เอกสารรับฟังความคิดเห็น

เลขที่ อตท. 40/2564

เรื่อง หลักการการแก้ไขหลักเกณฑ์การจัดให้มีระบบเทคโนโลยีสารสนเทศ

เผยแพร่เมื่อวันที่ 25 พฤศจิกายน 2564

สำนักงานได้จัดทำเอกสารฉบับนี้ขึ้นเพื่อสำรวจความคิดเห็นจากผู้เกี่ยวข้อง
ท่านสามารถ download เอกสารเผยแพร่ฉบับนี้ได้จาก www.sec.or.th

ท่านสามารถส่งความเห็นหรือข้อเสนอแนะให้สำนักงานได้
ตามที่ติดต่อด้านล่าง หรือ e-mail: cyberteam@sec.or.th nakharin@sec.or.th
thanakornb@sec.or.th หรือ chat@sec.or.th
วันสุดท้ายของการแสดงความคิดเห็น วันที่ 25 ธันวาคม 2564

ท่านสามารถติดต่อสอบถามข้อมูลเพิ่มเติมได้จากเจ้าหน้าที่ของสำนักงาน ดังนี้

1. นายนครินทร์ ลิ้มรังษี	โทรศัพท์ 0-2033-4660
2. นายธนากร บำรุงกิจเจริญ	โทรศัพท์ 0-2033-9765
3. นายฉัตร ทองสง	โทรศัพท์ 0-2263-6414

สำนักงานขอขอบคุณทุกท่านที่เข้าร่วมแสดงความคิดเห็น
และให้ข้อเสนอแนะมา ณ โอกาสนี้

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์
เลขที่ 333/3 ถนนวิภาวดีรังสิต แขวงจอมพล เขตจตุจักร กรุงเทพฯ 10900
โทรศัพท์ 1207 หรือ 0-2033-9999 โทรสาร: 0-2033-9660 email: info@sec.or.th

1. ที่มา

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน) ได้กำหนดหลักเกณฑ์การจัดให้มีระบบเทคโนโลยีสารสนเทศ (“หลักเกณฑ์ฯ”) ของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสัญญาซื้อขายล่วงหน้า (ประกาศสำนักงานคณะกรรมการ ก.ล.ต. ที่ สธ. 37/2559 เรื่อง ข้อกำหนดในรายละเอียดเกี่ยวกับการจัดให้มีระบบเทคโนโลยีสารสนเทศ ลงวันที่ 12 กันยายน พ.ศ. 2559) เพื่อให้ผู้ประกอบธุรกิจจัดให้มีนโยบายและมาตรการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศที่ดี รวมถึงมีการติดตาม ตรวจสอบ และทบทวนการปฏิบัติตามนโยบายและมาตรการดังกล่าวอย่างต่อเนื่องโดยมีเป้าหมายเพื่อให้ผู้ประกอบธุรกิจมีการกำกับดูแลความเสี่ยงในการนำเทคโนโลยีมาใช้ในการประกอบธุรกิจอย่างเหมาะสม

เพื่อให้ผู้ประกอบธุรกิจในตลาดทุนมีระบบเทคโนโลยีสารสนเทศที่มีความมั่นคงปลอดภัย หลักเกณฑ์ฯ ข้างต้น จึงได้ถูกอนุโลมใช้กับผู้ประกอบธุรกิจอื่น ๆ ได้แก่ ศูนย์ซื้อขายสัญญาซื้อขายล่วงหน้า สำนักหักบัญชีสัญญาซื้อขายล่วงหน้า สำนักหักบัญชีหลักทรัพย์ ศูนย์รับฝากหลักทรัพย์ ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล ผู้ให้บริการระบบเสนอขายโทเคนดิจิทัล ผู้ให้บริการระบบคราวด์ฟันดิง ผู้ให้บริการระบบสนับสนุนงานที่เกี่ยวข้องกับการซื้อขายหน่วยลงทุนและการจัดการกองทุน และผู้ให้บริการการจัดการข้อมูลการชำระเงินในการซื้อขายหลักทรัพย์

สำนักงานเห็นควรทบทวนและปรับปรุงหลักเกณฑ์ฯ ที่ใช้บังคับมาตั้งแต่ปี 2559 ให้มีความเหมาะสมสอดรับกับ (1) การใช้เทคโนโลยีในการประกอบธุรกิจที่มีการเปลี่ยนแปลงไป (2) ภัยคุกคามทางไซเบอร์ที่มีพัฒนาการด้านเทคนิคและวิธีการ ตลอดจนกลุ่มเป้าหมายในการโจมตีที่กว้างขึ้น (3) การป้องกันเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ ที่เกิดขึ้นในตลาดทุนในอดีต และ (4) การปรับปรุงเกณฑ์ด้านเทคโนโลยีสารสนเทศของหน่วยงานกำกับดูแลในภาคอุตสาหกรรมการเงินอื่น ๆ ทั้งนี้ เพื่อให้บรรลุเป้าหมายของสำนักงานในการสร้าง Cyber Resilience และเพื่อให้ผู้ประกอบธุรกิจมีระบบงานด้านเทคโนโลยีสารสนเทศที่มีประสิทธิภาพและมีความพร้อมรับมือต่อภัยคุกคามทางไซเบอร์ได้ ขณะเดียวกัน ผู้ประกอบธุรกิจสามารถปฏิบัติตามเกณฑ์ได้อย่างมีประสิทธิภาพและไม่ก่อให้เกิดภาระเกินสมควร

2. เป้าหมายที่ต้องการบรรลุ (Intended Outcome)

เพื่อให้ผู้ประกอบธุรกิจสามารถบริหารจัดการความเสี่ยงในการใช้เทคโนโลยีสารสนเทศได้อย่างมีประสิทธิผล และมีความพร้อมรับมือต่อภัยคุกคามทางไซเบอร์ที่เพิ่มขึ้นอย่างต่อเนื่อง พร้อมทั้งสร้างความเชื่อมั่นของผู้ลงทุนในการใช้บริการและผลิตภัณฑ์ของภาคตลาดทุน ซึ่งมีระบบเทคโนโลยีสารสนเทศเป็นส่วนสำคัญ

3. แนวทางการปรับปรุงหลักเกณฑ์

3.1 ขอบเขตการใช้บังคับ

ขอบเขตของการใช้บังคับหลักเกณฑ์ครอบคลุมผู้ประกอบธุรกิจดังต่อไปนี้

(1) ผู้ประกอบธุรกิจที่ได้รับใบอนุญาตประกอบธุรกิจหลักทรัพย์หรือธุรกิจสัญญาซื้อขายล่วงหน้าประเภทดังต่อไปนี้

- การเป็นนายหน้าซื้อขายหลักทรัพย์ การค้าหลักทรัพย์ หรือการจัดจำหน่ายหลักทรัพย์
- การเป็นที่ปรึกษาการลงทุนที่มีการวางแผนการลงทุนให้แก่ลูกค้า หรือใช้โปรแกรมสำเร็จรูปเพื่อประกอบการให้บริการแก่ลูกค้า
- การจัดการกองทุนรวม แต่ไม่รวมถึงการจัดการกองทุนรวมเพื่อผู้ลงทุน ซึ่งเป็นคนต่างด้าว
- การจัดการกองทุนส่วนบุคคล
- กิจการการยืมและให้ยืมหลักทรัพย์
- การให้สินเชื่อเพื่อธุรกิจหลักทรัพย์
- การเป็นตัวแทนซื้อขายสัญญาซื้อขายล่วงหน้า
- การเป็นที่ปรึกษาสัญญาซื้อขายล่วงหน้าที่มีการวางแผนการลงทุนให้แก่ลูกค้า หรือใช้โปรแกรมสำเร็จรูปประกอบการให้บริการแก่ลูกค้า
- การเป็นผู้จัดการเงินทุนสัญญาซื้อขายล่วงหน้า

(2) ศูนย์ซื้อขายสัญญาซื้อขายล่วงหน้า

(3) สำนักหักบัญชีสัญญาซื้อขายล่วงหน้า

(4) สำนักหักบัญชีหลักทรัพย์

(5) ศูนย์รับฝากหลักทรัพย์

(6) ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

(7) ผู้ให้บริการระบบเสนอขายโทเคนดิจิทัล

(8) ผู้ให้บริการระบบคราวด์ฟันดิง

(9) ผู้ให้บริการระบบสนับสนุนงานที่เกี่ยวข้องกับการซื้อขายหน่วยลงทุน และการจัดการกองทุน

(10) ผู้ให้บริการการจัดการข้อมูลการชำระเงินในการซื้อขายหลักทรัพย์

3.2 โครงสร้างของหลักเกณฑ์

เพื่อปรับปรุงเนื้อหาของหลักเกณฑ์ให้เป็นปัจจุบัน สอดคล้องกับมาตรฐานสากล และครอบคลุมความเสี่ยงด้านเทคโนโลยีสารสนเทศในเรื่องต่าง ๆ โครงสร้างของหลักเกณฑ์จึงแบ่งออกเป็น 3 หมวด ดังนี้

หมวดที่ 1 การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

- บทบาทหน้าที่และความรับผิดชอบของคณะกรรมการของผู้ประกอบธุรกิจ
- โครงสร้างการกำกับดูแล
- นโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ

หมวดที่ 2 การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security)

- โครงสร้างการบริหารงานเพื่อการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Organization of Information Security)
- การบริหารจัดการบุคลากร (Human Resource Security)
- การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT Asset Management)
- การรักษาความมั่นคงปลอดภัยของข้อมูล (Data Security)
- การควบคุมการเข้าถึง (Access Control)
- การบริหารจัดการการเข้ารหัสข้อมูล (Cryptography)
- การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environmental Security)
- การรักษาความมั่งคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT Operations Security)
- การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายคอมพิวเตอร์ (Communications Security)

- การบริหารจัดการโครงการด้านเทคโนโลยีสารสนเทศ และการจัดหา พัฒนาและบำรุงรักษาระบบระบบสารสนเทศ (IT Project Management, and System Acquisition, Development and Maintenance)
- การบริหารจัดการบุคคลภายนอก (Third Party Management)
- การบริหารจัดการเหตุการณ์ผิดปกติและปัญหาด้านเทคโนโลยีสารสนเทศ (IT Incident Management)
- การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan)

หมวดที่ 3 การตรวจสอบด้านเทคโนโลยีสารสนเทศ

- การจัดให้มีการตรวจสอบด้านเทคโนโลยีสารสนเทศตามหลักเกณฑ์

3.3 บทนิยาม

หลักเกณฑ์ปัจจุบัน	หลักเกณฑ์ที่เสนอปรับปรุง
“ทรัพย์สินสารสนเทศ” หมายถึง (1) ทรัพย์สินสารสนเทศประเภทระบบ ได้แก่ ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ (2) ทรัพย์สินสารสนเทศประเภทอุปกรณ์ ได้แก่ ตัวเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล และอุปกรณ์อื่นใด (3) ทรัพย์สินสารสนเทศประเภทข้อมูล ได้แก่ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์	แก้ไขนิยาม “ทรัพย์สินด้านเทคโนโลยีสารสนเทศ” หมายถึง ฮาร์ดแวร์ ซอฟต์แวร์ และข้อมูล โดยรวมถึงสิทธิ์ในการใช้งานฮาร์ดแวร์ และซอฟต์แวร์
“ระบบสารสนเทศที่มีความสำคัญ” หมายถึง ระบบสารสนเทศที่รองรับการปฏิบัติงานที่สำคัญ เช่น ระบบ	แก้ไขนิยาม “ระบบสารสนเทศที่มีความสำคัญ” (Critical System) หมายถึง ระบบคอมพิวเตอร์ หรือระบบเครือข่ายสำคัญ

