ประกาศแนวปฏิบัติ
ที่ นป. 3/2559
เรื่อง แนวปฏิบัติในการจัดให้มีระบบเทคโนโลยีสารสนเทศ

ตามที่ประกาศคณะกรรมการกำกับตลาดทุน ที่ ทธ. 35/2556 เรื่อง มาตรฐานการประกอบธุรกิจ โครงสร้างการบริหารงาน ระบบงาน และการให้บริการของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสัญญาซื้อขายล่วงหน้า ลงวันที่ 6 กันยายน พ.ศ. 2556 (ประกาศที่ ทธ. 35/2556) และประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ที่ สธ. 37/2559 เรื่อง ข้อกำหนดในรายละเอียดเกี่ยวกับการจัดให้มีระบบเทคโนโลยีสารสนเทศ ลงวันที่ 12 กันยายน พ.ศ. 2559 (ประกาศที่ สธ. 37/2559) กำหนดให้ผู้ประกอบธุรกิจต้องจัดให้มีนโยบาย มาตรการ และระบบงานในการกำกับดูแลและบริหารจัดการเทคโนโลยี และการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ โดยต้องดำเนินการควบคุมดูแล ติดตาม และตรวจสอบให้มีการปฏิบัติตามนโยบาย มาตรการ และระบบงานดังกล่าว ตลอดจนมีการทบทวนความเหมาะสมของเรื่องดังกล่าวเป็นประจำ นั้น

เพื่อประโยชน์ในการปฏิบัติตามข้อกำหนดข้างต้นของผู้ประกอบธุรกิจ สำนักงานโดยอาศัยอำนาจตามข้อ 5(3) ประกอบกับข้อ 12 วรรคหนึ่ง (11) และ (12) และข้อ 14 ของประกาศที่ ทธ. 35/2556 จึงออกประกาศแนวปฏิบัติไว้ดังต่อไปนี้

ข้อ 1 แนวปฏิบัตินี้เป็นแนวทางเกี่ยวกับเรื่องดังต่อไปนี้

(1) การจัดให้มีนโยบาย มาตรการ และระบบงานเกี่ยวกับการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรที่ดี และระบบงานในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

(2) การควบคุมดูแล ติดตาม และตรวจสอบให้มีการปฏิบัติตามนโยบาย มาตรการ และระบบงานตาม (1)

(3) การทบทวนความเหมาะสมของ (1)

ในกรณีที่ผู้ประกอบธุรกิจได้ปฏิบัติตามแนวทางตามวรรคหนึ่งจนครบถ้วน สำนักงานจะพิจารณาว่าผู้ประกอบธุรกิจได้ปฏิบัติตามประกาศที่ ทธ. 35/2556 และประกาศที่ สธ. 37/2559 แล้ว ทั้งนี้ หากผู้ประกอบธุรกิจดำเนินการต่างจากแนวปฏิบัตินี้ ผู้ประกอบธุรกิจมีภาระที่จะต้องพิสูจน์ให้เห็นได้ว่าการดำเนินการนั้นยังคงอยู่ภายใต้หลักการและข้อกำหนดของประกาศที่ ทธ. 35/2556 ในส่วนที่เกี่ยวกับระบบเทคโนโลยีสารสนเทศ และประกาศที่ สธ. 37/2559

ข้อ 2 แนวทางปฏิบัติตามข้อ 1 วรรคหนึ่งมีรายละเอียดตามที่กำหนดในภาคผนวกที่แนบท้ายประกาศแนวปฏิบัตินี้ ทั้งนี้ รายละเอียดดังกล่าวได้แก่เรื่องดังต่อไปนี้

(1) หมวดที่ 1 การกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรที่ดี (governance of enterprise IT)

(2) หมวดที่ 2 การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ (IT security) โดยมีรายละเอียดดังต่อไปนี้

2.1 แนวทางปฏิบัติเพิ่มเติมเกี่ยวกับนโยบายและมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (information security policy)

2.2 การจัดโครงสร้างความมั่นคงปลอดภัยของระบบสารสนเทศ (organization of information security)

2.3 การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร (human resource security)

2.4 การบริหารจัดการทรัพย์สินสารสนเทศ (asset management)

2.5 การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ (access control)

2.6 การควบคุมการเข้ารหัสข้อมูล (cryptographic control)

2.7 การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม (physical and environmental security)

2.8 การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ (operations security)

2.9 การรักษาความมั่นคงปลอดภัยด้านการสื่อสารข้อมูลสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์ (communications security)

2.10 การจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศ (system acquisition, development and maintenance)

2.11 การใช้บริการระบบสารสนเทศจากผู้รับดำเนินการ (IT outsourcing)

2.12 การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (information security incident management)

2.13 การบริหารความต่อเนื่องทางธุรกิจในด้านความมั่นคงปลอดภัยของระบบสารสนเทศ (information security aspects of business continuity management)

ประกาศ ณ วันที่ 12 กันยายน พ.ศ. 2559

(นายรพี สุจริตกุล)

เลขาธิการ

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์

ภาคผนวก

บทนิยาม

“ทรัพย์สินสารสนเทศ”	หมายถึง	(1) ทรัพย์สินสารสนเทศ**ประเภทระบบ** ซึ่งได้แก่ ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ (2) ทรัพย์สินสารสนเทศ**ประเภทอุปกรณ์** ซึ่งได้แก่ ตัวเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล และอุปกรณ์อื่นใด (3) ทรัพย์สินสารสนเทศ**ประเภทข้อมูล** ซึ่งได้แก่ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์
“ทรัพย์สินสารสนเทศที่มีความสำคัญ”	หมายถึง	ทรัพย์สินสารสนเทศที่เกี่ยวข้อง หรือจำเป็นต้องใช้ประกอบกับงานที่มีความสำคัญ
“ระบบสารสนเทศที่มีความสำคัญ”	หมายถึง	ระบบสารสนเทศที่รองรับการปฏิบัติงานที่สำคัญ เช่น ระบบซื้อขาย ระบบปฏิบัติการ back office และระบบจัดการลงทุน เป็นต้น
“งานที่สำคัญ”	หมายถึง	งานที่เกี่ยวกับการให้บริการ การทำธุรกรรม หรืองานอื่น ๆ ของผู้ประกอบธุรกิจ ซึ่งหากมีการหยุดชะงัก อาจส่งผลกระทบต่อลูกค้า การดำเนินงาน ธุรกิจ ชื่อเสียง ฐานะ และผลการดำเนินงานของผู้ประกอบธุรกิจอย่างมีนัยสำคัญ
“การใช้งานอุปกรณ์เคลื่อนที่ (mobile device)”	หมายถึง	การปฏิบัติงานที่มีการใช้อุปกรณ์เคลื่อนที่เพื่อเข้าถึงระบบสารสนเทศที่มีความสำคัญโดยผ่านการเชื่อมต่อกับระบบเครือข่ายคอมพิวเตอร์ภายในของผู้ประกอบธุรกิจโดยตรง

“การปฏิบัติงานจากเครือข่ายภายนอกบริษัท (teleworking)”	หมายถึง	การปฏิบัติงานที่มีการเข้าถึงระบบสารสนเทศที่มีความสำคัญโดยไม่ผ่านการเชื่อมต่อกับระบบเครือข่ายคอมพิวเตอร์ภายในของผู้ประกอบธุรกิจโดยตรง
“cloud computing”	หมายถึง	รูปแบบการใช้งานระบบสารสนเทศร่วมกันบนระบบเครือข่ายคอมพิวเตอร์ เพื่อการประมวลผลตามความต้องการของผู้ใช้งาน ทั้งนี้ ให้อ้างอิงจากนิยามที่กำหนดโดย National Institute of Standards and Technology (NIST)
“ผู้รับดำเนินการ (outsourcee)”	หมายถึง	บุคคลจากภายนอกองค์กรซึ่งผู้ประกอบธุรกิจว่าจ้างเพื่อให้ปฏิบัติงานอย่างต่อเนื่องและต้องใช้ดุลพินิจหรือการตัดสินใจในการปฏิบัติงานดังกล่าวแทนผู้ประกอบธุรกิจ
“ผู้ใช้งาน”	หมายถึง	พนักงานของผู้ประกอบธุรกิจและบุคลากรภายนอกที่มีการปฏิบัติงานโดยมีการเข้าถึงข้อมูลลับหรือระบบงานสำคัญภายในองค์กรโดยไม่รวมถึงลูกค้า
“สิ่งอำนวยความสะดวกในการประมวลผลข้อมูล (information processing facility)”	หมายถึง	อุปกรณ์ ระบบงาน หรือสภาพแวดล้อม ที่จำเป็นหรือมีส่วนช่วยให้การประมวลผลข้อมูลเป็นไปอย่างครบถ้วนถูกต้อง และมีประสิทธิภาพ เช่น อุปกรณ์หรือโปรแกรมประมวลผลข้อมูล ระบบเครือข่ายคอมพิวเตอร์ ขั้นตอนหรือสถานที่ประมวลผลข้อมูล เป็นต้น

หมวดที่ 1 : การกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรที่ดี

(governance of enterprise IT)

วัตถุประสงค์

โดยที่ระบบเทคโนโลยีสารสนเทศเข้ามามีบทบาทสำคัญในการขับเคลื่อนธุรกิจ และถือเป็นหนึ่งในระบบงานหลักที่หากเกิดขัดข้องขึ้น จะส่งผลกระทบต่อการดำเนินงานของผู้ประกอบธุรกิจ ผู้ลงทุน และความเชื่อมั่นต่อตลาดทุนโดยรวมได้ ผู้บริหารระดับสูงจึงต้องมีบทบาทสำคัญในการบริหารจัดการการนำเทคโนโลยีสารสนเทศมาใช้ในการประกอบธุรกิจ รวมถึงมีหน้าที่ในการส่งทอดเป้าหมายตามภารกิจ กลยุทธ์ นโยบาย และแผนงานระดับองค์กรสู่เป้าหมายที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศภายใต้การกำกับดูแลของคณะกรรมการบริษัท เพื่อให้มั่นใจว่าการนำเทคโนโลยีสารสนเทศดังกล่าวมาใช้ในการประกอบธุรกิจ ช่วยให้ผู้ประกอบธุรกิจสามารถบรรลุเป้าหมายได้ตามที่กำหนดไว้ โดยมีการใช้ทรัพยากรอย่างเหมาะสม และมีการบริหารจัดการความเสี่ยงอย่างเหมาะสม สอดคล้องกับการกำกับดูแลกิจการที่ดี (corporate governance)

ข้อกำหนดในประกาศที่ สธ. 37/2559

ข้อ 5 ผู้ประกอบธุรกิจต้องจัดให้มีนโยบายเป็นลายลักษณ์อักษรในการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศอย่างน้อยในเรื่องดังต่อไปนี้ ทั้งนี้ นโยบายดังกล่าวต้องได้รับความเห็นชอบจากคณะกรรมการของผู้ประกอบธุรกิจหรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบธุรกิจ

(1) การบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ซึ่งครอบคลุมถึงการระบุความเสี่ยง การประเมินความเสี่ยง และการควบคุมความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้

(2) การจัดสรรและบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศ ซึ่งครอบคลุมถึงการจัดสรรทรัพยากรให้เพียงพอต่อการดำเนินธุรกิจ และการกำหนดแนวทางเพื่อรองรับในกรณีที่ไม่สามารถจัดสรรทรัพยากรได้เพียงพอตามที่กำหนดไว้

(3) การจัดให้มีนโยบายและมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามข้อ 8 และข้อ 9

ข้อ 6 ผู้ประกอบธุรกิจต้องจัดให้มีการกำกับดูแลและบริหารจัดการด้านเทคโนโลยีสารสนเทศตามหลักเกณฑ์ดังต่อไปนี้ ทั้งนี้ เพื่อให้เป็นไปตามนโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจที่กำหนดไว้ตามข้อ 5

(1) สื่อสารนโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศให้แก่บุคลากรของผู้ประกอบธุรกิจที่เกี่ยวข้องอย่างทั่วถึงในลักษณะที่สามารถเข้าถึงได้ง่าย เพื่อให้บุคลากรดังกล่าวเข้าใจและสามารถปฏิบัติตามนโยบายดังกล่าวได้อย่างถูกต้อง

(2) กำหนดขั้นตอนและวิธีปฏิบัติงานให้เป็นไปตามนโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศ

ข้อกำหนดในประกาศที่ สธ. 37/2559

> (3) ทบทวนหรือปรับปรุงนโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศ อย่างน้อยปีละ 1 ครั้ง โดยต้องทบทวนโดยไม่ชักช้าเมื่อมีเหตุการณ์ใด ๆ ซึ่งอาจส่งผลกระทบต่อการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศอย่างมีนัยสำคัญ และต้องปรับปรุงขั้นตอนและวิธีปฏิบัติงานให้สอดคล้องกับนโยบายที่มีการเปลี่ยนแปลงด้วย

แนวทางปฏิบัติเพิ่มเติมจากข้อกำหนด

1. นโยบายการบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศตามข้อกำหนด 5(1) ควรสอดคล้องกับนโยบายและการบริหารความเสี่ยงองค์กร (enterprise risk) และควรมีเนื้อหาขั้นต่ำ ดังนี้

(1) การระบุความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (IT-related risk)

(2) การประเมินความเสี่ยง ซึ่งครอบคลุมถึงโอกาสหรือความถี่ที่จะเกิดความเสี่ยง และความมีนัยสำคัญหรือผลกระทบที่จะเกิดขึ้น เพื่อจัดลำดับความสำคัญในการบริหารจัดการความเสี่ยง

(3) การกำหนดเครื่องมือและมาตรการในการบริหารและจัดการความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้ (risk appetite)

(4) การกำหนดตัวชี้วัดระดับความเสี่ยง (IT risk indicator) สำหรับความเสี่ยงสำคัญที่สอดคล้องกับความเสี่ยงที่ระบุตาม (1) รวมถึงจัดให้มีการติดตามและรายงานผลตัวชี้วัดดังกล่าว เพื่อให้สามารถบริหารและจัดการความเสี่ยงได้อย่างเหมาะสมและทันต่อเหตุการณ์

(5) การกำหนดหน้าที่และความรับผิดชอบของผู้รับผิดชอบ (accountable person) และผู้ทำหน้าที่ (responsible person) การบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศตามข้อกำหนด 5(1)

2. นโยบายการจัดสรรและบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศตามข้อกำหนด 5(2) ควรสอดคล้องกับแผนกลยุทธ์องค์กร เพื่อให้บรรลุเป้าหมายตามภารกิจ กลยุทธ์ นโยบายและแผนการดำเนินงานที่กำหนดไว้ และควรมีเนื้อหาขั้นต่ำ ดังนี้

(1) การกำหนดหลักเกณฑ์และปัจจัยในการกำหนดลำดับความสำคัญของแผนงานด้านเทคโนโลยีสารสนเทศ (เช่น ความเหมาะสมสอดคล้องกับแผนกลยุทธ์ของบริษัท / ผลกระทบต่อการดำเนินธุรกิจ / ความเร่งด่วนในการใช้งาน)

(2) การจัดทำและอนุมัติงบประมาณด้านเทคโนโลยีสารสนเทศที่สอดคล้องกับแผนงบประมาณและแผนกลยุทธ์องค์กร

(3) การจัดให้มีทรัพยากรบุคคลอย่างเพียงพอต่องานด้านเทคโนโลยีสารสนเทศ (เช่น การจัดให้มีหรือการพัฒนาทักษะของบุคลากร / การจัดจ้างบุคลากรด้าน IT จากภายนอก)

(4) การจัดการความเสี่ยงสำคัญในกรณีที่ไม่สามารถจัดสรรทรัพยากรได้เพียงพอต่อการดำเนินงานด้านเทคโนโลยีสารสนเทศ (เช่น กรณีบุคลากรสำคัญด้าน IT ลาออก / งบประมาณไม่เพียงพอ / ความต้องการใช้งานเกินกว่าที่กำหนดไว้ใน capacity plan)

(5) การกำหนดหน้าที่และความรับผิดชอบของผู้รับผิดชอบ (accountable person) และผู้ทำหน้าที่ (responsible person) การจัดสรรและบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศตามข้อกำหนด 5(2)

3. นโยบายและมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามข้อกำหนด 5(3) ควรมีเนื้อหาขั้นต่ำตามที่กำหนดในหมวดที่ 2 ข้อ 1 เรื่อง แนวทางปฏิบัติเพิ่มเติมเกี่ยวกับนโยบายและมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (information security policy)

4. ผู้ประกอบธุรกิจควรกำหนดให้ผู้บริหารระดับสูงเป็นผู้รับผิดชอบในการปฏิบัติให้เป็นไปตามข้อกำหนด 6(2)

ข้อกำหนดในประกาศที่ สธ. 37/2559

ข้อ 6 ผู้ประกอบธุรกิจต้องจัดให้มีการกำกับดูแลและบริหารจัดการด้านเทคโนโลยีสารสนเทศตามหลักเกณฑ์ดังต่อไปนี้ ทั้งนี้ เพื่อให้เป็นไปตามนโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจที่กำหนดไว้ตามข้อ 5

(4) จัดให้มีการรายงานการปฏิบัติตามนโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศให้คณะกรรมการของผู้ประกอบธุรกิจทราบอย่างน้อยปีละ1 ครั้ง และในกรณีที่มีเหตุการณ์ใด ๆ ซึ่งอาจส่งผลกระทบต่อการปฏิบัติตามนโยบายดังกล่าวอย่างมีนัยสำคัญ ต้องรายงานให้คณะกรรมการของผู้ประกอบธุรกิจทราบโดยไม่ชักช้าด้วย

แนวทางปฏิบัติเพิ่มเติมจากข้อกำหนด

5. ในการปฏิบัติตามข้อกำหนด 6(4) ผู้ประกอบธุรกิจควรดำเนินการดังต่อไปนี้

(1) จัดให้มีขั้นตอนการจัดทำ การติดตาม และการควบคุมดูแลการจัดทำรายงานเพื่อให้มั่นใจได้ว่าสามารถจัดทำรายงานได้อย่างครบถ้วน ถูกต้อง และทันเวลา

(2) กำหนดให้จัดทำรายงานที่มีเนื้อหาครอบคลุมถึงเรื่องดังต่อไปนี้ ตามรอบระยะเวลาที่เหมาะสม

(ก) กิจกรรมที่เกี่ยวข้องกับการปฏิบัติงานด้านการบริหารความเสี่ยง หรือการจัดสรรและบริหารทรัพยากรด้าน IT เช่น สรุปผลการบริหารจัดการด้านความเสี่ยง / การจัดสรรทรัพยากร IT ในรอบปี เป็นต้น

(ข) ความคืบหน้าของงานโครงการ (ถ้ามี)

(ค) การปฏิบัติตามกฎระเบียบ ข้อบังคับ หรือข้อตกลงที่จัดทำกับบุคคลภายนอกและภายในบริษัท เช่น การจัดส่ง incident report ต่อสำนักงานเมื่อเกิดเหตุการณ์ที่ส่งผลกระทบต่อระบบ IT / การติดตามให้ผู้ให้บริการดำเนินการตามข้อตกลงที่กำหนดไว้ใน service level agreement

(ง) ความมีประสิทธิภาพของการนำเทคโนโลยีสารสนเทศมาใช้ เช่น การติดตามระยะเวลาในการปฏิบัติงานที่ลดลงภายหลังการนำเทคโนโลยีมาปรับปรุงกระบวนการทำงาน และความสอดคล้องกับวัตถุประสงค์ของการนำเทคโนโลยีสารสนเทศมาใช้งาน

