตามให้มีการแก้ไขช่องโหว่ภายในระยะเวลาที่กำหนดไว้ โดยนำเสนอความคืบหน้าของการดำเนินการต่อคณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมาย 4. ผู้ประกอบธุรกิจควรรวบรวมและวิเคราะห์ช่องโหว่ทางเทคนิคที่ตรวจพบ เพื่อช่วยในการกำหนดมาตรการรักษาความมั่นคงปลอดภัยของระบบ IT ที่จะมีการพัฒนาในอนาคต
8.10.2 การทดสอบการเจาะระบบข้างต้น ต้องดำเนินการโดยผู้เชี่ยวชาญภายในหรือภายนอกที่เป็นอิสระจากเจ้าของระบบ	1. ผู้ประกอบธุรกิจควรกำหนดให้ผู้ที่ทดสอบการเจาะระบบ เป็นผู้มีความรู้ความสามารถและเชี่ยวชาญในการทดสอบการเจาะระบบ โดยเป็นอิสระจากหน่วยงานเจ้าของระบบ และเป็นอิสระจากการพัฒนาระบบดังกล่าว 2. *[ความเสี่ยงสูง] ผู้ประกอบธุรกิจควรกำหนดคุณสมบัติให้ผู้ทดสอบการเจาะระบบ (penetration tester) ที่ทำการทดสอบการเจาะระบบ IT ที่มีนัยสำคัญได้รับการรับรองและมีประกาศนียบัตร (accreditations and certifications) ที่เป็นที่ยอมรับในอุตสาหกรรม เช่น* *(1) ประกาศนียบัตรการรับรองจากสถาบัน Council for Registered Ethical Security Testers (CREST) เช่น CREST Registered Penetration Tester, CREST Certified Web Application Tester, CREST Certified Infrastructure Tester เป็นต้น* *(2) ประกาศนียบัตรการรับรองจากสถาบัน Offensive Security เช่น Offensive Security Certified Professional (OSCP), Offensive Security Wireless Professional (OSWP), Offensive Security Certified Expert (OSCE), Offensive Security Exploitation Expert (OSEE) และ Offensive Security Web Expert (OSWE) เป็นต้น* *(3) ประกาศนียบัตรการรับรองจากสถาบัน Global Information Assurance Certification (GIAC) เช่น GIAC Certified*

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. 38/2565	แนวปฏิบัติ
	Incident Handler (GCIH), GIAC Mobile Device Security Analyst (GMOB), GIAC penetration tester (GPEN), GIAC Exploit Researcher and Advanced Penetration Tester (GXPN), GIAC Assessing and Auditing Wireless Networks (GAWN) และ GIAC Web Application Penetration Tester (GWAPT) เป็นต้น *โดยผู้ประกอบธุรกิจอาจพิจารณาประกาศนียบัตรการรับรองอื่นที่เทียบเคียงกับข้างต้นได้*
8.10.3 ในกรณีที่มีการตรวจพบช่องโหว่ ผู้ประกอบธุรกิจต้องดำเนินการแก้ไข และป้องกันภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นอย่างทันท่วงที เพื่อขจัดความเสี่ยงจากช่องโหว่ดังกล่าว	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]
8.10.4 ผู้ประกอบธุรกิจต้องจัดเก็บรายงานการดำเนินการตาม 8.10 เป็นระยะเวลาไม่น้อยกว่า 2 ปีนับแต่วันที่จัดทำเอกสารนั้น โดยต้องจัดเก็บไว้ในลักษณะที่พร้อมให้สำนักงานสามารถเรียกดูและตรวจสอบได้โดยไม่ชักช้า	1. ผู้ประกอบธุรกิจควรจัดให้มีรายงานผลการทดสอบการเจาะระบบซึ่งครอบคลุมรายละเอียดที่สำคัญ เช่น ขอบเขตการทดสอบ ช่วงเวลาที่ทดสอบ ผู้ทำการทดสอบ วิธีการและขั้นตอนดำเนินการทดสอบการเจาะระบบ และช่องโหว่ที่ตรวจพบ รวมถึงแผนการปรับปรุงแก้ไขช่องโหว่ตามระดับความเสี่ยง เป็นต้น โดยจัดเก็บรายงานดังกล่าวเป็นระยะเวลาไม่น้อยกว่า 2 ปีนับแต่วันที่จัดทำเอกสารนั้น โดยจัดเก็บไว้ในลักษณะที่พร้อมให้สำนักงานสามารถเรียกดูและตรวจสอบได้โดยไม่ชักช้า
8.10.5 ผู้ประกอบธุรกิจต้องนำส่งรายงานผลการทดสอบการเจาะระบบโดยไม่ชักช้าเมื่อได้รับการแจ้งจากสำนักงาน	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]
2.8.11 การบริหารจัดการโปรแกรมแก้ไขช่องโหว่ (patch management)	
8.11 การบริหารจัดการโปรแกรมแก้ไขช่องโหว่ (patch management) โดยจัดให้มีกระบวนการควบคุมการติดตั้งโปรแกรมแก้ไขช่องโหว่บนระบบและอุปกรณ์ เพื่อลดความเสี่ยงที่จะถูกโจมตีในอนาคต	1. ผู้ประกอบธุรกิจควรมีการกำหนดมาตรฐานและระเบียบวิธีปฏิบัติในการบริหารจัดการโปรแกรมแก้ไขช่องโหว่ (patch) ที่ครอบคลุมการดำเนินการอย่างน้อย ดังนี้ (1) การประเมินความเสี่ยงและความจำเป็นในการติดตั้ง patch (2) การกำหนดกรอบระยะเวลาการติดตั้ง patch โดยคำนึงถึงความจำเป็นและความเสี่ยงจากการถูกโจมตีจากช่องโหว่ (3) การตรวจสอบความถูกต้องและการทดสอบ patch ก่อนการดำเนินการติดตั้งบนระบบที่ให้บริการจริง เพื่อป้องกันผลกระทบที่ไม่พึงประสงค์จากการติดตั้ง patch ทั้งนี้ ในกรณีที่มีข้อจำกัดในการทดสอบ patch ผู้ประกอบธุรกิจอาจพิจารณาการควบคุมอื่น ๆ ทดแทน

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. 38/2565	แนวปฏิบัติ
	2. การติดตั้ง patch บนระบบงานจริง ควรดำเนินการตามกระบวนการบริหารจัดการการเปลี่ยนแปลง (change management) ที่กำหนดไว้ เพื่อป้องกันความเสี่ยงและข้อผิดพลาดจากการปฏิบัติงาน 3. กรณีมีเหตุที่ผู้ผลิตระบบงานหรืออุปกรณ์ยังไม่แจ้งการปรับปรุง security patch อย่างเป็นทางการเพื่อปิดช่องโหว่ใหม่ ๆ ที่เพิ่งค้นพบ ผู้ประกอบธุรกิจควรปฏิบัติตามคำแนะนำของผู้พัฒนาระบบ เจ้าของผลิตภัณฑ์ หรือผู้เชี่ยวชาญด้านความมั่นคงปลอดภัย หรือจัดให้มีมาตรการควบคุมทดแทน เพื่อลดความเสี่ยงจากการถูกโจมตีผ่านช่องโหว่นั้น ๆ 4. *[ความเสี่ยงสูง] ผู้ประกอบธุรกิจควรจัดให้มีเครื่องมือที่ใช้ติดตาม patch ด้านการรักษาความปลอดภัย (patch monitoring tool) ที่ยังไม่มีการติดตั้งบนระบบปฏิบัติการ (operation system) และระบบฐานข้อมูล (database system) ที่สำคัญของผู้ประกอบธุรกิจ*
2.9 การรักษาความมั่นคงปลอดภัยเกี่ยวกับระบบเครือข่ายสื่อสาร (communication system security)	
ส่วนที่ 9 การรักษาความมั่นคงปลอดภัยเกี่ยวกับระบบเครือข่ายสื่อสาร (communication system security) ผู้ประกอบธุรกิจต้องมีการรักษาความมั่นคงปลอดภัยเกี่ยวกับระบบเครือข่ายสื่อสารอย่างเหมาะสม เพื่อให้ระบบเครือข่ายสื่อสารและข้อมูลที่รับส่งผ่านระบบเครือข่ายสื่อสารมีความมั่นคงปลอดภัย สามารถป้องกันการบุกรุกหรือภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น รวมทั้งพร้อมให้บริการได้อย่างต่อเนื่อง	1. ผู้ประกอบธุรกิจควรจัดให้มีการรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร โดยมีการดำเนินการอย่างน้อย ดังนี้ (1) ออกแบบเครือข่ายสื่อสารที่มีการแบ่งแยกเครือข่ายอย่างเหมาะสม โดยคำนึงถึงระดับความสำคัญของระบบงาน (application system) ระดับความสำคัญของข้อมูล รวมถึงความจำเป็นในการเชื่อมต่อจากระบบงานอื่น ๆ หรือจากภายนอกองค์กร (2) จัดให้มีการควบคุมการเชื่อมต่อของระบบงาน (application system) ที่สำคัญอย่างเข้มงวด (3) การแบ่งแยกเครือข่ายให้มีความรัดกุมปลอดภัย ควรดำเนินการ ดังนี้ (ก) แบ่งแยกเครือข่ายภายใน (private network) และเครือข่ายภายนอก (public network) ออกจากกัน (ข) แบ่งแยกเครือข่ายของระบบ IT ที่มีนัยสำคัญ เครือข่ายสำหรับการปฏิบัติงานของพนักงาน และเครือข่ายสำหรับการใช้งานทั่วไป/เครือข่ายสำหรับบุคคลภายนอก (guest network) ออกจากกัน (ค) จุดที่มีการแบ่งแยกเครือข่ายที่มีความสำคัญและมีความเสี่ยง ควรติดตั้งอุปกรณ์รักษาความปลอดภัยเครือข่ายที่มีความสามารถในการควบคุมและคัดกรองข้อมูล (traffic) ที่รับส่งผ่านเครือข่าย เพื่อป้องกันและตรวจจับการบุกรุกของไวรัสหรือมัลแวร์ต่าง ๆ (4) ควบคุม และจำกัดให้มีเฉพาะอุปกรณ์ที่ได้รับอนุญาตเท่านั้นที่สามารถเชื่อมต่อกับระบบเครือข่ายภายในได้

