เอกสารเปรียบเทียบรายละเอียดของหลักเกณฑ์เดิม และหลักเกณฑ์ที่แก้ไข

หัวข้อ	รายละเอียดเดิม	รายละเอียดการแก้ไข
บทนิยาม	"ทรัพย์สินสารสนเทศ" หมายถึง (1) ทรัพย์สินสารสนเทศประเภทระบบ ซึ่งได้แก่ ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ (2) ทรัพย์สินสารสนเทศประเภทอุปกรณ์ ซึ่งได้แก่ ตัวเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล และอุปกรณ์อื่นใด (3) ทรัพย์สินสารสนเทศประเภทข้อมูล ซึ่งได้แก่ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์	"ทรัพย์สินด้านเทคโนโลยีสารสนเทศ" หมายถึง ฮาร์ดแวร์ ซอฟต์แวร์ และข้อมูล โดยรวมถึงสิทธิ์ในการใช้งานฮาร์ดแวร์ และซอฟต์แวร์
	"ระบบสารสนเทศที่มีความสำคัญ" หมายถึง ระบบสารสนเทศที่รองรับการปฏิบัติงานที่สำคัญ เช่น ระบบซื้อขาย ระบบปฏิบัติการ back office และระบบจัดการลงทุน เป็นต้น	"ระบบสารสนเทศที่มีความสำคัญ" (critical system) หมายถึง ระบบคอมพิวเตอร์ หรือระบบเครือข่ายสำคัญที่หากมีการหยุดชะงักจะส่งผลกระทบอย่างมีนัยสำคัญต่อความต่อเนื่องในการดำเนินงานของผู้ประกอบธุรกิจ หรือส่งผลกระทบอย่างมีนัยสำคัญต่อลูกค้าที่ใช้บริการ นอกจากนี้ อาจส่งผลกระทบต่อ ชื่อเสียง ฐานะ และผลการดำเนินงานของผู้ประกอบธุรกิจอย่างมีนัยสำคัญ เช่น ระบบซื้อขาย ระบบสนับสนุนการปฏิบัติการ (back office system) ระบบจัดเก็บและบริหารจัดการข้อมูลลูกค้าและนักลงทุน ระบบจัดการลงทุน และระบบจัดเก็บสินทรัพย์ดิจิทัล เป็นต้น
	- เดิมไม่ได้กำหนด -	"บุคคลภายนอก" (third party) หมายถึง บุคคลหรือนิติบุคคลภายนอก ซึ่งได้แก่ • ผู้รับดำเนินการด้านระบบสารสนเทศ (IT outsource) หรือ • ผู้ให้บริการ หรือ ผู้เสนอขายหรือติดตั้งผลิตภัณฑ์ด้านเทคโนโลยีสารสนเทศที่สามารถเข้าถึงหรือปรับปรุงข้อมูลหรือระบบงานแก่ผู้ประกอบธุรกิจ หรือ • ผู้ให้บริการ cloud computing (cloud service provider) หรือ • ผู้ที่มีการเชื่อมต่อกับระบบสารสนเทศของผู้ประกอบธุรกิจ หรือ • ผู้ที่สามารถเข้าถึงหรือมีการแลกเปลี่ยนข้อมูลสำคัญของผู้ประกอบธุรกิจหรือข้อมูลของลูกค้าที่อยู่ภายใต้การควบคุมดูแลโดยผู้ประกอบธุรกิจได้ ทั้งนี้ บุคคลภายนอกไม่ครอบคลุมถึงลูกค้าที่ใช้ผลิตภัณฑ์และบริการของผู้ประกอบธุรกิจ

เอกสารเปรียบเทียบรายละเอียดของหลักเกณฑ์เดิม และหลักเกณฑ์ที่แก้ไข

หัวข้อ	รายละเอียดเดิม	รายละเอียดการแก้ไข
	- เดิมไม่ได้กำหนด -	“เทคโนโลยีสารสนเทศ” (information technology - IT) หมายถึง เทคโนโลยีสารสนเทศที่นำมาใช้ในการดำเนินธุรกิจ ซึ่งครอบคลุมถึง ข้อมูล ระบบปฏิบัติการ (operating system) ระบบงาน (application system) ระบบฐานข้อมูล (database system) อุปกรณ์คอมพิวเตอร์ (hardware) และระบบเครือข่ายคอมพิวเตอร์ (communication) เป็นต้น
	- เดิมไม่ได้กำหนด -	“ความเสี่ยงด้านเทคโนโลยีสารสนเทศ” (IT risk) หมายถึง ความเสี่ยงที่อาจเกิดขึ้นจากการใช้เทคโนโลยีสารสนเทศในการดำเนินธุรกิจ ซึ่งมีผลกระทบต่อระบบหรือการปฏิบัติงานของผู้ประกอบธุรกิจ ความปลอดภัยหรือความเป็นส่วนตัวของข้อมูลลูกค้าหรือตลาดทุน ซึ่งรวมถึงความเสี่ยงที่เกิดจากภัยคุกคามทางไซเบอร์ (cyber threat)
	- เดิมไม่ได้กำหนด -	“ความมั่นคงปลอดภัยด้านสารสนเทศ” (information security) หมายถึง การรักษาความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) ความน่าเชื่อถือ (reliability) และการรักษาความเป็นส่วนตัวของข้อมูลสารสนเทศและบุคคล (privacy)
	- เดิมไม่ได้กำหนด -	"เหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ” (IT incident) หมายถึง เหตุการณ์ด้านเทคโนโลยีสารสนเทศที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (unwanted or unexpected) ซึ่งอาจทำให้ (1) ระบบของผู้ประกอบธุรกิจถูกบุกรุกหรือโจมตี หรือ (2) ความมั่นคงปลอดภัยด้านสารสนเทศถูกคุกคาม หรือ (3) ระบบไม่สามารถให้บริการได้ หรือ (4) ข้อมูลส่วนบุคคลถูกละเมิด
	- เดิมไม่ได้กำหนด -	“การใช้งานอุปกรณ์ส่วนตัว” (Bring Your Own Device : BYOD) หมายถึง การใช้งานอุปกรณ์ส่วนตัวของบุคลากรของผู้ประกอบธุรกิจเพื่อเข้าถึงระบบงานสารสนเทศ รวมถึงการเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ และตารางการประชุม เช่น ในรูปแบบโปรแกรม application และเว็บบราวเซอร์ เป็นต้น

เอกสารเปรียบเทียบรายละเอียดของหลักเกณฑ์เดิม และหลักเกณฑ์ที่แก้ไข

หัวข้อ	รายละเอียดเดิม	รายละเอียดการแก้ไข
	- เดิมไม่ได้กำหนด -	“สิ่งที่ใช้ยืนยันตัวตน” (authenticator) หมายถึง สิ่งที่ผู้ใช้งานครอบครองเพื่อใช้ในการยืนยันตัวตนเพื่อเข้าถึงข้อมูลหรือระบบสารสนเทศ เช่น รหัสผ่าน ลายนิ้วมือ และ SMS OTP เป็นต้น
	- เดิมไม่ได้กำหนด -	“โครงการด้านเทคโนโลยีสารสนเทศ” (IT project management) หมายถึง การจัดหา พัฒนา หรือแก้ไขเปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศที่มีนัยสำคัญต่อการให้บริการการดำเนินธุรกิจ หรือการบริหารโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ (infrastructure)
	- เดิมไม่ได้กำหนด -	“เครื่องมือชำระเงิน” หมายถึง เครื่องมือที่ใช้สำหรับให้บริการลูกค้าในทางการเงินและการลงทุน เช่น บริการซื้อขายหลักทรัพย์ บริการด้านการชำระราคา และ บริการฝากและถอนทรัพย์สิน เป็นต้น รวมถึงระบบสำหรับการระดมทุนในตลาดทุนในรูปแบบต่าง ๆ เช่น การออกเป็นหลักทรัพย์ (Securities Token Offering: STO) หรือออกเป็นโทเคนดิจิทัล (Initial Coin Offering: ICO) และการระดมทุนแบบคราวด์ฟันดิง เป็นต้น
การกำกับดูแลตามความเสี่ยง	ในกรณีที่ผู้ประกอบธุรกิจหลักทรัพย์หรือธุรกิจสัญญาซื้อขายล่วงหน้าเป็นธนาคารพาณิชย์ตามกฎหมายว่าด้วยธุรกิจสถาบันการเงิน บริษัทประกันชีวิตตามกฎหมายว่าด้วยการประกันชีวิต หรือสถาบันการเงินที่จัดตั้งขึ้นตามกฎหมายอื่น ให้ปฏิบัติตามประกาศนี้เฉพาะข้อ 11 และข้อ 23(4)	ยกเลิกข้อกำหนดเฉพาะสำหรับผู้ประกอบธุรกิจซึ่งเป็นธนาคารพาณิชย์ตามกฎหมายว่าด้วยธุรกิจสถาบันการเงิน บริษัทประกันชีวิตตามกฎหมายว่าด้วยการประกันชีวิต หรือสถาบันการเงินที่จัดตั้งขึ้นตามกฎหมายอื่น ผู้ประกอบธุรกิจทุกรายต้องกำกับดูแล และบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk) อย่างมีประสิทธิผลและประสิทธิภาพเพียงพอ โดยคำนึงถึงการรักษาความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของเทคโนโลยีสารสนเทศให้เหมาะสมกับผลการประเมินระดับความเสี่ยงของผู้ประกอบธุรกิจ
	- เดิมไม่ได้กำหนด -	ผู้ประกอบธุรกิจต้องจัดให้มีการประเมินความเสี่ยงตามเงื่อนไข (Criteria) ตามที่สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน) กำหนด และส่งผลการประเมินความเสี่ยงที่ได้รับความเห็นชอบจากผู้บริหารหรือคณะกรรมการที่มีอำนาจต่อสำนักงานภายในวันสิ้นปีปฏิทิน

เอกสารเปรียบเทียบรายละเอียดของหลักเกณฑ์เดิม และหลักเกณฑ์ที่แก้ไข

หัวข้อ	รายละเอียดเดิม	รายละเอียดการแก้ไข
		ผู้ประกอบธุรกิจต้องกำกับดูแลและจัดให้มีการควบคุมความปลอดภัยระบบเทคโนโลยีสารสนเทศที่เหมาะสมและมีประสิทธิภาพและประสิทธิผล สอดคล้องกับผลการประเมินความเสี่ยง โดยแบ่งแนวปฏิบัติออกเป็น 2 ระดับ คือ (1) แนวปฏิบัติระดับพื้นฐาน สำหรับผู้ประกอบธุรกิจที่มีความเสี่ยงภาพรวมในระดับต่ำหรือปานกลาง (2) แนวปฏิบัติระดับสูง สำหรับผู้ประกอบธุรกิจที่มีความเสี่ยงภาพรวมในระดับสูง ยกเว้น ผู้ประกอบธุรกิจขนาดเล็กที่ไม่มีการให้บริการระบบสารสนเทศในการรับส่งรายการธุรกรรมโดยตรงจากนักลงทุนผ่านเครือข่ายอินเทอร์เน็ต และไม่มีการดำเนินการในลักษณะการดูแลทรัพย์สินของนักลงทุน หรือไม่มีการให้บริการหรือเก็บรักษาเครื่องมือชำระเงินหรือข้อมูลที่ใช้ในการชำระเงิน ให้ดำเนินการเฉพาะการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศขั้นต่ำที่จำเป็น (cyber hygiene) ได้แก่ (ก) การบริหารบัญชีผู้ใช้งานสิทธิสูง (privileged user management) (ข) การบริหารจัดการมาตรฐานการตั้งค่าระบบ (system configuration management) (ค) การรักษาความมั่นคงปลอดภัยของเครื่องแม่ข่าย (server) และอุปกรณ์ที่ใช้ปฏิบัติงาน (endpoint) (ง) การประเมินช่องโหว่ทางเทคนิค (technical vulnerability assessment) (จ) การทดสอบเจาะระบบ (penetration test) (ฉ) การบริหารจัดการโปรแกรมแก้ไขช่องโหว่ (patch management)
บทบาทหน้าที่และความรับผิดชอบของคณะกรรมการของผู้ประกอบธุรกิจ	- เดิมไม่ได้กำหนด -	คณะกรรมการของผู้ประกอบธุรกิจมีหน้าที่ความรับผิดชอบในการกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศให้สอดรับกับระดับความเสี่ยงที่ยอมรับได้ และเป็นส่วนหนึ่งของการบริหารความเสี่ยงขององค์กร (enterprise risk management) ซึ่งอย่างน้อยต้องครอบคลุมความรับผิดชอบ ดังต่อไปนี้

เอกสารเปรียบเทียบรายละเอียดของหลักเกณฑ์เดิม และหลักเกณฑ์ที่แก้ไข

หัวข้อ	รายละเอียดเดิม	รายละเอียดการแก้ไข
		(1) จัดให้มีกรอบการกำกับดูแลด้านเทคโนโลยีสารสนเทศ และกำกับดูแลแผนงานด้านเทคโนโลยีสารสนเทศให้สอดคล้องกับแผนทางธุรกิจ และเพียงพอที่จะรองรับการเปลี่ยนแปลงด้านเทคโนโลยี และการเปลี่ยนแปลงการดำเนินธุรกิจในอนาคต (2) กำกับดูแลให้มีการจัดสรรทรัพยากรทางด้านเทคโนโลยีสารสนเทศให้มีความเพียงพอเหมาะสมและทรัพยากรบุคคลให้เพียงพอต่อการดำเนินธุรกิจ (3) กำกับดูแลการกำหนดนโยบายเกี่ยวกับความเสี่ยงด้านเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร โดยอย่างน้อยครอบคลุมนโยบายดังต่อไปนี้ - การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management Policy) และ - การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security Policy) (4) กำกับดูแลให้มีการนำนโยบายที่ได้รับการอนุมัติมาจัดทำแนวปฏิบัติในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ และการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ รวมถึงกำกับดูแลให้มีการนำไปปฏิบัติอย่างเหมาะสม (5) กำกับดูแลให้มีการสร้างความรู้และความตระหนักด้านความเสี่ยงด้านเทคโนโลยีสารสนเทศ แก่กรรมการ ผู้บริหาร และบุคลากรในองค์กรอย่างต่อเนื่องและมีประสิทธิผล (6) กำกับดูแลให้มีการติดตาม ตรวจสอบ และรายงานผลการปฏิบัติตามนโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศต่อคณะกรรมการของผู้ประกอบธุรกิจอย่างน้อยปีละ 1 ครั้ง และในกรณีที่มีเหตุการณ์หรือการเปลี่ยนแปลงใด ๆ ซึ่งอาจส่งผลกระทบต่อการปฏิบัติตามนโยบายดังกล่าวอย่างมีนัยสำคัญ ต้องจัดให้มีการรายงานให้คณะกรรมการของผู้ประกอบธุรกิจทราบโดยไม่ชักช้าด้วย
	การรายงานการปฏิบัติตามนโยบายฯ ให้คณะกรรมการทราบมีเนื้อหาครอบคลุมถึงเรื่องดังต่อไปนี้ (1) กิจกรรมที่เกี่ยวข้องกับการปฏิบัติงานด้านการบริหารความเสี่ยง หรือการจัดสรรและบริหารทรัพยากรด้าน IT	คณะกรรมการของผู้ประกอบธุรกิจควรกำกับดูแลให้มีการติดตาม ตรวจสอบ และรายงานผลการปฏิบัติตามนโยบายที่เกี่ยวข้องกับการกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยการรายงานต่อคณะกรรมการของผู้ประกอบธุรกิจ ควรมีเนื้อหาครอบคลุมถึงเรื่องดังต่อไปนี้ ตามรอบระยะเวลาที่เหมาะสม

เอกสารเปรียบเทียบรายละเอียดของหลักเกณฑ์เดิม และหลักเกณฑ์ที่แก้ไข

หัวข้อ	รายละเอียดเดิม	รายละเอียดการแก้ไข
	เช่น สรุปผลการบริหารจัดการด้านความเสี่ยง/การจัดสรรทรัพยากร IT ในรอบปี เป็นต้น (2) ความคืบหน้าของงานโครงการ (ถ้ามี) (3) การปฏิบัติตามกฎระเบียบ ข้อบังคับ หรือข้อตกลงที่จัดทำกับบุคคลภายนอกและภายในบริษัท (4) ความมีประสิทธิภาพของการนำเทคโนโลยีสารสนเทศมาใช้ (5) ประเด็นปัญหาและอุปสรรค	(1) ผลการประเมินและการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยหน่วยงานที่ทำหน้าที่บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศหรือหน่วยงานที่เกี่ยวข้อง (2) ผลการปฏิบัติตามกฎระเบียบ ข้อบังคับ หรือนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศในภาพรวมของบริษัท โดยหน่วยงานที่ทำหน้าที่กำกับดูแลการปฏิบัติงานด้านเทคโนโลยีสารสนเทศหรือหน่วยงานที่เกี่ยวข้อง (3) ผลการตรวจสอบด้านเทคโนโลยีสารสนเทศและความคืบหน้าในการดำเนินการแก้ไขข้อตรวจพบ โดยหน่วยงานที่ทำหน้าที่ตรวจสอบด้านเทคโนโลยีสารสนเทศหรือหน่วยงานที่เกี่ยวข้อง (4) ผลการปฏิบัติงานด้านเทคโนโลยีสารสนเทศที่สำคัญ เช่น (ก) ปัญหาหรือเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศที่สำคัญ (ข) ความเพียงพอของทรัพยากรด้านเทคโนโลยีสารสนเทศ (capacity and system utilization) (ค) ความคืบหน้าของโครงการด้านเทคโนโลยีสารสนเทศในภาพรวมและโครงการที่สำคัญ (ง) การปฏิบัติงานด้านเทคโนโลยีสารสนเทศตามข้อตกลงที่จัดทำกับบุคคลภายนอก เช่น ผลการดำเนินการตามข้อตกลงการให้บริการ (service level agreement) เป็นต้น (จ) ผลการทดสอบแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ และการใช้งานแผน (ถ้ามี)
โครงสร้างการกำกับดูแล	- เดิมไม่ได้กำหนด -	จัดให้มีโครงสร้างการกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศที่มีการถ่วงดุลอำนาจอย่างอิสระ (check and balance) และมีการแบ่งแยกหน้าที่อย่างเหมาะสม ตามหลักการแบ่งแยกหน้าที่ความรับผิดชอบ 3 ระดับ (Three Lines of Defense: 3 LoDs)

เอกสารเปรียบเทียบรายละเอียดของหลักเกณฑ์เดิม และหลักเกณฑ์ที่แก้ไข

หัวข้อ	รายละเอียดเดิม	รายละเอียดการแก้ไข
	- เดิมไม่ได้กำหนด -	[ปรับปรุงจาก Focus Group][1] [ผู้ประกอบธุรกิจความเสี่ยงสูง] จัดให้มีกรรมการหรือที่ปรึกษาอย่างน้อย 1 ท่าน ที่มีความรู้หรือประสบการณ์ด้านเทคโนโลยีสารสนเทศ โดยพิจารณาจาก (1) จบการศึกษาในสาขาเทคโนโลยีสารสนเทศ หรือสาขาที่เกี่ยวข้อง หรือ (2) มีประสบการณ์ในตำแหน่งหัวหน้าหน่วยงาน หรือมีหน้าที่รับผิดชอบเป็นผู้บริหารงานหลัก หรือมีประสบการณ์ในด้านการให้คำปรึกษาที่เกี่ยวข้องด้านเทคโนโลยีสารสนเทศ หรือ (3) มีประสบการณ์หรือได้รับแต่งตั้งเป็นสมาชิกในคณะกรรมการหรือคณะทำงานที่เกี่ยวข้องด้านเทคโนโลยีสารสนเทศ ทั้งนี้ ผู้ประกอบธุรกิจอาจใช้เกณฑ์ด้านอื่นในการพิจารณาตามความเหมาะสม กรณีที่คณะกรรมการของผู้ประกอบธุรกิจแต่งตั้งคณะกรรมการชุดย่อยเพื่อทำหน้าที่ให้คำปรึกษาด้านเทคโนโลยีสารสนเทศแก่คณะกรรมการ ควรกำหนดบทบาทหน้าที่อย่างชัดเจนและเป็นลายลักษณ์อักษร
	- เดิมไม่ได้กำหนด -	[ปรับปรุงจาก Focus Group] [ผู้ประกอบธุรกิจความเสี่ยงสูง] จัดให้มีผู้บริหารระดับสูง (Chief Information Security Officer: CISO) หรือหัวหน้าสายงานที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Head of Information Security) โดยมีคุณสมบัติ ขอบเขตอำนาจ และบทบาทและหน้าที่อย่างน้อยดังนี้ (1) มีความเป็นอิสระจากหน่วยงานที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT operation) และงานด้านพัฒนาระบบเทคโนโลยีสารสนเทศ (IT development) (2) เป็นผู้ที่มีความรู้ความสามารถหรือมีประสบการณ์ด้านเทคโนโลยีสารสนเทศและด้านการบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

[1] [ปรับปรุงจาก Focus Group] หมายถึง รายละเอียดมีการปรับปรุงเพิ่มเติมจากการหารือกลุ่มย่อยกับผู้ประกอบธุรกิจ (Focus group) เมื่อวันที่ 19 และ 21 ตุลาคม 2564

เอกสารเปรียบเทียบรายละเอียดของหลักเกณฑ์เดิม และหลักเกณฑ์ที่แก้ไข

หัวข้อ	รายละเอียดเดิม	รายละเอียดการแก้ไข
		(3) มีอำนาจหน้าที่ (authority) เพียงพอในการปฏิบัติหน้าที่ได้อย่างมีประสิทธิภาพและประสิทธิผล โดยสามารถดำเนินการอย่างน้อย ดังนี้ (ก) รายงานปัญหาหรือเหตุการณ์ที่มีนัยสำคัญซึ่งกระทบต่อความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศต่อผู้บริหารในตำแหน่งสูงสุดขององค์กร และคณะกรรมการที่เกี่ยวข้องโดยตรง (ข) ให้ความเห็นด้านภัยคุกคามทางไซเบอร์และการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศต่อคณะกรรมการของผู้ประกอบธุรกิจ หรือคณะกรรมการที่เกี่ยวข้องกับการบริหารจัดการและกำกับดูแลการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ และร่วมตัดสินใจดำเนินการในเรื่องความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และภัยคุกคามทางไซเบอร์ที่มีผลกระทบอย่างมีนัยสำคัญ
	- เดิมไม่ได้กำหนด -	[ผู้ประกอบธุรกิจความเสี่ยงสูง] คณะกรรมการของผู้ประกอบธุรกิจอาจแต่งตั้งคณะกรรมการเพื่อทำหน้าที่ที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ เช่น (1) คณะกรรมการกำกับดูแลและบริหารจัดการด้านเทคโนโลยีสารสนเทศ (เช่น IT Steering Committee หรือคณะกรรมการที่ได้รับมอบหมาย เป็นต้น) (2) คณะกรรมการกำกับดูแลการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (เช่น คณะกรรมการบริหารความเสี่ยง หรือคณะกรรมการที่ได้รับมอบหมาย เป็นต้น) (3) คณะกรรมการกำกับดูแลการตรวจสอบด้านเทคโนโลยีสารสนเทศ (เช่น คณะกรรมการตรวจสอบ หรือคณะกรรมการที่ได้รับมอบหมาย เป็นต้น)
นโยบายเรื่องการจัดสรรและบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศ	จัดให้มีนโยบายการเรื่องการจัดสรรและบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศ ซึ่งครอบคลุมถึงการจัดสรรทรัพยากรให้เพียงพอต่อการดำเนินธุรกิจ และการกำหนดแนวทางเพื่อรองรับในกรณีที่ไม่สามารถจัดสรรทรัพยากรได้เพียงพอตามที่กำหนดไว้	ยกเลิกข้อกำหนด

