เอกสารรับฟังความคิดเห็น

เลขที่ อตท. 26/2567

เรื่อง การปรับปรุงหลักเกณฑ์การจัดให้มีระบบเทคโนโลยีสารสนเทศ

เผยแพร่เมื่อวันที่ 14 มิถุนายน 2567

สำนักงานได้จัดทำเอกสารฉบับนี้ขึ้นเพื่อสำรวจความคิดเห็นจากผู้เกี่ยวข้อง
ท่านสามารถ download เอกสารเผยแพร่ฉบับนี้ได้จาก
เว็บไซต์ของสำนักงาน (www.sec.or.th) และระบบกลางทางกฎหมาย (law.go.th)

วันสุดท้ายของการแสดงความคิดเห็น วันที่ 15 กรกฎาคม 2567

ท่านสามารถส่งความเห็นหรือข้อเสนอแนะหรือติดต่อสอบถามข้อมูลเพิ่มเติมได้จาก
เจ้าหน้าที่ของสำนักงาน ดังนี้

1. ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ อีเมล cyberteam@sec.or.th
2. นายกฤษฎา ตุลารักษ์ โทรศัพท์ 0-2033-9653 อีเมล kritsadat@sec.or.th
3. นางสาวณัชชา จารุธเนศ โทรศัพท์ 0-2033-9985 อีเมล natchac@sec.or.th

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”) ได้ออกประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ที่ สธ. 38/2565 เรื่อง ข้อกำหนดในรายละเอียดเกี่ยวกับการจัดให้มีระบบเทคโนโลยีสารสนเทศ ลงวันที่ 28 กันยายน พ.ศ. 2565 (“ประกาศ ที่ สธ. 38/2565”) ซึ่งได้กำหนดหลักเกณฑ์การจัดให้มีระบบเทคโนโลยีสารสนเทศ เพื่อให้ผู้ประกอบธุรกิจจัดให้มีนโยบายและมาตรการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศที่ดี รวมถึงมีการติดตาม ตรวจสอบ และทบทวนการปฏิบัติตามนโยบายและมาตรการดังกล่าวอย่างต่อเนื่อง โดยมีเป้าหมายเพื่อให้ผู้ประกอบธุรกิจมีการกำกับดูแลความเสี่ยงในการนำเทคโนโลยีสารสนเทศมาใช้ในการประกอบธุรกิจอย่างเหมาะสม

ทั้งนี้ หลังจากประกาศ ที่ สธ. 38/2565 มีผลบังคับใช้ตั้งแต่วันที่ 1 กรกฎาคม 2566 เป็นต้นมา สำนักงานได้รับข้อเสนอแนะจากผู้ประกอบธุรกิจและผู้ที่เกี่ยวข้อง เพื่อประกอบการพิจารณาปรับปรุงประกาศ ที่ สธ. 38/2565 ในด้านต่าง ๆ อาทิ การปรับปรุงข้อกำหนดเพื่อให้บทบาทหน้าที่ในการปฏิบัติตามหลักเกณฑ์ดังกล่าวสะท้อนถึงความเสี่ยงของผู้ประกอบธุรกิจที่มีระดับความเสี่ยงต่ำหรือผู้ประกอบธุรกิจที่มีขนาดเล็กอย่างเหมาะสมมากยิ่งขึ้น และการปรับปรุงข้อกำหนดให้สอดคล้องกับการปฏิบัติมากขึ้น

ในการนี้ สำนักงานจึงเห็นควรปรับปรุงข้อกำหนดที่เกี่ยวข้องเพื่อให้ประกาศ ที่ สธ. 38/2565 ดังกล่าวมีประสิทธิภาพมากยิ่งขึ้น โดยที่ผู้ประกอบธุรกิจยังคงมีมาตรการควบคุมความเสี่ยงและระบบงานด้านเทคโนโลยีสารสนเทศที่มีประสิทธิภาพและประสิทธิผล อีกทั้งมีความพร้อมในการรับมือต่อภัยคุกคามทางไซเบอร์ (Cyber resilience) ที่อาจเกิดขึ้นได้

2. เป้าหมายที่ต้องการบรรลุ (Intended Outcome)

ผู้ประกอบธุรกิจสามารถบริหารจัดการความเสี่ยงในการใช้เทคโนโลยีสารสนเทศได้อย่างมีประสิทธิผล และมีความพร้อมในการรับมือต่อภัยคุกคามทางไซเบอร์ที่เพิ่มขึ้นอย่างต่อเนื่อง พร้อมทั้งสร้างความเชื่อมั่นให้กับผู้ลงทุนในการใช้บริการและผลิตภัณฑ์ของภาคตลาดทุน ซึ่งมีระบบเทคโนโลยีสารสนเทศเป็นส่วนสำคัญ โดยไม่ก่อให้เกิดภาระกับผู้ประกอบธุรกิจเกินสมควร

3. หลักการที่ปรับปรุง

3.1 การปรับปรุงขอบเขตการบังคับใช้ประกาศฯ สำหรับผู้ประกอบธุรกิจการเป็นที่ปรึกษาการลงทุน

ปรับปรุงจาก “การเป็นที่ปรึกษาการลงทุนที่มีการวางแผนการลงทุนให้แก่ลูกค้าหรือใช้โปรแกรมสำเร็จรูปประกอบการให้บริการแก่ลูกค้า” เป็น “การเป็นที่ปรึกษาการลงทุนที่มีการใช้เทคโนโลยีเพื่อการติดต่อและให้บริการแก่ลูกค้า” และเพิ่มคำจำกัดความ “เทคโนโลยีเพื่อการติดต่อและให้บริการแก่ลูกค้า” หมายความว่า “เทคโนโลยีหรือคอมพิวเตอร์ ที่ใช้ในการติดต่อลูกค้า การจัดทำหรือนำส่งข้อมูลบริการและผลิตภัณฑ์ให้แก่ลูกค้า รวมทั้งการใช้งานเพื่อประมวลผล วิเคราะห์ ออกผลลัพธ์หรือคำแนะนำ เพื่อให้ลูกค้าใช้ประกอบการตัดสินใจลงทุน”

<u>เหตุผล</u>: เพื่อให้ผู้ประกอบธุรกิจการเป็นที่ปรึกษาการลงทุนซึ่งมีการใช้งานเทคโนโลยีสารสนเทศ (“IT”) ในการประกอบธุรกิจ มีมาตรการควบคุมความเสี่ยงด้าน IT ที่เหมาะสม และครอบคลุมความเสี่ยงด้าน IT ที่เกี่ยวข้อง เช่น ความเสี่ยงด้านภัยคุกคามทางไซเบอร์ที่เกิดจากช่องทางเว็บไซต์ อีเมล หรือการใช้เทคโนโลยีระบบคลาวด์ และความเสี่ยงด้านการรั่วไหลของข้อมูลที่อยู่ในรูปแบบอิเล็กทรอนิกส์ เป็นต้น รวมทั้งเห็นควรเพิ่มเติมนิยาม “เทคโนโลยีเพื่อการติดต่อและให้บริการแก่ลูกค้า” ในส่วนแนบท้ายของประกาศ ที่ สธ. 38/2565 ภาคผนวก 1 คำศัพท์ เพื่อให้เกิดความเข้าใจและการถือปฏิบัติที่ตรงตามเจตนารมณ์ของประกาศที่ สธ. 38/2565

3.2 การปรับปรุงข้อกำหนดสำหรับผู้ประกอบธุรกิจที่เป็นสาขาของธนาคารพาณิชย์ต่างประเทศ

