ประกาศสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย
เรื่อง หลักเกณฑ์ วิธีการ และเงื่อนไขการขึ้นทะเบียนกิจกรรมทางอิเล็กทรอนิกส์
การขอรับความเห็นชอบการใช้บริการบุคคลภายนอก และการรับรองระบบสารสนเทศ
สำหรับธุรกิจประกันชีวิต
พ.ศ. ๒๕๖๖

อาศัยอำนาจตามความในข้อ ๒๒ และข้อ ๒๓ แห่งประกาศคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง หลักเกณฑ์ วิธีการออก และเสนอขายกรมธรรม์ประกันภัย การให้กู้ยืมเงินตามกรมธรรม์ประกันภัยเป็นประกัน และการชดใช้เงินตามสัญญาประกันชีวิต โดยใช้วิธีการทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๖๖ สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัยจึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง หลักเกณฑ์ วิธีการ และเงื่อนไขการขึ้นทะเบียนกิจกรรมทางอิเล็กทรอนิกส์ การขอรับความเห็นชอบการใช้บริการบุคคลภายนอก และการรับรองระบบสารสนเทศสำหรับธุรกิจประกันชีวิต พ.ศ. ๒๕๖๖”

ข้อ ๒ ให้ยกเลิกประกาศสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง หลักเกณฑ์ วิธีการ และเงื่อนไขการขึ้นทะเบียนกิจกรรมทางอิเล็กทรอนิกส์ การขอรับความเห็นชอบการใช้บริการบุคคลภายนอก และการรับรองระบบสารสนเทศ พ.ศ. ๒๕๖๐

ข้อ ๓ ประกาศนี้ให้ใช้บังคับตั้งแต่วันประกาศเป็นต้นไป

ข้อ ๔ ในประกาศนี้

"บริษัท” หมายความว่า บริษัทที่ได้รับใบอนุญาตประกอบธุรกิจประกันชีวิตตามกฎหมายว่าด้วยการประกันชีวิต และหมายความรวมถึงสาขาของบริษัทประกันชีวิตต่างประเทศที่ได้รับใบอนุญาตประกอบธุรกิจประกันชีวิตในราชอาณาจักรตามกฎหมายว่าด้วยการประกันชีวิต

“นายหน้าประกันชีวิต” หมายความว่า นายหน้าประกันชีวิตตามกฎหมายว่าด้วยการประกันชีวิต ไม่รวมถึงธนาคาร

"ธนาคาร” หมายความว่า ธนาคารที่ได้รับใบอนุญาตเป็นนายหน้าประกันชีวิตตามกฎหมายว่าด้วยการประกันชีวิต

“ผู้ให้บริการซึ่งเป็นบุคคลภายนอก” หมายความว่า ผู้ซึ่งมีระบบสารสนเทศไว้ให้บริการในการเสนอขายกรมธรรม์ประกันภัยผ่านทางอิเล็กทรอนิกส์ (Online) การเสนอขาย

กรมธรรม์ประกันภัยโดยใช้เครื่องมือทางอิเล็กทรอนิกส์ประกอบ การออกกรมธรรม์ประกันภัยโดยใช้วิธีการทางอิเล็กทรอนิกส์ หรือการให้กู้ยืมเงินโดยมีกรมธรรม์ประกันภัยเป็นประกัน และการชดใช้เงินตามสัญญาประกันชีวิตโดยใช้วิธีการทางอิเล็กทรอนิกส์ ตามประกาศคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัยว่าด้วย หลักเกณฑ์ วิธีการออกและเสนอขายกรมธรรม์ประกันภัย การให้กู้ยืมเงินตามกรมธรรม์ประกันภัยเป็นประกัน และการชดใช้เงินตามสัญญาประกันชีวิตโดยใช้วิธีการทางอิเล็กทรอนิกส์

“ผู้ตรวจสอบอิสระ” หมายความว่า ผู้ตรวจสอบภายนอกที่ได้รับประกาศนียบัตร Certified Information System Auditor (CISA), Certified Information Security Manager (CISM), Certified Information System Security Professional (CISSP), ISO ๒๗๐๐๑ Lead Auditor

“ผู้ตรวจสอบภายในองค์กร” หมายความว่า ผู้ตรวจสอบงานด้านเทคโนโลยีสารสนเทศของบริษัท ที่เป็นอิสระจากหน่วยงานที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ ที่ได้รับประกาศนียบัตร Certified Information System Auditor (CISA), Certified Information Security Manager (CISM), Certified Information System Security Professional (CISSP), ISO ๒๗๐๐๑ Lead Auditor

“หน่วยงานรับรองระบบสารสนเทศ” หมายความว่า หน่วยงานที่ทำหน้าที่ตรวจรับรองระบบสารสนเทศตามมาตรฐานด้านความปลอดภัยของข้อมูล ได้แก่ The British Standards Institution (BSI) หรือ Bureau Veritas หรือหน่วยงานอื่นที่ได้รับการขึ้นทะเบียนจากหน่วยรับรองระบบงาน (Accreditation Body) ได้แก่ United Kingdom Accreditation Service (UKAS) ANSI-ASQ National Accreditation Board (ANAB) และสำนักงานมาตรฐาผลิตภัณฑ์อุตสาหกรรม (สมอ.) หรือหน่วยรับรองระบบงานอื่นที่สำนักงานยอมรับ

“สำนักงาน” หมายความว่า สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจ ประกันภัย

ข้อ ๕ ในการตรวจรับรองระบบสารสนเทศโดยผู้ตรวจสอบอิสระหรือผู้ตรวจสอบภายในองค์กร บริษัท นายหน้าประกันชีวิต หรือธนาคาร หรือผู้ให้บริการซึ่งเป็นบุคคลภายนอก แล้วแต่กรณี สามารถใช้การรับรองระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศกับ ISO/IEC ๒๗๐๐๑ (ISMS : Information Security Management system) แทนได้