(จ) ประเด็นปัญหาและอุปสรรค

6. ผู้ประกอบธุรกิจควรกำหนดให้ผู้บริหารระดับสูงเป็นผู้รับผิดชอบในการปฏิบัติให้เป็นไปตามข้อกำหนด 6(4)

ข้อกำหนดในประกาศที่ สธ. 37/2559

ข้อ 6 ผู้ประกอบธุรกิจต้องจัดให้มีการกำกับดูแลและบริหารจัดการด้านเทคโนโลยีสารสนเทศตามหลักเกณฑ์ดังต่อไปนี้ ทั้งนี้ เพื่อให้เป็นไปตามนโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจที่กำหนดไว้ตามข้อ 5

(5) จัดให้มีระบบการควบคุมภายในสำหรับการปฏิบัติงานให้เป็นไปตามนโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศ อย่างน้อยดังนี้

(ก) มีการตรวจสอบภายในและการสอบทานการปฏิบัติงานให้เป็นไปตามนโยบายดังกล่าวอย่างเป็นระบบ

(ข) มีการปรับปรุงแก้ไขข้อบกพร่อง และติดตามการปรับปรุงแก้ไขดังกล่าวอย่างเป็นระบบ

แนวทางปฏิบัติเพิ่มเติมจากข้อกำหนด

7. ในการปฏิบัติให้เป็นไปตามข้อกำหนด 6(5) ผู้ประกอบธุรกิจควรจัดให้มีการติดตาม ประเมิน และปรับปรุงแก้ไขข้อบกพร่องของระบบควบคุมภายใน ดังต่อไปนี้

(1) จัดให้มีการติดตาม ตรวจสอบ และประเมินประสิทธิภาพของขั้นตอนการปฏิบัติงานของหน่วยงานที่ทำหน้าที่บริหารและจัดการในเรื่องดังต่อไปนี้ โดยผู้ตรวจสอบที่เป็นอิสระจากหน่วยงานดังกล่าว

(ก) การปฏิบัติงานให้เป็นไปตามนโยบายในข้อกำหนด 5(1) (2) และ (3)

(ข) การรายงานการปฏิบัติงานในข้อกำหนด 6(4)

(2) จัดให้มีการประเมินตนเองในด้านประสิทธิภาพของขั้นตอนการปฏิบัติงาน (control self-assessment : CSA)

(3) จัดให้ผู้ตรวจสอบที่เป็นอิสระเป็นผู้ประมวลและรายงานผลที่ได้จากการดำเนินการตาม (1) และ (2) พร้อมทั้งรายงานข้อบกพร่องที่ตรวจพบและผลการปรับปรุงแก้ไขให้คณะกรรมการบริษัทหรือคณะกรรมการตรวจสอบและผู้บริหารระดับสูงทราบตามรอบการประเมินและตามรอบการติดตามการปรับปรุงแก้ไขข้อบกพร่อง หรือโดยไม่ชักช้าเมื่อพบข้อบกพร่องที่มีนัยสำคัญ

หมวดที่ 2 : การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ (IT security)

1. แนวทางปฏิบัติเพิ่มเติมเกี่ยวกับนโยบายและมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (information security policy)

ข้อกำหนดในประกาศที่ สธ. 37/2559

> ข้อ 5 ผู้ประกอบธุรกิจต้องจัดให้มีนโยบายเป็นลายลักษณ์อักษรในการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศอย่างน้อยในเรื่องดังต่อไปนี้ ทั้งนี้ นโยบายดังกล่าวต้องได้รับความเห็นชอบจากคณะกรรมการของผู้ประกอบธุรกิจหรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบธุรกิจ
>
> (3) การจัดให้มีนโยบายและมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามข้อ 8 และข้อ 9

แนวทางปฏิบัติเพิ่มเติมจากข้อกำหนด

1. นโยบายและมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามข้อกำหนดในหมวดที่ 1 ข้อ 5(3) ควรมีเนื้อหาขั้นต่ำครอบคลุมในเรื่องดังต่อไปนี้

1. การรักษาความปลอดภัยต่อทรัพย์สินสารสนเทศ
   - การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ (access control) [อ้างอิงจากข้อ 5]
   - การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม (physical and environmental security) [อ้างอิงจากข้อ 7]

2. การจัดการข้อมูลสารสนเทศและการรักษาความลับ
   - การจำแนกประเภททรัพย์สินสารสนเทศ (asset classification) เพื่อกำหนดมาตรการรักษาความมั่นคงปลอดภัย [อ้างอิงจากข้อ 4.2]
   - การสำรองข้อมูล (backup) [อ้างอิงจากข้อ 8.3]
   - การควบคุมการเข้ารหัสข้อมูล (cryptographic control) [อ้างอิงจากข้อ 6]

3. การควบคุมดูแลบุคลากรผู้ปฏิบัติงาน
   - การควบคุมการใช้งานของผู้ใช้งาน (end user) เช่น
     - มาตรการป้องกันทรัพย์สินสารสนเทศประเภทอุปกรณ์ระหว่างที่ไม่มีผู้ใช้งาน (protection of unattended user equipment) [อ้างอิงจากข้อ 7.2 แนวทางปฏิบัติข้อ 6]
     - การใช้งานอุปกรณ์เคลื่อนที่และการปฏิบัติงานจากเครือข่ายภายนอกบริษัท (mobile device and teleworking) [อ้างอิงจากข้อ 2.2]
     - การควบคุมการติดตั้งซอฟต์แวร์บนระบบงาน (installation of software on operational systems) [อ้างอิงจากข้อ 8.5]
   - การควบคุมดูแลผู้รับดำเนินการด้านระบบสารสนเทศ (IT outsourcing) [อ้างอิงจากข้อ 11]

4. การจัดการระบบเครือข่ายคอมพิวเตอร์และการรับส่งข้อมูลสารสนเทศ
   - การรักษาความมั่นคงปลอดภัยด้านการสื่อสารข้อมูลสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์ (communications security) [อ้างอิงจากข้อ 9]
   - การควบคุมการรับส่งข้อมูลสารสนเทศ (information transfer) [อ้างอิงจากข้อ 9.2]
5. การป้องกันภัยคุกคามต่อระบบสารสนเทศ
   - การป้องกันภัยคุกคามจากโปรแกรมไม่ประสงค์ดี (protection from malware) [อ้างอิงจากข้อ 8.2]
   - การบริหารจัดการช่องโหว่ทางเทคนิค (technical vulnerability management) [อ้างอิงจากข้อ 8.6]
6. การจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศ (system acquisition, development and maintenance) [อ้างอิงจากข้อ 10]

2. การจัดโครงสร้างความมั่นคงปลอดภัยของระบบสารสนเทศ (organization of information security)

2.1 การจัดโครงสร้างภายในองค์กร (internal organization)

วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมการปฏิบัติหน้าที่ด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศสำหรับส่วนงานต่าง ๆ ภายในองค์กร ให้เป็นไปตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

ข้อกำหนดในประกาศที่ สธ. 37/2559

ข้อ 10 ผู้ประกอบธุรกิจต้องจัดให้มีโครงสร้างการบริหารงานเพื่อรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (organization of information security) ตามหลักเกณฑ์ดังต่อไปนี้

(1) กำหนดรายละเอียดเกี่ยวกับหน้าที่และความรับผิดชอบในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศเป็นลายลักษณ์อักษร และแนวทางในการปฏิบัติหน้าที่ ให้กับบุคลากรของผู้ประกอบธุรกิจ

(2) สอบทานการปฏิบัติงานเพื่อป้องกันความเสี่ยงในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศที่อาจเกิดขึ้นในการปฏิบัติหน้าที่

(3) จัดให้มีช่องทางในการติดต่อสำนักงาน หน่วยงานกำกับดูแลด้านเทคโนโลยีสารสนเทศ และหน่วยงานของผู้ให้บริการที่สนับสนุนการทำงานระบบสารสนเทศของบริษัท โดยต้องปรับปรุงรายชื่อและช่องทางสำหรับติดต่อดังกล่าวให้เป็นปัจจุบัน

แนวทางปฏิบัติเพิ่มเติมจากข้อกำหนด

1. ผู้ประกอบธุรกิจควรกำหนดให้ผู้บริหารระดับสูงเป็นผู้รับผิดชอบในการปฏิบัติให้เป็นไปตามข้อกำหนด 10(1) และ (2)

2. ในการปฏิบัติให้เป็นไปตามข้อกำหนด 10(2) ผู้ประกอบธุรกิจควรจัดให้มีการแบ่งแยกหน้าที่ในการปฏิบัติงานด้านต่าง ๆ ที่เกี่ยวกับความมั่นคงปลอดภัยของระบบสารสนเทศอย่างชัดเจน เพื่อให้มีการสอบทานการปฏิบัติงานระหว่างกันเพื่อป้องกันความเสี่ยงที่อาจเกิดขึ้น เช่น การแบ่งแยกบุคลากรที่ปฏิบัติหน้าที่ในส่วนการพัฒนาระบบงาน (developer) ออกจากบุคลากรที่ทำหน้าที่บริหารระบบ (system administrator) ซึ่งปฏิบัติงานอยู่ในส่วนระบบคอมพิวเตอร์ที่ใช้งานจริง (production environment) ทั้งนี้ ในกรณีที่ไม่สามารถแบ่งแยกหน้าที่ความรับผิดชอบเนื่องจากข้อจำกัดทางด้านขนาดของการประกอบธุรกิจ ผู้ประกอบธุรกิจควรจัดให้มีกระบวนการติดตาม และตรวจสอบการปฏิบัติงานของบุคลากรที่เกี่ยวข้องอย่างใกล้ชิดและสม่ำเสมอเพื่อลดความเสี่ยงที่อาจเกิดขึ้น

2.2 การปฏิบัติงานที่มีการใช้อุปกรณ์เคลื่อนที่ (mobile device) เพื่อเข้าถึงระบบสารสนเทศภายในองค์กร และการปฏิบัติงานจากเครือข่ายภายนอกบริษัท (teleworking)

วัตถุประสงค์
เพื่อกำหนดมาตรการรักษาความมั่นคงปลอดภัยสำหรับการปฏิบัติงานจากเครือข่ายภายนอกบริษัท รวมทั้งการใช้งานอุปกรณ์เคลื่อนที่เพื่อเข้าถึงระบบงานภายในองค์กร

ข้อกำหนดในประกาศที่ สธ. 37/2559

ข้อ 9 ผู้ประกอบธุรกิจต้องจัดให้มีมาตรการอย่างน้อยในเรื่องดังต่อไปนี้ เพื่อรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

(1) มาตรการรักษาความปลอดภัยที่รัดกุมเพียงพอสำหรับข้อมูลที่เป็นความลับหรือมีความสำคัญในกรณีที่มีการปฏิบัติงานจากเครือข่ายภายนอกบริษัทหรือมีการใช้งานอุปกรณ์เคลื่อนที่ โดยกรณีที่เป็นการใช้งานอุปกรณ์เคลื่อนที่ ต้องจัดให้มีการลงทะเบียนอุปกรณ์เคลื่อนที่ก่อนการใช้งาน และทบทวนทะเบียนดังกล่าวอย่างน้อยปีละ 1 ครั้งและเมื่อมีการเปลี่ยนอุปกรณ์เคลื่อนที่

แนวทางปฏิบัติเพิ่มเติมจากข้อกำหนด

1. ในการปฏิบัติงานที่มีการใช้อุปกรณ์เคลื่อนที่เพื่อเข้าถึงระบบงานภายในองค์กร (ไม่รวมถึงระบบ mail service) ผู้ประกอบธุรกิจควรจัดให้มีมาตรการป้องกันข้อมูลสารสนเทศที่สำคัญตามข้อกำหนด 9(1) โดยพิจารณาถึงแนวทางดังต่อไปนี้

(1) กำหนดให้มีการลงทะเบียนอุปกรณ์เคลื่อนที่ เช่น ยี่ห้อ รุ่น ระบบปฏิบัติการ รหัสประจำเครื่อง (serial number) และหมายเลขอ้างอิงอุปกรณ์เครือข่าย (MAC address) เป็นต้น ก่อนการใช้งาน รวมถึงจัดให้มีการทบทวนทะเบียนดังกล่าวอย่างน้อยปีละ 1 ครั้งและเมื่อมีการเปลี่ยนอุปกรณ์ พร้อมทั้งยกเลิกสิทธิการใช้งานของอุปกรณ์เดิม เพื่อให้มั่นใจได้ว่าการใช้งานอุปกรณ์ดังกล่าวมีความสอดคล้องเป็นไปตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ทั้งนี้ ผู้ประกอบธุรกิจอาจใช้ระบบเทคโนโลยีการลงทะเบียนอื่นทดแทนได้ หากพิจารณาแล้วเห็นว่าเหมาะสม

(2) มีมาตรการป้องกันข้อมูลที่เป็นความลับหรือมีความสำคัญ (sensitive data) กรณีที่อุปกรณ์เคลื่อนที่สูญหาย เช่น การกำหนดให้ใส่รหัสผ่านก่อนใช้งานอุปกรณ์ (lock screen) หรือการลบข้อมูลจากระยะไกล (remote wipe-out) เป็นต้น

(3) กำหนดประเภทบริการการใช้งาน (application service) ที่อนุญาตให้ใช้งานผ่านอุปกรณ์เคลื่อนที่ และกำหนดมาตรการควบคุมการเข้าถึงบริการการใช้งานดังกล่าวโดยคำนึงถึงความปลอดภัยของการเชื่อมต่อกับเครือข่าย เช่น จำกัดให้เข้าถึงบริการการใช้งานบางประเภทหากเป็นการเชื่อมต่อกับเครือข่ายภายนอก เป็นต้น

(4) จัดให้มีการเข้ารหัสข้อมูลสารสนเทศที่สำคัญทั้งที่จัดเก็บในอุปกรณ์เคลื่อนที่และที่รับส่งผ่านระบบเครือข่ายคอมพิวเตอร์

(5) จัดให้มีการสื่อสารให้ผู้ใช้งานพร้อมทั้งลงนามรับทราบ เพื่อสร้างความตระหนักและทราบถึงความเสี่ยงจากการใช้งาน และแนวทางการควบคุมความเสี่ยงดังกล่าว

(6) ควบคุมให้มีการติดตั้งเฉพาะซอฟต์แวร์ที่ถูกต้องตามลิขสิทธิ์ และโปรแกรมเพื่อปิดช่องโหว่ (patches) ที่เหมาะสม และกำหนดมาตรการป้องกันโปรแกรมไม่ประสงค์ดี (malware) ทั้งนี้ เพื่อป้องกันการบุกรุกหรือก่อให้เกิดความเสียหายต่อข้อมูลที่เป็นความลับและมีความสำคัญที่จัดเก็บในอุปกรณ์เคลื่อนที่

(7) จัดให้มีการดำเนินการเพื่อลดผลกระทบเมื่อเกิดเหตุการณ์ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยของข้อมูลสารสนเทศ เช่น ตัดการเชื่อมต่อโดยทันทีที่ทราบเหตุ เป็นต้น

ทั้งนี้ หากอุปกรณ์เคลื่อนที่เป็นทรัพย์สินของพนักงาน ผู้ประกอบธุรกิจควรพิจารณาแนวทางในข้อ (1) - (5) เป็นขั้นต่ำ พร้อมทั้งจัดให้มีมาตรการควบคุมที่เทียบเคียงหรือทดแทนแนวทางในข้อ (6) - (7) ได้ เช่น กำหนดให้มีการตรวจสอบอุปกรณ์เคลื่อนที่อย่างสม่ำเสมอ กำหนดบทลงโทษหรือตัดสิทธิการใช้งาน application service ในกรณีที่พนักงานละเมิดข้อกำหนด เป็นต้น

2. ในกรณีที่มีการปฏิบัติงานจากเครือข่ายภายนอกบริษัท (teleworking) ผู้ประกอบธุรกิจควรกำหนดมาตรการรักษาความมั่นคงปลอดภัยที่รัดกุมเพียงพอสำหรับข้อมูลสารสนเทศที่ถูกเข้าถึง ประมวลผล และจัดเก็บในพื้นที่ปฏิบัติงาน ตามข้อกำหนด 9(1) โดยพิจารณาถึง

(1) การกำหนดมาตรการรักษาความมั่นคงปลอดภัยด้านกายภาพที่เหมาะสม รัดกุมเพียงพอ กับขอบเขตการปฏิบัติงาน สำหรับพื้นที่ปฏิบัติงานนอกองค์กร

(2) การควบคุมสิทธิการใช้งานและการเข้าถึงข้อมูลสารสนเทศของผู้ใช้งานอย่างเหมาะสม

(3) การรักษาความมั่นคงปลอดภัยของระบบงานภายในองค์กรที่สำคัญและระบบเครือข่ายคอมพิวเตอร์ กรณีมีการเชื่อมต่อหรือรับส่งข้อมูลที่เป็นความลับหรือมีความสำคัญจากระยะไกล (remote access) เช่น การติดตั้ง firewall การ update โปรแกรมป้องกัน malware การกำหนดสิทธิการเข้าถึงและการเข้ารหัสข้อมูล (data encryption) หรือเข้ารหัสระบบเครือข่าย (network encryption) เป็นต้น

(4) การป้องกันการรั่วไหลของข้อมูลสารสนเทศในกรณีใช้เทคโนโลยี virtual desktop

(5) การป้องกันการเข้าถึงข้อมูลสารสนเทศจากบุคคลที่ไม่มีสิทธิในการใช้งาน เช่น ญาติพี่น้องและเพื่อน เป็นต้น

(6) การตรวจสอบสิทธิการเข้าถึงของพนักงานที่ได้รับอนุญาตให้ปฏิบัติงานจากภายนอกบริษัท

(7) การป้องกันโปรแกรมไม่ประสงค์ดี

ข้อกำหนดในประกาศที่ สธ. 37/2559

ข้อ 8 ผู้ประกอบธุรกิจต้องจัดให้มีการกำหนดนโยบายอย่างน้อยในเรื่องดังต่อไปนี้ ไว้เป็นลายลักษณ์อักษร เพื่อรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (information security policy)

(1) นโยบายการใช้งานระบบสารสนเทศร่วมกันบนระบบเครือข่ายคอมพิวเตอร์เพื่อการประมวลผลตามความต้องการของผู้ใช้งาน (cloud computing) ซึ่งครอบคลุมถึงวิธีการคัดเลือกและประเมินผู้ให้บริการ การทบทวนคุณสมบัติของผู้ให้บริการ ข้อกำหนดเกี่ยวกับการใช้บริการ และการตรวจสอบบันทึกหลักฐานต่าง ๆ ที่อาจส่งผลกระทบต่อการใช้บริการ

ข้อ 9 ผู้ประกอบธุรกิจต้องจัดให้มีมาตรการอย่างน้อยในเรื่องดังต่อไปนี้ เพื่อรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

(2) มาตรการในการใช้งานระบบสารสนเทศร่วมกันบนระบบเครือข่ายคอมพิวเตอร์เพื่อการประมวลผลตามความต้องการของผู้ใช้งานตามนโยบายที่กำหนดไว้ในข้อ 8(1) ที่ครอบคลุมเรื่องดังนี้

(ก) ข้อตกลงร่วมกันระหว่างผู้ให้บริการและผู้ใช้บริการซึ่งมีรายละเอียดในเรื่องดังต่อไปนี้เป็นอย่างน้อย