หลักเกณฑ์ปัจจุบัน	หลักเกณฑ์ที่เสนอปรับปรุง
ซื้อขาย ระบบปฏิบัติการ Back Office และระบบจัดการลงทุน เป็นต้น	ที่หากมีการหยุดชะงักจะส่งผลกระทบอย่างมีนัยสำคัญต่อความต่อเนื่องในการดำเนินงานของผู้ประกอบธุรกิจ หรือส่งผลกระทบอย่างมีนัยสำคัญต่อลูกค้าที่ใช้บริการ นอกจากนี้ อาจส่งผลกระทบต่อชื่อเสียง ฐานะ และผลการดำเนินงานของผู้ประกอบธุรกิจอย่างมีนัยสำคัญ เช่น ระบบซื้อขาย ระบบสนับสนุนการปฏิบัติการ (Back Office system) ระบบจัดเก็บและบริหารจัดการข้อมูลลูกค้าและนักลงทุน ระบบจัดการลงทุน และระบบจัดเก็บสินทรัพย์ดิจิทัล เป็นต้น
- เดิมไม่ได้กำหนด -	เพิ่มนิยาม (1) “บุคคลภายนอก” (Third Party) หมายถึง บุคคลหรือนิติบุคคลภายนอก ซึ่งได้แก่ ● ผู้รับดำเนินการด้านระบบสารสนเทศ (IT Outsource) หรือ ● ผู้ให้บริการ หรือผู้เสนอขายหรือติดตั้งผลิตภัณฑ์ด้านเทคโนโลยีสารสนเทศ ที่สามารถเข้าถึงหรือปรับปรุงข้อมูลหรือระบบงานแก่ผู้ประกอบธุรกิจ หรือ ● ผู้ให้บริการ Cloud Computing (Cloud Service Provider) หรือ ● ผู้ที่มีการเชื่อมต่อกับระบบสารสนเทศของผู้ประกอบธุรกิจ หรือ ● ผู้ที่สามารถเข้าถึงหรือมีการแลกเปลี่ยนข้อมูลสำคัญของผู้ประกอบธุรกิจหรือข้อมูลของลูกค้าที่อยู่ภายใต้การควบคุมดูแลโดยผู้ประกอบธุรกิจได้ ทั้งนี้ บุคคลภายนอกไม่ครอบคลุมถึงลูกค้าที่ใช้ผลิตภัณฑ์และบริการของผู้ประกอบธุรกิจ

หลักเกณฑ์ปัจจุบัน	หลักเกณฑ์ที่เสนอปรับปรุง
	(2) “เทคโนโลยีสารสนเทศ” (Information Technology - IT) หมายถึง เทคโนโลยีสารสนเทศที่นำมาใช้ในการดำเนินธุรกิจ ซึ่งครอบคลุมถึง ข้อมูล ระบบปฏิบัติการ (Operating System) ระบบงาน (Application System) ระบบฐานข้อมูล (Database System) อุปกรณ์คอมพิวเตอร์ (Hardware) และระบบเครือข่ายคอมพิวเตอร์ (Communication) เป็นต้น (3) “ความเสี่ยงด้านเทคโนโลยีสารสนเทศ” (IT Risk) หมายถึง ความเสี่ยงที่อาจเกิดขึ้นจากการใช้เทคโนโลยีสารสนเทศในการดำเนินธุรกิจ ซึ่งมีผลกระทบต่อระบบหรือการปฏิบัติงานของผู้ประกอบธุรกิจ ความปลอดภัยหรือความเป็นส่วนตัวของข้อมูลลูกค้า หรือตลาดทุน ซึ่งรวมถึงความเสี่ยงที่เกิดจากภัยคุกคามทางไซเบอร์ (Cyber Threat) (4) “ความมั่นคงปลอดภัยด้านสารสนเทศ” (Information Security) หมายถึง การรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (non-Repudiation) ความน่าเชื่อถือ (Reliability) และการรักษาความเป็นส่วนตัวของข้อมูลสารสนเทศและบุคคล (Privacy) (5) "เหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ” (IT Incident) หมายถึง เหตุการณ์ด้านเทคโนโลยีสารสนเทศที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ (1)

หลักเกณฑ์ปัจจุบัน	หลักเกณฑ์ที่เสนอปรับปรุง
	ระบบของผู้ประกอบธุรกิจถูกบุกรุกหรือโจมตี หรือ (2) ความมั่นคงปลอดภัยด้านสารสนเทศถูกคุกคาม หรือ (3) ระบบไม่สามารถให้บริการได้ หรือ (4) ข้อมูลส่วนบุคคลถูกละเมิด (6) “การใช้งานอุปกรณ์ส่วนตัว” (Bring Your Own Device: BYOD) หมายถึง การใช้งานอุปกรณ์ส่วนตัวของบุคลากรของผู้ประกอบธุรกิจเพื่อเข้าถึงระบบงานสารสนเทศ รวมถึงการเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ และตารางการประชุม เช่น ในรูปแบบโปรแกรม Application และเว็บบราวเซอร์ เป็นต้น (7) “สิ่งที่ใช้ยืนยันตัวตน” (Authenticator) หมายถึง สิ่งที่ผู้ใช้งานครอบครองเพื่อใช้ในการยืนยันตัวตนเพื่อเข้าถึงข้อมูลหรือระบบสารสนเทศ เช่น รหัสผ่าน ลายนิ้วมือ และ SMS OTP เป็นต้น (8) “โครงการด้านเทคโนโลยีสารสนเทศ” (IT Project Management) หมายถึง การจัดหา พัฒนา หรือแก้ไขเปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศที่มีนัยสำคัญต่อการให้บริการ การดำเนินธุรกิจ หรือการบริหารโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ (Infrastructure) (9) “เครื่องมือชำระเงิน” หมายถึง เครื่องมือที่ใช้สำหรับให้บริการลูกค้าในทางการเงินและการลงทุน เช่น บริการซื้อขายหลักทรัพย์ บริการด้านการชำระราคา และบริการฝากและถอนทรัพย์สิน เป็นต้น รวมถึงระบบสำหรับการระดมทุนในตลาดทุนในรูปแบบต่าง ๆ เช่น การออกเป็นหลักทรัพย์ (Securities Token Offering: STO) หรือออกเป็นโทเคนดิจิทัล (Initial Coin Offering: ICO) และการระดมทุนแบบคราวด์ฟันดิง เป็นต้น

3.4 การกำหนดมาตรการควบคุมตามระดับความเสี่ยงในการดำเนินธุรกิจ

หลักเกณฑ์ปัจจุบัน	หลักเกณฑ์ที่เสนอปรับปรุง
ในกรณีที่ผู้ประกอบธุรกิจหลักทรัพย์หรือธุรกิจสัญญาซื้อขายล่วงหน้าเป็นธนาคารพาณิชย์ตามกฎหมายว่าด้วยธุรกิจสถาบันการเงิน บริษัทประกันชีวิตตามกฎหมายว่าด้วยการประกันชีวิต หรือสถาบันการเงินที่จัดตั้งขึ้นตามกฎหมายอื่น ให้ปฏิบัติตามประกาศนี้เฉพาะข้อ 11 และข้อ 23(4)	ยกเลิกข้อกำหนดเฉพาะสำหรับผู้ประกอบธุรกิจ ซึ่งเป็นธนาคารพาณิชย์ตามกฎหมายว่าด้วยธุรกิจสถาบันการเงิน บริษัทประกันชีวิตตามกฎหมายว่าด้วยการประกันชีวิต หรือสถาบันการเงินที่จัดตั้งขึ้นตามกฎหมายอื่น ผู้ประกอบธุรกิจทุกรายตามข้อ 3.1 ต้องกำกับดูแล และบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk) อย่างมีประสิทธิผลและประสิทธิภาพเพียงพอ โดยคำนึงถึงการรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของเทคโนโลยีสารสนเทศให้เหมาะสมกับผลการประเมินระดับความเสี่ยงของผู้ประกอบธุรกิจ
- เดิมไม่ได้กำหนด -	ผู้ประกอบธุรกิจต้องจัดให้มีการประเมินความเสี่ยงตามเงื่อนไข (Criteria) ตามที่สำนักงานกำหนด และส่งผลการประเมินความเสี่ยงที่ได้รับความเห็นชอบจากผู้บริหารหรือคณะกรรมการที่มีอำนาจต่อสำนักงานภายในวันสิ้นปีปฏิทิน รวมทั้งกำกับดูแลและจัดให้มีการควบคุมความปลอดภัยของระบบเทคโนโลยีสารสนเทศที่เหมาะสมและมีประสิทธิภาพและประสิทธิผล สอดคล้องกับผลการประเมินความเสี่ยง
- เดิมไม่ได้กำหนด -	ผู้ประกอบธุรกิจต้องกำกับดูแลระบบเทคโนโลยีสารสนเทศตามระดับความเสี่ยงของผู้ประกอบธุรกิจ โดยแบ่งแนวปฏิบัติออกเป็น 2 ระดับ คือ (1) แนวปฏิบัติระดับพื้นฐาน สำหรับผู้ประกอบธุรกิจที่มีความเสี่ยงภาพรวมในระดับต่ำหรือปานกลาง และ (2) แนวปฏิบัติระดับสูง สำหรับผู้ประกอบธุรกิจที่มีความเสี่ยงภาพรวมในระดับสูง
- เดิมไม่ได้กำหนด -	กรณีผู้ประกอบธุรกิจขนาดเล็กที่ไม่มีการให้บริการระบบสารสนเทศในการรับส่งรายการธุรกรรมโดยตรง

หลักเกณฑ์ปัจจุบัน	หลักเกณฑ์ที่เสนอปรับปรุง
	จากนักลงทุนผ่านเครือข่ายอินเทอร์เน็ต และไม่มีการดำเนินการในลักษณะการดูแลทรัพย์สินของนักลงทุน หรือไม่มีการให้บริการหรือเก็บรักษาเครื่องมือชำระเงินหรือข้อมูลที่ใช้ในการชำระเงิน ให้ดำเนินการเฉพาะการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศขั้นต่ำที่จำเป็น (Cyber Hygiene) ได้แก่ (1) การบริหารบัญชีผู้ใช้งานสิทธิสูง (Privileged User Management) (2) การบริหารจัดการมาตรฐานการตั้งค่าระบบ (System Configuration Management) (3) การรักษาความมั่นคงปลอดภัยของเครื่องแม่ข่าย (Server) และอุปกรณ์ที่ใช้ปฏิบัติงาน (Endpoint) (4) การประเมินช่องโหว่ทางเทคนิค (Technical Vulnerability Assessment) (5) การทดสอบการเจาะระบบ (Penetration Test) (6) การบริหารจัดการโปรแกรมแก้ไขช่องโหว่ (Patch Management)

3.5 การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

3.5.1. บทบาทหน้าที่และความรับผิดชอบของคณะกรรมการของผู้ประกอบธุรกิจ

หลักเกณฑ์ปัจจุบัน	หลักเกณฑ์ที่เสนอปรับปรุง
- เดิมไม่ได้กำหนด -	เพิ่มเติมข้อกำหนดเรื่องบทบาทหน้าที่ของคณะกรรมการของผู้ประกอบธุรกิจ ซึ่งครอบคลุมเรื่องดังต่อไปนี้ (1) จัดให้มีกรอบการกำกับดูแลด้านเทคโนโลยีสารสนเทศ และกำกับดูแลแผนงานด้านเทคโนโลยีสารสนเทศให้สอดคล้องกับแผนทางธุรกิจ

