ประกาศคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย

เรื่อง หลักเกณฑ์การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัทประกันชีวิต

พ.ศ. ๒๕๖๓

ปัจจุบันธุรกิจประกันภัยต้องเผชิญความท้าทายจากสภาวะการแข่งขันที่รุนแรง และเทคโนโลยีที่เติบโตรวดเร็วแบบก้าวกระโดด ทำให้บริษัทต้องปรับตัวให้ทันต่อการเปลี่ยนแปลง และสามารถดำเนินธุรกิจต่อไปได้ หลายบริษัทจึงได้นำเทคโนโลยีเข้ามาช่วยในการดำเนินงาน พัฒนาผลิตภัณฑ์และบริการลูกค้า เช่น การขายผลิตภัณฑ์ประกันภัยผ่านสื่ออิเล็กทรอนิกส์ ระบบการจัดเก็บข้อมูลลูกค้า ระบบการพิจารณารับประกันภัย ระบบการเงินและบัญชี ระบบการจ่ายค่าสินไหมทดแทนและการชดใช้เงินหรือประโยชน์อื่นใดตามกรมธรรม์ประกันภัย ซึ่งการนำเทคโนโลยีเข้ามามีบทบาทในการดำเนินธุรกิจมากขึ้นนั้นย่อมมีความเสี่ยงแฝงมาด้วย ไม่ว่าจะเป็นความเสี่ยงด้านเทคโนโลยีสารสนเทศ และความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่ปัจจุบันมีแนวโน้มเพิ่มสูงขึ้นเป็นอย่างมากอาจก่อให้เกิดความเสียหายและมีผลกระทบต่อความเชื่อมั่นของลูกค้า

ดังนั้น คณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย จึงกำหนดให้มีหลักเกณฑ์การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อให้บริษัทประกันภัยมีการกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยคุกคามทางไซเบอร์ได้อย่างเหมาะสม และเป็นระบบ รวมทั้งมีการควบคุมและรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศได้อย่างเหมาะสม สอดคล้องกับมาตรฐานสากล มีการกำกับดูแลและพิจารณาแผนงานในการนำเทคโนโลยีสารสนเทศมาใช้ในองค์กร การบริหารงานโครงการด้านเทคโนโลยีสารสนเทศตลอดจนการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ และการตรวจสอบด้านเทคโนโลยีสารสนเทศ

อาศัยอำนาจตามความในมาตรา ๓๘ (๑๑) และ (๑๓) แห่งพระราชบัญญัติประกันชีวิต พ.ศ. ๒๕๓๕ ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัติประกันชีวิต (ฉบับที่ ๒) พ.ศ. ๒๕๕๑ ประกอบกับมติที่ประชุมคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย ครั้งที่ ๑๑/๒๕๖๒ เมื่อวันที่ ๒๕ ตุลาคม พ.ศ. ๒๕๖๒ และครั้งที่ ๖/๒๕๖๓ เมื่อวันที่ ๒๒ พฤษภาคม พ.ศ. ๒๕๖๓ คณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย ออกประกาศไว้ ดังนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง หลักเกณฑ์การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัทประกันชีวิต พ.ศ. ๒๕๖๓”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันที่ ๑ มกราคม พ.ศ. ๒๕๖๔ เป็นต้นไป

ข้อ ๓ ในประกาศนี้

“ความเสี่ยงด้านเทคโนโลยีสารสนเทศ” (IT risk) หมายความว่า ความเสี่ยงที่อาจเกิดขึ้นจากการใช้เทคโนโลยีสารสนเทศในการดำเนินธุรกิจ ซึ่งมีผลกระทบต่อระบบหรือการปฏิบัติงานของบริษัท รวมถึงความเสี่ยงที่เกิดจากภัยคุกคามทางไซเบอร์ (cyber threat)

“เทคโนโลยีสารสนเทศ” (information technology : IT) หมายความว่า เทคโนโลยีสารสนเทศที่นำมาใช้ในการดำเนินธุรกิจ ซึ่งครอบคลุมถึง ข้อมูลหรือสารสนเทศ (data/information) ระบบปฏิบัติการ (operating system) ระบบงาน (application system) ระบบฐานข้อมูล (database system) อุปกรณ์คอมพิวเตอร์ (hardware) และระบบเครือข่ายสื่อสาร (communication)

“ทรัพย์สินสารสนเทศ” หมายความว่า

(๑) ทรัพย์สินสารสนเทศประเภทระบบ ได้แก่ ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

(๒) ทรัพย์สินสารสนเทศประเภทอุปกรณ์ ได้แก่ ตัวเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล และอุปกรณ์อื่นใดที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ

(๓) ทรัพย์สินสารสนเทศประเภทข้อมูล ได้แก่ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์

“ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ” (IT security) หมายความว่า การป้องกันด้านเทคโนโลยีสารสนเทศและทรัพย์สินสารสนเทศจากการเข้าถึง ใช้ เปิดเผย ขัดขวาง เปลี่ยนแปลง แก้ไข ทำให้สูญหาย ทำให้เสียหาย ถูกทำลาย หรือล่วงรู้โดยมิชอบ รวมถึง ความมั่นคงปลอดภัยสารสนเทศ (information security) ซึ่งครอบคลุมถึงการธำรงไว้ซึ่งการรักษาความลับ (confidentiality) การรักษาความครบถ้วน (integrity) และการรักษาสภาพพร้อมใช้งาน (availability) ของเทคโนโลยีสารสนเทศและทรัพย์สินสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability)

“การรักษาความมั่นคงปลอดภัยไซเบอร์” (cybersecurity) หมายความว่า มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ทั้งจากภายในและภายนอกประเทศ ทั้งนี้ ให้เป็นไปตามกฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์

“ภัยคุกคามทางไซเบอร์” (cyber threat) หมายความว่า การกระทำหรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะก่อให้เกิดความเสียหาย หรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

“ไซเบอร์” (cyber) หมายความว่า ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกันที่เชื่อมต่อกันเป็นการทั่วไป

“การรักษาความลับ” (confidentiality) หมายความว่า การรักษาหรือสงวนไว้เพื่อป้องกันระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ หรือข้อมูลคอมพิวเตอร์จากการเข้าถึง การใช้ หรือเปิดเผยโดยบุคคลซึ่งไม่ได้รับอนุญาต

“การรักษาความครบถ้วน” (integrity) หมายความว่า การดำเนินการเพื่อให้ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ หรือข้อมูลคอมพิวเตอร์อยู่ในสภาพสมบูรณ์ขณะที่มีการใช้งาน ประมวลผล โอนหรือเก็บรักษาเพื่อมิให้มีการเปลี่ยนแปลงแก้ไข ทำให้สูญหาย ทำให้เสียหาย หรือถูกทำลายโดยไม่ได้รับอนุญาตหรือโดยมิชอบ

“การรักษาสภาพพร้อมใช้งาน” (availability) หมายความว่า การจัดทำให้ทรัพย์สินสารสนเทศหรือเทคโนโลยีสารสนเทศ สามารถทำงาน เข้าถึง หรือใช้งานได้ในเวลาที่ต้องการ

“บริษัท” หมายความว่า บริษัทที่ได้รับใบอนุญาตประกอบธุรกิจประกันชีวิตตามกฎหมายว่าด้วยการประกันชีวิต และหมายความรวมถึงสาขาของบริษัทประกันชีวิตต่างประเทศที่ได้รับใบอนุญาตประกอบธุรกิจประกันชีวิตในราชอาณาจักรตามกฎหมายว่าด้วยการประกันชีวิตด้วย