ข้อ ๖ ให้บริษัทที่ประสงค์จะขอขึ้นทะเบียนยื่นคำขอต่อสำนักงานตามแบบ อช. ๑ ที่แนบท้ายประกาศนี้ พร้อมเอกสารหลักฐานประกอบคำขอ ดังต่อไปนี้เป็นอย่างน้อย

(๑) เอกสารแสดงกิจกรรมและรายละเอียดที่ต้องการใช้วิธีการทางอิเล็กทรอนิกส์

(๒) แผนผัง (Flow chart) และขั้นตอนของกิจกรรมที่ใช้วิธีการทางอิเล็กทรอนิกส์

(๓) เอกสารแสดงระบบสารสนเทศและวิธีการทางอิเล็กทรอนิกส์ที่ใช้เพื่อรองรับกิจกรรมที่ใช้วิธีการทางอิเล็กทรอนิกส์

(๔) หนังสือรับรองการตรวจรับรองการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศในระดับเคร่งครัดสำหรับกิจกรรมตาม (๑) โดยผู้ตรวจสอบอิสระตามหนังสือรับรองตามแบบ อช. ๓ ที่แนบท้ายประกาศนี้ หรือประกาศนียบัตรที่ออกโดยหน่วยงานรับรองระบบสารสนเทศ ทั้งนี้

บริษัทต้องแสดงข้อมูลแก่สำนักงานจนเป็นที่พอใจได้ว่าระบบสารสนเทศที่ได้รับการรับรองตามประกาศนียบัตรดังกล่าว มีความมั่นคงปลอดภัยของระบบสารสนเทศในระดับเคร่งครัดสำหรับกิจกรรมตาม (๑)

(๕) เอกสารแนวทางการประเมินมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับเคร่งครัดตามหลักเกณฑ์ที่กำหนดในเอกสารแนบท้ายประกาศ (กรณีมีการตรวจรับรองจากผู้ตรวจสอบอิสระตามหนังสือรับรองตามแบบ อช. ๓)

ข้อ ๗ ให้นายหน้าประกันชีวิต หรือธนาคารที่ประสงค์จะขอขึ้นทะเบียนกิจกรรมทางอิเล็กทรอนิกส์ ยื่นคำขอต่อสำนักงานตามแบบ อช. ๒ ที่แนบท้ายประกาศนี้ พร้อมเอกสารหลักฐานประกอบคำขอ ดังต่อไปนี้เป็นอย่างน้อย

(๑) เอกสารแสดงกิจกรรมและรายละเอียดที่ต้องการใช้วิธีการทางอิเล็กทรอนิกส์

(๒) แผนผัง (Flow chart) และขั้นตอนของกิจกรรมที่ใช้วิธีการทางอิเล็กทรอนิกส์

(๓) เอกสารแสดงระบบสารสนเทศและวิธีการทางอิเล็กทรอนิกส์ที่ใช้เพื่อรองรับกิจกรรมที่ใช้วิธีการทางอิเล็กทรอนิกส์

(๔) หนังสือรับรองการตรวจรับรองการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของนายหน้าประกันชีวิต หรือธนาคาร ในระดับเคร่งครัดสำหรับกิจกรรมตาม (๑) โดยผู้ตรวจสอบอิสระตามหนังสือรับรองตามแบบ อช. ๓ ที่แนบท้ายประกาศนี้ หรือประกาศนียบัตรที่ออกโดยหน่วยงานรับรองระบบสารสนเทศ ทั้งนี้ นายหน้าประกันชีวิต หรือธนาคาร ต้องแสดงข้อมูลแก่สำนักงานจนเป็นที่พอใจได้ว่าระบบสารสนเทศที่ได้รับการรับรองตามประกาศนียบัตรดังกล่าวมีความมั่นคงปลอดภัยของระบบสารสนเทศในระดับเคร่งครัดสำหรับกิจกรรมตาม (๑)

(๕) เอกสารแนวทางการประเมินมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับเคร่งครัดตามหลักเกณฑ์ที่กำหนดในเอกสารแนบท้ายประกาศ (กรณีมีการตรวจรับรองจากผู้ตรวจสอบอิสระตามหนังสือรับรองตามแบบ อช. ๓)

(๖) หนังสือยินยอมของบริษัทให้เสนอขายกรมธรรม์ประกันภัยผ่านทางอิเล็กทรอนิกส์ (Online)

ข้อ ๘ ในการขอขึ้นทะเบียนและขอรับความเห็นชอบการใช้บริการผู้ให้บริการซึ่งเป็นบุคคลภายนอก ให้บริษัท หรือนายหน้าประกันชีวิต หรือธนาคาร ดำเนินการยื่นคำขอต่อสำนักงานตามแบบ อช. ๔ ที่แนบท้ายประกาศนี้ พร้อมเอกสารหลักฐานประกอบคำขอ ดังต่อไปนี้เป็นอย่างน้อย

(๑) เอกสารแสดงกิจกรรมและรายละเอียดที่ต้องการใช้วิธีการทางอิเล็กทรอนิกส์

(๒) แผนผัง (Flow chart) และขั้นตอนของกิจกรรมที่ใช้วิธีการทางอิเล็กทรอนิกส์

(๓) เอกสารแสดงระบบสารสนเทศและวิธีการทางอิเล็กทรอนิกส์ที่ใช้เพื่อรองรับกิจกรรมที่ใช้วิธีการทางอิเล็กทรอนิกส์

(๔) หนังสือรับรองการตรวจรับรองการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของผู้ให้บริการซึ่งเป็นบุคคลภายนอก และของบริษัท นายหน้าประกันชีวิต หรือธนาคาร ในระดับเคร่งครัดสำหรับกิจกรรมตาม (๑) โดยผู้ตรวจสอบอิสระตามหนังสือรับรองตามแบบ อช. ๓

ที่แนบท้ายประกาศนี้ หรือประกาศนียบัตรที่ออกโดยหน่วยงานรับรองระบบสารสนเทศ ทั้งนี้ บริษัท นายหน้าประกันชีวิต หรือธนาคาร ต้องแสดงข้อมูลแก่สำนักงานจนเป็นที่พอใจได้ว่า ระบบสารสนเทศที่ได้รับการรับรองตามประกาศนียบัตรดังกล่าว มีความมั่นคงปลอดภัยของระบบสารสนเทศในระดับเคร่งครัดสำหรับกิจกรรมตาม (๑)