เอกสารเปรียบเทียบรายละเอียดของหลักเกณฑ์เดิม และหลักเกณฑ์ที่แก้ไข

หัวข้อ	รายละเอียดเดิม	รายละเอียดการแก้ไข
นโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ	นโยบายการบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ควรมีรายละเอียดครอบคลุมในเรื่องดังต่อไปนี้ (1) การระบุความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (IT-related risk) (2) การประเมินความเสี่ยง ซึ่งครอบคลุมถึงโอกาสหรือความถี่ที่จะเกิดความเสี่ยง และความมีนัยสำคัญหรือผลกระทบที่จะเกิดขึ้น เพื่อจัดลำดับความสำคัญในการบริหารจัดการความเสี่ยง (3) การกำหนดเครื่องมือและมาตรการในการบริหารและจัดการความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้ (Risk Appetite) (4) การกำหนดตัวชี้วัดระดับความเสี่ยง (IT Risk Indicator) สำหรับความเสี่ยงสำคัญที่สอดคล้องกับความเสี่ยงที่ระบุตาม (1) รวมถึงจัดให้มีการติดตามและรายงานผลตัวชี้วัดดังกล่าว (5) การกำหนดหน้าที่และความรับผิดชอบของผู้รับผิดชอบและผู้ทำหน้าที่บริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ	นโยบายการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ควรมีรายละเอียดครอบคลุมในเรื่องดังต่อไปนี้ (1) บทบาทหน้าที่ของผู้ที่เกี่ยวข้องในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (2) เกณฑ์ความเสี่ยง (risk criteria) โดยครอบคลุมถึงโอกาสหรือความถี่ที่จะเกิดเหตุการณ์ความเสี่ยง และความมีนัยสำคัญหรือระดับผลกระทบที่อาจจะเกิดขึ้น เพื่อจัดลำดับความสำคัญในการบริหารจัดการความเสี่ยง (3) ระดับความเสี่ยงที่ยอมรับได้ (risk appetite) (4) การประเมินความเสี่ยง (risk assessment) ที่ครอบคลุมความเสี่ยงด้านเทคโนโลยีสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคล (privacy) จากการใช้งานเทคโนโลยีสารสนเทศ (5) การจัดการความเสี่ยง (risk treatment) ให้ความเสี่ยงที่เหลืออยู่ (residual risk) อยู่ในระดับความเสี่ยงที่ยอมรับได้ (6) การจัดทำทะเบียนความเสี่ยง (risk register) (7) การติดตามและทบทวนความเสี่ยง (risk monitor and review) (8) การรายงานความเสี่ยง (risk reporting) และผลการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศต่อคณะกรรมการของผู้ประกอบธุรกิจหรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบธุรกิจ อย่างน้อยปีละ 1 ครั้ง
	- เดิมไม่ได้กำหนด -	[ปรับปรุงจาก Focus Group] ในกรณีที่มีความจำเป็นหรือมีข้อจำกัดที่ทำให้ไม่สามารถปฏิบัติตามนโยบาย แนวปฏิบัติ และขั้นตอนที่กำหนดไว้ ผู้ประกอบธุรกิจควรดำเนินการขออนุมัติยกเว้น (exception) จากผู้มีอำนาจเพื่อประเมินความเสี่ยงและกำหนดมาตรการการควบคุมเพื่อลดความเสี่ยงอย่างเพียงพอเหมาะสมก่อนดำเนินการต่อไป นอกจากนี้ ควรจัดเก็บหลักฐานการอนุมัติยกเว้นดังกล่าวอย่างเป็นลายลักษณ์อักษร และจัดให้มีกระบวนการสอบทานความเหมาะสมของรายการขอยกเว้น ตลอดจนมาตรการในการจัดการเพื่อลดความเสี่ยงดังกล่าวอย่างน้อยปีละ 1 ครั้ง

เอกสารเปรียบเทียบรายละเอียดของหลักเกณฑ์เดิม และหลักเกณฑ์ที่แก้ไข

หัวข้อ	รายละเอียดเดิม	รายละเอียดการแก้ไข
โครงสร้างการบริหารงานเพื่อการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ	จัดให้มีการกำหนดนโยบายการใช้งานระบบสารสนเทศร่วมกันบนระบบเครือข่ายคอมพิวเตอร์เพื่อการประมวลผลตามความต้องการของผู้ใช้งาน (cloud computing) ซึ่งครอบคลุมถึงวิธีการคัดเลือก และประเมินผู้ให้บริการ การทบทวนคุณสมบัติของผู้ให้บริการ ข้อกำหนดเกี่ยวกับการใช้บริการ และการตรวจสอบบันทึกหลักฐานต่าง ๆ ที่อาจส่งผลกระทบต่อการใช้บริการ	ยกเลิกข้อกำหนด
การบริหารจัดการบุคลากร	- เดิมไม่ได้กำหนด -	มีกระบวนการคัดเลือกบุคลากรในการปฏิบัติหน้าที่โดยคำนึงถึงความรู้ ความสามารถ และความเพียงพอในการปฏิบัติงาน และมีการตรวจสอบข้อมูลของบุคลากรก่อนการว่าจ้างอย่างเพียงพอและสอดคล้องกับความเสี่ยงของตำแหน่งงานและหน้าที่ความรับผิดชอบ
	- เดิมไม่ได้กำหนด -	กำหนดบทบาทหน้าที่และความรับผิดชอบเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการไม่เปิดเผยข้อมูล (non-disclosure agreement) ในข้อตกลงการจ้างงาน
	- เดิมไม่ได้กำหนด -	จัดให้มีเอกสารข้อกำหนดในการใช้งานทรัพย์สินด้านเทคโนโลยีสารสนเทศ (acceptable use policy) โดยครอบคลุมขอบเขตความรับผิดชอบของผู้ใช้งาน รายการสิ่งที่ผู้ใช้งานต้องปฏิบัติและสิ่งที่ผู้ใช้งานห้ามปฏิบัติ
	ให้ความรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศที่เกี่ยวข้องกับการปฏิบัติหน้าที่แก่บุคลากรของผู้ประกอบธุรกิจและบุคคลภายนอกที่ปฏิบัติงานดังกล่าว	จัดอบรมและพัฒนาความรู้ด้านเทคโนโลยีสารสนเทศ (training program) ให้แก่บุคลากรของผู้ประกอบธุรกิจ และบุคคลภายนอกที่สามารถเข้าถึงข้อมูลที่มีความสำคัญของผู้ประกอบธุรกิจอย่างสม่ำเสมอ ซึ่งมีเนื้อหาครอบคลุม (1) การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (2) ความเสี่ยงด้านเทคโนโลยีสารสนเทศและความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคล (privacy) จากการใช้งานเทคโนโลยีสารสนเทศ หรือ (3) หลักเกณฑ์และกฎหมายที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ โดยทบทวนแผนอบรมและพัฒนาความรู้ด้านเทคโนโลยีสารสนเทศอย่างน้อยปีละ 1 ครั้ง

เอกสารเปรียบเทียบรายละเอียดของหลักเกณฑ์เดิม และหลักเกณฑ์ที่แก้ไข

หัวข้อ	รายละเอียดเดิม	รายละเอียดการแก้ไข
	- เดิมไม่ได้กำหนด -	กำหนดโปรแกรมในการเสริมสร้างความตระหนัก (awareness program) เรื่องการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ความเสี่ยงด้านเทคโนโลยีสารสนเทศและความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคล (privacy) จากการใช้งานเทคโนโลยีสารสนเทศให้แก่บุคลากร เช่น การทดสอบเรื่อง phishing และการทดสอบเรื่อง social engineering เป็นต้น
	- เดิมไม่ได้กำหนด -	จัดทำกระบวนการรองรับเมื่อมีการเปลี่ยนแปลงตำแหน่งงานหรือสิ้นสุดการจ้างงาน เช่น การคืนทรัพย์สินขององค์กร การปรับปรุงสิทธิให้เป็นปัจจุบัน และยกเลิกสิทธิเมื่อสิ้นสุดการจ้างงาน เป็นต้น รวมทั้งมีการสื่อสารให้ผู้ที่เกี่ยวข้องรับทราบถึงการเปลี่ยนแปลงสิทธิหน้าที่ และความรับผิดชอบ เป็นต้น
การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT Asset Management)	จัดทำทะเบียนทรัพย์สินสารสนเทศประเภทระบบหรืออุปกรณ์ และทบทวนทะเบียนดังกล่าวอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงทรัพย์สินสารสนเทศอย่างมีนัยสำคัญ	กำหนดรายละเอียดในการจัดทำทะเบียนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศประเภทอุปกรณ์ (hardware) ให้ครบถ้วนและเป็นปัจจุบัน โดยครอบคลุมรายการ เช่น (1) เลขทะเบียนทรัพย์สิน (2) ประเภทฮาร์ดแวร์ (3) รายละเอียดทางเทคนิค ยี่ห้อ รุ่น (4) ระบบปฏิบัติการและเวอร์ชัน (5) เจ้าของทรัพย์สิน (6) สถานที่ตั้ง (7) วันที่เริ่มใช้งาน/วันที่ติดตั้ง (8) วันที่สิ้นสุดการรับประกัน หรือสิ้นสุดการใช้งานตามสัญญา (9) ประเภทการครอบครอง (ซื้อ หรือเช่า)
		กำหนดรายละเอียดในการจัดทำทะเบียนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศประเภทระบบ (Software) ให้ครบถ้วนและเป็นปัจจุบัน โดยครอบคลุมรายการ เช่น (1) เลขทะเบียนทรัพย์สิน (2) ชื่อซอฟต์แวร์ (3) รายละเอียดทางเทคนิค / การใช้งาน

เอกสารเปรียบเทียบรายละเอียดของหลักเกณฑ์เดิม และหลักเกณฑ์ที่แก้ไข

หัวข้อ	รายละเอียดเดิม	รายละเอียดการแก้ไข
		(4) ระบบปฏิบัติการและเวอร์ชัน (5) หน่วยงานภายในผู้เป็นเจ้าของซอฟต์แวร์ (6) วันลงทะเบียนซอฟต์แวร์ (7) วันที่สิ้นสุดการใช้บริการ (8) เลขทะเบียนทรัพย์สินฮาร์ดแวร์ที่อ้างอิง
	- เดิมไม่ได้กำหนด -	มีการประเมินความเสี่ยงทรัพย์สินด้านเทคโนโลยีสารสนเทศ ในกรณีที่มีความจำเป็นต้องใช้ระบบปฏิบัติการและอุปกรณ์ที่สิ้นสุดอายุการใช้งาน (end of life) หรือสิ้นสุดการสนับสนุนหรือให้บริการ (end of support) ตลอดจนมีแนวทางในการควบคุมความเสี่ยงอย่างเหมาะสม
การรักษาความมั่นคงปลอดภัยของข้อมูล (Data Security)	- เดิมไม่ได้กำหนด -	ผู้ประกอบธุรกิจควรจัดทำทะเบียนทรัพย์สินประเภทข้อมูล (Data Inventory) ให้ครบถ้วนและเป็นปัจจุบัน โดยควรมีข้อมูล เช่น (1) เลขทะเบียนข้อมูล (2) ชื่อข้อมูลหรือชุดข้อมูล (3) รายละเอียดลักษณะ และประเภทของข้อมูล (4) ระดับชั้นความลับและระดับความสำคัญของข้อมูล (5) เจ้าของหรือผู้ดูแลข้อมูล (data owner) (6) สถานที่ หรือเครื่องแม่ข่ายที่จัดเก็บ
	- เดิมไม่ได้กำหนด -	กำหนดให้มีเจ้าของข้อมูล (data owner) หรือบุคคลที่ได้รับมอบหมายให้ทำหน้าที่รับผิดชอบในการกำหนดผู้ใช้งาน สิทธิการเข้าถึง และการใช้งานข้อมูลอย่างปลอดภัย
	- เดิมไม่ได้กำหนด -	กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล ตลอดจนการคุ้มครองข้อมูลส่วนบุคคลที่สอดคล้องตามชั้นความลับ ครอบคลุมข้อมูลที่อยู่บนอุปกรณ์ที่ใช้ปฏิบัติงาน (data at endpoint) ข้อมูลระหว่างการรับส่งผ่านเครือข่ายคอมพิวเตอร์ (data in transit) และการจัดเก็บข้อมูลบนระบบงานและสื่อบันทึกข้อมูล (data at rest)
	- เดิมไม่ได้กำหนด -	กำหนดระเบียบปฏิบัติในการทำลายข้อมูล (data disposal) โดยกำหนดหน้าที่ความรับผิดชอบของหน่วยงานที่เกี่ยวข้องและวิธีการทำลายข้อมูลให้สอดคล้องกับ

เอกสารเปรียบเทียบรายละเอียดของหลักเกณฑ์เดิม และหลักเกณฑ์ที่แก้ไข

หัวข้อ	รายละเอียดเดิม	รายละเอียดการแก้ไข
		ระดับชั้นความลับ รวมทั้งมีการควบคุมการทำลายข้อมูลที่ครอบคลุมการอนุมัติจากหน่วยงานเจ้าของข้อมูลก่อนดำเนินการ การสอบทานการปฏิบัติงาน และการทำทะเบียนการทำลายข้อมูล
การควบคุมการเข้าถึง (Access Control)	- เดิมไม่ได้กำหนด -	ในการบริหารจัดการบัญชีผู้ใช้งาน ควรดำเนินการอย่างน้อย ดังนี้ (1) กำหนดบัญชีผู้ใช้งาน (user ID) ที่สามารถระบุตัวตนผู้ใช้งานได้ โดยหลีกเลี่ยงการใช้บัญชีผู้ใช้งานที่มีผู้ใช้งานมากกว่า 1 ราย (shared ID) (2) ระงับหรือลบบัญชีผู้ใช้งานทันทีเมื่อสิ้นสุดสภาพการจ้างงาน (3) กำหนดรอบและดำเนินการตรวจสอบบัญชีผู้ใช้งาน อย่างน้อยปีละ 1 ครั้ง (4) ระงับหรือลบบัญชีผู้ใช้งานที่ไม่จำเป็น หรือไม่มีการใช้งานในรอบ 90 วันที่ผ่านมา
	จัดทำนโยบายควบคุมการเข้าถึงข้อมูลและสิ่งอำนวยความสะดวกในการประมวลผลข้อมูลต่าง ๆ โดยมีเนื้อหาครอบคลุมอย่างน้อยดังนี้ (1) กำหนดสิทธิการเข้าถึงข้อมูลและระบบสารสนเทศให้เหมาะสมกับการใช้งานและหน้าที่ความรับผิดชอบของผู้ใช้งาน รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ และยกเลิกสิทธิ ของบุคคลที่ไม่มีความจำเป็นในการเข้าถึงโดยทันที (2) การแบ่งแยกบทบาทหน้าที่ของบุคคลที่เกี่ยวข้อง เช่น บุคคลผู้ร้องขอ (access request) บุคคลผู้มีอำนาจอนุมัติ (access authorization) และบุคคลผู้บริหารสิทธิการเข้าถึง (access administration) เป็นต้น (3) รายละเอียดในส่วนที่เกี่ยวกับการควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ ขั้นต่ำควรครอบคลุมถึงการระบุประเภทหรือบริการทางเครือข่าย (network services) และบุคคลที่ได้รับอนุญาตให้เข้าถึง กระบวนการควบคุม	ในการบริหารจัดการสิทธิการเข้าถึงข้อมูลและระบบสารสนเทศ ควรดำเนินการอย่างน้อย ดังนี้ (1) แบ่งแยกบทบาทหน้าที่ของบุคคลที่เกี่ยวข้องในการจัดสรรสิทธิ เช่น ผู้ร้องขอ (access request) ผู้มีอำนาจอนุมัติ (access authorization) และผู้ดูแลสิทธิ์การเข้าถึง (access administration) เป็นต้น เพื่อให้สอดคล้องตามหลักการถ่วงดุล (check and balance) (2) มีกระบวนการอนุมัติสิทธิในการเข้าถึงข้อมูลและระบบสารสนเทศโดยผู้มีอำนาจ เช่น เจ้าของระบบ หรือเจ้าของข้อมูล (3) พิจารณาสิทธิ์ของผู้ใช้งานโดยคำนึงถึงความจำเป็นต้องรู้ (need-to-know) ความจำเป็นต้องใช้งาน (need-to-use) และหลักการแบ่งแยกหน้าที่ความรับผิดชอบ (segregation of duties) อย่างชัดเจน (4) จัดทำตารางควบคุมการให้สิทธิ (authorization matrix) ของบัญชีผู้ใช้งานที่สอดคล้องกับตำแหน่งหน้าที่งานตามหลักการตามความจำเป็นของหน้าที่รับผิดชอบ โดยมีการทบทวนตารางควบคุมการให้สิทธิ์ของบัญชีผู้ใช้งานอย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ (5) ปรับปรุงสิทธิของผู้ใช้งานเมื่อมีการเปลี่ยนแปลงหน้าที่ความรับผิดชอบหรือตำแหน่งงาน

เอกสารเปรียบเทียบรายละเอียดของหลักเกณฑ์เดิม และหลักเกณฑ์ที่แก้ไข

หัวข้อ	รายละเอียดเดิม	รายละเอียดการแก้ไข
	และป้องกันการเข้าถึง วิธีการเข้าถึงแบบปลอดภัย เทคนิคการระบุตัวตน และการติดตามการใช้งานของบุคคลที่ได้รับอนุญาตให้เข้าถึง (4) การมีระบบที่ระบุผู้ใช้งานในระบบเครือข่ายคอมพิวเตอร์ได้อย่างชัดเจน โดยเฉพาะกรณีที่ผู้ประกอบธุรกิจใช้หมายเลขประจำเครื่องแบบพลวัต (dynamic IP address) เพื่อให้ผู้ประกอบธุรกิจมีข้อมูลที่สามารถระบุผู้ใช้งานหมายเลข IP address ในช่วงเวลาที่ใช้งานได้	(6) เพิกถอนสิทธิของผู้ใช้งานทันทีเมื่อสิ้นสุดสภาพการเป็นพนักงาน หรือเมื่อไม่มีความจำเป็นต้องใช้งาน (7) ติดตามและทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ โดยกำหนดรอบระยะเวลาในการทบทวนสิทธิ์ให้สอดคล้องกับความเสี่ยงและความสำคัญของสิทธิ ควรจัดให้มีการทบทวนสิทธิ์ทุกประเภท อย่างน้อยปีละ 1 ครั้ง
	- เดิมไม่ได้กำหนด -	จัดให้มีกระบวนการยืนยันตัวตนผู้ใช้งาน (authentication) ที่มีประสิทธิภาพเหมาะสมกับความเสี่ยง และป้องกันการปฏิเสธความรับผิด โดยดำเนินการอย่างน้อย ดังนี้ (1) มีการยืนยันตัวตนผู้ใช้งานที่เหมาะสมกับความเสี่ยง เพื่อใช้ควบคุมการเข้าถึงข้อมูล และระบบสารสนเทศ (2) กรณีที่มีรหัสผ่านครั้งแรกสำหรับผู้ใช้งาน ต้องมีวิธีการจัดส่งรหัสผ่านให้แก่ผู้ใช้งานอย่างรัดกุมและปลอดภัย และกำหนดให้ผู้ใช้งานเปลี่ยนแปลงรหัสผ่านทันทีที่ได้รับรหัสดังกล่าว (3) กำหนดให้ผู้ใช้งานตั้งรหัสผ่านที่ซับซ้อนและยากต่อการคาดเดา เช่น มีความยาวขั้นต่ำอย่างน้อย 8 ตัวอักษร โดยอาจประกอบด้วยอักขระพิเศษ (เช่น “#”) เป็นต้น (4) จำกัดจำนวนครั้งที่ยืนยันตัวตนผิดพลาด หรือกำหนดให้ผู้ใช้งานรอหลังจากยืนยันตัวตนผิดพลาดเป็นระยะเวลาหนึ่ง หรือกำหนดวิธีการอื่น ๆ ที่เทียบเท่าเพื่อป้องกันการเข้าใช้งานโดยวิธีเดาสุ่ม (brute force) ทั้งนี้ ในทางปฏิบัติไม่ควรยอมให้ผู้ใช้งานยืนยันตัวตนผิดพลาดติดต่อกันเกิน 3 ครั้ง (5) ในการเปลี่ยนรหัสผ่านแต่ละครั้ง ไม่ควรกำหนดรหัสผ่านใหม่ซ้ำกับรหัสที่ใช้งานครั้งล่าสุดอย่างน้อย 12 ครั้ง (6) ระหว่างที่ผู้ใช้งานใส่รหัสผ่าน ระบบไม่ควรแสดงให้เห็นค่ารหัสผ่านบนหน้าจอ

เอกสารเปรียบเทียบรายละเอียดของหลักเกณฑ์เดิม และหลักเกณฑ์ที่แก้ไข

หัวข้อ	รายละเอียดเดิม	รายละเอียดการแก้ไข
		(7) มีวิธีจัดเก็บข้อมูลรหัสผ่านที่ปลอดภัย เพื่อป้องกันการล่วงรู้หรือแก้ไขเปลี่ยนแปลง รวมทั้งไม่จัดเก็บข้อมูลรหัสผ่านใน folder เดียวกันกับ folder ที่จัดเก็บข้อมูลของแอปพลิเคชัน (8) กำหนดให้ผู้ใช้งานรับผิดชอบการใช้งานบัญชีผู้ใช้งาน (user ID) การรักษาความปลอดภัยสิ่งที่ใช้ยืนยันตัวตน (authenticator) เช่น รหัสผ่าน รหัสที่ใช้ครั้งเดียว (one-time password) เป็นต้น รวมทั้งข้อมูลส่วนบุคคลที่อาจนำมาใช้เพื่อขอเปลี่ยนแปลงข้อมูลบัญชีผู้ใช้งาน เพื่อป้องกันการใช้งานจากผู้ไม่หวังดี
	- เดิมไม่ได้กำหนด -	กำหนดกระบวนการบริหารบัญชีผู้ใช้งานที่มีสิทธิสูง (privileged user management) อย่างเข้มงวด เช่น (1) ใช้งานสิทธิสูงเมื่อมีความจำเป็น โดยมีขั้นตอนการร้องขอ และการอนุมัติการใช้งานโดยผู้มีอำนาจ (2) ห้ามใช้งานบัญชีผู้ใช้งานสิทธิสูงร่วมกัน (shared account) (3) จำกัดจำนวนบัญชีผู้ใช้งานสิทธิสูงให้มีจำนวนน้อยที่สุด หรือเท่าที่จำเป็นเท่านั้น (4) กำหนดนโยบายการยืนยันตัวตนของบัญชีผู้ใช้งานสิทธิสูงที่เข้มงวดกว่าบัญชีผู้ใช้งานทั่วไป (5) กำหนดกระบวนการร้องขอเพื่อเข้าใช้งาน และกำหนดระยะเวลาการใช้งานที่ชัดเจน (6) ระงับ หรือยกเลิกบัญชีผู้ใช้งานสิทธิสูง เมื่อสิ้นสุดการปฏิบัติงาน (7) จัดเก็บข้อมูลประวัติการยืนยันตัวตนและการเข้าถึง (access log) และกิจกรรม (activity log) พร้อมทั้งสอบทานข้อมูลดังกล่าวอย่างสม่ำเสมอ
	- เดิมไม่ได้กำหนด -	จัดให้มีขั้นตอนหรือระบบติดตามแจ้งเตือนเมื่อมีการใช้งานสิทธิระดับสูง เช่น การแจ้งเตือนผู้เกี่ยวข้องเมื่อมีการเข้าใช้งาน หรือ การใช้เครื่องมือควบคุมบัญชีผู้ใช้งานที่มีสิทธิที่มีสูง (privilege access management: PAM)