หลักเกณฑ์ปัจจุบัน	หลักเกณฑ์ที่เสนอปรับปรุง
	(2) กำกับดูแลให้มีการจัดสรรและบริหารจัดการทรัพยากรทางด้านเทคโนโลยีสารสนเทศและทรัพยากรบุคคลให้เพียงพอต่อการดำเนินธุรกิจ (3) กำกับดูแลให้มีการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management Policy) และการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security Policy) (4) กำกับดูแลให้มีการนำนโยบายด้านเทคโนโลยีสารสนเทศไปปฏิบัติอย่างมีประสิทธิผล (5) กำกับดูแลให้มีการสร้างความรู้และความตระหนักด้านความเสี่ยงด้านเทคโนโลยีสารสนเทศ (6) กำกับดูแลให้มีการติดตาม ตรวจสอบ และรายงานผลการปฏิบัติตามนโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศต่อคณะกรรมการอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

3.5.2. โครงสร้างการกำกับดูแล

หลักเกณฑ์ปัจจุบัน	หลักเกณฑ์ที่เสนอปรับปรุง
- เดิมไม่ได้กำหนด -	เพิ่มเติมข้อกำหนดในการจัดให้มีโครงสร้างการกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ สอดคล้องตามหลักการแบ่งแยกหน้าที่ความรับผิดชอบ 3 ระดับ (Three Lines of Defense: 3 LoDs)
- เดิมไม่ได้กำหนด -	[ปรับปรุงจาก Focus Group][1] เพิ่มเติมข้อกำหนดสำหรับผู้ประกอบธุรกิจที่มีความเสี่ยงสูง โดยจัดให้มี

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

หลักเกณฑ์ปัจจุบัน	หลักเกณฑ์ที่เสนอปรับปรุง
	กรรมการหรือที่ปรึกษาอย่างน้อย 1 ท่าน ที่มีความรู้หรือประสบการณ์ด้าน IT โดยพิจารณาจาก (1) จบการศึกษาในสาขาเทคโนโลยีสารสนเทศ หรือสาขาที่เกี่ยวข้อง หรือ (2) มีประสบการณ์ในตำแหน่งหัวหน้าหน่วยงาน หรือมีหน้าที่รับผิดชอบเป็นผู้บริหารงานหลัก หรือมีประสบการณ์ในด้านการให้คำปรึกษาที่เกี่ยวข้องด้านเทคโนโลยีสารสนเทศ หรือ (3) มีประสบการณ์หรือได้รับแต่งตั้งเป็นสมาชิกในคณะกรรมการหรือคณะทำงานที่เกี่ยวข้องด้านเทคโนโลยีสารสนเทศ ทั้งนี้ ผู้ประกอบธุรกิจอาจใช้เกณฑ์ด้านอื่นในการพิจารณาตามความเหมาะสม กรณีที่คณะกรรมการของผู้ประกอบธุรกิจแต่งตั้งคณะกรรมการชุดย่อย เพื่อทำหน้าที่ให้คำปรึกษาด้านเทคโนโลยีสารสนเทศแก่คณะกรรมการ ควรกำหนดบทบาทหน้าที่อย่างชัดเจนและเป็นลายลักษณ์อักษร
- เดิมไม่ได้กำหนด -	[ปรับปรุงจาก Focus Group] เพิ่มเติมข้อกำหนดสำหรับผู้ประกอบธุรกิจที่มีความเสี่ยงสูง โดยจัดให้มีผู้บริหารระดับสูง (Chief Information Security Officer: CISO) หรือหัวหน้าสายงานที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Head of Information Security) โดยมีคุณสมบัติ ขอบเขตอำนาจและบทบาทและหน้าที่อย่างน้อยดังนี้ (1) มีความเป็นอิสระจากหน่วยงานที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT operation) และงานด้านพัฒนาระบบเทคโนโลยีสารสนเทศ (IT development) (2) เป็นผู้ที่มีความรู้ความสามารถหรือมีประสบการณ์ด้านเทคโนโลยีสารสนเทศและด้านการบริหาร

หลักเกณฑ์ปัจจุบัน	หลักเกณฑ์ที่เสนอปรับปรุง
	จัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (3) มีอำนาจหน้าที่ (authority) เพียงพอในการปฏิบัติหน้าที่ได้อย่างมีประสิทธิภาพและประสิทธิผล โดยสามารถดำเนินการอย่างน้อย ดังนี้ ก. รายงานปัญหาหรือเหตุการณ์ที่มีนัยสำคัญต่อผู้บริหารในตำแหน่งสูงสุดขององค์กร และคณะกรรมการที่เกี่ยวข้องโดยตรง ข. ให้ความเห็นด้านภัยคุกคามทางไซเบอร์และการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศต่อคณะกรรมการของผู้ประกอบธุรกิจ หรือคณะกรรมการที่เกี่ยวข้องกับการบริหารจัดการและกำกับดูแลการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ และร่วมตัดสินใจดำเนินการในเรื่องความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและภัยคุกคามทางไซเบอร์ที่มีผลกระทบอย่างมีนัยสำคัญ

3.5.3. นโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ

หลักเกณฑ์ปัจจุบัน	หลักเกณฑ์ที่เสนอปรับปรุง
ผู้ประกอบธุรกิจต้องจัดให้มีนโยบายเรื่องการจัดสรรและบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศ ซึ่งครอบคลุมถึงการจัดสรรทรัพยากรให้เพียงพอต่อการดำเนินธุรกิจ และการกำหนดแนวทางเพื่อรองรับในกรณีที่ไม่สามารถจัดสรรทรัพยากรได้เพียงพอตามที่กำหนดไว้	ยกเลิกข้อกำหนดในการจัดให้มีนโยบายการจัดสรรและบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศ โดยกำหนดให้การจัดสรรและบริหารจัดการทรัพยากรเทคโนโลยีและทรัพยากรบุคคล เป็นส่วนหนึ่งในหน้าที่ความรับผิดชอบของคณะกรรมการของผู้ประกอบธุรกิจ

หลักเกณฑ์ปัจจุบัน	หลักเกณฑ์ที่เสนอปรับปรุง
รายงานการปฏิบัติตามนโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศ ให้คณะกรรมการของผู้ประกอบธุรกิจทราบควรที่มีเนื้อหาครอบคลุมถึงเรื่องดังต่อไปนี้ ตามรอบระยะเวลาที่เหมาะสม (1) กิจกรรมที่เกี่ยวข้องกับการปฏิบัติงานด้านการบริหารความเสี่ยง หรือการจัดสรรและบริหารทรัพยากรด้าน IT เช่น สรุปผลการบริหารจัดการด้านความเสี่ยง / การจัดสรรทรัพยากร IT ในรอบปี เป็นต้น (2) ความคืบหน้าของงานโครงการ (ถ้ามี) (3) การปฏิบัติตามกฎระเบียบ ข้อบังคับ หรือข้อตกลงที่จัดทำกับบุคคลภายนอกและภายในบริษัท (4) ความมีประสิทธิภาพของการนำเทคโนโลยีสารสนเทศมาใช้ (5) ประเด็นปัญหาและอุปสรรค	เพิ่มเติมเนื้อหาของการรายงาน ดังนี้ (1) ผลการประเมินและการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยหน่วยงานที่ทำหน้าที่บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศหรือหน่วยงานที่เกี่ยวข้อง (2) ผลการปฏิบัติตามกฎระเบียบ ข้อบังคับ หรือนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศในภาพรวมของบริษัท โดยหน่วยงานที่ทำหน้าที่กำกับดูแลการปฏิบัติงานด้านเทคโนโลยีสารสนเทศหรือหน่วยงานที่เกี่ยวข้อง (3) ผลการตรวจสอบด้านเทคโนโลยีสารสนเทศและความคืบหน้าในการดำเนินการแก้ไขข้อตรวจพบ โดยหน่วยงานที่ทำหน้าที่ตรวจสอบด้านเทคโนโลยีสารสนเทศหรือหน่วยงานที่เกี่ยวข้อง (4) ผลการปฏิบัติงานด้านเทคโนโลยีสารสนเทศที่สำคัญ
นโยบายการบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศควรสอดคล้องกับนโยบายและการบริหารความเสี่ยงองค์กร และควรมีเนื้อหาขั้นต่ำ ดังนี้ (1) การระบุความเสี่ยง (2) การประเมินความเสี่ยง (3) การกำหนดเครื่องมือและมาตรการในการบริหารและจัดการความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้	เพิ่มเติมรายละเอียดของเนื้อหานโยบายการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ดังนี้ (1) บทบาทหน้าที่ของผู้ที่เกี่ยวข้องในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (2) เกณฑ์ความเสี่ยง (Risk Criteria) โดยครอบคลุมถึงโอกาสหรือความถี่ที่จะเกิดเหตุการณ์ความเสี่ยง และความมีนัยสำคัญหรือระดับผลกระทบที่อาจจะเกิดขึ้น เพื่อจัดลำดับความสำคัญในการบริหารจัดการความเสี่ยง (3) ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite)

หลักเกณฑ์ปัจจุบัน	หลักเกณฑ์ที่เสนอปรับปรุง
(4) การกำหนดตัวชี้วัดระดับความเสี่ยง รวมถึงจัดให้มีการติดตามและรายงานผลตัวชี้วัดดังกล่าว (5) การกำหนดหน้าที่และความรับผิดชอบของผู้รับผิดชอบ และผู้ทำหน้าที่บริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ	(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

3.6 การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security)

3.6.1. โครงสร้างการบริหารงานเพื่อการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Organization of Information Security)

หลักเกณฑ์ปัจจุบัน	หลักเกณฑ์ที่เสนอปรับปรุง
ผู้ประกอบธุรกิจต้องจัดให้มีการกำหนดนโยบายการใช้งานระบบสารสนเทศร่วมกันบนระบบเครือข่ายคอมพิวเตอร์เพื่อการประมวลผลตามความต้องการของผู้ใช้งาน (Cloud Computing) ซึ่งครอบคลุมถึงวิธีการคัดเลือก และประเมินผู้ให้บริการ การทบทวนคุณสมบัติของผู้ให้บริการ ข้อกำหนดเกี่ยวกับการใช้บริการ และการตรวจสอบบันทึกหลักฐานต่าง ๆ ที่อาจส่งผลกระทบต่อการใช้บริการ	ยกเลิกข้อกำหนดเรื่องนโยบายและมาตรการการใช้งาน Cloud computing โดยใช้ข้อกำหนดและแนวปฏิบัติตามหัวข้อการบริหารจัดการบุคคลภายนอก (Third Party Management)

3.6.2. การบริหารจัดการบุคลากร (Human Resource Security)

หลักเกณฑ์ปัจจุบัน	หลักเกณฑ์ที่เสนอปรับปรุง
ผู้ประกอบธุรกิจต้องสร้างความตระหนักรู้เกี่ยวกับนโยบายและมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศให้แก่บุคลากรของผู้ประกอบธุรกิจและบุคคลภายนอก (Human Resource Security) ที่มีการปฏิบัติงานโดยมีการเข้าถึงข้อมูลหรือระบบงานภายในองค์กร และดำเนินการให้บุคลากรดังกล่าวสามารถปฏิบัติหน้าที่ได้ตามนโยบายและมาตรการที่กำหนด ทั้งนี้ตามหลักเกณฑ์ดังต่อไปนี้	เพิ่มเติมข้อกำหนด ดังนี้ (1) มีกระบวนการคัดเลือกบุคลากรในการปฏิบัติหน้าที่โดยคำนึงถึงความรู้ ความสามารถ และความเพียงพอในการปฏิบัติงาน มีการตรวจสอบข้อมูลของบุคลากรก่อนการว่าจ้างอย่างเพียงพอและสอดคล้องกับความเสี่ยงของตำแหน่งงานและหน้าที่ความรับผิดชอบ (2) กำหนดบทบาทหน้าที่และความรับผิดชอบเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการไม่เปิดเผยข้อมูล (Non-Disclosure Agreement) ในข้อตกลงการจ้างงาน (3) จัดให้มีเอกสารข้อกำหนดในการใช้งานทรัพย์สินด้านเทคโนโลยีสารสนเทศ (Acceptable Use