“คณะกรรมการบริษัท” หมายความว่า คณะกรรมการของบริษัทตามกฎหมายว่าด้วยการประกันชีวิตและให้หมายความรวมถึง คณะกรรมการบริหารสาขาของบริษัทประกันชีวิตต่างประเทศที่ได้รับใบอนุญาตประกอบธุรกิจประกันชีวิตตามกฎหมายว่าด้วยการประกันชีวิต ซึ่งต้องมีผู้จัดการสาขาเป็นกรรมการรวมอยู่ด้วย

“ผู้บริหาร” หมายความว่า ผู้จัดการ ผู้ดำรงตำแหน่งระดับบริหารสี่รายแรกนับต่อจากผู้จัดการลงมา ผู้ซึ่งดำรงตำแหน่งเทียบเท่ากับผู้ดำรงตำแหน่งระดับบริหารรายที่สี่ทุกราย และให้หมายความรวมถึงผู้ดำรงตำแหน่งระดับบริหารในสายงานบัญชีหรือการเงินที่เป็นระดับผู้จัดการฝ่ายขึ้นไปหรือเทียบเท่า

“สำนักงาน” หมายความว่า สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย

ข้อ ๔ ให้สำนักงานมีอำนาจกำหนดแนวปฏิบัติเพื่อประโยชน์ในการปฏิบัติตามประกาศนี้ได้ หรือมีคำสั่งให้บริษัทดำเนินการเกี่ยวกับการบริหารจัดการความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ รวมถึงความเสี่ยงจากภัยคุกคามทางไซเบอร์ ตามขนาด ลักษณะความซับซ้อน และระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัท และเมื่อมีการปฏิบัติตามแนวปฏิบัติหรือคำสั่ง แล้วแต่กรณี ให้ถือว่าบริษัทได้ปฏิบัติตามประกาศนี้ในส่วนที่เกี่ยวข้องแล้ว

ข้อ ๕ บริษัทต้องมีหลักเกณฑ์การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัท ดังต่อไปนี้

(๑) การกำกับดูแลด้านเทคโนโลยีสารสนเทศ (IT governance)

(๒) การบริหารโครงการด้านเทคโนโลยีสารสนเทศ (IT project management)

(๓) การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security)

(๔) การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management)

(๕) การปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (IT compliance)

(๖) การตรวจสอบด้านเทคโนโลยีสารสนเทศ (IT audit)

(๗) การกำกับดูแลและการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (cybersecurity)

(๘) การรายงานเหตุการณ์ภัยคุกคามทางไซเบอร์หรือภัยคุกคามที่มีต่อระบบเทคโนโลยีสารสนเทศ (reporting)

หมวด ๑
การกำกับดูแลด้านเทคโนโลยีสารสนเทศ
(IT governance)

ข้อ ๖ บริษัทต้องมีการกำกับดูแลและการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและความเสี่ยงจากภัยคุกคามทางไซเบอร์ได้อย่างเหมาะสมตามขนาด ลักษณะ ความซับซ้อน และสภาพแวดล้อมในการดำเนินธุรกิจ มีการกำหนดบทบาทหน้าที่ความรับผิดชอบของคณะกรรมการบริษัท มีการจัดโครงสร้างการกำกับดูแลและการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อให้มีการถ่วงดุลอย่างเป็นอิสระ สอดคล้องตามหลักการผู้รับผิดชอบสามระดับ (three lines of defense) รวมทั้งมีนโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ข้อ ๗ คณะกรรมการบริษัทต้องมีองค์ประกอบตามประกาศคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัยว่าด้วยการกำกับดูแลกิจการที่ดีของบริษัทประกันชีวิต ทั้งนี้ บริษัทควรมีกรรมการที่มีความรู้ หรือประสบการณ์ด้านเทคโนโลยีสารสนเทศอย่างน้อยจำนวนหนึ่งคน เพื่อสามารถกำหนดทิศทางการดำเนินธุรกิจสอดคล้องกับบริบทในปัจจุบัน และกำกับดูแลการใช้เทคโนโลยีให้สอดรับกับกลยุทธ์ในการดำเนินธุรกิจ มีความรู้เท่าทันความเสี่ยงและพัฒนาการด้านเทคโนโลยีสารสนเทศที่เปลี่ยนแปลงไป รวมทั้งคณะกรรมการบริษัทควรได้รับการอบรมให้ความรู้เกี่ยวกับเทคโนโลยีสารสนเทศ แนวโน้มของภัยคุกคามทางไซเบอร์ และความเสี่ยงที่เกี่ยวข้องอย่างเหมาะสม

ข้อ ๘ คณะกรรมการบริษัทมีหน้าที่ความรับผิดชอบในการกำกับดูแล ให้บริษัทปฏิบัติตามหลักเกณฑ์ที่กำหนดไว้ในประกาศนี้ และมีหน้าที่ ดังต่อไปนี้

(๑) กำกับดูแลการใช้เทคโนโลยีสารสนเทศให้สอดรับกับกลยุทธ์ในการดำเนินธุรกิจ ให้มีความยืดหยุ่นเพียงพอที่จะรองรับการเปลี่ยนแปลงด้านเทคโนโลยีสารสนเทศ และคำนึงถึงการเปลี่ยนแปลงการดำเนินธุรกิจในอนาคต รวมทั้งความพร้อมในการรับมือภัยคุกคามทางไซเบอร์

(๒) กำกับดูแลให้มีการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ และความเสี่ยงจากภัยคุกคามทางไซเบอร์ ที่อาจเกิดขึ้นจากการนำเทคโนโลยีสารสนเทศมาใช้ดำเนินธุรกิจ โดยให้ถือเป็นความเสี่ยงหลักที่สำคัญในภาพรวมระดับองค์กร และให้เป็นส่วนหนึ่งของการบริหารความเสี่ยงแบบองค์รวม (enterprise risk management : ERM)

(๓) กำกับดูแลให้มีการกำหนดนโยบายที่เกี่ยวข้องกับการกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ และความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่เป็นลายลักษณ์อักษร ซึ่งมีรายละเอียดอย่างน้อย ดังต่อไปนี้

(ก) นโยบายการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management policy)

(ข) นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security policy) ซึ่งต้องมีแผนงานหรือแนวทางในการดำเนินการที่อย่างน้อยต้องครอบคลุมในเรื่อง ดังต่อไปนี้

๑) แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT continuity)

๒) แผนหรือแนวทางในการกำกับดูแลและบริหารจัดการความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ตามหมวด ๗

(๔) กำกับดูแลให้บริษัทนำนโยบายที่ได้รับการอนุมัติมาจัดทำแนวปฏิบัติในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ รวมถึงดูแลให้มีการนำไปปฏิบัติอย่างเหมาะสม และมีการทบทวนนโยบายและแนวทางปฏิบัติอย่างน้อยปีละหนึ่งครั้ง หรือทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

(๕) กำกับดูแลให้มีการรายงานต่อคณะกรรมการบริษัท หรือคณะกรรมการชุดย่อยที่ได้รับมอบหมาย อย่างน้อยในเรื่อง ดังต่อไปนี้

(ก) การรายงานผลการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศในภาพรวมของบริษัท ต้องมอบหมายให้หัวหน้าหน่วยงานบริหารความเสี่ยงเป็นผู้รายงานต่อคณะกรรมการบริษัทหรือคณะกรรมการชุดย่อยที่ได้รับมอบหมาย