เอกสารเปรียบเทียบรายละเอียดของหลักเกณฑ์เดิม และหลักเกณฑ์ที่แก้ไข

หัวข้อ	รายละเอียดเดิม	รายละเอียดการแก้ไข
	- เดิมไม่ได้กำหนด -	ใช้วิธีการยืนยันตัวตนแบบหลายปัจจัย (multi-factor authentication) เพื่อเข้าใช้งานหรือเปลี่ยนแปลงรหัสผ่านของบัญชีผู้ใช้งานที่มีสิทธิสูง สำหรับระบบปฏิบัติการและระบบฐานข้อมูลที่เกี่ยวข้องกับระบบสารสนเทศที่มีความสำคัญ ทั้งนี้ ในกรณีผู้ประกอบธุรกิจมีข้อจำกัดสำหรับการพิสูจน์ตัวตนแบบหลายปัจจัย สามารถใช้วิธีการอื่นใดที่มีประสิทธิภาพเทียบเท่าทดแทน และจัดให้มีการประเมินความเสี่ยงและพิจารณาแนวทางควบคุมความเสี่ยงก่อนดำเนินการเพื่อขออนุมัติยกเว้น (exception)
	- เดิมไม่ได้กำหนด -	[ผู้ประกอบธุรกิจความเสี่ยงสูง] มีระบบอัตโนมัติในการตรวจสอบและแจ้งเตือนพฤติกรรมต้องสงสัยในขั้นตอนการยืนยันตัวตนของผู้ใช้งาน เช่น การเข้าสู่ระบบงานจากเครื่องคอมพิวเตอร์ต้นทางพร้อมกันหลายเครื่อง หรือการเข้าสู่ระบบจากเครื่องคอมพิวเตอร์ต้นทางที่มีความแตกต่างกันด้านสถานที่ทางภูมิศาสตร์ภายในระยะเวลาอันสั้น เป็นต้น
การบริหารจัดการการเข้ารหัสข้อมูล (Cryptography)	ผู้ประกอบธุรกิจควรจัดให้มีนโยบายการบริหารกุญแจเพื่อการเข้ารหัสข้อมูลตลอดช่วงเวลาการใช้งาน (key management whole life cycle) โดยกำหนดแนวปฏิบัติเพื่อการคัดเลือกวิธีการเข้ารหัส การกำหนดความยาวของรหัส การใช้งานและการยกเลิกการใช้งานกุญแจเพื่อการเข้ารหัส กระบวนการบริหารจัดการกุญแจเพื่อการเข้ารหัส รวมทั้งติดตามให้มีการปฏิบัติให้เป็นไปตามนโยบายและแนวทางปฏิบัติดังกล่าวอย่างสม่ำเสมอ	ในการบริหารจัดการกุญแจเข้ารหัสข้อมูล (key management life cycle) ผู้ประกอบธุรกิจควรกำหนดกระบวนการที่ครอบคลุมอย่างน้อยในเรื่อง ดังนี้ (1) การสร้างและติดตั้งกุญแจเข้ารหัส (ก) มีมาตรการควบคุมสภาพแวดล้อมและกระบวนการในการสร้างกุญแจเข้ารหัสที่รัดกุมปลอดภัย เช่น เลือกใช้ผู้ให้บริการออกใบรับรอง (certification authority) ที่น่าเชื่อถือ และทำลายข้อมูลที่ใช้ในกระบวนการเข้ารหัสเพื่อควบคุมความเสี่ยงจากการเข้าถึงหรือกู้คืนกุญแจเข้ารหัสข้อมูลโดยไม่ได้รับอนุญาต (ข) กำหนดสิทธิการเข้าถึงกุญแจเข้ารหัส และระบบจัดการกุญแจเข้ารหัสให้สามารถเข้าถึงได้โดยผู้ที่มีความจำเป็นและได้รับอนุญาตเท่านั้น โดยในกรณีที่มีการบริหารจัดการกุญแจเข้ารหัสโดยบุคคล ต้องใช้วิธีการพิสูจน์ตัวตนอย่างรัดกุมปลอดภัย (ค) กำหนดความยาวของกุญแจเข้ารหัสที่เพียงพอในการป้องกันการถูกถอดรหัส เช่น การโจมตีแบบ brute force เป็นต้น (ง) การแลกเปลี่ยนกุญแจต้องผ่านกระบวนการและช่องทางที่ปลอดภัย

เอกสารเปรียบเทียบรายละเอียดของหลักเกณฑ์เดิม และหลักเกณฑ์ที่แก้ไข

หัวข้อ	รายละเอียดเดิม	รายละเอียดการแก้ไข
		(จ) กำหนดไม่ให้ใช้กุญแจเข้ารหัสข้อมูลเดียวกันกับหลายระบบงาน (2) การจัดเก็บและการสำรองกุญแจเข้ารหัส (ก) มีการรักษาความปลอดภัยในการจัดเก็บกุญแจเพื่อการเข้ารหัส เพื่อให้มั่นใจว่ากุญแจถูกจัดเก็บอย่างรัดกุมปลอดภัย เช่น การใช้อุปกรณ์รักษาความปลอดภัย HSM หรืออุปกรณ์ที่มีการควบคุมการเข้าถึงอย่างปลอดภัย เป็นต้น (ข) มีการสำรองกุญแจเข้ารหัส โดยการวิธีการเข้ารหัส (key encryption key) ที่มีความปลอดภัยไม่น้อยไปกว่ากุญแจเข้ารหัสชุดหลัก (ค) มีการจัดเก็บข้อมูลบันทึกเหตุการณ์กิจกรรมที่เกี่ยวกับการบริหารจัดการกุญแจเข้ารหัส (3) การเพิกถอนหรือทำลายกุญแจเข้ารหัส โดยกำหนดเกณฑ์ในการเพิกถอนกุญแจเข้ารหัส เช่น กุญแจเข้ารหัสหมดอายุการใช้งาน หรือไม่ปลอดภัย เป็นต้น และกำหนดกระบวนการเพิกถอนหรือทำลายกุญแจ เพื่อให้มั่นใจว่าจะไม่สามารถนำกุญแจนั้นมาใช้งานได้อีก
	-เดิมไม่ได้กำหนด-	หากไม่สามารถสร้างกุญแจการเข้ารหัสด้วยตนเองได้ ผู้ประกอบธุรกิจควรมีการดำเนินการเพื่อให้มั่นใจได้ว่ากุญแจการเข้ารหัสของบุคคลภายนอกไม่มีการนำมาใช้ร่วมกับผู้ใช้บริการรายอื่น และทราบถึงรายละเอียดเกี่ยวกับระบบการบริหารจัดการกุญแจเข้ารหัสข้อมูลของบุคคลภายนอก (due diigence) ได้แก่ (1) ประเภทของกุญแจเข้ารหัสข้อมูล (2) รายละเอียดของระบบหรือเครื่องมือเข้ารหัส รวมถึงกระบวนการบริหารจัดการการเข้ารหัสข้อมูลในแต่ละขั้นตอนตลอดวงจรการบริหารจัดการกุญแจการเข้ารหัส (3) ข้อแนะนำการใช้งานและการบริหารจัดการการเข้ารหัสข้อมูล
	-เดิมไม่ได้กำหนด-	ผู้ประกอบธุรกิจควรกำหนดกระบวนการรองรับกรณีเกิดการรั่วไหลของกุญแจเข้ารหัส เช่น การติดต่อหน่วยงานหรือผู้ที่เกี่ยวข้องกับชุดข้อมูลที่ใช้กุญแจเข้ารหัสชุดดังกล่าว

เอกสารเปรียบเทียบรายละเอียดของหลักเกณฑ์เดิม และหลักเกณฑ์ที่แก้ไข

หัวข้อ	รายละเอียดเดิม	รายละเอียดการแก้ไข
		การตรวจสอบชุดข้อมูลที่มีความเสี่ยงในการรั่วไหล การเปลี่ยนหรือเพิกถอนกุญแจ การเข้ารหัสข้อมูล เป็นต้น
การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environmental Security)	ผู้ประกอบธุรกิจต้องมีมาตรการเพื่อสร้างความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (physical and environmental security) ของทรัพย์สินสารสนเทศตามหลักเกณฑ์ดังต่อไปนี้ (1) ประเมินความเสี่ยงและความสำคัญของทรัพย์สินสารสนเทศ (2) กำหนดพื้นที่หวงห้ามและพื้นที่สำหรับจัดวางทรัพย์สินสารสนเทศที่มีความสำคัญให้มีความมั่นคงปลอดภัยและป้องกันมิให้บุคคลที่ไม่เกี่ยวข้องเข้าถึงพื้นที่ดังกล่าว	ผู้ประกอบธุรกิจต้องจัดให้มีการสร้างความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (physical and environmental security) รวมทั้งมีระบบการป้องกันและกระบวนการในการบำรุงรักษาอุปกรณ์คอมพิวเตอร์ และระบบสาธารณูปโภค (facilities) ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศอย่างเหมาะสม เพื่อให้สามารถป้องกันการเข้าถึง และป้องกันการสร้างความเสียหายต่อทรัพย์สินด้านเทคโนโลยีสารสนเทศที่จัดเก็บอยู่ในศูนย์คอมพิวเตอร์หลัก ศูนย์คอมพิวเตอร์สำรอง และศูนย์คอมพิวเตอร์จากผู้ให้บริการภายนอก (co-location) ตลอดจนมีการป้องกันความปลอดภัยทางกายภาพของอุปกรณ์เทคโนโลยีสารสนเทศอื่น ๆ
	ผู้ประกอบธุรกิจควรออกแบบพื้นที่หวงห้ามโดยคำนึงถึงความมั่นคงปลอดภัยจากภัยธรรมชาติและภัยคุกคามจากมนุษย์ และให้มีความมิดชิด รวมทั้งป้องกันมิให้มีการเปิดเผยข้อมูลและรายละเอียดของพื้นที่หวงห้ามต่อสาธารณะ	ผู้ประกอบธุรกิจจัดให้มีมาตรการรักษาความปลอดภัยสำหรับพื้นที่ตั้งของทรัพย์สินด้านเทคโนโลยีสารสนเทศสำคัญ และพื้นที่ปฏิบัติงานสำคัญด้านเทคโนโลยีสารสนเทศ โดยคำนึงถึงความมั่นคงปลอดภัยจากภัยธรรมชาติ และภัยคุกคามจากมนุษย์
	ผู้ประกอบธุรกิจควรมีการติดตามและควบคุมบุคคลภายนอกที่เข้าปฏิบัติงานภายในพื้นที่หวงห้ามอย่างใกล้ชิด	ผู้ประกอบธุรกิจควรควบคุมการเข้า-ออกพื้นที่ตั้งของทรัพย์สินด้านเทคโนโลยีสารสนเทศสำคัญและพื้นที่ปฏิบัติงานสำคัญด้านเทคโนโลยีสารสนเทศของพนักงานที่ไม่ได้มีหน้าที่ปฏิบัติงานประจำหรือบุคคลภายนอกที่เข้าถึงแบบชั่วคราว โดยจัดให้มีการอนุมัติจากผู้มีอำนาจ ลงบันทึกเข้า-ออก และมีการติดตามและควบคุม (escort) อย่างใกล้ชิด ตลอดระยะเวลาปฏิบัติงานในพื้นที่ดังกล่าว
	ผู้ประกอบธุรกิจควรจัดให้มีมาตรการป้องกันสายเคเบิลที่ใช้เพื่อการสื่อสาร สายไฟ และอุปกรณ์ที่เกี่ยวข้อง เช่น floor switch และท่อเดินสายเคเบิลและสายไฟ อย่างรัดกุมและบำรุงรักษาอย่างสม่ำเสมอเพื่อมิให้มีความเสียหาย	ผู้ประกอบธุรกิจควรจัดให้มีมาตรการป้องกันสายเคเบิลและสายไฟของพื้นที่ปฏิบัติงานทั้งภายในและภายนอกศูนย์คอมพิวเตอร์ จากการขัดขวางการทำงาน หรือการทำให้เสียหาย

เอกสารเปรียบเทียบรายละเอียดของหลักเกณฑ์เดิม และหลักเกณฑ์ที่แก้ไข

หัวข้อ	รายละเอียดเดิม	รายละเอียดการแก้ไข
	ผู้ประกอบธุรกิจควรจัดให้มีการดูแลและบำรุงรักษาทรัพย์สินสารสนเทศประเภทอุปกรณ์อย่างถูกวิธี เพื่อให้คงไว้ซึ่งความถูกต้องครบถ้วนและอยู่ในสภาพพร้อมใช้งานอยู่เสมอ	ผู้ประกอบธุรกิจควรจัดให้มีการดูแลและบำรุงรักษาทรัพย์สินด้านเทคโนโลยีสารสนเทศประเภทฮาร์ดแวร์อย่างถูกวิธี มีการทดสอบการใช้งานระบบสาธารณูปโภคอย่างสม่ำเสมอ เพื่อให้อยู่ในสภาพครบถ้วนสมบูรณ์และพร้อมใช้งาน
	ผู้ประกอบธุรกิจควรจัดให้มีการควบคุมป้องกันทรัพย์สินสารสนเทศประเภทอุปกรณ์ระหว่างที่ไม่มีผู้ใช้งาน (unattended user equipment) ให้มีความปลอดภัย รวมทั้งควรกำหนดการควบคุมเอกสาร ข้อมูลหรือสื่อบันทึกข้อมูลต่าง ๆ เช่น thumb drive และ external hard disk ที่มีข้อมูลสารสนเทศที่จัดเก็บหรือบันทึกอยู่ ไม่ให้วางทิ้งไว้บนโต๊ะทำงานหรือสถานที่ไม่ปลอดภัยในขณะที่ไม่ได้ใช้งาน (clear desk) ตลอดจนการควบคุมหน้าจอคอมพิวเตอร์ไม่ให้มีข้อมูลสำคัญปรากฏในขณะที่ไม่ได้ใช้งาน (clear screen) เช่น การตัดออกจากระบบ (session time out) หรือการล็อคหน้าจอ (lock screen) อัตโนมัติ เป็นต้น	ย้ายไปยังหมวดการรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ หัวข้อ การรักษาความปลอดภัยของเครื่องแม่ข่าย (server) และอุปกรณ์ที่ใช้ปฏิบัติงาน (endpoint)
การรักษาความมั่งคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT Operations Security)	กำหนดขั้นตอนการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศเพื่อให้การปฏิบัติงานนั้นเป็นไปอย่างถูกต้องและมั่นคงปลอดภัย	ยกเลิกหัวข้อการกำหนดขั้นตอนการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ
	ผู้ประกอบธุรกิจควรกำหนดขั้นตอนการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศเป็นลายลักษณ์อักษรเพื่อให้พนักงานปฏิบัติการคอมพิวเตอร์ (computer operator) สามารถปฏิบัติงานได้อย่างถูกต้องและเป็นไปตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ เช่น ขั้นตอนในการเปิด – ปิดระบบการประมวลผล การตรวจสอบประสิทธิภาพการทำงานของระบบ และตารางเวลาในการปฏิบัติงาน เป็นต้น และควรทบทวนขั้นตอนการปฏิบัติงาน	

เอกสารเปรียบเทียบรายละเอียดของหลักเกณฑ์เดิม และหลักเกณฑ์ที่แก้ไข

หัวข้อ	รายละเอียดเดิม	รายละเอียดการแก้ไข
	ดังกล่าวให้เป็นปัจจุบันอยู่เสมอ รวมทั้งจัดให้อยู่ในสภาพที่พร้อมใช้งานและเข้าถึงได้อยู่เสมอ	
	-เดิมไม่ได้กำหนด-	**การบริหารจัดการมาตรฐานการตั้งค่าระบบ (system configuration management)** ● ผู้ประกอบธุรกิจควรกำหนดมาตรฐานการกำหนดค่าขั้นตอนด้านความมั่นคงปลอดภัย (security configuration standards) สำหรับระบบปฏิบัติการ แอปพลิเคชัน อุปกรณ์รักษาความปลอดภัย และอุปกรณ์เครือข่ายโดยคำนึงถึงหลักการการรักษาความมั่นคงปลอดภัยที่รัดกุมและเหมาะสมกับการใช้งานและการทำงาน โดยครอบคลุมอย่างน้อย ดังต่อไปนี้ (1) ลบบัญชีผู้ใช้งานตั้งต้น หรือเปลี่ยนแปลงรหัสผ่านเมื่อเข้าใช้งานครั้งแรกให้มีความปลอดภัย (2) การกำหนดสิทธิ และวิธีการยืนยันตัวตนที่มีความรัดกุมปลอดภัย (3) กำหนดบริการ แอปพลิเคชันและพอร์ตการเชื่อมต่อตามความจำเป็น (4) กำหนดให้มีการเก็บข้อมูลเหตุการณ์เพื่อให้ตรวจสอบย้อนหลัง ● ผู้ประกอบธุรกิจควรกำหนดขั้นตอนการตรวจสอบการตั้งค่าด้านความมั่นคงปลอดภัยตามที่กำหนด (security hardening) ก่อนการนำไปใช้งานจริง และทุกครั้งที่มีการเปลี่ยนแปลงระบบงานดังกล่าวอย่างมีนัยสำคัญ ● ผู้ประกอบธุรกิจควรสอบทานมาตรฐานการตั้งค่าด้านความมั่นคงปลอดภัย (security configuration standards) อย่างสม่ำเสมอ
	ในการกำหนดมาตรการป้องกันและตรวจสอบโปรแกรมไม่ประสงค์ดี และมาตรการในการแก้ไขระบบสารสนเทศเพื่อให้กลับมาใช้งานได้ตามปกติ (recovery) ผู้ประกอบธุรกิจควรมีมาตรการขั้นต่ำ ดังนี้ (1) กำหนดนโยบายห้ามใช้ซอฟต์แวร์ที่ไม่ได้รับอนุญาต	ผู้ประกอบธุรกิจควรกำหนดมาตรการรักษาความปลอดภัยของเครื่องแม่ข่าย และอุปกรณ์ที่ใช้ในการปฏิบัติงาน เพื่อป้องกันและตรวจจับโปรแกรมไม่ประสงค์ดี (malware) และภัยคุกคามไซเบอร์ โดยอย่างน้อยครอบคลุม ดังนี้ (1) มีกระบวนการ วิธีการ หรือเครื่องมือในการควบคุม และติดตามไม่ให้มีการติดตั้งซอฟต์แวร์ที่ไม่ได้รับอนุญาต

เอกสารเปรียบเทียบรายละเอียดของหลักเกณฑ์เดิม และหลักเกณฑ์ที่แก้ไข

หัวข้อ	รายละเอียดเดิม	รายละเอียดการแก้ไข
	(2) มีกระบวนการป้องกัน และตรวจสอบการใช้ซอฟต์แวร์ที่ไม่ได้รับอนุญาต และการใช้งานเว็บไซต์ ที่อาจมีโปรแกรมไม่ประสงค์ดี (3) ติดตั้งซอฟต์แวร์ตรวจสอบโปรแกรมไม่ประสงค์ดี และปรับปรุงให้เป็นปัจจุบันอย่างสม่ำเสมอ พร้อมทั้งกำหนดผู้มีหน้าที่รับผิดชอบให้รายงานและแก้ไขปัญหากรณีพบภัยคุกคาม (4) ตรวจสอบซอฟต์แวร์ระบบงานที่มีความสำคัญอย่างสม่ำเสมอ หากพบการติดตั้งหรือเปลี่ยนแปลงที่ไม่ได้รับอนุญาต ควรจัดให้มีการตรวจสอบ	(2) ติดตั้งเครื่องมือในการป้องกันและตรวจจับโปรแกรมไม่ประสงค์ดี เช่น anti-virus, anti-malware และ intrusion prevention system เป็นต้น โดยปรับปรุงเครื่องมือที่ใช้งานให้เป็นปัจจุบัน (update) และเท่าทันภัยคุกคามใหม่อย่างสม่ำเสมอ (3) ควบคุมการใช้สื่อบันทึกข้อมูลพกพา (removable media) เช่น กำหนดแนวทางการใช้งาน external hard disk เป็นต้น
	-เดิมไม่ได้กำหนด-	**การติดตามดูแลระบบและเฝ้าระวังภัยคุกคาม (security monitoring)** ● ผู้ประกอบธุรกิจควรมีกระบวนการหรือเครื่องมือในการตรวจจับและตอบสนองต่อเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศอย่างทันท่วงที เพื่อให้รับทราบความผิดปกติหรือภัยคุกคาม และสามารถดำเนินการป้องกันหรือรับมือได้อย่างเหมาะสม ดังนี้ (ก) ตรวจสอบ วิเคราะห์ และแก้ไข/ตอบสนองต่อเหตุการณ์ผิดปกติจากการแจ้งเตือนของระบบงานและเครื่องมือที่สำคัญที่บริษัทใช้งาน (ข) กำหนดรอบและดำเนินการสอบทาน ติดตาม และวิเคราะห์บันทึกเหตุการณ์อย่างสม่ำเสมอ เพื่อตรวจสอบการใช้งานระบบสารสนเทศที่ผิดปกติ พร้อมทั้งจัดทำเป็นรายงาน (ค) รายงานผลการตรวจสอบและตอบสนองต่อเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศให้ผู้บริหารที่เกี่ยวข้องทราบ

เอกสารเปรียบเทียบรายละเอียดของหลักเกณฑ์เดิม และหลักเกณฑ์ที่แก้ไข

หัวข้อ	รายละเอียดเดิม	รายละเอียดการแก้ไข
		• ผู้ประกอบธุรกิจควรกำหนดกระบวนการติดตาม cyber threat intelligence เพื่อให้สามารถติดตามและวิเคราะห์ภัยคุกคามทางไซเบอร์ที่เกิดขึ้นใหม่ และสามารถรับมือกับเหตุการณ์ทางไซเบอร์อย่างทันการณ์ • [ผู้ประกอบธุรกิจความเสี่ยงสูง] ผู้ประกอบธุรกิจควรมีหน่วยงานที่รับผิดชอบในการเฝ้าระวัง ติดตาม วิเคราะห์ ประสานงาน และเป็นศูนย์กลางในการจัดการเหตุภัยคุกคาม เช่น หน่วยงาน Security Operations Center (SOC) เป็นต้น • [ผู้ประกอบธุรกิจความเสี่ยงสูง] มีระบบหรือมาตรการวิเคราะห์พฤติกรรมผู้ใช้งาน เครือข่าย หรืออุปกรณ์สารสนเทศ (behavioral based security) เพื่อวิเคราะห์ระดับความเสี่ยงและสหสัมพันธ์ของข้อมูลบันทึกเหตุการณ์ (log correlation) และการยกเลิกการเชื่อมต่อกับอุปกรณ์ที่ผิดปกติโดยอัตโนมัติ • [ผู้ประกอบธุรกิจความเสี่ยงสูง] มีมาตรการในการควบคุมและป้องกันความเสี่ยงจากการบุกรุกโจมตีประเภท zero-day attack และแจ้งเตือนไปยังคณะทำงานในการรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Incident response team) เมื่อมีการตรวจพบเหตุการณ์
	มีการสำรองข้อมูลสำคัญทางธุรกิจ ระบบปฏิบัติการ โปรแกรมประยุกต์ ระบบงานคอมพิวเตอร์และชุดคำสั่งที่ใช้ทำงานไว้อย่างครบถ้วน และต้องมีการทดสอบข้อมูลสำรองและกระบวนการกู้คืนข้อมูล อย่างน้อยปีละ 1 ครั้ง	มีการสำรองข้อมูล (data backup) ที่สำคัญด้วยวิธีการ และความถี่ที่เหมาะสม เพื่อให้ข้อมูลสำรองมีสภาพพร้อมใช้งานสอดคล้องกับเป้าหมายการกู้คืนระบบเทคโนโลยีสารสนเทศในกรณีที่ระบบสารสนเทศและข้อมูลหลักเกิดเหตุขัดข้องหรือได้รับความเสียหาย โดยต้องมีการทดสอบข้อมูลสำรองและกระบวนการกู้คืนข้อมูลอย่างน้อยปีละ 1 ครั้ง
	• กำหนดเป้าหมายในการกู้คืนข้อมูล เช่น กำหนดประเภทของข้อมูล และชุดข้อมูลล่าสุดที่จะกู้คืนได้ (recovery point objective : RPO) • ผู้ประกอบธุรกิจควรจัดให้มีนโยบายสำรองข้อมูลสำคัญทางธุรกิจ รวมถึงระบบปฏิบัติการ (operating system) แอพพลิเคชั่นระบบงานคอมพิวเตอร์ (application	ผู้ประกอบธุรกิจควรกำหนดกลยุทธ์การสำรองข้อมูล และขั้นตอนวิธีปฏิบัติที่สอดคล้องกับแผนการกู้คืนข้อมูล และเป้าหมายระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหายได้ (recovery point objective: RPO) โดยอย่างน้อยควรมีรายละเอียดครอบคลุม (1) ข้อมูลที่ต้องสำรอง (2) ความถี่หรือรอบเวลาในการสำรองข้อมูล (3) ขั้นตอนและวิธีการสำรองข้อมูล