หลักเกณฑ์ปัจจุบัน	หลักเกณฑ์ที่เสนอปรับปรุง
(1) ให้ความรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศที่เกี่ยวข้องกับการปฏิบัติหน้าที่แก่บุคลากรของผู้ประกอบธุรกิจและบุคคลภายนอกที่ปฏิบัติงานดังกล่าว (2) สื่อสารให้บุคลากรของผู้ประกอบธุรกิจและบุคคลภายนอกที่ปฏิบัติงานดังกล่าว ระมัดระวังและงดเว้นการใช้งานระบบสารสนเทศในลักษณะที่อาจก่อให้เกิดความเสียหาย และต้องรายงานผู้มีหน้าที่รับผิดชอบในการบริหารจัดการเหตุการณ์ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศโดยไม่ชักช้า เมื่อพบความผิดปกติใด ๆ อย่างมีนัยสำคัญ (3) กำหนดมาตรการในการลงโทษบุคลากรที่มีพฤติกรรมฝ่าฝืนหรือไม่ปฏิบัติตามนโยบายหรือหลักเกณฑ์เกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ	Policy) โดยครอบคลุมขอบเขตความรับผิดชอบของผู้ใช้งาน รายการสิ่งที่ผู้ใช้งานต้องปฏิบัติ และห้ามปฏิบัติ (4) จัดอบรมและพัฒนาความรู้ด้านเทคโนโลยีสารสนเทศ (Training Program) ให้แก่บุคลากรของผู้ประกอบธุรกิจและบุคคลภายนอกที่สามารถเข้าถึงข้อมูลที่มีความสำคัญของผู้ประกอบธุรกิจอย่างสม่ำเสมอ โดยทบทวนแผนอบรมและพัฒนาความรู้ด้านเทคโนโลยีสารสนเทศอย่างน้อยปีละ 1 ครั้ง (5) กำหนดโปรแกรมในการเสริมสร้างความตระหนัก (awareness program) เรื่องการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ความเสี่ยงด้านเทคโนโลยีสารสนเทศและความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคล (privacy) จากการใช้งานเทคโนโลยีสารสนเทศให้แก่บุคลากร (6) จัดทำกระบวนการรองรับเมื่อมีการเปลี่ยนแปลงตำแหน่งงานหรือสิ้นสุดการจ้างงาน เช่น การคืนทรัพย์สินขององค์กร การปรับปรุงสิทธิให้เป็นปัจจุบันและยกเลิกสิทธิเมื่อสิ้นสุดการจ้างงาน เป็นต้น รวมทั้งมีการสื่อสารให้ผู้ที่เกี่ยวข้องรับทราบถึงการเปลี่ยนแปลงสิทธิ หน้าที่ และความรับผิดชอบ เป็นต้น

3.6.3. การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT Asset Management)

หลักเกณฑ์ปัจจุบัน	หลักเกณฑ์ที่เสนอปรับปรุง
ในการบริหารจัดการทรัพย์สินสารสนเทศที่เป็นทรัพย์สินสารสนเทศ	เพิ่มเติมข้อกำหนดของรายการข้อมูลขั้นต่ำที่ควรมีในทะเบียนทรัพย์สินสารสนเทศ ดังนี้

หลักเกณฑ์ปัจจุบัน	หลักเกณฑ์ที่เสนอปรับปรุง
ประเภทระบบหรืออุปกรณ์ ผู้ประกอบธุรกิจต้องมีการจัดทำและจัดเก็บทะเบียนทรัพย์สินดังกล่าว ตลอดจนทบทวนทะเบียนดังกล่าวอย่างน้อยปีละ 1 ครั้งหรือเมื่อมีการเปลี่ยนแปลงทรัพย์สินสารสนเทศอย่างมีนัยสำคัญด้วย	(1) Hardware: เลขทะเบียนทรัพย์สิน ประเภทอุปกรณ์ รายละเอียดทางเทคนิค ระบบปฏิบัติการ/เวอร์ชัน เจ้าของทรัพย์สิน สถานที่ตั้ง วันที่เริ่มใช้งาน/วันที่ติดตั้ง วันที่สิ้นสุดประกันหรือสิ้นสุดการใช้งานตามสัญญา และประเภทการครอบครอง (ซื้อหรือเช่า) (2) Software: เลขทะเบียนทรัพย์สิน ชื่อซอฟต์แวร์ รายละเอียดทางเทคนิค/การใช้งาน ระบบปฏิบัติการ/เวอร์ชัน หน่วยงานภายในผู้เป็นเจ้าของซอฟต์แวร์ วันลงทะเบียนซอฟต์แวร์ วันที่สิ้นสุดการใช้บริการ และเลขทะเบียนทรัพย์สินฮาร์ดแวร์ที่อ้างอิง
- เดิมไม่ได้กำหนด -	มีการประเมินความเสี่ยงทรัพย์สินด้านเทคโนโลยีสารสนเทศในกรณีที่มีความจำเป็นต้องใช้ระบบปฏิบัติการและอุปกรณ์ที่หมดอายุแล้ว (end of life) หรือสิ้นสุดการสนับสนุนหรือให้บริการ (end of support) ตลอดจนมีแนวทางในการควบคุมความเสี่ยงอย่างเหมาะสม

3.6.4. การรักษาความมั่นคงปลอดภัยของข้อมูล (Data Security)

หลักเกณฑ์ปัจจุบัน	หลักเกณฑ์ที่เสนอปรับปรุง
ในการบริหารจัดการทรัพย์สินสารสนเทศที่เป็นทรัพย์สินสารสนเทศประเภทข้อมูล ผู้ประกอบธุรกิจต้องดำเนินการจัดประเภทข้อมูลดังกล่าวตามระดับชั้นความลับและจัดประเภททรัพย์สินสารสนเทศอื่น ๆ ตามระดับความสำคัญ เพื่อให้ทรัพย์สินสารสนเทศได้รับการปกป้องในระดับที่เหมาะสมตามระดับชั้นความลับหรือระดับความสำคัญแล้วแต่กรณีด้วย และในกรณีที่เป็นข้อมูลสารสนเทศ ผู้ประกอบธุรกิจ	เพิ่มเติมข้อกำหนดต่อไปนี้ในหลักเกณฑ์ปัจจุบัน (1) มีการจัดทำทะเบียนทรัพย์สินประเภทข้อมูล (Data Inventory) ให้ครบถ้วนและเป็นปัจจุบัน โดยควรมีข้อมูล เช่น เลขทะเบียนข้อมูล ชื่อข้อมูล/ชุดข้อมูล รายละเอียดลักษณะและประเภทของข้อมูล ระดับชั้นความลับและระดับความสำคัญของข้อมูล เจ้าของข้อมูลหรือผู้ดูแลข้อมูล และสถานที่หรือเครื่องแม่ข่ายที่จัดเก็บ (2) กำหนดให้มีเจ้าของข้อมูล (data owner) หรือบุคคลที่ได้รับมอบหมายให้ทำหน้าที่รับผิดชอบในการกำหนดผู้ใช้งาน สิทธิการเข้าถึง และการใช้งานข้อมูลอย่างปลอดภัย

หลักเกณฑ์ปัจจุบัน	หลักเกณฑ์ที่เสนอปรับปรุง
ต้องมีกระบวนการป้องกันการเปิดเผย เปลี่ยนแปลงแก้ไข หรือสร้างความเสียหายต่อข้อมูลสารสนเทศที่สำคัญ ที่ถูกจัดเก็บในสื่อบันทึกข้อมูลด้วย	(3) กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล ตลอดจนการคุ้มครองข้อมูลส่วนบุคคลที่สอดคล้องตามชั้นความลับ ครอบคลุมข้อมูลที่อยู่บนอุปกรณ์ที่ใช้ปฏิบัติงาน (Data at Endpoint) ข้อมูลระหว่างการรับส่งผ่านเครือข่ายคอมพิวเตอร์ (Data in Transit) และการจัดเก็บข้อมูลบนระบบงานและสื่อบันทึกข้อมูล (Data at Rest) (4) กำหนดระเบียบปฏิบัติในการทำลายข้อมูลอย่างปลอดภัย (Data Disposal)

3.6.5. การควบคุมการเข้าถึง (Access Control)

หลักเกณฑ์ปัจจุบัน	หลักเกณฑ์ที่เสนอปรับปรุง
ผู้ประกอบธุรกิจต้องมีการควบคุมการเข้าถึงระบบและข้อมูลสารสนเทศ (Access Control) ให้เป็นไปตามหลักเกณฑ์ดังต่อไปนี้ (1) มีการบริหารจัดการบัญชีผู้ใช้งานโดยจำกัดการเข้าถึงข้อมูลสารสนเทศให้สามารถเข้าถึงได้เฉพาะบุคคลที่ได้รับสิทธิการเข้าถึง (2) มีข้อกำหนดให้ผู้ใช้งานปฏิบัติตามขั้นตอนการใช้งานและดูแลรับผิดชอบรหัสผ่าน (3) มีการป้องกันมิให้มีการเข้าถึงระบบสารสนเทศและโปรแกรมประยุกต์โดยไม่ได้รับอนุญาต	เพิ่มเติมข้อกำหนดต่อไปนี้ในหลักเกณฑ์ปัจจุบัน (1) บริหารจัดการบัญชีผู้ใช้งานและสิทธิการเข้าถึงข้อมูลและระบบสารสนเทศให้มีความรัดกุมมากขึ้น เช่น กำหนดบัญชีผู้ใช้งานที่สามารถระบุตัวตนผู้ใช้งานได้โดยหลีกเลี่ยงการใช้งาน Shared ID กำหนดกระบวนการอนุมัติสิทธิในการเข้าถึงจากเจ้าของระบบหรือเจ้าของข้อมูล และจัดทำตารางควบคุมการให้สิทธิ (Authorization Matrix) ของบัญชีผู้ใช้งานที่สอดคล้องกับตำแหน่งหน้าที่และความรับผิดชอบ เป็นต้น (2) จัดให้มีกระบวนการยืนยันตัวตนผู้ใช้งาน (Authentication) ที่มีประสิทธิภาพเหมาะสมกับความเสี่ยง และป้องกันการปฏิเสธความรับผิด (3) ข้อกำหนดการใช้งานบัญชีผู้ใช้งานสิทธิสูง (Privileged User) สำหรับระบบปฏิบัติการและระบบฐานข้อมูลที่เกี่ยวข้องกับระบบสารสนเทศที่มีความสำคัญ ดังนี้ ● ใช้การยืนยันตัวตนและพิสูจน์ตัวตนแบบหลาย

หลักเกณฑ์ปัจจุบัน	หลักเกณฑ์ที่เสนอปรับปรุง
	ปัจจัย (Multi-Factor Authentication : MFA) เมื่อเข้าใช้งานหรือเปลี่ยนแปลงรหัสผ่าน ● กรณีผู้ประกอบธุรกิจมีข้อจำกัดสำหรับการพิสูจน์ตัวตนแบบ MFA สามารถใช้วิธีการอื่นใดที่มีประสิทธิภาพเทียบเท่าทดแทน และจัดให้มีการประเมินความเสี่ยงและพิจารณาแนวทางควบคุมความเสี่ยงก่อนดำเนินการเพื่อขออนุมัติยกเว้น (Exception) ● การควบคุมและติดตามตรวจสอบการใช้งานบัญชีผู้ใช้งานสิทธิสูงอย่างเข้มงวด (4) ทบทวนบัญชีผู้ใช้งานและสิทธิการเข้าถึงอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง (5) ลบหรือระงับการใช้งานของบัญชีผู้ใช้งานที่ไม่จำเป็นหรือไม่มีการใช้งาน