(ข) ข้อมูลเกี่ยวกับปัญหาหรือเหตุการณ์ด้านเทคโนโลยีสารสนเทศที่สำคัญ หรือที่อาจส่งผลกระทบในวงกว้าง หรือส่งผลกระทบต่อชื่อเสียงของบริษัท หรือต่อการดำเนินงานและการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

(ค) ผลการทดสอบและการปฏิบัติตามแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ

ทั้งนี้ คณะกรรมการบริษัทอาจมอบหมายให้คณะกรรมการชุดย่อย ทำหน้าที่กำกับดูแลการดำเนินการตามวรรคหนึ่งได้ ดังต่อไปนี้

(๑) คณะกรรมการกำกับดูแลและบริหารจัดการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT steering committee) หรือคณะกรรมการชุดย่อยอื่น ทำหน้าที่กำกับดูแลการใช้เทคโนโลยีสารสนเทศให้สอดรับกับกลยุทธ์ในการดำเนินธุรกิจตามวรรคหนึ่ง (๑)

(๒) คณะกรรมการบริหารความเสี่ยง (risk management committee) หรือคณะกรรมการชุดย่อยอื่น ทำหน้าที่กำกับดูแลให้มีการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ และความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามวรรคหนึ่ง (๒) หรือทำหน้าที่กำกับดูแลให้มีการกำหนดนโยบายที่เกี่ยวข้องกับการกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ และความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามวรรคหนึ่ง (๓)

ในกรณีที่คณะกรรมการบริษัทมอบหมายให้คณะกรรมการชุดย่อย ทำหน้าที่กำกับดูแลการดำเนินการตามวรรคหนึ่ง คณะกรรมการชุดย่อยที่ได้รับมอบหมายต้องรายงานผลการดำเนินการตามวรรคสอง ต่อคณะกรรมการบริษัทตามที่ประกาศนี้กำหนด

ข้อ ๙ บริษัทต้องจัดให้มีนโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เป็นลายลักษณ์อักษรสอดคล้องกับการนำเทคโนโลยีมาใช้ในการดำเนินธุรกิจ ความเสี่ยงที่อาจเกิดขึ้นจากการใช้เทคโนโลยี รวมทั้งความเสี่ยงจากการใช้เทคโนโลยีสารสนเทศภายในองค์กร และความเสี่ยงจากการใช้บริการจากผู้ให้บริการภายนอก โดยนโยบายต้องได้รับการพิจารณาอนุมัติจากคณะกรรมการบริษัท หรือคณะกรรมการชุดย่อยที่ได้รับมอบหมาย ดังต่อไปนี้

(๑) นโยบายการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management policy) ต้องสอดคล้องกับนโยบายการบริหารความเสี่ยงแบบองค์รวมของบริษัท โดยนโยบายต้องแสดงให้เห็นถึงโครงสร้างองค์กร บทบาทหน้าที่ของผู้ที่เกี่ยวข้องในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ และอธิบายแนวทางในการบริหารจัดการความเสี่ยง ซึ่งอย่างน้อยต้องมีรายละเอียดครอบคลุมในเรื่อง ดังต่อไปนี้

(ก) หน้าที่และความรับผิดชอบในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

(ข) กระบวนการหรือขั้นตอนในการประเมินความเสี่ยงและจัดการความเสี่ยง

(ค) ระดับความเสี่ยงที่ยอมรับได้ (IT risk appetite)

(ง) เกณฑ์การประเมินความเสี่ยง โดยครอบคลุมระดับของผลกระทบ และระดับของโอกาสการเกิดเหตุการณ์ เพื่อจัดลำดับความสำคัญในการบริหารจัดการความเสี่ยง

(จ) วิธีการหรือเครื่องมือในการบริหารและจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

(ฉ) การกำหนดดัชนีชี้วัดความเสี่ยง (IT risk indicator) รวมถึงจัดให้มีการติดตามและรายงานผลดัชนีชี้วัดความเสี่ยงดังกล่าวต่อผู้ที่มีหน้าที่รับผิดชอบ เพื่อให้สามารถบริหารจัดการความเสี่ยงได้อย่างเหมาะสม และทันต่อเหตุการณ์

(ช) การรายงานความเสี่ยง (risk reporting)

(๒) นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security policy) ตามข้อ ๑๔

หมวด ๒
การบริหารโครงการด้านเทคโนโลยีสารสนเทศ
(IT project management)

ข้อ ๑๐ บริษัทต้องมีการบริหารจัดการความเสี่ยงของการดำเนินโครงการด้านเทคโนโลยีสารสนเทศอย่างมีประสิทธิภาพ เพื่อไม่ให้เกิดผลกระทบต่อการดำเนินการตามแผนกลยุทธ์ โดยพิจารณาความเสี่ยง การจัดลำดับความสำคัญของโครงการ กรอบการบริหารจัดการโครงการ และการกำกับดูแลโครงการ

ข้อ ๑๑ บริษัทต้องประเมินความเสี่ยงและการจัดลำดับความสำคัญของโครงการด้านเทคโนโลยีสารสนเทศ โดยจะต้องมีการดำเนินการอย่างน้อย ดังต่อไปนี้

(๑) จัดให้มีการศึกษาความจำเป็นและประโยชน์ที่คาดว่าจะได้รับของโครงการที่มีการนำเทคโนโลยีสารสนเทศมาใช้ในการดำเนินธุรกิจก่อนเริ่มโครงการ โดยต้องมีการพิจารณาเลือกใช้เทคโนโลยีอย่างเหมาะสม

(๒) จัดให้มีการประเมินความเสี่ยงและผลกระทบที่อาจเกิดขึ้นกับฝ่ายงานอื่น และระบบที่เกี่ยวข้อง

(๓) ต้องมีการจัดลำดับความสำคัญของโครงการ และนำเสนอขออนุมัติโครงการต่อคณะกรรมการบริษัท หรือคณะกรรมการชุดย่อยที่ได้รับมอบหมาย หรือผู้บริหาร ตามที่ได้กำหนดไว้ กรณีที่บริษัทมีการนำเทคโนโลยีใด ๆ มาใช้เป็นครั้งแรก หรือมีการเปลี่ยนแปลงการใช้เทคโนโลยีที่อาจมีผลกระทบ หรือมีความเสี่ยงอย่างมีนัยสำคัญต่อการดำเนินธุรกิจในภาพรวม บริษัทต้องมีข้อกำหนดที่ชัดเจนในการพิจารณา และจัดให้มีการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ หรือพิจารณาประเด็นความเสี่ยงที่เกี่ยวข้อง รวมทั้งผลกระทบที่อาจเกิดขึ้นต่อการดำเนินงานของบริษัทในภาพรวม และดำเนินการให้คณะกรรมการบริษัท หรือคณะกรรมการที่ได้รับมอบหมาย พิจารณาอนุมัติแผนงานในการนำเทคโนโลยีสารสนเทศมาใช้ หรือการเปลี่ยนแปลงการใช้เทคโนโลยีสารสนเทศ

ข้อ ๑๒ บริษัทต้องมีการกำหนดกรอบการบริหารจัดการโครงการด้านเทคโนโลยีสารสนเทศที่ชัดเจนเป็นลายลักษณ์อักษร เพื่อใช้เป็นแนวทางในการบริหารจัดการโครงการ โดยกรอบการบริหารจัดการอย่างน้อยจะต้องมีรายละเอียดครอบคลุมในเรื่อง ดังต่อไปนี้