เอกสารเปรียบเทียบรายละเอียดของหลักเกณฑ์เดิม และหลักเกณฑ์ที่แก้ไข

<table>
<tr><th>หัวข้อ</th><th>รายละเอียดเดิม</th><th>รายละเอียดการแก้ไข</th></tr>
<tr><td></td><td>system) และชุดคำสั่งที่ใช้ทำงานให้ครบถ้วน ให้สามารถพร้อมใช้งานได้อย่างต่อเนื่อง โดยขั้นต่ำควรพิจารณา ดังนี้
■ กำหนดขั้นตอนหรือวิธีปฏิบัติในการสำรองข้อมูลเพื่อเป็นแนวทางให้แก่ผู้ปฏิบัติงาน โดยอย่างน้อย ควรมีรายละเอียดเกี่ยวกับ
(1) ข้อมูลที่ต้องสำรอง
(2) ความถี่ในการสำรอง
(3) ประเภทสื่อบันทึกข้อมูล
(4) จำนวนที่ต้องสำรอง
(5) ขั้นตอนและวิธีการสำรองโดยละเอียด
(6) สถานที่และวิธีการเก็บรักษาสื่อบันทึกข้อมูล
(7) กระบวนการกู้คืนข้อมูลในกรณีที่สูญหาย</td><td>(4) ขั้นตอนและวิธีการกู้คืนข้อมูล
(5) สถานที่และวิธีการเก็บรักษาสื่อบันทึกข้อมูล</td></tr>
<tr><td></td><td>-เดิมไม่ได้กำหนด-</td><td>กำหนดกระบวนการในการสอบทานการสำรองข้อมูลให้มีความถูกต้องและพร้อมใช้งาน โดยครอบคลุมถึงการบันทึกผลการตรวจสอบความครบถ้วนสมบูรณ์ในการสำรองข้อมูล หลักฐานการแก้ไขปัญหาและข้อผิดพลาดที่พบจากการสำรองข้อมูล และรายงานผลดังกล่าวไปยังผู้บริหารที่เกี่ยวข้องอย่างเป็นประจำ ตามที่กำหนดในแนวปฏิบัติของบริษัท</td></tr>
<tr><td></td><td>ตารางแสดงรายละเอียดการจัดเก็บหลักฐาน
<table><tr><th>ประเภทหลักฐานที่ต้องจัดเก็บ</th><th>รายละเอียดขั้นต่ำ</th><th>ระยะเวลาจัดเก็บขั้นต่ำ</th></tr><tr><td>หลักฐานการเข้าถึงพื้นที่หวงห้าม</td><td>บุคคลที่เข้าถึง / วันเวลาที่ผ่านเข้าออก / ความพยายามในการเข้าถึง (ถ้ามี)</td><td>ไม่น้อยกว่า 3 เดือน</td></tr><tr><td>หลักฐานการเข้าถึง</td><td>บัญชีผู้ใช้งาน / วันเวลาที่เข้าใช้งาน /</td><td>ไม่น้อยกว่า 3 เดือน</td></tr></table></td><td>ผู้ประกอบธุรกิจควรจัดเก็บข้อมูลบันทึกเหตุการณ์ของเครื่องแม่ข่าย ระบบงาน อุปกรณ์เครือข่ายที่สำคัญด้วยวิธีการที่ปลอดภัย โดยมีรายละเอียดครบถ้วนเพียงพอที่จะใช้เป็นหลักฐานในการตรวจสอบที่สามารถระบุตัวผู้กระทำได้ และจัดเก็บเป็นระยะเวลาอย่างน้อย 90 วัน หรือตามกฎหมายที่เกี่ยวข้องกำหนด ประกอบด้วยรายการหลักฐานอย่างน้อย ดังนี้
(1) บันทึกการเข้าถึง (access log / authentication log) ของพื้นที่สำคัญ (physical access) และระบบและข้อมูลสำคัญ (logical access) โดยรวมถึงความพยายามในการเข้าถึง
(2) บันทึกการดำเนินงาน (activity log) ที่สำคัญ โดยอย่างน้อยครอบคลุม</td></tr>
</table>

เอกสารเปรียบเทียบรายละเอียดของหลักเกณฑ์เดิม และหลักเกณฑ์ที่แก้ไข

<table>
<tr><th>หัวข้อ</th><th>รายละเอียดเดิม</th><th>รายละเอียดการแก้ไข</th></tr>
<tr><td></td><td>
<table>
<tr><td>ระบบปฏิบัติการฐานข้อมูล และระบบเครือข่ายคอมพิวเตอร์</td><td>ความพยายามในการเข้าใช้งาน</td><td></td></tr>
<tr><td>หลักฐานการเข้าถึงและใช้งานระบบสารสนเทศ</td><td>บัญชีผู้ใช้งาน / หมายเลขประจำเครื่องที่ใช้งาน (IP address) / วันเวลาที่มีการใช้งาน

กรณีที่เป็นระบบสารสนเทศเพื่อการซื้อขายหลักทรัพย์ (trading system) ให้เพิ่มรายละเอียดตามที่กำหนด

ทั้งนี้ ผู้ประกอบธุรกิจต้องสามารถระบุตัวตนผู้ใช้งาน และ local IP address ในช่วงเวลาที่ใช้งานได้ (เฉพาะการใช้งานผ่านอุปกรณ์ของบริษัท)</td><td>ไม่น้อยกว่า 1 ปี สำหรับผู้ประกอบธุรกิจนายหน้าซื้อขายหลักทรัพย์ การค้าหลักทรัพย์ หรือการจัดจำหน่ายหลักทรัพย์ซึ่งมิได้จำกัดเฉพาะหลักทรัพย์อันเป็นตราสารแห่งหนี้ หรือหน่วยลงทุน และตัวแทนซื้อขายสัญญาซื้อขายล่วงหน้า

ไม่น้อยกว่า 6 เดือน สำหรับผู้ประกอบธุรกิจประเภทอื่น</td></tr>
<tr><td>หลักฐานการใช้งานอินเทอร์เน็ตผ่านระบบเครือข่าย</td><td>บัญชีผู้ใช้งาน / หมายเลขประจำเครื่องที่ใช้งาน (IP</td><td></td></tr>
</table>
</td><td>(ก) การเปลี่ยนแปลงแก้ไขโครงสร้างข้อมูล และการเปลี่ยนแปลงแก้ไขข้อมูลในฐานข้อมูล
(ข) การเปลี่ยนแปลงการตั้งค่าของระบบ (configuration)
(ค) การเข้าถึง เปลี่ยนแปลง ลบ หรือถ่ายโอนข้อมูลสำคัญหรือข้อมูลส่วนบุคคล
(ง) การเปลี่ยนแปลงแก้ไขบัญชี และสิทธิของผู้ใช้งาน
(จ) การใช้งานอินเทอร์เน็ตผ่านระบบเครือข่ายภายในของผู้ประกอบธุรกิจ
(ฉ) การทำงานของ firewall (network firewall log)
(ช) หลักฐานการติดต่อสนทนาผ่านช่องทางอิเล็กทรอนิกส์ (electronic messaging) ของบุคคลที่สามารถเข้าถึงข้อมูลภายใน (access person)
(3) บันทึกการทำธุรกรรม (transaction log) ให้จัดเก็บเป็นระยะเวลาอย่างน้อย 1 ปี โดยในกรณีที่เป็นระบบสารสนเทศเพื่อการซื้อขายหลักทรัพย์ (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</td></tr>
</table>

เอกสารเปรียบเทียบรายละเอียดของหลักเกณฑ์เดิม และหลักเกณฑ์ที่แก้ไข

หัวข้อ	รายละเอียดเดิม			รายละเอียดการแก้ไข
	คอมพิวเตอร์ภายในของผู้ประกอบธุรกิจ (internet access log)	address) / หมายเลขอินเทอร์เน็ตของผู้ประกอบธุรกิจ (organization IP address) / วันเวลาที่มีการใช้งาน / ที่อยู่ของเว็บไซต์ปลายทาง (full URL) --- ทั้งนี้ ผู้ประกอบธุรกิจต้องสามารถระบุตัวตนผู้ใช้งาน และ IP address ในช่วงเวลาที่ใช้งานได้		
	หลักฐานการใช้งานแฟ้มข้อมูล (audit log)*	บัญชีผู้ใช้งาน / วันเวลาที่เข้าใช้งาน / บันทึกการเรียกดูและการแก้ไขข้อมูล	ไม่น้อยกว่า 6 เดือน	
	หลักฐานการบริหาร (event log) ระบบปฏิบัติการและ network firewall	วันและเวลาที่เกิดเหตุการณ์ / เหตุการณ์ที่เกิดขึ้นกับ OS (event services) เช่น สถานะการให้บริการของ service / เหตุการณ์ที่เกิดขึ้นกับ	ระยะเวลาตามที่จำเป็นและเพียงพอสำหรับการตรวจสอบซึ่งสอดคล้องกับความเสี่ยงที่ผู้ประกอบธุรกิจได้ประเมินไว้	

เอกสารเปรียบเทียบรายละเอียดของหลักเกณฑ์เดิม และหลักเกณฑ์ที่แก้ไข

<table>
<tr><th>หัวข้อ</th><th>รายละเอียดเดิม</th><th>รายละเอียดการแก้ไข</th></tr>
<tr><td></td><td>
<table>
<tr><td></td><td>network firewall เช่น การปรับปรุงหรือแก้ไข firewall rules</td><td></td></tr>
<tr><td>หลักฐานบันทึกข้อมูลจราจรคอมพิวเตอร์ของ network firewall</td><td>วันและเวลา / IP address ต้นทางและปลายทา / firewall action / port ที่ใช้ติดต่อ</td><td></td></tr>
<tr><td>หลักฐานการจัดการบริหารข้อมูล</td><td>บัญชีผู้ใช้งาน / วันเวลาที่เข้าใช้งาน</td><td></td></tr>
<tr><td>หลักฐานการติดต่อสนทนาผ่านช่องทางอิเล็กทรอนิกส์ (electronic messaging)**</td><td>บัญชีผู้ใช้งาน / วันเวลาที่เข้าใช้งาน / ข้อมูลการติดต่อตลอดระยะเวลาการสนทนา</td><td>ไม่น้อยกว่า 6 เดือน</td></tr>
</table>
* จัดเก็บเฉพาะบุคคลที่สามารถเข้าถึงข้อมูลภายใน (“access person”) ของผู้ประกอบธุรกิจทุกประเภท
** จัดเก็บเฉพาะบุคคลที่สามารถเข้าถึงข้อมูลภายใน (“access person”) ของผู้ประกอบธุรกิจนายหน้าซื้อขายหลักทรัพย์ การค้าหลักทรัพย์ หรือการจัดจำหน่ายหลักทรัพย์ ซึ่งมิได้จำกัดเฉพาะหลักทรัพย์อันเป็นตราสารแห่งหนี้หรือหน่วยลงทุน ตัวแทนซื้อขายสัญญาซื้อขายล่วงหน้า และ</td><td></td></tr>
</table>

เอกสารเปรียบเทียบรายละเอียดของหลักเกณฑ์เดิม และหลักเกณฑ์ที่แก้ไข

หัวข้อ	รายละเอียดเดิม	รายละเอียดการแก้ไข
	ผู้ประกอบธุรกิจจัดการกองทุนรวมหรือกองทุนส่วนบุคคลเท่านั้น *** นิยามว่าด้วย access person ให้เป็นไปตามประกาศแนวปฏิบัติว่าด้วยการกำหนดนโยบาย มาตรการ และระบบงานที่เกี่ยวกับการกระทำที่อาจมีความขัดแย้งทางผลประโยชน์กับลูกค้า	
	ผู้ประกอบธุรกิจที่เป็นสมาชิกของตลาดหลักทรัพย์ควรกำหนดระบบเวลาของอุปกรณ์และระบบสารสนเทศที่เกี่ยวกับการซื้อขายหลักทรัพย์และการชำระราคาให้ตรงกับเวลาอ้างอิงของระบบซื้อขายหลักทรัพย์ของตลาดหลักทรัพย์ ทั้งนี้ เพื่อให้การตรวจสอบธุรกรรมที่ไม่เหมาะสมทั้งหมดเป็นไปอย่างถูกต้องและมีประสิทธิภาพ	ผู้ประกอบธุรกิจควรมีการใช้ระบบในการควบคุมค่าเวลาของเครื่องแม่ข่าย ระบบงาน และอุปกรณ์เครือข่ายให้ตรงกับเครื่องแม่ข่าย Network Time Protocol: NTP (clock synchronization) เพื่อให้ค่าเวลาในการบันทึกเหตุการณ์มีความถูกต้องในลักษณะ real-time ซึ่งเครื่อง NTP ต้องรับสัญญาณให้ตรงกับเวลาอ้างอิงตามมาตรฐานสากล (Stratum 1) เช่น สถาบันมาตรวิทยาแห่งชาติ และกรมอุทกศาสตร์กองทัพเรือ เป็นต้น ทั้งนี้ ในกรณีผู้ประกอบธุรกิจที่เป็นสมาชิกของตลาดหลักทรัพย์ควรกำหนดระบบเวลาของอุปกรณ์และระบบสารสนเทศที่เกี่ยวกับการซื้อขายหลักทรัพย์และการชำระราคาให้ตรงกับเวลาอ้างอิงของระบบซื้อขายหลักทรัพย์ของตลาดหลักทรัพย์ ทั้งนี้ เพื่อให้การตรวจสอบธุรกรรมที่ไม่เหมาะสมทั้งหมดเป็นไปอย่างถูกต้องและมีประสิทธิภาพ
	- เดิมไม่ได้กำหนด-	ผู้ประกอบธุรกิจควรจัดเก็บข้อมูลบันทึกเหตุการณ์ที่เกี่ยวข้องกับข้อมูลส่วนบุคคล เพื่อใช้ระบุและตรวจสอบกิจกรรมของผู้ใช้งานและใช้เป็นหลักฐานหากเกิดเหตุการณ์การเข้าถึงใช้งาน แก้ไขเปลี่ยนแปลง หรือเปิดเผยข้อมูลส่วนบุคคล
	ผู้ประกอบธุรกิจควรจัดให้มีการป้องกันข้อมูลและระบบการบันทึกและจัดเก็บหลักฐานการใช้งานเกี่ยวกับระบบสารสนเทศของผู้ใช้งานทั่วไป รวมถึง system administrator logs และ system operator logs จากการถูกเปลี่ยนแปลงแก้ไข ทำความเสียหาย หรือเข้าถึงโดยไม่ได้รับอนุญาต และมีการตรวจสอบอย่างน้อยปีละ 1 ครั้งและเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ	ผู้ประกอบธุรกิจควรจัดเก็บข้อมูลบันทึกเหตุการณ์ของอุปกรณ์ที่สำคัญไว้ที่เครื่องแม่ข่ายที่ใช้จัดเก็บข้อมูลบันทึกเหตุการณ์ (logging server) ที่แยกเฉพาะ โดยมีการรักษาความปลอดภัยที่รัดกุมเพียงพอในการป้องกันการเปลี่ยนแปลง แก้ไข หรือทำลาย ซึ่งควรครอบคลุมอย่างน้อยดังนี้ (1) กำหนดหน้าที่และความรับผิดชอบผู้ที่สามารถเข้าถึงข้อมูลบันทึกเหตุการณ์ตามความจำเป็น

เอกสารเปรียบเทียบรายละเอียดของหลักเกณฑ์เดิม และหลักเกณฑ์ที่แก้ไข

หัวข้อ	รายละเอียดเดิม	รายละเอียดการแก้ไข
		(2) มีกระบวนการหรือเครื่องมือการพิสูจน์ตัวตนและยืนยันตัวตน รวมถึงสิทธิในการเข้าถึงของผู้ที่เข้าใช้งานระบบ และมีการสอบทานอย่างสม่ำเสมอ (3) ติดตั้งเครื่องแม่ข่ายให้อยู่ในโซนเครือข่ายที่มีความมั่นคงปลอดภัยอย่างเหมาะสม
	มีขั้นตอนควบคุมการติดตั้งซอฟท์แวร์บนระบบงาน และมีมาตรการจำกัดการติดตั้งซอฟท์แวร์โดยผู้ใช้งาน เพื่อให้ระบบปฏิบัติงานต่าง ๆ มีความถูกต้องครบถ้วนและน่าเชื่อถือ	ย้ายไปหัวข้อ การบริหารจัดการโครงการด้านเทคโนโลยีสารสนเทศ และมาตรการการจัดหา พัฒนา และบำรุงรักษาระบบสารสนเทศ
	ผู้ประกอบธุรกิจควรแบ่งแยกส่วนคอมพิวเตอร์ที่มีไว้สำหรับการพัฒนาระบบงาน (develop environment) และใช้งานจริง (production environment) ออกจากกัน และควบคุมให้มีการเข้าถึงเฉพาะผู้ที่เกี่ยวข้องในแต่ละส่วนเท่านั้น ทั้งนี้ การแบ่งแยกส่วนดังกล่าวอาจแบ่งโดยใช้เครื่องคอมพิวเตอร์คนละเครื่อง หรือแบ่งโดยการจัดเนื้อที่แยกไว้ต่างหากภายในเครื่องคอมพิวเตอร์เดียวกันก็ได้	ย้ายไปหัวข้อ การบริหารจัดการโครงการด้านเทคโนโลยีสารสนเทศ และมาตรการการจัดหา พัฒนา และบำรุงรักษาระบบสารสนเทศ
	การประเมินช่องโหว่ของระบบ (vulnerability assessment) กับระบบงานที่มีความสำคัญทุกระบบอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงระบบงานดังกล่าวอย่างมีนัยสำคัญ และรายงานผลไปยังหน่วยงานกำกับการปฏิบัติงาน หรือหน่วยงานตรวจสอบภายในโดยไม่ชักช้า	การประเมินช่องโหว่ทางเทคนิค (technical vulnerability assessment) ควรครอบคลุมการดำเนินการอย่างน้อย ดังนี้ (1) กำหนดขอบเขตของการประเมินช่องโหว่ทางเทคนิคให้ครอบคลุมทุกระบบงานตามระดับความเสี่ยง สำหรับระบบสารสนเทศที่มีความสำคัญ และระบบสารสนเทศที่เชื่อมต่อกับเครือข่ายสาธารณะทุกระบบต้องได้รับการประเมินช่องโหว่อย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ (2) วิเคราะห์และจัดระดับความรุนแรงของช่องโหว่ (severity) เพื่อประเมินความเสี่ยงและกำหนดระยะเวลาในการแก้ไข (3) รายงานผลการประเมินช่องโหว่ไปยังผู้รับผิดชอบ รวมถึงการติดตามให้มีการแก้ไขช่องโหว่ที่ตรวจพบภายในระยะเวลาที่เหมาะสมกับระดับความเสี่ยง โดยนำเสนอความคืบหน้าของการดำเนินการต่อคณะกรรมการหรือผู้บริหารที่ได้รับมอบหมาย

เอกสารเปรียบเทียบรายละเอียดของหลักเกณฑ์เดิม และหลักเกณฑ์ที่แก้ไข

หัวข้อ	รายละเอียดเดิม	รายละเอียดการแก้ไข
	มีการทดสอบเจาะระบบ (penetration test) กับระบบงานที่มีความสำคัญที่เชื่อมต่อกับระบบเครือข่ายภายนอก (untrusted network) โดยบุคคลที่เป็นอิสระจากหน่วยงานที่รับผิดชอบด้านเทคโนโลยีสารสนเทศ และเป็นไปตามการวิเคราะห์ความเสี่ยงและผลกระทบทางธุรกิจ (risk and business impact analysis) ดังนี้ (1) กรณีที่เป็นระบบงานสำคัญที่ประเมินแล้วมีความสำคัญสูง ต้องทดสอบอย่างน้อยทุก 3 ปี และเมื่อมีการเปลี่ยนแปลงระบบงานดังกล่าวอย่างมีนัยสำคัญ (2) กรณีที่เป็นระบบงานที่มีความสำคัญอื่น ๆ ต้องทดสอบอย่างน้อยทุก 6 ปี	● การทดสอบเจาะระบบ (penetration test) ควรครอบคลุมการดำเนินการอย่างน้อยดังนี้ (1) **[ปรับปรุงจาก Focus Group]** กำหนดขอบเขตของการทดสอบเจาะระบบให้ครอบคลุมระบบงานสารสนเทศและระบบเครือข่ายที่มีช่องทางเชื่อมต่อกับเครือข่ายสาธารณะ (internet facing) อย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงระบบงานดังกล่าวอย่างมีนัยสำคัญ โดยระบบงานอื่น ๆ ควรจัดให้มีการประเมินความเสี่ยงจากการบุกรุกผ่านระบบเครือข่ายคอมพิวเตอร์ที่ใช้สื่อสารภายในองค์กร เพื่อกำหนดขอบเขตและทดสอบเจาะระบบตามความเหมาะสม (2) ขอบเขตของการทดสอบเจาะระบบควรครอบคลุมการทดสอบเจาะระบบครอบคลุมตามความเสี่ยงที่เกี่ยวข้อง เช่น เครื่องโฮสต์ เครือข่าย และแอปพลิเคชันของระบบสารสนเทศที่มีความเสี่ยงสูง และครอบคลุมภัยคุกคามที่สำคัญ (3) การวิเคราะห์และจัดระดับความรุนแรงของช่องโหว่ (severity) เพื่อประเมินความเสี่ยงและกำหนดระยะเวลาในการแก้ไข (4) รายงานผลการทดสอบเจาะระบบไปยังผู้รับผิดชอบ รวมถึงการติดตามให้มีการแก้ไขช่องโหว่ที่ตรวจพบภายในระยะเวลาที่เหมาะสมกับระดับความเสี่ยง โดยนำเสนอความคืบหน้าของการดำเนินการต่อคณะกรรมการหรือผู้บริหารที่ได้รับมอบหมาย (5) รวบรวมและวิเคราะห์ช่องโหว่ทางเทคนิคที่ตรวจพบ เพื่อกำหนดเป็นมาตรการรักษาความมั่นคงปลอดภัยของระบบงานที่จะมีการพัฒนาในอนาคต (6) จัดเก็บรายงานผลการทดสอบเจาะระบบเป็นระยะเวลาไม่น้อยกว่า 3 ปี นับแต่วันที่จัดทำเอกสารนั้น โดยต้องนำส่งสำเนารายงานผลการเจาะระบบโดยไม่ชักช้าเมื่อได้รับการร้องจากสำนักงาน ยกเว้นกรณีธุรกิจที่มีการกำหนดไว้เป็นการเฉพาะ