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. 38/2565	แนวปฏิบัติ
	(5) เปิดใช้งานช่องทางเชื่อมต่อ (port) ตามความจำเป็นเท่านั้น ในกรณีที่ต้องใช้งาน port ที่ถูกปิดไว้ ควรกำหนดกระบวนการในการขออนุมัติจากผู้มีอำนาจ และจัดให้มีการควบคุมอย่างเหมาะสม (6) ติดตามสถานะความพร้อมใช้งานของระบบเครือข่ายให้อยู่ในระดับ service level agreement (SLA) ที่กำหนด (7) จัดให้มีระบบหรือมาตรการป้องกันการโจมตีผ่านเครือข่ายสาธารณะที่เหมาะสมตามความเสี่ยง เช่น การใช้อุปกรณ์การรักษาความปลอดภัย intrusion prevention system (IPS) และการป้องกันการโจมตีแบบ DDoS (DDoS protection) เป็นต้น (8) *[ความเสี่ยงสูง] ผู้ประกอบธุรกิจควรมีการติดตั้งอุปกรณ์รักษาความปลอดภัยเครือข่ายเพื่อคัดกรอง traffic ในระดับ application ในจุดที่มีการเชื่อมต่อกับเครือข่ายสาธารณะ เช่น การใช้ web application firewall (WAF) เป็นต้น* (9) *[ความเสี่ยงสูง] การเข้าถึงอุปกรณ์เครือข่าย และอุปกรณ์รักษาความปลอดภัยเพื่อบริหารจัดการหรือตั้งค่า (config) ต่าง ๆ ควรทำผ่านเครือข่ายเฉพาะที่แยกออกจากเครือข่ายปกติ เพื่อลดความเสี่ยงในการเปลี่ยนแปลงอุปกรณ์เครือข่าย และอุปกรณ์รักษาความปลอดภัยเครือข่ายโดยบุคคลที่ไม่ได้รับอนุญาต* 2. ผู้ประกอบธุรกิจควรจัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศที่รับส่งผ่านระบบเครือข่ายสื่อสาร (information transfer) โดยมีการดำเนินการอย่างน้อย ดังนี้ (1) กำหนดแนวปฏิบัติที่ดีในการรับส่งข้อมูลสารสนเทศผ่านช่องทางการสื่อสารอิเล็กทรอนิกส์ประเภทต่าง ๆ (2) นำเทคนิคการเข้ารหัสข้อมูลมาใช้ในการรับส่งข้อมูลสารสนเทศที่เป็นความลับและมีความสำคัญ (3) มีมาตรการป้องกันข้อมูลที่เป็นความลับหรือมีความสำคัญที่รับส่งในรูปแบบของไฟล์แนบ (attachment files) และการส่งต่ออีเมลแบบอัตโนมัติออกสู่ภายนอกองค์กร 3. ผู้ประกอบธุรกิจควรจัดให้มีการรักษาความมั่นคงปลอดภัยสำหรับการใช้งานระบบรับส่งข้อมูลสารสนเทศผ่านระบบเครือข่ายสื่อสาร (ระบบ electronic messaging) โดยมีการดำเนินการอย่างน้อย ดังนี้ (1) จัดให้มีมาตรการป้องกันการเปลี่ยนแปลงแก้ไข ทำความเสียหาย หรือเข้าถึงข้อมูลในระบบ electronic messaging โดยไม่ได้รับอนุญาต (2) มีกระบวนการยืนยันตัวตนผู้ใช้งานที่เหมาะสม โดยใช้วิธีการที่เข้มงวดรัดกุมในกรณีที่ใช้งานระบบ electronic messaging

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. 38/2565	แนวปฏิบัติ
	ผ่านเครือข่ายสาธารณะ (3) กรณีที่มีการใช้งานระบบ electronic messaging ที่ให้บริการโดยบุคคลภายนอก เช่น โปรแกรมสนทนาผ่านระบบอิเล็กทรอนิกส์ (instant messaging) ระบบเครือข่ายสังคมออนไลน์ (social networking) หรือโปรแกรมเรียกใช้แฟ้มข้อมูลร่วมกัน (file sharing) เป็นต้น ผู้ประกอบธุรกิจควรจัดให้มีการควบคุมดูแลอย่างเหมาะสมเพียงพอ และคำนึงถึงการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องอย่างเคร่งครัด (4) จัดให้มีมาตรการคัดกรอง (filter) อีเมลที่มีความเสี่ยงต่อการเกิดภัยคุกคามทางไซเบอร์ เช่น อีเมลที่มีไฟล์แนบชนิด .exe เป็นต้น (5) *[ความเสี่ยงสูง] ผู้ประกอบธุรกิจควรจัดให้มีกระบวนการหรือเครื่องมือจำลองสภาพแวดล้อมเสมือน (secure container / virtual environment) เพื่อวิเคราะห์พฤติกรรมการโจมตีจากข้อมูล และไฟล์แนบในอีเมลของผู้ใช้งาน เช่น การใช้งานเครื่องมือประเภท sandbox และระบบ advanced threat protection (ATP) เป็นต้น*
2.10 การบริหารจัดการโครงการด้าน IT (IT project management) การจัดหา พัฒนา และบำรุงรักษาระบบ IT (system acquisition, development and maintenance)	
ส่วนที่ 10 การบริหารจัดการโครงการด้าน IT (IT project management) การจัดหา พัฒนา และบำรุงรักษาระบบ IT (system acquisition, development and maintenance) ผู้ประกอบธุรกิจต้องมีการบริหารจัดการโครงการด้าน IT และมีการจัดหา พัฒนา รวมถึงบำรุงรักษาระบบ IT เพื่อให้มั่นใจว่ามีการรักษาความมั่นคงปลอดภัยตลอดวงจรชีวิตของระบบ IT (entire life cycle) ดังนี้	
2.10.1 การบริหารจัดการโครงการด้าน IT (IT project management)	
<u>10.1 บริหารจัดการโครงการด้าน IT (IT project management)</u>	1. ผู้ประกอบธุรกิจควรกำหนดกรอบการบริหารจัดการโครงการ (project management framework) เป็นลายลักษณ์อักษร โดยมีรายละเอียดขั้นต่ำ ดังนี้

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. 38/2565	แนวปฏิบัติ
กำหนดกรอบการบริหารจัดการโครงการ (project management framework) เพื่อให้การบริหารจัดการโครงการด้าน IT ที่มีนัยสำคัญเป็นไปอย่างมีประสิทธิภาพ สามารถส่งมอบโครงการได้อย่างถูกต้อง ครบถ้วนตามแผนงานและบรรลุวัตถุประสงค์ตามเป้าหมายที่กำหนดไว้	(1) โครงสร้างการควบคุมและกำกับดูแลโครงการ (project governance) ที่ชัดเจน เพื่อให้มีการควบคุมดูแลโครงการให้สำเร็จเป็นไปตามแผนงานที่กำหนด โดยพิจารณาการจัดให้มีผู้รับผิดชอบในบทบาทหน้าที่ตามความจำเป็นและความเหมาะสม เช่น (ก) คณะกรรมการกำกับดูแลโครงการ (project steering committee) มีบทบาทหน้าที่และความรับผิดชอบในการกำกับดูแลและติดตามความคืบหน้าของโครงการ รวมทั้งให้คำแนะนำ และพิจารณาตัดสินใจการดำเนินงานในโครงการที่สำคัญ เพื่อให้โครงการสามารถดำเนินการได้ตามแผนที่กำหนดไว้ โดยควรประกอบด้วยผู้บริหารจากหน่วยงานที่เกี่ยวข้อง และเจ้าของโครงการหรือผู้สนับสนุนโครงการ (project owner/project sponsor) (ข) หน่วยงานหรือทีมงานดูแลภาพรวมโครงการ (project management office) มีบทบาทหน้าที่และความรับผิดชอบในการกำหนดรูปแบบ กระบวนการ และเครื่องมือที่เป็นมาตรฐานในการบริหารจัดการและติดตามความคืบหน้าของโครงการ รวมทั้งรายงานภาพรวมโครงการสำคัญของผู้ประกอบธุรกิจ ให้กับคณะกรรมการของผู้ประกอบธุรกิจ และผู้บริหารระดับสูงที่เกี่ยวข้องได้รับทราบ เพื่อให้โครงการบรรลุตามเป้าหมายที่กำหนดไว้ (ค) ผู้จัดการโครงการ (project manager) มีบทบาทหน้าที่และความรับผิดชอบในการบริหารจัดการโครงการให้เป็นไปตามระเบียบขั้นตอนการบริหารจัดการโครงการ เพื่อให้โครงการสามารถส่งมอบได้อย่างถูกต้องครบถ้วนและสำเร็จตามแผนงานที่กำหนด (2) แนวทางการบริหารจัดการโครงการ โดยมีรายละเอียดขั้นต่ำ ดังนี้ (ก) ระเบียบขั้นตอนการบริหารจัดการโครงการ ครอบคลุมตั้งแต่ก่อนเริ่มโครงการ การดำเนินการและควบคุมโครงการ การปิดโครงการ และการสอบทานโครงการ (ข) ปัจจัยและเกณฑ์ในการประเมินหรือจัดระดับความสำคัญของโครงการที่ชัดเจน รวมถึงขอบเขตอำนาจหน้าที่ในการอนุมัติและกำกับดูแลโครงการตามระดับความสำคัญของโครงการ (ค) เอกสารหรือสิ่งส่งมอบในแต่ละขั้นตอนอย่างชัดเจน เช่น แผนการดำเนินโครงการ รายงานความคืบหน้า รายงานการปิดโครงการ เป็นต้น 2. การเริ่มโครงการ ผู้ประกอบธุรกิจควรดำเนินการอย่างน้อย ดังนี้