1. หน้าที่และความรับผิดชอบของผู้ให้บริการ รวมถึงความรับผิดต่อผู้ประกอบธุรกิจในกรณีที่ผู้ให้บริการไม่สามารถปฏิบัติตามข้อตกลงได้

2. ขั้นตอนการปฏิบัติงานที่เป็นไปตามมาตรฐานการรับรองความมั่นคงปลอดภัยด้านสารสนเทศในระดับสากล

3. มาตรการการรักษาความมั่นคงปลอดภัย การควบคุมการเข้าถึง และการเปิดเผยข้อมูลสารสนเทศ

4. การตรวจสอบการปฏิบัติงานจากผู้ตรวจสอบที่เป็นอิสระ

5. เงื่อนไขในกรณีที่ผู้ให้บริการจะให้ผู้ให้บริการรายอื่นรับดำเนินการช่วง (subcontract of the cloud provider) และข้อกำหนดความรับผิดต่อความเสียหายที่อาจเกิดขึ้นจากการดำเนินการของผู้ให้บริการรายอื่น

(ข) คุณสมบัติด้านความปลอดภัยของผู้ให้บริการรายอื่นที่รับดำเนินการช่วงซึ่งเทียบเท่ากับผู้ให้บริการหรือเป็นไปตามมาตรฐานสากล

(ค) การติดตาม ประเมิน และทบทวนการให้บริการของผู้ให้บริการ

(ง) ขั้นตอนในการโอนย้ายข้อมูลไปยังผู้ให้บริการรายใหม่ ในกรณีที่มีการเปลี่ยนตัวผู้ให้บริการ

แนวทางปฏิบัติเพิ่มเติมจากข้อกำหนด

3. ในกรณีที่ใช้บริการ cloud computing กับระบบสารสนเทศที่มีความสำคัญ ผู้ประกอบธุรกิจควรจัดให้มีข้อกำหนดเกี่ยวกับการใช้งาน โดยขั้นต่ำควรมีรายละเอียด ดังนี้

3.1 กำหนดนโยบายการใช้งาน cloud computing ตามข้อกำหนด 8(1) โดยอย่างน้อยมีเนื้อหา ดังนี้

(1) ประเมินความเสี่ยงเกี่ยวกับการใช้บริการ

(2) กำหนดประเภทงานที่จะใช้บริการ

(3) กำหนดรูปแบบของการใช้บริการ เช่น software as a service (saas), platform as a service (paas) และ infrastructure as a service (iaas)

(4) กำหนดวิธีการคัดเลือกและประเมินผู้ให้บริการ (due diligence) โดยควรให้ความสำคัญในเรื่องการรักษาความปลอดภัยของข้อมูลสารสนเทศที่สำคัญ (confidentiality) ความถูกต้องเชื่อถือได้ของข้อมูลและระบบสารสนเทศ (integrity) และความพร้อมใช้งานของระบบสารสนเทศที่ใช้บริการ (availability)

(5) กำหนดการทบทวนคุณสมบัติของผู้ให้บริการอย่างสม่ำเสมอ เช่น ฐานะทางการเงิน ความเพียงพอของการให้บริการ (capacity planning) เพื่อให้มั่นใจว่าผู้ให้บริการยังคงมีความพร้อมในการให้บริการที่เพียงพอต่อความต้องการของผู้ประกอบธุรกิจอย่างต่อเนื่อง

(6) จัดให้มีการเผยแพร่นโยบายเกี่ยวกับการใช้บริการ และสื่อสารให้พนักงานที่เกี่ยวข้องพร้อมทั้งลงนามรับทราบ เพื่อให้ตระหนักถึงความมั่นคงปลอดภัยจากการใช้บริการ cloud computing

(7) กำหนดบทบาทหน้าที่ความรับผิดชอบของผู้ให้บริการอย่างชัดเจน เช่น การสำรองข้อมูล การรับเรื่องแก้ไขปัญหา ขั้นตอนและกระบวนการแก้ไขปัญหา รายชื่อและช่องทางสำหรับติดต่อ เป็นต้น

(8) กำหนดความปลอดภัยของข้อมูลแต่ละประเภทที่จะใช้ใน cloud โดยแบ่งชั้นความลับของข้อมูล และกำหนดวิธีปฏิบัติแต่ละระดับชั้นความลับของข้อมูล

(9) กำหนดมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมตามการใช้งานแต่ละประเภท เพื่อป้องกันภัยคุกคามและการเข้าถึงข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต

(10) กำหนดใช้วิธีพิสูจน์ตัวตนแบบ multi-factor authentication[1] สำหรับการเข้าถึงหน้าผู้บริหารระบบ (administrator page) สำหรับระบบสารสนเทศที่มีความสำคัญ

(11) กำหนดให้มีการตรวจสอบบันทึกหลักฐานต่าง ๆ และติดตามปัญหาที่อาจส่งผลต่อการใช้บริการ

3.2 กำหนดข้อตกลงระหว่างผู้ให้บริการและผู้ใช้บริการตามข้อกำหนด 9(2)(ก) โดยมีลักษณะดังนี้

(1) ผู้ใช้บริการถือเป็นเจ้าของข้อมูลสารสนเทศ

(2) กำหนดประเภทบริการที่จะใช้ cloud computing

---

[1] ทั้งนี้ ในกรณีการติดต่อสนทนาผ่านช่องทางอิเล็กทรอนิกส์ (electronic messaging) เช่น email ผู้ประกอบธุรกิจอาจไม่ต้องใช้วิธีพิสูจน์ตัวตนแบบ multi-factor authentication ได้ โดยให้ใช้วิธีการเข้ารหัสข้อมูลสำหรับไฟล์ข้อมูลแนบ (attached file) ที่มีความสำคัญ อย่างมั่นคงปลอดภัย

(3) กำหนดมาตรฐานความปลอดภัยด้านเครือข่าย เช่น การเข้ารหัสข้อมูลที่รับส่งผ่านระบบเครือข่ายคอมพิวเตอร์ การป้องกันการโจมตีในลักษณะ DDoS (distributed denial of service) การป้องกันการบุกรุกจากโปรแกรมไม่ประสงค์ดี การป้องกันภัยคุกคามในรูปแบบใหม่ (advanced persistent threat) การแบ่งแยกเครือข่าย การเข้ารหัสระหว่างแอพพลิเคชั่น (application) การป้องกันการบุกรุกแบบลำดับชั้น (defense-in-depth) และการสร้างความมั่นคงปลอดภัยให้กับระบบสารสนเทศ (hardening) เป็นต้น

(4) ระบุข้อตกลงในการควบคุมการเข้าถึงข้อมูล เช่น วิธีการเข้าใช้งานระบบ วิธีการกำหนดสิทธิการใช้งาน การติดตามการแก้ปัญหา การรายงานข้อผิดพลาด ประสิทธิภาพ และสภาพโดยรวมของระบบ อย่างชัดเจน

(5) กำหนดบทบาทหน้าที่ความรับผิดชอบของผู้ให้บริการในด้านการสำรองข้อมูล กระบวนการแก้ไขปัญหา ระดับการให้บริการ (service level agreement) ระยะเวลาในการกลับคืนสู่สภาพการดำเนินงานปกติของระบบสารสนเทศ (recovery time objectives : RTO) และกำหนดเป้าหมายในการกู้คืนข้อมูล เช่น กำหนดประเภทของข้อมูล และชุดข้อมูลล่าสุดที่จะกู้คืนได้ (recovery point objective : RPO) อย่างชัดเจน

(6) กำหนดเงื่อนไขความรับผิดชอบในกรณีที่ผู้ให้บริการไม่สามารถให้บริการตามที่กำหนดในข้อตกลง

(7) กำหนดให้เนื้อหาหรือเอกสารที่เกี่ยวข้องกับข้อตกลงมีการระบุรายละเอียดที่เกี่ยวข้องกับนโยบายการป้องกันการรั่วไหลของข้อมูลที่อาจเกิดขึ้นจากผู้ให้บริการ

(8) ผู้ให้บริการไม่ควรมีสิทธิเข้าถึงและเปิดเผยข้อมูลของผู้ใช้บริการ เว้นแต่จะแจ้งและได้รับความยินยอมจากผู้ใช้บริการ หรือแจ้งให้ทราบหากเป็นไปตามกฎหมายของประเทศที่ผู้ให้บริการไปตั้งศูนย์ข้อมูล (cloud server hosting country) หรือเป็นไปตามกฎหมายเกี่ยวกับความมั่นคงของประเทศผู้ให้บริการ (origin country)

(9) ผู้ให้บริการควรปรับปรุงการปฏิบัติงานให้เป็นไปตามมาตรฐานการรับรองความมั่นคงปลอดภัยด้านสารสนเทศในระดับสากล[2] ฉบับปัจจุบันโดยไม่ชักช้า หากมาตรฐานดังกล่าวได้ถูกปรับปรุงให้เป็นปัจจุบัน (update)

(10) ผู้ประกอบธุรกิจควรมีมาตรการเพื่อให้มั่นใจได้ว่าผู้ให้บริการจัดให้มีการตรวจสอบขั้นตอนการปฏิบัติงานอย่างน้อยปีละ 1 ครั้ง จากผู้ตรวจสอบอิสระ

(11) มีข้อกำหนดเมื่อสิ้นสุดการใช้บริการ (exit plan) เช่น กำหนดระยะเวลารักษาข้อมูลและวิธีการทำลายข้อมูลเพื่อให้มั่นใจว่าไม่สามารถกู้คืนข้อมูลกลับมาได้

(12) มีข้อกำหนดในการใช้บริการ cloud computing ต่อจากผู้ให้บริการรายอื่น (subcontract) อย่างชัดเจน โดยอย่างน้อยควรมีเงื่อนไขกำหนดให้บริการดังกล่าวเป็นส่วนหนึ่งของผู้ให้บริการ และผู้ให้บริการควรรับผิดชอบต่อความเสียหายที่เกิดขึ้นจากการกระทำหรือการดำเนินการใด ๆ ของผู้ให้บริการรายอื่น

---

[2] ตัวอย่างเช่น มาตรฐาน ISO27001 เป็นต้น

3.3 ในการติดตาม ประเมิน และทบทวนการให้บริการของผู้ให้บริการให้เป็นไปตามข้อกำหนด 9(2)(ค) ผู้ประกอบธุรกิจควรดำเนินการเพิ่มเติม ดังนี้

(1) ติดตามตรวจสอบประสิทธิภาพของการให้บริการ รวมทั้งมาตรการด้านความมั่นคงปลอดภัยให้สอดคล้องกับข้อกำหนดตามสัญญาต่าง ๆ หรือข้อตกลงในการให้บริการ

(2) ประเมินความเพียงพอของระบบงานของผู้ให้บริการ (capacity planning) อย่างสม่ำเสมอ

(3) ทบทวนเงื่อนไขการบริการในกรณีที่มีการเปลี่ยนแปลง เพื่อให้มั่นใจได้ว่าการให้บริการยังคงสอดคล้องกับการใช้งานและนโยบายด้านความมั่นคงปลอดภัยของระบบสารสนเทศของผู้ประกอบธุรกิจ

(4) ทบทวนคุณสมบัติของผู้ให้บริการอย่างต่อเนื่อง เช่น การตรวจสอบความมั่นคงในฐานะทางการเงิน กระบวนการปฏิบัติงาน และประสิทธิภาพการปฏิบัติงาน เป็นต้น

3. การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร (human resource security)

วัตถุประสงค์
เพื่อให้พนักงานและบุคคลภายนอกที่ปฏิบัติงานโดยมีการเข้าถึงข้อมูลหรือระบบงานภายในองค์กร มีความตระหนักรู้ และปฏิบัติงานโดยคำนึงถึงการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

ข้อกำหนดในประกาศที่ สธ. 37/2559

ข้อ 13 ผู้ประกอบธุรกิจต้องสร้างความตระหนักรู้เกี่ยวกับนโยบายและมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศให้แก่บุคลากรของผู้ประกอบธุรกิจและบุคคลภายนอก (human resource security) ที่มีการปฏิบัติงานโดยมีการเข้าถึงข้อมูลหรือระบบงานภายในองค์กร และดำเนินการให้บุคลากรดังกล่าวสามารถปฏิบัติหน้าที่ได้ตามนโยบายและมาตรการที่กำหนด ทั้งนี้ ตามหลักเกณฑ์ดังต่อไปนี้

(1) ให้ความรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศที่เกี่ยวข้องกับการปฏิบัติหน้าที่แก่บุคลากรของผู้ประกอบธุรกิจและบุคคลภายนอกที่ปฏิบัติงานดังกล่าว

(2) สื่อสารให้บุคลากรของผู้ประกอบธุรกิจและบุคคลภายนอกที่ปฏิบัติงานดังกล่าว ระมัดระวังและงดเว้นการใช้งานระบบสารสนเทศในลักษณะที่อาจก่อให้เกิดความเสียหายแก่ผู้ประกอบธุรกิจ หรือตลาดทุนโดยรวม หรือกระทบต่อความมั่นคงของประเทศ และต้องรายงานผู้มีหน้าที่รับผิดชอบในการบริหารจัดการเหตุการณ์ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศโดยไม่ชักช้าเมื่อพบความผิดปกติใด ๆ อย่างมีนัยสำคัญ

(3) กำหนดมาตรการในการลงโทษบุคลากรที่มีพฤติกรรมฝ่าฝืนหรือไม่ปฏิบัติตามนโยบายหรือหลักเกณฑ์เกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

แนวทางปฏิบัติเพิ่มเติมจากข้อกำหนด

1. ตัวอย่างการใช้งานระบบสารสนเทศในลักษณะที่อาจก่อให้เกิดความเสียหายกับผู้ประกอบธุรกิจ ตลาดทุนโดยรวม หรือความมั่นคงของประเทศ ตามข้อกำหนด 13(2) เช่น การหมิ่นประมาท การข่มขู่ การปลอมแปลงเป็นบุคคลอื่น การส่งจดหมายอิเล็กทรอนิกส์แบบลูกโซ่ และการเปิดเผยข้อมูลที่เป็นความลับของผู้ประกอบธุรกิจ เป็นต้น

4. การบริหารจัดการทรัพย์สินสารสนเทศ (asset management)

4.1 หน้าที่ความรับผิดชอบต่อทรัพย์สินสารสนเทศ (responsibility for assets)

วัตถุประสงค์

เพื่อให้ทรัพย์สินสารสนเทศที่มีความสำคัญได้รับการป้องกันอย่างเหมาะสม ผู้ประกอบธุรกิจควรจัดให้มีการระบุและกำหนดหน้าที่ความรับผิดชอบในการรักษาความมั่นคงปลอดภัยของทรัพย์สินสารสนเทศ

ข้อกำหนดในประกาศที่ สธ. 37/2559

ข้อ 15 ผู้ประกอบธุรกิจต้องมีการบริหารจัดการทรัพย์สินสารสนเทศ (asset management) ให้เป็นไปตามหลักเกณฑ์ดังต่อไปนี้

(1) กำหนดบุคคลหรือหน่วยงานที่มีหน้าที่ดูแลรับผิดชอบทรัพย์สินสารสนเทศแต่ละประเภทตลอดอายุการใช้งานของทรัพย์สินดังกล่าว

(2) มีข้อกำหนดการใช้งานทรัพย์สินสารสนเทศที่เหมาะสม

(3) มีการทบทวนหน้าที่ความรับผิดชอบที่มีต่อทรัพย์สินสารสนเทศให้สอดคล้องกับหน้าที่ของผู้ปฏิบัติงานเมื่อมีการเปลี่ยนแปลงหน้าที่และความรับผิดชอบ

ข้อ 16 ในการบริหารจัดการทรัพย์สินสารสนเทศที่เป็นทรัพย์สินสารสนเทศประเภทระบบหรืออุปกรณ์ ผู้ประกอบธุรกิจต้องมีการจัดทำและจัดเก็บทะเบียนทรัพย์สินดังกล่าว ตลอดจนทบทวนทะเบียนดังกล่าวอย่างน้อยปีละ 1 ครั้งหรือเมื่อมีการเปลี่ยนแปลงทรัพย์สินสารสนเทศอย่างมีนัยสำคัญด้วย

แนวทางปฏิบัติเพิ่มเติมจากข้อกำหนด

- ไม่มีแนวปฏิบัติเพิ่มเติม -

4.2 การจำแนกประเภททรัพย์สินสารสนเทศ (asset classification) และการจัดการสื่อบันทึกข้อมูล (media handling)

วัตถุประสงค์

เพื่อให้ทรัพย์สินสารสนเทศที่มีความสำคัญได้รับการปกป้องในระดับที่เหมาะสม และเพื่อป้องกันการเปิดเผย เปลี่ยนแปลงแก้ไข หรือสร้างความเสียหายในกรณีที่เป็นข้อมูลสารสนเทศสำคัญซึ่งถูกจัดเก็บในสื่อบันทึกข้อมูล

ข้อกำหนดในประกาศที่ สธ. 37/2559

ข้อ 17 ในการบริหารจัดการทรัพย์สินสารสนเทศที่เป็นทรัพย์สินสารสนเทศประเภทข้อมูล ผู้ประกอบธุรกิจต้องดำเนินการจัดประเภทข้อมูลดังกล่าวตามระดับชั้นความลับและจัดประเภททรัพย์สินสารสนเทศอื่น ๆ ตามระดับความสำคัญ เพื่อให้ทรัพย์สินสารสนเทศได้รับการปกป้องในระดับที่เหมาะสมตามระดับชั้นความลับหรือระดับความสำคัญ แล้วแต่กรณีด้วย และในกรณีที่เป็นข้อมูลสารสนเทศ ผู้ประกอบธุรกิจต้องมีกระบวนการป้องกันการเปิดเผย เปลี่ยนแปลงแก้ไข หรือสร้างความเสียหายต่อข้อมูลสารสนเทศที่สำคัญที่ถูกจัดเก็บในสื่อบันทึกข้อมูลด้วย

แนวทางปฏิบัติเพิ่มเติมจากข้อกำหนด

1. ผู้ประกอบธุรกิจควรจัดให้มีมาตรการดูแลรักษาความมั่นคงปลอดภัยที่สอดคล้องเหมาะสมกับทรัพย์สินสารสนเทศแต่ละประเภทที่ได้จำแนกไว้ เช่น การควบคุมการเข้าถึง การจัดให้มีการเข้ารหัสข้อมูลที่เป็นความลับหรือต้องการความถูกต้องในระดับสูง เป็นต้น

2. ในการบริหารจัดการสื่อบันทึกข้อมูลเพื่อให้เป็นไปตามข้อกำหนด 17 ผู้ประกอบธุรกิจควรดำเนินการเพิ่มเติมดังต่อไปนี้

   2.1 จัดให้มีกระบวนการทำลายข้อมูลเพื่อป้องกันการรั่วไหลของข้อมูลและไม่ให้สามารถกู้คืนข้อมูลได้ในกรณีที่ไม่มีความจำเป็นต้องใช้ข้อมูล

   2.2 จัดให้มีกระบวนการทำลายสื่อบันทึกข้อมูลเพื่อป้องกันการรั่วไหลของข้อมูลที่เป็นความลับหรือมีความสำคัญ

   2.3 คำนึงถึงความเสี่ยงที่สื่อบันทึกข้อมูลอาจเสื่อมสภาพ รวมทั้งวิธีการนำข้อมูลกลับมาใช้งานใหม่ในกรณีที่จัดเก็บข้อมูลเป็นระยะเวลานาน