เอกสารเปรียบเทียบรายละเอียดของหลักเกณฑ์เดิม และหลักเกณฑ์ที่แก้ไข

หัวข้อ	รายละเอียดเดิม	รายละเอียดการแก้ไข
		• ผู้ทดสอบเจาะระบบ (penetration tester) ที่ทำการทดสอบเจาะระบบสารสนเทศที่ควรมีความเป็นอิสระจากหน่วยงานเจ้าของระบบ • [ผู้ประกอบธุรกิจความเสี่ยงสูง] ผู้ทดสอบเจาะระบบ (penetration tester) ที่ทำการทดสอบเจาะระบบสารสนเทศที่มีความสำคัญ ควรได้รับการรับรองและมีประกาศนียบัตร (accreditations and certifications) ที่เป็นที่ยอมรับในอุตสาหกรรม เช่น OSCP, OSWP, OSCE, OSEE และ OSWE เป็นต้น
	การตรวจสอบระบบสารสนเทศ (information system audit) ผู้ประกอบธุรกิจต้องมีมาตรการรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ (operations security) มีการตรวจสอบระบบสารสนเทศดังนี้ (ก) วางแผนการตรวจสอบระบบสารสนเทศให้สอดคล้องกับความเสี่ยงที่ได้ประเมินไว้ (ข) กำหนดขอบเขตในการตรวจสอบระบบสารสนเทศทางเทคนิคให้ครอบคลุมถึงจุดเสี่ยงที่สำคัญ โดยการตรวจสอบดังกล่าวต้องไม่กระทบต่อการปฏิบัติงาน (ค) ตรวจสอบระบบสารสนเทศนอกเวลาทำงาน ในกรณีที่การตรวจสอบนั้นอาจส่งผลกระทบต่อความพร้อมในการใช้งานระบบดังกล่าว	ย้ายไปหัวข้อ การตรวจสอบด้านเทคโนโลยีสารสนเทศ
	ผู้ประกอบธุรกิจควรจัดให้มีการควบคุมการปฏิบัติงานอย่างเคร่งครัด โดยเฉพาะในกรณีที่มีการเปลี่ยนแปลงโครงสร้างระบบงาน ขั้นตอนการปฏิบัติงาน หรือการทำงานของระบบงานต่าง ๆ ซึ่งอาจกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ ตัวอย่างของการควบคุมดังกล่าว เช่น	ผู้ประกอบธุรกิจควรจัดให้มีการบริหารจัดการการเปลี่ยนแปลงโครงสร้าง ระบบงาน ขั้นตอนการปฏิบัติงาน และการตั้งค่าความปลอดภัยหรือการทำงานของระบบงานต่าง ๆ ที่อาจกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (change management) • กำหนดขั้นตอนในการบริหารจัดการการเปลี่ยนแปลงอย่างเป็นลายลักษณ์อักษร โดยมีหลักเกณฑ์และขั้นตอนการเปลี่ยนแปลงที่เหมาะสมกับระดับความสำคัญหรือความจำเป็นเร่งด่วน เช่น การเปลี่ยนแปลงมาตรฐานที่ได้รับอนุมัติเป็นการทั่วไป

เอกสารเปรียบเทียบรายละเอียดของหลักเกณฑ์เดิม และหลักเกณฑ์ที่แก้ไข

หัวข้อ	รายละเอียดเดิม	รายละเอียดการแก้ไข
	• กำหนดขั้นตอนหรือวิธีปฏิบัติที่เป็นลายลักษณ์อักษรในกรณีการเปลี่ยนแปลงที่มีนัยสำคัญ • มีแผนรองรับ และดำเนินการทดสอบภายหลังการเปลี่ยนแปลง • มีการประเมินผลกระทบที่อาจเกิดขึ้นจากการเปลี่ยนแปลง • มีขั้นตอนการขออนุมัติจากผู้มีอำนาจ • มีขั้นตอนการตรวจสอบเพื่อให้มั่นใจว่ากระบวนการเปลี่ยนแปลงดังกล่าวเป็นไปตามนโยบายด้านความมั่นคงปลอดภัยของระบบสารสนเทศ	(standard change) การเปลี่ยนแปลงที่ต้องขออนุมัติตามกระบวนการปกติ (normal change) และการเปลี่ยนแปลงที่ต้องดำเนินการอย่างเร่งด่วน (emergency change) • แบ่งแยกหน้าที่ (segregation of duties) ผู้ที่เกี่ยวข้องในกระบวนการบริหารจัดการการเปลี่ยนแปลง เพื่อไม่ให้บุคคลใดบุคคลหนึ่งสามารถปฏิบัติงานได้ตั้งแต่เริ่มต้นจนจบกระบวนการการเปลี่ยนแปลง • มีระบบหรือทะเบียนในการจัดเก็บคำขอเปลี่ยนแปลงและเอกสารรายละเอียดที่เกี่ยวข้องเพื่อใช้ควบคุมการปฏิบัติงานตั้งแต่ต้นจนจบกระบวนการ และสามารถใช้ในการติดตามและสอบทานการปฏิบัติงานได้
	-เดิมไม่ได้กำหนด-	กรณีการเปลี่ยนแปลงที่ต้องดำเนินการอย่างเร่งด่วน (emergency change) ควรมีกระบวนการในการพิจารณาความเสี่ยงและผลกระทบรวมถึงขออนุมัติจากผู้บริหารที่ได้รับมอบหมายให้สามารถตัดสินใจได้กรณีเร่งด่วน โดยภายหลังดำเนินการให้มีการรายงานผู้บริหารที่เกี่ยวข้องได้รับทราบโดยเร็ว
	-เดิมไม่ได้กำหนด-	[ผู้ประกอบธุรกิจความเสี่ยงสูง] ผู้ประกอบธุรกิจควรกำหนดบทบาทหน้าที่และความรับผิดชอบของผู้บริหารที่ได้รับมอบหมายหรือคณะกรรมการบริหารจัดการการเปลี่ยนแปลง (change advisory board: CAB) ซึ่งควรประกอบด้วยผู้บริหารจากหน่วยงานเทคโนโลยีสารสนเทศ และหน่วยงานผู้ใช้งานเทคโนโลยีสารสนเทศที่เกี่ยวข้อง เพื่อทำหน้าที่ประเมินผลกระทบและพิจารณาเหตุผลความจำเป็นก่อนอนุมัติให้ดำเนินการเปลี่ยนแปลงระบบ เพื่อป้องกันการแก้ไขเปลี่ยนแปลงโดยไม่ได้รับอนุญาตและไม่ให้เกิดผลกระทบที่อาจเกิดกับระบบที่เกี่ยวข้อง รวมถึงการพิจารณาและอนุมัติกรณีการเปลี่ยนแปลงที่ต้องดำเนินการอย่างเร่งด่วน (emergency change)
	-เดิมไม่ได้กำหนด-	**การรักษาความปลอดภัยของเครื่องแม่ข่าย (server) และอุปกรณ์ที่ใช้ปฏิบัติงาน (endpoint)** เพิ่มเติมหลักการ ดังนี้

เอกสารเปรียบเทียบรายละเอียดของหลักเกณฑ์เดิม และหลักเกณฑ์ที่แก้ไข

หัวข้อ	รายละเอียดเดิม	รายละเอียดการแก้ไข
		• ผู้ประกอบธุรกิจควรกำหนดมาตรฐานและระเบียบปฏิบัติในการบริหารจัดการระบบเสมือนจริง (Virtualization) โดยครอบคลุมการควบคุมสิทธิการเข้าถึงและการรักษาความปลอดภัยของระบบ ตลอดจนการควบคุมข้อมูลที่เกิดจากระบบเสมือนจริง เช่น ข้อมูลระบบปฏิบัติการ (VM image) และข้อมูลสำรองระบบ (VM snapshot) เพื่อป้องกันการเข้าถึงและเปลี่ยนแปลงระบบโดยผู้ไม่มีสิทธิหรือไม่รับอนุญาต • [ผู้ประกอบธุรกิจความเสี่ยงสูง] ผู้ประกอบธุรกิจควรติดตั้งระบบตรวจสอบภัยคุกคามขั้นสูง (endpoint detection & response) บนเครื่องแม่ข่าย และอุปกรณ์ที่ใช้ปฏิบัติงานสำหรับตรวจจับ เก็บหลักฐาน และตอบสนองต่อภัยคุกคามไซเบอร์ได้อย่างทันการณ์ • [ผู้ประกอบธุรกิจความเสี่ยงสูง] ผู้ประกอบธุรกิจควรกำหนดมาตรการทางเทคนิคหรือเครื่องมือป้องกันข้อมูลสำคัญรั่วไหล (data leak prevention) จากการส่งข้อมูลออกโดยไม่ได้รับอนุญาตผ่านช่องทางต่าง ๆ เช่น อุปกรณ์พกพาและสื่อบันทึกข้อมูล จดหมายอิเล็กทรอนิกส์ และโปรแกรมการประชุมและสื่อสารผ่านสื่ออิเล็กทรอนิกส์ (online communication tool) เป็นต้น • [ผู้ประกอบธุรกิจความเสี่ยงสูง] กรณีที่มีฟังก์ชันเปิดการใช้งานพอร์ตการเชื่อมต่อให้ปิดพอร์ตการเชื่อมต่อภายนอกทั้งหมด (เช่น พอร์ต USB) ที่รองรับการเชื่อมต่อกับสื่อบันทึกข้อมูลพกพา (removable media) และอุปกรณ์คอมพิวเตอร์แบบพกพา โดยให้เปิดใช้งานเมื่อจำเป็นและได้รับอนุมัติโดยผู้มีอำนาจเท่านั้น
	ผู้ประกอบธุรกิจควรติดตามประสิทธิภาพการทำงานของระบบสารสนเทศและทรัพย์สินสารสนเทศประเภทอุปกรณ์ที่สำคัญให้ทำงานได้อย่างต่อเนื่องและมีประสิทธิภาพ เพื่อใช้เป็นข้อมูลในการประเมินสมรรถภาพและความเพียงพอ (capacity) ของระบบสารสนเทศ ทรัพย์สินสารสนเทศประเภทอุปกรณ์ และ	**การบริหารจัดการขีดความสามารถของระบบสารสนเทศ (capacity management)** เพิ่มเติมหลักการ ดังนี้ • ผู้ประกอบธุรกิจควรกำหนดมาตรฐานและระเบียบวิธีปฏิบัติในการติดตาม ประเมินความเพียงพอของทรัพยากรด้านเทคโนโลยีสารสนเทศ (performance, capacity และ utilization) ของโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศที่ครอบคลุมถึง

เอกสารเปรียบเทียบรายละเอียดของหลักเกณฑ์เดิม และหลักเกณฑ์ที่แก้ไข

หัวข้อ	รายละเอียดเดิม	รายละเอียดการแก้ไข
	บุคลากร รวมถึงเพื่อให้สามารถรองรับแผนการปฏิบัติงานในอนาคตได้อย่างมีประสิทธิภาพด้วย	ระบบคอมพิวเตอร์ ระบบฐานข้อมูล ระบบเครือข่ายคอมพิวเตอร์ และระบบสาธารณูปโภคที่เกี่ยวข้องกับงานเทคโนโลยีสารสนเทศ ● ผู้ประกอบธุรกิจควรประเมินแนวโน้มการใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศสอดคล้องกับการประมาณการ (Forecasting) ปริมาณธุรกรรมและปริมาณลูกค้าในภาวะปกติและภาวะวิกฤตที่อาจจะเกิดขึ้น ทั้งในปัจจุบันและอนาคต เพื่อวางแผนรองรับการใช้งานในอนาคต (capacity planning) โดยครอบคลุมทั้งระบบหลักและระบบสำรอง ● ผู้ประกอบธุรกิจควรมีเครื่องมือติดตามตัวชี้วัดการใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศ และแจ้งเตือนผู้เกี่ยวข้อง (threshold and trigger) เพื่อให้สามารถวางแผนรับมือ และจัดสรรทรัพยากรเพิ่มเติมได้อย่างทันการณ์ ● ผู้ประกอบธุรกิจควรรายงานความเพียงพอของทรัพยากรด้านเทคโนโลยีสารสนเทศต่อคณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมายทราบอย่างสม่ำเสมอ เพื่อให้มีการกำกับดูแลความพร้อมใช้และความเพียงพอของระบบในการรองรับการให้บริการทางธุรกิจได้อย่างต่อเนื่อง และสามารถลดความเสี่ยงได้อย่างทันการณ์
	-เดิมไม่ได้กำหนด-	ในกรณีที่มีการปฏิบัติงานจากเครือข่ายภายนอกบริษัท (teleworking) ผู้ประกอบธุรกิจควรกำหนดมาตรการรักษาความมั่นคงปลอดภัยที่รัดกุมเพียงพอสำหรับข้อมูล และระบบสารสนเทศที่มีความสำคัญ โดยพิจารณาถึงแนวทางดังต่อไปนี้ (1) การกำหนดมาตรการรักษาความมั่นคงปลอดภัยด้านกายภาพที่เหมาะสมรัดกุมเพียงพอกับขอบเขตการปฏิบัติงาน สำหรับพื้นที่ปฏิบัติงานนอกองค์กร (2) การลงทะเบียน และขออนุมัติการปฏิบัติงานจากเครือข่ายภายนอกบริษัทจากผู้มีอำนาจหรือผู้บริหารที่เกี่ยวข้อง (3) การยืนยันตัวตนพนักงานที่ได้รับอนุญาตให้ปฏิบัติงานจากภายนอกบริษัทด้วยวิธีการที่รัดกุมปลอดภัย เช่น การใช้วิธียืนยันตัวตนแบบหลายปัจจัย (multi-factor authentication) และการเข้าใช้งานผ่านอุปกรณ์ที่อนุญาตเท่านั้น เป็นต้น

เอกสารเปรียบเทียบรายละเอียดของหลักเกณฑ์เดิม และหลักเกณฑ์ที่แก้ไข

หัวข้อ	รายละเอียดเดิม	รายละเอียดการแก้ไข
		(4) กรณีที่มีการเชื่อมต่อหรือรับส่งข้อมูลที่เป็นความลับหรือมีความสำคัญจากระยะไกล (remote access) ควรจัดให้มีการรักษาความมั่นคงปลอดภัยของระบบเครือข่ายและระบบงานภายในองค์กรที่มีความสำคัญเพื่อป้องกันหรือตรวจจับการเข้าถึงโดยไม่ได้รับอนุญาต ดังนี้ (ก) การติดตั้ง firewall (ข) การปรับปรุงซอฟต์แวร์ตรวจสอบโปรแกรมไม่ประสงค์ดี (anti-virus / anti-malware) บนอุปกรณ์ที่ใช้ในการปฏิบัติงานให้ทันสมัยอยู่เสมอ (ค) การเชื่อมต่อหรือรับส่งข้อมูลควรใช้งานผ่านช่องทางที่มีการเข้ารหัสและมีความปลอดภัย เช่น SSH, VPN หรือ SSL/TLS เป็นต้น (ง) เปิดใช้งานการเชื่อมต่อระยะไกล เมื่อจำเป็นเท่านั้น (5) การป้องกันโปรแกรมไม่ประสงค์ดี
	-เดิมไม่ได้กำหนด-	ในการปฏิบัติงานที่มีการใช้อุปกรณ์เคลื่อนที่ (mobile devices) เพื่อเข้าถึงข้อมูลและระบบสารสนเทศขององค์กร (ไม่รวมถึงระบบ mail service) ผู้ประกอบธุรกิจควรจัดให้มีนโยบายและมาตรการป้องกันข้อมูล และระบบสารสนเทศที่มีความสำคัญ โดยพิจารณาถึงแนวทางดังต่อไปนี้ (1) มีการลงทะเบียนอุปกรณ์เคลื่อนที่ทั้งของพนักงานและบุคคลภายนอกก่อนการใช้งาน และมีการอนุมัติโดยผู้บริหารที่เกี่ยวข้อง ที่รวมถึงจัดให้มีการทบทวนทะเบียนดังกล่าวอย่างน้อยปีละ 1 ครั้งหรือเมื่อมีการเปลี่ยนอุปกรณ์ พร้อมทั้งยกเลิกสิทธิการใช้งานของอุปกรณ์เดิม เพื่อให้มั่นใจได้ว่าการใช้งานอุปกรณ์ดังกล่าวมีความมั่นคงปลอดภัยเพียงพอ ทั้งนี้ ผู้ประกอบธุรกิจอาจใช้ระบบเทคโนโลยีการลงทะเบียนอื่นทดแทนได้ หากพิจารณาแล้วเห็นว่าเหมาะสม (2) มีมาตรการป้องการข้อมูลที่เป็นความลับหรือมีความสำคัญ (sensitive data) กรณีที่อุปกรณ์เคลื่อนที่สูญหาย เช่น กำหนดให้ใส่รหัสผ่านก่อนใช้งานอุปกรณ์ (lock screen) หรือการลบข้อมูลจากระยะไกล (remote wipe-out) เป็นต้น

เอกสารเปรียบเทียบรายละเอียดของหลักเกณฑ์เดิม และหลักเกณฑ์ที่แก้ไข

หัวข้อ	รายละเอียดเดิม	รายละเอียดการแก้ไข
		(3) จัดให้มีการเข้ารหัสข้อมูลสำคัญทั้งที่จัดเก็บในอุปกรณ์เคลื่อนที่ และข้อมูลที่รับส่งผ่านระบบเครือข่ายคอมพิวเตอร์
	-เดิมไม่ได้กำหนด-	● กรณีที่อนุญาตให้พนักงานสามารถใช้อุปกรณ์ส่วนตัวของพนักงานเพื่อเข้าถึงข้อมูลและระบบสารสนเทศ (ไม่รวมถึงระบบ mail service) ผู้ประกอบธุรกิจควรพิจารณาความเสี่ยงที่เกี่ยวข้อง และจัดให้มีระเบียบปฏิบัติหรือเครื่องมือเพื่อควบคุมความเสี่ยงอย่างเหมาะสม โดยพิจารณาถึงแนวทางดังต่อไปนี้ (1) การใช้งานระบบ mobile device management (MDM) สำหรับลงทะเบียนอุปกรณ์ (2) การควบคุมให้มีการใช้ BYOD ในการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ ข้อมูลและระบบสารสนเทศเท่าที่จำเป็น (3) การตรวจสอบและวิเคราะห์ความเสี่ยงของอุปกรณ์ที่นำมาใช้งาน (4) การกำหนดรหัสผ่านเพื่อใช้ในการล็อคหรือปลดล็อคในการเข้าถึงอุปกรณ์ส่วนตัว (5) การติดตั้งซอฟต์แวร์ตรวจสอบโปรแกรมไม่ประสงค์ดี (anti-virus/anti-malware) และปรับปรุงให้ทันสมัยอยู่เสมอ (6) ไม่อนุญาตให้ใช้โทรศัพท์เคลื่อนที่ที่ถูกปรับแต่ง (rooted หรือ jailbroken) ● [ผู้ประกอบธุรกิจความเสี่ยงสูง] ผู้ประกอบธุรกิจควรมีการจัดหาเครื่องมือในการบริหารจัดการอุปกรณ์เคลื่อนที่ที่มีความสามารถในการบริหารจัดการชุดโปรแกรมแก้ไขข้อบกพร่องด้านความมั่นคงปลอดภัยสารสนเทศ (security patch) การบริหารและติดตั้งค่า configuration ของอุปกรณ์ การบริหารจัดการช่องโหว่ด้านความปลอดภัย รวมถึงการบริหารจัดการด้านการป้องกันไวรัสและโปรแกรมไม่พึงประสงค์
	มีกระบวนการจัดการช่องโหว่ด้านเทคนิคที่สอดคล้องกับกระบวนการจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (incident management) เพื่อเตรียมความพร้อมรองรับกรณีที่ระบบถูก	มีการบริหารจัดการโปรแกรมแก้ไขช่องโหว่ (patch management) อย่างน้อยครอบคลุมช่องโหว่ด้านความปลอดภัยสารสนเทศ โดยจัดให้มีกระบวนการควบคุมและปรับปรุงแก้ไขช่องโหว่อย่างสม่ำเสมอ

เอกสารเปรียบเทียบรายละเอียดของหลักเกณฑ์เดิม และหลักเกณฑ์ที่แก้ไข

หัวข้อ	รายละเอียดเดิม	รายละเอียดการแก้ไข
	บุกรุกผ่านช่องโหว่ ทั้งนี้ ให้รวมถึงกรณีที่ตรวจพบช่องโหว่แต่ยังไม่สามารถหาวิธีปิดช่องโหว่ได้	
	จัดให้มีการปิดช่องโหว่ที่พบโดยไม่ชักช้า โดยควรมีการประเมินความเสี่ยงของโปรแกรมเพื่อปิดช่องโหว่ (patches) ก่อนการติดตั้งโปรแกรมเพื่อทดสอบและประเมินผลกระทบที่อาจเกิดจากการติดตั้งโปรแกรมดังกล่าว ทั้งนี้ กรณีที่ไม่มีโปรแกรมเพื่อปิดช่องโหว่ ให้ปฏิบัติตามคำแนะนำของบริษัทผู้ผลิตทรัพย์สินสารสนเทศที่เกี่ยวข้อง	กำหนดผู้มีหน้าที่รับผิดชอบในการจัดการช่องโหว่ทางเทคนิค โดยครอบคลุมถึงการติดตามข้อมูลข่าวสารเกี่ยวกับช่องโหว่ การตรวจสอบหาช่องโหว่ การประเมินความเสี่ยงของช่องโหว่ที่ตรวจพบ และการปิดช่องโหว่ (patching) ตามลำดับความเสี่ยง ทั้งนี้ กรณีที่ไม่มีโปรแกรมแก้ไขช่องโหว่ ให้ปฏิบัติตามคำแนะนำของบริษัทผู้ผลิตทรัพย์สินด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้อง หรือจัดให้มีมาตรการควบคุมอื่นเพื่อจัดการความเสี่ยงอย่างเหมาะสมและทันการณ์
	-เดิมไม่ได้กำหนด-	• มีการกำหนดมาตรฐานและระเบียบวิธีปฏิบัติใน patch ที่ครอบคลุมอย่างน้อย ดังนี้ (1) กลยุทธ์การบริหารจัดการโปรแกรมปิดช่องโหว่ตามระดับความสำคัญ (2) หลักเกณฑ์การแก้ไขและกรอบระยะเวลา การแก้ไขช่องโหว่โดยพิจารณา ระดับความสำคัญ และความเสี่ยงจากการถูกโจมตีจากช่องโหว่ (3) กระบวนการทดสอบโปรแกรมปิดช่องโหว่ก่อนการดำเนินการติดตั้ง และลำดับการติดตั้ง (patch sequence) • ติดตามข้อมูลข่าวสารเกี่ยวกับช่องโหว่ทางเทคนิคที่อาจเป็นความเสี่ยงต่อระบบสารสนเทศของผู้ประกอบธุรกิจอย่างทันต่อเหตุการณ์ รวมทั้งจัดให้มีการตรวจหาช่องโหว่ดังกล่าว • ผู้ประกอบธุรกิจควรมีกระบวนการทดสอบ patch ที่ออกใหม่ทุกครั้งก่อนนำไปติดตั้งบนระบบที่ให้บริการจริงเพื่อป้องกันผลกระทบที่ไม่พึงประสงค์จากการติดตั้งโปรแกรมดังกล่าว ทั้งนี้ กรณีที่ไม่มีโปรแกรมเพื่อปิดช่องโหว่ ให้ปฏิบัติตามคำแนะนำของบริษัทผู้ผลิตทรัพย์สินด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้อง หรือจัดให้มีมาตรการควบคุมอื่นเพื่อจัดการความเสี่ยงอย่างเหมาะสม • ก่อนการติดตั้ง patch บนระบบงานจริง ผู้ประกอบธุรกิจควรดำเนินการตามกระบวนการบริหารจัดการการเปลี่ยนแปลง (change management) ที่กำหนดไว้เพื่อป้องกันความเสี่ยงและข้อผิดพลาดจากการปฏิบัติงาน