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. 38/2565	แนวปฏิบัติ
	(1) ประเมินความจำเป็นและประโยชน์ที่คาดว่าจะได้รับ รวมถึงความเสี่ยงและผลกระทบที่อาจเกิดขึ้นต่อระบบและหน่วยงานที่เกี่ยวข้องกับโครงการ (2) จัดทำแผนการดำเนินโครงการที่มีรายละเอียดครบถ้วนเพียงพอต่อการบริหารจัดการโครงการอย่างน้อยครอบคลุม (ก) เป้าหมายโครงการ (ข) ทรัพยากร และเทคโนโลยีที่ใช้ (ค) บทบาทหน้าที่และความรับผิดชอบของทีมงานในการดำเนินโครงการ (ง) ขอบเขตและระยะเวลาของการดำเนินโครงการในแต่ละขั้นตอน (จ) ผลงานที่จะส่งมอบในแต่ละขั้นตอน (ฉ) ข้อกำหนดเงื่อนไขที่เกี่ยวข้องกับโครงการ (ถ้ามี) เช่น ข้อกำหนดของผู้ว่าจ้าง ภาระผูกพัน ข้อจำกัด เป็นต้น (3) มีการนำเสนอแผนการดำเนินโครงการ เพื่อขออนุมัติโครงการต่อคณะกรรมการของผู้ประกอบธุรกิจ คณะกรรมการที่ได้รับมอบหมาย หรือผู้บริหารระดับสูง ตามขอบเขตในการอนุมัติที่กำหนดไว้ 3. การดำเนินงานและควบคุมโครงการ ผู้ประกอบธุรกิจควรดำเนินการอย่างน้อย ดังนี้ (1) ติดตามและประเมินการดำเนินโครงการอย่างต่อเนื่องและครอบคลุมขอบเขต ระยะเวลา และทรัพยากรที่วางแผนไว้ (2) ในกรณีที่มีการเปลี่ยนแปลงขอบเขต ระยะเวลาหรือทรัพยากร หรือยกเลิกโครงการ ควรมีการนำเสนอผู้มีอำนาจเพื่อขออนุมัติการเปลี่ยนแปลงหรือยกเลิกโครงการ (3) รายงานความคืบหน้า ปัญหา อุปสรรคและข้อจำกัดในการดำเนินโครงการ ต่อคณะกรรมการกำกับดูแลโครงการหรือผู้บริหารระดับสูงที่ได้รับมอบหมายอย่างสม่ำเสมอ โดยโครงการที่ส่งผลกระทบต่อธุรกิจของผู้ประกอบธุรกิจอย่างมีนัยสำคัญควรได้รับการนำเสนอแก่คณะกรรมการของผู้ประกอบธุรกิจ หรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบธุรกิจด้วย 4. การปิดโครงการ ผู้ประกอบธุรกิจควรดำเนินการอย่างน้อย ดังนี้ (1) สรุปประโยชน์ที่ได้รับจากโครงการเปรียบเทียบกับเป้าหมายที่กำหนด (2) รวบรวมปัญหา อุปสรรคจากการบริหารจัดการโครงการ เพื่อนำมาเป็นสิ่งที่ได้เรียนรู้ (lesson learned) ใช้สำหรับวิเคราะห์

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. 38/2565	แนวปฏิบัติ
	ปรับปรุง และพัฒนากระบวนการหรือเครื่องมือในการบริหารจัดการโครงการต่อไปให้มีประสิทธิภาพมากขึ้น 5. ผู้ประกอบธุรกิจควรสอบทานโครงการที่มีนัยสำคัญ เพื่อให้มั่นใจได้ว่าโครงการสอดคล้องกับเป้าหมายของโครงการ นโยบาย มาตรฐาน ระเบียบและวิธีปฏิบัติของผู้ประกอบธุรกิจ รวมทั้งกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง 6. *[ความเสี่ยงสูง] ผู้ประกอบธุรกิจควรกำหนดให้ผู้สอบทานโครงการที่มีนัยสำคัญมีความเป็นอิสระจากผู้ดำเนินโครงการ เช่น หน่วยงาน project quality assurance เป็นต้น*
2.10.2 การจัดหาระบบ IT (system acquisition)	
10.2 จัดหาระบบ IT (system acquisition) จัดให้มีหลักเกณฑ์ในการจัดหาระบบ IT และผู้ให้บริการ เพื่อให้มั่นใจว่าระบบที่จัดหาสามารถตอบสนองความต้องการทางธุรกิจและความต้องการด้านความมั่นคงปลอดภัย IT โดยคำนึงถึงความยืดหยุ่นในการเปลี่ยนแปลงผู้ให้บริการ การเปลี่ยนแปลงเทคโนโลยี รวมถึงการเปลี่ยนแปลงต่าง ๆ ที่เกี่ยวข้องกับการดำเนินธุรกิจอย่างมีนัยสำคัญ	1. ผู้ประกอบธุรกิจควรจัดให้มีหลักเกณฑ์การคัดเลือกระบบ IT และผู้ให้บริการ เพื่อให้มั่นใจว่าระบบที่จัดหาสามารถตอบสนองความต้องการทางธุรกิจและความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ ซึ่งควรคำนึงถึงเรื่อง ดังนี้ (1) รายละเอียดทั่วไป เช่น เทคโนโลยีที่ใช้ สิทธิการใช้งานซอฟต์แวร์ (software license) ฟังก์ชันการทำงานของระบบ เป็นต้น (2) ความมั่นคงปลอดภัยของระบบ (3) ความน่าเชื่อถือของระบบ IT และผู้ให้บริการ เช่น ฐานะการเงิน ชื่อเสียง และความสามารถด้านเทคนิค เป็นต้น (4) การได้รับการรับรองตามมาตรฐานสากลหรือมาตรฐานด้าน IT ที่เกี่ยวข้องที่ได้รับการยอมรับโดยทั่วไป (certificate) (5) การสนับสนุนและการบำรุงรักษาระบบ (6) การทดสอบการทำงานขั้นต้น (proof of concept) ในกรณีที่เป็นระบบ IT ที่มีนัยสำคัญ (7) มาตรการรองรับหรือการบริหารความเสี่ยง ในกรณีที่ผู้พัฒนาระบบหรือผู้ให้บริการซอฟต์แวร์ไม่ปฏิบัติตามข้อตกลงในการบำรุงรักษาระบบหรือให้การสนับสนุนการดำเนินงานตามที่ตกลงไว้ เช่น จัดให้มีข้อตกลงการรับฝากชุดคำสั่งคอมพิวเตอร์ต้นฉบับ (source code escrow agreement) เพื่อให้มั่นใจได้ว่าผู้ประกอบธุรกิจจะมีสิทธิในการเข้าถึง source code ของระบบหรือซอฟต์แวร์ดังกล่าว เป็นต้น
2.10.3 การพัฒนาระบบ IT (system development)	
10.3 พัฒนาระบบ IT (system development) จัดให้มีมาตรการควบคุมเกี่ยวกับการพัฒนาระบบ IT ในการออกแบบ พัฒนา ทดสอบระบบ และนำระบบขึ้นใช้งาน	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. 38/2565	แนวปฏิบัติ
จริง เพื่อให้มั่นใจว่าระบบมีความถูกต้อง มั่นคงปลอดภัย เชื่อถือได้ พร้อมใช้งาน และมีความยืดหยุ่นเพียงพอจะรองรับการใช้งานได้ สอดคล้องกับแผนการดำเนินธุรกิจ โดยต้องดำเนินการอย่างน้อยดังนี้	
(1) มีการกำหนดรายละเอียดความต้องการของระบบ (requirement) และคุณสมบัติทางเทคนิค (technical specification) ของระบบที่พัฒนา ดังนี้ (1.1) ความมั่นคงปลอดภัย (security) (1.2) สภาพพร้อมใช้งาน (availability) (1.3) ขีดความสามารถที่รองรับ (capacity)	<u>การออกแบบระบบ</u> 1. ผู้ประกอบธุรกิจควรกำหนดให้หน่วยงานธุรกิจที่เกี่ยวข้องมีส่วนร่วมในการกำหนดรายละเอียดความต้องการของระบบ 2. ผู้ประกอบธุรกิจควรจัดทำเอกสารระบุรายละเอียดความต้องการของระบบ (functional requirement และ non-functional requirement) และคุณสมบัติทางเทคนิค (technical specification) ที่ครอบคลุมเรื่อง ดังนี้ (1) ความมั่นคงปลอดภัย (security) ตามนโยบายหรือมาตรฐานที่ผู้ประกอบธุรกิจกำหนด เช่น การควบคุมการเข้าถึง และการเข้ารหัสข้อมูล เป็นต้น (2) ความพร้อมใช้งาน (availability) เช่น การออกแบบให้มีระบบทดแทน high availability หรือ redundancy รวมถึงมีระบบสำรอง (DR strategy) เป็นต้น เพื่อให้ระบบสามารถให้บริการได้อย่างต่อเนื่อง และลดความเสี่ยงที่จุดใดจุดหนึ่งทำให้ระบบเกิดปัญหาหรือล้มเหลวทั้งหมด (single point of failure) (3) ขีดความสามารถที่รองรับ (capacity) ทั้งนี้ เอกสารข้างต้นควรผ่านการสอบทานความถูกต้องครบถ้วนและได้รับอนุมัติจากผู้เกี่ยวข้องก่อนเริ่มพัฒนาระบบ
(2) มีการแบ่งแยกบทบาทหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องในการพัฒนาระบบ เพื่อให้มีการสอบทานก่อนนำระบบขึ้นไปให้บริการจริง	<u>การพัฒนาระบบ</u> 1. ผู้ประกอบธุรกิจควรแบ่งแยกบทบาทหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องในการพัฒนาระบบ (segregation of duty) เพื่อให้มีการสอบทานก่อนนำระบบขึ้นไปให้บริการจริง เช่น แยกผู้พัฒนาระบบ ออกจากผู้นำระบบขึ้นใช้งานจริง เป็นต้น
(3) มีการแบ่งแยกสภาพแวดล้อมของระบบงานที่ใช้สำหรับการพัฒนา (development) และการทดสอบ (testing) ออกจากระบบงานที่ให้บริการจริง (production)	1. ผู้ประกอบธุรกิจควรแบ่งแยกสภาพแวดล้อมของระบบงานที่ใช้สำหรับการพัฒนา (development) และการทดสอบ (testing) ออกจากระบบงานที่ให้บริการจริง (production) เพื่อควบคุมการทดสอบและลดผลกระทบที่อาจเกิดขึ้นต่อระบบงานที่ให้บริการจริง 2. ผู้ประกอบธุรกิจควรจัดให้มีการรักษาความมั่นคงปลอดภัยของเครื่องที่ไม่ได้อยู่บนระบบที่ให้บริการจริง (non-production) ให้เพียงพอกับระดับความเสี่ยงของการเข้าถึงระบบและข้อมูลโดยไม่ได้รับอนุญาต และการรั่วไหลของข้อมูลที่ใช้ทดสอบ