(๑) การเริ่มโครงการ

(๒) การดำเนินการ

(๓) การควบคุมโครงการ

(๔) การปิดโครงการ

(๕) การสอบทานโครงการ

ข้อ ๑๓ บริษัทต้องกำกับดูแลโครงการด้านเทคโนโลยีสารสนเทศ โดยกำหนดโครงสร้างการควบคุมและกำกับดูแลโครงการที่ชัดเจน (project governance) มีคณะกรรมการกำกับดูแลโครงการเพื่อกำกับดูแลและติดตามความคืบหน้าการดำเนินงานของโครงการ รวมทั้งให้คำแนะนำและพิจารณาตัดสินใจการดำเนินงานในโครงการที่สำคัญ เพื่อให้โครงการสามารถดำเนินการได้ตามแผนที่กำหนดไว้

หมวด ๓
การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ
(IT security)

ข้อ ๑๔ บริษัทต้องจัดให้มีนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security policy) ที่เป็นลายลักษณ์อักษรสอดคล้องกับการนำเทคโนโลยีมาใช้ในการดำเนินธุรกิจและความเสี่ยงที่อาจเกิดขึ้นจากการใช้เทคโนโลยีนั้น โดยนโยบายต้องได้รับการพิจารณาอนุมัติจากคณะกรรมการบริษัท หรือคณะกรรมการชุดย่อยที่ได้รับมอบหมาย มีการทบทวนอย่างน้อยปีละหนึ่งครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ และมีการสื่อสารให้กับบุคลากรของบริษัททั่วทั้งองค์กร โดยนโยบายที่จัดทำขึ้นอย่างน้อยต้องมีรายละเอียดครอบคลุมในเรื่อง ดังต่อไปนี้

(๑) การบริหารจัดการทรัพย์สินสารสนเทศ (IT asset management)

(๒) การควบคุมการเข้าถึงข้อมูลหรือระบบ (access control)

(๓) การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (physical and environmental security)

(๔) การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT operations security)

(๕) การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT continuity)

(๖) แนวทางในการกำกับดูแลและบริหารจัดการความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (cybersecurity)

ข้อ ๑๕ บริษัทต้องมีการบริหารจัดการความมั่นคงปลอดภัยด้านทรัพยากรบุคคล (human resource security) โดยบุคลากรที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ มีหลักเกณฑ์ในการคัดเลือกเพื่อบรรจุเป็นพนักงาน กฎระเบียบ หรือข้อบังคับระหว่างการปฏิบัติงาน และการสิ้นสุดการปฏิบัติงาน

ข้อ ๑๖ บริษัทต้องจัดให้มีการบริหารจัดการทรัพย์สินสารสนเทศ (asset management) โดยจะต้องมีการดำเนินการอย่างน้อยในเรื่อง ดังต่อไปนี้

(๑) ต้องจัดให้มีการจัดทำทะเบียนรายการทรัพย์สินสารสนเทศ โดยต้องมีการบำรุงรักษาทรัพย์สินสารสนเทศอย่างสม่ำเสมอ รวมถึงต้องจัดให้มีมาตรการด้านความมั่นคงปลอดภัยสำหรับ

การใช้งานเครื่องคอมพิวเตอร์ และอุปกรณ์อื่น ๆ ที่เกี่ยวข้อง เช่น อุปกรณ์ส่วนตัว (bring-your-own-device : BYOD) ที่เชื่อมต่อกับระบบเครือข่ายของบริษัท อุปกรณ์จัดเก็บข้อมูลแบบพกพา (external hard disk/flash drive) เป็นต้น

(๒) ต้องจัดให้มีแนวปฏิบัติการจัดชั้นสารสนเทศ (information classification) ที่เหมาะสมตามชั้นความลับ และความสำคัญของสารสนเทศขององค์กร และมีการกำหนดแนวทางการรักษาความมั่นคงปลอดภัยที่สอดคล้องตามชั้นความลับ ซึ่งรวมถึงการรักษาความมั่นคงปลอดภัยของข้อมูลระหว่างการรับส่งข้อมูลผ่านเครือข่ายสื่อสาร การจัดเก็บข้อมูลในระบบงานหรือสื่อบันทึกข้อมูลต่าง ๆ และการทำลายข้อมูลที่เหมาะสมกับชั้นความลับ

ข้อ ๑๗ บริษัทต้องจัดให้มีการควบคุมการเข้าถึงระบบ ข้อมูล และทรัพย์สินสารสนเทศ (access control) เพื่อป้องกันการเข้าถึงและเปลี่ยนแปลงระบบหรือข้อมูลโดยผู้ที่ไม่มีสิทธิหรือไม่ได้รับอนุญาต โดยจะต้องมีการดำเนินการอย่างน้อยในเรื่อง ดังต่อไปนี้

(๑) กำหนดนโยบายการเข้าถึงหรือเข้าใช้งานระบบ ข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศ รวมถึงนโยบายการใช้บริการเครือข่ายสื่อสารขององค์กร สอดคล้องตามข้อกำหนดการดำเนินธุรกิจ

(๒) กำหนดให้มีการบริหารจัดการสิทธิการใช้งานและตรวจสอบยืนยันตัวตนตามสิทธิที่กำหนดไว้ โดยคำนึงถึงความจำเป็นในการใช้งานและระดับความเสี่ยง

(๓) กำหนดให้มีการทบทวนปรับปรุงสิทธิการใช้งานตามรอบระยะเวลาที่กำหนด

(๔) กำหนดให้มีการเพิกถอนสิทธิการใช้งานเมื่อมีการเปลี่ยนแปลงหน้าที่งาน หรือสิ้นสุดสภาพการเป็นพนักงาน

ข้อ ๑๘ บริษัทต้องจัดให้มีแนวปฏิบัติด้านการเข้ารหัสข้อมูล (cryptography) ในการรักษาความมั่นคงปลอดภัยของข้อมูลที่เหมาะสมตามชั้นความลับและความสำคัญของข้อมูลสารสนเทศ

ข้อ ๑๙ บริษัทต้องจัดให้มีการรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (physical and environmental security) ของศูนย์คอมพิวเตอร์ สถานที่ปฏิบัติงานที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ และพื้นที่ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศที่สำคัญ โดยจะต้องมีการดำเนินการอย่างน้อย ดังต่อไปนี้

(๑) ต้องจัดให้มีระเบียบปฏิบัติการเข้าถึงศูนย์คอมพิวเตอร์เป็นลายลักษณ์อักษร

(๒) ต้องจัดให้มีการควบคุมการเข้าและออกศูนย์คอมพิวเตอร์ โดยจำกัดสิทธิการเข้าถึงศูนย์คอมพิวเตอร์อย่างเหมาะสม รวมทั้งมีการบันทึกและจัดเก็บข้อมูลการเข้าและออก

(๓) ต้องจัดให้มีระบบการป้องกันและกระบวนการบำรุงรักษาอุปกรณ์ คอมพิวเตอร์ และระบบสาธารณูปโภค (facility) ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ เช่น ระบบไฟฟ้าสำรองสำหรับศูนย์คอมพิวเตอร์ ระบบทำความเย็น ระบบป้องกันหรือสัญญาณเตือนไฟไหม้ และกล้องวงจรปิด เป็นต้น

ข้อ ๒๐ บริษัทต้องจัดให้มีการรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสารของบริษัท (network and communication security) โดยจะต้องมีการดำเนินการอย่างน้อย ดังต่อไปนี้