เอกสารเปรียบเทียบรายละเอียดของหลักเกณฑ์เดิม และหลักเกณฑ์ที่แก้ไข

หัวข้อ	รายละเอียดเดิม	รายละเอียดการแก้ไข
		• [ผู้ประกอบธุรกิจความเสี่ยงสูง] มีการติดตั้งเครื่องมือที่ใช้ติดตาม Patch ด้านการรักษาความปลอดภัย (patch monitoring software) ที่ยังไม่มีการติดตั้งของระบบปฏิบัติการ (operation system) ระบบงาน (application system) และระบบฐานข้อมูล (database system) ที่สำคัญ
การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายคอมพิวเตอร์ (communications security)	จัดทำข้อตกลงการใช้บริการผ่านระบบเครือข่ายคอมพิวเตอร์ที่เกี่ยวกับวิธีการบริหารจัดการคุณภาพการให้บริการ และกระบวนการรักษาความมั่นคงปลอดภัยของระบบเครือข่ายคอมพิวเตอร์กับผู้รับดำเนินการ	• บริหารระบบเครือข่ายคอมพิวเตอร์ให้สามารถมีความพร้อมใช้งาน และสอดคล้องกับระดับการให้บริการด้านเทคโนโลยีสารสนเทศ (Service Level Agreement: SLA) ที่กำหนดไว้
	แบ่งแยกระบบเครือข่ายคอมพิวเตอร์ตามความเหมาะสม โดยระบุขอบเขตของระบบเครือข่ายย่อยอย่างชัดเจน และมีกระบวนการควบคุมการเข้าถึงขอบเขตดังกล่าวอย่างเหมาะสม	• มีการจัดโครงสร้างของระบบเครือข่ายและแบ่งเครือข่ายอย่างเหมาะสม โดยคำนึงถึงระดับความสำคัญของระบบสารสนเทศ ระดับความสำคัญของข้อมูล และระดับความเสี่ยง และจัดให้มีการควบคุมการเชื่อมต่อจากระบบงานต่าง ๆ มายังระบบสารสนเทศที่มีความสำคัญอย่างเข้มงวด • กรณีที่มีการแบ่งแยกเครือข่ายเป็นหลายชั้น ควรกำหนดมาตรการการควบคุมทางเทคนิคที่แตกต่างกันในแต่ละจุด เช่น ใช้ access control list (ACL) หรือใช้อุปกรณ์รักษาความปลอดภัยในทุกจุดที่มีการเชื่อมต่อเพื่อเพิ่มประสิทธิภาพในการคัดกรอง traffic และลดความเสี่ยงที่แต่ละจุดการเชื่อมต่ออาจมีช่องโหว่เดียวกัน
	แบ่งแยกหน้าที่ความรับผิดชอบระหว่าง network administrator และ computer administrator ออกจากกัน พร้อมทั้งกำหนดหน้าที่ความรับผิดชอบและขั้นตอนในการบริหารจัดการระบบ และอุปกรณ์เครือข่ายให้ชัดเจน	ยกเลิกข้อกำหนด
	จำกัดการเชื่อมต่อระบบคอมพิวเตอร์ระหว่างเครือข่าย เช่น จำกัดการใช้งานจุดเชื่อมต่อระบบเครือข่าย (port outlet)	จำกัดการเชื่อมต่อระบบคอมพิวเตอร์เข้าถึงระบบเครือข่ายคอมพิวเตอร์ เช่น จำกัดการใช้งานจุดเชื่อมต่อระบบเครือข่าย (port outlet) กำหนดมาตรการทางเทคนิคหรือเครื่องมือที่สามารถระบุตัวตนของอุปกรณ์ที่มาเชื่อมต่อกับระบบเครือข่าย (network port security) เป็นต้น

เอกสารเปรียบเทียบรายละเอียดของหลักเกณฑ์เดิม และหลักเกณฑ์ที่แก้ไข

หัวข้อ	รายละเอียดเดิม	รายละเอียดการแก้ไข
	เปิดใช้งาน service port ที่เชื่อมต่อตามความจำเป็น พร้อมทั้งมีวิธีการเพื่อระบุถึงอุปกรณ์ที่เชื่อมต่อ (authenticate) อย่างชัดเจน เช่น IP address และประเภทของอุปกรณ์ เป็นต้น	เปิดใช้งานช่องทางเชื่อมต่อ (port) ตามความจำเป็นเท่านั้น ในกรณีที่ต้องใช้งาน port ที่ถูกปิดไว้ ควรกำหนดกระบวนการในการขออนุมัติจากผู้มีอำนาจ และจัดให้มีการควบคุมอย่างเหมาะสม
	-เดิมไม่ได้กำหนด-	สอบทานกฎของอุปกรณ์ firewall อย่างสม่ำเสมอ หรืออย่างน้อยปีละ 1 ครั้งพร้อมจัดทำรายงานการสอบทานอย่างเป็นลายลักษณ์อักษร รวมถึงกำหนดให้มีการรายงานต่อผู้บริหารที่เกี่ยวข้อง
	มีการบันทึกและจัดเก็บหลักฐาน (logs) ที่ติดต่อกับระบบงานสำคัญและมีความเสี่ยงสูง เพื่อติดตามตรวจสอบการทำงานที่เกี่ยวข้อง หรืออาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบเครือข่ายคอมพิวเตอร์ ทั้งนี้ กรณีการใช้งานอินเทอร์เน็ตที่เกิดขึ้นจากการใช้งานผ่านเครือข่ายสารสนเทศของผู้ประกอบธุรกิจ ให้บันทึกและจัดเก็บหลักฐาน internet access log	ย้ายไปหัวข้อ การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ
	การควบคุมการรับส่งข้อมูลสารสนเทศ (information transfer) ● ผู้ประกอบธุรกิจต้องจัดให้มีการกำหนดนโยบายอย่างน้อยในเรื่องดังต่อไปนี้ ไว้เป็นลายลักษณ์อักษร เพื่อรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (information security policy)	ย้ายไปหัวข้อ การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ
	จัดให้มีนโยบายและหลักปฏิบัติเพื่อปกป้องข้อมูลสารสนเทศที่รับส่งผ่านระบบและอุปกรณ์ในการสื่อสารทุกประเภท โดยมีเนื้อหาขั้นต่ำครอบคลุมถึง ● กระบวนการป้องกันการรับส่งข้อมูลสารสนเทศนอกเส้นทางที่ได้กำหนดไว้ (mis-routing) การดักรับสัญญาณ การเปลี่ยนแปลงแก้ไขหรือทำความเสียหายกับข้อมูล และ	มีกระบวนการป้องกันข้อมูลที่เป็นความลับหรือมีความสำคัญที่ถูกรับส่งผ่านระบบเครือข่ายคอมพิวเตอร์ เช่น จดหมายอิเล็กทรอนิกส์ โดยมีเนื้อหาครอบคลุมถึง (ก) การนำเทคนิคการเข้ารหัสข้อมูลมาใช้ในการรับส่งข้อมูลสารสนเทศที่เป็นความลับและมีความสำคัญ (ข) การป้องกันข้อมูลที่รับส่งในรูปแบบของไฟล์แนบ (attachment files) (ค) การส่งต่อจดหมายอิเล็กทรอนิกส์แบบอัตโนมัติออกสู่ภายนอกองค์กร

เอกสารเปรียบเทียบรายละเอียดของหลักเกณฑ์เดิม และหลักเกณฑ์ที่แก้ไข

หัวข้อ	รายละเอียดเดิม	รายละเอียดการแก้ไข
	โปรแกรมไม่ประสงค์ดี (malware) ที่ถูกส่งผ่านช่องทางการสื่อสาร	(ง) การกำหนดการบริหารจัดการหรือมาตรการคัดกรอง (filter) ภัยคุกคามทางไซเบอร์ที่ปะปนมากับจดหมายอิเล็กทรอนิกส์ เช่น โปรแกรม malware ที่ส่งมาจากผู้ส่งที่น่าสงสัย (จ) กระบวนการในการควบคุมการเชื่อมต่อเครือข่ายระหว่างระบบงานภายในและหน่วยงานภายนอก (external party) ให้จำกัดเฉพาะบริการทางเครือข่ายตามความจำเป็นในการใช้งาน และมีการควบคุมโดยอุปกรณ์รักษาความปลอดภัย
	-เดิมไม่ได้กำหนด-	● ผู้ประกอบธุรกิจมีการจัดหาระบบและมาตรการรักษาความปลอดภัย ในการป้องกันการถูกโจมตีจากเครือข่ายสาธารณะที่เหมาะสมตามความเสี่ยง เช่น การใช้อุปกรณ์การรักษาความปลอดภัย intrusion prevention system (IPS) web application firewall (WAF) และมาตรการป้องกันการโจมตีแบบ DDoS (DDoS protection) เป็นต้น ● ผู้ประกอบธุรกิจควรมีมาตรการป้องกันความพยายามในการใช้งานและการปลอมแปลงหมายเลขประจำตัวเครือข่าย (IP address) ต้นทางเป็นหมายเลขเครือข่ายภายใน หรือ IP spoofing โดยการกำหนดมาตรการ เช่น ACL IP spoofing บน router หรือ firewall เป็นต้น ● [ผู้ประกอบธุรกิจความเสี่ยงสูง] ผู้ประกอบธุรกิจควรมีเครื่องมือในการวิเคราะห์พฤติกรรมการใช้งาน และเอกสารไฟล์แนบจากจดหมายอิเล็กทรอนิกส์ของผู้ใช้งานในสภาพแวดล้อมเสมือน เช่น การใช้งานเครื่องมือประเภท sandbox และระบบ advanced threat protection (ATP) เป็นต้น เพื่อตรวจสอบพฤติกรรมเสี่ยง และป้องกันความเสียหายจากการเข้าถึงข้อมูลและระบบงานสำคัญของบริษัท เป็นต้น ● [ผู้ประกอบธุรกิจความเสี่ยงสูง] ผู้ประกอบธุรกิจควรกำหนดกระบวนการในการติดตามและวิเคราะห์เพื่อใช้แจ้งเตือนพฤติกรรมต้องสงสัยของผู้ใช้งานตามระดับความเสี่ยง ได้แก่ พฤติกรรมการใช้งานเครือข่ายที่ผิดปกติ การถ่ายโอนข้อมูลเป็นจำนวนมาก การเข้าใช้งานในระบบงานในช่วงเวลาผิดปกติ หรือการเข้าใช้งาน

เอกสารเปรียบเทียบรายละเอียดของหลักเกณฑ์เดิม และหลักเกณฑ์ที่แก้ไข

หัวข้อ	รายละเอียดเดิม	รายละเอียดการแก้ไข
		จากเครื่องคอมพิวเตอร์ที่ไม่เคยมีการใช้งาน หรืออาจพิจารณาใช้เทคโนโลยีที่สนับสนุนกระบวนการข้างต้น อาทิ ระบบ security analytics ● [ผู้ประกอบธุรกิจความเสี่ยงสูง] ผู้ประกอบธุรกิจควรกำหนดกระบวนการตรวจจับเพื่อป้องกันการเปลี่ยนแปลงแก้ไขการตั้งค่าอุปกรณ์คอมพิวเตอร์ โปรแกรม และระบบงานโดยไม่ได้รับอนุญาต และอาจพิจารณาใช้เทคโนโลยีที่สนับสนุนกระบวนการข้างต้น เช่น การใช้งานซอฟต์แวร์ file integrity monitoring (FIM) รวมถึงความพยายามในการเข้าถึงและแก้ไขเปลี่ยนแปลงการตั้งค่าอุปกรณ์รักษาความปลอดภัย เช่น อุปกรณ์ไฟร์วอลล์ อุปกรณ์ตรวจจับและป้องกันผู้บุกรุก หรือระบบรักษาความปลอดภัยอื่น ๆ ● [ผู้ประกอบธุรกิจความเสี่ยงสูง] ผู้ประกอบธุรกิจควรมีการติดตั้งอุปกรณ์รักษาความปลอดภัยเครือข่ายเพื่อคัดกรอง traffic ในระดับ application ในจุดที่มีการเชื่อมต่อกับเครือข่ายสาธารณะ เช่น การใช้ Web Application Firewall (WAF) เป็นต้น ● [ผู้ประกอบธุรกิจความเสี่ยงสูง] การเข้าถึงอุปกรณ์เครือข่าย และอุปกรณ์รักษาความปลอดภัยเพื่อบริหารจัดการค่าต่างๆ ควรทำผ่านเครือข่ายเฉพาะที่แยกออกจากเครือข่ายปกติ เพื่อลดความเสี่ยงในการเปลี่ยนแปลงอุปกรณ์เครือข่ายและอุปกรณ์รักษาความปลอดภัยเครือข่ายโดยบุคคลที่ไม่ได้รับอนุญาต
	ข้อตกลงเกี่ยวกับการรักษาความลับหรือไม่เปิดเผยข้อมูล ควรมีเนื้อหาขั้นต่ำครอบคลุมถึง (1) การระบุความเป็นเจ้าของข้อมูลสำคัญทางธุรกิจ ทรัพย์สินทางปัญญา และวิธีป้องกันการรั่วไหลของข้อมูล (2) การป้องกันการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต โดยจัดให้มีการลงนามโดยผู้รับผิดชอบ (3) การกำหนดขั้นตอนการขออนุญาตเข้าถึงข้อมูลหรือกำหนดสิทธิการเข้าถึงข้อมูลตามที่ได้ลงนาม	ย้ายไปยังหัวข้อ การบริหารจัดการบุคลากร

เอกสารเปรียบเทียบรายละเอียดของหลักเกณฑ์เดิม และหลักเกณฑ์ที่แก้ไข

หัวข้อ	รายละเอียดเดิม	รายละเอียดการแก้ไข
	(4) การกำหนดสิทธิการเข้าถึงข้อมูลเพื่อตรวจสอบหรือติดตามการใช้งานข้อมูลที่มีความสำคัญ (5) การกำหนดกระบวนการแจ้งเตือนและรายงานผู้เกี่ยวข้องหากพบการรั่วไหลหรือเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต (6) การกำหนดมาตรการดำเนินการกรณีละเมิดหรือยกเลิกข้อตกลง รวมทั้งข้อกำหนดในการคืนหรือทำลายข้อมูลที่มีความสำคัญเมื่อสิ้นสุดข้อตกลง	
การบริหารจัดการโครงการด้านเทคโนโลยีสารสนเทศ และการจัดหา พัฒนาและบำรุงรักษาระบบระบบสารสนเทศ (IT Project Management, and System Acquisition, Development and Maintenance)	การจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศ (system acquisition, development and maintenance)	แบ่งหัวข้อการจัดหาและพัฒนาระบบงาน ได้แก่ system acquisition, system development, system change IT project management การจัดหาระบบสารสนเทศ (system acquisition)
	-เดิมไม่ได้กำหนด-	**การจัดหาระบบสารสนเทศ (system acquisition)** ผู้ประกอบธุรกิจต้องจัดให้มีหลักเกณฑ์ในการคัดเลือกเทคโนโลยี ระบบและผู้ให้บริการเพื่อมั่นใจว่าระบบที่จัดหาสามารถตอบสนองความต้องการทางธุรกิจและความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ โดยคำนึงถึงความยืดหยุ่นในการเปลี่ยนแปลงผู้ให้บริการ การเปลี่ยนแปลงเทคโนโลยี และการเปลี่ยนแปลงกลยุทธ์ในการดำเนินธุรกิจ ประกอบด้วย (1) รายละเอียดทั่วไป เช่น สิทธิ์การใช้งานซอฟต์แวร์ (software license) (2) ความมั่นคงปลอดภัยของระบบ (3) ฐานะการเงิน ชื่อเสียง และความสามารถด้านเทคนิค (4) การได้รับการรับรองตามมาตรฐานสากลหรือมาตรฐานด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้องที่ได้รับการยอมรับโดยทั่วไป (certificate) (5) การสนับสนุนและการบำรุงรักษาระบบ (6) ความน่าเชื่อถือของระบบและผู้ให้บริการ (7) การทดสอบการทำงานขั้นต้น (proof of concept) ในกรณีที่เป็นระบบสำคัญ

เอกสารเปรียบเทียบรายละเอียดของหลักเกณฑ์เดิม และหลักเกณฑ์ที่แก้ไข

หัวข้อ	รายละเอียดเดิม	รายละเอียดการแก้ไข
		(8) ข้อตกลงการรับฝากโคดต้นฉบับ (source code escrow agreement) เพื่อให้มั่นใจว่าในกรณีที่ผู้พัฒนาระบบหรือผู้ให้บริการซอฟต์แวร์ไม่ปฏิบัติตามข้อตกลงในการบำรุงรักษาระบบหรือให้การสนับสนุนการดำเนินงานตามที่ตกลงไว้ ผู้ประกอบธุรกิจจะมีสิทธิ์ในการเข้าถึง source code ของระบบหรือซอฟต์แวร์ดังกล่าว (9) ความยืดหยุ่นในการเปลี่ยนแปลงผู้ให้บริการ การเปลี่ยนแปลงเทคโนโลยี และการเปลี่ยนแปลงกลยุทธ์ในการดำเนินธุรกิจ (10) การควบคุมดูแลผู้ให้บริการปฏิบัติตามมาตรฐานและระเบียบวิธีปฏิบัติการออกแบบเชิงสถาปัตยกรรม
	การรักษาความมั่นคงปลอดภัยในกระบวนการพัฒนาระบบสารสนเทศ (security in development and support process) ผู้ประกอบธุรกิจต้องจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศ (system acquisition, development and maintenance) ตามหลักเกณฑ์ ● มีการควบคุมการพัฒนาหรือการแก้ไขเปลี่ยนแปลงระบบสารสนเทศในทุกขั้นตอนให้เป็นไปตามขั้นตอนการควบคุมความมั่นคงปลอดภัยด้านสารสนเทศที่กำหนดไว้ ● มีการควบคุมบุคลากร ขั้นตอน และเทคโนโลยีสำหรับการพัฒนาระบบสารสนเทศให้มีความมั่นคงปลอดภัยตลอดขั้นตอนการพัฒนาระบบ ● มีการดูแล ติดตาม และควบคุมการพัฒนาระบบสารสนเทศของผู้รับดำเนินการให้เป็นไปตามข้อตกลงการใช้บริการ	**การพัฒนาระบบสารสนเทศ (system development)** การออกแบบระบบ ● จัดทำเอกสารความต้องการของระบบทั้งความต้องการที่เป็นหน้าที่หลัก (functional requirement) และความต้องการที่ไม่ใช่หน้าที่หลัก (non-functional requirement) โดยครอบคลุมการรักษาความมั่นคงปลอดภัยและข้อมูลส่วนบุคคลที่ถูกจัดเก็บและประมวลผลบนระบบงานของผู้ประกอบธุรกิจ (security and privacy specification) โดยให้หน่วยงานธุรกิจที่เกี่ยวข้องมีส่วนในการสอบทานความถูกต้องของความต้องการทางธุรกิจ (business requirement) ก่อนเริ่มออกแบบระบบ ● มีการจัดทำเอกสารรายละเอียดคุณสมบัติทางเทคนิค (technical specification) ของระบบที่พัฒนา โดยที่ครอบคลุมเรื่องข้อกำหนดด้านการรักษาความมั่นคงปลอดภัย การคุ้มครองข้อมูลส่วนบุคคล (privacy) ความพร้อมใช้ (availability) และขีดความสามารถที่รองรับ (capacity) รวมทั้งจัดให้มีการสอบทานความถูกต้องครบถ้วนและอนุมัติจากผู้ที่เกี่ยวข้องก่อนเริ่มพัฒนาระบบ

เอกสารเปรียบเทียบรายละเอียดของหลักเกณฑ์เดิม และหลักเกณฑ์ที่แก้ไข

หัวข้อ	รายละเอียดเดิม	รายละเอียดการแก้ไข
	การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ ● มีการควบคุมการเข้าถึงสภาพแวดล้อมของการพัฒนาระบบสารสนเทศอย่างรัดกุมเหมาะสม	
		การพัฒนาระบบสารสนเทศ (system development) การพัฒนาระบบ ● มีการแบ่งแยกบทบาทหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องในการพัฒนาระบบ (segregation of duty) เพื่อให้มีการสอบทานก่อนนำระบบขึ้นไปให้บริการจริง เช่น แยกผู้พัฒนาระบบ ออกจากผู้นำระบบขึ้นใช้งานจริง เป็นต้น ● แบ่งแยกสภาพแวดล้อมของระบบงานที่ใช้สำหรับการพัฒนา (development) และการทดสอบ (testing) ออกจากระบบงานที่ให้บริการจริง (production) โดยควบคุมให้มีการเข้าถึงเฉพาะผู้ที่เกี่ยวข้องในแต่ละส่วนเท่านั้น ● กำหนดมาตรฐานและระเบียบวิธีปฏิบัติในการออกแบบและพัฒนาระบบอย่างปลอดภัย (secure coding) และสอดคล้องกับมาตรฐานสากล รวมทั้งควบคุมให้ผู้พัฒนาระบบปฏิบัติตามมาตรฐานและระเบียบวิธีปฏิบัติดังกล่าว ● สอบทานคำสั่งในการเขียนโปรแกรม (source code review) อย่างเป็นอิสระทุกครั้งที่มีการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบสารสนเทศที่มีความสำคัญและระบบงานที่เชื่อมต่อกับเครือข่ายสาธารณะ (internet facing) เพื่อระบุช่องโหว่ด้านความมั่นคงปลอดภัย และปิดช่องโหว่ที่พบทุกครั้งก่อนนำไปใช้งานจริง ● [ผู้ประกอบธุรกิจที่มีความเสี่ยงสูง] สอบทานคำสั่งในการเขียนโปรแกรมโดยบุคคล (Manual Source Code Review) ที่เป็นอิสระจากผู้พัฒนาโปรแกรม ทุกครั้งที่มีการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบสารสนเทศที่มีความสำคัญ ● มีกระบวนการหรือเครื่องมือควบคุมเวอร์ชันของชุดคำสั่งคอมพิวเตอร์ (source code version control)