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. 38/2565	แนวปฏิบัติ
	3. ผู้ประกอบธุรกิจควรจัดให้มีการควบคุมไม่ให้มีการติดตั้งเครื่องมือการพัฒนาระบบ (development tools) และเครื่องมือแปลโปรแกรม (compilers) ไว้บนระบบที่ให้บริการจริง เพื่อป้องกันความเสี่ยงที่อาจถูกปรับเปลี่ยนหรือติดตั้งโปรแกรมโดยไม่ได้รับอนุญาต
(4) มีกระบวนการหรือเครื่องมือควบคุมการพัฒนาชุดคำสั่งคอมพิวเตอร์ให้มีความปลอดภัย	1. ผู้ประกอบธุรกิจควรกำหนดมาตรฐานและระเบียบวิธีปฏิบัติในการออกแบบและพัฒนาระบบอย่างปลอดภัย (secure coding) สอดคล้องกับมาตรฐานสากล รวมทั้งควบคุมให้ผู้พัฒนาระบบปฏิบัติตามมาตรฐานและระเบียบวิธีปฏิบัติดังกล่าว 2. ผู้ประกอบธุรกิจควรมีกระบวนการหรือเครื่องมือควบคุมเวอร์ชันของชุดคำสั่งคอมพิวเตอร์ (source code version control) 3. ผู้ประกอบธุรกิจควรสอบทานคำสั่งในการเขียนโปรแกรม (source code review) โดยใช้ระบบอัตโนมัติ (automated review) หรือแบบ manual review ซึ่งดำเนินการโดยบุคคลที่ไม่ใช่ผู้พัฒนาโปรแกรม เมื่อมีการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบ IT ที่มีนัยสำคัญ และมีความเสี่ยงด้านความมั่นคงปลอดภัย เพื่อให้สามารถระบุข้อบกพร่องด้านความมั่นคงปลอดภัย และมีการแก้ไขก่อนนำระบบไปใช้งานจริง 4. *[ความเสี่ยงสูง] ผู้ประกอบธุรกิจควรสอบทานคำสั่งในการเขียนโปรแกรมแบบ manual (manual source code review) โดยผู้เชี่ยวชาญที่มีความเป็นอิสระจากผู้พัฒนาโปรแกรม เมื่อมีการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบ IT ที่มีนัยสำคัญ ซึ่งมีความเสี่ยงด้านความมั่นคงปลอดภัย*

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. 38/2565	แนวปฏิบัติ
(5) มีการทดสอบระบบ IT ที่ได้รับการพัฒนาหรือแก้ไขเปลี่ยนแปลง เพื่อให้มั่นใจได้ว่าระบบดังกล่าวสามารถประมวลผลได้อย่างถูกต้องครบถ้วน และเป็นไปตามความต้องการของผู้ใช้งาน	<u>การทดสอบระบบ</u> 1. ผู้ประกอบธุรกิจควรจัดให้มีการทดสอบระบบก่อนนำไปใช้งานหรือให้บริการจริง เพื่อให้มั่นใจได้ว่าระบบดังกล่าวสามารถทำงานได้อย่างถูกต้อง ปลอดภัย มีประสิทธิภาพ และเป็นไปตามความต้องการของผู้ใช้งาน โดยครอบคลุมอย่างน้อย ดังนี้ (1) ทดสอบการทำงานของแต่ละหน่วย (unit test) (2) ทดสอบการทำงานของระบบและการเชื่อมต่อ (system and integration test) (3) ทดสอบความต้องการของผู้ใช้งาน (user acceptance test) (4) ทดสอบการรักษาความปลอดภัย (security test) ได้แก่ การประเมินช่องโหว่ (vulnerabilities assessment) และการทดสอบการเจาะระบบ (penetration test) ตามความจำเป็น สำหรับระบบใหม่ใด ๆ ที่มีการเชื่อมต่อกับระบบ IT ที่มีนัยสำคัญ เพื่อให้สามารถตรวจพบช่องโหว่และดำเนินการปรับปรุงแก้ไขอย่างเหมาะสมก่อนเริ่มให้บริการจริง 2. ผู้ประกอบธุรกิจควรกำหนดสถานการณ์ที่ใช้ทดสอบ (test scenario) หรือกรณีที่ใช้ทดสอบ (test case) แบบ end-to-end และมีกระบวนการสอบทาน test scenario หรือ test case เพื่อให้มั่นใจว่ามีความครอบคลุมเพียงพอและตรงกับความต้องการของหน่วยงานธุรกิจ (business requirement) 3. ผู้ประกอบธุรกิจควรทดสอบระบบบนสภาพแวดล้อม (test environment) ที่ใกล้เคียงระบบที่ให้บริการจริง เพื่อลดความเสี่ยงที่อาจเกิดขึ้นจากการเปลี่ยนแปลงบนระบบงานที่ให้บริการจริง 4. ผู้ประกอบธุรกิจควรมีการจัดการข้อบกพร่อง (defect) ของระบบที่พบในการทดสอบ โดยพิจารณาแนวทางปรับปรุง หรือลดความเสี่ยงและผลกระทบของข้อบกพร่องดังกล่าว 5. ผู้ประกอบธุรกิจควรมีการขออนุมัติผลการทดสอบจากฝ่ายงานที่เกี่ยวข้อง ก่อนนำระบบขึ้นใช้งานจริง
(6) มีมาตรการควบคุมความถูกต้องครบถ้วนของการแปลงข้อมูล (data conversion)	1. มาตรการควบคุมความถูกต้องครบถ้วนของการแปลงข้อมูล (data conversion) ควรครอบคลุมกรณีที่มีการโอนย้ายข้อมูลจากระบบเดิมไปยังระบบใหม่ (data migration) เช่น การทำ storage migration, cloud migration หรือ application migration เป็นต้น
(7) มีมาตรการรักษาความมั่นคงปลอดภัย และความลับของข้อมูลสำคัญที่นำไปใช้ในการทดสอบ	1. กรณีที่มีการนำข้อมูลสำคัญจากระบบจริงมาใช้เพื่อทดสอบระบบ ผู้ประกอบธุรกิจควรจัดให้มีแนวทางการรักษาความปลอดภัยและความลับของข้อมูลดังกล่าว เช่น การทำ data masking เป็นต้น เพื่อป้องกันความเสี่ยงในการรั่วไหลของข้อมูล

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. 38/2565	แนวปฏิบัติ
(8) มีการทดสอบประสิทธิภาพ (performance test) ของระบบที่เกี่ยวข้องกับการให้บริการหรือการทำธุรกรรมทางอิเล็กทรอนิกส์ เมื่อมีการพัฒนาหรือเปลี่ยนแปลงระบบอย่างมีนัยสำคัญ เพื่อให้มั่นใจว่าระบบดังกล่าวสามารถรองรับปริมาณการใช้งานได้สอดคล้องกับความต้องการทางธุรกิจ	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]
(9) ในกรณีที่มีการมอบให้มอบหมายให้บุคคลภายนอกเป็นผู้พัฒนาหรือแก้ไขเปลี่ยนแปลงระบบ IT ผู้ประกอบธุรกิจต้องจัดให้มีการติดตาม และควบคุมการดำเนินการให้เป็นไปตามข้อตกลงในการมอบหมายงาน	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]
(10) มีกระบวนการขออนุมัติจากผู้บริหารหรือคณะกรรมการที่ได้รับมอบหมายจากผู้ประกอบธุรกิจ ก่อนนำระบบขึ้นใช้งานจริง	<u>การนำระบบขึ้นใช้งานจริง</u> 1. ผู้ประกอบธุรกิจควรดำเนินการนำระบบขึ้นใช้งานจริง โดยผ่านกระบวนการบริหารจัดการการเปลี่ยนแปลงที่กำหนดไว้ 2. ผู้ประกอบธุรกิจควรเตรียมความพร้อมในการนำระบบขึ้นใช้งานจริง โดยจัดเก็บระบบเวอร์ชันก่อนการเปลี่ยนแปลงให้พร้อมนำกลับมาใช้งานได้ 3. ผู้ประกอบธุรกิจควรกำหนดแผนหรือเงื่อนไขการนำระบบใหม่เข้าไปทดแทน (cutover หรือ go-live technique) ที่เหมาะสมกับระดับความเสี่ยง เช่น การเปลี่ยนแปลงไปยังระบบใหม่ทันที (direct changeover) การเปลี่ยนแปลงระบบโดยการใช้งานคู่ขนาน (parallel changeover) หรือ การเปลี่ยนแปลงระบบทีละเฟส (phased changeover) เป็นต้น
2.10.4 การแก้ไขเปลี่ยนแปลงระบบ IT (system change)	
<u>10.4 แก้ไขเปลี่ยนแปลงระบบ IT (system change)</u>	1. การแก้ไขเปลี่ยนแปลงระบบ IT (system change) ควรพิจารณาดำเนินการตามแนวปฏิบัติเรื่องการบริหารจัดการการเปลี่ยนแปลง (change management) และแนวปฏิบัติเรื่องการพัฒนาระบบ
(1) มีการประเมินผลกระทบ และจัดลำดับความสำคัญของการเปลี่ยนแปลง	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. 38/2565	แนวปฏิบัติ
(2) มีกระบวนการขออนุมัติการเปลี่ยนแปลง (change request) โดยต้องได้รับการอนุมัติจากหน่วยงานเจ้าของระบบ (system owner) เป็นลายลักษณ์อักษร เพื่อให้มั่นใจได้ว่าการเปลี่ยนแปลงได้รับการพิจารณาความจำเป็นอย่างเหมาะสมแล้ว	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]
(3) มีการทดสอบระบบก่อนนำไปตั้งค่า หรือนำไปติดตั้งบนระบบที่ให้บริการจริง เพื่อลดความเสี่ยงและผลกระทบที่อาจเกิดขึ้น	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]
(4) มีกระบวนการขออนุมัติจากผู้บริหารหรือคณะกรรมการที่ได้รับมอบหมายจากผู้ประกอบธุรกิจก่อนนำระบบขึ้นใช้งานจริง	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]
(5) มีกระบวนการหรือเครื่องมือควบคุมการเปลี่ยนแปลงรุ่น (version) ของชุดคำสั่งคอมพิวเตอร์ (source code version control) และรองรับการถอยกลับสู่สภาพเดิม (fallback)	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]
(6) ปรับปรุงรายละเอียดประกอบระบบงานที่ได้มีการแก้ไขเปลี่ยนแปลง เพื่อให้เป็นปัจจุบัน	1. ผู้ประกอบธุรกิจควรปรับปรุงขั้นตอนการปฏิบัติงาน ระบบงานสำรอง และแผนบริหารความต่อเนื่องทางธุรกิจ (business continuity plan) เมื่อมีการแก้ไขเปลี่ยนแปลงระบบ IT เพื่อให้เป็นปัจจุบันอยู่เสมอ นอกจากนี้ ควรสื่อสารการเปลี่ยนแปลงให้บุคคลที่เกี่ยวข้องได้รับทราบเพื่อให้สามารถปฏิบัติงานได้อย่างถูกต้อง
2.11 การบริหารจัดการเหตุการณ์ผิดปกติด้าน IT (IT incident management)	
ส่วนที่ 11 การบริหารจัดการเหตุการณ์ผิดปกติด้าน IT (IT incident management) ผู้ประกอบธุรกิจต้องมีการบริหารจัดการเหตุการณ์	