(๑) ต้องจัดให้มีการจำแนกโซนเครือข่ายสื่อสาร โดยมีการจัดแบ่งเครือข่ายอย่างเหมาะสม และจัดให้มีการควบคุมการเชื่อมต่อจากระบบงานต่าง ๆ มายังระบบงานที่มีความสำคัญอย่างเข้มงวด

(๒) ต้องจัดให้มีการควบคุมและจำกัดสิทธิการเข้าถึงระบบเครือข่าย และระบบสารสนเทศจากระยะไกล (remote access) โดยมีการควบคุมความปลอดภัยในการเชื่อมต่อระบบเครือข่ายจากภายนอก และต้องได้รับการอนุมัติให้มีการเข้าถึงอย่างเหมาะสม

ข้อ ๒๑ บริษัทต้องจัดให้มีการรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT operations security) โดยจะต้องมีการบริหารจัดการและดำเนินการอย่างน้อยดังต่อไปนี้

(๑) จัดให้มีการบริหารจัดการการเปลี่ยนแปลง (change management) และอนุมัติการเปลี่ยนแปลงทุกครั้งอย่างเป็นลายลักษณ์อักษร

(๒) จัดให้มีการบริหารจัดการขีดความสามารถของระบบ (capacity management) ให้สามารถรองรับการดำเนินธุรกิจในปัจจุบัน และวางแผนการจัดการให้รองรับการใช้งานในอนาคตได้อย่างมีประสิทธิภาพ

(๓) จัดให้มีการรักษาความมั่นคงปลอดภัยของเครื่องแม่ข่าย (server) โดยการบริหารจัดการการตั้งค่าระบบ (system configuration management) การบริหารจัดการ patch (patch management) การกำหนดสิทธิการเข้าถึงและจำกัดสิทธิการใช้งานของผู้ใช้งานที่มีสิทธิสูง (high privileged ID)

(๔) กำหนดวิธีการและกระบวนการที่ใช้ในการสำรองข้อมูล (data backup) รวมทั้งความถี่ในการสำรองข้อมูลที่เหมาะสมกับลักษณะและความซับซ้อนของการดำเนินงานของบริษัท

(๕) จัดให้มีการจัดเก็บข้อมูลบันทึกเหตุการณ์ (logging) ของเครื่องแม่ข่าย ระบบงาน และอุปกรณ์เครือข่ายที่สำคัญ โดยจะต้องมีความมั่นคงปลอดภัยเพียงพอในการป้องกันการเปลี่ยนแปลงแก้ไข หรือทำลาย รวมถึงมีการสอบทาน log ด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ

(๖) จัดให้มีการติดตามดูแลระบบและการเฝ้าระวังภัยคุกคาม (security monitoring) โดยมีกระบวนการหรือเครื่องมือในการตรวจจับเหตุการณ์ผิดปกติ หรือภัยคุกคามที่มีผลกระทบต่อความมั่นคงปลอดภัยของระบบที่สำคัญ รวมถึงต้องมีการบริหารจัดการช่องโหว่ (vulnerability management) ของระบบที่เหมาะสมตามระดับความเสี่ยง และจัดให้มีผู้เชี่ยวชาญจากภายนอกทำหน้าที่ทดสอบเจาะระบบ โดยเฉพาะระบบงาน (application) และระบบเครือข่าย (network) ที่มีการเชื่อมต่อกับระบบเครือข่ายสื่อสารสาธารณะ (internet facing) อย่างสม่ำเสมอ หรือทุกครั้งที่มีการเปลี่ยนแปลงระบบอย่างมีนัยสำคัญ

ข้อ ๒๒ บริษัทต้องมีหลักเกณฑ์และกระบวนการในการจัดหาและการพัฒนาระบบ (system acquisition and development) ดังต่อไปนี้

(๑) ในการจัดหาระบบ (system acquisition) บริษัทต้องมีการกำหนดหลักเกณฑ์ที่ชัดเจนในการประเมินและคัดเลือกผู้ขาย หรือผู้รับจ้างพัฒนาระบบ ซึ่งต้องทำสัญญาซื้อขายหรือสัญญาจ้างที่กำหนดเงื่อนไขในการพัฒนาระบบที่ชัดเจน

(๒) ในการพัฒนาระบบ (system development) บริษัทต้องจัดให้มีการออกแบบ พัฒนาและทดสอบระบบ เพื่อให้มั่นใจว่าระบบ มีความถูกต้อง มั่นคงปลอดภัย เชื่อถือได้ และพร้อมใช้งาน โดยจะต้องมีการดำเนินการอย่างน้อย ดังนี้

(ก) มีการจัดทำเอกสารความต้องการของระบบงาน (requirement) และเอกสารรายละเอียดคุณสมบัติทางเทคนิค (technical specification) โดยครอบคลุมถึงเรื่องการรักษาความมั่นคงปลอดภัย ซึ่งรวมถึงกระบวนการในการทดสอบระบบงาน

(ข) มีกระบวนการหรือเครื่องมือในการควบคุมเวอร์ชั่นของคำสั่งในการเขียนโปรแกรม (source code version control) โดยจะต้องจำกัดสิทธิผู้ที่จะดำเนินการติดตั้งโปรแกรมในระบบงานที่ให้บริการจริง (production) เท่าที่จำเป็นเท่านั้น

(ค) มีการแบ่งแยกบทบาทหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องในกระบวนการพัฒนาระบบ เช่น การแบ่งแยกระหว่างผู้พัฒนาระบบ (developer) และผู้บริหารจัดการระบบ (administrator)

(ง) มีการแบ่งแยกสภาพแวดล้อมของระบบงานที่ใช้สำหรับการพัฒนา (development) และการทดสอบ (testing) ออกจากระบบงานที่ให้บริการจริง (production)

(จ) มีการทดสอบระบบก่อนการใช้งานจริง เช่น ทดสอบการทำงานของแต่ละระบบ (unit test) ทดสอบการทำงานร่วมกันของระบบต่าง ๆ (system integration test) ทดสอบความพร้อมใช้งานตามกระบวนการและความต้องการของผู้ใช้งาน (user acceptance test) และทดสอบความปลอดภัยของระบบ (security test) ตามกระบวนการในการรักษาความมั่นคงปลอดภัยที่กำหนดในเอกสารรายละเอียดคุณสมบัติทางเทคนิค (technical specification) รวมถึงต้องควบคุมการรักษาความมั่นคงปลอดภัยและความลับของข้อมูลสำคัญที่นำไปใช้ในการทดสอบ

(ฉ) มีการทดสอบประสิทธิภาพ (performance test) สำหรับระบบที่เกี่ยวข้องกับการให้บริการหรือการทำธุรกรรมทางอิเล็กทรอนิกส์

(ช) การจัดทำคู่มือและอบรมผู้ใช้งานระบบและผู้ดูแลระบบ

ข้อ ๒๓ ในกรณีที่บริษัทมีการจัดจ้างผู้ให้บริการภายนอก (third party management) หรือมีพันธมิตรทางธุรกิจที่มีการเชื่อมต่อกับระบบเทคโนโลยีสารสนเทศของบริษัท หรือสามารถเข้าถึงข้อมูลสำคัญของบริษัท หรือของลูกค้าของบริษัทได้ บริษัทต้องมีการกำหนดกระบวนการและหลักเกณฑ์ในการประเมินและคัดเลือกผู้ให้บริการภายนอก โดยต้องจัดทำสัญญาจ้างในการให้บริการ และกำหนดเงื่อนไขให้ผู้ให้บริการภายนอกปฏิบัติตามนโยบายการรักษาความปลอดภัยของบริษัท รวมถึงต้องกำหนดข้อตกลงระดับการให้บริการ (service level agreement : SLA) พร้อมทั้งมีการตรวจสอบและติดตามการให้บริการอย่างสม่ำเสมอ