(๕) ข้อรับรองเกี่ยวกับการกำหนดนโยบาย และวิธีปฏิบัติที่ชัดเจน เช่น ระบบการประเมินความเสี่ยง การบริหารความเสี่ยง ขั้นตอนของการบริการ การควบคุมภายใน การรักษาความปลอดภัย และแผนรองรับกรณีที่ผู้ให้บริการซึ่งเป็นบุคคลภายนอกไม่สามารถให้บริการได้

(๖) สำเนาสัญญาใช้บริการระบบสารสนเทศระหว่างผู้ให้บริการซึ่งเป็นบุคคลภายนอกและบริษัท นายหน้าประกันชีวิต หรือธนาคาร แล้วแต่กรณี ซึ่งครอบคลุมเงื่อนไข ดังต่อไปนี้

(ก) มาตรการรักษาความมั่นคงปลอดภัยเพื่อคุ้มครองข้อมูลส่วนบุคคลให้เป็นไปตาม กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

(ข) การป้องกันการใช้หรือเปิดเผยโดยมิชอบ

(ค) การรายงานถึงความผิดปกติและการรายงานถึงการละเมิดข้อมูลส่วนบุคคล

(ง) ความรับผิดชอบในการจ้างช่วงของผู้ให้บริการซึ่งเป็นบุคคลภายนอก โดยต้องกำหนดความรับผิดชอบของผู้ให้บริการซึ่งเป็นบุคคลภายนอกเสมือนหนึ่งเป็นผู้ดำเนินการเอง หากมีการจ้างช่วงตามสัญญา

(จ) สิทธิการตรวจสอบโดยบริษัทและสำนักงาน

(ฉ) การคืน ทำลาย หรือลบข้อมูลส่วนบุคคล

(ช) ผลของการละเมิดเงื่อนไข

(๗) เอกสารแนวทางการประเมินมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับเคร่งครัดตามหลักเกณฑ์ที่กำหนดในเอกสารแนบท้ายประกาศ (กรณีมีการตรวจรับรองจากผู้ตรวจสอบอิสระตามหนังสือรับรองตามแบบ อช. ๓)

(๘) หนังสือรับรองนิติบุคคลจากกรมพัฒนาธุรกิจการค้ากรณีผู้ให้บริการซึ่งเป็นบุคคลภายนอกเป็นนิติบุคคล

ข้อ ๙ ในกรณีที่บริษัท นายหน้าประกันชีวิต หรือธนาคาร ยื่นคำขอขึ้นทะเบียนกิจกรรมทางอิเล็กทรอนิกส์หรือคำขอรับความเห็นชอบการใช้บริการผู้ให้บริการซึ่งเป็นบุคคลภายนอก พร้อมเอกสารหลักฐานประกอบคำขอไม่ถูกต้องครบถ้วน สำนักงานจะแจ้งให้บริษัท นายหน้าประกันชีวิต หรือธนาคาร ดำเนินการแก้ไข หรือยื่นเอกสารหลักฐานประกอบคำขอเพิ่มเติม ภายในระยะเวลาที่สำนักงานกำหนด

หากไม่ดำเนินการแก้ไข หรือยื่นเอกสารหลักฐานประกอบคำขอเพิ่มเติมให้ถูกต้องครบถ้วนภายในระยะเวลาดังกล่าว โดยปราศจากเหตุอันสมควร สำนักงานมีสิทธิปฏิเสธการพิจารณาคำขอดังกล่าวได้

ข้อ ๑๐ ในการพิจารณาคำขอขึ้นทะเบียนกิจกรรมทางอิเล็กทรอนิกส์ หรือคำขอรับความเห็นชอบการใช้บริการผู้ให้บริการซึ่งเป็นบุคคลภายนอก สำนักงานจะพิจารณาคำขอให้แล้วเสร็จภายในสามสิบวันนับแต่วันที่ได้รับคำขอพร้อมเอกสารประกอบคำขอครบถ้วนแล้ว หรือภายในสามสิบวัน

นับแต่วันที่บริษัทได้นำส่งคำขอและเอกสารประกอบคำขอที่มีการแก้ไขเพิ่มเติม ตามที่สำนักงานได้มีความเห็นหรือข้อสังเกตให้ปรับปรุงแก้ไข เว้นแต่กรณีจำเป็นหรือมีเหตุอันสมควร สำนักงานอาจขยายระยะเวลาออกไปก็ได้ ทั้งนี้ ไม่เกินสองครั้ง และครั้งละไม่เกินสิบห้าวัน และเมื่อได้รับความเห็นชอบแล้ว บริษัท นายหน้าประกันชีวิต หรือธนาคาร แล้วแต่กรณี ต้องดำเนินการให้เป็นไปตามที่ยื่นขอขึ้นทะเบียนหรือขอรับความเห็นชอบไว้ตลอดเวลา

ในกรณีมีการแก้ไขเพิ่มเติม หรือเปลี่ยนแปลงข้อมูลที่เคยได้รับความเห็นชอบให้ดำเนินการดังต่อไปนี้