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. 38/2565	แนวปฏิบัติ
ผิดปกติด้าน IT อย่างเหมาะสมและทันท่วงที ดังนี้	
11.1 จัดให้มีช่องทางรับแจ้งเหตุการณ์ผิดปกติด้าน IT จากบุคลากร ผู้ใช้บริการ และผู้ที่เกี่ยวข้อง	1. ผู้ประกอบธุรกิจควรจัดให้มีหน่วยงานหรือบุคลากรที่มีหน้าที่รับแจ้งเหตุการณ์ (point of contact) โดยทำหน้าที่ในการบันทึกข้อมูล แก้ไขในเบื้องต้น หรือส่งต่อเหตุการณ์ผิดปกติไปยังหน่วยงานด้าน IT ที่เกี่ยวข้อง
11.2 กำหนดแผน หรือขั้นตอนการบริหารจัดการเหตุการณ์ผิดปกติด้าน IT	1. ผู้ประกอบธุรกิจควรจัดให้มีแผนการบริหารจัดการ หรือแผนการรับมือกับเหตุการณ์ผิดปกติ (incident response plan) ตามความสำคัญของเหตุการณ์ เพื่อให้สามารถรับมือและตอบสนองต่อเหตุการณ์ได้อย่างรวดเร็วและทันการณ์ โดยมีรายละเอียดครอบคลุมอย่างน้อย ดังนี้ (1) การตรวจสอบความถูกต้องข้อมูลที่ได้รับแจ้ง (2) การจัดประเภท และความเร่งด่วนของเหตุการณ์ เพื่อดำเนินการแก้ไขปัญหาภายในระยะเวลาที่เหมาะสม (3) การแก้ไขเหตุการณ์ ได้แก่ การวิเคราะห์ข้อมูล (analysis) การจำกัดความเสียหาย (containment) การจัดเก็บหลักฐานอย่างปลอดภัย (evidence gathering) การหาแนวทางแก้ไข (resolution research) และการแก้ไขปัญหาและฟื้นฟูระบบ (eradication and recovery) ตลอดจนการจัดให้มีช่องทางประสานงานจากผู้เชี่ยวชาญทั้งภายในและภายนอก (4) แนวทางการรายงานเหตุการณ์ผิดปกติ (incident escalation) และรายงานความคืบหน้าของเหตุการณ์ต่อผู้บริหารระดับสูง และคณะกรรมการของผู้ประกอบธุรกิจให้รับทราบ ตามระดับความรุนแรงของเหตุการณ์ (5) การแจ้งหรือสื่อสารลูกค้า โดยกำหนดผู้รับผิดชอบในการสื่อสารไปยังลูกค้า และช่องทางการสื่อสาร เพื่อให้ลูกค้ารับทราบผลกระทบและความคืบหน้าการแก้ไขเหตุการณ์ผิดปกติ ตลอดจนให้คำแนะนำการใช้บริการในทางช่องทางอื่น (ถ้ามี) ระหว่างที่บริการที่เกิดเหตุยังไม่สามารถกลับมาใช้งานได้ปกติ เพื่อให้ลูกค้าได้มีทางเลือกในการจัดการธุรกรรมของตนเอง (6) การตรวจพิสูจน์พยานหลักฐานทางดิจิทัล (digital forensic) ในกรณีภัยคุกคามทางไซเบอร์ซึ่งส่งผลกระทบอย่างมีนัยสำคัญต่อทรัพย์สินและข้อมูลของลูกค้า โดยผู้ที่มีความเชี่ยวชาญเพื่อให้ทราบสาเหตุหรือช่องโหว่ของระบบ และสามารถดำเนินการปิดช่องโหว่ได้อย่างปลอดภัย
11.3 รายงานเหตุการณ์ผิดปกติด้าน IT เหตุการณ์การละเมิดต่อข้อมูลส่วนบุคคล และเหตุการณ์ที่ส่งผลให้ทรัพย์สินของผู้ใช้งานเสียหายอันเกิดจากเหตุการณ์ด้าน	1. ผู้ประกอบธุรกิจควรรายงานเหตุการณ์ที่มีการละเมิดกฎหมาย กฎ และระเบียบที่เกี่ยวข้องกับผู้ประกอบธุรกิจ ต่อหน่วยงานที่เกี่ยวข้องโดยไม่ชักช้า ภายในระยะเวลาที่กฎหมายกำหนดไว้ เช่น รายงานเหตุการณ์ที่ส่งผลกระทบต่อลูกค้าในวงกว้างต่อสำนักงานภายใน 3 ชั่วโมง และรายงานเหตุการณ์ข้อมูลส่วนบุคคลของลูกค้ารั่วไหลต่อสำนักงานคณะกรรมการคุ้มครองข้อมูล

<table>
<tr><th>ข้อกำหนดในภาคผนวก 3
แนบท้ายประกาศที่ สธ. 38/2565</th><th>แนวปฏิบัติ</th></tr>
<tr><td>ความมั่นคงปลอดภัยของระบบ IT ต่อผู้มีหน้าที่รับผิดชอบเหตุการณ์ และสำนักงานโดยไม่ชักช้าเมื่อทราบเหตุการณ์ดังกล่าว</td><td>
ส่วนบุคคลภายใน 72 ชั่วโมง เป็นต้น
2. ผู้ประกอบธุรกิจควรรายงานสำนักงานในกรณีที่มีเหตุการณ์ด้าน IT ซึ่งอาจส่งผลกระทบต่อการดำเนินงาน ธุรกิจ ชื่อเสียง ฐานะ ผลการดำเนินงานของผู้ประกอบธุรกิจ หรือลูกค้าในวงกว้าง โดยครอบคลุมเหตุการณ์ ดังนี้
(1) การละเมิดต่อข้อมูลส่วนบุคคลที่เกิดจากเหตุการณ์ผิดปกติด้าน IT
(2) ทรัพย์สินของผู้ใช้งานสูญหาย หรือเสียหาย
(3) การบุกรุก เข้าถึง หรือใช้งานระบบโดยไม่ได้รับอนุญาต (system compromised)
(4) เหตุการณ์ที่ส่งผลกระทบต่อชื่อเสียงของผู้ประกอบธุรกิจ (harm to reputation) เช่น ถูกปลอมแปลงหน้าเว็บไซต์ของบริษัท (website defacement) เป็นต้น
(5) การหยุดชะงักของระบบงาน (system disruption) ในช่วงเวลาทำการของผู้ประกอบธุรกิจ ดังนี้
<table>
<tr><th>ระบบงาน</th><th>ระยะเวลาหยุดชะงักก่อนที่จะรายงานสำนักงาน</th></tr>
<tr><td>ระบบจับคู่คำสั่งซื้อขาย (order matching system)</td><td>การหยุดชะงักทุกกรณี</td></tr>
<tr><td>ระบบจัดการคำสั่งซื้อขาย (order management system) หรือ ระบบรับส่งคำสั่งซื้อขาย</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
3.1 หากทราบเหตุการณ์ในวันทำการของสำนักงาน ระหว่างเวลา 8.30 น.– 16.30 น.
(1) รายงานโดยไม่ชักช้า ภายใน 3 ชั่วโมงนับแต่ทราบเหตุการณ์ โดยมีเนื้อหาครอบคลุมถึงวันเวลา ประเภทเหตุการณ์ เหตุการณ์ และผลกระทบที่คาดว่าจะเกิดขึ้น ทั้งนี้ สามารถแจ้งโดยวาจาหรือรายงานผ่านช่องทางอิเล็กทรอนิกส์ตามที่สำนักงานกำหนดตามความเหมาะสม
</td></tr>
</table>

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. 38/2565	แนวปฏิบัติ
	(2) รายงานความคืบหน้า เมื่อมีการเปลี่ยนแปลงสถานการณ์ หรือตามที่สำนักงานร้องขอ จนกว่าระบบ IT จะกลับสู่การให้บริการได้อย่างเป็นปกติ โดยมีเนื้อหาครอบคลุมถึงวันเวลา ประเภทเหตุการณ์ เหตุการณ์ ผลกระทบที่เกิดขึ้น และความคืบหน้าในการแก้ไขปัญหา ทั้งนี้ ให้รายงานผ่านช่องทางอิเล็กทรอนิกส์ที่สำนักงานกำหนด (3) รายงานเมื่อเหตุการณ์ยุติหรือแก้ไขปัญหาแล้วเสร็จ โดยมีเนื้อหาครอบคลุมถึงวันเวลา ประเภทเหตุการณ์ เหตุการณ์ ผลกระทบที่เกิดขึ้น การดำเนินการแก้ไขปัญหา ผลการแก้ไขปัญหา ระยะเวลาในการแก้ไข สาเหตุที่เกิดปัญหา และแนวทางป้องกันในอนาคต ทั้งนี้ ให้รายงานผ่านช่องทางอิเล็กทรอนิกส์ที่สำนักงานกำหนด <u>ตัวอย่างเช่น</u> (กรณีบริษัทหลักทรัพย์) พบเหตุการณ์เวลา 08.30 น. ของวันศุกร์ที่ 1 กันยายน - ให้รายงานตาม (1) ภายในเวลา 11.30 น. ของวันศุกร์ที่ 1 กันยายน - ให้รายงานตาม (2) เมื่อมีความคืบหน้า (มีการเปลี่ยนแปลงสถานการณ์ หรือตามที่สำนักงานร้องขอ) จนกว่าระบบ IT จะกลับสู่การให้บริการปกติ - ให้รายงานตาม (3) เมื่อเหตุการณ์ยุติหรือแก้ไขปัญหาแล้วเสร็จ 3.2 **หากพบเหตุการณ์นอกเวลาที่กำหนดใน 3.1** (1) รายงานโดยไม่ชักช้า ภายในเวลา 10.00 น. ของวันทำการ[3] ถัดไป โดยมีเนื้อหาครอบคลุมถึงวันเวลา ประเภทเหตุการณ์ เหตุการณ์ และผลกระทบที่คาดว่าจะเกิดขึ้น ทั้งนี้ สามารถแจ้งโดยวาจาหรือรายงานผ่านช่องทางอิเล็กทรอนิกส์ตามที่สำนักงานกำหนดตามความเหมาะสม (2) รายงานความคืบหน้า เมื่อมีการเปลี่ยนแปลงสถานการณ์ หรือตามที่สำนักงานร้องขอ จนกว่าระบบ IT จะกลับสู่การให้บริการได้อย่างเป็นปกติ โดยมีเนื้อหาครอบคลุมถึงวันเวลา ประเภทเหตุการณ์ เหตุการณ์ ผลกระทบที่เกิดขึ้น และความคืบหน้าในการแก้ไขปัญหา ทั้งนี้ ให้รายงานผ่านช่องทางอิเล็กทรอนิกส์ที่สำนักงานกำหนด (3) รายงานเมื่อเหตุการณ์ยุติหรือแก้ไขปัญหาแล้วเสร็จ โดยมีเนื้อหาครอบคลุมถึงวันเวลา ประเภทเหตุการณ์ เหตุการณ์