ทั้งนี้ การใช้บริการเทคโนโลยีสารสนเทศจากผู้ให้บริการภายนอก (IT outsourcing) บริษัทสามารถพิจารณาแนวทางในการดำเนินการตามแนวปฏิบัติของสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัยว่าด้วยหลักเกณฑ์การกำกับดูแลการใช้บริการจากผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศ

ข้อ ๒๔ บริษัทต้องจัดให้มีการบริหารจัดการเหตุการณ์ผิดปกติและปัญหา (IT incident and problem management) ที่เกิดจากการใช้เทคโนโลยีสารสนเทศอย่างเหมาะสมและทันท่วงที โดยจัดให้มีวิธีปฏิบัติ ขั้นตอนปฏิบัติ หรือแผนรองรับ ในการบริหารจัดการเหตุการณ์ผิดปกติและปัญหาที่เกิดจากการใช้เทคโนโลยีสารสนเทศ รวมถึงต้องมีการบันทึก วิเคราะห์ และรายงานเหตุการณ์ผิดปกติและปัญหา และการแก้ไขให้คณะกรรมการบริษัท หรือคณะกรรมการชุดย่อยที่ได้รับมอบหมายทราบในระยะเวลาที่เหมาะสม ทั้งนี้ บริษัทต้องมีการวิเคราะห์สาเหตุที่แท้จริง (root cause) ของปัญหาเพื่อหาแนวทางแก้ไขจากสาเหตุที่แท้จริงและป้องกันไม่ให้เกิดเหตุการณ์ผิดปกติซ้ำในอนาคต

ข้อ ๒๕ บริษัทต้องจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT continuity planning) โดยจะต้องมีการดำเนินการอย่างน้อย ดังต่อไปนี้

(๑) จัดให้มีกระบวนการสำรองข้อมูลที่ครอบคลุมระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบงาน ระบบปฏิบัติการ และฐานข้อมูล เป็นต้น โดยต้องรองรับการกู้คืนข้อมูลตามความเหมาะสมทางธุรกิจ

(๒) จัดเก็บข้อมูลสำรองไว้นอกสถานที่อย่างปลอดภัย โดยบริษัทต้องมีการเฝ้าติดตามกระบวนการสำรองข้อมูลที่สำคัญ รวมถึงทดสอบการกู้คืนข้อมูลสำรอง และดำเนินการให้ข้อมูลสำรองพร้อมใช้งานอยู่เสมอ

(๓) จัดทำแผนการกู้คืนระบบสารสนเทศ (disaster recovery plan) เป็นลายลักษณ์อักษร โดยจะต้องมีการอนุมัติ และสื่อสารให้บุคลากรของบริษัทรับทราบ รวมถึงต้องมีการทบทวนอย่างสม่ำเสมอหรือเมื่อมีการปรับปรุงแก้ไขที่เป็นสาระสำคัญ

(๔) จัดให้มีทดสอบแผนการกู้คืนระบบสารสนเทศอย่างน้อยปีละหนึ่งครั้ง และรายงานผลการทดสอบต่อผู้บริหารของบริษัทให้รับทราบ

หมวด ๔
การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ
(IT risk management)

ข้อ ๒๖ บริษัทต้องบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศให้มีประสิทธิภาพ โดยกำหนดนโยบายการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ครอบคลุมเรื่องโครงสร้างองค์กร และบทบาทหน้าที่ของผู้เกี่ยวข้อง และนำนโยบายดังกล่าวมาจัดทำแนวปฏิบัติ รวมทั้งกระบวนการในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ข้อ ๒๗ บริษัทต้องจัดให้มีแนวทางในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ระบุบริบท ขอบเขต และเกณฑ์การบริหารความเสี่ยง อย่างน้อย ดังต่อไปนี้

(๑) การพิจารณาโอกาสและความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยการระบุบริบทและขอบเขตในการประเมินความเสี่ยงให้ครอบคลุมถึง แผนงาน งานประจำ และการนำเทคโนโลยีสารสนเทศมาใช้

(๒) เกณฑ์การบริหารความเสี่ยงที่มีรายละเอียดเกี่ยวกับเกณฑ์การประเมินความเสี่ยง โดยกำหนดระดับของผลกระทบและระดับของโอกาสการเกิดเหตุการณ์

(๓) ระดับความเสี่ยงที่ยอมรับได้สำหรับความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk appetite)

(๔) กระบวนการประเมินความเสี่ยง เพื่อใช้ในการระบุ วิเคราะห์ และประเมินผลความเสี่ยง

(๕) กระบวนการจัดการความเสี่ยง เพื่อใช้พิจารณาทางเลือก และมาตรการในการจัดการความเสี่ยง รวมถึงการจัดทำแผนบริหารจัดการความเสี่ยง

ข้อ ๒๘ บริษัทต้องจัดให้มีกระบวนการประเมินความเสี่ยง (risk assessment) ด้านเทคโนโลยีสารสนเทศ ตามหลักเกณฑ์และวิธีการ ดังต่อไปนี้

(๑) ระบุความเสี่ยง (risk identification) ด้านเทคโนโลยีสารสนเทศ ซึ่งรวมถึงภัยคุกคามทางไซเบอร์ และช่องโหว่ที่สำคัญ โดยเหตุการณ์ความเสี่ยงดังกล่าวอาจมีสาเหตุมาจากกระบวนการปฏิบัติงาน ระบบงาน บุคลากร หรือปัจจัยภายนอก ตลอดจนระบุการควบคุมที่มีอยู่ในปัจจุบัน และผู้รับผิดชอบหรือเจ้าของความเสี่ยง (risk owners)

(๒) วิเคราะห์ความเสี่ยง (risk analysis) ด้านเทคโนโลยีสารสนเทศ โดยมีการประเมินระดับของผลกระทบ และระดับของโอกาสการเกิดเหตุการณ์ เพื่อจัดลำดับความสำคัญของความเสี่ยง

(๓) ประเมินค่าความเสี่ยง (risk evaluation) โดยการพิจารณาระดับความเสี่ยงกับระดับความเสี่ยงที่ยอมรับได้ (IT risk appetite) เพื่อจัดลำดับและหาแนวทางในการตอบสนองความเสี่ยงที่เหมาะสม

ข้อ ๒๙ บริษัทต้องมีการจัดการความเสี่ยง (risk treatment) โดยมีแนวทางในการจัดการควบคุม และป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อให้ความเสี่ยงที่เหลืออยู่ (residual risk) อยู่ในระดับความเสี่ยงที่ยอมรับได้ คำนึงถึงความสมดุลระหว่างต้นทุนในการป้องกันความเสี่ยง และผลประโยชน์ที่คาดว่าจะได้รับ รวมทั้งกำหนดดัชนีชี้วัดความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT key risk indicators) เพื่อใช้ในการติดตามและทบทวนความเสี่ยง

ข้อ ๓๐ บริษัทต้องจัดให้มีกระบวนการติดตามและทบทวนความเสี่ยง (risk monitoring and review) ด้านเทคโนโลยีสารสนเทศที่มีประสิทธิภาพ เพื่อให้ความเสี่ยงอยู่ในระดับที่ยอมรับได้