(๑) หากเป็นกรณีที่ระบบสารสนเทศที่ใช้กับกิจกรรมอยู่นอกเหนือขอบเขตของการตรวจรับรองระบบสารสนเทศเดิมอย่างมีนัยสำคัญ เช่น มีการเปลี่ยนระบบโครงสร้างพื้นฐาน (Infrastructure) ระบบ (System) หรือแพลตฟอร์ม (Platform) หรือผู้ให้บริการซึ่งเป็นบุคคลภายนอก ให้บริษัท นายหน้าประกันชีวิต หรือธนาคาร แล้วแต่กรณี ต้องจัดให้มีการตรวจรับรองระบบสารสนเทศใหม่ โดยผู้ตรวจสอบอิสระ หรือโดยหน่วยงานรับรองระบบสารสนเทศ และยื่นคำขอรับความเห็นชอบแก้ไขเพิ่มเติมหรือเปลี่ยนแปลงข้อมูลตามแบบ ปช. ๑ ปช. ๒ หรือ ปช. ๔ ที่แนบท้ายประกาศนี้ พร้อมเอกสารหลักฐานประกอบคำขอที่มีการแก้ไขเพิ่มเติม หรือเปลี่ยนแปลงข้อมูล ทั้งนี้ หากสำนักงานมิได้แจ้งผลการพิจารณาให้ความเห็นชอบ ไปยังบริษัท นายหน้าประกันชีวิต หรือธนาคาร หรือเรียกให้บริษัท นายหน้าประกันชีวิต หรือธนาคาร มาชี้แจงหรือให้ส่งเอกสารเพิ่มเติมภายในสามสิบวัน นับแต่วันที่สำนักงานได้รับคำขอ หรือภายในสามสิบวันนับแต่วันที่บริษัทได้นำส่งคำขอและเอกสารประกอบคำขอที่มีการแก้ไขเพิ่มเติม ตามที่สำนักงานได้มีความเห็นหรือข้อสังเกตให้ปรับปรุงแก้ไข ให้ถือว่าสำนักงานให้ความเห็นชอบการแก้ไขเพิ่มเติม หรือเปลี่ยนแปลงข้อมูลดังกล่าวแล้ว และให้บริษัท นายหน้าประกันชีวิต หรือธนาคาร สามารถดำเนินการตามที่ยื่นขอรับความเห็นชอบดังกล่าวได้

(๒) ในกรณีบริษัท นายหน้าประกันชีวิต หรือธนาคาร ได้รับการขึ้นทะเบียนกิจกรรมการเสนอขายกรมธรรม์ประกันภัยผ่านทางอิเล็กทรอนิกส์ (Online) แล้ว และมีความประสงค์จะขอเพิ่มเติมผลิตภัณฑ์ประกันภัยประเภทกลุ่ม และประเภทอุตสาหกรรม ที่จะเสนอขายกรมธรรม์ประกันภัยผ่านทางอิเล็กทรอนิกส์ (Online) ให้บริษัท นายหน้าประกันชีวิต หรือธนาคาร ยื่นคำขอขึ้นทะเบียนหรือขอรับความเห็นชอบตามแบบ ปช. ๑ ปช. ๒ หรือ ปช. ๔ ที่แนบท้ายประกาศนี้ พร้อมเอกสารหลักฐานประกอบคำขอต่อสำนักงาน ทั้งนี้ บริษัท หรือนายประกันชีวิต หรือธนาคารจะสามารถดำเนินการตามที่ยื่นขอรับความเห็นชอบดังกล่าวได้ก็ต่อเมื่อได้รับความเห็นชอบจากนายทะเบียนแล้ว

ข้อ ๑๑ ในการเสนอขายกรมธรรม์ประกันภัยผ่านทางอิเล็กทรอนิกส์ (Online) การเสนอขายกรมธรรม์ประกันภัยโดยใช้เครื่องมือทางอิเล็กทรอนิกส์ประกอบ การออกกรมธรรม์ประกันภัยโดยใช้วิธีการทางอิเล็กทรอนิกส์ การให้กู้ยืมเงินโดยมีกรมธรรม์ประกันภัยเป็นประกัน หรือการชดใช้เงินตามสัญญาประกันชีวิตโดยใช้วิธีการทางอิเล็กทรอนิกส์ ให้บริษัท นายหน้าประกันชีวิต หรือธนาคาร แล้วแต่กรณี ต้องจัดให้มีการตรวจรับรองระบบสารสนเทศ ตามหลักเกณฑ์ ดังต่อไปนี้

(๑) จัดให้มีการตรวจรับรองระบบสารสนเทศเป็นประจำทุกปี ซึ่งเป็นการตรวจที่มีระยะเวลาห่างกันไม่เกินหนึ่งปี โดยต้องจัดให้มีการตรวจรับรองระบบสารสนเทศโดยผู้ตรวจสอบอิสระหรือผู้ตรวจสอบภายในองค์กร หรือหน่วยงานรับรองระบบสารสนเทศ

(๒) จัดให้มีการตรวจรับรองระบบสารสนเทศทุกรอบสามปี ซึ่งเป็นการตรวจที่มีระยะเวลาห่างกันไม่เกินสามปี โดยต้องจัดให้มีการตรวจรับรองระบบสารสนเทศโดยผู้ตรวจสอบอิสระหรือหน่วยงานรับรองระบบสารสนเทศ

(๓) ในกรณีที่เป็นการขอขึ้นทะเบียนการทำธุรกรรมอิเล็กทรอนิกส์เป็นครั้งแรก หรือกรณีที่มีการแก้ไขระบบที่ได้มีการขึ้นทะเบียนธุรกรรมอย่างมีนัยสำคัญ หรือกรณีที่มีเหตุจำเป็นอย่างมีนัยสำคัญที่ต้องมีการตรวจรับรองระบบสารสนเทศเพิ่มเติม ต้องจัดให้มีการตรวจรับรองระบบสารสนเทศโดยผู้ตรวจสอบอิสระ หรือหน่วยงานรับรองระบบสารสนเทศ

ทั้งนี้ ให้บริษัท นายหน้าประกันชีวิต หรือธนาคาร แล้วแต่กรณี ส่งผลการตรวจภายในสามสิบวัน นับจากวันที่ได้รับการตรวจรับรองระบบสารสนเทศ และดำเนินการส่งหนังสือรับรองการตรวจรับรองการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศในระดับเคร่งครัด ที่จัดทำโดยผู้ตรวจสอบที่มีการตรวจรับรองระบบตามประเภทของการตรวจสอบในวรรคหนึ่ง ตามหนังสือรับรองตามแบบ อช. ๓ ที่แนบท้ายประกาศนี้ หรือส่งประกาศนียบัตรที่ออกโดยหน่วยงานรับรองระบบสารสนเทศต่อสำนักงาน