[3] “วันทำการ” หมายความว่า วันทำการของสำนักงาน

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. 38/2565	แนวปฏิบัติ
	ผลกระทบที่เกิดขึ้น การดำเนินการแก้ไขปัญหา ผลการแก้ไขปัญหา ระยะเวลาในการแก้ไข สาเหตุที่เกิดปัญหา และแนวทางป้องกันในอนาคต ทั้งนี้ ให้รายงานผ่านช่องทางอิเล็กทรอนิกส์ที่สำนักงานกำหนด <u>ตัวอย่างเช่น</u> (กรณีบริษัทหลักทรัพย์) พบเหตุการณ์เวลา 03.30 น. ของวันศุกร์ที่ 1 กันยายน - ให้รายงานตาม (1) ภายในเวลา 10.00 น. ของวันศุกร์ที่ 1 กันยายน - ให้รายงานตาม (2) เมื่อมีความคืบหน้า (มีการเปลี่ยนแปลงสถานการณ์ หรือตามที่สำนักงานร้องขอ) จนกว่าระบบ IT จะกลับสู่การให้บริการปกติ - ให้รายงานตาม (3) เมื่อเหตุการณ์ยุติหรือแก้ไขปัญหาแล้วเสร็จ 4. กรณีของหน่วยงานโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศ (critical information infrastructure organization หรือ CII organization)[4] ให้รายงานสำนักงานและหน่วยงานกำกับดูแลที่เกี่ยวข้อง ภายในกรอบระยะเวลาตามที่คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติกำหนด
11.4 วิเคราะห์สาเหตุที่แท้จริง (root cause) ของเหตุการณ์ผิดปกติด้าน IT เพื่อกำหนดแนวทางการแก้ไข และป้องกันไม่ให้เกิดเหตุการณ์ซ้ำในอนาคต	1. ผู้ประกอบธุรกิจควรวิเคราะห์สาเหตุที่แท้จริงของเหตุการณ์ และนำบทเรียน (lesson learned) จากเหตุการณ์ไปป้องกันไม่ให้เกิดเหตุการณ์นี้อีกในอนาคต หรือปรับปรุงกระบวนการรับมือเหตุการณ์ผิดปกติให้มีประสิทธิภาพดีขึ้น
11.5 บันทึกข้อมูลที่เกี่ยวข้องกับการบริหารจัดการเหตุการณ์ผิดปกติด้าน IT และจัดเก็บข้อมูลดังกล่าวเป็นระยะเวลาไม่น้อยกว่า 2 ปีนับแต่วันที่เกิดเหตุการณ์นั้น โดยต้องจัดเก็บไว้ในลักษณะที่พร้อมให้สำนักงานสามารถเรียกดู	1. ผู้ประกอบธุรกิจควรจัดเก็บบันทึกข้อมูลเหตุการณ์ที่เกิดขึ้นในรูปแบบที่เป็นมาตรฐาน และมีเนื้อหาขั้นต่ำประกอบด้วย วันเวลาที่เกิดเหตุการณ์ รายละเอียดเหตุการณ์ ผลกระทบ วิธีการแก้ไข วันเวลาที่สิ้นสุดเหตุการณ์ สาเหตุที่เกิดปัญหา และแนวทางการป้องกันในอนาคต โดยจัดเก็บข้อมูลดังกล่าวเป็นระยะเวลาไม่น้อยกว่า 2 ปีนับแต่วันที่เกิดเหตุการณ์นั้น โดยต้องจัดเก็บไว้ในลักษณะที่พร้อมให้สำนักงานสามารถเรียกดูและตรวจสอบได้โดยไม่ชักช้า

[4] “หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ” หมายความว่า หน่วยงานของรัฐหรือหน่วยงานเอกชน ซึ่งมีภารกิจหรือให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศเป็นไปตามคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติประกาศกำหนด

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. 38/2565	แนวปฏิบัติ
และตรวจสอบได้โดยไม่ชักช้า	
11.6 ทดสอบและทบทวนขั้นตอนปฏิบัติหรือแผนการบริหารจัดการเหตุการณ์ผิดปกติด้าน IT อย่างน้อยปีละ 1 ครั้ง โดยต้องครอบคลุมถึงการทดสอบการบริหารจัดการเหตุการณ์ด้านภัยคุกคามทางไซเบอร์ (cyber security drill) และจัดให้มีการรายงานผลการทดสอบและทบทวนต่อคณะกรรมการของผู้ประกอบธุรกิจหรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบธุรกิจ	1. ผู้ประกอบธุรกิจควรทดสอบและทบทวนขั้นตอนปฏิบัติหรือแผนการบริหารจัดการเหตุการณ์ผิดปกติ อย่างน้อยปีละ 1 ครั้ง เพื่อให้สามารถจัดการแก้ไขเหตุการณ์ให้กลับสู่สภาพปกติได้อย่างรวดเร็วและจำกัดความเสียหายที่ส่งผลกระทบต่อธุรกิจ โดยดำเนินการดังนี้ (1) จัดให้มีการจำลองสถานการณ์เสี่ยง (risk scenario) ด้านเหตุการณ์ภัยคุกคามทางไซเบอร์ที่มีความเป็นไปได้ที่จะเกิดขึ้น สอดคล้องกับลักษณะ ขอบเขต และความซับซ้อนในการประกอบธุรกิจ และสอดคล้องกับแนวโน้มภัยคุกคามไซเบอร์ที่อาจเกิดขึ้นกับผู้ประกอบธุรกิจ โดยสถานการณ์ดังกล่าวควรเป็นสถานการณ์ที่เกิดขึ้นแล้วส่งผลกระทบต่อระบบ IT อย่างมีนัยสำคัญ (2) จัดเก็บเอกสารที่เกี่ยวข้องกับการทดสอบให้ครบถ้วนและเป็นปัจจุบัน ดังนี้ (ก) สถานการณ์ความเสี่ยง (risk scenario) รูปแบบการทดสอบ วัน เวลา สถานที่ในการทดสอบ บทบาทหน้าที่ของผู้ที่เกี่ยวข้องที่ใช้ในการทดสอบ (ข) สรุปผลการทดสอบ และผลการทบทวนขั้นตอนการบริหารจัดการเหตุการณ์ (3) จัดให้มีการรายงานผลการทดสอบและทบทวนต่อคณะกรรมการของผู้ประกอบธุรกิจหรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบธุรกิจ *(4) [ความเสี่ยงสูง] จัดให้มีการรายงานผลการทดสอบและทบทวนต่อคณะกรรมการของผู้ประกอบธุรกิจ*
2.12 แผนฉุกเฉินด้าน IT (IT contingency plan)	
ส่วนที่ 12 แผนฉุกเฉินด้าน IT (IT contingency plan) ผู้ประกอบธุรกิจต้องจัดให้มีแผนฉุกเฉินด้าน IT เพื่อรองรับเหตุการณ์ผิดปกติด้าน IT ซึ่งส่งผลกระทบให้ไม่สามารถให้บริการได้ตามปกติ หรือไม่สามารถดำเนินธุรกิจอย่างต่อเนื่อง โดยต้องกู้คืนระบบให้กลับคืนสู่สภาพปกติภายในระยะเวลาที่เหมาะสมได้ ดังนี้	

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. 38/2565	แนวปฏิบัติ
12.1 จัดให้มีคณะทำงานหรือหน่วยงานที่รับผิดชอบในการจัดทำแผนฉุกเฉินด้าน IT	1. ผู้ประกอบธุรกิจควรจัดให้มีคณะทำงานหรือหน่วยงานที่รับผิดชอบในการจัดทำแผนฉุกเฉินด้าน IT ไว้อย่างเป็นลายลักษณ์อักษร โดยมีผู้บริหารและบุคลากรของหน่วยงานด้านต่าง ๆ ที่เกี่ยวข้องเข้าร่วมด้วย เช่น ด้าน IT ด้านธุรกิจ และด้านสื่อสารองค์กร เป็นต้น
12.2 กระบวนการจัดทำแผนฉุกเฉินด้าน IT ต้องครอบคลุมการดำเนินการ ดังนี้	
12.2.1 ประเมินความเสี่ยง (risk analysis) เพื่อให้สามารถระบุเหตุการณ์ความเสี่ยงที่อาจทำให้กระบวนการและระบบ IT หยุดชะงัก ไม่สามารถให้บริการได้ตามปกติ หรือไม่สามารถดำเนินธุรกิจอย่างต่อเนื่อง	1. ผู้ประกอบธุรกิจควรประเมินความเสี่ยง (risk analysis) เพื่อให้สามารถระบุเหตุการณ์ความเสี่ยงที่อาจทำให้กระบวนการและระบบ IT หยุดชะงัก ไม่สามารถให้บริการได้ตามปกติ หรือไม่สามารถดำเนินธุรกิจอย่างต่อเนื่อง โดยมีแนวทางดำเนินการ ดังนี้ (1) ระบุเหตุการณ์ความเสี่ยง (risk scenarios) ที่อาจทำให้กระบวนการและระบบ IT หยุดชะงัก ทั้งจากภายในและภายนอก เช่น การโจมตีด้านไซเบอร์ ไฟไหม้ เป็นต้น (2) ประเมินความเสี่ยงโดยพิจารณาผลกระทบและโอกาสที่จะเกิดขึ้น รวมถึงการควบคุมที่มีอยู่ (3) จัดให้มีกระบวนการและทรัพยากรที่จำเป็นในการควบคุมความเสี่ยงให้อยู่ในระดับที่ยอมรับได้
12.2.2 วิเคราะห์ผลกระทบทางธุรกิจ (business impact analysis) จากเหตุการณ์ความเสี่ยงตามข้อ 12.2.1 เพื่อกำหนดระยะเวลาเป้าหมายในการกู้คืนระบบ IT (Recovery Time Objective : RTO) ระยะเวลาเป้าหมายสูงสุดที่ยอมให้ข้อมูลเสียหาย (Recovery Point Objective : RPO) และระยะเวลาสูงสุดที่ยอมให้กระบวนการทางธุรกิจหยุดชะงัก (Maximum Tolerable Downtime : MTD) อย่างเหมาะสม	1. ผู้ประกอบธุรกิจควรวิเคราะห์ผลกระทบทางธุรกิจ (business impact analysis) เพื่อให้ทราบถึงความสำคัญของระบบ IT ที่มีผลต่อการดำเนินธุรกิจ โดยมีแนวทางการดำเนินการ ดังนี้ (1) ระบุรายการกระบวนการทางธุรกิจ (business process) และระบบ IT ที่กระบวนการทางธุรกิจพึ่งพา (2) วิเคราะห์ผลกระทบที่เกิดจากการหยุดชะงักของระบบ IT เพื่อกำหนดระยะเวลา RTO, RPO และ MTD ทั้งนี้ (ก) RTO ไม่ควรเกิน 2 ชั่วโมง สำหรับระบบ IT ที่สนับสนุนกระบวนการทางธุรกิจที่สำคัญของหน่วยงานโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศ (critical information infrastructure organization หรือ CII organization) (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