ข้อ ๓๑ บริษัทต้องจัดให้มีการรายงานความเสี่ยง (risk reporting) โดยหัวหน้าหน่วยงานบริหารความเสี่ยงต้องเป็นผู้ทำหน้าที่รายงานผลการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและแนวโน้มของความเสี่ยงด้านเทคโนโลยีสารสนเทศที่อาจเกิดขึ้นต่อคณะกรรมการบริษัทหรือคณะกรรมการชุดย่อยที่ได้รับมอบหมายในระยะเวลาที่เหมาะสม

หมวด ๕
การปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ
(IT compliance)

ข้อ ๓๒ บริษัทต้องจัดให้มีการกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (IT compliance) เช่น กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ กฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล รวมถึงกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงิน และกฎหมายอื่นในลักษณะเดียวกัน เพื่อป้องกันไม่ให้เกิดการฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมายและหลักเกณฑ์ของหน่วยงานกำกับดูแลที่เกี่ยวข้อง

หมวด ๖
การตรวจสอบด้านเทคโนโลยีสารสนเทศ
(IT audit)

ข้อ ๓๓ บริษัทต้องมีการกำหนดบทบาทหน้าที่และแผนงานในการตรวจสอบ ด้านเทคโนโลยีสารสนเทศ โดยจะต้องมีการดำเนินการอย่างน้อย ดังต่อไปนี้

(๑) จัดให้มีผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศที่มีความรู้ ประสบการณ์ และความเชี่ยวชาญเกี่ยวกับการตรวจสอบด้านเทคโนโลยีสารสนเทศ ซึ่งอาจเป็นผู้ตรวจสอบภายใน หรือผู้ตรวจสอบจากภายนอกก็ได้

(๒) ต้องจัดให้มีแผนงานและขอบเขตการตรวจสอบด้านเทคโนโลยีสารสนเทศที่ครอบคลุมความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัท โดยแผนงานและขอบเขตในการตรวจสอบต้องได้รับความเห็นชอบจากคณะกรรมการตรวจสอบ และต้องจัดให้มีการทบทวนอย่างน้อยปีละหนึ่งครั้ง หรือทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

ข้อ ๓๔ บริษัทต้องจัดให้มีการปฏิบัติงานตรวจสอบด้านเทคโนโลยีสารสนเทศ โดยจะต้องมีการดำเนินการอย่างน้อย ดังต่อไปนี้

(๑) ตรวจสอบด้านเทคโนโลยีสารสนเทศให้เหมาะสมตามแผนงานและขอบเขตที่กำหนด และเมื่อมีเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศที่มีนัยสำคัญ

(๒) ในกรณีที่ระบบเทคโนโลยีของบริษัทมีความซับซ้อนหรือเป็นเทคโนโลยีใหม่ โดยบริษัทมีข้อจำกัดที่ไม่สามารถประเมินหรือตรวจสอบเองได้ บริษัทสามารถว่าจ้างผู้เชี่ยวชาญภายนอกทำหน้าที่ในการตรวจสอบแทนได้

ข้อ ๓๕ บริษัทต้องจัดให้มีการรายงานผลและติดตามผลการตรวจสอบ โดยจะต้องมีการดำเนินการอย่างน้อย ดังต่อไปนี้

(๑) จัดทำรายงานผลการตรวจสอบด้านเทคโนโลยีสารสนเทศเสนอต่อคณะกรรมการตรวจสอบและจัดเก็บรายงานผลการตรวจสอบดังกล่าวไว้ที่บริษัทเพื่อรองรับการตรวจสอบ หรือร้องขอจากสำนักงาน

(๒) จัดให้มีการติดตามประเด็นจากการตรวจสอบด้านเทคโนโลยีสารสนเทศ และรายงานประเด็นสำคัญให้กับคณะกรรมการตรวจสอบ และฝ่ายงานที่เกี่ยวข้องทราบ

หมวด ๗
การกำกับดูแลและการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (cybersecurity)

ข้อ ๓๖ บริษัทต้องจัดให้มีแนวทางการกำกับดูแลการเตรียมความพร้อมรับมือภัยคุกคามทางไซเบอร์ (cyber resilience) โดยมีกรอบการดำเนินงานและแนวทางที่ใช้ในการกำกับดูแลและบริหารจัดการความเสี่ยงจากภัยคุกคามทางไซเบอร์ในภาพรวมขององค์กร ที่สอดคล้องกับกฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้งเหมาะสมสอดคล้องกับขนาด และความซับซ้อนของการดำเนินธุรกิจ

ข้อ ๓๗ บริษัทต้องมีการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์และการระบุความเสี่ยง (identification) โดยจะต้องมีการดำเนินการอย่างน้อย ดังต่อไปนี้

(๑) กำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (cybersecurity governance)

(๒) จัดทำรายการทรัพย์สินสารสนเทศ และบริหารจัดการทรัพย์สินสารสนเทศ

(๓) กำหนดขอบเขตและวิธีการในการประเมินความเสี่ยงด้านไซเบอร์ที่สอดคล้องกับการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ หรือความมั่นคงปลอดภัยสารสนเทศ

(๔) จัดให้มีการจัดทำแผนบริหารจัดการความเสี่ยง มาตรการจัดการความเสี่ยง หรือแนวทางในการดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์ ที่สอดคล้องกับผลการประเมินความเสี่ยงด้านไซเบอร์

(๕) มีการบริหารจัดการความเสี่ยงเกี่ยวกับห่วงโซ่ของผู้ให้บริการภายนอก (supply chain risk management) แนวทางในการบริหารจัดการผู้ให้บริการภายนอก การทำสัญญาจ้าง การประเมินความเหมาะสม การติดตามและประเมินผลการปฏิบัติงาน และการสอบทานผลการปฏิบัติงาน

ข้อ ๓๘ บริษัทต้องมีการป้องกันความเสี่ยง (protection) โดยจะต้องมีการดำเนินการอย่างน้อย ดังต่อไปนี้

(๑) กำหนดแนวทางการควบคุมและป้องกันความเสี่ยงของโครงสร้างพื้นฐานสำคัญทางสารสนเทศของบริษัท เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย อุปกรณ์ฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูล และระบบงาน เป็นต้น รวมทั้งการตั้งค่าระบบงาน การเข้าถึงระบบงานและการจัดการสิทธิ์ การรักษาความมั่นคงปลอดภัยของข้อมูล การพัฒนาระบบงานที่มีความปลอดภัยตามขั้นตอนหรือกระบวนการในการพัฒนาระบบงาน (system development life cycle: SDLC) การบริหารจัดการ patch โดยมีการใช้เทคโนโลยีอย่างเหมาะสม เพื่อให้บริษัทมีกระบวนการ เครื่องมือ และวิธีการในการควบคุมหรือลดผลกระทบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่อาจเกิดขึ้น

(๒) มีเอกสารการปฏิบัติงานสำหรับดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์สอดคล้องตามมาตรฐานและแนวปฏิบัติที่ดี

(๓) มีแนวทางในการรวบรวมและวิเคราะห์ข้อมูลภัยคุกคามไซเบอร์ ตลอดจนกำหนดวิธีการรวมทั้งช่องทางในการแลกเปลี่ยนข้อมูล และสร้างความร่วมมือในการบริหารจัดการ และรับมือภัยคุกคามทางไซเบอร์ทั้งภายในและภายนอกองค์กร

ข้อ ๓๙ บริษัทต้องมีการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (detection) โดยจะต้องมีการดำเนินการอย่างน้อย ดังต่อไปนี้

