เอกสารรับฟังความคิดเห็น

เลขที่ อตท. 12/2565

เรื่อง ร่างประกาศเกี่ยวกับหลักเกณฑ์การจัดให้มีระบบเทคโนโลยีสารสนเทศ

เผยแพร่เมื่อวันที่ 6 พฤษภาคม 2565

สำนักงานได้จัดทำเอกสารฉบับนี้ขึ้นเพื่อสำรวจความคิดเห็นจากผู้เกี่ยวข้อง
ท่านสามารถ download เอกสารเผยแพร่ฉบับนี้ได้จาก www.sec.or.th

ท่านสามารถส่งความเห็นหรือข้อเสนอแนะให้สำนักงานได้
ตามที่ติดต่อด้านล่าง หรือ e-mail: cyberteam@sec.or.th nakharin@sec.or.th
natchac@sec.or.th หรือ chat@sec.or.th
วันสุดท้ายของการแสดงความคิดเห็น วันที่ 6 มิถุนายน 2565

ท่านสามารถติดต่อสอบถามข้อมูลเพิ่มเติมได้จากเจ้าหน้าที่ของสำนักงาน ดังนี้

1. นายนครินทร์ ลิ้มรังษี	โทรศัพท์ 0-2033-4660
2. นางสาวณัชชา จารุธเนศ	โทรศัพท์ 0-2033-9913
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

ตามที่สำนักงานมีแนวคิดที่จะทบทวนและแก้ไขหลักเกณฑ์การจัดให้มีระบบเทคโนโลยีสารสนเทศ (“หลักเกณฑ์ฯ”) ที่ใช้บังคับมาตั้งแต่ปี 2559 ให้มีความเหมาะสมสอดรับกับ (1) การใช้เทคโนโลยีสารสนเทศในการประกอบธุรกิจที่มีการเปลี่ยนแปลงไป (2) ภัยคุกคามทางไซเบอร์ที่มีพัฒนาการด้านเทคนิคและวิธีการ ตลอดจนกลุ่มเป้าหมายในการโจมตีที่กว้างขึ้น (3) การป้องกันเหตุการณ์ด้านความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศที่เกิดขึ้นในตลาดทุนในอดีต และ (4) การปรับปรุงเกณฑ์ด้านเทคโนโลยีสารสนเทศของหน่วยงานกำกับดูแลในภาคอุตสาหกรรมการเงินอื่น ๆ โดยได้เปิดรับฟังความคิดเห็นจากผู้เกี่ยวข้องต่อหลักการตามเอกสารรับฟังความคิดเห็นเลขที่ อตท. 40/2564 ระหว่างวันที่ 25 พฤศจิกายน ถึง 25 ธันวาคม 2564 นั้น

สำนักงานได้รับความเห็นและข้อเสนอแนะเกี่ยวกับหลักการแก้ไขหลักเกณฑ์ฯ ดังกล่าว โดยได้พิจารณาในรายละเอียดและนำไปใช้ประกอบการยกร่างประกาศและแนวปฏิบัติที่เกี่ยวข้องแล้ว ดังนี้

1. ร่างประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ที่ สธ. /2565 เรื่อง ข้อกำหนดในรายละเอียดเกี่ยวกับการจัดให้มีระบบเทคโนโลยีสารสนเทศ **(เอกสารแนบ 1)** พร้อมกับภาคผนวกแนบท้ายประกาศ ดังนี้

ภาคผนวก 1 คำศัพท์ **(เอกสารแนบ 2)**

ภาคผนวก 2 การกำกับดูแลและบริหารจัดการด้านเทคโนโลยีสารสนเทศ **(เอกสารแนบ 3)**

ภาคผนวก 3 การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ **(เอกสารแนบ 4)**

ภาคผนวก 4 การตรวจสอบด้านเทคโนโลยีสารสนเทศ **(เอกสารแนบ 5)**

2. ร่างประกาศแนวปฏิบัติ ที่ นป. /2565 เรื่อง แนวปฏิบัติในการจัดให้มีระบบเทคโนโลยีสารสนเทศ **(เอกสารแนบ 6)**

3. ร่างแบบประเมินระดับความเสี่ยงเกี่ยวกับระบบเทคโนโลยีสารสนเทศซึ่งส่งผลต่อการดำเนินธุรกิจของผู้ประกอบธุรกิจ (แบบ ITRA: IT Risk Assessment) **(เอกสารแนบ 7)**

4. ร่างแบบรายงานผลการตรวจประเมินทางด้านเทคโนโลยีสารสนเทศ **(เอกสารแนบ 8)**

ทั้งนี้ เพื่อให้ประกาศมีความสอดคล้องเหมาะสมกับผู้ประกอบธุรกิจยิ่งขึ้น สำนักงานจึงเห็นควรจัดให้มีการรับฟังความคิดเห็นร่างประกาศหลักเกณฑ์ฯ และเอกสารที่เกี่ยวข้องเพื่อขอรับฟังความเห็นจากผู้ประกอบธุรกิจและบุคคลทั่วไป

2. เป้าหมายที่ต้องการบรรลุ (Intended Outcome)

เพื่อให้ผู้ประกอบธุรกิจสามารถบริหารจัดการความเสี่ยงในการใช้เทคโนโลยีสารสนเทศได้อย่างมีประสิทธิผล และมีความพร้อมรับมือต่อภัยคุกคามทางไซเบอร์ที่เพิ่มขึ้นอย่างต่อเนื่อง พร้อมทั้งสร้างความเชื่อมั่นของผู้ลงทุนในการใช้บริการและผลิตภัณฑ์ของภาคตลาดทุน ซึ่งมีระบบเทคโนโลยีสารสนเทศเป็นส่วนสำคัญ

3. สรุปสาระสำคัญของร่างประกาศ

สำนักงานได้ปรับปรุงหลักเกณฑ์การจัดให้มีระบบเทคโนโลยีสารสนเทศ จึงขอเปิดรับฟังความคิดเห็นร่างประกาศ โดยสรุปสาระสำคัญได้ดังนี้

3.1 ร่างประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ที่ สธ. /2565 เรื่อง ข้อกำหนดในรายละเอียดเกี่ยวกับการจัดให้มีระบบเทคโนโลยีสารสนเทศ

(1) <u>ขอบเขตของการใช้บังคับหลักเกณฑ์</u>

ปรับปรุงขอบเขตให้ครอบคลุมผู้ประกอบธุรกิจดังต่อไปนี้

(ก) ผู้ประกอบธุรกิจหลักทรัพย์ แต่ไม่รวมถึงผู้ประกอบธุรกิจหลักทรัพย์ประเภทการจัดการเงินร่วมลงทุน หรือการเป็นนายหน้าระหว่างผู้ค้าหลักทรัพย์

(ข) ผู้ได้รับใบอนุญาตประกอบธุรกิจสัญญาซื้อขายล่วงหน้า

(ค) ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

(ง) สำนักหักบัญชีหลักทรัพย์

(จ) ศูนย์รับฝากหลักทรัพย์

(ฉ) ศูนย์ซื้อขายสัญญาซื้อขายล่วงหน้า

(ช) สำนักหักบัญชีสัญญาซื้อขายล่วงหน้า

(ซ) ผู้ให้บริการระบบเสนอขายโทเคนดิจิทัล

(ฌ) ผู้ให้บริการระบบคราวด์ฟันดิง

(2) <u>การกำหนดมาตรการควบคุมตามระดับความเสี่ยงในการดำเนินธุรกิจ</u>

ผู้ประกอบธุรกิจทุกรายภายใต้ขอบเขตของการบังคับใช้หลักเกณฑ์นี้ ต้อง (1) จัดให้มีการกำกับดูแลและบริหารจัดการด้านเทคโนโลยีสารสนเทศ (2) รักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และ (3) จัดให้มีการตรวจสอบการควบคุมด้านเทคโนโลยีสารสนเทศ

ให้เหมาะสมสอดคล้องกับผลการประเมินระดับความเสี่ยงของผู้ประกอบธุรกิจตามแบบ IT Risk Assessment (ITRA)

ผู้ประกอบธุรกิจต้องส่งผลการประเมิน ITRA ที่ผ่านการพิจารณาจากคณะกรรมการหรือผู้ที่ได้รับมอบหมายให้รับผิดชอบในเรื่องดังกล่าว ต่อสำนักงานภายในทุกวันสิ้นปีปฏิทินตามแบบและวิธีการที่กำหนดไว้บนเว็บไซต์ของสำนักงาน

(3) <u>ภาคผนวก 1 คำศัพท์</u>

กำหนดคำอธิบายคำศัพท์ที่มีการปรับปรุงให้มีความเหมาะสมกับบริบทการใช้งานเทคโนโลยีสารสนเทศในการประกอบธุรกิจและความเสี่ยงด้านเทคโนโลยีสารสนเทศที่มีการเปลี่ยนแปลงไป อาทิ

- “ระบบ IT ที่มีนัยสำคัญ” (critical system) หมายถึง ระบบคอมพิวเตอร์หรือระบบเครือข่ายที่หากมีการหยุดชะงักจะส่งผลกระทบอย่างมีนัยสำคัญต่อการดำเนินงานหรือความต่อเนื่องในการดำเนินงาน ชื่อเสียง หรือฐานะของผู้ประกอบธุรกิจ หรือการใช้บริการของลูกค้า เช่น ระบบซื้อขาย ระบบสนับสนุนการปฏิบัติการ (back office system) ระบบจัดเก็บและบริหารจัดการข้อมูลลูกค้า ระบบจัดการลงทุน หรือระบบจัดเก็บทรัพย์สิน เป็นต้น
- “บุคคลภายนอก” (third party) หมายถึง บุคคลที่มีความเกี่ยวข้องกับผู้ประกอบธุรกิจดังนี้ แต่ไม่รวมถึงลูกค้าที่ใช้บริการหรือผลิตภัณฑ์ของผู้ประกอบธุรกิจ และบุคลากรของผู้ประกอบธุรกิจ
    - ผู้รับดำเนินการด้านระบบ IT (IT outsourcee)
    - ผู้ให้บริการ หรือผู้เสนอขายหรือติดตั้งผลิตภัณฑ์ด้าน IT ที่สามารถเข้าถึงหรือปรับปรุงข้อมูลหรือระบบงานของผู้ประกอบธุรกิจ
    - ผู้ให้บริการ cloud computing
    - ผู้ที่สามารถเข้าถึงระบบ IT ของผู้ประกอบธุรกิจ
    - ผู้ที่สามารถเข้าถึงหรือมีการแลกเปลี่ยนข้อมูลสำคัญของผู้ประกอบธุรกิจหรือข้อมูลของลูกค้าที่อยู่ภายใต้การควบคุมดูแลของผู้ประกอบธุรกิจ
- “ผู้ประกอบธุรกิจ ขนาดเล็ก” หมายถึง ผู้ประกอบธุรกิจที่เข้าลักษณะเป็นผู้ประกอบธุรกิจขนาดเล็กตามที่กำหนด ในแบบ ITRA (IT Risk Assessment)
- “ผู้ประกอบธุรกิจที่มีความเสี่ยงระดับต่ำ ระดับปานกลาง หรือระดับสูง” หมายถึง ผู้ประกอบธุรกิจที่มีผลการประเมินตามแบบ ITRA (IT Risk Assessment) อยู่ในระดับต่ำ ระดับปานกลาง หรือระดับสูง แล้วแต่กรณี

(4) ภาคผนวก 2 การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

กำหนดกรอบการกำกับดูแลด้านเทคโนโลยีสารสนเทศและบทบาทหน้าที่ของคณะกรรมการของผู้ประกอบธุรกิจเพื่อให้การบริหารงานด้านเทคโนโลยีสารสนเทศเป็นไปอย่างมีประสิทธิภาพและประสิทธิผล และมีการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศที่เหมาะสม ดังนี้

(ก) ผู้ประกอบธุรกิจต้องดำเนินการให้การควบคุมดูแลการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ผ่านการกำกับดูแลโดยคณะกรรมการของผู้ประกอบธุรกิจ เพื่อให้สอดคล้องกับระดับความเสี่ยง

(ข) ผู้ประกอบธุรกิจต้องจัดให้มีโครงสร้างการกำกับดูแลและบริหารจัดการความเสี่ยงด้าน IT ที่ทำให้เกิดการถ่วงดุลอย่างอิสระ และสอดคล้องตามหลักการแบ่งแยกหน้าที่ 3 ระดับ (3 Lines of Defense: 3 LoDs)

(ค) ผู้ประกอบธุรกิจต้องให้มี (1) นโยบายการบริหารจัดการความเสี่ยงด้าน IT (IT risk management policy) และ (2) นโยบายการรักษาความมั่นคงปลอดภัยด้าน IT (IT security policy)

(5) ภาคผนวก 3 การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security)

(ก) ผู้ประกอบธุรกิจที่มีความเสี่ยงระดับต่ำ ระดับปานกลาง หรือระดับสูง ต้องจัดให้มีการควบคุมด้านเทคโนโลยีสารสนเทศอย่างเหมาะสมครอบคลุมกิจกรรม ดังนี้

1. โครงสร้างการบริหารงานเพื่อการรักษาความมั่นคงปลอดภัยด้าน IT
2. การบริหารจัดการบุคลากรที่ปฏิบัติงานด้าน IT
3. การบริหารจัดการทรัพย์สินด้าน IT (IT asset management)
4. การรักษาความมั่นคงปลอดภัยของข้อมูล
5. การควบคุมการเข้าถึงข้อมูลและระบบ IT
6. การรักษาความมั่นคงปลอดภัยของข้อมูล
7. การสร้างความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม
8. มาตรการรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้าน IT
9. มาตรการรักษาความมั่นคงปลอดภัยเกี่ยวกับระบบเครือข่ายสื่อสาร
10. การบริหารจัดการโครงการด้าน IT และมีมาตรการการจัดหา พัฒนา รวมถึงบำรุงรักษาระบบ IT
11. การบริหารจัดการเหตุการณ์ผิดปกติด้าน IT และปัญหาด้าน IT
12. จัดทำแผนฉุกเฉินด้าน IT

(ข) ผู้ประกอบธุรกิจขนาดเล็ก ให้ดำเนินการอย่างน้อย ตาม (ก) ในข้อดังต่อไปนี้

1. ข้อ 2 การบริหารจัดการบุคลากรที่ปฏิบัติงานด้าน IT หรือบุคคลภายนอก
2. ข้อ 5 การควบคุมการเข้าถึงข้อมูลและระบบ IT เรื่อง การกำหนดมาตรการควบคุม จำกัด และติดตามการใช้งานบัญชี privileged user
3. ข้อ 8 มาตรการรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้าน IT เรื่อง การตั้งค่าระบบ (system configuration management), การรักษาความมั่นคงปลอดภัยของเครื่องแม่ข่าย (server) และอุปกรณ์ที่ใช้ปฏิบัติงาน (endpoint), การประเมินช่องโหว่ทางเทคนิค (technical vulnerability assessment), การทดสอบเจาะระบบงาน (penetration test) และ การบริหารจัดการโปรแกรมแก้ไขช่องโหว่ (patch management)

(6) <u>ภาคผนวก 4 การตรวจสอบด้านเทคโนโลยีสารสนเทศ (information technology audit)</u>

ผู้ประกอบธุรกิจภายใต้ขอบเขตของการบังคับใช้หลักเกณฑ์นี้ ต้องจัดให้มีการตรวจสอบด้านเทคโนโลยีสารสนเทศ และรายงานผลการตรวจสอบต่อสำนักงาน ตามขอบเขตและเงื่อนไข ดังนี้

(ก) จัดให้มีผู้ตรวจสอบลักษณะดังนี้ (1) ผ่านการรับรองและมีวุฒิบัตรที่กำหนด และ (2) มีความเป็นอิสระจากผู้ทำหน้าที่ด้าน IT ในระดับ first line of defense และ second line of defense

(ข) ดำเนินการวางแผนและกำหนดขอบเขตการตรวจสอบให้สอดคล้องกับความเสี่ยงด้าน IT และประกาศที่ สธ. /2565 โดยจัดให้มีการตรวจสอบและรายงานผลการตรวจสอบด้าน IT อย่างน้อยปีละ 1 ครั้ง โดยมีเงื่อนไขเพิ่มเติมดังนี้

ผู้ประกอบธุรกิจ	ขอบเขตการตรวจสอบ	การตรวจสอบแบบเต็มรูปแบบ (full scope)
ผู้ประกอบธุรกิจขนาดเล็ก	เฉพาะหัวข้อที่ผู้ประกอบธุรกิจขนาดเล็กต้องปฏิบัติ	อย่างน้อยทุก 2 ปี
ความเสี่ยงระดับต่ำ	ทุกหัวข้อการควบคุม (full scope)	อย่างน้อยทุก 2 ปี
ความเสี่ยงระดับกลางหรือระดับสูง	ทุกหัวข้อการควบคุม (full scope)	อย่างน้อยปีละ 1 ครั้ง

(ค) จัดให้มีแผนการปรับปรุงแก้ไขข้อบกพร่องจากการตรวจสอบ และการติดตามความคืบหน้าการดำเนินการแก้ไขข้อบกพร่อง (ถ้ามี) พร้อมทั้งจัดทำและรายงานผลการตรวจสอบ

ต่อสำนักงาน ตามรูปแบบและวิธีการที่กำหนดไว้บนเว็บไซต์ของสำนักงาน และภายในระยะเวลาที่กำหนด

3.2 ร่างประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ที่ นป. /2565 เรื่อง แนวปฏิบัติในการจัดให้มีระบบเทคโนโลยีสารสนเทศ

เพื่อประโยชน์ในการปฏิบัติตามข้อกำหนดของประกาศที่ สธ. /2565 และภาคผนวกแนบท้ายประกาศ ให้ผู้ประกอบธุรกิจพิจารณาดำเนินการตามเอกสารแนบ 6 โดย

- ผู้ประกอบธุรกิจความเสี่ยงระดับต่ำ และ ระดับกลาง ควรดำเนินการตามแนวปฏิบัติเพิ่มเติมทุกข้อ ยกเว้นข้อที่ระบุ “ความเสี่ยงสูง”
- ผู้ประกอบธุรกิจระดับความเสี่ยงสูง ให้ดำเนินการตามข้อกำหนดและแนวปฏิบัติเพิ่มเติมทุกข้อ

3.3 ร่างแบบประเมินระดับความเสี่ยงเกี่ยวกับระบบเทคโนโลยีสารสนเทศซึ่งส่งผลต่อการดำเนินธุรกิจของผู้ประกอบธุรกิจ (แบบ ITRA: IT Risk Assessment)

ให้ผู้ประกอบธุรกิจทุกรายประเมินระดับความเสี่ยงเกี่ยวกับระบบเทคโนโลยีสารสนเทศซึ่งส่งผลต่อการดำเนินธุรกิจของผู้ประกอบธุรกิจตามเอกสารแนบ 7 เพื่อให้ทราบว่าผู้ประกอบธุรกิจจัดอยู่ในกรณีใดกรณีหนึ่ง ดังนี้

- ผู้ประกอบธุรกิจขนาดเล็ก
- ผู้ประกอบธุรกิจที่มีความเสี่ยงระดับต่ำ
- ผู้ประกอบธุรกิจที่ที่มีความเสี่ยงระดับปานกลาง
- ผู้ประกอบธุรกิจที่มีความเสี่ยงระดับสูง

3.4 ร่างแบบรายงานผลการตรวจประเมินทางด้านเทคโนโลยีสารสนเทศ

ให้ผู้ประกอบธุรกิจทุกรายจัดให้มีการตรวจสอบด้าน IT และรายงานผลการตรวจสอบตามข้อกำหนดในภาคผนวก 4 การตรวจสอบด้านเทคโนโลยีสารสนเทศ และตามรูปแบบที่กำหนดในเอกสารแนบ 8 ต่อสำนักงาน

4. ช่วงเวลาที่คาดว่าประกาศจะมีผลใช้บังคับ

วันที่ 1 มกราคม 2566 เป็นต้นไป

แบบสำรวจความคิดเห็น

เรื่อง ร่างประกาศเกี่ยวกับหลักเกณฑ์การจัดให้มีระบบเทคโนโลยีสารสนเทศ

ข้อมูลทั่วไป

ชื่อผู้ตอบ _____ ตำแหน่ง _____

ชื่อบริษัท/องค์กร _____

โทรศัพท์ _____ โทรสาร _____

อีเมล _____

สถานะของผู้ให้ข้อคิดเห็น (ตอบได้มากกว่า 1 ข้อ)

- ☐ บริษัทหลักทรัพย์
- ☐ ผู้ประกอบธุรกิจสัญญาซื้อขายล่วงหน้า
- ☐ ผู้ให้บริการระบบเสนอขายโทเคนดิจิทัล
- ☐ ผู้ให้บริการระบบคราวด์ฟันดิง (funding portal)
- ☐ บริษัทหลักทรัพย์จัดการกองทุนรวม/กองทุนส่วนบุคคล
- ☐ อื่น ๆ (โปรดระบุ)_____
- ☐ ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล
- ☐ ธนาคารพาณิชย์
- ☐ บริษัทประกัน
- ☐ ผู้ลงทุน

สำนักงาน ก.ล.ต. ขอข้อมูลส่วนบุคคลของท่าน โดยมีวัตถุประสงค์ เพื่อใช้พิจารณาประกอบการรับฟังความคิดเห็น และประโยชน์ในการติดต่อกลับเพื่อขอข้อมูลประกอบเอกสารรับฟังความคิดเห็นของท่านเพิ่มเติม โดย สำนักงาน ก.ล.ต. คำนึงถึงความสำคัญของข้อมูลและเคารพสิทธิความเป็นส่วนตัวของท่าน จึงขอให้ท่านอ่านและทำความเข้าใจในโยบายการคุ้มครองข้อมูลส่วนบุคคล Privacy Policy แล้วจึงพิจารณาให้ความยินยอมให้ สำนักงาน ก.ล.ต. ประมวลผลข้อมูลส่วนบุคคลของท่าน

☐ ยินยอม ☐ ไม่ยินยอม

กรณีต้องการยกเลิกความยินยอมหรือขอใช้สิทธิ โปรดติดต่อไปที่ email: DPO@sec.or.th

กรุณาส่งแบบสำรวจความคิดเห็นกลับไปที่

ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ สำนักงาน ก.ล.ต.

เลขที่ 333/3 ถนนวิภาวดีรังสิต แขวงจอมพล เขตจตุจักร กรุงเทพฯ 10900

โทรศัพท์ 1207 หรือ email : cyberteam@sec.or.th

***** สำนักงานขอขอบคุณท่านที่ได้ให้ความร่วมมือในการแสดงความคิดเห็นในครั้งนี้ *****

แบบสำรวจความคิดเห็น

ท่านเห็นด้วยหรือไม่กับร่างประกาศเกี่ยวกับหลักเกณฑ์การจัดให้มีระบบเทคโนโลยีสารสนเทศตามที่สำนักงาน ก.ล.ต. กำหนดมาข้างต้น

1. ร่างประกาศข้อกำหนดในรายละเอียดและแนวปฏิบัติในการจัดให้มีระบบเทคโนโลยีสารสนเทศ

1.1 ขอบเขตการใช้บังคับ

☐ เห็นด้วย

☐ ไม่เห็นด้วย

ข้อเสนอแนะ / ข้อสังเกตเพิ่มเติม .....

1.2 การกำหนดมาตรการควบคุมตามระดับความเสี่ยงในการดำเนินธุรกิจ

☐ เห็นด้วย

☐ ไม่เห็นด้วย

ข้อเสนอแนะ / ข้อสังเกตเพิ่มเติม .....

1.3 คำศัพท์

☐ เห็นด้วย

☐ ไม่เห็นด้วย

ข้อเสนอแนะ / ข้อสังเกตเพิ่มเติม .....

1.4 การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

1.4.1 บทบาทหน้าที่และความรับผิดชอบของคณะกรรมการของผู้ประกอบธุรกิจ

☐ เห็นด้วย

☐ ไม่เห็นด้วย

ข้อเสนอแนะ / ข้อสังเกตเพิ่มเติม .....

1.4.2 การกำกับดูแลและบริหารจัดการความเสี่ยงด้าน IT ในระดับองค์กร

☐ เห็นด้วย

☐ ไม่เห็นด้วย

ข้อเสนอแนะ / ข้อสังเกตเพิ่มเติม .....

1.5 การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security)

1.5.1 โครงสร้างการบริหารงานเพื่อการรักษาความมั่นคงปลอดภัยด้าน IT

☐ เห็นด้วย

☐ ไม่เห็นด้วย

ข้อเสนอแนะ / ข้อสังเกตเพิ่มเติม .....

1.5.2 การบริหารจัดการบุคลากรที่ปฏิบัติงานด้าน IT หรือบุคคลภายนอก

☐ เห็นด้วย

☐ ไม่เห็นด้วย

ข้อเสนอแนะ / ข้อสังเกตเพิ่มเติม .....

1.5.3 การบริหารจัดการทรัพย์สินด้าน IT (IT asset management)

☐ เห็นด้วย

☐ ไม่เห็นด้วย

ข้อเสนอแนะ / ข้อสังเกตเพิ่มเติม .....

1.5.4 การรักษาความมั่นคงปลอดภัยของข้อมูล

☐ เห็นด้วย

☐ ไม่เห็นด้วย

ข้อเสนอแนะ / ข้อสังเกตเพิ่มเติม .....

1.5.5 การควบคุมการเข้าถึงข้อมูลและระบบ IT

☐ เห็นด้วย

☐ ไม่เห็นด้วย

ข้อเสนอแนะ / ข้อสังเกตเพิ่มเติม .....

1.5.6 การรักษาความมั่นคงปลอดภัยของข้อมูล

☐ เห็นด้วย

☐ ไม่เห็นด้วย

ข้อเสนอแนะ / ข้อสังเกตเพิ่มเติม .....

1.5.7 การสร้างความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม

☐ เห็นด้วย

☐ ไม่เห็นด้วย

ข้อเสนอแนะ / ข้อสังเกตเพิ่มเติม .....

1.5.8 มาตรการรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้าน IT

☐ เห็นด้วย

☐ ไม่เห็นด้วย

ข้อเสนอแนะ / ข้อสังเกตเพิ่มเติม .....

1.5.9 มาตรการรักษาความมั่นคงปลอดภัยเกี่ยวกับระบบเครือข่ายสื่อสาร

☐ เห็นด้วย

☐ ไม่เห็นด้วย

ข้อเสนอแนะ / ข้อสังเกตเพิ่มเติม .....

1.5.10 การบริหารจัดการโครงการด้าน IT และมาตรการการจัดหา พัฒนา รวมถึงบำรุงรักษาระบบ IT

☐ เห็นด้วย

☐ ไม่เห็นด้วย

ข้อเสนอแนะ / ข้อสังเกตเพิ่มเติม .....

1.5.11 การบริหารจัดการเหตุการณ์ผิดปกติด้าน IT และปัญหาด้าน IT

☐ เห็นด้วย

☐ ไม่เห็นด้วย

ข้อเสนอแนะ / ข้อสังเกตเพิ่มเติม .....

1.5.12 แผนฉุกเฉินด้าน IT

☐ เห็นด้วย

☐ ไม่เห็นด้วย

ข้อเสนอแนะ / ข้อสังเกตเพิ่มเติม .....

1.6 การตรวจสอบด้านเทคโนโลยีสารสนเทศ

☐ เห็นด้วย

☐ ไม่เห็นด้วย

ข้อเสนอแนะ / ข้อสังเกตเพิ่มเติม .....

2. ร่างแบบประเมินระดับความเสี่ยงเกี่ยวกับระบบเทคโนโลยีสารสนเทศซึ่งส่งผลต่อการดำเนินธุรกิจของผู้ประกอบธุรกิจ ตามแบบ ITRA (IT Risk Assessment)

☐ เห็นด้วย

☐ ไม่เห็นด้วย

ข้อเสนอแนะ / ข้อสังเกตเพิ่มเติม .....

3. ร่างแบบรายงานผลการตรวจประเมินทางด้านเทคโนโลยีสารสนเทศ

☐ เห็นด้วย

☐ ไม่เห็นด้วย

ข้อเสนอแนะ / ข้อสังเกตเพิ่มเติม .....

4. ข้อเสนอแนะ/ข้อสังเกตเพิ่มเติมอื่น ๆ