3.6.6. การบริหารจัดการการเข้ารหัสข้อมูล (Cryptography)

หลักเกณฑ์ปัจจุบัน	หลักเกณฑ์ที่เสนอปรับปรุง
ผู้ประกอบธุรกิจต้องจัดให้มีการกำหนดนโยบายการใช้งานระบบการเข้ารหัสข้อมูลและการบริหารกุญแจเข้ารหัสข้อมูลที่สามารถป้องกันการเข้าถึงหรือเปลี่ยนแปลงแก้ไขข้อมูลที่เป็นความลับหรือมีความสำคัญ	เพิ่มเติมข้อกำหนดต่อไปนี้ในหลักเกณฑ์ปัจจุบัน (1) กำหนดวิธีการเข้ารหัส (Algorithm และ Cipher Suite) ที่ปลอดภัย และเป็นไปตามมาตรฐานสากล รวมทั้งมีการทบทวนอย่างสม่ำเสมอ (2) บริหารจัดการกุญแจเข้ารหัสอย่างปลอดภัย โดยครอบคลุมตั้งแต่การสร้างและติดตั้งกุญแจเข้ารหัส การจัดเก็บและสำรอง ไปจนถึงการเพิกถอนหรือทำลายกุญแจเข้ารหัส (3) ในกรณีที่กุญแจเข้ารหัสถูกสร้างขึ้นโดยบุคคลภายนอก ต้องตรวจสอบเพื่อให้มั่นใจได้ว่ากุญแจการเข้ารหัสที่สร้างขึ้นไม่มีการนำมาใช้ร่วมกับบุคคลอื่น

	(4) กำหนดกระบวนการรองรับกรณีเกิดการรั่วไหลของกุญแจเข้ารหัส เช่น การติดต่อหน่วยงานหรือผู้ที่เกี่ยวข้องกับชุดข้อมูลที่ใช้กุญแจเข้ารหัสชุดดังกล่าว การตรวจสอบชุดข้อมูลที่มีความเสี่ยงในการรั่วไหล การเปลี่ยนหรือเพิกถอนกุญแจการเข้ารหัสข้อมูล เป็นต้น

3.6.7. การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environmental Security)

หลักเกณฑ์ปัจจุบัน	หลักเกณฑ์ที่เสนอปรับปรุง
ผู้ประกอบธุรกิจต้องมีมาตรการเพื่อสร้างความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อมของทรัพย์สินสารสนเทศตามหลักเกณฑ์ดังต่อไปนี้ (1) ประเมินความเสี่ยงและความสำคัญของทรัพย์สินสารสนเทศ (2) กำหนดพื้นที่หวงห้ามและพื้นที่สำหรับจัดวางทรัพย์สินสารสนเทศที่มีความสำคัญให้มีความมั่นคงปลอดภัยและป้องกันมิให้บุคคลที่ไม่เกี่ยวข้องเข้าถึงพื้นที่ดังกล่าว	ปรับปรุงข้อกำหนดในหลักเกณฑ์ปัจจุบัน โดยแก้ไขเป็น ผู้ประกอบธุรกิจต้องจัดให้มีการสร้างความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม รวมทั้งมีระบบการป้องกันและกระบวนการในการบำรุงรักษาอุปกรณ์คอมพิวเตอร์ และระบบสาธารณูปโภค (Facilities) ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศอย่างเหมาะสม เพื่อให้สามารถป้องกันการเข้าถึง และป้องกันการสร้างความเสียหายต่อทรัพย์สินด้านเทคโนโลยีสารสนเทศที่จัดเก็บอยู่ในศูนย์คอมพิวเตอร์หลัก ศูนย์คอมพิวเตอร์สำรอง และศูนย์คอมพิวเตอร์จากบุคคลภายนอก (Co-location) ตลอดจนมีการป้องกันความปลอดภัยทางกายภาพของอุปกรณ์เทคโนโลยีสารสนเทศอื่น ๆ

3.6.8. การรักษาความมั่งคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT Operations Security)

หลักเกณฑ์ปัจจุบัน	หลักเกณฑ์ที่เสนอปรับปรุง
กำหนดขั้นตอนการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศเพื่อให้การปฏิบัติงานนั้นเป็นไปอย่างถูกต้องและมั่นคงปลอดภัย	ยกเลิกหัวข้อการกำหนดขั้นตอนการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ เนื่องจากมีข้อกำหนดในการจัดให้มีขั้นตอนการปฏิบัติงานสำหรับแต่ละหัวข้อการควบคุมแล้ว

หลักเกณฑ์ปัจจุบัน	หลักเกณฑ์ที่เสนอปรับปรุง
มีมาตรการป้องกันและตรวจสอบโปรแกรมไม่ประสงค์ดี (Malware) และมาตรการในการแก้ไขระบบสารสนเทศให้สามารถกลับมาใช้งานได้ตามปกติ	เพิ่มเติมข้อกำหนดต่อไปนี้ในหลักเกณฑ์ปัจจุบัน (1) การรักษาความมั่นคงปลอดภัยของเครื่องแม่ข่าย (Server) และอุปกรณ์ที่ใช้ปฏิบัติงาน (Endpoint) ซึ่งครอบคลุมเรื่องการติดตั้งซอฟต์แวร์ การเชื่อมต่อสื่อบันทึกข้อมูล การป้องกันและตรวจจับโปรแกรมไม่ประสงค์ดี และการบริหารจัดการระบบเสมือนจริง (Virtualization) (2) สำหรับผู้ประกอบธุรกิจที่มีความเสี่ยงสูง ควรจัดหาระบบ Endpoint Detection and Response รวมถึงมาตรการทางเทคนิคหรือเครื่องมือป้องกันข้อมูลสำคัญรั่วไหลบนเครื่องแม่ข่าย (Server) และอุปกรณ์ที่ใช้ปฏิบัติงาน (Endpoint)
จัดเก็บและบันทึกหลักฐาน (Logs) ต่าง ๆ ให้ครบถ้วนและเพียงพอสำหรับการตรวจสอบการล่วงรู้ข้อมูลภายในระหว่างหน่วยงานและบุคลากร การสอบทานการใช้งานข้อมูลและระบบสารสนเทศตามหน้าที่ที่ผู้ปฏิบัติงานได้รับมอบหมาย การตรวจสอบการเข้าใช้งานระบบสารสนเทศโดยบุคคลที่ไม่มีหน้าที่เกี่ยวข้อง การตรวจสอบและป้องกันการใช้งานระบบสารสนเทศที่มีความผิดปกติหรือไม่เป็นไปตามกฎหมายหรือกฎเกณฑ์ที่เกี่ยวข้อง และการตรวจสอบตัวตนของลูกค้าที่ทำรายการซื้อขายผ่านระบบอิเล็กทรอนิกส์	เพิ่มเติมข้อกำหนดต่อไปนี้ในหลักเกณฑ์ปัจจุบัน (1) การจัดเก็บข้อมูล Log ควรครอบคลุมถึงเหตุการณ์ที่เกี่ยวข้องกับข้อมูลส่วนบุคคล (2) จัดเก็บข้อมูลบันทึกเหตุการณ์ของอุปกรณ์ที่สำคัญไว้ที่เครื่องแม่ข่ายที่ใช้จัดเก็บข้อมูลบันทึกเหตุการณ์ (logging server) ที่แยกเฉพาะ โดยมีการรักษาความปลอดภัยที่รัดกุมเพียงพอในการป้องกันการเปลี่ยนแปลง แก้ไข หรือทำลาย
มีการทดสอบการเจาะระบบ (Penetration Test) กับระบบงานที่มีความสำคัญที่เชื่อมต่อกับระบบเครือข่ายภายนอก (Untrusted	ปรับปรุงข้อกำหนดต่อไปนี้ในหลักเกณฑ์ปัจจุบัน (1) **[ปรับปรุงจาก Focus Group]** กำหนดขอบเขตของการทดสอบให้ครอบคลุมระบบงานสารสนเทศและระบบเครือข่ายที่มีช่องทางเชื่อมต่อกับเครือข่าย

หลักเกณฑ์ปัจจุบัน	หลักเกณฑ์ที่เสนอปรับปรุง
Network) โดยบุคคลที่เป็นอิสระจากหน่วยงานที่รับผิดชอบด้านเทคโนโลยีสารสนเทศ และเป็นไปตามการวิเคราะห์ความเสี่ยงและผลกระทบทางธุรกิจ (Risk and Business Impact Analysis) กรณีที่เป็นระบบงานสำคัญที่ประเมินแล้วมีความสำคัญสูง ต้องทดสอบอย่างน้อยทุก 3 ปีและเมื่อมีการเปลี่ยนแปลงระบบงานดังกล่าวอย่างมีนัยสำคัญ	สาธารณะ (Internet Facing) อย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงระบบงานดังกล่าวอย่างมีนัยสำคัญ โดยระบบงานอื่น ๆ ควรจัดให้มีการประเมินความเสี่ยงจากการบุกรุกผ่านระบบเครือข่ายคอมพิวเตอร์ที่ใช้สื่อสารภายในองค์กร เพื่อกำหนดขอบเขตและทดสอบเจาะระบบตามความเหมาะสม (2) สำหรับผู้ประกอบธุรกิจที่มีความเสี่ยงสูง ผู้ทดสอบเจาะระบบงานสารสนเทศที่มีความสำคัญควรมีความเป็นอิสระจากหน่วยงานเจ้าของระบบ และควรได้รับการรับรองหรือมีวุฒิบัตรที่เป็นที่ยอมรับในอุตสาหกรรมเช่น OSCP, OSWP, OSCE, OSEE และ OSWE เป็นต้น
มาตรการรักษาความปลอดภัยที่รัดกุมเพียงพอสำหรับข้อมูลที่เป็นความลับหรือมีความสำคัญ ในกรณีที่มีการปฏิบัติงานจากเครือข่ายภายนอกบริษัทหรือมีการใช้งานอุปกรณ์เคลื่อนที่ โดยกรณีที่เป็นการใช้งานอุปกรณ์เคลื่อนที่ ต้องจัดให้มีการลงทะเบียนอุปกรณ์เคลื่อนที่ก่อนการใช้งาน และทบทวนทะเบียนดังกล่าวอย่างน้อยปีละ 1 ครั้งและเมื่อมีการเปลี่ยนอุปกรณ์เคลื่อนที่	เพิ่มเติมข้อกำหนดต่อไปนี้ในหลักเกณฑ์ปัจจุบัน (1) การใช้งานอุปกรณ์ส่วนตัวของพนักงาน (Bring Your Own Device: BYOD) ให้พิจารณาความเสี่ยงที่เกี่ยวข้อง และจัดให้มีมาตรการควบคุมอย่างเหมาะสม รวมถึงการตรวจสอบและป้องกัน Rooting หรือ Jailbreaking (2) สำหรับผู้ประกอบธุรกิจที่มีความเสี่ยงสูงควรมีเครื่องมือในการบริหารจัดการอุปกรณ์เคลื่อนที่
- เดิมไม่ได้กำหนด -	เพิ่มเติมข้อกำหนดต่อไปนี้ในหลักเกณฑ์ปัจจุบัน (1) การบริหารจัดการมาตรฐานการตั้งค่าระบบ (System Configuration Management) โดยจัดให้มีมาตรการควบคุมในการตั้งค่าความมั่นคงปลอดภัยของระบบ และสอบทานการตั้งค่าอย่างสม่ำเสมอ

หลักเกณฑ์ปัจจุบัน	หลักเกณฑ์ที่เสนอปรับปรุง
	(2) การบริหารจัดการขีดความสามารถของระบบสารสนเทศ (Capacity Management) โดยจัดให้มีมาตรฐานและวิธีปฏิบัติเรื่องการจัดการขีดความสามารถ การติดตามประสิทธิภาพการทำงานของระบบ และการประเมินแนวโน้มการใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศ เพื่อให้สามารถรองรับการดำเนินธุรกิจในปัจจุบัน และสามารถวางแผนการจัดสรรทรัพยากรให้รองรับการใช้งานในอนาคตได้อย่างมีประสิทธิภาพ (3) การติดตามดูแลระบบและเฝ้าระวังภัยคุกคาม (Security Monitoring) โดยจัดให้มีกระบวนการหรือเครื่องมือป้องกันและตรวจจับเหตุการณ์ผิดปกติ โปรแกรมไม่ประสงค์ดี (Malware) หรือภัยคุกคามต่อความมั่นคงปลอดภัย (4) การบริหารจัดการโปรแกรมแก้ไขช่องโหว่ (Patch Management) โดยจัดให้มีกระบวนการควบคุมการติดตั้งโปรแกรมแก้ไขช่องโหว่บนระบบที่ใช้งานจริง

3.6.9. การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายคอมพิวเตอร์ (Communications Security)

หลักเกณฑ์ปัจจุบัน	หลักเกณฑ์ที่เสนอปรับปรุง
ผู้ประกอบธุรกิจต้องมีมาตรการรักษาความมั่นคงปลอดภัยด้านการสื่อสารข้อมูลสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์ (Communications Security) ให้เป็นไปตามหลักเกณฑ์ดังต่อไปนี้ (1) มีการบริหารจัดการและควบคุมระบบเครือข่ายคอมพิวเตอร์ แบ่งแยกระบบเครือข่าย	เพิ่มเติมข้อกำหนดต่อไปนี้ในหลักเกณฑ์ปัจจุบัน (1) มีการบริหารจัดการและควบคุมระบบเครือข่ายคอมพิวเตอร์อย่างมั่นคงปลอดภัย เช่น การจัดโครงสร้างของระบบเครือข่ายและแบ่งเครือข่ายตามความเสี่ยงและลักษณะการให้บริการ การกำหนดมาตรการการควบคุมทางเทคนิค และสอบทานกฎของอุปกรณ์ Firewall อย่างสม่ำเสมอ เป็นต้น

คอมพิวเตอร์อย่างมั่นคงและปลอดภัย มีกระบวนการควบคุมการเข้าถึง กำหนดมาตรการในการรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศที่มีการรับส่งผ่านระบบเครือข่ายคอมพิวเตอร์ (2) จัดทำข้อตกลงการใช้บริการผ่านระบบเครือข่ายคอมพิวเตอร์ที่เกี่ยวกับวิธีการบริหารจัดการคุณภาพการให้บริการ และกระบวนการรักษาความมั่นคงปลอดภัยของระบบเครือข่ายคอมพิวเตอร์กับผู้รับดำเนินการ (3) ดำเนินการให้บุคลากรของผู้ประกอบธุรกิจและผู้รับดำเนินการ (ถ้ามี) มีข้อตกลงเกี่ยวกับการรักษาความลับหรือไม่เปิดเผยข้อมูลที่มีความสำคัญ	(2) มีกระบวนการควบคุมการเชื่อมต่อเครือข่ายระหว่างระบบงานภายในและหน่วยงานภายนอก (External Party) (3) จัดหาระบบและมาตรการรักษาความปลอดภัยในการป้องกันการถูกโจมตีจากเครือข่ายสาธารณะที่เหมาะสมตามความเสี่ยง

3.6.10. การบริหารจัดการโครงการด้านเทคโนโลยีสารสนเทศ และการจัดหา พัฒนา และบำรุงรักษาระบบระบบสารสนเทศ (IT Project Management, and System Acquisition, Development and Maintenance)

หลักเกณฑ์ปัจจุบัน	หลักเกณฑ์ที่เสนอปรับปรุง
ผู้ประกอบธุรกิจต้องจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศ (System Acquisition, Development and Maintenance) ตามหลักเกณฑ์ดังต่อไปนี้ (1) มีข้อกำหนดในการจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศให้มีความมั่นคงปลอดภัย เมื่อมี	ปรับปรุงโครงสร้างมาตรการควบคุมให้ชัดเจน โดยแบ่งเป็นเรื่องการบริหารโครงการ การจัดหาระบบงาน การพัฒนาระบบงาน และการแก้ไขเปลี่ยนแปลง และเพิ่มเติมข้อกำหนดต่อไปนี้ (1) ในการบริหารจัดการโครงการด้านเทคโนโลยีสารสนเทศ ต้องมีกรอบการบริหารจัดการโครงการที่ชัดเจน และมีการบริหารจัดการความเสี่ยงอย่างเหมาะสม

ระบบสารสนเทศใหม่หรือมีการปรับปรุงระบบเดิม (2) จัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศในกรณีที่มีการเข้าถึงระบบการให้บริการการใช้งาน (Application Service) (3) มีการควบคุมการพัฒนาหรือการแก้ไขเปลี่ยนแปลงระบบสารสนเทศในทุกขั้นตอนให้เป็นไปตามขั้นตอนการควบคุมความมั่นคงปลอดภัยด้านสารสนเทศที่กำหนดไว้ (4) มีการทดสอบระบบสารสนเทศที่ได้รับการพัฒนาหรือแก้ไขเปลี่ยนแปลง และ มีการทดสอบการทำงานของระบบสารสนเทศที่ได้รับการพัฒนา โดยผู้ใช้งานหรือผู้ทดสอบที่เป็นอิสระจากผู้พัฒนาระบบสารสนเทศดังกล่าว รวมถึงมีการดูแล ติดตาม และควบคุมการพัฒนาระบบสารสนเทศของผู้รับดำเนินการให้เป็นไปตามข้อตกลงการใช้บริการ (5) ปรับปรุงแผนบริหารความต่อเนื่องทางธุรกิจให้สอดคล้องกับการพัฒนาหรือการแก้ไขเปลี่ยนแปลงระบบสารสนเทศ (6) มีการควบคุมบุคลากร ขั้นตอน และเทคโนโลยีสำหรับการพัฒนาระบบสารสนเทศให้มีความมั่นคงปลอดภัยตลอดขั้นตอนการพัฒนาระบบ	(2) ในการพัฒนาระบบสารสนเทศ ต้องมีการจัดทำเอกสารรายละเอียดคุณสมบัติทางเทคนิคโดยที่ครอบคลุมเรื่องข้อกำหนดด้านการรักษาความมั่นคงปลอดภัย การคุ้มครองข้อมูลส่วนบุคคล (Privacy) และขีดความสามารถที่รองรับ (Capacity) มีมาตรการควบคุมความถูกต้องครบถ้วนของการแปลงข้อมูล (3) การแก้ไขเปลี่ยนแปลงระบบสารสนเทศ (System Change) กำหนดให้มีแนวทางการแก้ไขเปลี่ยนแปลงระบบสารสนเทศ กระบวนการขออนุมัติการเปลี่ยนแปลง บันทึกและจัดเก็บหลักฐานและปรับปรุงขั้นตอนการปฏิบัติงาน

3.6.11. การบริหารจัดการบุคคลภายนอก (Third Party Management)

หลักเกณฑ์ปัจจุบัน	หลักเกณฑ์ที่เสนอปรับปรุง
ในกรณีที่ผู้ประกอบธุรกิจแต่งตั้งบุคคลอื่นเป็นผู้รับดำเนินการในงานที่เกี่ยวกับระบบสารสนเทศของผู้ประกอบธุรกิจ ผู้ประกอบธุรกิจต้องดำเนินการให้เป็นไปตามหลักเกณฑ์ดังต่อไปนี้ (1) มีข้อตกลงและกระบวนการควบคุมเกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (2) มีการติดตาม ประเมิน ทบทวน และตรวจสอบผู้รับดำเนินการอย่างสม่ำเสมอ รวมถึงมีการประเมินความเสี่ยงและกำหนดกระบวนการบริหารจัดการความเสี่ยงในกรณีที่ผู้รับดำเนินการมีการเปลี่ยนแปลงกระบวนการขั้นตอน หรือวิธีการปฏิบัติงานในการรักษาความมั่นคงปลอดภัยในการปฏิบัติงาน หรือเปลี่ยนตัวผู้รับดำเนินการ (3) มีมาตรการตรวจสอบดูแลให้ผู้รับดำเนินการปฏิบัติตามหลักเกณฑ์การปฏิบัติงานที่คณะกรรมการ ก.ล.ต. คณะกรรมการกำกับตลาดทุน หรือสำนักงาน กำหนด รวมทั้งกำหนดสิทธิในการเข้าตรวจสอบกระบวนการปฏิบัติงานของผู้รับดำเนินการและควบคุมให้การปฏิบัติงานมีข้อกำหนดให้ผู้รับ	แก้ไขจากข้อกำหนดเรื่องผู้รับดำเนินการ (IT Outsourcing) เป็นข้อกำหนดเรื่องบุคคลภายนอก (Third Party) โดยจะมีความครอบคลุมถึงผู้ที่เชื่อมต่อระบบ และผู้ที่สามารถเข้าถึงข้อมูลสำคัญของผู้ประกอบธุรกิจ เพิ่มเติมข้อกำหนดต่อไปนี้ (1) มีการประเมินความเสี่ยงของบุคคลภายนอก เพื่อกำหนดมาตรการควบคุมที่เหมาะสม และสอดคล้องกับความมีนัยสำคัญ (2) การประเมินศักยภาพบุคคลภายนอก (due diligence) ที่มีความสำคัญอย่างยิ่งต่อผู้ประกอบธุรกิจ (critical third party) โดยควรคำนึงถึงเรื่องในการพิจารณาความมั่นคงปลอดภัยของบุคคลภายนอก และศักยภาพในการให้บริการ (3) จัดให้มีข้อตกลงการไม่เปิดเผยข้อมูล (non-disclosure agreement) กรณีที่บุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญของผู้ประกอบธุรกิจหรือข้อมูลของลูกค้าที่ควบคุมดูแลโดยผู้ประกอบธุรกิจได้ นอกจากนี้ บุคคลภายนอกต้องไม่เปิดเผยข้อมูลต่อ subcontract โดยไม่ได้รับความยินยอมจากผู้ประกอบธุรกิจ (4) ข้อตกลงหรือสัญญาการให้บริการต้องระบุสิทธิ์ให้ผู้ประกอบธุรกิจ สำนักงาน และผู้ตรวจสอบภายนอกที่ได้รับการแต่งตั้งจากผู้ประกอบธุรกิจหรือสำนักงาน สามารถเข้าตรวจสอบการดำเนินงานของบุคคลภายนอกได้ ทั้งนี้ หากมีเหตุจำเป็นที่ไม่สามารถดำเนินการระบุสิทธิหรือเงื่อนไขการตรวจสอบลงในสัญญาหรือข้อตกลงได้ ต้องมี