(๑) จัดให้มีช่องทางในการรายงานช่องโหว่ จุดอ่อน เหตุการณ์ หรือสถานการณ์ที่เกี่ยวข้องด้านความมั่นคงปลอดภัยไซเบอร์ โดยกำหนดขอบเขตหน้าที่ความรับผิดชอบของหน่วยงานที่เกี่ยวข้องทั้งหน่วยงานภายในและหน่วยงานภายนอก

(๒) กำหนดแนวทางในการค้นหา ทดสอบ และบริหารจัดการช่องโหว่ทางด้านเทคโนโลยีสารสนเทศ เพื่อให้สามารถตรวจจับ วิเคราะห์ ติดตาม และแจ้งเตือนเหตุการณ์ผิดปกติหรือภัยคุกคามทางไซเบอร์ให้แก่หน่วยงานหรือผู้รับผิดชอบรับทราบ และกำหนดแนวทางในการสื่อสารและการดำเนินการแก้ไขในเบื้องต้นได้อย่างทันการณ์

ข้อ ๔๐ บริษัทต้องมีมาตรการในการรับมือและตอบสนองเมื่อตรวจพบภัยคุกคามทางไซเบอร์ (response) โดยจะต้องมีการดำเนินการอย่างน้อย ดังต่อไปนี้

(๑) กำหนดแนวทางในการบริหารจัดการการรับมือเหตุการณ์ผิดปกติหรือภัยคุกคามทางไซเบอร์ เพื่อให้บริษัทสามารถตอบสนองและรับมือกับความเสี่ยงได้อย่างทันการณ์

(๒) กำหนดให้มีการจัดทำ ซักซ้อม หรือทดสอบแผนรับมือภัยคุกคามทางไซเบอร์ (cybersecurity) แผนฉุกเฉิน การสืบสวน และวิเคราะห์สาเหตุการแก้ปัญหา และจัดทำรายงานเพื่อเสนอต่อคณะกรรมการบริษัท หรือคณะกรรมการที่ได้รับมอบหมาย

(๓) กำหนดแนวทางในการสื่อสาร เพื่อดำเนินการแก้ไขเหตุการณ์หรือสถานการณ์จากภัยคุกคามทางไซเบอร์

ข้อ ๔๑ บริษัทต้องมีแนวทางเพื่อฟื้นฟูความเสียหายจากภัยคุกคามทางไซเบอร์ (recovery) โดยจะต้องมีการดำเนินการอย่างน้อย ดังต่อไปนี้

(๑) กำหนดแนวทางและมาตรการในการฟื้นฟูความเสียหายจากเหตุการณ์ หรือสถานการณ์จากภัยคุกคามทางไซเบอร์ สอดคล้องกับผลการประเมินความเสี่ยงและผลกระทบตามกรอบการดำเนินงานความมั่นคงปลอดภัยไซเบอร์และการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัท

(๒) กำหนดแนวทางในการสื่อสารเพื่อดำเนินการฟื้นฟูความเสียหายจากเหตุการณ์หรือสถานการณ์จากภัยคุกคามทางไซเบอร์

ข้อ ๔๒ บริษัทต้องมีการประเมินความเสี่ยงจากภัยคุกคามทางไซเบอร์ (cybersecurity risk assessment) โดยการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ หรือภัยคุกคามทางไซเบอร์ เพื่อให้ทราบถึงสถานภาพความเสี่ยงจากภัยคุกคามทางไซเบอร์ของบริษัทตามสภาพปัจจัยความเสี่ยง สถานการณ์ความเสี่ยง ภัยคุกคามหรือช่องโหว่ที่เกี่ยวข้องในการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยพิจารณาปัจจัยความเสี่ยงจากภัยคุกคามทางไซเบอร์ ดังต่อไปนี้

(๑) เกณฑ์ในการประเมินและจัดระดับความรุนแรง และผลกระทบของเหตุการณ์หรือสถานการณ์การถูกโจมตีทางไซเบอร์ รวมทั้งโอกาสเกิดของเหตุการณ์ ตลอดจนการประเมินระดับความเสี่ยงจากภัยคุกคามทางไซเบอร์ โดยเกณฑ์ผลกระทบของเหตุการณ์ ให้พิจารณาตามหลักเกณฑ์ทั้งสี่ด้าน ดังนี้

(ก) ด้านการรักษาความลับ (confidentiality)

(ข) ด้านการรักษาความครบถ้วน (integrity)

(ค) ด้านการรักษาสภาพพร้อมใช้ (availability) และ

(ง) ด้านการปฏิบัติตามกฎเกณฑ์ (law & regulation compliance)

(๒) จัดให้มีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์หรือภัยคุกคามทางไซเบอร์ และต้องมีการรายงานผลการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ และแนวโน้มของ

ความเสี่ยงด้านเทคโนโลยีสารสนเทศที่อาจเกิดขึ้นต่อคณะกรรมการบริษัท หรือคณะกรรมการชุดย่อยที่ได้รับมอบหมาย ในระยะเวลาที่เหมาะสม

หมวด ๘
การรายงานเหตุการณ์ภัยคุกคามทางไซเบอร์หรือภัยคุกคามที่มีต่อระบบเทคโนโลยีสารสนเทศ
(reporting)

ข้อ ๔๓ บริษัทต้องมีการรายงานเหตุการณ์ภัยคุกคามทางไซเบอร์หรือภัยคุกคามที่มีต่อระบบเทคโนโลยีสารสนเทศ ดังต่อไปนี้

(๑) รายงานต่อสำนักงานในกรณีที่เกิดปัญหาหรือเหตุการณ์ที่มีนัยสำคัญในการใช้เทคโนโลยีสารสนเทศซึ่งส่งผลกระทบต่อการให้บริการ หรือระบบ หรือข้อมูลผู้เอาประกันภัย หรือชื่อเสียงของบริษัท และให้รวมถึงกรณีที่เทคโนโลยีสารสนเทศที่สำคัญของบริษัทถูกโจมตี หรือถูกขู่โจมตีจากภัยคุกคามทางไซเบอร์ และเป็นปัญหาหรือเหตุการณ์ที่บริษัทต้องรายงานต่อผู้บริหารสูงสุดของบริษัททราบ ให้บริษัทรายงานต่อสำนักงานทันทีเมื่อเกิดหรือรับรู้เหตุการณ์นั้น พร้อมแจ้งรายละเอียดและสาเหตุของเหตุการณ์ที่เกิดขึ้น ผลกระทบที่คาดว่าจะเกิดขึ้น การดำเนินการแก้ไขปัญหา ผลการแก้ไขปัญหา ระยะเวลาในการแก้ไข และแนวทางป้องกันในอนาคต

(๒) กรณีที่บริษัทถูกโจมตีจากภัยคุกคามทางไซเบอร์ เป็นปัญหาหรือเหตุการณ์ที่เกี่ยวข้องกับการให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่เป็นภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง และภัยคุกคามทางไซเบอร์ในระดับวิกฤติ ต้องแจ้งเหตุการณ์ละเมิดโดยไม่ชักช้าภายในเจ็ดสิบสองชั่วโมงไปยังสำนักงานหรือหน่วยงานตามที่กฎหมายกำหนด รวมถึงการให้ข้อมูลหรือประสานกับหน่วยงานของรัฐ หรือหน่วยงานองค์กรที่แต่งตั้งขึ้นตามกฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ในการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์

ประกาศ ณ วันที่ ๑ กันยายน พ.ศ. ๒๕๖๓
ประสงค์ พูนธเนศ
ปลัดกระทรวงการคลัง
ประธานกรรมการ
คณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย