- ร่าง –

ประกาศคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย
เรื่อง หลักเกณฑ์การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของ
บริษัทประกันชีวิต พ.ศ. ....

ปัจจุบัน ธุรกิจประกันภัยต้องเผชิญความท้าทายจากสภาวะการแข่งขันที่รุนแรงและเทคโนโลยีที่เติบโตรวดเร็วแบบก้าวกระโดด ทำให้บริษัทประกันภัยต้องปรับตัวให้เท่าทันและสามารถดำเนินธุรกิจต่อไปได้ หลายบริษัทได้นำเทคโนโลยีเข้ามาช่วยในการดำเนินงาน พัฒนาผลิตภัณฑ์ และบริการลูกค้า อาทิเช่น การขายผลิตภัณฑ์ประกันภัยผ่านช่องทางออนไลน์ ระบบการจัดเก็บข้อมูลลูกค้า ระบบการพิจารณารับประกันภัย ระบบการเงินและบัญชี ระบบการจ่ายค่าสินไหมทดแทนและการจ่ายผลประโยชน์ตามกรมธรรม์ประกันชีวิต ซึ่งการนำเทคโนโลยีเข้ามามีบทบาทในการดำเนินธุรกิจมากขึ้น ย่อมมีความเสี่ยงแฝงมาด้วย ไม่ว่าจะเป็นความเสี่ยงด้านเทคโนโลยีสารสนเทศ และความเสี่ยงจากภัยคุกคามทางไซเบอร์ ซึ่งปัจจุบันมีแนวโน้มเพิ่มสูงขึ้นเป็นอย่างมาก ที่อาจก่อให้เกิดความเสียหายและมีผลกระทบต่อความเชื่อมั่นของลูกค้า

ดังนั้น คณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (คปภ.) จึงกำหนดให้มีหลักเกณฑ์การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ และด้านความมั่นคงปลอดภัยไซเบอร์ให้บริษัทประกันภัยมีการกำกับดูแลและบริหารจัดการที่ดีด้านเทคโนโลยีสารสนเทศ การบริหารจัดการที่ดีในการพิจารณาและจัดการแผนงานในการนำเทคโนโลยีสารสนเทศมาใช้ในองค์กร การบริหารงานโครงการด้านเทคโนโลยีสารสนเทศ การปฏิบัติงานและการให้บริการด้านเทคโนโลยีสารสนเทศ รวมทั้งให้มีการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการบริหารจัดการความเสี่ยงดังกล่าวอย่างเหมาะสม ตลอดจนการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ และการตรวจสอบด้านเทคโนโลยีสารสนเทศ

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

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

ข้อ ๒ ประกาศนี้ให้ใช้บังคับเมื่อพ้นเก้าสิบวันนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป เว้นแต่หมวด ๗ ให้มีผลบังคับใช้ตั้งแต่วันที่ ๑ มกราคม ๒๕๖๔ เป็นต้นไป

ข้อ ๓ ในประกาศนี้

(๑) “ความเสี่ยงด้านเทคโนโลยีสารสนเทศ” (IT Risk) หมายความว่า ความเสี่ยงที่อาจเกิดขึ้นจากการใช้เทคโนโลยีสารสนเทศในการดำเนินธุรกิจ ซึ่งมีผลกระทบต่อระบบหรือการปฏิบัติงานของบริษัท รวมถึงความเสี่ยงที่เกิดจากภัยคุกคามทางไซเบอร์ (Cyber Threat)

(๒) “เทคโนโลยีสารสนเทศ” (Information Technology: IT) หมายความว่า เทคโนโลยีสารสนเทศที่นำมาใช้ในการดำเนินธุรกิจ ซึ่งครอบคลุมถึง ข้อมูลหรือสารสนเทศ (Data/Information) ระบบปฏิบัติการ (Operating System) ระบบงาน (Application System) ระบบฐานข้อมูล (Database System) อุปกรณ์คอมพิวเตอร์ (Hardware) และระบบเครือข่ายสื่อสาร (Communication)

(๓) “ทรัพย์สินสารสนเทศ” หมายความว่า

๑) ทรัพย์สินสารสนเทศประเภทระบบ ได้แก่ ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

๒) ทรัพย์สินสารสนเทศประเภทอุปกรณ์ ได้แก่ ตัวเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล และอุปกรณ์อื่นใด

๓) ทรัพย์สินสารสนเทศประเภทข้อมูล ได้แก่ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์

(๔) “ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ” (IT Security) หมายความว่า การป้องกันด้านเทคโนโลยีสารสนเทศ/ทรัพย์สินสารสนเทศจากการเข้าถึง ใช้ เปิดเผย ขัดขวาง เปลี่ยนแปลงแก้ไข ทำให้สูญหาย ทำให้เสียหาย ถูกทำลาย หรือล่วงรู้โดยมิชอบ โดยมีความหมายรวมถึง ความมั่นคงปลอดภัยสารสนเทศ (Information Security) ซึ่งครอบคลุมถึงการธำรงไว้ซึ่งการรักษาความลับ (Confidentiality) การรักษาความครบถ้วน (Integrity) และการรักษาสภาพพร้อมใช้งาน (Availability) ของเทคโนโลยีสารสนเทศและทรัพย์สินสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-repudiation) และความน่าเชื่อถือ (Reliability)

(๕) “การรักษาความมั่นคงปลอดภัยไซเบอร์” (Cybersecurity) หมายความว่า มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศ ทั้งนี้ ให้เป็นไปตามนิยามของกฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์

(๖) “ไซเบอร์” (Cyber) หมายความว่า ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการ โดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกันที่เชื่อมต่อกันเป็นการทั่วไป

(๗) “ภัยคุกคามทางไซเบอร์” (Cyber Threat) หมายความว่า การกระทำหรือการดำเนินการใดๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

กรณีภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบต่อภารกิจหรือการดำเนินการที่เกี่ยวข้องในการให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ให้บริษัทดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับภัยคุกคามทางไซเบอร์ ๓ ระดับ ได้แก่ ระดับไม่ร้ายแรง ระดับร้ายแรง และระดับวิกฤติ ตามกฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์

(๘) “การรักษาความลับ” (Confidentiality) หมายความว่า การรักษาหรือสงวนไว้เพื่อป้องกันระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ หรือข้อมูลคอมพิวเตอร์จากการเข้าถึง ใช้ หรือเปิดเผยโดยบุคคลซึ่งไม่ได้รับอนุญาต

(๙) “การรักษาความครบถ้วน” (Integrity) หมายความว่า การดำเนินการเพื่อให้ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ หรือข้อมูลคอมพิวเตอร์อยู่ในสภาพสมบูรณ์ขณะที่มีการใช้งาน ประมวลผล โอนหรือเก็บรักษา เพื่อมิให้มีการเปลี่ยนแปลงแก้ไข ทำให้สูญหาย ทำให้เสียหาย หรือถูกทำลายโดยไม่ได้รับอนุญาตหรือโดยมิชอบ

(๑๐) “การรักษาสภาพพร้อมใช้งาน” (Availability) หมายความว่า การจัดทำให้ทรัพย์สินสารสนเทศหรือเทคโนโลยีสารสนเทศ สามารถทำงาน เข้าถึง หรือใช้งานได้ในเวลาที่ต้องการ

(๑๑) “บริษัท” หมายความว่า บริษัทมหาชนจำกัดที่ได้รับใบอนุญาตประกอบธุรกิจประกันชีวิตตามกฎหมายว่าด้วยประกันชีวิต และหมายความรวมถึงสาขาของบริษัทประกันชีวิตต่างประเทศที่ได้รับใบอนุญาตประกอบธุรกิจประกันชีวิตในราชอาณาจักรตามกฎหมายว่าด้วยประกันชีวิตด้วย

(๑๒) “คณะกรรมการบริษัท” หมายความว่า คณะกรรมการของบริษัทตามกฎหมายว่าด้วยประกันชีวิตและให้หมายความรวมถึง คณะกรรมการบริหารสาขาของบริษัทประกันชีวิตต่างประเทศที่ได้รับใบอนุญาตประกอบธุรกิจประกันชีวิตตามกฎหมายว่าด้วยประกันชีวิต ซึ่งต้องมีผู้จัดการสาขาเป็นกรรมการรวมอยู่ด้วย

(๑๓) “ผู้บริหาร” หมายความว่า ผู้จัดการ ผู้ดำรงตำแหน่งระดับบริหารสี่รายแรกนับต่อจากผู้จัดการลงมา ผู้ซึ่งดำรงตำแหน่งเทียบเท่ากับผู้ดำรงตำแหน่งระดับบริหารรายที่สี่ทุกราย และให้หมายความรวมถึงผู้ดำรงตำแหน่งระดับบริหารในสายงานบัญชีหรือการเงินที่เป็นระดับผู้จัดการฝ่ายขึ้นไปหรือเทียบเท่า

(๑๔) “สำนักงาน” หมายความว่า สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย

ข้อ ๔ ให้สำนักงานมีอำนาจกำหนดแนวทางปฏิบัติ และสั่งการให้บริษัทดำเนินการเกี่ยวกับการบริหารจัดการความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ รวมถึงความเสี่ยงที่เกิดจากภัยคุกคามทางไซเบอร์ ตามขนาด ลักษณะ ความซับซ้อน และระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัท

ข้อ ๕ หลักเกณฑ์การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัท ครอบคลุม ๘ หมวด 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) การรายงานเหตุการณ์ภัยคุกคามและความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Reporting)

หมวด ๑
การกำกับดูแลด้านเทคโนโลยีสารสนเทศ
(IT Governance)

เพื่อให้บริษัทมีการกำกับดูแลและการบริหารจัดการที่ดีด้านเทคโนโลยีสารสนเทศที่สามารถบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและด้านภัยคุกคามทางไซเบอร์ได้อย่างเหมาะสมกับขนาด ลักษณะความซับซ้อน และสภาพแวดล้อมในการดำเนินธุรกิจ โดยบริษัทต้องกำหนดบทบาทหน้าที่ความรับผิดชอบของคณะกรรมการบริษัท รวมทั้งจัดให้มีโครงสร้างการกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศเพื่อให้มีการถ่วงดุลอย่างเป็นอิสระ สอดคล้องตามหลักการผู้รับผิดชอบ ๓ ระดับ (๓ line of defense) และนโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยมีรายละเอียดดังนี้

ข้อ ๖ องค์ประกอบของคณะกรรมการบริษัท

คณะกรรมการบริษัทต้องมีองค์ประกอบตามประกาศคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัยว่าด้วยเรื่องการกำกับดูแลกิจการที่ดีของบริษัทประกันชีวิต ทั้งนี้ บริษัทควรมีกรรมการที่มีความรู้ หรือประสบการณ์เกี่ยวข้องด้านเทคโนโลยีสารสนเทศอย่างน้อย ๑ ท่าน เพื่อสามารถกำหนดทิศทางการดำเนินธุรกิจสอดคล้องกับบริบทในปัจจุบัน และกำกับดูแลการใช้เทคโนโลยีสอดรับกับกลยุทธ์ในการดำเนินธุรกิจ มีความรู้เท่าทันความเสี่ยง และพัฒนาการด้านเทคโนโลยีสารสนเทศที่เปลี่ยนแปลงไป รวมทั้ง คณะกรรมการบริษัทควรได้รับการอบรมให้ความรู้เกี่ยวกับเทคโนโลยีสารสนเทศ แนวโน้มเกี่ยวกับภัยคุกคามทางไซเบอร์ และความเสี่ยงที่เกี่ยวข้องอย่างเหมาะสม

ข้อ ๗ หน้าที่ความรับผิดชอบของคณะกรรมการบริษัท

คณะกรรมการบริษัทมีหน้าที่รับผิดชอบในการกำกับดูแลให้บริษัทปฏิบัติตามหลักเกณฑ์ที่กำหนดไว้ในประกาศฉบับนี้ และมีหน้าที่ดังต่อไปนี้

(๑) กำกับดูแลให้มีการใช้เทคโนโลยีสารสนเทศที่สอดรับกับกลยุทธ์ในการดำเนินธุรกิจ และมีความยืดหยุ่นเพียงพอที่จะรองรับการเปลี่ยนแปลงด้านเทคโนโลยีสารสนเทศ และต้องคำนึงถึงการเปลี่ยนแปลงการดำเนินธุรกิจในอนาคต รวมทั้งความพร้อมในการรับมือภัยคุกคามทางไซเบอร์

(๒) กำกับดูแลให้มีการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นจากการนำเทคโนโลยีสารสนเทศมาใช้ดำเนินธุรกิจ โดยให้ถือเป็นความเสี่ยงหลักที่สำคัญในภาพรวมระดับองค์กร และต้องเป็นส่วนหนึ่งของการบริหารความเสี่ยงแบบองค์รวม (Enterprise Risk Management: ERM)

(๓) กำกับดูแลให้มีการกำหนดนโยบายที่เกี่ยวข้องในการกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่เป็นลายลักษณ์อักษร ในเรื่องต่อไปนี้เป็นอย่างน้อย

๑) นโยบายการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management Policy)

๒) นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security Policy) โดยอย่างน้อยต้องครอบคลุมในเรื่องดังต่อไปนี้

๒.๑) แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT Continuity)

๒.๒) แผนหรือแนวทางในการกำกับดูแลและบริหารจัดการความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ทั้งนี้ คณะกรรมการบริษัทสามารถมอบหมายให้คณะกรรมการชุดย่อย เช่น IT Steering Committee ทำหน้าที่บริหารจัดการและกำกับดูแลการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ รวมทั้งพิจารณาอนุมัตินโยบายที่เกี่ยวข้องกับการกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและความเสี่ยงจากภัยคุกคามทางไซเบอร์ได้ และให้รายงานต่อคณะกรรมการบริษัทตามที่ประกาศกำหนด

(๔) กำกับดูแลให้บริษัทนำนโยบายที่ได้รับการอนุมัติมาจัดทำแนวปฏิบัติในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ รวมถึงดูแลให้มีการนำไปปฏิบัติอย่างเหมาะสม และมีการทบทวนนโยบายและแนวทางปฏิบัติอย่างน้อยปีละหนึ่งครั้ง หรือทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

(๕) กำกับดูแลให้มีการรายงานต่อคณะกรรมการบริษัท หรือคณะกรรมการชุดย่อยหรือคณะทำงานที่ได้รับมอบหมาย อย่างน้อยในเรื่องดังต่อไปนี้

- ผลการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศในภาพรวมของบริษัท

- ข้อมูลเกี่ยวกับปัญหาหรือเหตุการณ์ด้านเทคโนโลยีสารสนเทศที่สำคัญหรือที่อาจส่งผลกระทบในวงกว้างหรือส่งผลกระทบต่อชื่อเสียงของบริษัท หรือต่อการดำเนินงานและการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ
- ผลการทดสอบและการปฏิบัติตามแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ

ข้อ ๘ นโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ

บริษัทต้องจัดให้มีนโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เป็นลายลักษณ์อักษร สอดคล้องกับการนำเทคโนโลยีมาใช้ในการดำเนินธุรกิจของบริษัท ความเสี่ยงที่อาจเกิดขึ้นจากการใช้เทคโนโลยี รวมทั้งความเสี่ยงจากการใช้เทคโนโลยีสารสนเทศภายในองค์กรและความเสี่ยงจากการใช้บริการจากผู้ให้บริการภายนอก โดยนโยบายต้องได้รับการพิจารณาอนุมัติจากคณะกรรมการบริษัทหรือคณะกรรมการที่ได้รับมอบหมาย

๑) นโยบายการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management Policy) ต้องสอดคล้องกับนโยบายการบริหารความเสี่ยงแบบองค์รวมของบริษัท โดยนโยบายต้องแสดงให้เห็นถึงโครงสร้างองค์กร บทบาทหน้าที่ของผู้ที่เกี่ยวข้องในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ และอธิบายแนวทางในการบริหารจัดการความเสี่ยงอย่างน้อยควรครอบคลุมในเรื่องดังต่อไปนี้

- หน้าที่และความรับผิดชอบในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ
- กระบวนการหรือขั้นตอนในการประเมินความเสี่ยงและจัดการความเสี่ยง
- ระดับความเสี่ยงที่ยอมรับได้ (IT Risk Appetite)
- เกณฑ์การประเมินความเสี่ยงที่ครอบคลุมถึงโอกาสหรือความถี่ที่จะเกิดความเสี่ยง และผลกระทบที่จะเกิดขึ้น เพื่อจัดลำดับความสำคัญในการบริหารจัดการความเสี่ยง
- วิธีการหรือเครื่องมือในการบริหารและจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้
- การกำหนดดัชนีชี้วัดความเสี่ยง (IT Risk Indicator: Key Risk Indicator: KRI) รวมถึงจัดให้มีการติดตามและรายงานผลดัชนีชี้วัดความเสี่ยงดังกล่าวต่อผู้ที่มีหน้าที่รับผิดชอบ เพื่อให้สามารถบริหารจัดการความเสี่ยงได้อย่างเหมาะสมและทันต่อเหตุการณ์
- การรายงานความเสี่ยง (Risk Reporting)

๒) นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security Policy) รายละเอียดปรากฏตามหมวด ๓ ข้อ ๑๒

หมวด ๒
การบริหารโครงการด้านเทคโนโลยีสารสนเทศ
(IT Project Management)

เพื่อให้มีการบริหารจัดการความเสี่ยงของการดำเนินโครงการด้านเทคโนโลยีสารสนเทศอย่างมีประสิทธิภาพ และไม่ก่อให้เกิดผลกระทบต่อการดำเนินการตามแผนกลยุทธ์ของบริษัท ให้บริษัทพิจารณาประเด็นความเสี่ยงและการจัดลำดับความสำคัญของโครงการ กรอบการบริหารจัดการโครงการ การกำกับดูแลโครงการ โดยมีรายละเอียด ดังนี้

ข้อ ๙ การประเมินความเสี่ยงและการจัดลำดับความสำคัญของโครงการ ต้องดำเนินการ ดังนี้

(๑) จัดให้มีการศึกษาความจำเป็นและประโยชน์ที่คาดว่าจะได้รับของโครงการที่มีการนำเทคโนโลยีสารสนเทศมาใช้ในการดำเนินธุรกิจก่อนเริ่มโครงการ โดยต้องมีการพิจารณาเลือกใช้เทคโนโลยีอย่างเหมาะสม

(๒) จัดให้มีการประเมินความเสี่ยงและผลกระทบที่อาจเกิดขึ้นกับฝ่ายงานอื่นและระบบที่เกี่ยวข้อง

(๓) ต้องมีการจัดลำดับความสำคัญของโครงการและนำเสนอขออนุมัติโครงการต่อคณะกรรมการบริษัท หรือคณะกรรมการที่ได้รับมอบหมาย หรือผู้บริหารระดับสูงตามที่ได้กำหนดไว้

กรณีที่บริษัทมีการนำเทคโนโลยีใดๆ มาใช้เป็นครั้งแรก หรือมีการเปลี่ยนแปลงการใช้เทคโนโลยีที่อาจมีผลกระทบหรือมีความเสี่ยงอย่างมีนัยสำคัญต่อการดำเนินธุรกิจในภาพรวม บริษัทต้องมีข้อกำหนดที่ชัดเจนในการพิจารณาและจัดให้มีการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศหรือพิจารณาประเด็นความเสี่ยงที่เกี่ยวข้อง รวมทั้งผลกระทบที่อาจเกิดขึ้นต่อการดำเนินงานของบริษัทในภาพรวม และดำเนินการให้คณะกรรมการบริษัท หรือคณะกรรมการที่ได้รับมอบหมายพิจารณาอนุมัติแผนงานในการนำเทคโนโลยีสารสนเทศมาใช้หรือการเปลี่ยนแปลงการใช้เทคโนโลยีสารสนเทศ

ข้อ ๑๐ กรอบการบริหารจัดการโครงการด้านเทคโนโลยีสารสนเทศ

บริษัทต้องมีการกำหนดกรอบการบริหารจัดการโครงการที่ชัดเจนเป็นลายลักษณ์อักษร เพื่อเป็นแนวทางในการบริหารจัดการโครงการ โดยอย่างน้อยต้องครอบคลุมในเรื่องดังต่อไปนี้

(๑) การเริ่มโครงการ

(๒) การดำเนินการ

(๓) การควบคุมโครงการ

(๔) การปิดโครงการ

(๕) การสอบทานโครงการ

ข้อ ๑๑ การกำกับดูแลโครงการด้านเทคโนโลยีสารสนเทศ

บริษัทต้องกำหนดโครงสร้างการควบคุมและกำกับดูแลโครงการที่ชัดเจน (Project Governance) โดยควรกำหนดให้มีคณะกรรมการกำกับดูแลโครงการเพื่อกำกับดูแลและติดตามความคืบหน้าการดำเนินงานของโครงการ รวมทั้งให้คำแนะนำ และพิจารณาตัดสินใจการดำเนินงานในโครงการที่สำคัญ เพื่อให้โครงการสามารถดำเนินการได้ตามแผนที่กำหนดไว้

หมวด ๓
การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ
(IT Security)

ข้อ ๑๒ นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security Policy)

บริษัทต้องจัดให้มีนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security Policy) ที่เป็นลายลักษณ์อักษร สอดคล้องกับการนำเทคโนโลยีมาใช้ในการดำเนินธุรกิจ และความเสี่ยงที่อาจเกิดขึ้นจากการใช้เทคโนโลยีนั้น โดยนโยบายต้องได้รับการพิจารณาอนุมัติจากคณะกรรมการบริษัท หรือคณะกรรมการที่ได้รับมอบหมาย มีการทบทวนอย่างน้อยปีละหนึ่งครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ และมีการสื่อสารให้กับบุคลากรของบริษัททั่วทั้งองค์กร โดยนโยบายจะต้องครอบคลุมรายละเอียดอย่างน้อย ดังนี้

๑) การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (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 ๑๓ การบริหารจัดการความมั่นคงปลอดภัยด้านทรัพยากรบุคคล (Human Resource Security)

บริษัทต้องมีการบริหารจัดการบุคลากรที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ โดยต้องจัดให้มีหลักเกณฑ์ในการคัดเลือกเพื่อบรรจุเป็นพนักงาน กฎระเบียบหรือข้อบังคับระหว่างการปฏิบัติงาน และการสิ้นสุดการปฏิบัติงาน

ข้อ ๑๔ การบริหารจัดการทรัพย์สินสารสนเทศ (Asset Management)

บริษัทต้องจัดให้มีการบริหารจัดการทรัพย์สินสารสนเทศ อย่างน้อยในเรื่องดังต่อไปนี้

(๑) ต้องจัดให้มีการจัดทำทะเบียนรายการทรัพย์สินสารสนเทศ โดยต้องมีการบำรุงรักษาทรัพย์สินสารสนเทศอย่างสม่ำเสมอ รวมถึงต้องจัดให้มีมาตรการด้านความมั่นคงปลอดภัยสำหรับการใช้งานเครื่องคอมพิวเตอร์ และอุปกรณ์อื่นๆ ที่เกี่ยวข้อง อาทิ อุปกรณ์ส่วนตัว (Bring-your-own-device: BYOD) ที่เชื่อมต่อกับระบบเครือข่ายของบริษัท อุปกรณ์จัดเก็บข้อมูลแบบพกพา (External Hard Disk/Flash Drive) เป็นต้น

(๒) ต้องจัดให้มีแนวปฏิบัติการจัดชั้นสารสนเทศ (Information Classification) ที่เหมาะสมตามชั้นความลับและความสำคัญของสารสนเทศขององค์กร และมีการกำหนดแนวทางการรักษาความมั่นคงปลอดภัยที่สอดคล้องตามชั้นความลับ ซึ่งรวมถึงการรักษาความมั่นคงปลอดภัยของข้อมูล ระหว่างการรับส่งข้อมูลผ่านเครือข่ายสื่อสาร การจัดเก็บข้อมูลในระบบงานหรือสื่อบันทึกข้อมูลต่างๆ และการทำลายข้อมูลที่เหมาะสมกับชั้นความลับ

ข้อ ๑๕ การควบคุมการเข้าถึงทรัพย์สินสารสนเทศ (Access Control)

บริษัทต้องจัดให้มีการควบคุมการเข้าถึงระบบ ข้อมูล และทรัพย์สินสารสนเทศ เพื่อป้องกันการเข้าถึงและเปลี่ยนแปลงระบบหรือข้อมูลโดยผู้ที่ไม่มีสิทธิหรือไม่ได้รับอนุญาต อย่างน้อยในเรื่องดังต่อไปนี้

(๑) กำหนดนโยบายการเข้าถึงหรือเข้าใช้งานระบบ ข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศ รวมถึงนโยบายการใช้บริการเครือข่ายสื่อสารขององค์กร สอดคล้องตามข้อกำหนดการดำเนินธุรกิจ

(๒) กำหนดให้มีการบริหารจัดการสิทธิการใช้งาน และตรวจสอบยืนยันตัวตนตามสิทธิที่กำหนดไว้ โดยคำนึงถึงความจำเป็นในการใช้งานและระดับความเสี่ยง

(๓) กำหนดให้มีการทบทวนปรับปรุงสิทธิการใช้งาน ตามรอบระยะเวลาที่กำหนด

(๔) กำหนดให้มีการเพิกถอนสิทธิการใช้งานเมื่อมีการเปลี่ยนแปลงหน้าที่งานหรือสิ้นสุดสภาพการเป็นพนักงาน

ข้อ ๑๖ การเข้ารหัสข้อมูล (Cryptography)

บริษัทต้องจัดให้มีแนวปฏิบัติด้านการเข้ารหัสข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลที่เหมาะสมตามชั้นความลับและความสำคัญของข้อมูลสารสนเทศ

ข้อ ๑๗ การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environmental Security)

บริษัทต้องจัดให้มีการรักษาความมั่นคงปลอดภัยของศูนย์คอมพิวเตอร์ สถานที่ปฏิบัติงานที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ และพื้นที่ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศที่สำคัญ อย่างน้อยในเรื่องดังต่อไปนี้

(๑) ต้องจัดให้มีระเบียบปฏิบัติการเข้าถึงศูนย์คอมพิวเตอร์เป็นลายลักษณ์อักษร

(๒) ต้องจัดให้มีการควบคุมการเข้า-ออกศูนย์คอมพิวเตอร์โดยจำกัดสิทธิการเข้าถึงศูนย์คอมพิวเตอร์อย่างเหมาะสม และมีการบันทึกและจัดเก็บข้อมูลการเข้าถึงศูนย์คอมพิวเตอร์ของผู้เยี่ยมชม

(๓) ต้องจัดให้มีระบบการป้องกันและกระบวนการในการบำรุงรักษาอุปกรณ์ คอมพิวเตอร์และระบบสาธารณูปโภค (Facility) ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ อาทิ ระบบไฟฟ้าสำรองสำหรับศูนย์คอมพิวเตอร์ ระบบทำความเย็น ระบบป้องกันหรือสัญญาณเตือนไฟไหม้ และกล้องวงจรปิด เป็นต้น

ข้อ ๑๘ การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร (Network and Communication Security)

บริษัทต้องจัดให้มีการรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสารของบริษัท อย่างน้อยในเรื่องดังต่อไปนี้

(๑) ต้องจัดให้มีการจำแนกโซนเครือข่ายสื่อสาร โดยมีการจัดแบ่งเครือข่ายอย่างเหมาะสม และจัดให้มีการควบคุมการเชื่อมต่อจากระบบงานต่างๆ มายังระบบงานที่มีความสำคัญอย่างเข้มงวด

(๒) ต้องจัดให้มีการควบคุม และจำกัดสิทธิการเข้าถึงระบบเครือข่าย และระบบสารสนเทศจากระยะไกล (Remote Access) โดยมีการควบคุมความปลอดภัยในการเชื่อมต่อระบบเครือข่ายจากภายนอก และต้องได้รับการอนุมัติให้มีการเข้าถึงอย่างเหมาะสม

ข้อ ๑๙ การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT Operations Security)

บริษัทต้องจัดให้มีการรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ เพื่อให้การปฏิบัติงานด้านนี้มีความมั่นคงปลอดภัย โดยครอบคลุมอย่างน้อยในเรื่องดังต่อไปนี้

(๑) การบริหารจัดการการเปลี่ยนแปลง (Change Management)

จัดให้มีกระบวนการในการบริหารจัดการการเปลี่ยนแปลง และมีการอนุมัติการเปลี่ยนแปลงทุกครั้งอย่างเป็นลายลักษณ์อักษร

(๒) การบริหารจัดการขีดความสามารถของระบบ (Capacity Management)

จัดให้มีการบริหารจัดการขีดความสามารถของระบบให้สามารถรองรับการดำเนินธุรกิจในปัจจุบัน และวางแผนการจัดการให้รองรับการใช้งานในอนาคตได้อย่างมีประสิทธิภาพ

(๓) การรักษาความมั่นคงปลอดภัยของเครื่องแม่ข่าย (Server)

จัดให้มีการบริหารจัดการการตั้งค่าระบบ (System Configuration Management) การบริหารจัดการ Patch (Patch Management) การกำหนดสิทธิการเข้าถึงและจำกัดสิทธิการใช้งานของผู้ใช้งานที่มีสิทธิสูง (High Privileged ID)

(๔) การสำรองข้อมูล (Data Backup)

กำหนดวิธีการและกระบวนการที่ใช้สำรองข้อมูล รวมทั้งความถี่ในการสำรองข้อมูลที่เหมาะสมกับลักษณะและความซับซ้อนของการดำเนินงานของบริษัท

(๕) การจัดเก็บข้อมูลบันทึกเหตุการณ์ (Logging)

จัดให้มีการจัดเก็บข้อมูลบันทึกเหตุการณ์ของเครื่องแม่ข่าย ระบบงาน และอุปกรณ์เครือข่ายที่สำคัญ โดยจะต้องมีความมั่นคงปลอดภัยเพียงพอในการป้องกันการเปลี่ยนแปลง แก้ไข หรือทำลาย รวมถึงมีการสอบทาน Log ด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ

(๖) การติดตามดูแลระบบและการเฝ้าระวังภัยคุกคาม (Security Monitoring)

จัดให้มีกระบวนการหรือเครื่องมือในการตรวจจับเหตุการณ์ผิดปกติ หรือภัยคุกคามที่มีผลกระทบต่อความมั่นคงปลอดภัยของระบบที่สำคัญ รวมถึงควรมีการบริหารจัดการช่องโหว่ (Vulnerability Management) ของระบบที่เหมาะสมตามระดับความเสี่ยง และจัดให้มีผู้เชี่ยวชาญจากภายนอกทำหน้าที่ทดสอบเจาะระบบ โดยเฉพาะระบบงาน (Application) และระบบเครือข่าย (Network) ที่มีการเชื่อมต่อกับระบบเครือข่ายสื่อสารสาธารณะ (Internet Facing) อย่างสม่ำเสมอ หรือทุกครั้งที่มีการเปลี่ยนแปลงระบบอย่างมีนัยสำคัญ

ข้อ ๒๐ การจัดหาและการพัฒนาระบบ (System Acquisition and Development)

(๑) การจัดหาระบบ (System Acquisition)

บริษัทต้องกำหนดหลักเกณฑ์ที่ชัดเจนในการประเมินและคัดเลือกผู้ขาย/ผู้รับจ้างพัฒนาระบบ โดยต้องจัดทำสัญญาซื้อขาย/สัญญาจ้าง ที่กำหนดเงื่อนไขในการพัฒนาระบบที่ชัดเจน

(๒) การพัฒนาระบบ (System Development)

บริษัทต้องจัดให้มีการออกแบบ พัฒนา และทดสอบระบบ เพื่อให้มั่นใจว่าระบบ มีความถูกต้อง มั่นคงปลอดภัย เชื่อถือได้ พร้อมใช้งาน โดยบริษัทต้องจัดให้มีอย่างน้อยในเรื่องดังต่อไปนี้

๑) มีการจัดทำเอกสารความต้องการของระบบงาน (Requirement) และเอกสารรายละเอียดคุณสมบัติทางเทคนิค (Technical Specification) โดยครอบคลุมถึงเรื่องการรักษาความมั่นคงปลอดภัย ซึ่งรวมถึงกระบวนการในการทดสอบระบบงาน

๒) มีกระบวนการหรือเครื่องมือในการควบคุมเวอร์ชันของคำสั่งในการเขียนโปรแกรม (Source Code Version Control) โดยจะต้องจำกัดสิทธิผู้ที่จะดำเนินการติดตั้งโปรแกรมในระบบงานที่ให้บริการจริง (Production) เท่าที่จำเป็นเท่านั้น

๓) มีการแบ่งแยกบทบาทหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องในกระบวนการพัฒนาระบบ เช่น การแบ่งแยกระหว่างผู้พัฒนาระบบ (Developer) และผู้บริหารจัดการระบบ (Administrator)

๔) มีการแบ่งแยกสภาพแวดล้อมของระบบงานที่ใช้สำหรับการพัฒนา (Development) และการทดสอบ (Testing) ออกจากระบบงานที่ให้บริการจริง (Production)

๕) มีการทดสอบระบบก่อนการใช้งานจริง เช่น ทดสอบการทำงานของแต่ละระบบ (Unit Test) ทดสอบการทำงานร่วมกันของระบบต่าง ๆ (System Integration Test) ทดสอบความพร้อมใช้งานตามกระบวนการและความต้องการของผู้ใช้งาน (User Acceptance Test) และทดสอบความปลอดภัยของระบบ (Security Test) ตามกระบวนการในการรักษาความมั่นคงปลอดภัยที่กำหนดในเอกสารรายละเอียดคุณสมบัติทางเทคนิค (Technical Specification) รวมถึงต้องควบคุมการรักษาความมั่นคงปลอดภัยและความลับของข้อมูลสำคัญที่นำไปใช้ในการทดสอบ

๖) มีการทดสอบประสิทธิภาพ (Performance Test) สำหรับระบบที่เกี่ยวข้องกับการให้บริการหรือการทำธุรกรรมทางอิเล็กทรอนิกส์

๗) การจัดทำคู่มือและอบรมผู้ใช้งานระบบและผู้ดูแลระบบ

ข้อ ๒๑ การบริหารจัดการผู้ให้บริการภายนอก (Third Party Management)

ในกรณีที่บริษัทมีการจัดจ้างผู้ให้บริการภายนอก หรือมีพันธมิตรทางธุรกิจที่มีการเชื่อมต่อกับระบบเทคโนโลยีสารสนเทศของบริษัท หรือสามารถเข้าถึงข้อมูลสำคัญของบริษัทหรือของลูกค้าของบริษัทได้ บริษัทต้องมีการกำหนดกระบวนการและหลักเกณฑ์ในการประเมินและคัดเลือกผู้ให้บริการภายนอก โดยต้องจัดทำสัญญาจ้างในการให้บริการ และกำหนดเงื่อนไขให้ผู้ให้บริการภายนอกปฏิบัติตามนโยบายการรักษาความปลอดภัยของบริษัท รวมถึงต้องกำหนดข้อตกลงระดับการให้บริการ (Service Level Agreement : SLA) พร้อมทั้งมีการตรวจสอบและติดตามการให้บริการอย่างสม่ำเสมอ

ทั้งนี้ การใช้บริการเทคโนโลยีสารสนเทศจากผู้ให้บริการภายนอก (IT Outsourcing) บริษัทสามารถพิจารณาแนวทางในการดำเนินการตามแนวปฏิบัติของสำนักงานเรื่องหลักเกณฑ์การกำกับดูแลการใช้บริการจากผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศ

ข้อ ๒๒ การบริหารจัดการเหตุการณ์ผิดปกติและปัญหา (IT Incident and Problem Management)

บริษัทต้องจัดให้มีการบริหารจัดการเหตุการณ์ผิดปกติและปัญหาที่เกิดจากการใช้เทคโนโลยีสารสนเทศอย่างเหมาะสมและทันท่วงที โดยต้องจัดให้มีวิธีปฏิบัติ ขั้นตอนปฏิบัติ หรือแผนรองรับ ในการบริหารจัดการเหตุการณ์ผิดปกติและปัญหาที่เกิดจากการใช้เทคโนโลยีสารสนเทศ รวมถึงต้องมีการบันทึก วิเคราะห์ และรายงานเหตุการณ์ผิดปกติและปัญหาและการแก้ไขให้คณะกรรมการ หรือผู้ที่ได้รับมอบหมาย ทราบในระยะเวลาที่เหมาะสม ทั้งนี้ บริษัทต้องมีการวิเคราะห์สาเหตุที่แท้จริง (Root Cause) ของปัญหาเพื่อหาแนวทางแก้ไขจากสาเหตุที่แท้จริงและป้องกันไม่ให้เกิดเหตุการณ์ผิดปกติซ้ำในอนาคต

ข้อ ๒๓ การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT Continuity Planning)

(๑) บริษัทต้องจัดให้มีกระบวนการสำรองข้อมูลที่ครอบคลุมระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบงาน ระบบปฏิบัติการ และฐานข้อมูล เป็นต้น โดยต้องรองรับการกู้คืนข้อมูลตามความเหมาะสมทางธุรกิจ

(๒) บริษัทต้องจัดเก็บข้อมูลสำรองไว้นอกสถานที่อย่างปลอดภัย โดยบริษัทต้องมีการเฝ้าติดตามกระบวนการสำรองข้อมูลที่สำคัญ รวมถึงต้องมีการทดสอบการกู้คืนข้อมูลสำรองและดำเนินการให้ข้อมูลสำรองพร้อมใช้งานอยู่เสมอ

(๓) บริษัทต้องจัดทำแผนการกู้คืนระบบสารสนเทศ (Disaster Recovery Plan) เป็นลายลักษณ์อักษร โดยจะต้องมีการอนุมัติ และสื่อสารให้บุคลากรของบริษัทรับทราบ รวมถึงต้องมีการทบทวนอย่างสม่ำเสมอ หรือเมื่อมีการปรับปรุงแก้ไขที่เป็นสาระสำคัญ

(๔) บริษัทต้องมีการทดสอบแผนการกู้คืนระบบสารสนเทศอย่างน้อยปีละ ๑ ครั้ง และรายงานผลการทดสอบต่อผู้บริหารของบริษัทให้รับทราบ

ข้อ ๒๔ การปฏิบัติตามกฎเกณฑ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Compliance)

บริษัทต้องจัดให้มีการดำเนินการตามกฎเกณฑ์ด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อหลีกเลี่ยงการละเมิดข้อกำหนดที่มีผลบังคับใช้ตามกฎหมายและกฎระเบียบที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศและข้อกำหนดใดๆ ด้านความมั่นคงปลอดภัย โดยครอบคลุมอย่างน้อยในเรื่องดังต่อไปนี้

(๑) ระบุข้อกำหนดที่เกี่ยวข้องตามบทบัญญัติของกฎหมายและกฎระเบียบพร้อมทั้งแนวทางที่บริษัทจะต้องดำเนินการด้านเทคโนโลยีสารสนเทศ ความมั่นคงปลอดภัยสารสนเทศ และความมั่นคงปลอดภัยไซเบอร์ โดยให้มีการทบทวนปรับปรุงข้อมูลให้เป็นปัจจุบัน

(๒) ต้องมีวิธีปฏิบัติที่เหมาะสมสำหรับการดำเนินการ เพื่อปฏิบัติตามข้อกำหนดของกฎหมาย กฎระเบียบ ในส่วนที่เกี่ยวกับสิทธิในทรัพย์สินทางปัญญา และการใช้ซอฟต์แวร์ลิขสิทธิ์

(๓) มีแนวทางดำเนินการในการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (IT Compliance)

หมวด ๔
การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ
(IT Risk Management)

เพื่อให้บริษัทสามารถบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศได้อย่างมีประสิทธิภาพ โดยบริษัทต้องกำหนดนโยบายการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศให้ครอบคลุมเรื่องโครงสร้างองค์กรและบทบาทหน้าที่ของผู้ที่เกี่ยวข้องในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ และต้องนำนโยบายดังกล่าวมาจัดทำแนวปฏิบัติและกระบวนการในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยครอบคลุมอย่างน้อยในเรื่องดังต่อไปนี้

ข้อ ๒๕ การระบุบริบท ขอบเขต และเกณฑ์ความเสี่ยง

บริษัทต้องจัดให้มีกรอบการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ หรือแนวทางการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยครอบคลุมอย่างน้อย ดังนี้

(๑) แนวทางการบริหารจัดการความเสี่ยงในการพิจารณาโอกาสและความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยให้มีการระบุบริบท และขอบเขตในการประเมินความเสี่ยง ครอบคลุมถึงแผนงาน งานประจำ และการนำเทคโนโลยีสารสนเทศมาใช้

(๒) เกณฑ์การบริหารความเสี่ยง ประกอบด้วย เกณฑ์การประเมินความเสี่ยง โดยมีการกำหนดระดับผลกระทบและระดับโอกาสเกิดของเหตุการณ์

(๓) ระดับความเสี่ยงที่ยอมรับได้สำหรับความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Appetite)

(๔) กระบวนการประเมินความเสี่ยง เพื่อใช้ดำเนินการระบุความเสี่ยง วิเคราะห์ความเสี่ยงและประเมินผลความเสี่ยง

(๕) กระบวนการจัดการความเสี่ยง เพื่อใช้พิจารณาทางเลือกและมาตรการในการจัดการความเสี่ยง รวมถึงการจัดทำแผนบริหารจัดการความเสี่ยง

ข้อ ๒๖ การประเมินความเสี่ยง (Risk Assessment)

บริษัทต้องจัดให้มีกระบวนการประเมินความเสี่ยงด้านเทคโนโลยี โดยครอบคลุมดังนี้

(๑) การระบุความเสี่ยง (Risk Identification)

บริษัทต้องระบุถึงความเสี่ยงด้านเทคโนโลยีสารสนเทศ ซึ่งรวมถึงภัยคุกคามทางไซเบอร์และช่องโหว่ที่สำคัญ โดยเหตุการณ์ความเสี่ยงดังกล่าวอาจมีสาเหตุมาจากกระบวนการปฏิบัติงาน ระบบงาน บุคลากร หรือปัจจัยภายนอก ตลอดจนการระบุการควบคุมที่มีอยู่ในปัจจุบันและผู้รับผิดชอบต่อความเสี่ยงหรือเจ้าของความเสี่ยง (Risk Owners)

(๒) การวิเคราะห์ความเสี่ยง (Risk Analysis)

บริษัทต้องมีการวิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยมีการประเมินระดับผลกระทบและระดับโอกาสของเหตุการณ์ความเสี่ยง เพื่อระบุระดับค่าความเสี่ยงของชุดรายการความเสี่ยงในแต่ละเหตุการณ์ความเสี่ยงด้านเทคโนโลยีสารสนเทศ สำหรับจัดลำดับความสำคัญของรายการความเสี่ยง

(๓) การประเมินค่าความเสี่ยง (Risk Evaluation)

บริษัทต้องมีการพิจารณาระดับค่าความเสี่ยงของชุดรายการความเสี่ยง เทียบกับเกณฑ์ระดับความเสี่ยงที่ยอมรับได้ (IT Risk Appetite) เพื่อจัดลำดับความเสี่ยงด้านเทคโนโลยีสารสนเทศแสดงในแผนภาพความเสี่ยง และหาแนวทางในการตอบสนองความเสี่ยงที่เหมาะสม

ข้อ ๒๗ การจัดการความเสี่ยง (Risk Treatment)

บริษัทต้องมีแนวทางในการจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อให้ความเสี่ยงที่เหลืออยู่ (Residual Risk) อยู่ในระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ยอมรับได้ โดยต้องคำนึงถึงความสมดุลระหว่างต้นทุนในการป้องกันความเสี่ยงและผลประโยชน์ที่คาดว่าจะได้รับ นอกจากนี้ บริษัทประกันภัยต้องจัดให้มีการกำหนดดัชนีชี้วัดความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Key Risk Indicators) ที่เกี่ยวข้องกับการดำเนินธุรกิจ ให้สอดคล้องกับความสำคัญของเทคโนโลยีสารสนเทศแต่ละงาน เพื่อใช้ในการติดตามและทบทวนความเสี่ยง

ข้อ ๒๘ การติดตามและทบทวนความเสี่ยง (Risk Monitoring and Review)

บริษัทต้องจัดให้มีกระบวนการที่มีประสิทธิภาพในการติดตามและทบทวนความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อให้อยู่ภายใต้ระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ยอมรับได้ที่กำหนดไว้

ข้อ ๒๙ การรายงานความเสี่ยง (Risk Reporting)

บริษัทต้องมีการรายงานผลการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ และแนวโน้มของความเสี่ยงด้านเทคโนโลยีสารสนเทศที่อาจเกิดขึ้นต่อคณะกรรมการบริษัทหรือคณะกรรมการที่ได้รับมอบหมายในระยะเวลาที่เหมาะสม

หมวด ๕
การปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ
(IT Compliance)

ข้อ ๓๐ การปฏิบัติตามกฎหมายและหลักเกณฑ์

บริษัทต้องจัดให้มีการกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (IT Compliance) เช่น กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ กฎหมายว่าด้วยระบบการชำระเงิน กฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล และไม่ขัดหรือแย้งกับการปฏิบัติตามกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงิน และกฎหมายอื่นในลักษณะเดียวกัน เพื่อป้องกันการละเมิดหรือการไม่ปฏิบัติตามกฎหมายและหลักเกณฑ์ของหน่วยงานกำกับดูแลที่เกี่ยวข้อง

หมวด ๖
การตรวจสอบด้านเทคโนโลยีสารสนเทศ
(IT Audit)

ข้อ ๓๑ บทบาทหน้าที่และแผนงานในการตรวจสอบด้านเทคโนโลยีสารสนเทศ

(๑) บริษัทต้องจัดให้มีผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศที่มีความรู้ ประสบการณ์ และความเชี่ยวชาญเกี่ยวกับการตรวจสอบด้านเทคโนโลยีสารสนเทศ ซึ่งอาจเป็นผู้ตรวจสอบภายใน หรือผู้ตรวจสอบจากภายนอกก็ได้

(๒) บริษัทต้องจัดให้มีแผนงานและขอบเขตการตรวจสอบด้านเทคโนโลยีสารสนเทศที่ครอบคลุมความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัท โดยแผนงานและขอบเขตในการตรวจสอบต้องได้รับความเห็นชอบจากคณะกรรมการตรวจสอบ และต้องจัดให้มีการทบทวนอย่างน้อยปีละหนึ่งครั้ง หรือทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

ข้อ ๓๒ การปฏิบัติงานตรวจสอบด้านเทคโนโลยีสารสนเทศ

(๑) บริษัทต้องจัดให้มีการตรวจสอบด้านเทคโนโลยีสารสนเทศให้เหมาะสมตามแผนงานและขอบเขตที่กำหนด และเมื่อมีเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศที่มีนัยสำคัญ

(๒) ในกรณีที่ระบบเทคโนโลยีของบริษัทมีความซับซ้อนหรือเป็นเทคโนโลยีใหม่ โดยบริษัทมีข้อจำกัดไม่สามารถประเมินหรือตรวจสอบเองได้ บริษัทสามารถจ้างผู้เชี่ยวชาญภายนอกทำหน้าที่ในการตรวจสอบแทนได้

ข้อ ๓๓ การรายงานผลและติดตามผลการตรวจสอบ

(๑) บริษัทต้องจัดทำรายงานผลการตรวจสอบด้านเทคโนโลยีสารสนเทศและเสนอต่อคณะกรรมการตรวจสอบ ตลอดจนจัดเก็บรายงานผลการตรวจสอบดังกล่าวไว้ที่บริษัท พร้อมไว้สำหรับการตรวจสอบหรือเมื่อร้องขอโดยสำนักงาน

(๒) บริษัทต้องจัดให้มีการติดตามประเด็นจากการตรวจสอบด้านเทคโนโลยีสารสนเทศและรายงานประเด็นสำคัญให้กับคณะกรรมการตรวจสอบและฝ่ายงานที่เกี่ยวข้องทราบ

หมวด ๗
การกำกับดูแลและการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์
(Cybersecurity)

บริษัทต้องจัดให้มีแนวทางการกำกับดูแลในการเตรียมความพร้อมรับมือภัยคุกคามทางไซเบอร์ (Cyber Resilience) โดยมีกรอบการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ แนวทางที่ใช้ในการกำกับดูแลและบริหารจัดการความเสี่ยงที่เกี่ยวข้องด้านภัยคุกคามทางไซเบอร์ในภาพรวมขององค์กร ที่สอดคล้องกับกฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์เหมาะสม สอดคล้องกับขนาด และความซับซ้อนของการดำเนินธุรกิจ โดยครอบคลุมในเรื่องดังต่อไปนี้

ข้อ ๓๔ การกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์และการระบุความเสี่ยง (Identification)

(๑) บริษัทต้องมีการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Governance)

(๒) บริษัทต้องจัดทำรายการทรัพย์สินสารสนเทศ การบริหารจัดการทรัพย์สินสารสนเทศ

(๓) บริษัทต้องกำหนดขอบเขตและวิธีการในการประเมินความเสี่ยงด้านไซเบอร์ สอดคล้องตามการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ หรือความมั่นคงปลอดภัยสารสนเทศ

(๔) บริษัทต้องจัดให้มีการจัดทำแผนบริหารจัดการความเสี่ยง มาตรการจัดการความเสี่ยง หรือแนวทางในการดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์ สอดคล้องตามผลการประเมินความเสี่ยงด้านไซเบอร์

(๕) บริษัทต้องมีการบริหารจัดการความเสี่ยงเกี่ยวกับห่วงโซ่ของผู้ให้บริการภายนอก (Supply Chain Risk Management) แนวทางในการบริการจัดการผู้ให้บริการภายนอก การทำสัญญาจ้าง การประเมินความเหมาะสม การติดตามและประเมินผลการปฏิบัติงาน และการสอบทานผลการปฏิบัติงาน

ข้อ ๓๕ การป้องกันความเสี่ยง (Protection)

(๑) บริษัทต้องกำหนดแนวทางการควบคุมและป้องกันความเสี่ยงของโครงสร้างพื้นฐานสำคัญทางสารสนเทศของบริษัท เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย อุปกรณ์ฮาร์ดแวร์ ซอฟแวร์ ข้อมูล และระบบงาน เป็นต้น รวมทั้งการตั้งค่าระบบงาน การเข้าถึงระบบงานและการจัดการสิทธิ์ การรักษาความมั่นคงปลอดภัยของข้อมูล การพัฒนาระบบงานที่มีความปลอดภัยตามขั้นตอนหรือกระบวนการในการพัฒนาระบบงาน (System Development Life Cycle: SDLC) การบริหารจัดการ Patch โดยมีการใช้เทคโนโลยีอย่างเหมาะสม เพื่อให้บริษัทมีกระบวนการ เครื่องมือ และวิธีการในการควบคุมหรือลดผลกระทบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่อาจเกิดขึ้น

(๒) บริษัทต้องมีเอกสารการปฏิบัติงานสำหรับดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์สอดคล้องตามมาตรฐานและแนวปฏิบัติที่ดี

(๓) บริษัทต้องมีแนวทางในการรวบรวมและวิเคราะห์ข้อมูลภัยคุกคามไซเบอร์ ตลอดจนกำหนดวิธีการและช่องทางในการแลกเปลี่ยนข้อมูลและสร้างความร่วมมือในการบริหารจัดการและรับมือภัยคุกคามทางไซเบอร์ทั้งภายในและภายนอกองค์กร

ข้อ ๓๖ การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detection)

(๑) บริษัทต้องจัดให้มีช่องทางในการรายงานช่องโหว่ จุดอ่อน เหตุการณ์ หรือสถานการณ์ที่เกี่ยวข้องด้านความมั่นคงปลอดภัยไซเบอร์ โดยกำหนดขอบเขตหน้าที่ความรับผิดชอบของหน่วยงานที่เกี่ยวข้องทั้งหน่วยงานภายในและหน่วยงานภายนอก

(๒) บริษัทต้องกำหนดแนวทางในการค้นหา ทดสอบ และบริหารจัดการช่องโหว่ทางด้านเทคโนโลยีสารสนเทศ เพื่อให้สามารถตรวจจับ วิเคราะห์ ติดตาม และแจ้งเตือนเหตุการณ์ผิดปกติหรือภัยคุกคามทางไซเบอร์ให้แก่หน่วยงานหรือผู้รับผิดชอบรับทราบ และกำหนดแนวทางในการสื่อสารและการดำเนินการแก้ไขในเบื้องต้นได้อย่างทันการณ์

ข้อ ๓๗ การดำเนินการมาตรการเผชิญเหตุเมื่อตรวจพบภัยคุกคามทางไซเบอร์ (Response)

(๑) บริษัทต้องกำหนดแนวทางในการบริหารจัดการการรับมือเหตุการณ์ผิดปกติหรือภัยคุกคามทางไซเบอร์ เพื่อให้บริษัทสามารถตอบสนองและรับมือกับความเสี่ยงได้อย่างทันการณ์

(๒) บริษัทต้องจัดให้มีการจัดทำ ซักซ้อมหรือทดสอบแผนรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity) แผนฉุกเฉิน การสืบสวนและวิเคราะห์สาเหตุการแก้ปัญหา และจัดทำรายงานเพื่อเสนอต่อคณะกรรมการบริษัท และผู้บริหาร เป็นต้น

(๓) บริษัทต้องกำหนดแนวทางในการสื่อสาร เพื่อดำเนินการแก้ไขเหตุการณ์หรือสถานการณ์จากภัยคุกคามทางไซเบอร์

ข้อ ๓๘ การดำเนินการฟื้นฟูความเสียหายจากภัยคุกคามทางไซเบอร์ (Recovery)

(๑) บริษัทต้องกำหนดแนวทางและมาตรการในการฟื้นฟูความเสียหายจากเหตุการณ์หรือสถานการณ์จากภัยคุกคามทางไซเบอร์ สอดคล้องกับผลการประเมินความเสี่ยงและผลกระทบตามกรอบการดำเนินงานความมั่นคงปลอดภัยไซเบอร์และการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัท

(๒) บริษัทต้องกำหนดแนวทางในการสื่อสาร เพื่อดำเนินการฟื้นฟูความเสียหายจากเหตุการณ์หรือสถานการณ์จากภัยคุกคามทางไซเบอร์

ข้อ ๓๙ การประเมินความเสี่ยงด้านภัยคุกคามทางไซเบอร์

บริษัทต้องมีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์หรือภัยคุกคามทางไซเบอร์ (Cybersecurity Risk Assessment) เพื่อให้ทราบถึงสถานภาพความเสี่ยงด้านภัยคุกคามทางไซเบอร์ของบริษัทตามสภาพปัจจัยความเสี่ยง สถานการณ์ความเสี่ยง ภัยคุกคามหรือช่องโหว่ ที่เกี่ยวข้องในการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยมีข้อพิจารณาปัจจัยความเสี่ยงด้านภัยคุกคามทางไซเบอร์ ดังนี้

(๑) เกณฑ์ในการประเมินและจัดระดับความรุนแรงและผลกระทบของเหตุการณ์หรือสถานการณ์การถูกโจมตีทางไซเบอร์ รวมทั้งโอกาสเกิดของเหตุการณ์ ตลอดจนการประเมินระดับความเสี่ยงด้านภัยคุกคามทางไซเบอร์ โดยเกณฑ์ผลกระทบของเหตุการณ์ ให้พิจารณาครอบคลุมอย่างน้อย ๔ ด้าน ได้แก่ ด้านการรักษาความลับ (Confidentiality) ด้านการรักษาความครบถ้วน (Integrity) ด้านการรักษาสภาพพร้อมใช้ (Availability) และด้านการปฏิบัติตามกฎเกณฑ์ (Law & Regulation Compliance)

(๒) บริษัทต้องจัดให้มีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์หรือภัยคุกคามทางไซเบอร์ และต้องมีการรายงานผลการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ และแนวโน้มของความเสี่ยงด้านเทคโนโลยีสารสนเทศที่อาจเกิดขึ้นต่อคณะกรรมการบริษัท หรือคณะกรรมการที่ได้รับมอบหมายในระยะเวลาที่เหมาะสม

หมวด ๘
การรายงานเหตุการณ์ภัยคุกคามและความเสี่ยงด้านเทคโนโลยีสารสนเทศ
(Reporting)

ข้อ ๔๐ การรายงานเหตุการณ์ภัยคุกคามทางไซเบอร์หรือภัยคุกคามที่มีต่อระบบเทคโนโลยีสารสนเทศ

(๑) บริษัทต้องรายงานต่อสำนักงานในกรณีที่เกิดปัญหาหรือเหตุการณ์ที่มีนัยสำคัญในการใช้เทคโนโลยีสารสนเทศซึ่งส่งผลกระทบต่อการให้บริการ หรือระบบ หรือข้อมูลผู้เอาประกันภัย หรือชื่อเสียงของบริษัท และให้รวมถึงกรณีที่เทคโนโลยีสารสนเทศที่สำคัญของบริษัทถูกโจมตีหรือถูกขู่โจมตีจากภัยคุกคามทางไซเบอร์ และเป็นปัญหาหรือเหตุการณ์ที่บริษัทต้องรายงานต่อผู้บริหารสูงสุดของบริษัททราบ ให้บริษัทรายงานมายังสำนักงานทันทีเมื่อเกิดหรือรับรู้เหตุการณ์นั้น โดยให้แจ้งรายละเอียดและสาเหตุของเหตุการณ์ที่เกิดขึ้นผลกระทบที่คาดว่าจะเกิดขึ้น การดำเนินการแก้ไขปัญหา ผลการแก้ไขปัญหา และระยะเวลาในการแก้ไข และแนวทางป้องกันในอนาคตเพิ่มเติมได้ในภายหลัง

(๒) กรณีที่บริษัทถูกโจมตีจากภัยคุกคามทางไซเบอร์ เป็นปัญหาหรือเหตุการณ์ที่เกี่ยวข้องกับการให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ที่เป็นภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง และภัยคุกคามทางไซเบอร์ในระดับวิกฤติ ต้องแจ้งเหตุการณ์ละเมิดโดยไม่ชักช้าภายในเจ็ดสิบสองชั่วโมง ไปยังสำนักงานหรือหน่วยงานตามที่กฎหมายกำหนด รวมถึงการให้ข้อมูลหรือประสานกับหน่วยงานของรัฐหรือหน่วยงานองค์กรที่แต่งตั้งขึ้นตามกฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ในการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์

แบบฟอร์มรายงานเหตุการณ์ความเสี่ยงด้านเทคโนโลยีสารสนเทศ

แบบฟอร์มรายงานเหตุการณ์ภัยคุกคามและความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัทประกันภัย			
ส่วนที่ ๑ ข้อมูลอ้างอิง			
เลขที่อ้างอิง		วันที่รายงาน	
รหัสสมาชิก		☐ บริษัทประกันวินาศภัย	☐ บริษัทประกันชีวิต
ชื่อบริษัทประกันภัย			
สถานที่ตั้ง			
ชื่อผู้บริหาร (ผู้รับผิดชอบ)		ตำแหน่ง	
ชื่อผู้ติดต่อ/ประสานงาน		โทรศัพท์	
E-mail Address			
ส่วนที่ ๒ ข้อมูลเหตุการณ์			
วัน/เวลาที่เกิดเหตุการณ์			
หน่วยงาน/ระบบที่เกิดเหตุ			
รายละเอียด/สาเหตุของเหตุการณ์			
ส่วนที่ ๓ ข้อมูลการรายงาน			
☐ Report ๑ รายงานทันทีเมื่อเกิดเหตุ	๓.๑.๑) ผลกระทบที่คาดว่าจะเกิดขึ้น		
☐ Report ๒ ระหว่างดำเนินการแก้ไข (รายงานภายใน ๒ วันทำการถัดไป ภายหลังทราบเหตุการณ์และตรวจสอบยืนยันแล้ว)	๓.๒.๑) ผลกระทบที่คาดว่าจะเกิดขึ้นโดยประเมินมูลค่าความเสียหายที่อาจเกิดขึ้นกับผู้เอาประกันภัยและบริษัท		
	๓.๒.๒) การดำเนินการแก้ไขปัญหา	๓.๒.๓) ระยะเวลาในการแก้ไข	
	๓.๒.๔) ความคืบหน้าในการแก้ไขปัญหา		
☐ Report ๓ แก้ไขปัญหาได้และเหตุยุติ (รายงานเมื่อเหตุการณ์ยุติ หรือแก้ไขปัญหาแล้วเสร็จภายใน ๑๕ วัน)	๓.๓.๑) ผลกระทบที่คาดว่าจะเกิดขึ้นโดยประเมินมูลค่าความเสียหายที่อาจเกิดขึ้นกับผู้เอาประกันภัยและบริษัท		
	๓.๓.๒) การดำเนินการแก้ไขปัญหา	๓.๓.๓) ระยะเวลาในการแก้ไข	
	๓.๓.๔) ผลการแก้ไขปัญหา		
	๓.๓.๕) แนวทางป้องกันในอนาคต และการเก็บรวบรวมหลักฐาน เพื่อระบุสาเหตุและแนวทางแก้ไขต่อไป		
ลงชื่อ (ผู้มีอำนาจลงนาม)			
ตำแหน่ง			
วันที่ (วัน/เดือน/ปี พ.ศ.)			

หมายเหตุ		
Report ๑ รายงานโดยไม่ชักช้าเมื่อทราบเหตุการณ์และตรวจสอบยืนยันในเบื้องต้นแล้ว	Report ๒ รายงานภายใน ๒ วันทำการถัดไปภายหลังทราบเหตุการณ์และตรวจสอบยืนยันแล้ว	Report ๓ รายงานเมื่อเหตุการณ์ยุติหรือแก้ไขปัญหาแล้วเสร็จภายใน ๑๕ วัน