หลักเกณฑ์ปัจจุบัน	หลักเกณฑ์ที่เสนอปรับปรุง
ดำเนินการยินยอมให้สำนักงานเรียกดู ตรวจสอบเอกสารหลักฐานที่เกี่ยวข้อง หรือสามารถเข้าตรวจสอบการปฏิบัติงานของผู้รับดำเนินการ (4) มีแผนรองรับในกรณีที่เกิดเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (Incident Response Policy)	แนวทางที่จะใช้ประเมินหรือติดตามการดำเนินงานและการควบคุมภายในของบุคคลภายนอกให้รัดกุมเพียงพอสอดคล้องกับความเสี่ยงและความมีนัยสำคัญของการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูล
- เดิมไม่ได้กำหนด -	เพิ่มเติมข้อกำหนดสำหรับผู้ประกอบธุรกิจที่มีความเสี่ยงสูง ควรมีการจัดทำรายชื่อผู้ให้บริการ และจัดให้มีการประเมินด้านคุณภาพและความเชื่อถือของผู้ให้บริการ หรือผู้รับดำเนินการ (Trusted Vendor) โดยพิจารณาจากประสบการณ์ คุณภาพของบริการ และผลงานที่ส่งมอบตลอดจนมาตรฐานด้านความปลอดภัยเทคโนโลยีสารสนเทศที่เกี่ยวข้องกับสินค้าและบริการ เพื่อใช้เป็นส่วนหนึ่งขององค์ประกอบในการคัดเลือกผู้ให้บริการในอนาคต

3.6.12. การบริหารจัดการเหตุการณ์ผิดปกติและปัญหาด้านเทคโนโลยีสารสนเทศ (IT Incident Management)

หลักเกณฑ์ปัจจุบัน	หลักเกณฑ์ที่เสนอปรับปรุง
ผู้ประกอบธุรกิจต้องมีการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Incident Management) ให้เป็นไปตามหลักเกณฑ์ดังต่อไปนี้ (1) กำหนดขั้นตอนและกระบวนการในการบริหารจัดการเหตุการณ์ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ	ปรับปรุงข้อกำหนดในการรายงานสำนักงานในกรณีที่มีเหตุการณ์ที่ส่งผลกระทบต่อระบบงานสำคัญและมีผลกระทบต่อลูกค้าในวงกว้าง โดยครอบคลุมเหตุการณ์ดังนี้ (1) การละเมิดต่อข้อมูลส่วนบุคคลที่เกิดจากเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ (2) ทรัพย์สินของผู้ใช้งานสูญหาย หรือเสียหาย (3) การบุกรุก เข้าถึง หรือใช้งานระบบโดยไม่ได้รับอนุญาต (System Compromised)

<table>
<tr><th>หลักเกณฑ์ปัจจุบัน</th><th>หลักเกณฑ์ที่เสนอปรับปรุง</th></tr>
<tr><td>(2) กำหนดผู้มีหน้าที่รับผิดชอบในการบริหารจัดการเหตุการณ์ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ
(3) รายงานต่อผู้มีหน้าที่รับผิดชอบในการบริหารจัดการเหตุการณ์ตาม (2) และสำนักงานโดยไม่ชักช้าเมื่อเกิดเหตุการณ์ดังกล่าว
(4) ทดสอบขั้นตอนและกระบวนการในการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ ตาม (1) อย่างน้อยปีละ 1 ครั้ง โดยอย่างน้อยต้องครอบคลุมถึงการบริหารจัดการความเสี่ยงไซเบอร์ (Cyber Security Drill)
(5) พิจารณาทบทวนขั้นตอนและกระบวนการในการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ หลังจากที่มีการทดสอบตาม (4) แล้วอย่างน้อยปีละ 1 ครั้ง
(6) จัดให้มีการประเมินผลการทดสอบตาม (4) และประเมินผลพิจารณาทบทวนตาม (5) โดยต้องรายงานผลต่อคณะกรรมการของผู้ประกอบธุรกิจหรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบ</td><td>(4) ส่งผลกระทบต่อชื่อเสียงของผู้ประกอบธุรกิจ (Harm to Reputation) เช่น ถูกปลอมแปลงหน้าเว็บไซต์ของบริษัท (Website Defacement)
(5) การหยุดชะงักของระบบงาน (System Disruption) ในช่วงเวลาทำการซื้อขาย เป็นระยะเวลาถึงระดับที่ต้องรายงานสำนักงาน ดังนี้
<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>
(6) รายงานสำนักงานโดยไม่ชักช้าภายใน 3 ชั่วโมง นับแต่ทราบเหตุการณ์
(7) ในกรณีหน่วยงานโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศ (Critical Information Infrastructure หรือ CII) ให้รายงานโดยไม่ชักช้าภายใน 1 ชั่วโมง นับแต่ทราบเหตุการณ์
(8) รายงานความคืบหน้าเป็นลายลักษณ์อักษรเมื่อมีความคืบหน้า อย่างน้อยทุกวันทำการภายในเวลา 15:00 น. เริ่มจากวันทำการถัดไปหลังทราบเหตุการณ์หรือตามที่สำนักงานร้องขอ จนกว่าระบบสารสนเทศจะกลับสู่การให้บริการได้อย่างเป็นปกติ
(9) ในกรณีหน่วยงานโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศ (Critical Information Infrastructure</td></tr>
</table>

หลักเกณฑ์ปัจจุบัน	หลักเกณฑ์ที่เสนอปรับปรุง
ธุรกิจอย่างน้อยปีละ 1 ครั้ง ทั้งนี้ การดำเนินการดังกล่าวต้องกระทำโดยบุคคลที่เป็นอิสระจากผู้มีหน้าที่รับผิดชอบในการบริหารจัดการเหตุการณ์ตาม (2) (7) จัดเก็บเอกสารหลักฐานที่เกี่ยวข้องกับการดำเนินการในการบริหารจัดการเหตุการณ์ดังกล่าวเป็นระยะเวลาไม่น้อยกว่า 2 ปีนับแต่วันที่จัดทำเอกสารนั้น โดยต้องเก็บรักษาไว้ในลักษณะที่พร้อมให้สำนักงานสามารถเรียกดูและตรวจสอบได้โดยไม่ชักช้า	หรือ CII) ให้รายงานความคืบหน้าเป็นลายลักษณ์อักษรครั้งแรก ภายใน 2 ชั่วโมงนับแต่ทราบเหตุการณ์ และรายงานครั้งต่อไปเมื่อมีความคืบหน้าอย่างน้อยทุกวันทำการ เริ่มจากวันทำการถัดไปหลังทราบเหตุการณ์หรือตามที่สำนักงานร้องขอ จนกว่าระบบสารสนเทศจะกลับสู่การให้บริการได้อย่างเป็นปกติ เพิ่มเติมข้อกำหนดต่อไปนี้ในหลักเกณฑ์ปัจจุบัน (1) จัดให้มีช่องทางรับแจ้งเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศจากพนักงาน ผู้ใช้บริการและผู้ที่เกี่ยวข้อง (2) วิเคราะห์สาเหตุที่แท้จริง (Root Cause) ของเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ เพื่อหาแนวทางการแก้ไขจากสาเหตุที่แท้จริง และป้องกันไม่ให้เกิดเหตุการณ์ซ้ำในอนาคต

3.6.13. การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan)

หลักเกณฑ์ปัจจุบัน	หลักเกณฑ์ที่เสนอปรับปรุง
ผู้ประกอบธุรกิจต้องมีการบริหารความต่อเนื่องทางธุรกิจในด้านความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security of Business Continuity Management) ให้เป็นไปตามหลักเกณฑ์ดังต่อไปนี้ (1) กำหนดมาตรการรองรับสำหรับกรณีที่อาจเกิดเหตุการณ์ไม่พึงประสงค์ (2) กำหนดขั้นตอน กระบวนการดำเนินการ และการควบคุมเกี่ยวกับความมั่นคงปลอดภัยของระบบสารสนเทศให้สอดคล้องกับ	เพิ่มเติมข้อกำหนดต่อไปนี้ในหลักเกณฑ์ปัจจุบัน (1) จัดให้มีแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan) ที่สอดคล้องกับแผนการบริหารความต่อเนื่องทางธุรกิจ (BCP) และทบทวนอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ (2) กำหนดคณะทำงานหรือหน่วยงานที่รับผิดชอบในการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ โดยมีผู้บริหารและบุคลากรของหน่วยงานด้านต่าง ๆ ที่เกี่ยวข้องเข้าร่วมด้วย เช่น ด้านเทคโนโลยีสารสนเทศ ด้านธุรกิจ และด้านสื่อสารองค์กร เป็นต้น (3) มีการประเมินความเสี่ยง (Risk Analysis) เพื่อให้สามารถระบุเหตุการณ์ความเสี่ยงซึ่งส่งผลกระทบต่อ

หลักเกณฑ์ปัจจุบัน	หลักเกณฑ์ที่เสนอปรับปรุง
แผนบริหารความต่อเนื่องทางธุรกิจ (3) กำหนดระยะเวลาในการกลับคืนสู่สภาพการดำเนินงานปกติของระบบสารสนเทศและจัดลำดับการกู้คืนระบบงานสารสนเทศที่มีความสำคัญให้สอดคล้องกับผลกระทบที่อาจเกิดขึ้น (4) มีระบบสารสนเทศสำรองที่อยู่ในสภาพพร้อมใช้งาน ซึ่งต้องสอดคล้องกับระยะเวลาในการกลับคืนสู่สภาพการดำเนินงานตามปกติของระบบสารสนเทศ	การหยุดชะงักของกระบวนการและระบบเทคโนโลยีสารสนเทศ (4) วิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis) จากการหยุดชะงักของกระบวนการทางธุรกิจ (Business Process) เพื่อกำหนดระยะเวลาเป้าหมายในการกู้คืนระบบสารสนเทศ (RTO) ระยะเวลาเป้าหมายสูงสุดที่ยอมให้ข้อมูลเสียหาย (RPO) และระยะเวลาสูงสุดที่ยอมให้กระบวนการทางธุรกิจหยุดชะงัก (MTD) อย่างเหมาะสม (5) กำหนดระยะเวลาในการกู้คืนระบบ (RTO) ไม่เกิน 2 ชั่วโมง สำหรับระบบเทคโนโลยีสารสนเทศที่สนับสนุนกระบวนการทางธุรกิจที่สำคัญของศูนย์ซื้อขายสัญญาซื้อขายล่วงหน้า สำนักหักบัญชีสัญญาซื้อขายล่วงหน้า สำนักหักบัญชีหลักทรัพย์ และศูนย์รับฝากหลักทรัพย์ (6) กำหนดระยะเวลาในการกู้คืนระบบ (RTO) ไม่เกิน 4 ชั่วโมง สำหรับระบบเทคโนโลยีสารสนเทศที่สนับสนุนกระบวนการทางธุรกิจที่สำคัญสำหรับธุรกิจอื่น ๆ นอกเหนือจาก (5) (7) กรณีที่ผู้ประกอบธุรกิจไม่สามารถกำหนด RTO ของระบบเทคโนโลยีสารสนเทศได้ตามที่กำหนดข้างต้น ผู้ประกอบธุรกิจสามารถใช้วิธีการให้บริการแบบ Manual ทดแทนได้ โดยวิธีการดังกล่าวต้องไม่ส่งผลต่อประสิทธิภาพการให้บริการอย่างมีนัยสำคัญ (8) สื่อสารให้พนักงานที่เกี่ยวข้องมีความเข้าใจและสามารถปฏิบัติตามแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศอย่างถูกต้อง (9) ทบทวน และทดสอบการปฏิบัติตามแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ อย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ โดยรายงาน

หลักเกณฑ์ปัจจุบัน	หลักเกณฑ์ที่เสนอปรับปรุง
	ผลการทดสอบต่อคณะกรรมการของผู้ประกอบธุรกิจหรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบธุรกิจ (10) กำหนดกระบวนการดำเนินงาน เพื่อรับมือเหตุการณ์การใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศหรือการใช้ประสิทธิภาพของระบบงานเกินขีดจำกัดของตัวชี้วัดที่กำหนดไว้ เช่น การจำกัดการให้บริการบางช่องทาง หรือตัดการเชื่อมต่อกับผู้ให้บริการหรือบุคคลภายนอกที่มีผลกระทบต่อระบบ