   2.4 จัดเก็บสื่อบันทึกข้อมูลในพื้นที่ที่มีความมั่นคงปลอดภัย และเป็นไปตามคำแนะนำของผู้ผลิต (ถ้ามี)

   2.5 จัดให้มีกระบวนการดูแลรักษาความปลอดภัยกรณีที่มีการเคลื่อนย้ายสื่อบันทึกข้อมูลออกจากพื้นที่ทำการ

5. การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ (access control)

5.1 การควบคุมการเข้าถึงตามข้อกำหนดทางธุรกิจ (business requirements of access control)

วัตถุประสงค์

เพื่อควบคุมการเข้าถึงข้อมูลและสิ่งอำนวยความสะดวกในการประมวลผลข้อมูล (information processing facilities)

ข้อกำหนดในประกาศที่ สธ. 37/2559

ข้อ 8 ผู้ประกอบธุรกิจต้องจัดให้มีการกำหนดนโยบายอย่างน้อยในเรื่องดังต่อไปนี้ ไว้เป็นลายลักษณ์อักษร เพื่อรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (information security policy)

(4) นโยบายควบคุมการเข้าถึงข้อมูลและสิ่งอำนวยความสะดวกในการประมวลผลข้อมูลต่าง ๆ (information processing facilities) ให้สอดคล้องกับข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

เพื่อประโยชน์ตามวรรคหนึ่ง (4) คำว่า “สิ่งอำนวยความสะดวกในการประมวลผลข้อมูล” หมายความว่า อุปกรณ์ ระบบงาน หรือสภาพแวดล้อม ที่จำเป็นหรือมีส่วนช่วยให้การประมวลผลข้อมูลเป็นไปอย่างครบถ้วน ถูกต้อง และมีประสิทธิภาพ เช่น อุปกรณ์หรือโปรแกรมประมวลผลข้อมูล ระบบเครือข่ายคอมพิวเตอร์ ขั้นตอน หรือสถานที่ประมวลผลข้อมูล

แนวทางปฏิบัติเพิ่มเติมจากข้อกำหนด

1. ผู้ประกอบธุรกิจควรจัดทำนโยบายตามข้อกำหนด 8(4) เป็นลายลักษณ์อักษร โดยมีเนื้อหาขั้นต่ำครอบคลุมเรื่องดังต่อไปนี้ พร้อมทั้งจัดให้มีการทบทวนนโยบายดังกล่าวอย่างสม่ำเสมอ
   (1) การกำหนดสิทธิการเข้าถึงข้อมูลและระบบสารสนเทศให้เหมาะสมกับการใช้งานและหน้าที่ความรับผิดชอบของผู้ใช้งาน รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ และยกเลิกสิทธิของบุคคลที่ไม่มีความจำเป็นในการเข้าถึงโดยทันที
   (2) การแบ่งแยกบทบาทหน้าที่ของบุคคลที่เกี่ยวข้อง เช่น บุคคลผู้ร้องขอ (access request) บุคคลผู้มีอำนาจอนุมัติ (access authorization) และบุคคลผู้บริหารสิทธิการเข้าถึง (access administration) เป็นต้น
   (3) รายละเอียดในส่วนที่เกี่ยวกับการควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ ขั้นต่ำควรครอบคลุมถึงการระบุประเภทหรือบริการทางเครือข่าย (network services) และบุคคลที่ได้รับอนุญาตให้เข้าถึง กระบวนการควบคุมและป้องกันการเข้าถึง วิธีการเข้าถึงแบบปลอดภัย เทคนิคการระบุตัวตน และการติดตามการใช้งานของบุคคลที่ได้รับอนุญาตให้เข้าถึง
   (4) การมีระบบที่ระบุผู้ใช้งานในระบบเครือข่ายคอมพิวเตอร์ได้อย่างชัดเจน โดยเฉพาะกรณีที่ผู้ประกอบธุรกิจใช้หมายเลขประจำเครื่องแบบพลวัต (dynamic IP address) เพื่อให้ผู้ประกอบธุรกิจมีข้อมูลที่สามารถระบุผู้ใช้งานหมายเลข IP address ในช่วงเวลาที่ใช้งานได้

5.2 การบริหารจัดการบัญชีผู้ใช้งาน (user access management)

วัตถุประสงค์
เพื่อให้มีการควบคุมสิทธิการใช้งานระบบสารสนเทศอย่างเหมาะสมและป้องกันไม่ให้ผู้ที่ไม่มีสิทธิใช้งานสามารถเข้าถึงระบบสารสนเทศได้

ข้อกำหนดในประกาศที่ สธ. 37/2559

ข้อ 20 ผู้ประกอบธุรกิจต้องมีการควบคุมการเข้าถึงระบบและข้อมูลสารสนเทศ (access control) ให้เป็นไปตามหลักเกณฑ์ดังต่อไปนี้

(1) มีการบริหารจัดการบัญชีผู้ใช้งานโดยจำกัดการเข้าถึงข้อมูลสารสนเทศให้สามารถเข้าถึงได้เฉพาะบุคคลที่ได้รับสิทธิการเข้าถึงดังนี้

(ก) มีการลงทะเบียนบัญชีผู้ใช้งานระบบสารสนเทศ

(ข) มีการจัดสรรสิทธิการเข้าถึงระดับสูงอย่างจำกัดและมีการควบคุมการเข้าถึงสิทธิดังกล่าวอย่างเคร่งครัด

(ค) มีขั้นตอนการบริหารจัดการในการกำหนดรหัสผ่านอย่างเหมาะสม

(ง) มีการติดตามและทบทวนระดับสิทธิการเข้าถึงอย่างสม่ำเสมอ

แนวทางปฏิบัติเพิ่มเติมจากข้อกำหนด

- ไม่มีแนวปฏิบัติเพิ่มเติม –

5.3 หน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities)

วัตถุประสงค์
เพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิ สามารถเข้าถึงระบบสารสนเทศได้

ข้อกำหนดในประกาศที่ สธ. 37/2559

ข้อ 20 ผู้ประกอบธุรกิจต้องมีการควบคุมการเข้าถึงระบบและข้อมูลสารสนเทศ (access control) ให้เป็นไปตามหลักเกณฑ์ดังต่อไปนี้

(2) มีข้อกำหนดให้ผู้ใช้งานปฏิบัติตามขั้นตอนการใช้งานและดูแลรับผิดชอบรหัสผ่านอย่างมั่นคงปลอดภัย

แนวทางปฏิบัติเพิ่มเติมจากข้อกำหนด

1. ในการปฏิบัติให้เป็นไปตามข้อกำหนด 20(2) ผู้ประกอบธุรกิจควรระบุในข้อกำหนดให้ผู้ใช้งานเป็นผู้ดูแลรับผิดชอบบัญชีผู้ใช้งาน (user ID) และรหัสผ่าน (password) รวมทั้งข้อมูลส่วนบุคคลที่อาจ

นำมาใช้เพื่อขอเปลี่ยนแปลงข้อมูลบัญชีการใช้งานระบบได้ (accountable for safeguard)

5.4 การควบคุมการเข้าถึงระบบสารสนเทศและโปรแกรมประยุกต์ (system and application access control)

วัตถุประสงค์
เพื่อป้องกันการเข้าถึงระบบสารสนเทศและแอพพลิเคชั่นโดยไม่ได้รับอนุญาต

ข้อกำหนดในประกาศที่ สธ. 37/2559

ข้อ 20 ผู้ประกอบธุรกิจต้องมีการควบคุมการเข้าถึงระบบและข้อมูลสารสนเทศ (access control) ให้เป็นไปตามหลักเกณฑ์ดังต่อไปนี้

(3) มีการป้องกันมิให้มีการเข้าถึงระบบสารสนเทศและโปรแกรมประยุกต์ (application software) โดยไม่ได้รับอนุญาต ดังนี้

(ก) ควบคุมการเข้าถึงข้อมูลสารสนเทศและฟังก์ชั่นต่าง ๆ ในโปรแกรมประยุกต์ของผู้ใช้งานและผู้ดูแลระบบสารสนเทศ ให้สอดคล้องกับสิทธิที่ได้รับ

(ข) ควบคุมการเข้าใช้งานระบบสารสนเทศและโปรแกรมประยุกต์

(ค) จัดให้มีระบบการบริหารจัดการรหัสผ่านที่มีความมั่นคงปลอดภัย

(ง) จำกัดการใช้งานโปรแกรมอรรถประโยชน์ต่าง ๆ (utility program) และจำกัดการเข้าถึงชุดคำสั่งควบคุมการทำงานของโปรแกรมอย่างเข้มงวด

แนวทางปฏิบัติเพิ่มเติมจากข้อกำหนด

1. ตัวอย่างของการควบคุมการเข้าใช้งานระบบสารสนเทศและโปรแกรมประยุกต์ตามข้อกำหนด 20(3)(ข) เช่น มีการป้องกันการเข้าใช้งานโดยวิธีเดาสุ่ม (brute force) จัดเก็บและตรวจสอบ log-in attempt log อย่างสม่ำเสมอ เป็นต้น

2. ในการปฏิบัติให้เป็นไปตามข้อกำหนด 20(3)(ค) ผู้ประกอบธุรกิจควรพิจารณากำหนดกระบวนการที่จำเป็น ดังนี้

(1) กำหนดให้ผู้ใช้งานแต่ละรายรับผิดชอบ (accountable) บัญชีผู้ใช้งาน (user ID) และรหัสผ่าน (password) ของตนเอง

(2) กำหนดให้ผู้ใช้งานสามารถตั้งค่าหรือเปลี่ยนแปลงรหัสผ่านได้ด้วยตนเอง และระบบควรมีขั้นตอนให้ยืนยันความถูกต้อง

(3) กำหนดให้ผู้ใช้งานตั้งรหัสผ่านที่ยากต่อการคาดเดา เช่น มีความยาวขั้นต่ำ 6-8 ตัวอักษร โดยอาจมีอักขระพิเศษ (เช่น “#”) ประกอบด้วย

(4) กำหนดให้ผู้ใช้งานเปลี่ยนแปลงรหัสผ่านทันทีที่ได้รับรหัสผ่านครั้งแรก และควรเปลี่ยนรหัสผ่านอย่างน้อยทุก 6 เดือน

(5) ในการเปลี่ยนรหัสผ่านแต่ละครั้ง ไม่ควรกำหนดรหัสผ่านใหม่ให้ซ้ำกับรหัสที่ใช้งานครั้งล่าสุด

(6) ระหว่างที่ผู้ใช้งานใส่รหัสผ่าน ระบบไม่ควรแสดงให้เห็นค่ารหัสผ่านบนหน้าจอ

(7) มีระบบการเข้ารหัส (encryption) ข้อมูลรหัสผ่าน เพื่อป้องกันการล่วงรู้หรือแก้ไขเปลี่ยนแปลง รวมทั้งไม่จัดเก็บข้อมูลรหัสผ่านใน folder เดียวกันกับ folder ที่จัดเก็บข้อมูลของแอพพลิเคชั่น

(8) ควรกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิด ซึ่งในทางปฏิบัติโดยทั่วไปไม่ควรเกิน 10 ครั้ง

(9) ควรมีวิธีการจัดส่งรหัสผ่านให้แก่ผู้ใช้งานอย่างรัดกุมและปลอดภัย เช่น การใส่ซองปิดผนึก เป็นต้น

6. การควบคุมการเข้ารหัสข้อมูล (cryptographic control)

วัตถุประสงค์
เพื่อให้การใช้งานระบบการเข้ารหัสข้อมูลมีความเหมาะสม มีประสิทธิภาพ และสามารถป้องกันการเข้าถึงหรือเปลี่ยนแปลงแก้ไขข้อมูลที่เป็นความลับหรือมีความสำคัญ

ข้อกำหนดในประกาศที่ สธ. 37/2559

ข้อ 8 ผู้ประกอบธุรกิจต้องจัดให้มีการกำหนดนโยบายอย่างน้อยในเรื่องดังต่อไปนี้ ไว้เป็นลายลักษณ์อักษรเพื่อรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (information security policy)

(2) นโยบายการใช้งานระบบการเข้ารหัสข้อมูลและการบริหารกุญแจเข้ารหัสข้อมูลที่สามารถป้องกันการเข้าถึงหรือเปลี่ยนแปลงแก้ไขข้อมูลที่เป็นความลับหรือมีความสำคัญ

แนวทางปฏิบัติเพิ่มเติมจากข้อกำหนด

1. นโยบายการใช้งานระบบการเข้ารหัสข้อมูลและการบริหารกุญแจเข้ารหัสข้อมูลตามข้อกำหนด 8(2) ควรมีเนื้อหาที่คำนึงถึงชนิด และขั้นตอนวิธีการเข้ารหัสข้อมูล (algorithm) ที่สอดคล้องเหมาะสมกับระดับความเสี่ยงที่อาจเกิดขึ้นกับข้อมูลที่เป็นความลับหรือมีความสำคัญ รวมทั้งกำหนดผู้รับผิดชอบในการดำเนินนโยบายและบริหารจัดการกุญแจเพื่อการเข้ารหัสข้อมูล (key management)

2. ผู้ประกอบธุรกิจควรจัดให้มีนโยบายการบริหารกุญแจเพื่อการเข้ารหัสข้อมูลตามแนวทางปฏิบัติข้อ 1 ตลอดช่วงเวลาการใช้งาน (key management whole life cycle) โดยกำหนดแนวปฏิบัติเพื่อการคัดเลือกวิธีการเข้ารหัส การกำหนดความยาวของรหัส การใช้งานและการยกเลิกการใช้งานกุญแจเพื่อการเข้ารหัส กระบวนการบริหารจัดการกุญแจเพื่อการเข้ารหัส รวมทั้งติดตามให้มีการปฏิบัติให้เป็นไปตามนโยบายและแนวทางปฏิบัติดังกล่าวอย่างสม่ำเสมอ

7. การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม (physical and environmental security)

7.1 พื้นที่หวงห้าม (secure areas)

วัตถุประสงค์

เพื่อป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าถึงพื้นที่หวงห้าม เช่น ศูนย์คอมพิวเตอร์ (data center) ศูนย์สำรอง (backup site) และพื้นที่ที่ตั้งอุปกรณ์ระบบเครือข่ายคอมพิวเตอร์ ได้แก่ floor swith หรือ router ซึ่งอาจก่อให้เกิดความเสียหายต่ออุปกรณ์สารสนเทศหรือมีผลกระทบต่อข้อมูลที่เป็นความลับหรือมีความสำคัญ

ข้อกำหนดในประกาศที่ สธ. 37/2559

ข้อ 18 ผู้ประกอบธุรกิจต้องมีมาตรการเพื่อสร้างความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (physical and environmental security) ของทรัพย์สินสารสนเทศตามหลักเกณฑ์ดังต่อไปนี้

(1) ประเมินความเสี่ยงและความสำคัญของทรัพย์สินสารสนเทศ

(2) กำหนดพื้นที่หวงห้ามและพื้นที่สำหรับจัดวางทรัพย์สินสารสนเทศที่มีความสำคัญให้มีความมั่นคงปลอดภัยและป้องกันมิให้บุคคลที่ไม่เกี่ยวข้องเข้าถึงพื้นที่ดังกล่าว

แนวทางปฏิบัติเพิ่มเติมจากข้อกำหนด

1. ผู้ประกอบธุรกิจควรออกแบบพื้นที่หวงห้ามโดยคำนึงถึงความมั่นคงปลอดภัยจากภัยธรรมชาติและภัยคุกคามจากมนุษย์ และให้มีความมิดชิด รวมทั้งป้องกันมิให้มีการเปิดเผยข้อมูลและรายละเอียดของพื้นที่หวงห้ามต่อสาธารณะ

2. ผู้ประกอบธุรกิจควรกำหนดสิทธิการเข้าออกพื้นที่หวงห้ามให้เฉพาะบุคคลที่มีหน้าที่เกี่ยวข้อง รวมทั้งควรจัดให้มีระบบการควบคุมการเข้าออกอย่างรัดกุม และทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

3. ผู้ประกอบธุรกิจควรจัดให้มีการรักษาความมั่นคงปลอดภัยให้กับศูนย์คอมพิวเตอร์ เช่น มีระบบกล้องวงจรปิด อุปกรณ์เตือนไฟไหม้ ถังดับเพลิงหรือระบบดับเพลิงแบบอัตโนมัติ ระบบไฟฟ้าสำรอง (uninterrupted power supply) และระบบควบคุมอุณหภูมิและความชื้นที่เหมาะสม เป็นต้น พร้อมทั้งมีการบำรุงรักษาอย่างสม่ำเสมอ

4. ผู้ประกอบธุรกิจควรมีการติดตามและควบคุมบุคคลภายนอกที่เข้าปฏิบัติงานภายในพื้นที่หวงห้ามอย่างใกล้ชิด

5. ผู้ประกอบธุรกิจควรแยกพื้นที่จุดรับส่งของ (delivery and loading area) ซึ่งเป็นพื้นที่ส่วนที่ต้องมีการเข้าถึงโดยพนักงานฝ่ายอื่น เช่น ส่วนที่ใช้เก็บรายงานที่ฝ่ายคอมพิวเตอร์ได้จัดพิมพ์ให้หน่วยงานต่าง ๆ เป็นต้น ออกจากศูนย์คอมพิวเตอร์

6. ผู้ประกอบธุรกิจควรจัดเก็บอุปกรณ์คอมพิวเตอร์ที่สำคัญ เช่น เครื่องแม่ข่าย อุปกรณ์เครือข่าย เป็นต้น ไว้ในพื้นที่หวงห้ามอย่างมั่นคงปลอดภัย

7.2 ทรัพย์สินสารสนเทศประเภทอุปกรณ์ (equipment)

วัตถุประสงค์
เพื่อป้องกันทรัพย์สินสารสนเทศประเภทอุปกรณ์มิให้สูญหาย ถูกโจรกรรม เกิดความเสียหาย เข้าถึงหรือถูกใช้งานโดยบุคคลที่ไม่เกี่ยวข้อง รวมทั้งเพื่อให้ทรัพย์สินดังกล่าวสามารถทำงานได้อย่างต่อเนื่อง

ข้อกำหนดในประกาศที่ สธ. 37/2559

ข้อ 19 ในกรณีที่เป็นทรัพย์สินสารสนเทศประเภทอุปกรณ์ นอกจากมาตรการเพื่อสร้างความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อมของทรัพย์สินสารสนเทศตามข้อ 18 แล้ว ผู้ประกอบธุรกิจต้องป้องกันทรัพย์สินดังกล่าวมิให้เกิดความเสียหาย สูญหาย ถูกโจรกรรม เข้าถึง หรือถูกใช้งานโดยบุคคลที่ไม่เกี่ยวข้อง เพื่อให้สามารถปฏิบัติงานได้อย่างต่อเนื่อง

แนวทางปฏิบัติเพิ่มเติมจากข้อกำหนด

1. ผู้ประกอบธุรกิจควรจัดให้มีการป้องกันทรัพย์สินสารสนเทศประเภทอุปกรณ์ที่อาจหยุดชะงักจากการทำงานผิดพลาดของระบบโครงสร้างพื้นฐาน เช่น ระบบไฟฟ้า ระบบโทรคมนาคม ระบบระบายอากาศ และระบบปรับอากาศ เป็นต้น

2. ผู้ประกอบธุรกิจควรจัดให้มีมาตรการป้องกันสายเคเบิลที่ใช้เพื่อการสื่อสาร สายไฟ และอุปกรณ์ที่เกี่ยวข้อง เช่น floor switch และท่อเดินสายเคเบิลและสายไฟ อย่างรัดกุมและบำรุงรักษาอย่างสม่ำเสมอ เพื่อมิให้มีความเสียหาย