เอกสารเปรียบเทียบรายละเอียดของหลักเกณฑ์เดิม และหลักเกณฑ์ที่แก้ไข

หัวข้อ	รายละเอียดเดิม	รายละเอียดการแก้ไข
		• ในกรณีที่มีการมอบให้มอบหมายให้บุคคลภายนอกเป็นผู้พัฒนาหรือแก้ไขเปลี่ยนแปลงระบบสารสนเทศ ควรจัดให้มีการติดตาม และควบคุมการดำเนินการให้ไปตามข้อตกลงการจ้างงาน • มีการควบคุมเครื่องที่ไม่ได้อยู่บนระบบที่ให้บริการจริง (non-production) ให้มีความปลอดภัยเพียงพอตามระดับความเสี่ยงเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต • มีการควบคุมไม่ให้มีการติดตั้งเครื่องมือการพัฒนาระบบ (development tools) และเครื่องมือแปลโปรแกรม (compilers) ไว้บนระบบที่ให้บริการจริง เพื่อป้องกันความเสี่ยงที่อาจถูกปรับเปลี่ยนหรือติดตั้งโปรแกรมโดยไม่ได้รับอนุญาต
		การพัฒนาระบบสารสนเทศ (system development) การทดสอบระบบ • ทดสอบระบบสารสนเทศที่ได้รับการพัฒนาหรือแก้ไขเปลี่ยนแปลง โดยผู้ทดสอบที่เป็นอิสระจากผู้พัฒนาระบบ เพื่อให้มั่นใจได้ว่าระบบที่ได้รับการพัฒนาดังกล่าวสามารถทำงานได้อย่างถูกต้องตรงความต้องการของผู้ใช้งาน และเป็นไปตามนโยบายด้านความมั่นคงปลอดภัยของระบบสารสนเทศ • ทดสอบระบบสารสนเทศที่ได้รับการพัฒนาหรือแก้ไขเปลี่ยนแปลงก่อนนำไปใช้งานหรือให้บริการจริง ควรครอบคลุมการทดสอบ ดังนี้ (ก) ทดสอบการทำงานของแต่ละโมดูล (unit test) (ข) ทดสอบการทำงานของระบบและการเชื่อมต่อ (system and integration test) (ค) ทดสอบความต้องการของผู้ใช้งาน (user acceptance test) ทั้งนี้ ในกรณีที่พบปัญหาหรือข้อบกพร่องในการทดสอบ ควรจัดให้มีการแก้ไขอย่างเหมาะสมเพื่อไม่ให้มีผลกระทบกับการให้บริการจริง • ทดสอบการรักษาความปลอดภัย (security test) ได้แก่ การประเมินช่องโหว่ (vulnerabilities assessment) และการทดสอบเจาะระบบ (penetration test) ตามความจำเป็น สำหรับระบบใหม่ใด ๆ ที่มีการเชื่อมต่อกับระบบสารสนเทศที่มี

เอกสารเปรียบเทียบรายละเอียดของหลักเกณฑ์เดิม และหลักเกณฑ์ที่แก้ไข

หัวข้อ	รายละเอียดเดิม	รายละเอียดการแก้ไข
		ความสำคัญ เพื่อให้สามารถตรวจพบช่องโหว่และดำเนินการปรับปรุงแก้ไขได้ก่อนเริ่มให้บริการจริง ● ทดสอบประสิทธิภาพ (performance test) ระบบที่เกี่ยวข้องกับการให้บริการหรือการทำธุรกรรมทางอิเล็กทรอนิกส์ และทุกครั้งที่มีการพัฒนาหรือเปลี่ยนแปลงมีนัยสำคัญ เพื่อให้มั่นใจได้ว่าระบบมีเสถียรภาพเพียงพอในการรองรับการเข้าใช้งานจำนวนมาก และแผนการดำเนินธุรกิจ ● มีมาตรการควบคุมความถูกต้องครบถ้วนของการแปลงข้อมูล (data conversion) และการโอนย้ายข้อมูลจากระบบเดิมไปยังระบบใหม่ (data migration) เพื่อให้มั่นใจว่าข้อมูลมีความถูกต้องครบถ้วน ● ในกรณีผู้ประกอบธุรกิจมีการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบสารสนเทศที่มีการกำหนดรอบการพัฒนาย่อย ๆ (sprint) เช่น การพัฒนาระบบสารสนเทศแบบ agile ควรจัดให้มีการควบคุมด้านความมั่นคงปลอดภัยด้านสารสนเทศตั้งแต่การ ออกแบบ พัฒนา และทดสอบระบบ ในแต่ละรอบการพัฒนา เพื่อให้มั่นใจว่าระบบมีความถูกต้อง มั่นคงปลอดภัย เชื่อถือได้ พร้อมใช้งาน และมีความยืดหยุ่นเพียงพอที่จะรองรับการปรับปรุงเปลี่ยนแปลง
		การพัฒนาระบบสารสนเทศ (system development) การนำระบบขึ้นใช้งานจริง ● การนำระบบขึ้นใช้งานจริง ควรผ่านกระบวนการบริหารจัดการการเปลี่ยนแปลงที่กำหนดไว้ เพื่อป้องกันความเสี่ยงหรือข้อผิดพลาดในการปฏิบัติงาน ● ระบบงานสำรองควรมีการปรับปรุงให้เป็นปัจจุบัน เพื่อรองรับเหตุการณ์ฉุกเฉิน
	การรักษาความมั่นคงปลอดภัยในกระบวนการพัฒนาระบบสารสนเทศ (security in development and support process) กำหนดวิธีปฏิบัติให้คำขอให้แก้ไขหรือพัฒนาต้องมาจากผู้ที่มีสิทธิและอนุมัติคำขอโดยผู้มีอำนาจ ตรวจรับจากผู้มีอำนาจ	**การแก้ไขเปลี่ยนแปลงระบบสารสนเทศ (system change)** (1) ย้ายแนวปฏิบัติบางส่วนเพื่อระบุภายในหัวข้อ การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ – การบริหารจัดการการเปลี่ยนแปลงด้านเทคโนโลยีสารสนเทศ (change management) (2) แก้ไขผู้มีอำนาจอนุมัติ

เอกสารเปรียบเทียบรายละเอียดของหลักเกณฑ์เดิม และหลักเกณฑ์ที่แก้ไข

หัวข้อ	รายละเอียดเดิม	รายละเอียดการแก้ไข
	ภายหลังการแก้ไขหรือพัฒนาแล้วเสร็จก่อนโอนย้ายระบบงาน รวมทั้งจัดเก็บรายละเอียดของคำขอไว้	กระบวนการขออนุมัติการเปลี่ยนแปลง (change request) ควรได้รับการอนุมัติจากหน่วยงานเจ้าของระบบ (system owner) อย่างเป็นลายลักษณ์อักษร
	-เดิมไม่ได้กำหนด-	**IT project management** ผู้ประกอบธุรกิจควรกำหนดกรอบการบริหารจัดการโครงการ (project management framework) ที่ชัดเจนเป็นลายลักษณ์อักษร เพื่อเป็นแนวทางดำเนินโครงการจัดหาหรือพัฒนาระบบเทคโนโลยีสารสนเทศ โดยควรครอบคลุม ดังนี้ (1) โครงสร้างการควบคุมและกำกับดูแลโครงการ (project governance) ที่ชัดเจน เพื่อให้มีการควบคุมดูแลโครงการให้สำเร็จเป็นไปตามแผนงานที่กำหนด ซึ่งประกอบด้วย (ก) คณะกรรมการกำกับดูแลโครงการ (project steering committee) (ข) เจ้าของโครงการหรือผู้สนับสนุนโครงการ (project owner/ project sponsor) (ค) หน่วยงานหรือทีมงานดูแลภาพรวมโครงการ (project management office) (ง) ผู้จัดการโครงการ (project manager) (2) แนวทางการบริหารจัดการโครงการ ควรครอบคลุมอย่างน้อย ดังนี้ (ก) กรอบการบริหารจัดการโครงการ ครอบคลุมตั้งแต่ก่อนเริ่มโครงการ การดำเนินการและควบคุมโครงการ การปิดโครงการ และการสอบทานโครงการ (ข) ปัจจัยและเกณฑ์ในการประเมินหรือจัดระดับความสำคัญของโครงการที่ชัดเจน รวมถึงขอบเขตอำนาจหน้าที่ในการอนุมัติและกำกับดูแลโครงการตามระดับความสำคัญของโครงการ (ค) ขั้นตอนการดำเนินการ (Action Item) ที่ต้องส่งมอบในแต่ละขั้นตอนอย่างชัดเจน เช่น แผนการดำเนินโครงการ รายงานความคืบหน้า รายงานการปิดโครงการ เป็นต้น **การเริ่มโครงการ**

เอกสารเปรียบเทียบรายละเอียดของหลักเกณฑ์เดิม และหลักเกณฑ์ที่แก้ไข

หัวข้อ	รายละเอียดเดิม	รายละเอียดการแก้ไข
		(1) มีการประเมินความจำเป็นและประโยชน์ที่คาดว่าจะได้รับ ประเมินความเสี่ยงและผลกระทบที่อาจเกิดขึ้นต่อฝ่ายงานอื่นและระบบที่เกี่ยวข้อง รวมทั้งเลือกใช้เทคโนโลยีที่เหมาะสม ทั้งนี้ โครงการต้องมีเป้าหมายที่ชัดเจน (project objective) สอดคล้องกับกลยุทธ์ขององค์กรและคำนึงถึงการรักษาความมั่นคงปลอดภัย มีแผนการดำเนินโครงการที่มีรายละเอียดครบถ้วนเพียงพอต่อการบริหารจัดการโครงการอย่างน้อยครอบคลุม เป้าหมายโครงการ ทรัพยากร บทบาทหน้าที่ขอบเขตและระยะเวลา ผลที่จะส่งมอบ ข้อกำหนดเงื่อนไข เป็นต้น (2) มีการนำเสนอแผนการดำเนินโครงการ เพื่อขออนุมัติโครงการต่อคณะกรรมการหรือผู้บริหารของผู้ประกอบธุรกิจที่ได้รับมอบหมายตามขอบเขตในการอนุมัติที่กำหนดไว้ **การดำเนินการและควบคุมโครงการ** (1) มีการประเมินและติดตามการดำเนินโครงการอย่างต่อเนื่องและครอบคลุมขอบเขต ระยะเวลา และทรัพยากรที่วางแผน (2) ในกรณีที่มีการเปลี่ยนแปลงขอบเขต ระยะเวลาและหรือทรัพยากร หรือยกเลิกโครงการ ควรมีการนำเสนอเพื่อขออนุมัติการเปลี่ยนแปลงหรือยกเลิกโครงการ (3) มีการรายงานความคืบหน้า ปัญหา อุปสรรคและข้อจำกัดในการดำเนินโครงการต่อคณะกรรมการกำกับดูแลโครงการหรือผู้บริหารที่ได้รับมอบหมายอย่างสม่ำเสมอ (4) โครงการที่ส่งผลกระทบต่อธุรกิจของผู้ประกอบธุรกิจอย่างมีนัยสำคัญ ควรได้รับการนำเสนอแก่คณะกรรมการของผู้ประกอบธุรกิจด้วย **การปิดโครงการ** (1) มีการสรุปประโยชน์ที่ได้รับจากโครงการเปรียบเทียบกับเป้าหมายที่กำหนด (2) มีการรวบรวมปัญหา อุปสรรคจากการบริหารจัดการโครงการ เพื่อนำมาเป็นสิ่งที่ได้เรียนรู้ (lesson learned) ใช้สำหรับวิเคราะห์ ปรับปรุง และพัฒนา **การสอบทานโครงการ**

เอกสารเปรียบเทียบรายละเอียดของหลักเกณฑ์เดิม และหลักเกณฑ์ที่แก้ไข

หัวข้อ	รายละเอียดเดิม	รายละเอียดการแก้ไข
		(1) มีการสอบทานโครงการที่สำคัญ โดยหน่วยงานอิสระ เพื่อให้มั่นใจได้ว่าโครงการสอดคล้องกับเป้าหมายของโครงการ นโยบาย มาตรฐาน ระเบียบและวิธีปฏิบัติของผู้ประกอบธุรกิจ รวมทั้งกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง
การบริหารจัดการบุคคลภายนอก (Third Party Management)	ในกรณีที่ผู้ประกอบธุรกิจแต่งตั้งบุคคลอื่นเป็นผู้รับดำเนินการในงานที่เกี่ยวกับระบบสารสนเทศของผู้ประกอบธุรกิจ ผู้ประกอบธุรกิจต้องดำเนินการให้เป็นไปตามหลักเกณฑ์ที่กำหนด	ในกรณีที่ผู้ประกอบธุรกิจ (1) ใช้บริการงานด้านเทคโนโลยีสารสนเทศจากบุคคลภายนอก (third party) หรือ (2) เชื่อมต่อระบบสารสนเทศกับบุคคลภายนอก หรือ (3) อนุญาตให้บุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญหรือข้อมูลของลูกค้าที่ควบคุมดูแลโดยผู้ประกอบธุรกิจได้ ผู้ประกอบธุรกิจต้องบริหารจัดการบุคคลภายนอก รวมถึงความเสี่ยงจากผู้รับดำเนินการช่วง (subcontract) ตลอดทั้งห่วงโซ่อุปทาน (supply chain) อย่างมีประสิทธิภาพบนพื้นฐานที่ผู้ประกอบธุรกิจต้องรับผิดชอบต่อการดำเนินธุรกิจ และการให้บริการแก่ลูกค้า และคงไว้ซึ่งความน่าเชื่อถือ ชื่อเสียง ประสิทธิ์ภาพในการบริการ ตามหลักเกณฑ์ที่กำหนด
	มีนโยบายเพื่อรองรับในกรณีที่ผู้ประกอบธุรกิจแต่งตั้งบุคคลอื่นเป็นผู้รับดำเนินการในงานที่เกี่ยวกับระบบสารสนเทศของผู้ประกอบธุรกิจ ซึ่งครอบคลุมถึงวิธีการคัดเลือกและประเมินผู้รับดำเนินการการทบทวนคุณสมบัติของผู้รับดำเนินการ และการมีข้อกำหนดเกี่ยวกับการใช้บริการ เพื่อลดความเสี่ยงจากการเข้าถึงทรัพย์สินสารสนเทศอย่างไม่เหมาะสม	มีการกำหนดกระบวนการและหลักเกณฑ์ในการประเมินความเสี่ยง เพื่อคัดเลือกบุคคลภายนอก ซึ่งครอบคลุมกรณีที่บุคคลภายนอกใช้บริการจากผู้รับดำเนินการช่วง (subcontract)
	-เดิมไม่ได้กำหนด-	การประเมินความเสี่ยงและผลกระทบทั้งก่อนใช้บริการงานด้านเทคโนโลยีสารสนเทศจากผู้ให้บริการภายนอก หรือเชื่อมต่อระบบเทคโนโลยีสารสนเทศกับบุคคลภายนอก หรือให้บุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญของผู้ประกอบธุรกิจหรือข้อมูลของลูกค้าที่ควบคุมดูแลโดยผู้ประกอบธุรกิจ รวมถึงประเมินเป็นประจำตามรอบระยะเวลาที่สอดคล้องกับระดับความเสี่ยงและความสำคัญ และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ โดยคำนึงถึงความเสี่ยงดังต่อไปนี้

เอกสารเปรียบเทียบรายละเอียดของหลักเกณฑ์เดิม และหลักเกณฑ์ที่แก้ไข

หัวข้อ	รายละเอียดเดิม	รายละเอียดการแก้ไข
		(1) ความเสี่ยงด้านกฎหมาย และกฎเกณฑ์ที่เกี่ยวข้องทั้งในประเทศและต่างประเทศ เช่น กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล และกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ เป็นต้น (2) ความเสี่ยงจากการกำกับดูแลและบริหารจัดการบุคคลภายนอกที่ไม่รัดกุมเพียงพอ (operational risk) (3) ความเสี่ยงจากการกระจุกตัว (concentration risk) เช่น ผู้ประกอบธุรกิจ และบริษัทในกลุ่มธุรกิจเดียวกันใช้บริการจากบุคคลภายนอกเพียงรายเดียว เป็นต้น (4) ความเสี่ยงจากการพึ่งพาบุคคลภายนอกรายใดรายหนึ่งเป็นหลัก (third party/vendor locked-in) ซึ่งทำให้มีข้อจำกัดในการเปลี่ยนแปลงเทคโนโลยีผู้ให้บริการ หรือข้อจำกัดในการนำระบบหรือข้อมูลกลับมาดำเนินการเอง (5) ความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยทางไซเบอร์ เช่น ระบบของบุคคลภายนอกมีช่องโหว่ทำให้ข้อมูลเกิดการสูญหายหรือรั่วไหล ระบบที่ให้บริการโดยบุคคลภายนอกเกิดขัดข้อง เป็นต้น (6) ความเสี่ยงกรณีบุคคลภายให้ผู้อื่นดำเนินการแทน (sub-contracting) เช่น subcontractor ปฏิบัติงานบกพร่อง เป็นต้น
	กำหนดวิธีการคัดเลือกและประเมินผู้รับดำเนินการ (due diligence) โดยควรให้ความสำคัญในเรื่องการรักษาความปลอดภัยของข้อมูลสารสนเทศที่สำคัญ (confidentiality) ความถูกต้องเชื่อถือได้ของข้อมูลและระบบสารสนเทศ (integrity) และความพร้อมใช้งานของระบบสารสนเทศที่ใช้บริการ (availability)	ผู้ประกอบธุรกิจควรทำการประเมินศักยภาพบุคคลภายนอก (due diligence) ที่มีความสำคัญอย่างยิ่งต่อผู้ประกอบธุรกิจ (critical 3rd party) โดยควรคำนึงถึงเรื่องดังต่อไปนี้ (1) ฐานะทางการเงิน ชื่อเสียง ความรู้ความเชี่ยวชาญ ประสบการณ์ และความสามารถในการให้บริการในช่วงที่ผ่านมา และระบบการบริหารงานภายใน (2) การบริหารจัดการความเสี่ยง การควบคุมภายใน การตรวจสอบภายใน และการติดตามผลการปฏิบัติงาน (3) การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (4) การบริหารจัดการความต่อเนื่องทางธุรกิจ และความพร้อมรับมือภัยหรือเหตุการณ์ต่าง ๆ

เอกสารเปรียบเทียบรายละเอียดของหลักเกณฑ์เดิม และหลักเกณฑ์ที่แก้ไข

หัวข้อ	รายละเอียดเดิม	รายละเอียดการแก้ไข
		(5) การปฏิบัติตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้อง เช่น การขอตรวจสอบเอกสารหลักฐานหรือใบรับรองจากบุคคลภายนอกในการดำเนินการตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้อง เป็นต้น (6) การปฏิบัติตามมาตรฐานสากลด้านเทคโนโลยีสารสนเทศ เช่น การขอตรวจสอบ หรือสามารถแสดงเอกสารหลักฐานการได้รับการรองรับตามมาตรฐาน ISO 27001 เป็นต้น โดยการรับรองการปฏิบัติตามมาตรฐานสากล บริษัทควรพิจารณาว่าบุคคลภายนอกได้รับการรับรองการให้บริการในส่วนที่สำคัญ เช่น ศูนย์คอมพิวเตอร์ และ/หรือ ได้รับการรับรองครอบคลุมทั้งองค์กร ทั้งนี้ การพิจารณาคัดเลือกผู้ให้บริการระบบคลาวด์ บริษัทควรคำนึงถึงความพร้อมและมาตรฐานในการให้บริการของผู้ให้บริการดังกล่าว โดยผู้ให้บริการระบบคลาวด์ควรได้รับการตรวจสอบรับรองมาตรฐานสากลที่เกี่ยวข้อง (7) การใช้เทคโนโลยีแบบเปิด (open technology) เพื่อให้สามารถนำระบบไปใช้งานหรือเชื่อมโยงกับระบบอื่นได้ (interoperability) และลดข้อจำกัดในการย้ายหรือเปลี่ยนแปลง เทคโนโลยีผู้ให้บริการหรือพันธมิตร รวมถึงข้อจำกัดในการนำระบบหรือข้อมูลกลับมา ดำเนินการเอง เช่น การใช้รูปแบบการรับส่งข้อมูลกับบุคคลภายนอกที่เป็นมาตรฐานแบบเปิด (open standard หรือ open source) เป็นต้น (8) กรณีที่บุคคลภายนอกมอบหมายการปฏิบัติงานที่สำคัญให้กับบุคคลอื่นต่อ (sub-contracting to another supplier) ผู้ประกอบธุรกิจควรพิจารณารายละเอียดด้านความมั่นคงปลอดภัยสารสนเทศของบุคคลดังกล่าวด้วย
	มีข้อตกลงและกระบวนการควบคุมเกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศอย่างเป็นลายลักษณ์อักษรในการใช้บริการจากผู้รับดำเนินการ โดยผู้ประกอบธุรกิจและผู้รับดำเนินการต้องมีการลงนามร่วมกันในข้อตกลงและกระบวนการดังกล่าว	ข้อตกลงหรือสัญญาการให้บริการต้องระบุขอบเขตของงาน สิทธิ์ และความรับผิดชอบของผู้ประกอบธุรกิจและบุคคลภายนอก ซึ่งรวมถึงความรับผิดชอบในด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ การคุ้มครองข้อมูลส่วนบุคคล และการปฏิบัติตามกฎหมายอื่น ๆ ที่เกี่ยวข้องอย่างชัดเจนเป็นลายลักษณ์อักษร โดยผู้ประกอบธุรกิจและบุคคลภายนอกต้องมีการลงนามร่วมกันในข้อตกลงหรือสัญญาดังกล่าว

เอกสารเปรียบเทียบรายละเอียดของหลักเกณฑ์เดิม และหลักเกณฑ์ที่แก้ไข

หัวข้อ	รายละเอียดเดิม	รายละเอียดการแก้ไข
	-เดิมไม่ได้กำหนด-	มีข้อตกลงการไม่เปิดเผยข้อมูล (non-disclosure agreement) กรณีที่บุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญของผู้ประกอบธุรกิจหรือข้อมูลของลูกค้าที่ควบคุมดูแลโดยผู้ประกอบธุรกิจได้ นอกจากนี้ บุคคลภายนอกต้องไม่เปิดเผยข้อมูลต่อ subcontract โดยไม่ได้รับความยินยอมจากผู้ประกอบธุรกิจ
	ผู้รับดำเนินการควรมีแผนรองรับกรณีเกิดเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (incident response policy) โดยคำนึงถึงแผนของผู้ประกอบธุรกิจ รวมทั้งมีกระบวนการการกู้คืนระบบงานให้เป็นไปตามข้อตกลงที่ได้กำหนดไว้ เพื่อให้ข้อมูลและการประมวลผลข้อมูลอยู่ในสภาพที่พร้อมใช้งานเสมอ เป็นต้น	กำหนดให้บุคคลภายนอกมีแผนรองรับในกรณีที่เกิดเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ (incident response policy) ครอบคลุมอย่างน้อย เหตุการณ์ที่เกี่ยวข้องกับเหตุการณ์ความปลอดภัยทางไซเบอร์ และเหตุการณ์การละเมิดต่อข้อมูลส่วนบุคคล
	• กำหนดสิทธิในการเข้าตรวจสอบกระบวนการปฏิบัติงานของผู้รับดำเนินการและควบคุมให้การปฏิบัติงานเป็นไปตามข้อตกลงที่กำหนดไว้ • มีข้อกำหนดให้ผู้รับดำเนินการยินยอมให้สำนักงานเรียกดูตรวจสอบเอกสารหลักฐานที่เกี่ยวข้องหรือสามารถเข้าตรวจสอบการปฏิบัติงานของผู้รับดำเนินการ	ข้อตกลงหรือสัญญาการให้บริการต้องระบุต้องระบุสิทธิ์ให้ผู้ประกอบธุรกิจ สำนักงาน และผู้ตรวจสอบภายนอกที่ได้รับการแต่งตั้งจากผู้ประกอบธุรกิจหรือสำนักงาน สามารถเข้าตรวจสอบการดำเนินงานและการควบคุมภายในของบุคคลภายนอกในส่วนที่เกี่ยวข้องการกับใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอกของผู้ประกอบธุรกิจ ทั้งนี้ หากมีเหตุจำเป็นที่ผู้ประกอบธุรกิจไม่สามารถดำเนินการระบุสิทธิหรือเงื่อนไขการตรวจสอบลงในสัญญาหรือข้อตกลงได้ ผู้ประกอบธุรกิจต้องมีมาตรการประเมินหรือติดตามการดำเนินงานและการควบคุมภายในของบุคคลภายนอกให้รัดกุมเพียงพอสอดคล้องกับความเสี่ยงและความมีนัยสำคัญของการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูล
	กำหนดหน้าที่ความรับผิดชอบของผู้รับดำเนินการในการปฏิบัติงานภายใต้การควบคุมต่าง ๆ	รายละเอียดและเงื่อนไขที่สำคัญในสัญญาหรือข้อตกลงกับบุคคภายนอก ควรคำนึงถึงเรื่องดังต่อไปนี้ (1) ขอบเขตการให้บริการ

เอกสารเปรียบเทียบรายละเอียดของหลักเกณฑ์เดิม และหลักเกณฑ์ที่แก้ไข

หัวข้อ	รายละเอียดเดิม	รายละเอียดการแก้ไข
		(2) ข้อตกลงระดับการให้บริการด้านเทคโนโลยีสารสนเทศ (service level agreement: SLA) และการดำเนินการกรณีที่ผู้ให้บริการภายนอกไม่สามารถให้บริการได้ตามข้อตกลงระดับการให้บริการ (3) รายละเอียดของข้อมูลที่จำเป็นต้องใช้หรือเข้าถึงโดยผู้ให้บริการภายนอก รวมทั้งวิธีการเข้าถึงข้อมูลดังกล่าว (4) การจัดให้มีแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT contingency plan) หรือแผนกู้คืนระบบเทคโนโลยีสารสนเทศ (disaster recovery plan) โดยผู้ให้บริการภายนอก (5) การทำลายข้อมูลเมื่อสิ้นสุดหรือยกเลิกการใช้บริการงานด้านเทคโนโลยีสารสนเทศจากผู้ให้บริการภายนอก (6) ในกรณีที่ผู้ประกอบธุรกิจไม่สามารถระบุสิทธิ์ในการเข้าตรวจสอบ (right to audit) ลงในข้อตกลงหรือสัญญาการให้บริการได้ ผู้ประกอบธุรกิจควรมีแนวทางที่จะใช้ประเมินหรือติดตามการดำเนินงานและการควบคุมภายในของบุคคลภายนอกให้รัดกุมเพียงพอสอดคล้องกับระดับความเสี่ยง และความมีนัยสำคัญของการใช้บริการ การเชื่อมต่อหรือ การเข้าถึงข้อมูล โดยอาจใช้ผลการตรวจสอบด้านเทคโนโลยีสารสนเทศของบุคคลภายนอกที่ได้รับการรับรองจากผู้ตรวจสอบภายนอกที่มีความเป็นอิสระและได้มาตรฐานสากล เช่น ผลการตรวจสอบตามมาตรฐาน SSAE 18 (SOC 2 Type 2 Report) หรือ PCI-DSS Attestation of Compliance (AOC) เป็นต้น และรับทราบโดยคณะกรรมการหรือผู้บริหารระดับสูงของผู้ประกอบธุรกิจ (7) ข้อตกลงในการเปลี่ยนแปลงผู้ให้บริการภายนอกและการยกเลิกหรือสิ้นสุดสัญญา (exit strategy) (8) หากมีข้อจำกัดในรายละเอียดและเงื่อนไขข้อตกลงหรือสัญญาการให้บริการ ผู้ประกอบธุรกิจควรมีการประเมินความเสี่ยงและพิจารณาแนวทางควบคุมความเสี่ยงที่เพียงพอเหมาะสมก่อนดำเนินการเพื่อขออนุมัติยกเว้น (exception)

เอกสารเปรียบเทียบรายละเอียดของหลักเกณฑ์เดิม และหลักเกณฑ์ที่แก้ไข

หัวข้อ	รายละเอียดเดิม	รายละเอียดการแก้ไข
	-เดิมไม่ได้กำหนด-	ผู้ประกอบธุรกิจควรมีมาตรการกำกับดูแลให้บุคคลภายนอกปฏิบัติตามหลักเกณฑ์การปฏิบัติงานที่คณะกรรมการ ก.ล.ต. คณะกรรมการกำกับตลาดทุน หรือสำนักงานกำหนด รวมทั้งระเบียบวิธีปฏิบัติที่ผู้ประกอบธุรกิจกำหนดขึ้น โดยอย่างน้อยมาตรการดังกล่าวต้องสามารถควบคุมให้บุคคลภายนอกไม่มีลักษณะที่จะทำให้มีเหตุอันควรเชื่อได้ว่ามีข้อบกพร่องหรือมีความไม่เหมาะสมเกี่ยวกับการควบคุมและการปฏิบัติงานอันดีของธุรกิจ
	-เดิมไม่ได้กำหนด-	ผู้ประกอบธุรกิจควรจัดให้มีมาตรการรองรับในกรณีที่บุคคลภายนอกมีการเปลี่ยนแปลงกระบวนการ ขั้นตอน หรือวิธีการปฏิบัติงานในการรักษาความมั่นคงปลอดภัยในการปฏิบัติงาน หรือเปลี่ยนผู้ให้บริการ
	-เดิมไม่ได้กำหนด-	[ผู้ประกอบธุรกิจที่มีความเสี่ยงภาพรวมในระดับสูง] ผู้ประกอบธุรกิจควรมีการจัดทำรายชื่อผู้ให้บริการ และจัดให้มีการประเมินด้านคุณภาพและความเชื่อถือของผู้ให้บริการหรือผู้รับดำเนินการ (trusted vendor) โดยพิจารณาจากประสบการณ์ คุณภาพของบริการและผลงานที่ส่งมอบ ตลอดจนมาตรฐานด้านความปลอดภัยเทคโนโลยีสารสนเทศที่เกี่ยวข้องกับสินค้าและบริการ เพื่อใช้เป็นส่วนหนึ่งขององค์ประกอบในการคัดเลือกผู้ให้บริการในอนาคต
การบริหารจัดการเหตุการณ์ผิดปกติและปัญหาด้านเทคโนโลยีสารสนเทศ (IT Incident Management)	รายงานสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์เมื่อมีเหตุการณ์ที่ส่งผลกระทบต่อระบบสารสนเทศที่มีความสำคัญ ประเภทดังต่อไปนี้ (1) ระบบหยุดชะงัก (system disruption) (2) มีการบุกรุก เข้าถึง หรือใช้งานระบบโดยไม่ได้รับอนุญาต (system compromised) (3) ส่งผลกระทบต่อชื่อเสียงของผู้ประกอบธุรกิจ (harm to reputation) เช่น ถูกปลอมแปลงหน้าเว็บไซต์ของบริษัท (website defacement)	รายงานสำนักงานในกรณีที่มีเหตุการณ์ที่ส่งผลกระทบต่อระบบงานสำคัญและมีผลกระทบต่อลูกค้าในวงกว้าง โดยครอบคลุมเหตุการณ์ดังนี้ (1) การละเมิดต่อข้อมูลส่วนบุคคลที่เกิดจากเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ (2) ทรัพย์สินของผู้ใช้งานสูญหาย หรือเสียหาย (3) การบุกรุก เข้าถึง หรือใช้งานระบบโดยไม่ได้รับอนุญาต (system compromised) (4) ส่งผลกระทบต่อชื่อเสียงของผู้ประกอบธุรกิจ (harm to reputation) เช่น ถูกปลอมแปลงหน้าเว็บไซต์ของบริษัท (website defacement) (5) การหยุดชะงักของระบบงาน (system disruption) ในช่วงเวลาทำการซื้อขายระหว่างวัน เป็นระยะเวลาถึงระดับที่ต้องรายงานสำนักงาน

เอกสารเปรียบเทียบรายละเอียดของหลักเกณฑ์เดิม และหลักเกณฑ์ที่แก้ไข

<table>
<tr><th>หัวข้อ</th><th>รายละเอียดเดิม</th><th>รายละเอียดการแก้ไข</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><th>ระบบงาน</th><th>ระยะเวลาหยุดชะงัก</th></tr>
<tr><td>● ระบบจับคู่คำสั่งซื้อขาย (trading system)</td><td>0 นาที</td></tr>
<tr><td>● ระบบจัดการคำสั่งซื้อขาย (order management system)</td><td>15 นาที</td></tr>
<tr><td>● ระบบอื่น ๆ เช่น หน้าเว็บไซต์หลัก ระบบฝากและถอนทรัพย์สิน เป็นต้น</td><td>60 นาที</td></tr>
</table>
</td></tr>
<tr><td></td><td>รายงานสำนักงานโดยไม่ชักช้าเมื่อทราบเหตุการณ์</td><td>● รายงานสำนักงานโดยไม่ชักช้าภายใน 3 ชั่วโมงนับแต่ทราบเหตุการณ์
● ในกรณีหน่วยงานโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศ (Critical Information Infrastructure หรือ CII) ให้รายงานโดยไม่ชักช้าภายใน 1 ชั่วโมงนับแต่ทราบเหตุการณ์
● โดยมีเนื้อหาครอบคลุมถึงวันเวลา ประเภทเหตุการณ์ เหตุการณ์ และผลกระทบที่คาดว่าจะเกิดขึ้น ทั้งนี้ อาจแจ้งโดยวาจาหรือรายงานผ่านช่องทางอิเล็กทรอนิกส์ตามที่สำนักงานกำหนดตามความเหมาะสม</td></tr>
<tr><td></td><td>รายงานภายในวันทำการถัดไปหลังทราบเหตุการณ์เป็นลายลักษณ์อักษร</td><td>● รายงานความคืบหน้าเป็นลายลักษณ์อักษรเมื่อมีความคืบหน้า อย่างน้อยทุกวันทำการภายในเวลา 15:00 น. เริ่มจากวันทำการถัดไปหลังทราบเหตุการณ์ หรือตามที่สำนักงานร้องขอ จนกว่าระบบสารสนเทศจะกลับสู่การให้บริการได้อย่างเป็นปกติ โดยมีเนื้อหาครอบคลุมถึงวันเวลา ประเภทเหตุการณ์ เหตุการณ์ ผลกระทบที่เกิดขึ้น และความคืบหน้าในการแก้ไขปัญหา ทั้งนี้ ให้รายงานผ่านช่องทางอิเล็กทรอนิกส์ที่สำนักงานกำหนด
● ในกรณีหน่วยงานโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศ (Critical Information Infrastructure หรือ CII) ให้รายงานความคืบหน้าเป็นลายลักษณ์อักษรครั้งแรกภายใน 2 ชั่วโมงหลังจากตรวจพบเหตุการณ์ และรายงานครั้งต่อไปเมื่อมีความคืบหน้า อย่างน้อยทุกวันทำการ เริ่มจากวันทำการถัดไปหลังทราบเหตุการณ์</td></tr>
</table>

เอกสารเปรียบเทียบรายละเอียดของหลักเกณฑ์เดิม และหลักเกณฑ์ที่แก้ไข

หัวข้อ	รายละเอียดเดิม	รายละเอียดการแก้ไข
		หรือตามที่สำนักงานร้องขอ จนกว่าระบบสารสนเทศจะกลับสู่การให้บริการได้อย่างเป็นปกติ ● รายงานเมื่อเหตุการณ์ยุติหรือแก้ไขปัญหาแล้วเสร็จ โดยมีเนื้อหาครอบคลุมถึงวัน เวลา ประเภทเหตุการณ์ เหตุการณ์ ผลกระทบที่เกิดขึ้น การดำเนินการแก้ไขปัญหา ผลการแก้ไขปัญหา ระยะเวลาในการแก้ไข สาเหตุที่เกิดปัญหา และแนวทางป้องกันในอนาคต ทั้งนี้ ให้รายงานผ่านช่องทางอิเล็กทรอนิกส์ที่สำนักงานกำหนด
	- เดิมไม่ได้กำหนด -	ผู้ประกอบการควรจัดให้มีช่องทางรับแจ้งเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศจากพนักงาน ผู้ใช้บริการ และผู้ที่เกี่ยวข้อง เช่น อีเมล โทรศัพท์ แบบฟอร์มติดต่อทางเว็บไซต์ และสื่อสังคมออนไลน์
	- เดิมไม่ได้กำหนด -	ในกรณีเหตุการณ์ที่เกิดจากภัยคุกคามไซเบอร์ ควรจัดให้มีกระบวนการวิเคราะห์ข้อมูล (analysis) จำกัดความเสียหาย (containment) จัดเก็บหลักฐานอย่างปลอดภัย (evidence gathering) แก้ไขปัญหาและฟื้นฟูระบบ (eradication and recovery)
	- เดิมไม่ได้กำหนด -	กรณีเหตุการณ์ที่เกิดขึ้นเป็นภัยคุกคามไซเบอร์ซึ่งส่งผลกระทบอย่างมีนัยสำคัญต่อทรัพย์สิน และข้อมูลของลูกค้า รวมถึงการรักษา ผู้ประกอบธุรกิจควรจัดให้มีกระบวนการตรวจพิสูจน์พยานหลักฐานทางดิจิทัล (digital forensic) โดยผู้ที่มีความเชี่ยวชาญเพื่อให้ทราบสาเหตุหรือช่องโหว่ของระบบ และสามารถดำเนินการปิดช่องโหว่ได้อย่างปลอดภัย
การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT contingency plan)	กำหนดขั้นตอน กระบวนการดำเนินการ และการควบคุมเกี่ยวกับความมั่นคงปลอดภัยของระบบสารสนเทศให้สอดคล้องกับแผนบริหารความต่อเนื่องทางธุรกิจ	ผู้ประกอบธุรกิจควรจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศที่สอดคล้องกับแผนการบริหารความต่อเนื่องทางธุรกิจ (business continuity plan: BCP) อย่างเป็นลายลักษณ์อักษร และได้รับการทบทวนอย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ
	- เดิมไม่ได้กำหนด -	ผู้ประกอบธุรกิจควรจัดให้มีคณะทำงานหรือหน่วยงานที่รับผิดชอบในการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ โดยมีผู้บริหารและบุคลากรของหน่วยงานด้านต่าง ๆ ที่เกี่ยวข้องเข้าร่วมด้วย เช่น ด้านเทคโนโลยีสารสนเทศ ด้านธุรกิจ และด้านสื่อสารองค์กร เป็นต้น
	กำหนดระยะเวลาในการกลับคืนสู่สภาพการดำเนินงานปกติของระบบสารสนเทศและจัดลำดับการกู้คืนระบบงาน	กระบวนการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ ควรครอบคลุมการดำเนินการเพิ่มเติมจากเกณฑ์เดิม ดังต่อไปนี้

เอกสารเปรียบเทียบรายละเอียดของหลักเกณฑ์เดิม และหลักเกณฑ์ที่แก้ไข

หัวข้อ	รายละเอียดเดิม	รายละเอียดการแก้ไข
	สารสนเทศที่มีความสำคัญให้สอดคล้องกับผลกระทบที่อาจเกิดขึ้น	(1) การประเมินความเสี่ยง (risk analysis) เพื่อให้สามารถระบุเหตุการณ์ความเสี่ยงซึ่งส่งผลกระทบต่อการหยุดชะงักของกระบวนการและระบบเทคโนโลยีสารสนเทศ โดยมีแนวทางดำเนินการอย่างเหมาะสมเพียงพอดังนี้ (ก) ระบุเหตุการณ์ความเสี่ยง (risk scenarios) ที่อาจทำให้กระบวนการและระบบเทคโนโลยีสารสนเทศหยุดชะงักทั้งจากภายในและภายนอก เช่น การโจมตีด้านไซเบอร์ เป็นต้น (ข) ประเมินความเสี่ยงโดยพิจารณาการควบคุมที่มีอยู่ รวมถึงผลกระทบและโอกาสที่จะเกิดขึ้นพร้อมทั้งกำหนดกระบวนการและทรัพยากรที่จะใช้ในการควบคุมความเสี่ยง (ค) จัดทำแผนในการจัดการความเสี่ยง เพื่อปรับปรุงกระบวนการและจัดเตรียมทรัพยากรที่จำเป็นในการควบคุมความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ (2) วิเคราะห์ผลกระทบทางธุรกิจ (business impact analysis) จากการหยุดชะงักของกระบวนการทางธุรกิจ (business process) เพื่อกำหนดระยะเวลาเป้าหมายในการกู้คืนระบบสารสนเทศ (RTO) ระยะเวลาเป้าหมายสูงสุดที่ยอมให้ข้อมูลเสียหาย (RPO) และระยะเวลาสูงสุดที่ยอมให้กระบวนการทางธุรกิจหยุดชะงัก (MTD) อย่างเหมาะสม
	- เดิมไม่ได้กำหนด -	กำหนด RTO ของระบบเทคโนโลยีสารสนเทศ ดังนี้ (1) RTO ไม่เกิน 2 ชั่วโมง สำหรับระบบเทคโนโลยีสารสนเทศที่สนับสนุนกระบวนการทางธุรกิจที่สำคัญของศูนย์ซื้อขายสัญญาซื้อขายล่วงหน้า สำนักหักบัญชีสัญญาซื้อขายล่วงหน้า สำนักหักบัญชีหลักทรัพย์ และศูนย์รับฝากหลักทรัพย์ (2) RTO ไม่เกิน 4 ชั่วโมง สำหรับระบบเทคโนโลยีสารสนเทศที่สนับสนุนกระบวนการทางธุรกิจที่สำคัญของผู้ประกอบธุรกิจอื่น ๆ (3) กรณีที่ผู้ประกอบธุรกิจไม่สามารถกำหนด RTO ของระบบเทคโนโลยีสารสนเทศได้ตามที่กำหนดข้างต้น ผู้ประกอบธุรกิจสามารถใช้วิธีการให้บริการแบบ Manual

เอกสารเปรียบเทียบรายละเอียดของหลักเกณฑ์เดิม และหลักเกณฑ์ที่แก้ไข

หัวข้อ	รายละเอียดเดิม	รายละเอียดการแก้ไข
		ทดแทนได้ โดยวิธีการดังกล่าวต้องไม่ส่งผลต่อประสิทธิภาพการให้บริการอย่างมีนัยสำคัญ
	- เดิมไม่ได้กำหนด -	สื่อสารแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ ให้พนักงานทุกคนที่มีส่วนเกี่ยวข้องกับการดำเนินการตามแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศมีความเข้าใจ และสามารถปฏิบัติตามแผนได้
	- เดิมไม่ได้กำหนด -	ผู้ประกอบธุรกิจควรกำหนดกระบวนการดำเนินงาน เพื่อรับมือเหตุการณ์การใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศหรือการใช้ประสิทธิภาพของระบบงานเกินขีดจำกัดของตัวชี้วัดที่กำหนดไว้ เช่น การจำกัดการให้บริการบางช่องทาง หรือตัดการเชื่อมต่อกับผู้ให้บริการหรือบุคคลภายนอกที่มีผลกระทบต่อระบบ
		ผู้ประกอบธุรกิจควรประเมินเหตุการณ์ที่ใช้ในการทดสอบ (test scenario) ประจำปีซึ่งครอบคลุมเหตุการณ์ที่มีโอกาสที่จะเกิดขึ้น เช่น การหยุดชะงักของระบบเทคโนโลยีสารสนเทศภายในบริษัท การหยุดชะงักของผู้ให้บริการภายนอกที่สำคัญ รวมถึงผู้ให้บริการคลาวด์ และการโจมตีทางไซเบอร์ เป็นต้น
	- เดิมไม่ได้กำหนด -	ทบทวน และทดสอบการปฏิบัติตามแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เพื่อให้แน่ใจว่าแผนยังคงมีประสิทธิภาพเมื่อต้องรับมือกับเหตุการณ์ผิดปกติ และทำการรายงานผลการทดสอบแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศต่อคณะกรรมการของผู้ประกอบธุรกิจหรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบธุรกิจ
การตรวจสอบด้านเทคโนโลยีสารสนเทศ (Information Technology Audit)	- เดิมไม่ได้กำหนด -	จัดให้มีการตรวจสอบด้านเทคโนโลยีสารสนเทศ โดยมีข้อกำหนดดังต่อไปนี้ (1) ผู้ตรวจสอบมีความเป็นอิสระ โดยอาจเป็นผู้ตรวจสอบภายในหรือภายนอกที่มีความเป็นอิสระจากจาก (ก) ผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (First line of defense) และ (ข) ผู้บริหารความเสี่ยงและกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ (Second line of defense) (2) ผู้ตรวจสอบหรือผู้ควบคุมการตรวจสอบต้องผ่านการรับรองหรือมีวุฒิบัตร Certified Information System Auditor (CISA), Certified Information Security Manager (CISM), Certified Information Security Professional (CISSP),

เอกสารเปรียบเทียบรายละเอียดของหลักเกณฑ์เดิม และหลักเกณฑ์ที่แก้ไข

หัวข้อ	รายละเอียดเดิม	รายละเอียดการแก้ไข
		ISO/IEC 27001 Lead Auditor หรือใบรับรองอื่น ๆ ตามที่สำนักงานประกาศกำหนด (3) วางแผนงานและกำหนดขอบเขตการตรวจสอบให้สอดคล้องกับความเสี่ยงด้านเทคโนโลยีสารสนเทศและข้อกำหนดของสำนักงาน โดยทบทวนแผนงานและขอบเขตของการตรวจสอบอย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ (4) จัดให้มีการตรวจสอบตามแผนงานและขอบเขตที่กำหนดไว้อย่างน้อยปีละ 1 ครั้ง โดยมีขอบเขตของการตรวจสอบ ดังนี้ (ก) ผู้ประกอบธุรกิจขนาดเล็ก ควรมีการตรวจสอบตามการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีขั้นต้นที่จำเป็น (cyber hygiene) ให้ครบถ้วนทุกหัวข้อการควบคุมอย่างน้อย 1 ครั้งในทุก 2 ปี (ข) ผู้ประกอบธุรกิจที่มีความเสี่ยงภาพรวมต่ำ ควรจัดให้มีการตรวจสอบด้านเทคโนโลยีสารสนเทศ อย่างน้อยปีละ 1 ครั้ง โดยเป็นการตรวจสอบแบบเต็มรูปแบบที่ครอบคลุมหลักเกณฑ์ครบถ้วนทุกหัวข้อการควบคุม (Full Scope) อย่างน้อย 1 ครั้งในทุก 2 ปี (ค) ผู้ประกอบธุรกิจที่มีความเสี่ยงภาพรวมปานกลางหรือสูง ควรจัดให้มีการตรวจสอบด้านเทคโนโลยีสารสนเทศ อย่างน้อยปีละ 1 ครั้ง โดยเป็นการตรวจสอบแบบเต็มรูปแบบที่ครอบคลุมหลักเกณฑ์ครบถ้วนทุกหัวข้อการควบคุม (Full Scope) อย่างน้อย 1 ครั้งในทุกปี (5) จัดให้มีแผนการแก้ไขปรับปรุงประเด็นจากการตรวจสอบ และการติดตามความคืบหน้าในการดำเนินการแก้ไขอย่างเหมาะสม (6) จัดทำรายงานผลการตรวจสอบ พร้อมทั้งรายงานข้อบกพร่องที่ตรวจพบ และแผนการปรับปรุงแก้ไขต่อคณะกรรมการของผู้ประกอบธุรกิจหรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบธุรกิจ ตลอดจนจัดเก็บรายงานผลการตรวจสอบเป็นระยะเวลาไม่น้อยกว่า 3 ปีนับแต่วันที่จัดทำเอกสารนั้น

เอกสารเปรียบเทียบรายละเอียดของหลักเกณฑ์เดิม และหลักเกณฑ์ที่แก้ไข

หัวข้อ	รายละเอียดเดิม	รายละเอียดการแก้ไข
		โดยต้องเก็บรักษาไว้ในลักษณะที่พร้อมให้สำนักงานสามารถเรียกดูและตรวจสอบได้โดยไม่ชักช้า (7) รายงานผลการตรวจสอบต่อสำนักงานในรูปแบบและวิธีการที่กำหนดภายใน 30 วันนับจากวันที่ได้รับผลการทดสอบอย่างเป็นทางการ แต่ไม่เกิน 90 วันนับจากวันที่สิ้นสุดกระบวนการทดสอบและไม่เกินสองเดือนนับแต่วันสิ้นปีปฏิทิน