ปรับปรุงข้อกำหนด ดังนี้

ข้อกำหนดปัจจุบัน	หลักการที่เสนอ
ภาคผนวก 1 [ไม่มีการกำหนดนิยามเรื่องนี้]	<u>เพิ่มเติมนิยาม</u> “สาขาของธนาคารพาณิชย์ต่างประเทศ” หมายความว่า สาขาของธนาคารพาณิชย์ต่างประเทศ ที่ได้รับอนุญาตให้ประกอบธุรกิจธนาคารพาณิชย์ในประเทศไทย
ภาคผนวก 2 ข้อ 1.6 1.6 การติดตาม ตรวจสอบ และรายงานผลการปฏิบัติงานเพื่อให้เป็นไปตามนโยบายในข้อ 1.3 ต่อคณะกรรมการของผู้ประกอบธุรกิจ โดยมีการรายงานอย่างน้อยปีละ 1 ครั้ง และในกรณีที่มีเหตุการณ์ หรือการเปลี่ยนแปลงใด ๆ ซึ่งอาจส่งผลกระทบอย่างมีนัยสำคัญต่อการปฏิบัติงานเพื่อให้เป็นไปตามนโยบายดังกล่าว ต้องมีการรายงานให้คณะกรรมการของผู้ประกอบธุรกิจทราบโดยไม่ชักช้าด้วย	<u>ปรับปรุงข้อกำหนด ดังนี้</u> 1.6 การติดตาม ตรวจสอบ และรายงานผลการปฏิบัติงานเพื่อให้เป็นไปตามนโยบายในข้อ 1.3 ต่อคณะกรรมการของผู้ประกอบธุรกิจ **<u>หรือคณะกรรมการที่ได้รับมอบหมายอย่างเป็นลายลักษณ์อักษรจากคณะกรรมการของผู้ประกอบธุรกิจเฉพาะกรณีเป็นสาขาของธนาคารพาณิชย์ต่างประเทศ</u>** โดยมีการรายงานอย่างน้อยปีละ 1 ครั้ง และในกรณีที่มีเหตุการณ์หรือการเปลี่ยนแปลงใด ๆ ซึ่งอาจส่งผลกระทบอย่างมีนัยสำคัญต่อการปฏิบัติงานเพื่อให้เป็นไปตามนโยบายดังกล่าว ต้องมีการรายงานให้คณะกรรมการของผู้ประกอบธุรกิจ **<u>หรือคณะกรรมการที่ได้รับมอบหมายอย่างเป็นลายลักษณ์อักษรจากคณะกรรมการของผู้ประกอบธุรกิจ เฉพาะกรณีเป็นสาขาของธนาคารพาณิชย์ต่างประเทศ</u>** โดยไม่ชักช้าด้วย
ภาคผนวก 4 ข้อ 5 5.1 เสนอรายงานผลการตรวจสอบตามข้อ 3. และแผนการปรับปรุงแก้ไขข้อบกพร่องต่อคณะกรรมการของผู้ประกอบธุรกิจหรือคณะกรรมการ	<u>ปรับปรุงข้อกำหนด ดังนี้</u> 5.1 เสนอรายงานผลการตรวจสอบตามข้อ 3. และแผนการปรับปรุงแก้ไขข้อบกพร่องต่อคณะกรรมการของผู้ประกอบธุรกิจ หรือคณะกรรมการตรวจสอบของผู้ประกอบธุรกิจ **<u>หรือคณะกรรมการที่ได้รับมอบหมายอย่างเป็นลายลักษณ์อักษรจาก</u>**

ข้อกำหนดปัจจุบัน	หลักการที่เสนอ
ตรวจสอบของผู้ประกอบธุรกิจโดยไม่ชักช้า 5.2 รายงานผลการตรวจสอบและแผนการปรับปรุงแก้ไขข้อบกพร่องที่ผ่านการพิจารณาจากคณะกรรมการของผู้ประกอบธุรกิจหรือคณะกรรมการตรวจสอบของผู้ประกอบธุรกิจตามข้อ 5.1 ต่อสำนักงานตามรูปแบบและวิธีการที่กำหนดไว้บนเว็บไซต์ของสำนักงาน ภายในระยะเวลา ...	**คณะกรรมการของผู้ประกอบธุรกิจเฉพาะกรณีเป็นสาขาของธนาคารพาณิชย์ต่างประเทศ** โดยไม่ชักช้า 5.2 รายงานผลการตรวจสอบและแผนการปรับปรุงแก้ไขข้อบกพร่องที่ผ่านการพิจารณาจากคณะกรรมการของผู้ประกอบธุรกิจหรือคณะกรรมการตรวจสอบของผู้ประกอบธุรกิจ **หรือคณะกรรมการที่ได้รับมอบหมายอย่างเป็นลายลักษณ์อักษรจากคณะกรรมการของผู้ประกอบธุรกิจเฉพาะกรณีเป็นสาขาของธนาคารพาณิชย์ต่างประเทศ** ตามข้อ 5.1 ต่อสำนักงานตามรูปแบบและวิธีการที่กำหนดไว้บนเว็บไซต์ของสำนักงาน ภายในระยะเวลา ...

เหตุผล: เนื่องด้วยผู้ประกอบธุรกิจ ซึ่งเป็นสาขาของธนาคารพาณิชย์ต่างประเทศมิได้มีการจดทะเบียนเป็นบริษัทมหาชนจำกัด จึงไม่มีสถานะเป็นนิติบุคคลแยกต่างหากจากธนาคารพาณิชย์ต่างประเทศ และไม่มีการจัดตั้งคณะกรรมการในประเทศไทย จึงอาจทำให้มีข้อจำกัดในการรายงานผลการตรวจสอบและแผนการปรับปรุงข้อบกพร่องต่อคณะกรรมการที่ดำรงตำแหน่งอยู่ที่สำนักงานใหญ่ต่างประเทศ (oversea headquarters) หรืออาจทำให้เกิดการพิจารณาที่ไม่ทันต่อความเสี่ยง และระยะเวลาการนำส่งรายงานต่อสำนักงานตามที่ประกาศ ที่ สธ. 38/2565 กำหนด

ดังนั้น เพื่อให้ผู้ประกอบธุรกิจ ซึ่งเป็นสาขาของธนาคารพาณิชย์ต่างประเทศสามารถปฏิบัติตามประกาศ ที่ สธ. 38/2565 ได้อย่างครบถ้วนและสอดคล้องกับการดำเนินการในทางปฏิบัติมากยิ่งขึ้น โดยยังคงไว้ซึ่งการกำกับดูแลและบริหารจัดการตามระดับความเสี่ยงได้อย่างเหมาะสม จึงเสนอให้มีการปรับปรุงประกาศ ที่ สธ. 38/2565 ให้เหมาะสมกับแนวทางปฏิบัติมากขึ้น

3.3 การตรวจสอบด้านเทคโนโลยีสารสนเทศ

ยกเลิกข้อกำหนดให้ผู้ประกอบธุรกิจที่มีขนาดเล็ก และผู้ประกอบธุรกิจที่มีระดับความเสี่ยงต่ำ ดำเนินการตรวจสอบด้าน IT อย่างน้อยปีละ 1 ครั้ง และให้ดำเนินการ ดังนี้

(1) ให้ผู้ประกอบธุรกิจที่มีขนาดเล็ก จัดให้มีการตรวจสอบด้าน IT ที่ครอบคลุมประกาศ ที่ สธ. 38/2565 ทั้งหมดที่บังคับใช้กับผู้ประกอบธุรกิจที่มีขนาดเล็ก อย่างน้อยทุก 3 ปี

ในรอบปีที่สำนักงานกำหนด หรือเมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยของระบบ IT อย่างมีนัยสำคัญ[1] (ตามรูปที่ 1)

ทั้งนี้ ในกรณีที่สำนักงานเห็นว่าจำเป็นหรือสมควร สำนักงานอาจสั่งให้ผู้ประกอบธุรกิจดำเนินการตรวจสอบด้าน IT เพิ่มเติมจากการตรวจสอบตามรอบที่ประกาศที่ สธ. 38/2565 กำหนด และให้รายงานผลการตรวจสอบให้สำนักงานทราบได้

(2) ให้ผู้ประกอบธุรกิจที่มีระดับความเสี่ยงต่ำ จัดให้มีการตรวจสอบด้าน IT ที่ครอบคลุมประกาศ ที่ สธ. 38/2565 ทั้งหมดที่บังคับใช้กับผู้ประกอบธุรกิจที่มีระดับความเสี่ยงต่ำอย่างน้อย ทุก 3 ปี ในรอบปีที่สำนักงานกำหนด หรือเมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยของระบบ IT อย่างมีนัยสำคัญ (ตามรูปที่ 1)

ทั้งนี้ ในกรณีที่สำนักงานเห็นว่าจำเป็นหรือสมควร สำนักงานอาจสั่งให้ผู้ประกอบธุรกิจดำเนินการตรวจสอบด้าน IT เพิ่มเติมจากการตรวจสอบตามรอบที่ประกาศที่ สธ. 38/2565 กำหนด และให้รายงานผลการตรวจสอบให้สำนักงานทราบ

		2568	2569	2570	2571	2572	2573	2574
สธ.38/2565	ความเสี่ยงสูง/ปานกลาง	Full	Full	Full	Full	Full	Full	Full
	ความเสี่ยงต่ำ/ขนาดเล็ก	Full	Partial	Full	Partial	Full	Partial	Full
หลักการที่เสนอ	ความเสี่ยงสูง/ปานกลาง	Full	Full	Full	Full	Full	Full	Full
	ความเสี่ยงต่ำ/ขนาดเล็ก	Full			Full			Full
	ความเสี่ยงต่ำ/ขนาดเล็ก (เกิด incident)	Full	Full เนื่องจากเกิด major incident		Full		Full เนื่องจากเกิด major incident	Full

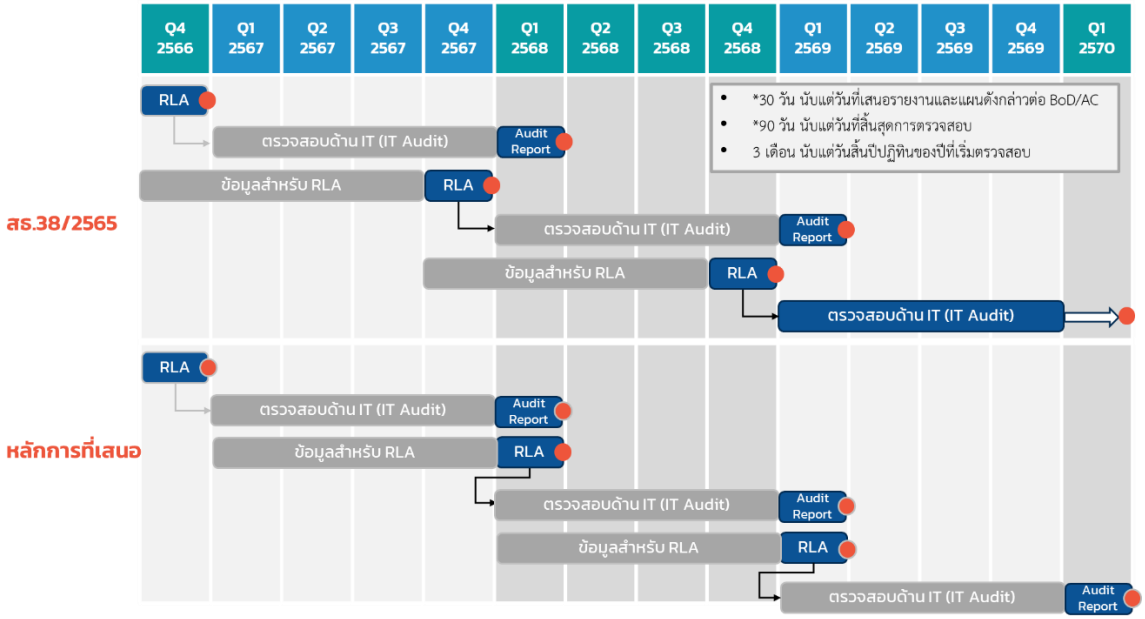
รูปที่ 1 การตรวจสอบด้าน IT ของผู้ประกอบธุรกิจแต่ละระดับความเสี่ยง ตามผลการประเมินแบบ Risk Level Assessment (“RLA”)

เหตุผล: เพื่อปรับปรุงให้รอบการจัดให้มีการตรวจสอบด้าน IT เหมาะสมกับระดับความเสี่ยงของผู้ประกอบธุรกิจมากยิ่งขึ้น โดยยังคงมีมาตรการรักษาความมั่นคงปลอดภัยของระบบ IT อย่างเพียงพอ

[1] เหตุการณ์ด้านความมั่นคงปลอดภัยของระบบ IT อย่างมีนัยสำคัญ ครอบคลุมถึง เหตุการณ์ที่เกี่ยวกับภัยคุกคามทางไซเบอร์ (cyber incident) และเหตุการณ์ที่ไม่เกี่ยวกับภัยคุกคามทางไซเบอร์ (non-cyber incident) ซึ่งส่งผลกระทบต่อทรัพย์สิน หรือข้อมูลของลูกค้าในวงกว้าง

3.4 การจัดส่งรายงานผลการตรวจสอบด้านเทคโนโลยีสารสนเทศ

กำหนดให้ผู้ประกอบธุรกิจรายงานผลการตรวจสอบด้าน IT และแผนการปรับปรุงแก้ไขข้อบกพร่องที่ผ่านการพิจารณาจากคณะกรรมการของผู้ประกอบธุรกิจ[2] หรือคณะกรรมการตรวจสอบของผู้ประกอบธุรกิจต่อสำนักงานตามรูปแบบและวิธีการที่กำหนดไว้บนเว็บไซต์ของสำนักงาน ภายใน 3 เดือน นับแต่วันสิ้นปีปฏิทินของรอบการตรวจสอบ (ตามรูปที่ 2)



รูปที่ 2 การจัดส่งแบบ RLA และรายงานผลการตรวจสอบด้าน IT

<u>เหตุผล</u>: ตามประกาศ ที่ สธ. 38/2565 ปัจจุบัน ผู้ประกอบธุรกิจต้องจัดส่งรายงานผลการตรวจสอบด้าน IT ต่อสำนักงานภายในระยะเวลาที่กำหนด โดยคำนึงถึง 3 เงื่อนไข ดังนี้

(1) 30 วัน นับแต่วันที่เสนอรายงานและแผนดังกล่าวต่อคณะกรรมการของผู้ประกอบธุรกิจหรือคณะกรรมการตรวจสอบของผู้ประกอบธุรกิจ

(2) 90 วัน นับแต่วันที่สิ้นสุดการตรวจสอบ

(3) 3 เดือน นับแต่วันสิ้นปีปฏิทินของปีที่เริ่มตรวจสอบ กรณีที่ไม่สามารถจัดทำรายงานผลการตรวจสอบให้เสร็จสิ้นภายในปีที่เริ่มการตรวจสอบ

---

[2] คณะกรรมการที่ได้รับมอบหมายอย่างเป็นลายลักษณ์อักษรจากคณะกรรมการของผู้ประกอบธุรกิจเฉพาะกรณีเป็นสาขาของธนาคารพาณิชย์ต่างประเทศ (ภายหลังมีการปรับปรุงประกาศที่ สธ. 38/2565)

ซึ่งการมีเงื่อนไขในการรายงานหลายส่วน อาจส่งผลกระทบต่อความเข้าใจในการปฏิบัติตามประกาศ ที่ สธ. 38/2565 และอาจนำไปสู่การปฏิบัติที่ไม่เป็นไปตามที่ประกาศที่ สธ. 38/2565 กำหนดโดยมิได้เจตนา ดังนั้น จึงปรับปรุงข้อกำหนดตามหลักการที่เสนอ

3.5 การจัดส่งแบบ RLA

ปรับปรุงรอบการจัดส่งแบบ RLA โดยกำหนดให้จัดส่งผลการประเมินดังกล่าวต่อสำนักงาน ภายในไตรมาสที่ 1 ของทุกปีปฏิทิน โดยข้อมูลที่ใช้ประเมินได้มาจากข้อมูลระหว่างวันที่ 1 มกราคม ถึง 31 ธันวาคม ของปีก่อนหน้าปีที่ต้องนำส่ง รายละเอียดตามรูปที่ 2 ข้างต้น

<u>เหตุผล</u>: เพื่อให้ผู้ประกอบธุรกิจสามารถปฏิบัติตามประกาศ ที่ สธ. 38/2565 ได้อย่างถูกต้อง ลดปัญหาความเข้าใจคลาดเคลื่อน และลดโอกาสที่อาจมีการนำส่งรายงานล่าช้าหรือปฏิบัติไม่ชอบตามประกาศ ที่ สธ. 38/2565 โดยให้ดำเนินการจัดส่งข้อมูลทั้งแบบ RLA และรายงานผลการตรวจสอบด้าน IT ในช่วงเวลาเดียวกัน ดังนั้น ในช่วงไตรมาส 1 ของแต่ละปี ผู้ประกอบธุรกิจจะมีหน้าที่ (1) จัดส่งรายงานผลการตรวจสอบด้าน IT ของปีก่อนหน้า และ (2) จัดส่งแบบ RLA ของปีปัจจุบัน

3.6 การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศสำหรับผู้ประกอบธุรกิจที่มีขนาดเล็ก

(1) การทดสอบการเจาะระบบ (penetration test)

กำหนดให้ผู้ประกอบธุรกิจที่มีขนาดเล็กจัดให้มีการทดสอบการเจาะระบบ (penetration test) บนระบบงาน (application system) และระบบเครือข่ายที่มีการเชื่อมต่อกับเครือข่ายสาธารณะ (internet facing) อย่างน้อยทุก 3 ปี และทุกครั้งที่มีการเปลี่ยนแปลงระบบดังกล่าวอย่างมีนัยสำคัญ[3]

<u>เหตุผล</u>: โดยทั่วไป ผู้ประกอบธุรกิจที่มีขนาดเล็กมีการพึ่งพาเทคโนโลยีจำนวนน้อย เพื่อการประกอบธุรกิจ เช่น มีเพียงการใช้งานเว็บไซต์ที่เป็นรูปแบบ static เพื่อใช้ในการแสดงข้อมูลบริการหรือผลิตภัณฑ์ทั่วไปแก่นักลงทุน โดยไม่รองรับการตอบโต้กับผู้ใช้งาน เป็นต้น ส่งผลให้ความเสี่ยงด้านความมั่นคงปลอดภัยด้าน IT ของผู้ประกอบธุรกิจที่มีขนาดเล็ก อยู่ในระดับ

---

[3] ผู้ประกอบธุรกิจสามารถพิจารณา “ความมีนัยสำคัญ” โดยคำนึงถึงกรอบหลักการของความเสี่ยง (inherent risk) และผลกระทบต่อการให้บริการหรือดำเนินธุรกิจในวงกว้าง (enterprise-wide impact) โดยยังไม่นำมาตรการควบคุม (controls) มาประกอบการพิจารณาความเสี่ยงนั้น ทั้งนี้ ตัวอย่างของการเปลี่ยนแปลงระบบที่มีนัยสำคัญ เช่น การเปลี่ยนโครงสร้างพื้นฐานจาก on-premise เป็นระบบคลาวด์ การนำระบบงานใหม่มาใช้งาน และการเปลี่ยนแปลงระบบที่มีผลต่อความมั่นคงปลอดภัย เป็นต้น

ที่น้อยกว่าผู้ประกอบธุรกิจประเภทอื่น ๆ ดังนั้น การปรับปรุงรอบการจัดทำการทดสอบการเจาะระบบดังกล่าว จะทำให้การทดสอบการเจาะระบบมีความเหมาะสมกับความเสี่ยงสำหรับผู้ประกอบธุรกิจที่มีขนาดเล็ก

(2) การควบคุมการเข้าถึงข้อมูลและระบบ IT (access control)

กำหนดให้ผู้ประกอบธุรกิจที่มีขนาดเล็กจัดให้มีการควบคุมการเข้าถึงข้อมูลและระบบ IT (access control) เทียบเท่ากับผู้ประกอบธุรกิจระดับความเสี่ยงอื่น ๆ โดยไม่จำกัดเฉพาะการควบคุมเพียงแค่บัญชี privileged user (privileged user management)

<u>เหตุผล</u>: เพื่อลดความเสี่ยงของการเข้าถึงข้อมูลและระบบ รวมถึงการเปลี่ยนแปลงแก้ไขค่าต่าง ๆ โดยผู้ไม่มีสิทธิหรือไม่ได้รับอนุญาต ซึ่งความเสี่ยงดังกล่าวอาจเกิดจากการขาดการควบคุมบัญชีในระดับผู้ใช้งาน (พนักงาน และลูกค้า) ที่ไม่มีประสิทธิภาพ

(3) การบริหารจัดการเหตุการณ์ผิดปกติด้าน IT

กำหนดให้ผู้ประกอบธุรกิจที่มีขนาดเล็กจัดให้มีการดำเนินการดังนี้ กรณีที่เกิดเหตุการณ์ผิดปกติด้าน IT

ก. วิเคราะห์สาเหตุที่แท้จริง (root cause) ของเหตุการณ์ผิดปกติด้าน IT เพื่อกำหนดแนวทางการแก้ไขและป้องกันไม่ให้เกิดเหตุการณ์ซ้ำในอนาคต

ข. บันทึกข้อมูลที่เกี่ยวข้องกับการบริหารจัดการเหตุการณ์ผิดปกติด้าน IT และจัดเก็บข้อมูลดังกล่าวเป็นระยะเวลาไม่น้อยกว่า 2 ปี นับแต่วันที่เกิดเหตุการณ์นั้น โดยต้องจัดเก็บไว้ในลักษณะที่พร้อมให้สำนักงานสามารถเรียกดูและตรวจสอบได้โดยไม่ชักช้า

<u>เหตุผล</u>: เพื่อให้ผู้ประกอบธุรกิจที่มีขนาดเล็กมีการดำเนินการเมื่อเกิดเหตุการณ์ผิดปกติด้าน IT ที่เหมาะสม และสามารถป้องกันการเกิดเหตุการณ์ซ้ำในอนาคตได้อย่างมีประสิทธิผล

3.7 การแก้ไขรายละเอียดอื่น ๆ ของประกาศ ที่ สธ. 38/2565

ข้อกำหนดปัจจุบัน	ข้อกำหนดที่เสนอ
ภาคผนวก 1 คำศัพท์ บุคคลภายนอก (third party) หมายถึง บุคคลภายนอกที่มีความเกี่ยวข้องกับผู้ประกอบธุรกิจดังนี้ แต่ไม่รวมถึงลูกค้าที่ใช้บริการหรือผลิตภัณฑ์ของผู้ประกอบธุรกิจ	<u>ปรับปรุงข้อกำหนด ดังนี้</u> บุคคลภายนอก (third party) หมายถึง บุคคลภายนอกที่มีความเกี่ยวข้องกับผู้ประกอบธุรกิจดังนี้ แต่ไม่รวมถึงลูกค้าที่ใช้บริการหรือผลิตภัณฑ์ของผู้ประกอบธุรกิจ

ข้อกำหนดปัจจุบัน	ข้อกำหนดที่เสนอ
(1) ผู้ให้บริการงานด้าน IT (2) ผู้ที่มีการเชื่อมต่อกับระบบ IT ของผู้ประกอบธุรกิจ (3) ผู้ที่สามารถเข้าถึงข้อมูลสำคัญของผู้ประกอบธุรกิจหรือข้อมูลของลูกค้า**ที่อยู่ภายใต้การควบคุมดูแลของผู้ประกอบธุรกิจ**	(1) ผู้ให้บริการงานด้าน IT (2) ผู้ที่มีการเชื่อมต่อกับระบบ IT ของผู้ประกอบธุรกิจ (3) ผู้ที่สามารถเข้าถึงข้อมูลสำคัญของผู้ประกอบธุรกิจหรือข้อมูลของลูกค้า**ที่อยู่ในรูปแบบอิเล็กทรอนิกส์** เหตุผล: เพื่อให้ตรงตามเจตนารมณ์ของประกาศที่ สธ. 38/2565 และมีความชัดเจนในการนำไปปฏิบัติมากยิ่งขึ้น
ภาคผนวก 1 คำศัพท์ [ไม่มีการกำหนดนิยามเรื่องนี้]	เพิ่มเติมนิยาม “เทคโนโลยีเพื่อการติดต่อและให้บริการแก่ลูกค้า” หมายความว่า “เทคโนโลยีหรือคอมพิวเตอร์ ที่ใช้ในการติดต่อลูกค้า การจัดทำหรือนำส่งข้อมูลบริการและผลิตภัณฑ์ให้แก่ลูกค้า รวมทั้งการใช้งานเพื่อประมวลผล วิเคราะห์ ออกผลลัพธ์หรือคำแนะนำเพื่อให้ลูกค้าใช้ประกอบการตัดสินใจลงทุน” เหตุผล: เพื่อให้ตรงตามเจตนารมณ์ของประกาศที่ สธ. 38/2565 และมีความชัดเจนในการนำไปปฏิบัติมากยิ่งขึ้น
ภาคผนวก 3 ข้อ 2.2 (7) รักษาความมั่นคงปลอดภัยด้าน IT จากการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอกที่สอดคล้องกับ**มาตรฐาน**การรักษาความมั่นคงปลอดภัยด้าน IT ของผู้ประกอบธุรกิจ	ปรับปรุงข้อกำหนด ดังนี้ (7) รักษาความมั่นคงปลอดภัยด้าน IT จากการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก ที่สอดคล้องกับการรักษาความมั่นคงปลอดภัยด้าน IT ของผู้ประกอบธุรกิจ**หรือสอดคล้องกับมาตรฐานสากลที่ได้รับการยอมรับโดยทั่วไป** เหตุผล: ในบางกรณี ผู้ประกอบธุรกิจอาจมีข้อจำกัดในการกำหนดให้บุคคลภายนอกปฏิบัติตามมาตรฐาน

ข้อกำหนดปัจจุบัน	ข้อกำหนดที่เสนอ
	การรักษาความมั่นคงปลอดภัยด้าน IT ของตน จึงปรับปรุงข้อกำหนดให้รองรับกรณีบุคคลภายนอกมีมาตรการรักษาความมั่นคงปลอดภัยด้าน IT ที่ได้มาตรฐานสากลที่ได้รับการยอมรับโดยทั่วไป
ภาคผนวก 3 ข้อ 8.4 การรักษาความมั่นคงปลอดภัยของเครื่องแม่ข่าย (server) และอุปกรณ์ที่ใช้ปฏิบัติงาน (endpoint) เพื่อไม่ให้ถูกใช้เป็นช่องทางที่ทำให้ข้อมูลสำคัญรั่วไหล หรือมีการเข้าใช้งานระบบ IT โดยไม่ได้รับอนุญาต	ปรับปรุงข้อกำหนด ดังนี้ การรักษาความมั่นคงปลอดภัยของเครื่องแม่ข่าย (server) และอุปกรณ์ที่ใช้ปฏิบัติงาน (endpoint) **ให้สามารถป้องกันการโจมตีด้วยรูปแบบต่าง ๆ หรือภัยจากโปรแกรมไม่ประสงค์ดี (malware)** เพื่อไม่ให้ถูกใช้เป็นช่องทางที่ทำให้ข้อมูลสำคัญรั่วไหล หรือมีการเข้าใช้งานระบบ IT โดยไม่ได้รับอนุญาต เหตุผล: ขยายความให้ชัดเจนขึ้น
ภาคผนวก 3 ข้อ 8.8 การติดตามดูแลระบบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (security monitoring) โดยมีกระบวนการหรือเครื่องมือป้องกันและตรวจจับเหตุการณ์ผิดปกติด้าน IT **โปรแกรมไม่ประสงค์ดี (malware)** หรือภัยคุกคามทางไซเบอร์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยต่อระบบ IT ที่มีนัยสำคัญ	ปรับปรุงข้อกำหนด ดังนี้ การติดตามดูแลระบบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (security monitoring) โดยมีกระบวนการหรือเครื่องมือป้องกันและตรวจจับเหตุการณ์ผิดปกติด้าน IT หรือภัยคุกคามทางไซเบอร์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยต่อระบบ IT ที่มีนัยสำคัญ เหตุผล: เพื่อลดความซ้ำซ้อน เนื่องจากการตรวจจับโปรแกรมไม่ประสงค์ดีจะถูกกล่าวถึงในเรื่องการรักษาความมั่นคงปลอดภัยของเครื่องแม่ข่าย (server) และอุปกรณ์ที่ใช้ปฏิบัติงาน (endpoint) แล้ว

ภาคผนวก 3 ข้อ 11.3 รายงานเหตุการณ์ผิดปกติด้าน IT เหตุการณ์การละเมิดต่อข้อมูลส่วนบุคคล และเหตุการณ์ที่ส่งผลให้ทรัพย์สินของ**ผู้ใช้งาน**สูญหายหรือเสียหายอันเกิดจากเหตุการณ์ด้านความมั่นคงปลอดภัยของระบบ IT ต่อผู้มีหน้าที่รับผิดชอบเหตุการณ์ และสำนักงาน โดยไม่ชักช้าเมื่อทราบเหตุการณ์ดังกล่าว	ปรับปรุงข้อกำหนด ดังนี้ รายงานเหตุการณ์ผิดปกติด้าน IT เหตุการณ์การละเมิดต่อข้อมูลส่วนบุคคล และเหตุการณ์ที่ส่งผลให้ทรัพย์สินของ**ลูกค้า**สูญหายหรือเสียหาย อันเกิดจากเหตุการณ์ด้านความมั่นคงปลอดภัยของระบบ IT ต่อผู้มีหน้าที่รับผิดชอบเหตุการณ์ และสำนักงาน ก.ล.ต. โดยไม่ชักช้าเมื่อทราบเหตุการณ์ดังกล่าว เหตุผล: เพื่อให้ตรงตามเจตนารมณ์ของประกาศที่ สธ. 38/2565 และมีความชัดเจนในการนำไปปฏิบัติมากยิ่งขึ้น

3.8 การแก้ไขแนวปฏิบัติในการจัดให้มีระบบเทคโนโลยีสารสนเทศ

ปรับปรุงแนวปฏิบัติให้สอดคล้องกับประกาศ ที่ สธ. 38/2565 ที่เปลี่ยนแปลงไปตามข้อ 3.1 – 3.7 และแนวปฏิบัติอื่น ๆ ดังนี้

แนวปฏิบัติปัจจุบัน	แนวปฏิบัติที่เสนอ
ภาคผนวก 2 ข้อ 1.5 การสร้างความรู้และความตระหนักด้านความเสี่ยงด้าน IT แก่กรรมการและบุคลากรอย่างต่อเนื่องและมีประสิทธิผล [ไม่มีการกำหนดแนวปฏิบัติเรื่องนี้]	เพิ่มเติมแนวปฏิบัติ “คณะกรรมการของผู้ประกอบธุรกิจควรได้รับการอบรมให้ความรู้ด้าน IT อย่างเพียงพอตามระยะเวลาที่เหมาะสม เพื่อให้เท่าทันกับภัยคุกคามใหม่และสภาพแวดล้อมด้าน IT ที่เปลี่ยนแปลงไป” เหตุผล: เพื่อให้คณะกรรมการของผู้ประกอบธุรกิจมีความรู้และความตระหนักต่อภัยคุกคามใหม่ และสภาพแวดล้อมด้าน IT ที่เปลี่ยนแปลงไป และสามารถกำกับดูแลความเสี่ยงด้าน IT ขององค์กรเป็นไปอย่างมีประสิทธิภาพ

แนวปฏิบัติปัจจุบัน	แนวปฏิบัติที่เสนอ
ภาคผนวก 2 ข้อ 2.3.2 การกำหนดขั้นตอนและวิธีปฏิบัติงานให้เป็นไปตามนโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้าน IT 2. ผู้ประกอบธุรกิจควรกำหนดวิธีปฏิบัติสำหรับการอนุมัติยกเว้น (exception) กรณีที่มีความจำเป็นให้ไม่สามารถปฏิบัติตามขั้นตอนและวิธีปฏิบัติงานที่ผู้ประกอบธุรกิจกำหนดไว้ โดยจัดให้มีการประเมินความเสี่ยง ควบคุมความเสี่ยงอย่างเพียงพอเหมาะสม และขออนุมัติยกเว้นจากผู้มีอำนาจก่อนดำเนินการต่อไป พร้อมนี้ ควรจัดเก็บหลักฐานการอนุมัติยกเว้นดังกล่าวอย่างเป็นลายลักษณ์อักษร	<u>เพิ่มเติมข้อความ</u> “ทั้งนี้ การกำหนดผู้มีอำนาจในการอนุมัติยกเว้น (exception) บุคคลดังกล่าวต้องไม่ก่อให้เกิดความขัดแย้งทางผลประโยชน์ (conflict of interest) และต้องปฏิบัติตามหลักการบริหารจัดการความเสี่ยงที่ดี (good governance)” <u>เหตุผล</u>: เพื่อให้หลักการการอนุมัติยกเว้นมีความชัดเจนมากยิ่งขึ้น และสอดคล้องกับหลักการแนวทางการกำกับดูแลที่ดี โดยผู้ที่มีอำนาจอนุมัติยกเว้นไม่ควรเป็นบุคคลที่ปฏิบัติหน้าที่โดยตรงกับการบริหารจัดการด้าน IT (first line of defense) ซึ่งจะช่วยให้ผู้ประกอบธุรกิจสามารถกำกับดูแลความเสี่ยงขององค์กรได้อย่างมีประสิทธิผล
ภาคผนวก 3 ข้อ 2.2 (3) กำหนดบทบาท หน้าที่ และความรับผิดชอบของผู้ประกอบธุรกิจและบุคคลภายนอกอย่างชัดเจนและเป็นลายลักษณ์อักษร 1. ผู้ประกอบธุรกิจควรจัดทำสัญญาหรือข้อตกลงการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอกเป็นลายลักษณ์อักษร โดยมีการลงนามร่วมกันระหว่างผู้ประกอบธุรกิจและบุคคลภายนอก เพื่อให้มั่นใจได้ว่า	<u>ปรับปรุงแนวปฏิบัติ ดังนี้</u> 1. ผู้ประกอบธุรกิจควรจัดทำสัญญาหรือข้อตกลงการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอกเป็นลายลักษณ์อักษร โดยมีการลงนามร่วมกันระหว่างผู้ประกอบธุรกิจและบุคคลภายนอก เพื่อให้มั่นใจได้ว่าบุคคลภายนอกมีหน้าที่รับผิดชอบในการรักษาความมั่นคงปลอดภัย

แนวปฏิบัติปัจจุบัน	แนวปฏิบัติที่เสนอ
บุคคลภายนอกมีหน้าที่รับผิดชอบในการรักษาความมั่นคงปลอดภัยของระบบ IT ในระดับที่เหมาะสม โดยมีรายละเอียดสอดคล้องกับความเสี่ยง และความมีนัยสำคัญของบุคคลภายนอก ดังนี้	ของระบบ IT ในระดับที่เหมาะสม โดยมีรายละเอียดสอดคล้องกับความเสี่ยง และความมีนัยสำคัญของบุคคลภายนอก ดังนี้
...	...
(4) ข้อตกลงระดับการให้บริการด้าน IT (service level agreement : SLA) สำหรับการใช้บริการจากบุคคลภายนอก	(4) ข้อตกลงระดับการให้บริการด้าน IT (service level agreement : SLA) สำหรับการใช้บริการจากบุคคลภายนอก **และความรับผิดชอบต่อความเสียหายที่เกิดจากบุคคลภายนอก เช่น กรณีการให้บริการไม่เป็นไปตาม SLA ที่กำหนดไว้ เป็นต้น**
...	...
(9) การจัดให้มีแผนฉุกเฉินด้าน IT (IT contingency plan) ที่สอดคล้องกับแผนฉุกเฉินด้าน IT ของผู้ประกอบธุรกิจ	**(9) การจัดให้มีระบบที่สอดรับกับแผนฉุกเฉินด้าน IT ของผู้ประกอบธุรกิจ (Recovery Point Objective (RPO) Maximum Tolerable Downtime (MTD) และ Recovery Time Objective (RTO))**
(10) ความรับผิดชอบต่อความเสียหายที่เกิดจากบุคคลภายนอก เช่น กรณีการให้บริการไม่เป็นไปตาม SLA ที่กำหนดไว้ เป็นต้น	
หากมีข้อจำกัดในการระบุรายละเอียดและกำหนดเงื่อนไขที่สำคัญลงในข้อตกลงหรือสัญญาที่ทำกับบุคคลภายนอก ผู้ประกอบธุรกิจควรมีการประเมินความเสี่ยงและพิจารณาแนวทางควบคุมความเสี่ยงที่เพียงพอเหมาะสม พร้อมทั้งขออนุมัติยกเว้น (exception) จากผู้มีอำนาจ	หากมีข้อจำกัดในการระบุรายละเอียดและกำหนดเงื่อนไขที่สำคัญลงในข้อตกลงหรือสัญญาที่ทำกับบุคคลภายนอก ผู้ประกอบธุรกิจควรมีการประเมินความเสี่ยงและพิจารณาแนวทางควบคุมความเสี่ยงที่เพียงพอเหมาะสม พร้อมทั้งขออนุมัติยกเว้น (exception) จากผู้มีอำนาจ เหตุผล: ขยายความและปรับปรุงให้ชัดเจนตามเจตนารมณ์ของประกาศ ที่ สธ. 38/2565 มากยิ่งขึ้น

แนวปฏิบัติปัจจุบัน	แนวปฏิบัติที่เสนอ
ภาคผนวก 3 ข้อ 2.2(5) การบริหารจัดการบุคคลภายนอก 1. non-disclosure agreement ควรมีรายละเอียดครอบคลุมขอบเขตความรับผิดชอบในการเก็บรักษาความลับ การไม่เปิดเผยข้อมูลโดยไม่ได้รับอนุญาต การรายงานผู้ประกอบธุรกิจเมื่อพบการรั่วไหลหรือเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต และการทำลายข้อมูลที่มีความสำคัญเมื่อสิ้นสุดข้อตกลงหรือสัญญา	<u>เพิ่มเติมข้อความ</u> “ทั้งนี้ non-disclosure agreement อาจกำหนดไว้เป็นส่วนหนึ่งของสัญญาหรือข้อตกลงกับบุคคลภายนอกได้” <u>เหตุผล</u>: ขยายความให้ชัดเจนขึ้น
ภาคผนวก 3 ข้อ 4.4 การจัดทำทะเบียนทรัพย์สินด้าน IT ประเภทข้อมูล (data inventory) ให้ครบถ้วนและเป็นปัจจุบัน 1. ผู้ประกอบธุรกิจควรจัดทำทะเบียนทรัพย์สินประเภทข้อมูล (data inventory) ให้ครบถ้วนและเป็นปัจจุบัน โดยมีตัวอย่างของรายละเอียด ดังนี้ ...	<u>เพิ่มเติมแนวปฏิบัติ</u> 1. ผู้ประกอบธุรกิจควรจัดทำทะเบียนทรัพย์สินประเภทข้อมูล (data inventory) ให้ครบถ้วนและเป็นปัจจุบัน โดยมีตัวอย่างของรายละเอียด ดังนี้ ... **<u>2. ผู้ประกอบธุรกิจควรปรับปรุงทรัพย์สินด้าน IT ประเภทข้อมูล (data inventory) ให้ครบถ้วนและเป็นปัจจุบันอยู่อย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงระบบ IT อย่างมีนัยสำคัญ</u>** <u>เหตุผล</u>: เพื่อให้ทะเบียนทรัพย์สินด้าน IT ประเภทข้อมูล มีการติดตามและปรับปรุงให้เป็นปัจจุบันอยู่เสมอ ซึ่งจะช่วยให้สามารถบริหารจัดการ

แนวปฏิบัติปัจจุบัน	แนวปฏิบัติที่เสนอ
	ความเสี่ยงของข้อมูลได้มีประสิทธิภาพมากยิ่งขึ้น พร้อมนี้ เพื่อให้สอดคล้องกับข้อกำหนดการปรับปรุงทะเบียนทรัพย์สินสารสนเทศต่าง ๆ เช่น ฮาร์ดแวร์และซอฟต์แวร์ เป็นต้น
ภาคผนวก 3 ข้อ 8.7 การจัดเก็บข้อมูลบันทึกเหตุการณ์การใช้งานเกี่ยวกับระบบ IT (log) 1. ผู้ประกอบธุรกิจควรจัดเก็บข้อมูลบันทึกเหตุการณ์ (log) ด้วยวิธีการที่ปลอดภัย โดยมีรายละเอียดครบถ้วนเพียงพอที่จะใช้เป็นหลักฐานในการตรวจสอบที่สามารถระบุตัวบุคคลผู้กระทำได้ และจัดเก็บเป็นระยะเวลาอย่างน้อย 90 วัน หรือจัดเก็บตามกฎหมายที่เกี่ยวข้องกำหนด ประกอบด้วยรายการหลักฐานอย่างน้อย ดังนี้ (1) บันทึกเหตุการณ์การเข้า-ออกศูนย์คอมพิวเตอร์ และพื้นที่ที่เกี่ยวข้องกับระบบ IT ที่มีนัยสำคัญ (physical access log) (2) บันทึก**<u>การยืนยันตัวตน</u>**และการเข้าถึง **<u>(authentication log และ access log)</u>** ของเครื่องแม่ข่าย ระบบงาน อุปกรณ์เครือข่าย และข้อมูลที่มีความสำคัญ โดยรวมถึงความพยายามใน**<u>การเข้าถึง (log-in attempt)</u>** (3) บันทึกการดำเนินงาน (activity log) ที่สำคัญ โดยอย่างน้อยครอบคลุม	<u>ปรับปรุงแนวปฏิบัติ ดังนี้</u> 1. ผู้ประกอบธุรกิจควรจัดเก็บข้อมูลบันทึกเหตุการณ์ (log) ด้วยวิธีการที่ปลอดภัย โดยมีรายละเอียดครบถ้วนเพียงพอที่จะใช้เป็นหลักฐานในการตรวจสอบที่สามารถระบุตัวบุคคลผู้กระทำได้ และจัดเก็บเป็นระยะเวลาอย่างน้อย 90 วัน หรือจัดเก็บตามกฎหมายที่เกี่ยวข้องกำหนดประกอบด้วยรายการหลักฐานอย่างน้อย ดังนี้ (1) บันทึกเหตุการณ์การเข้า-ออกศูนย์คอมพิวเตอร์และพื้นที่ที่เกี่ยวข้องกับระบบ IT ที่มีนัยสำคัญ (physical access log) (2) บันทึกการเข้าถึง **<u>(access log)</u>** ของเครื่องแม่ข่าย ระบบงาน อุปกรณ์เครือข่าย และข้อมูลที่มีความสำคัญ โดยรวมถึงความพยายามในการเข้าสู่ระบบ (log-in attempt) (3) บันทึกการดำเนินงาน (activity log) ที่สำคัญ โดยอย่างน้อยครอบคลุม

แนวปฏิบัติปัจจุบัน	แนวปฏิบัติที่เสนอ
(ก) การเปลี่ยนแปลงแก้ไขโครงสร้างข้อมูล **(ข) การเปลี่ยนแปลงแก้ไข และลบข้อมูลสำคัญ** (ค) การเปลี่ยนแปลงแก้ไขการตั้งค่าของระบบ (system configuration) (ง) การเปลี่ยนแปลงแก้ไขบัญชี และสิทธิของผู้ใช้งาน (จ) การใช้งานอินเทอร์เน็ตผ่านระบบเครือข่ายของผู้ประกอบธุรกิจ (ฉ) การทำงานของ firewall (network firewall log)	**(ก) การเปลี่ยนแปลงแก้ไขโครงสร้างฐานข้อมูลและการเปลี่ยนแปลงแก้ไขข้อมูล (update/ insert/ delete) ในตารางที่สำคัญ** (ข) การเปลี่ยนแปลงแก้ไขการตั้งค่าของระบบ (system configuration) (ค) การเปลี่ยนแปลงแก้ไขบัญชี และสิทธิของผู้ใช้งาน (ง) การใช้งานอินเทอร์เน็ตผ่านระบบเครือข่ายของผู้ประกอบธุรกิจ **(internet traffic log)** (จ) การทำงานของ firewall (network firewall log) เหตุผล: ขยายความและปรับปรุงให้ชัดเจนตามเจตนารมณ์ของประกาศ ที่ สธ. 38/2565 มากยิ่งขึ้น
ภาคผนวก 3 ข้อ 8.7 การจัดเก็บข้อมูลบันทึกเหตุการณ์การใช้งานเกี่ยวกับระบบ IT (log) (5) บันทึกการทำธุรกรรม (transaction log) ควรมีระยะเวลาจัดเก็บขั้นต่ำ 1 ปี โดยในกรณีที่เป็นระบบ IT เพื่อการซื้อขายหลักทรัพย์ (trading system) ให้บันทึก • บัญชีผู้ใช้งาน • ข้อมูลรายละเอียดชื่อย่อหลักทรัพย์ (securities symbol) • หมายเลขบริษัทสมาชิก (broker no. 4 หลัก : xxxx) • เลขที่คำสั่งซื้อขายหลักทรัพย์ (SET order ID)	ปรับปรุงแนวปฏิบัติ ดังนี้ (5) บันทึกการทำธุรกรรม (transaction log) ควรมีระยะเวลาจัดเก็บขั้นต่ำ 1 ปี โดยในกรณีที่เป็นระบบ IT เพื่อการซื้อขายหลักทรัพย์ (trading system) ให้บันทึก • บัญชีผู้ใช้งาน (user ID) **ที่ใช้ส่งคำสั่งซื้อขาย** • **เลขบัตรประจำตัวประชาชนหรือเลขทะเบียนนิติบุคคลของลูกค้า** • **ชื่อ-สกุลของลูกค้า** • หมายเลขบริษัทสมาชิก (broker no. 4 หลัก : xxxx) • เลขที่บัญชีซื้อขายหลักทรัพย์ (account no.) • ชื่อย่อหลักทรัพย์ (securities symbol)

แนวปฏิบัติปัจจุบัน	แนวปฏิบัติที่เสนอ
• 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	• เลขที่คำสั่งซื้อขายหลักทรัพย์ (SET order no.) • **วันที่ส่งคำสั่งซื้อขาย (order date : yyyy/mm/dd)** • **เวลาที่ส่งคำสั่งซื้อขาย (order time : hh:mm:ss:sss)** • **วันที่จับคู่ซื้อขายได้ (matched date : yyyy/mm/dd)** • หมายเลข public IP address ต้นทาง (client public IP) • หมายเลข public IP address ปลายทาง (destination public IP) • ที่อยู่ของเว็บไซต์ปลายทาง (full URL) • terminal type (ถ้ามี) เช่น **mobile,** iPad, iPhone, **PC** เป็นต้น • **กรณีส่งคำสั่งจากอุปกรณ์ของบริษัทหลักทรัพย์ ให้จัดเก็บข้อมูลที่สามารถระบุได้ว่า คำสั่งซื้อขายจัดส่งจากเครื่องคอมพิวเตอร์ใด และใครเป็นผู้ใช้งานเครื่องคอมพิวเตอร์ในขณะที่ส่งคำสั่งนั้น** เหตุผล: ปรับปรุง field การเก็บข้อมูลให้ชัดเจนขึ้น เพื่อรองรับการสอบทานธุรกิจในภายหลัง

3.9 การมีผลใช้บังคับ

ให้ประกาศฉบับปรับปรุงนี้ มีผลใช้บังคับตั้งแต่วันที่ 1 มกราคม 2568 เป็นต้นไป

4. ผู้เกี่ยวข้อง/บุคคลที่อาจได้รับผลกระทบ และผลกระทบที่อาจเกิดขึ้น

ผู้เกี่ยวข้อง	ผลกระทบเชิงบวก	ผลกระทบเชิงลบ
1. ผู้ประกอบธุรกิจ	• ประกาศที่ สธ. 38/2565 มีข้อกำหนดที่ชัดเจนยิ่งขึ้น ทำให้สามารถนำไปปฏิบัติได้ตามจุดประสงค์ของประกาศ ที่ สธ. 38/2565 อย่างมีประสิทธิภาพ • มีมาตรการควบคุมและบริหารจัดการด้าน IT ที่เหมาะสมและเป็นไปตามหลักการที่ดีมากยิ่งขึ้น • ลดภาระในการติดตามและควบคุมการจัดส่งแบบรายงานต่อสำนักงาน เนื่องจากมีการกำหนดวันที่ชัดเจนขึ้น • ผู้ประกอบธุรกิจที่มีขนาดเล็ก และผู้ประกอบธุรกิจระดับความเสี่ยงต่ำ: การจัดการความเสี่ยงด้าน IT ที่มีความเหมาะสมกับขนาดและระดับความเสี่ยงของผู้ประกอบธุรกิจมากยิ่งขึ้น ในขณะที่ยังคงมีมาตรการควบคุมด้านการรักษาความมั่นคงปลอดภัยด้าน IT ไว้อย่างเพียงพอ	• ผู้ประกอบธุรกิจทุกรายยังคงมีหน้าที่ในการกำกับดูแลและควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศ ตามระดับความเสี่ยงของตน • ผู้ประกอบธุรกิจที่มีขนาดเล็ก: อาจต้องมีทรัพยากรเพิ่มเติมเพื่อจัดให้มีการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (cyber hygiene) เพิ่มเติม ตามข้อ 3.6
2. สำนักงาน ก.ล.ต.	• การปรับปรุงด้านความชัดเจนในเนื้อหาของประกาศที่ สธ. 38/2565 จะช่วยให้สำนักงาน สามารถสื่อสารจุดประสงค์ของประกาศที่ สธ. 38/2565 ให้ผู้ประกอบ	• ข้อมูลผลการตรวจสอบด้าน IT ซึ่งใช้ในการวิเคราะห์ cyber landscape ของตลาดทุน สำหรับผู้ประกอบธุรกิจที่มีขนาดเล็กและผู้ประกอบธุรกิจระดับความเสี่ยงต่ำ จะไม่ได้รับ

ผู้เกี่ยวข้อง	ผลกระทบเชิงบวก	ผลกระทบเชิงลบ
	ธุรกิจมีความเข้าใจ และสามารถปฏิบัติได้เหมาะสมมากยิ่งขึ้น ● สามารถส่งเสริมให้ผู้ประกอบธุรกิจมีการบริหารจัดการด้าน IT ได้อย่างมีประสิทธิภาพมากยิ่งขึ้น ซึ่งจะเป็นการยกระดับความพร้อมด้านความมั่นคงปลอดภัยด้าน IT และเพิ่มความเชื่อมั่นต่อภาคตลาดทุนของประเทศ	การปรับปรุง (update) เป็นรายปี แต่จะปรับปรุงทุก 3 ปี จึงต้องใช้กลไกอื่น ๆ เพื่อติดตามความเสี่ยงของผู้ประกอบธุรกิจกลุ่มดังกล่าวอย่างเพียงพอ เช่น ติดตามการจัดส่งแบบ RLA ประจำปี และติดตามการรายงานเหตุการณ์ผิดปกติด้าน IT เป็นต้น

5. เหตุผลความจำเป็นของการให้มีระบบอนุญาต ระบบคณะกรรมการ หรือการกำหนดโทษอาญา รวมทั้งหลักเกณฑ์การใช้ดุลพินิจของเจ้าหน้าที่ (ถ้ามี)

หลักการที่นำมารับฟังความคิดเห็น ไม่มีการกำหนดให้มีระบบอนุญาต ระบบคณะกรรมการ หรือการกำหนดโทษอาญา และหลักเกณฑ์การใช้ดุลพินิจของเจ้าหน้าที่ขึ้นใหม่

แบบสำรวจความคิดเห็น

เรื่อง หลักการการปรับปรุงหลักเกณฑ์การจัดให้มีระบบเทคโนโลยีสารสนเทศ

ข้อมูลทั่วไป

ชื่อผู้ตอบ _____ ตำแหน่ง _____

ชื่อบริษัท/องค์กร _____

โทรศัพท์ _____ โทรสาร _____

อีเมล _____

สถานะของผู้ให้ข้อคิดเห็น (ตอบได้มากกว่า 1 ข้อ)

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

สำนักงานขอข้อมูลส่วนบุคคลของท่าน โดยมีวัตถุประสงค์เพื่อใช้พิจารณาประกอบการรับฟังความคิดเห็น และประโยชน์ในการติดต่อกลับเพื่อขอข้อมูลประกอบเอกสารรับฟังความคิดเห็นของท่านเพิ่มเติม โดยสำนักงานคำนึงถึงความสำคัญของข้อมูลและเคารพสิทธิความเป็นส่วนตัวของท่าน จึงขอให้ท่านอ่านและทำความเข้าใจนโยบายการคุ้มครองข้อมูลส่วนบุคคล privacy policy แล้วจึงพิจารณาให้ความยินยอมให้สำนักงานประมวลผลข้อมูลส่วนบุคคลของท่าน

☐ 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

ท่านเห็นด้วยหรือไม่กับหลักการการปรับปรุงหลักเกณฑ์การจัดให้มีระบบเทคโนโลยีสารสนเทศตามที่สำนักงานกำหนดมาข้างต้น

1. การปรับปรุงขอบเขตการบังคับใช้สำหรับผู้ประกอบธุรกิจการเป็นที่ปรึกษาการลงทุน	**เห็นด้วย** ☐	**ไม่เห็นด้วย** ☐
ข้อเสนอแนะ หรือข้อสังเกตเพิ่มเติม		
2. การปรับปรุงข้อกำหนดสำหรับผู้ประกอบธุรกิจที่เป็นสาขาของธนาคารพาณิชย์ต่างประเทศ	**เห็นด้วย** ☐	**ไม่เห็นด้วย** ☐
ข้อเสนอแนะ หรือข้อสังเกตเพิ่มเติม		
3. การตรวจสอบด้านเทคโนโลยีสารสนเทศ	**เห็นด้วย** ☐	**ไม่เห็นด้วย** ☐
ข้อเสนอแนะ หรือข้อสังเกตเพิ่มเติม		
4. การจัดส่งรายงานผลการตรวจสอบด้านเทคโนโลยีสารสนเทศ	**เห็นด้วย** ☐	**ไม่เห็นด้วย** ☐
ข้อเสนอแนะ หรือข้อสังเกตเพิ่มเติม		

5. การจัดส่งแบบ RLA (Risk Level Assessment)	เห็นด้วย	ไม่เห็นด้วย
	☐	☐
ข้อเสนอแนะ หรือข้อสังเกตเพิ่มเติม		
6. การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศสำหรับผู้ประกอบธุรกิจที่มีขนาดเล็ก	**เห็นด้วย**	**ไม่เห็นด้วย**
	☐	☐
ข้อเสนอแนะ หรือข้อสังเกตเพิ่มเติม		
7. การแก้ไขรายละเอียดอื่น ๆ ของประกาศ ที่ สธ. 38/2565	**เห็นด้วย**	**ไม่เห็นด้วย**
	☐	☐
ข้อเสนอแนะ หรือข้อสังเกตเพิ่มเติม (กรณีไม่เห็นด้วย โปรดระบุรายละเอียด/ข้อที่ท่านไม่เห็นด้วย)		

8. การแก้ไขแนวปฏิบัติในการจัดให้มีระบบเทคโนโลยีสารสนเทศ	เห็นด้วย	ไม่เห็นด้วย
	☐	☐
ข้อเสนอแนะ หรือข้อสังเกตเพิ่มเติม (กรณีไม่เห็นด้วย โปรดระบุรายละเอียด/ข้อที่ท่านไม่เห็นด้วย)		
9. ข้อเสนอแนะอื่น ๆ (ถ้ามี)		
ข้อเสนอแนะ หรือข้อสังเกตเพิ่มเติม		