3. ผู้ประกอบธุรกิจควรจัดให้มีการดูแลและบำรุงรักษาทรัพย์สินสารสนเทศประเภทอุปกรณ์อย่างถูกวิธี เพื่อให้คงไว้ซึ่งความถูกต้องครบถ้วนและอยู่ในสภาพพร้อมใช้งานอยู่เสมอ

4. ผู้ประกอบธุรกิจควรควบคุมมิให้มีการนำทรัพย์สินสารสนเทศประเภทอุปกรณ์ออกนอกพื้นที่โดยมิได้รับอนุญาต โดยในกรณีที่ได้รับอนุญาต ผู้ประกอบธุรกิจควรจัดให้มีการทำทะเบียนคุมและมีกระบวนการรักษาความมั่นคงปลอดภัย โดยให้คำนึงถึงระดับความเสี่ยงที่แตกต่างกันจากการนำไปใช้งานในสถานที่ต่าง ๆ

5. ก่อนการยกเลิกการใช้งานหรือจำหน่ายทรัพย์สินสารสนเทศประเภทอุปกรณ์ด้านเครือข่าย เช่น switch, firewall และ router เป็นต้น ผู้ประกอบธุรกิจควรตรวจสอบทรัพย์สินนั้นว่าได้มีการลบ ย้าย ทำลายข้อมูลเกี่ยวกับการปรับแต่ง (configuration) ที่สำคัญ หรือปรับค่าดังกล่าวกลับไปสู่ค่าตั้งต้น (restore from factory) ด้วยวิธีการที่ทำให้มั่นใจได้ว่าไม่สามารถกู้คืนได้อีก

6. ผู้ประกอบธุรกิจควรจัดให้มีการควบคุมป้องกันทรัพย์สินสารสนเทศประเภทอุปกรณ์ระหว่างที่ไม่มีผู้ใช้งาน (unattended user equipment) ให้มีความปลอดภัย รวมทั้งควรกำหนดการควบคุมเอกสารข้อมูลหรือสื่อบันทึกข้อมูลต่าง ๆ เช่น thumb drive และ external hard disk ที่มีข้อมูลสารสนเทศที่จัดเก็บหรือบันทึกอยู่ ไม่ให้วางทิ้งไว้บนโต๊ะทำงานหรือสถานที่ไม่ปลอดภัยในขณะที่ไม่ได้ใช้งาน (clear desk) ตลอดจนการควบคุมหน้าจอคอมพิวเตอร์ไม่ให้มีข้อมูลสำคัญปรากฏในขณะที่ไม่ได้ใช้งาน (clear screen) เช่น การตัดออกจากระบบ (session time out) หรือการล็อคหน้าจอ (lock screen) อัตโนมัติ เป็นต้น

8. การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ (operations security)

8.1 หน้าที่ความรับผิดชอบและขั้นตอนการปฏิบัติงาน (operational procedures and responsibilities)

วัตถุประสงค์
เพื่อให้มั่นใจว่าการปฏิบัติงานด้านระบบสารสนเทศเป็นไปอย่างถูกต้องและมั่นคงปลอดภัย

ข้อกำหนดในประกาศที่ สธ. 37/2559

ข้อ 23 ผู้ประกอบธุรกิจต้องมีมาตรการรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ (operations security) ตามหลักเกณฑ์ดังต่อไปนี้

(1) กำหนดขั้นตอนการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศเพื่อให้การปฏิบัติงานนั้นเป็นไปอย่างถูกต้องและมั่นคงปลอดภัย

แนวทางปฏิบัติเพิ่มเติมจากข้อกำหนด

1. ผู้ประกอบธุรกิจควรกำหนดขั้นตอนการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศเป็นลายลักษณ์อักษร เพื่อให้พนักงานปฏิบัติการคอมพิวเตอร์ (computer operator) สามารถปฏิบัติงานได้อย่างถูกต้องและเป็นไปตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ เช่น ขั้นตอนในการเปิด - ปิดระบบ การประมวลผล การตรวจสอบประสิทธิภาพการทำงานของระบบ และตารางเวลาในการปฏิบัติงาน เป็นต้น และควรทบทวนขั้นตอนการปฏิบัติงานดังกล่าวให้เป็นปัจจุบันอยู่เสมอ รวมทั้งจัดให้อยู่ในสภาพที่พร้อมใช้งานและเข้าถึงได้อยู่เสมอ

2. ผู้ประกอบธุรกิจควรจัดให้มีการควบคุมการปฏิบัติงานอย่างเคร่งครัด โดยเฉพาะในกรณีที่มีการเปลี่ยนแปลงโครงสร้างระบบงาน ขั้นตอนการปฏิบัติงาน หรือการทำงานของระบบงานต่าง ๆ ซึ่งอาจกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ ตัวอย่างของการควบคุมดังกล่าว เช่น

- กำหนดขั้นตอนหรือวิธีปฏิบัติที่เป็นลายลักษณ์อักษร ในกรณีการเปลี่ยนแปลงที่มีนัยสำคัญ
- มีแผนรองรับ และดำเนินการทดสอบภายหลังการเปลี่ยนแปลง
- มีการประเมินผลกระทบที่อาจเกิดขึ้นจากการเปลี่ยนแปลง
- มีขั้นตอนการขออนุมัติจากผู้มีอำนาจ
- มีขั้นตอนการตรวจสอบเพื่อให้มั่นใจว่ากระบวนการเปลี่ยนแปลงดังกล่าวเป็นไปตามนโยบายด้านความมั่นคงปลอดภัยของระบบสารสนเทศ
- มีการสื่อสารให้บุคคลที่เกี่ยวข้องได้รับทราบเพื่อให้สามารถปฏิบัติงานได้อย่างถูกต้อง
- มีกระบวนการถอยกลับสู่สภาพเดิม (fall-back) ของระบบงาน หากเกิดข้อผิดพลาดระหว่างการเปลี่ยนแปลง

3. ผู้ประกอบธุรกิจควรติดตามประสิทธิภาพการทำงานของระบบสารสนเทศและทรัพย์สินสารสนเทศประเภทอุปกรณ์ที่สำคัญ ให้ทำงานได้อย่างต่อเนื่องและมีประสิทธิภาพ เพื่อใช้เป็นข้อมูลในการประเมินสมรรถภาพและความเพียงพอ (capacity) ของระบบสารสนเทศ ทรัพย์สินสารสนเทศประเภทอุปกรณ์และบุคลากร รวมถึงเพื่อให้สามารถรองรับแผนการปฏิบัติงานในอนาคตได้อย่างมีประสิทธิภาพด้วย

4. ผู้ประกอบธุรกิจควรแบ่งแยกส่วนคอมพิวเตอร์ที่มีไว้สำหรับการพัฒนาระบบงาน (develop environment) และใช้งานจริง (production environment) ออกจากกัน และควบคุมให้มีการเข้าถึงเฉพาะผู้ที่เกี่ยวข้องในแต่ละส่วนเท่านั้น ทั้งนี้ การแบ่งแยกส่วนดังกล่าวอาจแบ่งโดยใช้เครื่องคอมพิวเตอร์คนละเครื่อง หรือแบ่งโดยการจัดเนื้อที่แยกไว้ต่างหากภายในเครื่องคอมพิวเตอร์เดียวกันก็ได้

8.2 การป้องกันภัยคุกคามจากโปรแกรมไม่ประสงค์ดี (protection from malware)

วัตถุประสงค์
เพื่อให้มั่นใจว่าระบบสารสนเทศได้รับการป้องกันภัยคุกคามจากโปรแกรมไม่ประสงค์ดี

ข้อกำหนดในประกาศที่ สธ. 37/2559

ข้อ 23 ผู้ประกอบธุรกิจต้องมีมาตรการรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ (operations security) ตามหลักเกณฑ์ดังต่อไปนี้

(2) มีมาตรการป้องกันและตรวจสอบโปรแกรมไม่ประสงค์ดี (malware) และมาตรการในการแก้ไขระบบสารสนเทศให้สามารถกลับมาใช้งานได้ตามปกติ

แนวทางปฏิบัติเพิ่มเติมจากข้อกำหนด

1. ในการกำหนดมาตรการป้องกันและตรวจสอบโปรแกรมไม่ประสงค์ดี และมาตรการในการแก้ไขระบบสารสนเทศเพื่อให้กลับมาใช้งานได้ตามปกติ (recovery) ตามข้อกำหนด 23(2) นั้น ผู้ประกอบธุรกิจควรมีมาตรการขั้นต่ำ ดังนี้

(1) กำหนดนโยบายห้ามใช้ซอฟต์แวร์ที่ไม่ได้รับอนุญาต
(2) มีกระบวนการป้องกัน และตรวจสอบการใช้ซอฟต์แวร์ที่ไม่ได้รับอนุญาต และการใช้งานเว็บไซต์ที่อาจมีโปรแกรมไม่ประสงค์ดี
(3) ติดตั้งซอฟต์แวร์ตรวจสอบโปรแกรมไม่ประสงค์ดี และปรับปรุงให้เป็นปัจจุบันอย่างสม่ำเสมอ พร้อมทั้งกำหนดผู้มีหน้าที่รับผิดชอบให้รายงานและแก้ไขปัญหากรณีพบภัยคุกคาม
(4) ตรวจสอบซอฟต์แวร์ระบบงานที่มีความสำคัญอย่างสม่ำเสมอ หากพบการติดตั้งหรือเปลี่ยนแปลงที่ไม่ได้รับอนุญาต ควรจัดให้มีการตรวจสอบ

(5) จัดให้มีการติดตามและกลั่นกรองข่าวสารเกี่ยวกับภัยคุกคาม เพื่อให้ทราบข้อเท็จจริง รวมทั้งแจ้งให้ผู้ที่เกี่ยวข้องได้ตระหนักถึงภัยคุกคามดังกล่าว

8.3 การสำรองข้อมูล (backup)

วัตถุประสงค์
เพื่อป้องกันการสูญหายของข้อมูล

ข้อกำหนดในประกาศที่ สธ. 37/2559

ข้อ 23 ผู้ประกอบธุรกิจต้องมีมาตรการรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ (operations security) ตามหลักเกณฑ์ดังต่อไปนี้

(3) มีการสำรองข้อมูลสำคัญทางธุรกิจ ระบบปฏิบัติการ โปรแกรมประยุกต์ ระบบงานคอมพิวเตอร์ และชุดคำสั่งที่ใช้ทำงาน ไว้อย่างครบถ้วน และต้องมีการทดสอบข้อมูลสำรองและกระบวนการกู้คืนข้อมูลอย่างน้อยปีละ 1 ครั้ง

แนวทางปฏิบัติเพิ่มเติมจากข้อกำหนด

1. ผู้ประกอบธุรกิจควรจัดให้มีนโยบายสำรองข้อมูลสำคัญทางธุรกิจ รวมถึงระบบปฏิบัติการ (operating system) แอพพลิเคชั่นระบบงานคอมพิวเตอร์ (application system) และชุดคำสั่งที่ใช้ทำงานให้ครบถ้วน ให้สามารถพร้อมใช้งานได้อย่างต่อเนื่อง โดยขั้นต่ำควรพิจารณา ดังนี้

(1) กำหนดขั้นตอนหรือวิธีปฏิบัติในการสำรองข้อมูลเพื่อเป็นแนวทางให้แก่ผู้ปฏิบัติงาน โดยอย่างน้อยควรมีรายละเอียดเกี่ยวกับ

(ก) ข้อมูลที่ต้องสำรอง

(ข) ความถี่ในการสำรอง

(ค) ประเภทสื่อบันทึกข้อมูล

(ง) จำนวนที่ต้องสำรอง

(จ) ขั้นตอนและวิธีการสำรองโดยละเอียด

(ฉ) สถานที่และวิธีการเก็บรักษาสื่อบันทึกข้อมูล

(ช) กระบวนการกู้คืนข้อมูลในกรณีที่สูญหาย

(2) จัดเก็บสื่อบันทึกข้อมูลสำรอง พร้อมทั้งสำเนาขั้นตอนหรือวิธีปฏิบัติต่าง ๆ ไว้นอกสถานที่ เพื่อความปลอดภัยในกรณีที่สถานที่ปฏิบัติงานได้รับความเสียหาย โดยสถานที่ดังกล่าวควรจัดให้มีระบบควบคุมการเข้าออกและระบบป้องกันความเสียหายตามที่กล่าวในหัวข้อการสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อมด้วย

(3) กำหนดเป้าหมายในการกู้คืนข้อมูล เช่น กำหนดประเภทของข้อมูล และชุดข้อมูลล่าสุดที่จะกู้คืนได้ (recovery point objective : RPO)

(4) ในกรณีที่จำเป็นต้องจัดเก็บข้อมูลเป็นระยะเวลานาน ควรคำนึงถึงวิธีการนำข้อมูลกลับมาใช้งานในอนาคตด้วย เช่น กรณีที่จัดเก็บข้อมูลในสื่อบันทึกประเภทใด ควรมีการเก็บอุปกรณ์และโปรแกรมที่เกี่ยวข้องสำหรับใช้อ่านสื่อบันทึกประเภทนั้นไว้ด้วยเช่นกัน เป็นต้น

8.4 การบันทึก จัดเก็บหลักฐานและติดตาม (logging and monitoring)

วัตถุประสงค์

เพื่อบันทึกและจัดเก็บหลักฐานการใช้งานเกี่ยวกับระบบสารสนเทศอย่างครบถ้วนและเพียงพอสำหรับการตรวจสอบการล่วงรู้ข้อมูลภายในระหว่างหน่วยงานและบุคลากร การสอบทานการใช้งานข้อมูลและระบบสารสนเทศตามหน้าที่ที่ผู้ปฏิบัติงานได้รับมอบหมาย การตรวจสอบการเข้าใช้งานระบบสารสนเทศโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง การตรวจสอบและป้องกันการใช้งานระบบสารสนเทศที่มีความผิดปกติหรือไม่เป็นไปตามกฎหมายหรือหลักเกณฑ์ของทางการ และการตรวจสอบตัวตนของลูกค้าที่ทำรายการซื้อขายผ่านระบบอินเทอร์เน็ต รวมทั้งเพื่อให้มีการติดตามและวิเคราะห์หลักฐานที่จัดเก็บ

ข้อกำหนดในประกาศที่ สธ. 37/2559

ข้อ 23 ผู้ประกอบธุรกิจต้องมีมาตรการรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ (operations security) ตามหลักเกณฑ์ดังต่อไปนี้

(4) จัดเก็บและบันทึกหลักฐาน (logs) ต่าง ๆ ให้ครบถ้วนและเพียงพอสำหรับการตรวจสอบการล่วงรู้ข้อมูลภายในระหว่างหน่วยงานและบุคลากร การสอบทานการใช้งานข้อมูลและระบบสารสนเทศตามหน้าที่ที่ผู้ปฏิบัติงานได้รับมอบหมาย การตรวจสอบการเข้าใช้งานระบบสารสนเทศโดยบุคคลที่ไม่มีหน้าที่เกี่ยวข้อง การตรวจสอบและป้องกันการใช้งานระบบสารสนเทศที่มีความผิดปกติหรือไม่เป็นไปตามกฎหมายหรือกฎเกณฑ์ที่เกี่ยวข้อง และการตรวจสอบตัวตนของลูกค้าที่ทำรายการซื้อขายผ่านระบบอิเล็กทรอนิกส์ ทั้งนี้ ตามตารางแสดงรายละเอียดการจัดเก็บหลักฐานที่แนบท้ายประกาศนี้ โดยต้องมีการติดตามและวิเคราะห์หลักฐานที่จัดเก็บสำหรับการใช้งานสารสนเทศที่มีความสำคัญให้สอดคล้องกับการประเมินความเสี่ยงขององค์กร

ตารางแสดงรายละเอียดการจัดเก็บหลักฐาน

ประเภทหลักฐานที่ต้องจัดเก็บ	รายละเอียดขั้นต่ำ	ระยะเวลาจัดเก็บขั้นต่ำ
หลักฐานการเข้าถึงพื้นที่หวงห้าม (physical access log)	บุคคลที่เข้าถึง / วันเวลาที่ผ่านเข้าออก / ความพยายามในการเข้าถึง (ถ้ามี)	ไม่น้อยกว่า 3 เดือน
หลักฐานการเข้าถึงระบบปฏิบัติการ ฐานข้อมูล และระบบเครือข่ายคอมพิวเตอร์ (authentication log)	บัญชีผู้ใช้งาน / วันเวลาที่เข้าใช้งาน / ความพยายามในการเข้าใช้งาน	ไม่น้อยกว่า 3 เดือน

ข้อกำหนดในประกาศที่ สธ. 37/2559

ตารางแสดงรายละเอียดการจัดเก็บหลักฐาน

ประเภทหลักฐานที่ต้องจัดเก็บ	รายละเอียดขั้นต่ำ	ระยะเวลาจัดเก็บขั้นต่ำ
หลักฐานการเข้าถึงและใช้งานระบบสารสนเทศ (application log)	บัญชีผู้ใช้งาน / หมายเลขประจำเครื่องที่ใช้งาน (IP address) / วันเวลาที่มีการใช้งาน --- กรณีที่เป็นระบบสารสนเทศเพื่อการซื้อขายหลักทรัพย์ (trading system) ให้เพิ่มรายละเอียดชื่อย่อหลักทรัพย์ (securities symbol) / หมายเลขบริษัทสมาชิก (broker No. 4 หลัก : xxxx) / เลขที่คำสั่งซื้อขายหลักทรัพย์ (SET order ID) / เลขที่บัญชีซื้อขายหลักทรัพย์ (account ID) / วันและเวลาในการส่งคำสั่งซื้อขายหลักทรัพย์ (yyyy/mm/dd - hh:mm:ss:sss) / หมายเลข Public และ Local IP address ต้นทาง (source) / หมายเลข IP address ปลายทาง(destination) / ที่อยู่ของเว็บไซต์ปลายทาง (full URL) / terminal type (ถ้ามี) เช่น iPad, iPhone เป็นต้น --- ทั้งนี้ ผู้ประกอบธุรกิจต้องสามารถระบุตัวตนผู้ใช้งาน และ local IP address ในช่วงเวลาที่ใช้งานได้ (เฉพาะการใช้งานผ่านอุปกรณ์ของบริษัท)	ไม่น้อยกว่า 1 ปี สำหรับผู้ประกอบธุรกิจนายหน้าซื้อขายหลักทรัพย์ การค้าหลักทรัพย์ หรือการจัดจำหน่ายหลักทรัพย์ซึ่งมิได้จำกัดเฉพาะหลักทรัพย์อันเป็นตราสารแห่งหนี้หรือหน่วยลงทุน และตัวแทนซื้อขายสัญญาซื้อขายล่วงหน้า ไม่น้อยกว่า 6 เดือน สำหรับผู้ประกอบธุรกิจประเภทอื่น
หลักฐานการใช้งานอินเทอร์เน็ตผ่านระบบเครือข่ายคอมพิวเตอร์ภายในของผู้ประกอบธุรกิจ (internet access log)	บัญชีผู้ใช้งาน / หมายเลขประจำเครื่องที่ใช้งาน (IP address) / หมายเลขอินเทอร์เน็ตของผู้ประกอบธุรกิจ (organization IP address) / วันเวลาที่มีการใช้งาน / ที่อยู่ของเว็บไซต์ปลายทาง (full URL) --- ทั้งนี้ ผู้ประกอบธุรกิจต้องสามารถระบุตัวตนผู้ใช้งาน และ IP address ในช่วงเวลาที่ใช้งานได้	
หลักฐานการใช้งานแฟ้มข้อมูล (audit log)*	บัญชีผู้ใช้งาน / วันเวลาที่เข้าใช้งาน / บันทึกการเรียกดูและการแก้ไขข้อมูล	ไม่น้อยกว่า 6 เดือน
หลักฐานการบริหาร (event log) ระบบปฏิบัติการ และ network firewall	วันและเวลาที่เกิดเหตุการณ์ / เหตุการณ์ที่เกิดขึ้นกับ OS (event services) เช่น สถานะการให้บริการของ service /เหตุการณ์ที่เกิดขึ้นกับ network firewall เช่น การปรับปรุงหรือแก้ไข firewall rules	ระยะเวลาตามที่จำเป็นและเพียงพอสำหรับการตรวจสอบซึ่งสอดคล้องกับความเสี่ยงที่ผู้ประกอบธุรกิจได้ประเมินไว้
หลักฐานบันทึกข้อมูลจราจรคอมพิวเตอร์ของ network firewall (network firewall log)	วันและเวลา / IP address ต้นทาง (source) และปลายทาง (destination) / firewall action / port ที่ใช้ติดต่อ	
หลักฐานการจัดการบริหารข้อมูล (database log)	บัญชีผู้ใช้งาน / วันเวลาที่เข้าใช้งาน	
หลักฐานการติดต่อสนทนาผ่านช่องทางอิเล็กทรอนิกส์ (electronic messaging)**	บัญชีผู้ใช้งาน / วันเวลาที่เข้าใช้งาน / ข้อมูลการติดต่อตลอดระยะเวลาการสนทนา	ไม่น้อยกว่า 6 เดือน

* จัดเก็บเฉพาะบุคคลที่สามารถเข้าถึงข้อมูลภายใน (“access person”) ของผู้ประกอบธุรกิจทุกประเภท

** จัดเก็บเฉพาะบุคคลที่สามารถเข้าถึงข้อมูลภายใน (“access person”) ของผู้ประกอบธุรกิจนายหน้าซื้อขายหลักทรัพย์ การค้าหลักทรัพย์ หรือการจัดจำหน่ายหลักทรัพย์ ซึ่งมิได้จำกัดเฉพาะหลักทรัพย์อันเป็นตราสารแห่งหนี้หรือหน่วยลงทุน ตัวแทนซื้อขายสัญญาซื้อขายล่วงหน้า และผู้ประกอบธุรกิจจัดการกองทุนรวมหรือกองทุนส่วนบุคคล เท่านั้น

*** นิยามว่าด้วย access person ให้เป็นไปตามประกาศแนวปฏิบัติว่าด้วยการกำหนดนโยบาย มาตรการ และระบบงานที่เกี่ยวกับการกระทำที่อาจมีความขัดแย้งทางผลประโยชน์กับลูกค้า

แนวทางปฏิบัติเพิ่มเติมจากข้อกำหนด

1. ผู้ประกอบธุรกิจควรจัดให้มีการป้องกันข้อมูลและระบบการบันทึกและจัดเก็บหลักฐานการใช้งานเกี่ยวกับระบบสารสนเทศของผู้ใช้งานทั่วไป รวมถึง system administrator logs และ system operator logs จากการถูกเปลี่ยนแปลงแก้ไข ทำความเสียหาย หรือเข้าถึงโดยไม่ได้รับอนุญาต และมีการตรวจสอบอย่างน้อยปีละ 1 ครั้งและเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ

2. ผู้ประกอบธุรกิจที่เป็นสมาชิกของตลาดหลักทรัพย์ควรกำหนดระบบเวลาของอุปกรณ์และระบบสารสนเทศที่เกี่ยวกับการซื้อขายหลักทรัพย์และการชำระราคาให้ตรงกับเวลาอ้างอิงของระบบซื้อขายหลักทรัพย์ของตลาดหลักทรัพย์ ทั้งนี้ เพื่อให้การตรวจสอบธุรกรรมที่ไม่เหมาะสมทั้งหมดเป็นไปอย่างถูกต้องและมีประสิทธิภาพ

3. กรณีที่ผู้ประกอบธุรกิจใช้งานระบบสารสนเทศที่มีความสำคัญร่วมกันกับบริษัทในเครือที่อยู่ในต่างประเทศ ผู้ประกอบธุรกิจอาจกำหนดให้บริษัทในเครือนั้นเป็นผู้ติดตามวิเคราะห์หลักฐาน พร้อมทั้งจัดเก็บผลการวิเคราะห์ดังกล่าวได้

8.5 การควบคุมการติดตั้งซอฟต์แวร์บนระบบงาน (installation of software on operational systems)

วัตถุประสงค์
เพื่อควบคุมให้ระบบงานทำงานโดยมีความถูกต้อง ครบถ้วน และน่าเชื่อถือ (integrity of operational system)

ข้อกำหนดในประกาศที่ สธ. 37/2559

ข้อ 23 ผู้ประกอบธุรกิจต้องมีมาตรการรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ (operations security) ตามหลักเกณฑ์ดังต่อไปนี้

(5) มีขั้นตอนควบคุมการติดตั้งซอฟท์แวร์บนระบบงาน และมีมาตรการจำกัดการติดตั้งซอฟท์แวร์โดยผู้ใช้งาน เพื่อให้ระบบปฏิบัติงานต่าง ๆ มีความถูกต้องครบถ้วนและน่าเชื่อถือ

แนวทางปฏิบัติเพิ่มเติมจากข้อกำหนด

- ไม่มีแนวปฏิบัติเพิ่มเติม -

8.6 การบริหารจัดการช่องโหว่ทางเทคนิค (technical vulnerability management)

วัตถุประสงค์
เพื่อป้องกันภัยคุกคามจากช่องโหว่ทางเทคนิค

ข้อกำหนดในประกาศที่ สธ. 37/2559

ข้อ 23 ผู้ประกอบธุรกิจต้องมีมาตรการรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ (operations security) ตามหลักเกณฑ์ดังต่อไปนี้

(6) มีระบบในการบริหารจัดการกรณีช่องโหว่ทางเทคนิค (technical vulnerability management) ที่อาจเกิดขึ้นอย่างเพียงพอและเหมาะสมดังนี้

(ก) มีการทดสอบการเจาะระบบ (penetration test) กับระบบงานที่มีความสำคัญที่เชื่อมต่อกับระบบเครือข่ายภายนอก (untrusted network) โดยบุคคลที่เป็นอิสระจากหน่วยงานที่รับผิดชอบด้านเทคโนโลยีสารสนเทศ และเป็นไปตามการวิเคราะห์ความเสี่ยงและผลกระทบทางธุรกิจ (risk and business impact analysis) ดังนี้

1. กรณีที่เป็นระบบงานสำคัญที่ประเมินแล้วมีความสำคัญสูง ต้องทดสอบอย่างน้อยทุก 3 ปี และเมื่อมีการเปลี่ยนแปลงระบบงานดังกล่าวอย่างมีนัยสำคัญ

2. กรณีที่เป็นระบบงานที่มีความสำคัญอื่น ๆ ต้องทดสอบอย่างน้อยทุก 6 ปี

(ข) มีการประเมินช่องโหว่ของระบบ (vulnerability assessment) กับระบบงานที่มีความสำคัญทุกระบบอย่างน้อยปีละ 1 ครั้งและเมื่อมีการเปลี่ยนแปลงระบบงานดังกล่าวอย่างมีนัยสำคัญ และรายงานผลไปยังหน่วยงานกำกับการปฏิบัติงาน หรือหน่วยงานตรวจสอบภายในโดยไม่ชักช้า

แนวทางปฏิบัติเพิ่มเติมจากข้อกำหนด

1. ผู้ประกอบธุรกิจควรจัดให้มีการติดตามข้อมูลข่าวสารเกี่ยวกับช่องโหว่ทางเทคนิคที่อาจเป็นความเสี่ยงต่อระบบสารสนเทศของผู้ประกอบธุรกิจอย่างทันต่อเหตุการณ์ รวมทั้งควรจัดให้มีการตรวจสอบหาช่องโหว่ดังกล่าวและมีมาตรการดำเนินการเพื่อปิดช่องโหว่หรือกำหนดแผนรองรับกรณีที่ระบบถูกบุกรุกผ่านช่องโหว่ดังกล่าว โดยควรกำหนดแนวทางดำเนินการดังนี้

(1) กำหนดผู้มีหน้าที่รับผิดชอบในการจัดการเกี่ยวกับช่องโหว่ทางเทคนิค โดยครอบคลุมถึงการประเมินความเสี่ยงของทรัพย์สินสารสนเทศที่เกี่ยวข้องซึ่งอาจได้รับผลกระทบจากช่องโหว่ดังกล่าว โดยเฉพาะทรัพย์สินสารสนเทศที่มีความเสี่ยงสูง การดำเนินการเพื่อปิดช่องโหว่ (patching) และการประสานงานกับบุคคลที่เกี่ยวข้อง

(2) จัดให้มีการปิดช่องโหว่ที่พบโดยไม่ชักช้า โดยควรมีการประเมินความเสี่ยงของโปรแกรมเพื่อปิดช่องโหว่ (patches) ก่อนการติดตั้งโปรแกรมเพื่อทดสอบและประเมินผลกระทบที่อาจเกิดจากการติดตั้งโปรแกรมดังกล่าว ทั้งนี้ กรณีที่ไม่มีโปรแกรมเพื่อปิดช่องโหว่ ให้ปฏิบัติตามคำแนะนำของบริษัทผู้ผลิตทรัพย์สินสารสนเทศที่เกี่ยวข้อง

(3) มีกระบวนการจัดการช่องโหว่ด้านเทคนิคที่สอดคล้องกับกระบวนการจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (incident management) เพื่อเตรียมความพร้อมรองรับกรณีที่ระบบถูกบุกรุกผ่านช่องโหว่ ทั้งนี้ ให้รวมถึงกรณีที่ตรวจพบช่องโหว่แต่ยังไม่สามารถหาวิธีปิดช่องโหว่ได้

(4) มีการบันทึกและจัดเก็บหลักฐานเพื่อการตรวจสอบในการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับการจัดการช่องโหว่ทางเทคนิค ทั้งนี้ กรณีที่ผู้ประกอบธุรกิจใช้วิธีปรับปรุงโปรแกรมเพื่อปิดช่องโหว่แบบอัตโนมัติ (automatic patching) สำหรับระบบหรืออุปกรณ์ใด ๆ ซึ่งผู้ประกอบธุรกิจได้ประเมินความเสี่ยงและผลกระทบจากการดำเนินการดังกล่าวแล้วพบว่าไม่สร้างความเสียหายต่อระบบงาน ผู้ประกอบธุรกิจอาจงดเว้นการบันทึกและจัดเก็บหลักฐานสำหรับการ patching ระบบหรืออุปกรณ์นั้นได้

8.7 การตรวจสอบระบบสารสนเทศ (information systems audit)

วัตถุประสงค์

เพื่อจัดให้มีการวางแผนการตรวจสอบระบบสารสนเทศอย่างเพียงพอเหมาะสม โดยการตรวจสอบดังกล่าวควรส่งผลกระทบต่อการปฏิบัติงานน้อยที่สุด

ข้อกำหนดในประกาศที่ สธ. 37/2559

ข้อ 23 ผู้ประกอบธุรกิจต้องมีมาตรการรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ (operations security) ตามหลักเกณฑ์ดังต่อไปนี้

(7) มีการตรวจสอบระบบสารสนเทศดังนี้

(ก) วางแผนการตรวจสอบระบบสารสนเทศให้สอดคล้องกับความเสี่ยงที่ได้ประเมินไว้

(ข) กำหนดขอบเขตในการตรวจสอบระบบสารสนเทศทางเทคนิคให้ครอบคลุมถึงจุดเสี่ยงที่สำคัญ โดยการตรวจสอบดังกล่าวต้องไม่กระทบต่อการปฏิบัติงาน

(ค) ตรวจสอบระบบสารสนเทศนอกเวลาทำงาน ในกรณีที่การตรวจสอบนั้นอาจส่งผลกระทบต่อความพร้อมในการใช้งานระบบดังกล่าว

แนวทางปฏิบัติเพิ่มเติมจากข้อกำหนด

- ไม่มีแนวปฏิบัติเพิ่มเติม -

9. การรักษาความมั่นคงปลอดภัยด้านการสื่อสารข้อมูลสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์ (communications security)

9.1 การบริหารจัดการระบบเครือข่ายคอมพิวเตอร์ (network security management)

วัตถุประสงค์
เพื่อป้องกันการกระทำที่มีความเสี่ยงต่อข้อมูลสารสนเทศในระบบเครือข่ายคอมพิวเตอร์ และป้องกันโครงสร้างพื้นฐานที่สนับสนุนระบบเครือข่ายคอมพิวเตอร์

ข้อกำหนดในประกาศที่ สธ. 37/2559

ข้อ 22 ผู้ประกอบธุรกิจต้องมีมาตรการรักษาความมั่นคงปลอดภัยด้านการสื่อสารข้อมูลสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์ (communications security) ให้เป็นไปตามหลักเกณฑ์ดังต่อไปนี้

(1) มีการบริหารจัดการและควบคุมระบบเครือข่ายคอมพิวเตอร์อย่างมั่นคงและปลอดภัย โดยต้องสามารถป้องกันมิให้เกิดการกระทำที่มีความเสี่ยงต่อข้อมูลสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์

(2) จัดทำข้อตกลงการใช้บริการผ่านระบบเครือข่ายคอมพิวเตอร์ที่เกี่ยวกับวิธีการบริหารจัดการคุณภาพการให้บริการ และกระบวนการรักษาความมั่นคงปลอดภัยของระบบเครือข่ายคอมพิวเตอร์กับผู้รับดำเนินการ

(3) แบ่งแยกระบบเครือข่ายคอมพิวเตอร์ตามความเหมาะสม โดยระบุขอบเขตของระบบเครือข่ายย่อยอย่างชัดเจน และมีกระบวนการควบคุมการเข้าถึงขอบเขตดังกล่าวอย่างเหมาะสม

แนวทางปฏิบัติเพิ่มเติมจากข้อกำหนด

1. การบริหารจัดการและควบคุมระบบเครือข่ายคอมพิวเตอร์อย่างมั่นคงปลอดภัยตามข้อกำหนด 22(1) ควรมีการดำเนินการขั้นต่ำ ดังนี้

(1) แบ่งแยกหน้าที่ความรับผิดชอบระหว่าง network administrator และ computer administrator ออกจากกัน พร้อมทั้งกำหนดหน้าที่ความรับผิดชอบและขั้นตอนในการบริหารจัดการระบบและอุปกรณ์เครือข่ายให้ชัดเจน

(2) จำกัดการเชื่อมต่อระบบคอมพิวเตอร์ระหว่างเครือข่าย เช่น จำกัดการใช้งานจุดเชื่อมต่อระบบเครือข่าย (port outlet)

(3) เปิดใช้งาน service port ที่เชื่อมต่อตามความจำเป็น พร้อมทั้งมีวิธีการเพื่อระบุถึงอุปกรณ์ที่เชื่อมต่อ (authenticate) อย่างชัดเจน เช่น IP address และประเภทของอุปกรณ์ เป็นต้น

(4) มีการควบคุมการเชื่อมต่อกับระบบเครือข่ายสาธารณะ (public network) และระบบเครือข่ายไร้สาย (wireless network) อย่างรัดกุม เพื่อป้องกันการรั่วไหลหรือเปลี่ยนแปลงแก้ไขข้อมูลที่ส่งผ่านระบบเครือข่ายดังกล่าว รวมทั้งเพื่อป้องกันระบบที่เชื่อมต่อและแอพพลิเคชั่นที่ใช้งาน เช่น การเข้ารหัส

เครือข่าย หรือการแบ่งแยกระบบเครือข่ายคอมพิวเตอร์ออกจากกัน เป็นต้น นอกจากนี้ ควรจัดให้มีการควบคุมเป็นพิเศษเพื่อให้ระบบเครือข่ายดังกล่าวอยู่ในสภาพที่พร้อมใช้งานอยู่เสมอ เช่น จัดให้มีระบบเครือข่ายคอมพิวเตอร์ที่ใช้งานทดแทนกันได้ (network load balance) เป็นต้น

(5) มีการบันทึกและจัดเก็บหลักฐาน (logs) ที่ติดต่อกับระบบงานสำคัญและมีความเสี่ยงสูง เพื่อติดตามตรวจสอบการทำงานที่เกี่ยวข้อง หรืออาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบเครือข่ายคอมพิวเตอร์ ทั้งนี้ กรณีการใช้งานอินเทอร์เน็ตที่เกิดขึ้นจากการใช้งานผ่านเครือข่ายสารสนเทศของผู้ประกอบธุรกิจ ให้บันทึกและจัดเก็บหลักฐาน internet access log ตามข้อ 8.4

9.2 การควบคุมการรับส่งข้อมูลสารสนเทศ (information transfer)

วัตถุประสงค์

เพื่อรักษาความมั่นคงปลอดภัยในการรับส่งข้อมูลสารสนเทศผ่านระบบเครือข่ายภายในองค์กร และระหว่างระบบเครือข่ายภายในองค์กรกับระบบเครือข่ายภายนอก

ข้อกำหนดในประกาศที่ สธ. 37/2559

ข้อ 8 ผู้ประกอบธุรกิจต้องจัดให้มีการกำหนดนโยบายอย่างน้อยในเรื่องดังต่อไปนี้ ไว้เป็นลายลักษณ์อักษรเพื่อรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (information security policy)

(3) นโยบายการรับส่งข้อมูลสารสนเทศผ่านระบบเครือข่ายภายในองค์กร และระหว่างเครือข่ายภายในองค์กรกับระบบเครือข่ายภายนอกองค์กร ให้มีความมั่นคงปลอดภัย

ข้อ 22 ผู้ประกอบธุรกิจต้องมีมาตรการรักษาความมั่นคงปลอดภัยด้านการสื่อสารข้อมูลสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์ (communications security) ให้เป็นไปตามหลักเกณฑ์ดังต่อไปนี้

(4) กำหนดมาตรการในการรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศที่มีการรับส่งผ่านระบบเครือข่ายคอมพิวเตอร์

(5) ดำเนินการให้บุคลากรของผู้ประกอบธุรกิจและผู้รับดำเนินการ (ถ้ามี) มีข้อตกลงเกี่ยวกับการรักษาความลับหรือไม่เปิดเผยข้อมูลที่มีความสำคัญ

แนวทางปฏิบัติเพิ่มเติมจากข้อกำหนด

1. ในการปฏิบัติให้เป็นไปตามข้อกำหนด 8(3) และ 22(4) ผู้ประกอบธุรกิจควรดำเนินการดังต่อไปนี้
   (1) จัดให้มีนโยบายและหลักปฏิบัติเพื่อปกป้องข้อมูลสารสนเทศที่รับส่งผ่านระบบและอุปกรณ์ในการสื่อสารทุกประเภท โดยมีเนื้อหาขั้นต่ำครอบคลุมถึง
   (ก) แนวปฏิบัติที่ดีในการรับส่งข้อมูลสารสนเทศผ่านช่องทางการสื่อสารอิเล็กทรอนิกส์ประเภทต่าง ๆ
   (ข) กระบวนการป้องกันการรับส่งข้อมูลสารสนเทศนอกเส้นทางที่ได้กำหนดไว้ (mis-routing) การดักรับสัญญาณ การเปลี่ยนแปลงแก้ไขหรือทำความเสียหายกับข้อมูล และโปรแกรมไม่ประสงค์ดี (malware) ที่ถูกส่งผ่านช่องทางการสื่อสาร

(ค) กระบวนการป้องกันข้อมูลที่เป็นความลับหรือมีความสำคัญที่รับส่งในรูปแบบของไฟล์แนบ (attachment files) และการส่งต่อจดหมายอิเล็กทรอนิกส์แบบอัตโนมัติออกสู่ภายนอกองค์กร

(ง) การนำเทคนิคการเข้ารหัสข้อมูลมาใช้ในการรับส่งข้อมูลสารสนเทศที่เป็นความลับและมีความสำคัญผ่านช่องทางการสื่อสารบางประเภทที่ต้องการการรักษาความมั่นคงปลอดภัย เช่น การใช้งานระบบ cloud computing เป็นต้น

(2) ในการใช้งานระบบรับส่งข้อมูลสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์ (electronic messaging) ผู้ประกอบธุรกิจควรกำหนดมาตรการในการรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศที่รับส่งผ่านช่องทางดังกล่าว โดยควรจัดให้มีมาตรการป้องกันการเปลี่ยนแปลงแก้ไข ทำความเสียหาย หรือเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และมีกระบวนการตรวจสอบผู้ใช้งานอย่างเข้มงวดในกรณีที่ใช้งานผ่านเครือข่ายสาธารณะรวมทั้งควรจัดการและควบคุมให้ระบบทำงานรับส่งข้อมูลได้อย่างถูกต้องและพร้อมใช้งานอยู่เสมอ ทั้งนี้ การใช้งานระบบรับส่งข้อมูลสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์ที่ให้บริการโดยบุคคลภายนอก เช่น โปรแกรมสนทนาผ่านระบบอิเล็กทรอนิกส์ (instant messaging) ระบบเครือข่ายสังคมออนไลน์ (social networking) หรือโปรแกรมเรียกใช้แฟ้มข้อมูลร่วมกัน (file sharing) ผู้ประกอบธุรกิจควรจัดให้มีการควบคุมดูแลอย่างเหมาะสมเพียงพอ เช่น มีการขออนุมัติก่อนการใช้งาน รวมถึงควรปฏิบัติตามกฎหมายและหลักเกณฑ์ของทางการอย่างเคร่งครัด

2. ข้อตกลงเกี่ยวกับการรักษาความลับหรือไม่เปิดเผยข้อมูลที่มีความสำคัญตามข้อกำหนด 22(5) ควรมีเนื้อหาขั้นต่ำครอบคลุมถึง

(1) การระบุความเป็นเจ้าของข้อมูลสำคัญทางธุรกิจ ทรัพย์สินทางปัญญา และวิธีป้องกันการรั่วไหลของข้อมูล

(2) การป้องกันการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต โดยจัดให้มีการลงนามโดยผู้รับผิดชอบ

(3) การกำหนดขั้นตอนการขออนุญาตเข้าถึงข้อมูลหรือกำหนดสิทธิการเข้าถึงข้อมูลตามที่ได้ลงนาม

(4) การกำหนดสิทธิการเข้าถึงข้อมูลเพื่อตรวจสอบหรือติดตามการใช้งานข้อมูลที่มีความสำคัญ

(5) การกำหนดกระบวนการแจ้งเตือนและรายงานผู้เกี่ยวข้องหากพบการรั่วไหลหรือเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

(6) การกำหนดมาตรการดำเนินการกรณีละเมิดหรือยกเลิกข้อตกลง รวมทั้งข้อกำหนดในการคืนหรือทำลายข้อมูลที่มีความสำคัญเมื่อสิ้นสุดข้อตกลง

10. การจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศ (system acquisition, development and maintenance)

10.1 การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (security requirements of information systems)

วัตถุประสงค์

เพื่อกำหนดให้กระบวนการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเป็นส่วนหนึ่งของระบบสารสนเทศของทั้งภายในองค์กรและที่เกี่ยวข้องกับการให้บริการภายนอกผ่านเครือข่ายสาธารณะ ตลอดช่วงอายุการใช้งานระบบสารสนเทศ (entire life cycle) ได้แก่ กระบวนการจัดหา กระบวนการพัฒนาระบบ (system development life cycle) การใช้งาน และการดูแลรักษา

ข้อกำหนดในประกาศที่ สธ. 37/2559

ข้อ 24 ผู้ประกอบธุรกิจต้องจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศ (system acquisition, development and maintenance) ตามหลักเกณฑ์ดังต่อไปนี้

(1) มีข้อกำหนดในการจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศให้มีความมั่นคงปลอดภัย เมื่อมีระบบสารสนเทศใหม่หรือมีการปรับปรุงระบบเดิม

(2) จัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศ ในกรณีที่มีการเข้าถึงระบบการให้บริการการใช้งาน (application service)

แนวทางปฏิบัติเพิ่มเติมจากข้อกำหนด

- ไม่มีแนวปฏิบัติเพิ่มเติม -

10.2 การรักษาความมั่นคงปลอดภัยในกระบวนการพัฒนาระบบสารสนเทศ (security in development and support process)

วัตถุประสงค์
เพื่อให้การพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบสารสนเทศประมวลผลได้อย่างถูกต้องครบถ้วน และเป็นไปตามความต้องการของผู้ใช้งาน (change management) รวมถึงการรักษาไว้ซึ่งความมั่นคงปลอดภัยของระบบสารสนเทศตลอดช่วงการพัฒนาระบบงานสารสนเทศ (system development life cycle)

ข้อกำหนดในประกาศที่ สธ. 37/2559

ข้อ 24 ผู้ประกอบธุรกิจต้องจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศ (system acquisition, development and maintenance) ตามหลักเกณฑ์ดังต่อไปนี้

(3) มีการควบคุมการพัฒนาหรือการแก้ไขเปลี่ยนแปลงระบบสารสนเทศในทุกขั้นตอน ให้เป็นไปตามขั้นตอนการควบคุมความมั่นคงปลอดภัยด้านสารสนเทศที่กำหนดไว้

(4) มีการทดสอบระบบสารสนเทศที่ได้รับการพัฒนาหรือแก้ไขเปลี่ยนแปลง เพื่อให้มั่นใจได้ว่าระบบสารสนเทศดังกล่าวทำงานได้อย่างมีประสิทธิภาพ สามารถประมวลผลได้อย่างถูกต้องครบถ้วน และเป็นไปตามความต้องการของผู้ใช้งาน

(5) ปรับปรุงแผนบริหารความต่อเนื่องทางธุรกิจให้สอดคล้องกับการพัฒนาหรือการแก้ไขเปลี่ยนแปลงระบบสารสนเทศ

(6) มีการควบคุมบุคลากร ขั้นตอน และเทคโนโลยีสำหรับการพัฒนาระบบสารสนเทศให้มีความมั่นคงปลอดภัยตลอดขั้นตอนการพัฒนาระบบ

(7) มีการดูแล ติดตาม และควบคุมการพัฒนาระบบสารสนเทศของผู้รับดำเนินการให้เป็นไปตามข้อตกลงการใช้บริการ

(8) มีการทดสอบการทำงานของระบบสารสนเทศที่ได้รับการพัฒนา โดยผู้ใช้งานหรือผู้ทดสอบที่เป็นอิสระจากผู้พัฒนาระบบสารสนเทศดังกล่าว

แนวทางปฏิบัติเพิ่มเติมจากข้อกำหนด

1. การควบคุมการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบสารสนเทศตามข้อกำหนด 24(3) ควรมีกระบวนการขั้นต่ำ ดังนี้

(1) ประเมินผลกระทบที่อาจเกิดขึ้นจากการเปลี่ยนแปลง

(2) กำหนดวิธีปฏิบัติให้คำขอให้แก้ไขหรือพัฒนาต้องมาจากผู้ที่มีสิทธิและอนุมัติคำขอโดยผู้มีอำนาจควบคุมผลข้างเคียงที่อาจเกิดขึ้นเนื่องจากมีการแก้ไข ตรวจรับจากผู้มีอำนาจภายหลังการแก้ไขหรือพัฒนาแล้วเสร็จก่อนโอนย้ายระบบงาน รวมทั้งจัดเก็บรายละเอียดของคำขอไว้

(3) กำหนดวิธีปฏิบัติในกรณีที่มีการแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ในกรณีฉุกเฉิน บันทึกเหตุผลความจำเป็นและขออนุมัติจากผู้มีอำนาจทุกครั้ง

(4) ปรับปรุงเอกสารประกอบระบบงานทั้งหมดหลังจากที่ได้มีการแก้ไขเปลี่ยนแปลง เพื่อให้ทันสมัยอยู่เสมอ เช่น เอกสารประกอบรายละเอียดโครงสร้างข้อมูล คู่มือระบบงาน ทะเบียนรายชื่อผู้มีสิทธิใช้งาน ขั้นตอนการทำงานของโปรแกรม และควรจัดเก็บเอกสารดังกล่าวในที่ปลอดภัยและสะดวกต่อการใช้งาน

(5) จัดเก็บโปรแกรม version ก่อนการเปลี่ยนแปลงไว้ใช้งาน หรือมีกระบวนการถอยกลับสู่สภาพเดิม (fall-back) ของระบบงาน ในกรณีระบบงานผิดพลาดหรือไม่สามารถใช้งานได้

(6) สื่อสารให้กับบุคคลที่เกี่ยวข้องได้รับทราบและสามารถปฏิบัติงานได้อย่างถูกต้อง

(7) บันทึกและจัดเก็บหลักฐานทั้งหมด (audit trail) ที่เกี่ยวข้องกับการเปลี่ยนแปลง เพื่อใช้ประกอบในกรณีที่มีการตรวจสอบ

2. ในการปฏิบัติให้เป็นไปตามข้อกำหนด 24(5) ผู้ประกอบธุรกิจควรจัดให้มีการทดสอบระบบสารสนเทศที่ได้รับการพัฒนาหรือแก้ไขเปลี่ยนแปลง เพื่อให้มั่นใจว่าการทำงานมีประสิทธิภาพ การประมวลผลถูกต้องครบถ้วน และเป็นไปตามความต้องการของผู้ใช้งาน พร้อมทั้งปรับปรุงแผนบริหารความต่อเนื่องทางธุรกิจ (business continuity plan)

3. ในการปฏิบัติให้เป็นไปตามข้อกำหนด 24(6) ผู้ประกอบธุรกิจควรคำนึงถึงเรื่องดังต่อไปนี้

(1) การรักษาความลับของข้อมูลที่นำมาประมวลผล จัดเก็บ และส่งผ่านระบบ และการควบคุมการนำข้อมูลเข้าและออกจากระบบที่อยู่ระหว่างการพัฒนา

(2) การควบคุมการเข้าถึงสภาพแวดล้อมของการพัฒนาระบบสารสนเทศอย่างรัดกุมเหมาะสม

(3) การติดตามหากมีการเปลี่ยนแปลงสภาพแวดล้อมของการพัฒนาระบบสารสนเทศ

(4) มีการจัดเก็บข้อมูลสำรองในพื้นที่นอกองค์กรที่มีความมั่นคงปลอดภัย

4. ในการทดสอบการทำงานของระบบสารสนเทศที่ได้รับการพัฒนาโดยผู้ใช้งานหรือผู้ทดสอบที่เป็นอิสระตามข้อกำหนด 24(8) เพื่อให้มั่นใจได้ว่าระบบที่ได้รับการพัฒนาดังกล่าวสามารถทำงานได้อย่างถูกต้องตรงความต้องการของผู้ใช้งาน และเป็นไปตามนโยบายด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ผู้ประกอบธุรกิจควรจัดให้มีแนวทางควบคุมและป้องกันการรั่วไหลของข้อมูลที่ใช้ในการทดสอบ หากข้อมูลดังกล่าวเป็นความลับหรือมีความสำคัญ

11. การใช้บริการระบบสารสนเทศจากผู้รับดำเนินการ (IT outsourcing)

11.1 การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศจากผู้รับดำเนินการ (information security in IT outsourcing)

วัตถุประสงค์

เพื่อป้องกันทรัพย์สินสารสนเทศของผู้ประกอบธุรกิจจากการเข้าถึงโดยผู้รับดำเนินการอย่างไม่เหมาะสม

ข้อกำหนดในประกาศที่ สธ. 37/2559

ข้อ 8 ผู้ประกอบธุรกิจต้องจัดให้มีการกำหนดนโยบายอย่างน้อยในเรื่องดังต่อไปนี้ ไว้เป็นลายลักษณ์อักษร เพื่อรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (information security policy)

(5) นโยบายเพื่อรองรับในกรณีที่ผู้ประกอบธุรกิจแต่งตั้งบุคคลอื่นเป็นผู้รับดำเนินการในงานที่เกี่ยวกับระบบสารสนเทศของผู้ประกอบธุรกิจ ซึ่งครอบคลุมถึงวิธีการคัดเลือกและประเมินผู้รับดำเนินการ การทบทวนคุณสมบัติของผู้รับดำเนินการ และการมีข้อกำหนดเกี่ยวกับการใช้บริการ เพื่อลดความเสี่ยงจากการเข้าถึงทรัพย์สินสารสนเทศอย่างไม่เหมาะสม

ข้อ 25 ในกรณีที่ผู้ประกอบธุรกิจแต่งตั้งบุคคลอื่นเป็นผู้รับดำเนินการในงานที่เกี่ยวกับระบบสารสนเทศของผู้ประกอบธุรกิจ ผู้ประกอบธุรกิจต้องดำเนินการให้เป็นไปตามหลักเกณฑ์ดังต่อไปนี้

(1) มีข้อตกลงและกระบวนการควบคุมเกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศอย่างเป็นลายลักษณ์อักษรในการใช้บริการจากผู้รับดำเนินการ โดยผู้ประกอบธุรกิจและผู้รับดำเนินการต้องมีการลงนามร่วมกันในข้อตกลงและกระบวนการดังกล่าว

(4) มีมาตรการตรวจสอบดูแลให้ผู้รับดำเนินการปฏิบัติตามหลักเกณฑ์การปฏิบัติงานที่คณะกรรมการ ก.ล.ต. คณะกรรมการกำกับตลาดทุน หรือสำนักงาน กำหนดเกี่ยวกับงานที่รับดำเนินการ รวมทั้งระเบียบวิธีปฏิบัติที่ผู้ประกอบธุรกิจกำหนดขึ้นเพื่อให้เป็นไปตามหลักเกณฑ์ดังกล่าว โดยอย่างน้อยมาตรการดังกล่าวต้องสามารถควบคุมให้ผู้รับดำเนินการไม่มีลักษณะที่จะทำให้มีเหตุอันควรเชื่อได้ว่ามีข้อบกพร่องหรือมีความไม่เหมาะสมเกี่ยวกับการควบคุมและการปฏิบัติงานอันดีของธุรกิจ

(5) มีแผนรองรับในกรณีที่เกิดเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (incident response policy)

(6) กำหนดสิทธิในการเข้าตรวจสอบกระบวนการปฏิบัติงานของผู้รับดำเนินการและควบคุมให้การปฏิบัติงานเป็นไปตามข้อตกลงที่กำหนดไว้ เว้นแต่ในกรณีที่ผู้รับดำเนินการมีข้อจำกัดในการเข้าตรวจสอบการปฏิบัติงานดังกล่าว ผู้ประกอบธุรกิจต้องมีมาตรการเพื่อให้มั่นใจได้ว่าสามารถควบคุมการปฏิบัติงานของผู้รับดำเนินการให้เป็นไปตามข้อตกลงที่กำหนดไว้ได้

(7) มีข้อกำหนดให้ผู้รับดำเนินการยินยอมให้สำนักงานเรียกดู ตรวจสอบเอกสารหลักฐานที่เกี่ยวข้อง หรือสามารถเข้าตรวจสอบการปฏิบัติงานของผู้รับดำเนินการ

แนวทางปฏิบัติเพิ่มเติมจากข้อกำหนด

1. นโยบายเกี่ยวกับการให้บุคคลอื่นเป็นผู้รับดำเนินการในงานที่เกี่ยวกับระบบสารสนเทศของผู้ประกอบธุรกิจตามข้อกำหนด 8(5) ควรมีเนื้อหาขั้นต่ำครอบคลุมประเด็นดังต่อไปนี้

(1) กำหนดวิธีการคัดเลือกและประเมินผู้รับดำเนินการ (due diligence) โดยควรให้ความสำคัญในเรื่องการรักษาความปลอดภัยของข้อมูลสารสนเทศที่สำคัญ (confidentiality) ความถูกต้องเชื่อถือได้ของข้อมูลและระบบสารสนเทศ (integrity) และความพร้อมใช้งานของระบบสารสนเทศที่ใช้บริการ (availability) เช่น ผู้รับดำเนินการควรมีแผนรองรับกรณีเกิดเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (incident response policy) โดยคำนึงถึงแผนของผู้ประกอบธุรกิจ รวมทั้งมีกระบวนการการกู้คืนระบบงานให้เป็นไปตามข้อตกลงที่ได้กำหนดไว้ เพื่อให้ข้อมูลและการประมวลผลข้อมูลอยู่ในสภาพที่พร้อมใช้งานเสมอ เป็นต้น

(2) กำหนดการทบทวนคุณสมบัติของผู้รับดำเนินการอย่างสม่ำเสมอ เช่น ฐานะทางการเงิน ความเพียงพอของการให้บริการ (capacity planning) เพื่อให้มั่นใจว่าผู้รับดำเนินการยังคงมีความพร้อมในการให้บริการที่เพียงพอต่อความต้องการของผู้ประกอบธุรกิจอย่างต่อเนื่อง

(3) กำหนดข้อตกลงเกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและกระบวนการควบคุมอย่างเป็นลายลักษณ์อักษร และมีการลงนามร่วมกันระหว่างผู้ประกอบธุรกิจและผู้รับดำเนินการ ทั้งนี้ ผู้ประกอบธุรกิจควรมั่นใจว่าผู้รับดำเนินการมีหน้าที่รับผิดชอบในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศเสมือนกับผู้ประกอบธุรกิจดำเนินการด้วยตนเอง

(4) กำหนดหน้าที่ความรับผิดชอบของผู้รับดำเนินการ

(5) ระบุประเภทข้อมูลสารสนเทศที่อนุญาตให้ผู้รับดำเนินการเข้าถึง เพื่อให้การกำหนดมาตรการควบคุมและติดตามการเข้าถึงข้อมูลเป็นไปอย่างเหมาะสม ภายใต้หลักความจำเป็นในการรู้ข้อมูล (need-to-know basis)

(6) จัดให้มีขั้นตอนและกระบวนการติดตามควบคุมการเข้าถึงสารสนเทศอย่างเหมาะสม

(7) มีการรักษาความมั่นคงปลอดภัยในกรณีที่มีการเคลื่อนย้ายหรือถ่ายโอนข้อมูลสารสนเทศ

(8) มีการควบคุมความครบถ้วนถูกต้องของข้อมูลและการประมวลผลข้อมูลที่ได้รับจากผู้รับดำเนินการ

(9) กำหนดกระบวนการควบคุมอย่างเป็นมาตรฐานเพื่อติดตามการทำงานของผู้รับดำเนินการ

2. ข้อตกลงเกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามข้อกำหนด 25(1) ควรมีเนื้อหาขั้นต่ำดังนี้

(1) รายละเอียดของข้อมูลที่จำเป็นต้องใช้หรือเข้าถึงโดยผู้รับดำเนินการ รวมทั้งวิธีการเข้าถึงข้อมูลดังกล่าว

(2) การจัดแบ่งประเภทข้อมูลซึ่งสอดคล้องกับนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

(3) มีมาตรการดำเนินการเพื่อให้มั่นใจได้ว่าข้อมูลที่เป็นความลับหรือมีความสำคัญ ทรัพย์สินทางปัญญา และลิขสิทธิ์ของผู้ประกอบธุรกิจได้รับการคุ้มครองอย่างปลอดภัยตามกฎหมายและหลักเกณฑ์ของทางการที่เกี่ยวข้อง

(4) กำหนดหน้าที่ความรับผิดชอบของผู้รับดำเนินการในการปฏิบัติงานภายใต้การควบคุมต่าง ๆ เช่น กำหนดเงื่อนไขการเข้าถึงข้อมูลของผู้ประกอบธุรกิจ ติดตามตรวจสอบการปฏิบัติงานของผู้รับดำเนินการให้เป็นไปตามข้อตกลงของผู้ประกอบธุรกิจ กำหนดให้ผู้รับดำเนินการรายงานผลการปฏิบัติงานให้ผู้ประกอบธุรกิจทราบเมื่อร้องขอ การแก้ไขปัญหาต่าง ๆ ภายในระยะเวลาที่กำหนด รวมทั้งการปฏิบัติงานให้เป็นไปตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของผู้ประกอบธุรกิจ

(5) แนวทางการใช้งานข้อมูลสารสนเทศอย่างถูกต้องเหมาะสม

(6) แนวทางการแก้ไขปัญหากรณีที่เกิดข้อผิดพลาดจากการปฏิบัติหน้าที่

(7) รายชื่อและช่องทางสำหรับติดต่อบุคคลหรือหน่วยงานอื่น ๆ ที่เกี่ยวข้อง โดยเฉพาะอย่างยิ่งบุคคลหรือหน่วยงานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

(8) มีข้อกำหนดเพิ่มเติมเกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ กรณีที่ผู้ให้บริการภายนอกมอบหมายการปฏิบัติงานให้กับบุคคลอื่นต่อ (sub-contracting to another supplier)

11.2 การควบคุมการส่งมอบงานของผู้รับดำเนินการ (Supplier Service Delivery Management)

วัตถุประสงค์
เพื่อควบคุมผู้รับดำเนินการส่งมอบงานให้เป็นไปตามข้อตกลงที่จัดทำไว้กับผู้ประกอบธุรกิจ

ข้อกำหนดในประกาศที่ สธ. 37/2559

ข้อ 25 ในกรณีที่ผู้ประกอบธุรกิจแต่งตั้งบุคคลอื่นเป็นผู้รับดำเนินการในงานที่เกี่ยวกับระบบสารสนเทศของผู้ประกอบธุรกิจ ผู้ประกอบธุรกิจต้องดำเนินการให้เป็นไปตามหลักเกณฑ์ดังต่อไปนี้

(2) มีการติดตาม ประเมิน ทบทวน และตรวจสอบผู้รับดำเนินการอย่างสม่ำเสมอ

(3) มีการประเมินความเสี่ยงและกำหนดกระบวนการบริหารจัดการความเสี่ยงในกรณีที่ผู้รับดำเนินการมีการเปลี่ยนแปลงกระบวนการ ขั้นตอน หรือวิธีการปฏิบัติงานในการรักษาความมั่นคงปลอดภัยในการปฏิบัติงาน หรือเปลี่ยนตัวผู้รับดำเนินการ

แนวทางปฏิบัติเพิ่มเติมจากข้อกำหนด

1. ในการติดตาม ประเมิน ทบทวน และตรวจสอบผู้รับดำเนินการตามข้อกำหนด 25(2) ผู้ประกอบควรพิจารณาฐานะทางการเงิน กระบวนการปฏิบัติงาน และประสิทธิภาพการให้บริการของผู้รับดำเนินการประกอบกัน

12. การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (information security incident management)

วัตถุประสงค์

เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยของระบบสารสนเทศได้รับการดำเนินการอย่างถูกต้อง มีประสิทธิภาพ ในช่วงระยะเวลาที่เหมาะสม

ข้อกำหนดในประกาศที่ สธ. 37/2559

ข้อ 11 ผู้ประกอบธุรกิจต้องมีการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (information security incident management) ให้เป็นไปตามหลักเกณฑ์ดังต่อไปนี้

(1) กำหนดขั้นตอนและกระบวนการในการบริหารจัดการเหตุการณ์ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ

(2) กำหนดผู้มีหน้าที่รับผิดชอบในการบริหารจัดการเหตุการณ์ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ

(3) รายงานต่อผู้มีหน้าที่รับผิดชอบในการบริหารจัดการเหตุการณ์ตาม (2) และสำนักงานโดยไม่ชักช้าเมื่อเกิดเหตุการณ์ดังกล่าว

(4) ทดสอบขั้นตอนและกระบวนการในการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศตาม (1) อย่างน้อยปีละ 1 ครั้ง โดยอย่างน้อยต้องครอบคลุมถึงการบริหารจัดการความเสี่ยงไซเบอร์ (cyber security drill)

(5) พิจารณาทบทวนขั้นตอนและกระบวนการในการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ หลังจากที่มีการทดสอบตาม (4) แล้วอย่างน้อยปีละ 1 ครั้ง

(6) จัดให้มีการประเมินผลการทดสอบตาม (4) และประเมินผลพิจารณาทบทวนตาม (5) โดยต้องรายงานผลต่อคณะกรรมการของผู้ประกอบธุรกิจหรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบธุรกิจอย่างน้อยปีละ 1 ครั้ง ทั้งนี้ การดำเนินการดังกล่าวต้องกระทำโดยบุคคลที่เป็นอิสระจากผู้มีหน้าที่รับผิดชอบในการบริหารจัดการเหตุการณ์ตาม (2)

(7) จัดเก็บเอกสารหลักฐานที่เกี่ยวข้องกับการดำเนินการในการบริหารจัดการเหตุการณ์ดังกล่าวเป็นระยะเวลาไม่น้อยกว่า 2 ปีนับแต่วันที่จัดทำเอกสารนั้น โดยต้องเก็บรักษาไว้ในลักษณะที่พร้อมให้สำนักงานสามารถเรียกดูและตรวจสอบได้โดยไม่ชักช้า

เพื่อประโยชน์ตามวรรคหนึ่ง (4) ให้คำว่า “ความเสี่ยงไซเบอร์” หมายความว่า ภัยคุกคามที่ส่งผลกระทบหรือสร้างความเสียหาย หรือก่อให้เกิดความเสี่ยงต่อการประกอบธุรกิจของผู้ประกอบธุรกิจ ซึ่งเกิดจากการใช้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ อินเทอร์เน็ต โครงข่ายโทรคมนาคม หรือการให้บริการโดยปกติของดาวเทียม

แนวทางปฏิบัติเพิ่มเติมจากข้อกำหนด

1. ในการกำหนดขั้นตอนและกระบวนการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ รวมทั้งกำหนดผู้มีหน้าที่รับผิดชอบซึ่งมีความรู้ความสามารถและประสบการณ์ตามข้อกำหนด 11(1) และ (2) ผู้ประกอบธุรกิจควรกำหนดขั้นตอนและกระบวนการขั้นต่ำดังต่อไปนี้

(1) กำหนดแผนรองรับในกรณีที่เกิดเหตุการณ์อย่างเป็นลายลักษณ์อักษร

(2) ประเมินเหตุการณ์หรือจุดอ่อนของมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ และพิจารณาว่าควรจัดเป็นเหตุการณ์และมีระดับความรุนแรงที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ

(3) จัดให้มีบุคคลหรือหน่วยงานเพื่อทำหน้าที่รับแจ้งเหตุการณ์ (point of contact) และรายงานเหตุการณ์ต่อคณะผู้บริหารหรือผู้เกี่ยวข้องให้ทราบและดำเนินการต่อไป (escalation)

(4) ดำเนินการเพื่อตอบสนองต่อเหตุการณ์ที่เกิดขึ้นอย่างมีประสิทธิภาพ เพื่อทำให้เหตุการณ์คลี่คลายหรือกลับสู่ภาวะปกติอย่างรวดเร็ว

(5) รวบรวมและจัดเก็บหลักฐานโดยไม่ชักช้า เมื่อเกิดเหตุการณ์ที่ส่งผลกระทบต่อระบบสารสนเทศที่มีความสำคัญอย่างมีนัยสำคัญ เช่น ก่อให้เกิดความเสียหายกับข้อมูลหรือทรัพย์สินของลูกค้า โดยคำนึงถึงประเด็นสำคัญต่าง ๆ เช่น มีกระบวนการการจัดเก็บอย่างมั่นคงปลอดภัย การกำหนดหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้อง การคัดเลือกบุคคลที่มีความรู้ความสามารถหรือมีประสบการณ์ด้านการรวบรวมและจัดเก็บหลักฐาน เพื่อวิเคราะห์ตรวจสอบและจัดทำเอกสารสรุปนำเสนอต่อบุคคลที่มีหน้าที่รับผิดชอบ เป็นต้น ทั้งนี้ การรวบรวม จัดเก็บ และนำเสนอหลักฐานควรสอดคล้องกับหลักเกณฑ์ของกฎหมายที่ใช้บังคับ

(6) บันทึกและจัดเก็บหลักฐานการบริหารจัดการตามความจำเป็นและเหมาะสม

(7) รายงานให้สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์รับทราบถึงสถานการณ์และผลการบริหารจัดการ

(8) ตรวจหา ติดตาม วิเคราะห์ และรายงานเหตุการณ์ ทั้งนี้ ให้รวมถึงการวิเคราะห์ภายหลังเหตุการณ์ยุติแล้ว เพื่อระบุถึงสาเหตุของเหตุการณ์และเพื่อใช้ประโยชน์จากผลการวิเคราะห์ในการเตรียมความพร้อมรองรับเหตุการณ์ที่อาจเกิดขึ้นได้อีกในอนาคต

2. ในการรายงานสถานการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยต่อบุคคลหรือหน่วยงานที่ทำหน้าที่รับแจ้งเหตุการณ์ (point of contact) ตามข้อกำหนด 11(3) ผู้ประกอบธุรกิจควรดำเนินการดังนี้

(1) จัดทำแบบฟอร์มที่เป็นมาตรฐานเพื่อรองรับการรายงานสถานการณ์ และสร้างความเข้าใจให้กับผู้รายงานเกี่ยวกับการดำเนินการต่าง ๆ ที่จำเป็นในกรณีที่เกิดเหตุการณ์ ทั้งนี้ เนื้อหาขั้นต่ำควรประกอบด้วย วันเวลา เหตุการณ์ ผลกระทบที่คาดว่าจะเกิดขึ้น การดำเนินการแก้ไข ผลการแก้ไข ระยะเวลาในการแก้ไข สาเหตุที่เกิดปัญหา และแนวทางการป้องกันในอนาคต

(2) รายงานคณะผู้บริหารขององค์กรเมื่อทราบเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัย เช่น พบช่องโหว่ในการควบคุมความมั่นคงปลอดภัย (ineffective security control) เกิดเหตุการณ์ที่อาจส่งผลกระทบต่อการรักษาความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของระบบสารสนเทศ ข้อผิดพลาดจากการปฏิบัติงาน (human errors) การบุกรุกด้านกายภาพ (breaches of physical security arrangements) การปฏิบัติงานที่ไม่เป็นไปตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (non-compliances with policies) การเปลี่ยนแปลงระบบปฏิบัติการหรือชุดคำสั่งที่ควบคุมระบบงานโดยไม่ได้รับอนุญาต (uncontrolled system changes) การทำงานผิดพลาดของโปรแกรมและอุปกรณ์คอมพิวเตอร์ (malfunctions of software or hardware) และการเข้าถึงโดยไม่ได้รับอนุญาต (access violations)

(3) รายงานสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์เมื่อมีเหตุการณ์ที่ส่งผลกระทบต่อระบบสารสนเทศที่มีความสำคัญ ประเภทดังต่อไปนี้

(ก) ระบบหยุดชะงัก (system disruption)

(ข) มีการบุกรุก เข้าถึง หรือใช้งานระบบโดยไม่ได้รับอนุญาต (system compromised)

(ค) ส่งผลกระทบต่อชื่อเสียงของผู้ประกอบธุรกิจ (harm to reputation) เช่น ถูกปลอมแปลงหน้าเว็บไซต์ของบริษัท (website defacement) โดยให้รายงาน ดังนี้

- รายงานโดยไม่ชักช้าเมื่อทราบเหตุการณ์ โดยมีเนื้อหาครอบคลุมถึงวันเวลา ประเภทเหตุการณ์ เหตุการณ์ และผลกระทบที่คาดว่าจะเกิดขึ้น ทั้งนี้ อาจแจ้งโดยวาจาหรือผ่านระบบรับส่งข้อความผ่านทางอิเล็กทรอนิกส์ (electronic messaging) ตามความเหมาะสม
- รายงานภายในวันทำการถัดไปหลังทราบเหตุการณ์ เป็นลายลักษณ์อักษร โดยมีเนื้อหาครอบคลุมถึงวันเวลา ประเภทเหตุการณ์ เหตุการณ์ ผลกระทบที่เกิดขึ้น การดำเนินการแก้ไขปัญหา และความคืบหน้าในการแก้ไขปัญหา
- รายงานเมื่อเหตุการณ์ยุติหรือแก้ไขปัญหาแล้วเสร็จ เป็นลายลักษณ์อักษร โดยมีเนื้อหาครอบคลุมถึงวันเวลา ประเภทเหตุการณ์ เหตุการณ์ ผลกระทบที่เกิดขึ้น การดำเนินการแก้ไขปัญหา ผลการแก้ไขปัญหา ระยะเวลาในการแก้ไข สาเหตุที่เกิดปัญหา และแนวทางป้องกันในอนาคต

(4) แจ้งบุคคลที่เกี่ยวข้อง เช่น ลูกค้า รับทราบโดยไม่ชักช้า ในกรณีที่เหตุการณ์ส่งผลกระทบต่อบุคคลดังกล่าว

(5) จัดให้มีการรายงานความคืบหน้าในการบริหารจัดการสถานการณ์และผลการบริหารจัดการเป็นระยะ และเมื่อเหตุการณ์ยุติแล้ว

3. ในการปฏิบัติให้เป็นไปตามข้อกำหนด 11(4) (5) และ (7) ผู้ประกอบธุรกิจควรดำเนินการ ดังต่อไปนี้

(1) จัดให้มีการจำลองสถานการณ์เสี่ยง (risk scenarios) เพื่อทดสอบการเตรียมความพร้อมรับมือต่อเหตุการณ์ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ โดย risk scenarios ดังกล่าวควรมีลักษณะดังต่อไปนี้

(ก) เป็นสถานการณ์ที่สอดคล้องกับลักษณะ ขอบเขต และความซับซ้อนในการประกอบธุรกิจของผู้ประกอบธุรกิจ

(ข) เป็นสถานการณ์ที่เมื่อเกิดขึ้นแล้ว จะส่งผลกระทบต่อระบบสารสนเทศอย่างมีนัยสำคัญ

(ค) เป็นสถานการณ์ที่สามารถวัดผลได้ และนำผลที่ได้ไปใช้ในการทบทวนขั้นตอนและกระบวนการในการบริหารจัดการเหตุการณ์ เพื่อให้เกิดความมั่นคงปลอดภัยของระบบสารสนเทศ

(ง) เป็นสถานการณ์ที่มีความสมเหตุสมผล สามารถปฏิบัติได้จริงโดยไม่ขัดแย้งกัน

(จ) เป็นสถานการณ์ที่มีความเป็นไปได้ และสอดคล้องกับสถานการณ์จริงในปัจจุบัน

(2) จัดเก็บเอกสารที่เกี่ยวข้องกับการทดสอบให้ครบถ้วนและเป็นปัจจุบัน ดังนี้

(ก) สถานการณ์เสี่ยง (risk scenario) ที่ใช้ในการทดสอบ

(ข) สรุปผลการทดสอบ ผลการประเมิน และผลการทบทวนแผนรองรับในกรณีที่เกิดเหตุการณ์

13. การบริหารความต่อเนื่องทางธุรกิจในด้านความมั่นคงปลอดภัยของระบบสารสนเทศ (information security aspects of business continuity management)

วัตถุประสงค์
เพื่อให้การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศเป็นส่วนหนึ่งของการบริหารความต่อเนื่องทางธุรกิจ (business continuity management) ของผู้ประกอบธุรกิจ ทั้งนี้ เพื่อให้ระบบสารสนเทศอยู่ในสภาพที่พร้อมใช้งานอยู่เสมอ

ข้อกำหนดในประกาศที่ สธ. 37/2559

ข้อ 12 ผู้ประกอบธุรกิจต้องมีการบริหารความต่อเนื่องทางธุรกิจในด้านความมั่นคงปลอดภัยของระบบสารสนเทศ (information security of business continuity management) ให้เป็นไปตามหลักเกณฑ์ดังต่อไปนี้

(1) กำหนดมาตรการรองรับสำหรับกรณีที่อาจเกิดเหตุการณ์ไม่พึงประสงค์

(2) กำหนดขั้นตอน กระบวนการดำเนินการ และการควบคุม เกี่ยวกับความมั่นคงปลอดภัยของระบบสารสนเทศให้สอดคล้องกับแผนบริหารความต่อเนื่องทางธุรกิจ

(3) กำหนดระยะเวลาในการกลับคืนสู่สภาพการดำเนินงานปกติของระบบสารสนเทศและจัดลำดับการกู้คืนระบบงานสารสนเทศที่มีความสำคัญให้สอดคล้องกับผลกระทบที่อาจเกิดขึ้น

(4) มีระบบสารสนเทศสำรองที่อยู่ในสภาพพร้อมใช้งาน ซึ่งต้องสอดคล้องกับระยะเวลาในการกลับคืนสู่สภาพการดำเนินงานตามปกติของระบบสารสนเทศตาม (3)

แนวทางปฏิบัติเพิ่มเติมจากข้อกำหนด

1. ในการกำหนดขั้นตอน กระบวนการดำเนินการ และการควบคุมด้านความมั่นคงปลอดภัยของระบบสารสนเทศตามข้อกำหนด 12(2) ควรมีรายละเอียดขั้นต่ำดังต่อไปนี้

(1) กำหนดขั้นตอนดำเนินการเพื่อตอบสนองต่อเหตุการณ์ที่เกิดขึ้น (incident response process) ให้เป็นไปตามนโยบายการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ

(2) มีขั้นตอนการแก้ไขปัญหาในแต่ละเหตุการณ์โดยละเอียด ชัดเจน พร้อมทั้งกำหนดผู้มีหน้าที่รับผิดชอบที่สามารถปฏิบัติงานได้ในแต่ละเหตุการณ์

(3) มีรายละเอียดของอุปกรณ์ที่จำเป็นต้องใช้ในกรณีฉุกเฉินของแต่ละระบบงาน เช่น รุ่นของเครื่องคอมพิวเตอร์ คุณลักษณะของเครื่องคอมพิวเตอร์ (specification) ขั้นต่ำ ข้อมูลเกี่ยวกับการปรับแต่ง (configuration) และอุปกรณ์เครือข่ายคอมพิวเตอร์ เป็นต้น

(4) ระบุรายละเอียดเกี่ยวกับศูนย์คอมพิวเตอร์สำรอง (ถ้ามี) ให้ชัดเจน เช่น สถานที่ตั้ง แผนที่ เป็นต้น