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. 38/2565	แนวปฏิบัติ
	(4) จัดลำดับความสำคัญของระบบ IT เพื่อให้ระบบ IT ที่สนับสนุนกระบวนการทางธุรกิจที่สำคัญสูงได้รับการกู้คืนเป็นลำดับแรก
12.2.3 จัดทำแผนฉุกเฉินด้าน IT อย่างเป็นลายลักษณ์อักษร ซึ่งได้รับความเห็นชอบจากคณะกรรมการของผู้ประกอบธุรกิจหรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบธุรกิจ	1. ผู้ประกอบธุรกิจควรจัดให้มีแผนฉุกเฉินด้าน IT ที่ได้รับความเห็นชอบจากคณะกรรมการของผู้ประกอบธุรกิจหรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบธุรกิจ ซึ่งมีรายละเอียดของกระบวนการหรือขั้นตอนการปฏิบัติงานที่ชัดเจน เพื่อให้สามารถดำเนินการได้อย่างรวดเร็วและง่ายต่อการปฏิบัติ โดยครอบคลุมรายละเอียดอย่างน้อย ดังนี้ (1) หน้าที่ และความรับผิดชอบของผู้บริหารระดับสูง และผู้ที่เกี่ยวข้องในการดำเนินการตามแผน (2) รายละเอียดของระบบ IT เช่น โครงสร้างสถาปัตยกรรม แผนภาพแสดงระบบเครือข่ายสื่อสาร เป็นต้น (3) เงื่อนไขและขั้นตอนในการประกาศใช้แผนฉุกเฉินด้าน IT การตอบสนองต่อเหตุการณ์ฉุกเฉิน และแผนการสื่อสารให้ผู้ที่เกี่ยวข้องรับทราบ (4) ขั้นตอนการกู้คืนระบบและข้อมูล โดยมีรายละเอียดที่ชัดเจนและเพียงพอที่ผู้ปฏิบัติงานสามารถใช้เป็นขั้นตอนปฏิบัติได้อย่างถูกต้อง และเป็นไปตามเป้าหมายเวลาที่กำหนดไว้ โดยอาจจัดทำในรูปแบบรายการตรวจสอบขั้นตอนปฏิบัติ (checklist) (5) ขั้นตอนการตรวจสอบความถูกต้องครบถ้วนของระบบ IT และข้อมูลที่กู้คืน ก่อนกลับสู่การดำเนินกระบวนการทางธุรกิจอย่างปกติ (return to normal) (6) ขั้นตอนการประกาศยกเลิกแผนฉุกเฉินด้าน IT (7) การจัดเก็บแผนฉุกเฉินด้าน IT ไว้ในสถานที่ปลอดภัยและมีความพร้อมใช้งานในสถานที่ปฏิบัติงานหลักและสถานที่สำรอง 2. ผู้ประกอบธุรกิจควรจัดให้มีรายชื่อของบุคลากรและช่องทางการติดต่อ เพื่อใช้ในการสื่อสารกรณีเกิดภาวะวิกฤตหรือมีเหตุจำเป็นเร่งด่วนได้ 3. *[ความเสี่ยงสูง] แผนฉุกเฉินด้าน IT ควรได้รับความเห็นชอบจากคณะกรรมการของผู้ประกอบธุรกิจ*
12.3 จัดให้มีระบบ IT สำรอง และทรัพยากรที่จำเป็นเพื่อให้สามารถกู้คืนระบบได้ตามระยะเวลาเป้าหมายที่กำหนดไว้	1. ผู้ประกอบธุรกิจควรจัดให้มีระบบ IT สำรอง และทรัพยากรที่จำเป็นเพื่อให้สามารถกู้คืนระบบ IT ได้ตามระยะเวลาเป้าหมายที่กำหนดไว้ โดยกรณีที่ผู้ประกอบธุรกิจมีศูนย์คอมพิวเตอร์สำรอง ควรระบุรายละเอียดเกี่ยวกับศูนย์คอมพิวเตอร์สำรองให้ชัดเจน เช่น ทรัพยากรที่มี สถานที่ตั้งและแผนที่ เป็นต้น
12.4 สื่อสารให้บุคลากรที่เกี่ยวข้องมีความเข้าใจและสามารถปฏิบัติตามแผนฉุกเฉินด้าน IT อย่างเหมาะสม	1. ผู้ประกอบธุรกิจควรสื่อสารแผนฉุกเฉินด้าน IT ให้พนักงานทุกคนที่มีส่วนเกี่ยวข้องกับการปฏิบัติตามแผนฉุกเฉินด้าน IT มีความเข้าใจ และสามารถปฏิบัติตามแผนได้อย่างถูกต้อง

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. 38/2565	แนวปฏิบัติ
12.5 ทบทวนและทดสอบการปฏิบัติตามแผนฉุกเฉินด้าน IT อย่างน้อยปีละ 1 ครั้ง และเมื่อมีเหตุจำเป็นที่ควรได้รับการทบทวนและทดสอบดังกล่าว โดยรายงานผลการทบทวนและทดสอบต่อคณะกรรมการของผู้ประกอบธุรกิจหรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบธุรกิจ	1. ผู้ประกอบธุรกิจควรทบทวน (review) และทดสอบ (test) การปฏิบัติตามแผนฉุกเฉินด้าน IT อย่างน้อยปีละ 1 ครั้ง และเมื่อมีเหตุจำเป็นที่ควรได้รับการทบทวนและทดสอบดังกล่าว เช่น มีการเปลี่ยนแปลงกลยุทธ์ทางธุรกิจ นโยบายการบริหารความเสี่ยงโดยรวม สภาพแวดล้อมของการให้บริการหรือดำเนินธุรกิจ ทรัพยากร หรือโครงสร้างระบบ IT เป็นต้น 2. ผู้ประกอบธุรกิจควรกำหนดเหตุการณ์ที่ใช้ในการทดสอบประจำปี (test scenario) โดยเป็นเหตุการณ์ที่มีโอกาสที่จะเกิดขึ้นและอาจส่งผลกระทบให้กระบวนการทางธุรกิจที่สำคัญหยุดชะงัก เช่น การหยุดชะงักของระบบ IT ที่สนับสนุนกระบวนการทางธุรกิจที่สำคัญ การหยุดชะงักของผู้ให้บริการภายนอกที่สำคัญ (รวมถึงผู้ให้บริการคลาวด์) และการโจมตีทางไซเบอร์ เป็นต้น 3. ผู้ประกอบธุรกิจควรรายงานผลการทดสอบแผนฉุกเฉินด้าน IT ต่อคณะกรรมการของผู้ประกอบธุรกิจหรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบธุรกิจ โดยมีรายละเอียดอย่างน้อยครอบคลุมวัตถุประสงค์ ขอบเขตการทดสอบ สถานการณ์จำลอง ผลการทดสอบ ข้อผิดพลาดและปัญหาหรืออุปสรรคที่พบ พร้อมทั้งแนวทางปรับปรุงแก้ไข 4. *[ความเสี่ยงสูง] ผู้ประกอบธุรกิจควรรายงานผลการทดสอบแผนฉุกเฉินด้าน IT ต่อคณะกรรมการของผู้ประกอบธุรกิจ โดยมีรายละเอียดอย่างน้อยครอบคลุมวัตถุประสงค์ ขอบเขตการทดสอบสถานการณ์จำลอง ผลการทดสอบ ข้อผิดพลาดและปัญหาหรืออุปสรรคที่พบ พร้อมทั้งแนวทางปรับปรุงแก้ไข* 5. *[ความเสี่ยงสูง] ผู้ประกอบธุรกิจควรทดสอบแผนฉุกเฉินด้าน IT โดยครอบคลุมการเปลี่ยนแปลงกระบวนการทำงาน (business process) หรือการโอนย้ายการประมวลผลไปยังศูนย์คอมพิวเตอร์สำรอง / ระบบ IT สำรอง*
12.6 กำหนดกระบวนการดำเนินงาน เพื่อรับมือเหตุการณ์การใช้ทรัพยากรด้าน IT หรือการใช้ประสิทธิภาพของระบบงานเกินขีดจำกัดของตัวชี้วัดที่กำหนดไว้ เช่น การจำกัดการให้บริการบางช่องทาง หรือตัดการเชื่อมต่อกับผู้ให้บริการหรือบุคคลภายนอกที่มีผลกระทบต่อระบบ IT เป็นต้น	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]
12.7 จัดให้มีรายละเอียดในการติดต่อดังนี้ เพื่อให้สามารถประสานงานในการรายงานเหตุการณ์ผิดปกติด้าน IT หรือขอความช่วยเหลือจากหน่วยงานภายนอกที่เกี่ยวข้องได้อย่าง	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]

ข้อกำหนดในภาคผนวก 3 แนบท้ายประกาศที่ สธ. 38/2565	แนวปฏิบัติ
มีประสิทธิภาพ โดยต้องปรับปรุงข้อมูลดังกล่าวให้เป็นปัจจุบันอยู่เสมอ 12.7.1 รายชื่อหน่วยงานกำกับดูแลและบุคคลภายนอกที่ให้บริการหรือที่มีการเชื่อมต่อกับระบบ IT ของผู้ประกอบธุรกิจ 12.7.2 ช่องทางในการติดต่อ และรายชื่อผู้ที่เกี่ยวข้องของหน่วยงานกำกับดูแลหรือบุคคลภายนอกตามข้อ 12.7.1	

หมวดที่ 3 การตรวจสอบด้านเทคโนโลยีสารสนเทศ (Information Technology Audit)

ให้ผู้ประกอบธุรกิจดำเนินการตามที่กำหนดในภาคผนวกนี้

ข้อกำหนดในภาคผนวก 4 แนบท้ายประกาศที่ สธ. 38/2565	แนวปฏิบัติ
1. <u>การจัดให้มีผู้ตรวจสอบ</u> ผู้ตรวจสอบตาม 1. ต้องมีลักษณะดังนี้ 1.1 มีความเป็นอิสระจากผู้ทำหน้าที่ด้าน IT ในระดับ ดังนี้ 1.1.1 ระดับที่ 1 (first line of defense) : การปฏิบัติงาน 1.1.2 ระดับที่ 2 (second line of defense) : การบริหารความเสี่ยงและกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง 1.2 ในกรณีที่เป็นการตรวจสอบด้าน IT ตั้งแต่วันที่ 1 มกราคม พ.ศ. 2567 เป็นต้นไป ผู้ตรวจสอบต้องผ่านการรับรองและมีวุฒิบัตรอย่างหนึ่งอย่างใดดังนี้ 1.2.1 Certified Information Systems Auditor (CISA) 1.2.2 Certified Information Security Manager (CISM) 1.2.3 Certified Information Systems Security Professional (CISSP) 1.2.4 ISO/IEC 27001 Lead Auditor 1.2.5 ใบรับรองอื่นตามที่กำหนดเพิ่มเติมบนเว็บไซต์ของสำนักงาน	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]
2. <u>การวางแผนและกำหนดขอบเขตการตรวจสอบ</u> ทบทวนแผนงานและขอบเขตการตรวจสอบให้สอดคล้องกับความเสี่ยงด้าน IT และประกาศที่ สธ. 38/2565 โดยต้องดำเนินการอย่างน้อยปีละ 1 ครั้ง และเมื่อมีเหตุจำเป็นที่ควรได้รับการทบทวนดังกล่าว	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]
3. <u>การตรวจสอบด้าน IT ตามแผนงานและขอบเขตที่กำหนด</u> 3.1 จัดให้มีการตรวจสอบและรายงานผลการตรวจสอบด้าน IT โดยมีรายละเอียดดังนี้ 3.1.1 กรณีเป็นผู้ประกอบธุรกิจขนาดเล็ก ต้องจัดให้มีการตรวจสอบด้าน IT อย่างน้อยปีละ 1 ครั้ง โดยเป็นการตรวจสอบที่ครอบคลุมหลักเกณฑ์ทั้งหมดที่บังคับใช้กับผู้ประกอบธุรกิจขนาดเล็ก	1. กรณีของผู้ประกอบธุรกิจขนาดเล็ก และผู้ประกอบธุรกิจที่มีความเสี่ยงต่ำ (1) ในรอบปีที่ไม่ได้ตรวจแบบครอบคลุมหลักเกณฑ์ทั้งหมดที่บังคับใช้หรือแบบเต็มรูปแบบ (full scope) ผู้ประกอบธุรกิจสามารถกำหนดขอบเขตของการตรวจสอบด้าน IT ให้เหมาะสมกับความเสี่ยงที่เกี่ยวข้อง

ข้อกำหนดในภาคผนวก 4 แนบท้ายประกาศที่ สธ. 38/2565	แนวปฏิบัติ
อย่างน้อยทุก 2 ปี 3.1.2 กรณีเป็นผู้ประกอบธุรกิจที่มีความเสี่ยงระดับต่ำ ต้องจัดให้มีการตรวจสอบด้าน IT อย่างน้อยปีละ 1 ครั้ง โดยเป็นการตรวจสอบแบบเต็มรูปแบบ (full scope) ที่ครอบคลุมหลักเกณฑ์ทั้งหมด อย่างน้อยทุก 2 ปี 3.1.3 กรณีเป็นผู้ประกอบธุรกิจที่มีความเสี่ยงระดับปานกลางหรือหรือระดับสูง ต้องจัดให้มีการตรวจสอบด้าน IT แบบเต็มรูปแบบ (full scope) ที่ครอบคลุมหลักเกณฑ์ทั้งหมด อย่างน้อยปีละ 1 ครั้ง 3.2 จัดให้มีการบันทึกข้อมูลเกี่ยวกับการตรวจสอบ เช่น กระดาษทำการ (working paper) และหลักฐานประกอบการตรวจ เป็นต้น เป็นระยะเวลาไม่น้อยกว่า 2 ปีนับแต่วันที่จัดทำรายงานและแผนดังกล่าว โดยต้องจัดเก็บไว้ในลักษณะที่พร้อมให้สำนักงานสามารถเรียกดูและตรวจสอบได้โดยไม่ชักช้า	(2) ในรอบปีที่ตรวจแบบครอบคลุมหลักเกณฑ์ทั้งหมดที่บังคับใช้หรือแบบเต็มรูปแบบ (full scope) ให้ผู้ประกอบธุรกิจจัดให้มีการตรวจสอบที่ครอบคลุมแนวปฏิบัติทุกหัวข้อ
4. <u>การจัดให้มีแผนการปรับปรุงแก้ไขข้อบกพร่องจากการตรวจสอบด้าน IT และการติดตามความคืบหน้า</u> จัดให้มีแผนการปรับปรุงแก้ไขข้อบกพร่องจากการตรวจสอบด้าน IT ตาม 3. ที่เหมาะสมกับระดับความเสี่ยงจากข้อบกพร่อง และติดตามความคืบหน้าในการดำเนินการตามแผนดังกล่าว	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]
5. <u>การจัดทำและรายงานผลการตรวจสอบ</u> 5.1 เสนอรายงานผลการตรวจสอบตามข้อ 3. และแผนการปรับปรุงแก้ไขข้อบกพร่องต่อคณะกรรมการของผู้ประกอบธุรกิจหรือคณะกรรมการตรวจสอบของผู้ประกอบธุรกิจโดยไม่ชักช้า 5.2 [5]รายงานผลการตรวจสอบและแผนการปรับปรุงแก้ไขข้อบกพร่องที่ผ่านการพิจารณาจากคณะกรรมการของผู้ประกอบธุรกิจหรือคณะกรรมการตรวจสอบของผู้ประกอบธุรกิจตามข้อ 5.1 ต่อสำนักงานตามรูปแบบและ	ตัวอย่างการนับเวลารายงานผลการตรวจสอบต่อสำนักงาน เช่น (1) เริ่มตรวจสอบ วันที่ 15 สิงหาคม, สิ้นสุดการตรวจสอบ วันที่ 30 กันยายน และ

[5] เว้นแต่กรณีเป็นผู้ประกอบธุรกิจที่เป็นธนาคารพาณิชย์ตามกฎหมายว่าด้วยธุรกิจสถาบันการเงิน บริษัทประกันชีวิตตามกฎหมายว่าด้วยการประกันชีวิต หรือสถาบันการเงินที่จัดตั้งขึ้นตามกฎหมายอื่น ซึ่งได้รับใบอนุญาตประกอบธุรกิจหลักทรัพย์ดังนี้ โดยไม่ได้มีการประกอบธุรกิจหลักทรัพย์ประเภทอื่น โดยให้ได้รับยกเว้นการดำเนินการตามข้อ 5.2

1. การเป็นนายหน้าซื้อขายหลักทรัพย์ การค้าหลักทรัพย์ และการจัดจำหน่ายขายหลักทรัพย์อันเป็นตราสารแห่งหนี้ หรือ
2. กิจการการยืมและให้ยืมหลักทรัพย์

ข้อกำหนดในภาคผนวก 4 แนบท้ายประกาศที่ สธ. 38/2565	แนวปฏิบัติ
วิธีการที่กำหนดไว้บนเว็บไซต์ของสำนักงาน ภายในระยะเวลาดังนี้ แล้วแต่ระยะเวลาใดจะครบกำหนดก่อน * 5.2.1 30 วัน นับแต่วันที่เสนอรายงานและแผนดังกล่าวต่อคณะกรรมการของผู้ประกอบธุรกิจหรือคณะกรรมการตรวจสอบของผู้ประกอบธุรกิจ 5.2.2 90 วัน นับแต่วันที่สิ้นสุดการตรวจสอบตามข้อ 3. 5.2.3 3 เดือน นับแต่วันสิ้นปีปฏิทินของปีที่เริ่มตรวจสอบตามข้อ 3. กรณีที่ไม่สามารถจัดทำรายงานผลการตรวจสอบให้เสร็จสิ้นภายในปีที่เริ่มการตรวจสอบ (* หมายเหตุ สำหรับการรายงานผลการตรวจสอบรอบปี พ.ศ. 2566 ให้ผู้ประกอบธุรกิจรายงานภายใน 3 เดือนนับแต่วันสิ้นปีปฏิทินของปี พ.ศ. 2566) 5.3 จัดเก็บรายงานผลการตรวจสอบและแผนการปรับปรุงแก้ไขข้อบกพร่องเป็นระยะเวลาไม่น้อยกว่า 2 ปีนับแต่วันที่จัดทำรายงานและแผนดังกล่าว โดยต้องจัดเก็บไว้ในลักษณะที่พร้อมให้สำนักงานสามารถเรียกดูและตรวจสอบได้โดยไม่ชักช้า	เสนอรายงานและแผนการปรับปรุงแก้ไขข้อบกพร่องต่อคณะกรรมการของผู้ประกอบธุรกิจหรือคณะกรรมการตรวจสอบของผู้ประกอบธุรกิจ วันที่ 15 ตุลาคม ผู้ประกอบธุรกิจจะมีกรอบระยะเวลาที่ต้องปฏิบัติ ดังนี้ ● ภายใน 30 วัน หลังจากเสนอต่อคณะกรรมการฯ คือ ภายในวันที่ 14 พฤศจิกายน ● ภายใน 90 วัน นับแต่วันที่สิ้นสุดการตรวจสอบ คือ ภายในวันที่ 29 ธันวาคม ● ภายใน 3 เดือน นับแต่วันสิ้นปีของปีที่เริ่มตรวจสอบ คือ ภายในวันที่ 31 มีนาคม โดยระยะเวลาที่ครบกำหนดก่อนคือวันที่ 14 พฤศจิกายน ดังนั้น ผู้ประกอบธุรกิจต้องรายงานสำนักงานภายในวันที่ 14 พฤศจิกายน (2) เริ่มตรวจสอบ วันที่ 15 ธันวาคม, สิ้นสุดการตรวจสอบ วันที่ 20 มกราคม และเสนอรายงานและแผนการปรับปรุงแก้ไขข้อบกพร่องต่อคณะกรรมการของผู้ประกอบธุรกิจหรือคณะกรรมการตรวจสอบของผู้ประกอบธุรกิจ วันที่ 5 มีนาคม ผู้ประกอบธุรกิจจะมีกรอบระยะเวลาที่ต้องปฏิบัติ ดังนี้ ● ภายใน 30 วัน หลังจากเสนอต่อคณะกรรมการฯ คือ ภายในวันที่ 4 เมษายน ● ภายใน 90 วัน นับแต่วันที่สิ้นสุดการตรวจสอบ คือ ภายในวันที่ 20 เมษายน ● ภายใน 3 เดือน นับแต่วันสิ้นปีของปีที่เริ่มตรวจสอบ คือ ภายในวันที่ 31 มีนาคม โดยระยะเวลาที่ครบกำหนดก่อนคือวันที่ 31 มีนาคม ดังนั้น ผู้ประกอบธุรกิจต้องรายงานสำนักงานภายในวันที่ 31 มีนาคม