3.7 การตรวจสอบด้านเทคโนโลยีสารสนเทศ

หลักเกณฑ์ปัจจุบัน	หลักเกณฑ์ที่เสนอปรับปรุง
มีการตรวจสอบระบบสารสนเทศดังนี้ (ก) วางแผนการตรวจสอบระบบสารสนเทศให้สอดคล้องกับความเสี่ยงที่ได้ประเมินไว้ (ข) กำหนดขอบเขตในการตรวจสอบระบบสารสนเทศทางเทคนิคให้ครอบคลุมถึงจุดเสี่ยงที่สำคัญ โดยการตรวจสอบดังกล่าวต้องไม่กระทบต่อการปฏิบัติงาน (ค) ตรวจสอบระบบสารสนเทศนอกเวลาทำงาน ในกรณีที่การตรวจสอบนั้นอาจส่งผลกระทบต่อความพร้อมในการใช้งานระบบดังกล่าว	เพิ่มเติมข้อกำหนดด้านการตรวจสอบด้านเทคโนโลยีสารสนเทศ ได้แก่ (1) ผู้ตรวจสอบซึ่งอาจเป็นผู้ตรวจสอบภายในหรือภายนอกที่มีความเป็นอิสระจาก (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), ISO/IEC 27001 Lead Auditor หรือใบรับรองอื่น ๆ ตามที่สำนักงานประกาศกำหนด (3) วางแผนงานและกำหนดขอบเขตการตรวจสอบให้สอดคล้องกับความเสี่ยงด้านเทคโนโลยีสารสนเทศและข้อกำหนดของสำนักงาน โดยทบทวนแผนงานและ

หลักเกณฑ์ปัจจุบัน	หลักเกณฑ์ที่เสนอปรับปรุง
	ขอบเขตของการตรวจสอบอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ (4) จัดให้มีการตรวจสอบตามแผนงานและขอบเขตที่กำหนดไว้อย่างน้อยปีละ 1 ครั้ง โดยมีขอบเขตของการตรวจสอบ ดังนี้ ● ผู้ประกอบธุรกิจขนาดเล็ก ควรมีการตรวจสอบตามการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีขั้นต้นที่จำเป็น (cyber hygiene) ให้ครบถ้วนทุกหัวข้อการควบคุม อย่างน้อย 1 ครั้งในทุก 2 ปี ● ผู้ประกอบธุรกิจที่มีความเสี่ยงภาพรวมต่ำ ควรจัดให้มีการตรวจสอบด้านเทคโนโลยีสารสนเทศอย่างน้อยปีละ 1 ครั้ง โดยเป็นการตรวจสอบแบบเต็มรูปแบบที่ครอบคลุมหลักเกณฑ์ครบถ้วนทุกหัวข้อการควบคุม อย่างน้อย 1 ครั้งในทุก 2 ปี ● ผู้ประกอบธุรกิจที่มีความเสี่ยงภาพรวมปานกลางหรือสูง ควรจัดให้มีการตรวจสอบด้านเทคโนโลยีสารสนเทศ อย่างน้อยปีละ 1 ครั้ง โดยเป็นการตรวจสอบแบบเต็มรูปแบบที่ครอบคลุมหลักเกณฑ์ครบถ้วนทุกหัวข้อการควบคุม อย่างน้อย 1 ครั้งในทุกปี (5) จัดให้มีแผนการแก้ไขปรับปรุงประเด็นจากการตรวจสอบ และการติดตามความคืบหน้าในการดำเนินการแก้ไขอย่างเหมาะสม (6) จัดทำรายงานผลการตรวจสอบ พร้อมทั้งรายงานข้อบกพร่องที่ตรวจพบ และแผนการปรับปรุงแก้ไขต่อคณะกรรมการของผู้ประกอบธุรกิจหรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบธุรกิจ ตลอดจนจัดเก็บรายงานผลการตรวจสอบเป็นระยะเวลาไม่น้อยกว่า 3 ปีนับแต่วันที่จัดทำเอกสารนั้น

หลักเกณฑ์ปัจจุบัน	หลักเกณฑ์ที่เสนอปรับปรุง
	โดยต้องเก็บรักษาไว้ในลักษณะที่พร้อมให้สำนักงานสามารถเรียกดูและตรวจสอบได้โดยไม่ชักช้า (7) รายงานผลการตรวจสอบต่อสำนักงานในรูปแบบและวิธีการที่กำหนดภายใน 30 วันนับจากวันที่ได้รับผลการทดสอบอย่างเป็นทางการ แต่ไม่เกิน 90 วันนับจากวันที่สิ้นสุดกระบวนการทดสอบและไม่เกินสองเดือนนับแต่วันสิ้นปีปฏิทิน

ทั้งนี้ สำนักงานได้จัดทำเอกสารแนบแสดงการเปรียบเทียบรายละเอียดของหลักเกณฑ์เดิม และหลักเกณฑ์ที่แก้ไข

แบบสำรวจความคิดเห็น

เรื่อง หลักการการแก้ไขหลักเกณฑ์การจัดให้มีระบบเทคโนโลยีสารสนเทศ

ข้อมูลทั่วไป

ชื่อผู้ตอบ _____ ตำแหน่ง _____

ชื่อบริษัท/องค์กร _____

โทรศัพท์ _____ โทรสาร _____

อีเมล _____

สถานะของผู้ให้ข้อคิดเห็น (ตอบได้มากกว่า 1 ข้อ)

☐ บริษัทหลักทรัพย์

☐ บริษัทหลักทรัพย์จัดการกองทุนรวม/กองทุนส่วนบุคคล

☐ ผู้ประกอบธุรกิจสัญญาซื้อขายล่วงหน้า

☐ ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

☐ ผู้ให้บริการระบบเสนอขายโทเคนดิจิทัล

☐ ผู้ให้บริการระบบคราวด์ฟันดิง (funding portal)

☐ ธนาคารพาณิชย์

☐ บริษัทประกัน

☐ ผู้ลงทุน

☐ อื่น ๆ (โปรดระบุ)_____

กรุณาส่งแบบสำรวจความคิดเห็นกลับไปที่

ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ สำนักงาน ก.ล.ต.

เลขที่ 333/3 ถนนวิภาวดีรังสิต แขวงจอมพล เขตจตุจักร กรุงเทพฯ 10900 โทรศัพท์ 1207

หรือ email : nakharin@sec.or.th thanakornb@sec.or.th หรือ chat@sec.or.th

***** สำนักงานขอขอบคุณท่านที่ได้ให้ความร่วมมือในการแสดงความคิดเห็นในครั้งนี้ *****

แบบสำรวจความคิดเห็น

ท่านเห็นด้วยหรือไม่กับหลักการการแก้ไขหลักเกณฑ์การจัดให้มีระบบเทคโนโลยีสารสนเทศตามที่สำนักงาน ก.ล.ต. กำหนดมาข้างต้น

1. ขอบเขตการใช้บังคับ

   ☐ เห็นด้วย

   ☐ ไม่เห็นด้วย

   ข้อเสนอแนะ / ข้อสังเกตเพิ่มเติม .....

2. โครงสร้างของประกาศและแนวปฏิบัติ

   ☐ เห็นด้วย

   ☐ ไม่เห็นด้วย

   ข้อเสนอแนะ / ข้อสังเกตเพิ่มเติม .....

3. บทนิยาม

   ☐ เห็นด้วย

   ☐ ไม่เห็นด้วย

   ข้อเสนอแนะ / ข้อสังเกตเพิ่มเติม .....

4. การกำหนดมาตรการควบคุมตามระดับความเสี่ยงในการดำเนินธุรกิจ

   ☐ เห็นด้วย

   ☐ ไม่เห็นด้วย

   ข้อเสนอแนะ / ข้อสังเกตเพิ่มเติม .....

5. การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

   5.1 บทบาทหน้าที่และความรับผิดชอบของคณะกรรมการของผู้ประกอบธุรกิจ

   ☐ เห็นด้วย

   ☐ ไม่เห็นด้วย

   ข้อเสนอแนะ / ข้อสังเกตเพิ่มเติม .....

5.2 โครงสร้างการกำกับดูแล

☐ เห็นด้วย

☐ ไม่เห็นด้วย

ข้อเสนอแนะ / ข้อสังเกตเพิ่มเติม .....

5.3 นโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ

☐ เห็นด้วย

☐ ไม่เห็นด้วย

ข้อเสนอแนะ / ข้อสังเกตเพิ่มเติม .....

6. การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security)

6.1 โครงสร้างการบริหารงานเพื่อการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Organization of Information Security)

☐ เห็นด้วย

☐ ไม่เห็นด้วย

ข้อเสนอแนะ / ข้อสังเกตเพิ่มเติม .....

6.2 การบริหารจัดการบุคลากร (Human Resource Security)

☐ เห็นด้วย

☐ ไม่เห็นด้วย

ข้อเสนอแนะ / ข้อสังเกตเพิ่มเติม .....

6.3 การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT Asset Management)

☐ เห็นด้วย

☐ ไม่เห็นด้วย

ข้อเสนอแนะ / ข้อสังเกตเพิ่มเติม .....

6.4 การรักษาความมั่นคงปลอดภัยของข้อมูล (Data Security)

☐ เห็นด้วย

☐ ไม่เห็นด้วย

ข้อเสนอแนะ / ข้อสังเกตเพิ่มเติม .....

6.5 การควบคุมการเข้าถึง (Access Control)

☐ เห็นด้วย

☐ ไม่เห็นด้วย

ข้อเสนอแนะ / ข้อสังเกตเพิ่มเติม .....

6.6 การบริหารจัดการการเข้ารหัสข้อมูล (Cryptography)

☐ เห็นด้วย

☐ ไม่เห็นด้วย

ข้อเสนอแนะ / ข้อสังเกตเพิ่มเติม .....

6.7 การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environmental Security)

☐ เห็นด้วย

☐ ไม่เห็นด้วย

ข้อเสนอแนะ / ข้อสังเกตเพิ่มเติม .....

6.8 การรักษาความมั่งคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT Operations Security)

☐ เห็นด้วย

☐ ไม่เห็นด้วย

ข้อเสนอแนะ / ข้อสังเกตเพิ่มเติม .....

6.9 การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายคอมพิวเตอร์ (Communications Security)

☐ เห็นด้วย

☐ ไม่เห็นด้วย

ข้อเสนอแนะ / ข้อสังเกตเพิ่มเติม .....

6.10 การบริหารจัดการโครงการด้านเทคโนโลยีสารสนเทศ และการจัดหา พัฒนาและบำรุงรักษาระบบระบบสารสนเทศ (IT Project Management, and System Acquisition, Development and Maintenance)

☐ เห็นด้วย

☐ ไม่เห็นด้วย

ข้อเสนอแนะ / ข้อสังเกตเพิ่มเติม .....

6.11 การบริหารจัดการบุคคลภายนอก (Third Party Management)

☐ เห็นด้วย

☐ ไม่เห็นด้วย

ข้อเสนอแนะ / ข้อสังเกตเพิ่มเติม .....

6.12 การบริหารจัดการเหตุการณ์ผิดปกติและปัญหาด้านเทคโนโลยีสารสนเทศ (IT Incident Management)

☐ เห็นด้วย

☐ ไม่เห็นด้วย

ข้อเสนอแนะ / ข้อสังเกตเพิ่มเติม .....

6.13 การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan)

☐ เห็นด้วย

☐ ไม่เห็นด้วย

ข้อเสนอแนะ / ข้อสังเกตเพิ่มเติม .....

7. การตรวจสอบด้านเทคโนโลยีสารสนเทศ

☐ เห็นด้วย

☐ ไม่เห็นด้วย

ข้อเสนอแนะ / ข้อสังเกตเพิ่มเติม .....

8. ข้อเสนอแนะ/ข้อสังเกตเพิ่มเติมอื่น ๆ