ประกาศ ณ วันที่ ๒๐ มิถุนายน พ.ศ. ๒๕๖๖

(นายสุทธิพล ทวีชัยการ)
เลขาธิการ
คณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย

หมายเหตุ :- เพื่อกำหนดหลักเกณฑ์และเงื่อนไขการขึ้นทะเบียน และการขอรับความเห็นชอบการรับรองระบบสารสนเทศ และกำหนดระดับมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ สำหรับการออกกรมธรรม์ประกันภัย การเสนอขายกรมธรรม์ประกันภัย การให้กู้ยืมเงิน และการชดใช้เงินตามสัญญาประกันชีวิต โดยใช้วิธีการทางอิเล็กทรอนิกส์

แบบ อช. ๑

คำขอขึ้นทะเบียนกิจกรรมทางอิเล็กทรอนิกส์และการรับรองระบบสารสนเทศ

(กรณีบริษัทประกันชีวิต)

เขียนที่ .....

วันที่ ..... เดือน..... พ.ศ. .....

๑. บริษัท ..... มีความประสงค์ขอขึ้นทะเบียนกิจกรรมทางอิเล็กทรอนิกส์ เพื่อใช้วิธีการทางอิเล็กทรอนิกส์ในเรื่อง

(....) การเสนอขายกรมธรรม์ประกันภัยผ่านทางอิเล็กทรอนิกส์ (Online)

(....) การเสนอขายกรมธรรม์ประกันภัยโดยใช้เครื่องมือทางอิเล็กทรอนิกส์ประกอบ

(....) การออกกรมธรรม์ประกันภัยโดยใช้วิธีการทางอิเล็กทรอนิกส์

(....) การให้กู้ยืมเงินโดยมีกรมธรรม์ประกันภัยเป็นประกัน และการชดใช้เงินตามสัญญาประกันชีวิตโดยใช้วิธีการทางอิเล็กทรอนิกส์

๒. บริษัทได้มอบหมายให้ นาย/นาง/นางสาว .....เป็นผู้ได้รับมอบหมายให้มีหน้าที่ดูแลรับผิดชอบงานด้านสารสนเทศที่เกี่ยวข้องตามที่ยื่นขอขึ้นทะเบียนหรือขอรับความเห็นชอบในครั้งนี้ ติดต่อ โทร.....Email.....

๓. บริษัทขอรับรองว่าระบบสารสนเทศของบริษัทมีมาตรฐานความมั่นคงและปลอดภัยในระดับเคร่งครัดสำหรับกิจกรรมตามข้อ ๑. โดยได้รับการตรวจสอบและรับรองจากผู้ตรวจสอบอิสระตามหนังสือรับรองตามแบบ อช. ๓ หรือประกาศนียบัตรรับรองระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ISO/IEC ๒๗๐๐๑ (ISMS : Information Security Management system)

๔. บริษัทได้แนบเอกสาร โดยมีรายการดังต่อไปนี้

(....) เอกสารแสดงกิจกรรมและรายละเอียดที่ต้องการใช้วิธีการทางอิเล็กทรอนิกส์ (ตัวอย่างหน้าจอ)

(....) แผนผัง (Flow chart) และขั้นตอนของกิจกรรมที่ใช้วิธีการทางอิเล็กทรอนิกส์

(....) เอกสารแสดงระบบสารสนเทศและวิธีการทางอิเล็กทรอนิกส์ที่ใช้เพื่อรองรับกิจกรรมที่ใช้วิธีการทางอิเล็กทรอนิกส์ (system architecture)

(....) หนังสือรับรองการตรวจรับรองการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศโดยผู้ตรวจสอบอิสระตามแบบ อช. ๓ หรือประกาศนียบัตรที่ออกโดยหน่วยงานรับรองระบบสารสนเทศ (ISO๒๗๐๐๑)

(....) เอกสารแนวทางการประเมินมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับเคร่งครัดตามหลักเกณฑ์ที่กำหนดในเอกสารแนบท้ายประกาศ (กรณีมีการตรวจรับรองจากผู้ตรวจสอบอิสระตามหนังสือรับรองตามแบบ อช. ๓)

บริษัท ..... ขอรับรองว่า ข้อความและข้อมูลในแบบ อช. ๑ นี้ ถูกต้องตรงตามความเป็นจริงทุกประการ

ประทับตรา (ถ้ามี)

ลงชื่อ .....

(.....)

กรรมการผู้มีอำนาจ/

ผู้รับมอบอำนาจของบริษัท

คำขอขึ้นทะเบียนกิจกรรมทางอิเล็กทรอนิกส์และการรับรองระบบสารสนเทศ

(กรณีนายหน้าประกันชีวิตหรือธนาคาร)

เขียนที่ .....

วันที่ ..... เดือน..... พ.ศ. .....

๑. ข้าพเจ้า .....ซึ่งมีใบอนุญาตเป็นนายหน้าประกันชีวิตเลขที่ ..... ใบอนุญาตหมดอายุ..... มีความประสงค์ขอขึ้นทะเบียนกิจกรรมทางอิเล็กทรอนิกส์ เพื่อใช้วิธีการทางอิเล็กทรอนิกส์ในเรื่อง

(....) การเสนอขายกรมธรรม์ประกันภัยผ่านทางอิเล็กทรอนิกส์ (Online) ซึ่งได้รับความยินยอมจากบริษัท..... ในการทำกิจกรรม

(....) การเสนอขายกรมธรรม์ประกันภัยโดยใช้เครื่องมือทางอิเล็กทรอนิกส์ประกอบ

๒. ข้าพเจ้าได้มอบหมายให้ นาย/นาง/นางสาว .....เป็นผู้ได้รับมอบหมายให้มีหน้าที่ดูแลรับผิดชอบงานด้านสารสนเทศที่เกี่ยวข้องตามที่ยื่นขอขึ้นทะเบียนหรือขอรับความเห็นชอบในครั้งนี้ ติดต่อ โทร.....Email.....

๓. ข้าพเจ้าขอรับรองว่าระบบสารสนเทศของข้าพเจ้ามีมาตรฐานความมั่นคงและปลอดภัยในระดับเคร่งครัดสำหรับกิจกรรมตามข้อ ๑. ตามหลักเกณฑ์ที่กำหนดในเอกสารแนบท้ายประกาศนี้ โดยได้รับการตรวจสอบและรับรองจากผู้ตรวจสอบอิสระตามหนังสือรับรองตามแบบ อช. ๓ หรือประกาศนียบัตรรับรองระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ISO/IEC ๒๗๐๐๑ (ISMS : Information Security Management system)

๔. ข้าพเจ้าได้แนบเอกสาร โดยมีรายการดังต่อไปนี้

(....) เอกสารแสดงกิจกรรมและรายละเอียดที่ต้องการใช้วิธีการทางอิเล็กทรอนิกส์ (ตัวอย่างหน้าจอ)

(....) แผนผัง (Flow chart) และขั้นตอนของกิจกรรมที่ใช้วิธีการทางอิเล็กทรอนิกส์

(....) เอกสารแสดงระบบสารสนเทศและวิธีการทางอิเล็กทรอนิกส์ที่ใช้เพื่อรองรับกิจกรรมที่ใช้วิธีการทางอิเล็กทรอนิกส์ (system architecture)

(....) หนังสือรับรองการตรวจรับรองการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของข้าพเจ้าโดยผู้ตรวจสอบอิสระตามแบบ อช. ๓ หรือประกาศนียบัตรที่ออกโดยหน่วยงานรับรองระบบสารสนเทศ (ISO๒๗๐๐๑)

(....) เอกสารแนวทางการประเมินมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับเคร่งครัดตามหลักเกณฑ์ที่กำหนดในเอกสารแนบท้ายประกาศ (กรณีมีการตรวจรับรองจากผู้ตรวจสอบอิสระตามหนังสือรับรองตามแบบ อช. ๓)

(....) หนังสือยินยอมของบริษัทให้เสนอขายกรมธรรม์ประกันภัยผ่านทางอิเล็กทรอนิกส์ (Online)

ข้าพเจ้า..... ขอรับรองว่าข้อความและข้อมูลในแบบ อช. ๒ นี้ ถูกต้องตรงตามความเป็นจริงทุกประการ

ประทับตรา (ถ้ามี)

ลงชื่อ .....

(.....)

กรรมการผู้มีอำนาจ/

ผู้รับมอบอำนาจของนายหน้าประกันชีวิตหรือธนาคาร

หนังสือรับรอง

การตรวจรับรองการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศโดยผู้ตรวจสอบอิสระ

เขียนที่ .....

วันที่ ..... เดือน..... พ.ศ. .....

๑. (....) ข้าพเจ้า .....ได้รับประกาศนียบัตรหลักสูตร ..... (CISA, CISM , CISSP แล้วแต่กรณี)..... ประกาศนียบัตรหมดอายุ.....และได้แนบสำเนาประกาศนียบัตรมาพร้อมนี้ (กรณีบุคคลธรรมดา)

(....) หน่วยงานรับรองระบบสารสนเทศ (ชื่อ).....เป็นหน่วยงานรับรองระบบสารสนเทศ ที่ไม่อยู่ระหว่างการถูกระงับหรือเพิกถอนการขึ้นทะเบียน และได้รับการขึ้นทะเบียนจากหน่วยงาน..... และได้แนบสำเนาเอกสารการขึ้นทะเบียนมาด้วยพร้อมกันนี้

๒. ข้าพเจ้าขอรับรองว่าได้ตรวจสอบระบบสารสนเทศของ

(....) บริษัท .....

(....) นายหน้าประกันชีวิตหรือธนาคาร.....

(....) ผู้ให้บริการซึ่งเป็นบุคคลภายนอก.....

เพื่อใช้วิธีการทางอิเล็กทรอนิกส์ในเรื่อง

(....) การเสนอขายกรมธรรม์ประกันภัยผ่านทางอิเล็กทรอนิกส์ (Online)

(....) การเสนอขายกรมธรรม์ประกันภัยโดยใช้เครื่องมือทางอิเล็กทรอนิกส์ประกอบ

(....) การออกกรมธรรม์ประกันภัยโดยใช้วิธีการทางอิเล็กทรอนิกส์

(....) การให้กู้ยืมเงินโดยมีกรมธรรม์ประกันภัยเป็นประกัน และการชดใช้เงินตามสัญญาประกันชีวิตโดยใช้วิธีการทางอิเล็กทรอนิกส์

มีมาตรฐานความมั่นคงและปลอดภัยตามแนวทางการประเมินมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับเคร่งครัดที่แนบท้ายประกาศนี้

๓. ข้าพเจ้าได้ตรวจสอบระบบสารสนเทศเป็นที่เรียบร้อยแล้วตามหลักวิชาชีพและตามมาตรฐานที่อ้างอิงตามประกาศสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง หลักเกณฑ์ วิธีการ และเงื่อนไขการขึ้นทะเบียนกิจกรรมทางอิเล็กทรอนิกส์ การขอรับความเห็นชอบการใช้บริการบุคคลภายนอก และการรับรองระบบสารสนเทศ พ.ศ. ๒๕๖๕ และยินยอมให้สำนักงานสามารถตรวจสอบความถูกต้องของข้อมูลประกาศนียบัตรกับหน่วยงานออกประกาศนียบัตรหรือเอกสารการขึ้นทะเบียนหน่วยงานรับรองระบบสารสนเทศกับหน่วยงานขึ้นทะเบียนตามข้อ ๑. ได้ ข้าพเจ้าจึงลงลายมือชื่อไว้เป็นหลักฐาน

ประทับตรา (ถ้ามี)

ลงชื่อ .....

(.....)

ผู้ตรวจสอบอิสระ/หน่วยงานรับรองระบบสารสนเทศ

๔. ข้าพเจ้าซึ่งเป็นบุคคลตามข้อ ๒. ขอรับรองว่าข้อมูลที่ได้ให้แก่ผู้ตรวจสอบอิสระเพื่อใช้ตรวจรับรองการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศเป็นข้อมูลที่ถูกต้องตรงตามความเป็นจริงทุกประการ จึงได้ลงลายมือชื่อไว้เป็นหลักฐาน

ประทับตรา (ถ้ามี)

ลงชื่อ .....

(.....)

กรรมการผู้มีอำนาจ/ผู้รับมอบอำนาจ*

*กรรมการผู้มีอำนาจ/ผู้รับมอบอำนาจของบริษัท/นายหน้าประกันชีวิตหรือธนาคาร หรือผู้ให้บริการซึ่งเป็นบุคคลภายนอก แล้วแต่กรณี

คำขอรับความเห็นชอบการใช้บริการบุคคลภายนอก และการรับรองระบบสารสนเทศ

ส่วนที่ ๑ กรณีบริษัทใช้บริการบุคคลภายนอก

๑. บริษัท .....

มีความประสงค์ขอขึ้นทะเบียนกิจกรรมทางอิเล็กทรอนิกส์และขอรับความเห็นชอบในการใช้บริการระบบสารสนเทศของผู้ให้บริการซึ่งเป็นบุคคลภายนอก.....(ระบุชื่อผู้ให้บริการ)..... เพื่อใช้วิธีการทางอิเล็กทรอนิกส์ในเรื่อง

(....) การเสนอขายกรมธรรม์ประกันภัยผ่านทางอิเล็กทรอนิกส์ (Online)

(....) การเสนอขายกรมธรรม์ประกันภัยโดยใช้เครื่องมือทางอิเล็กทรอนิกส์ประกอบ

(....) การออกกรมธรรม์ประกันภัยโดยใช้วิธีการทางอิเล็กทรอนิกส์

(....) การให้กู้ยืมเงินโดยมีกรมธรรม์ประกันภัยเป็นประกัน และการชดใช้เงินตามสัญญาประกันชีวิตโดยใช้วิธีการทางอิเล็กทรอนิกส์

๒. บริษัทขอรับรองว่า

๒.๑ ผู้ให้บริการซึ่งเป็นบุคคลภายนอกมีระบบสารสนเทศที่มีมาตรฐานความมั่นคงและปลอดภัยในระดับเคร่งครัดสำหรับกิจกรรมตามข้อ ๑. ตามหลักเกณฑ์ที่กำหนดในเอกสารแนบท้ายประกาศนี้ โดยได้รับการตรวจสอบและรับรองจากผู้ตรวจสอบอิสระตามหนังสือรับรองตามแบบ อช. ๓ หรือประกาศนียบัตรรับรองระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ISO/IEC ๒๗๐๐๑ (ISMS : Information Security Management system) และ

บริษัทมีระบบสารสนเทศที่มีมาตรฐานความมั่นคงและปลอดภัยในระดับเคร่งครัดสำหรับกิจกรรมตามข้อ ๑. ตามหลักเกณฑ์ที่กำหนดในเอกสารแนบท้ายประกาศนี้ โดยได้รับการตรวจสอบและรับรองจากผู้ตรวจสอบอิสระตามหนังสือรับรองตามแบบ อช. ๓ หรือประกาศนียบัตรรับรองระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ISO/IEC ๒๗๐๐๑ (ISMS : Information Security Management system)

๒.๒ ได้กำหนดนโยบาย กระบวนการและวิธีปฏิบัติที่ชัดเจน เช่น ระบบการประเมินความเสี่ยง การบริหารความเสี่ยง ขั้นตอนของการบริการ การควบคุมภายใน การรักษาความปลอดภัย และแผนรองรับกรณีที่บุคคลภายนอกไม่สามารถให้บริการได้

๒.๓ สัญญาใช้บริการระบบสารสนเทศระหว่างบริษัทกับผู้ให้บริการซึ่งเป็นบุคคลภายนอกครอบคลุมเงื่อนไข ดังต่อไปนี้

(ก) มาตรการรักษาความมั่นคงปลอดภัยเพื่อคุ้มครองข้อมูลส่วนบุคคล ให้เป็นไปตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

(ข) การป้องกันการใช้หรือเปิดเผยโดยมิชอบ

(ค) การรายงานถึงความผิดปกติและการรายงานถึงการละเมิดข้อมูลส่วนบุคคล

(ง) ความรับผิดในการจ้างช่วงของผู้ให้บริการภายนอก โดยต้องกำหนดความรับผิดชอบของผู้ให้บริการบุคคลภายนอกเสมือนหนึ่งเป็นผู้ดำเนินการเอง หากมีการจ้างช่วงตามสัญญา

(จ) สิทธิการตรวจสอบโดยบริษัทและสำนักงาน

(ฉ) การคืน ทำลาย หรือลบข้อมูลส่วนบุคคล

(ช) ผลของการละเมิดเงื่อนไข

๓. บริษัทได้แนบเอกสาร โดยมีรายการดังต่อไปนี้

(....) หนังสือรับรองนิติบุคคลจากกรมพัฒนาธุรกิจการค้ากรณีผู้ให้บริการซึ่งเป็นบุคคลภายนอกเป็นนิติบุคคล

(....) เอกสารแสดงกิจกรรมและรายละเอียดที่ต้องการใช้วิธีการทางอิเล็กทรอนิกส์ (ตัวอย่างหน้าจอ)

(....) แผนผัง (Flow chart) และขั้นตอนของกิจกรรมที่ใช้วิธีการทางอิเล็กทรอนิกส์

(....) เอกสารแสดงระบบสารสนเทศและวิธีการทางอิเล็กทรอนิกส์ที่ใช้เพื่อรองรับกิจกรรมที่ใช้วิธีการทางอิเล็กทรอนิกส์ (system architecture)

(....) หนังสือรับรองการตรวจรับรองการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของผู้ให้บริการซึ่งเป็นบุคคลภายนอกโดยผู้ตรวจสอบอิสระตามแบบ อช. ๓ หรือประกาศนียบัตรที่ออกโดยหน่วยงานรับรองระบบสารสนเทศ (ISO๒๗๐๐๑)

(....) หนังสือรับรองการตรวจรับรองการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของบริษัทโดยผู้ตรวจสอบอิสระตามแบบ อช. ๓ หรือประกาศนียบัตรที่ออกโดยหน่วยงานรับรองระบบสารสนเทศ (ISO๒๗๐๐๑)

(....) เอกสารแนวทางการประเมินมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับเคร่งครัดตามหลักเกณฑ์ที่กำหนดในเอกสารแนบท้ายประกาศ (กรณีมีการตรวจรับรองจากผู้ตรวจสอบอิสระตามหนังสือรับรองตามแบบ อช. ๓)

(....) สำเนาสัญญาใช้บริการระบบสารสนเทศระหว่างบริษัทกับผู้ให้บริการซึ่งเป็นบุคคลภายนอก

ส่วนที่ ๒ กรณีนายหน้าประกันชีวิตหรือธนาคารใช้บริการบุคคลภายนอก

๔. ข้าพเจ้า .....ซึ่งมีใบอนุญาตเป็นนายหน้าประกันชีวิต เลขที่ ..... ใบอนุญาตหมดอายุ.....มีความประสงค์ขอขึ้นทะเบียนกิจกรรมทางอิเล็กทรอนิกส์และขอรับความเห็นชอบในการใช้บริการระบบสารสนเทศของผู้ให้บริการซึ่งเป็นบุคคลภายนอก.....(ระบุชื่อผู้ให้บริการ).....เพื่อใช้วิธีการทางอิเล็กทรอนิกส์ในเรื่อง

(....) การเสนอขายกรมธรรม์ประกันภัยผ่านทางอิเล็กทรอนิกส์ (Online) ซึ่งได้รับความยินยอมจากบริษัท..... ในการทำกิจกรรม

(....) การเสนอขายกรมธรรม์ประกันภัยโดยใช้เครื่องมือทางอิเล็กทรอนิกส์ประกอบและได้รับความยินยอมจากบริษัท..... ในกิจกรรมข้างต้น

๕. ข้าพเจ้าขอรับรองว่า

๕.๑ ระบบสารสนเทศของผู้ให้บริการซึ่งเป็นบุคคลภายนอกมีมาตรฐานความมั่นคงและปลอดภัยในระดับเคร่งครัดสำหรับกิจกรรมตามข้อ ๔. ตามหลักเกณฑ์ที่กำหนดในเอกสารแนบท้ายประกาศนี้ โดยได้รับการตรวจสอบและรับรองจากผู้ตรวจสอบอิสระตามหนังสือรับรองตามแบบ อช. ๓ หรือประกาศนียบัตรรับรองระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ISO/IEC ๒๗๐๐๑ (ISMS : Information Security Management system) และ

ข้าพเจ้ามีระบบสารสนเทศที่มีมาตรฐานความมั่นคงและปลอดภัยในระดับเคร่งครัดสำหรับกิจกรรมตามข้อ ๔. ตามหลักเกณฑ์ที่กำหนดในเอกสารแนบท้ายประกาศนี้ โดยได้รับการตรวจสอบและรับรองจากผู้ตรวจสอบอิสระตามหนังสือรับรองตามแบบ อช. ๓ หรือประกาศนียบัตรรับรองระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ISO/IEC ๒๗๐๐๑ (ISMS : Information Security Management system)

๕.๒ ได้กำหนดนโยบาย กระบวนการและวิธีปฏิบัติที่ชัดเจน เช่น ระบบการประเมินความเสี่ยง การบริหารความเสี่ยง ขั้นตอนของการบริการ การควบคุมภายใน การรักษาความปลอดภัย และแผนรองรับกรณีที่บุคคลภายนอกไม่สามารถให้บริการได้

๕.๓ สัญญาใช้บริการระบบสารสนเทศระหว่างข้าพเจ้ากับผู้ให้บริการซึ่งเป็นบุคคลภายนอกครอบคลุมเงื่อนไข ดังต่อไปนี้

(ก) มาตรการรักษาความมั่นคงปลอดภัยเพื่อคุ้มครองข้อมูลส่วนบุคคล ให้เป็นไปตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

(ข) การป้องกันการใช้หรือเปิดเผยโดยมิชอบ

(ค) การรายงานถึงความผิดปกติและการรายงานถึงการละเมิดข้อมูลส่วนบุคคล

(ง) ความรับผิดในการจ้างช่วงของผู้ให้บริการภายนอก โดยต้องกำหนดความรับผิดชอบของผู้ให้บริการบุคคลภายนอกเสมือนหนึ่งเป็นผู้ดำเนินการเอง หากมีการจ้างช่วงตามสัญญา

(จ) สิทธิการตรวจสอบโดยบริษัทและสำนักงาน

(ฉ) การคืน ทำลาย หรือลบข้อมูลส่วนบุคคล

(ช) ผลของการละเมิดเงื่อนไข

๖. ข้าพเจ้าได้แนบเอกสาร โดยมีรายการดังต่อไปนี้

(....) หนังสือรับรองนิติบุคคลจากกรมพัฒนาธุรกิจการค้ากรณีผู้ให้บริการซึ่งเป็นบุคคลภายนอกเป็นนิติบุคคล

(....) เอกสารแสดงกิจกรรมและรายละเอียดที่ต้องการใช้วิธีการทางอิเล็กทรอนิกส์ (ตัวอย่างหน้าจอ)

(....) แผนผัง (Flow chart) และขั้นตอนของกิจกรรมที่ใช้วิธีการทางอิเล็กทรอนิกส์

(....) เอกสารแสดงระบบสารสนเทศและวิธีการทางอิเล็กทรอนิกส์ที่ใช้เพื่อรองรับกิจกรรมที่ใช้วิธีการทางอิเล็กทรอนิกส์ (system architecture)

(....) หนังสือรับรองการตรวจรับรองการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของผู้ให้บริการซึ่งเป็นบุคคลภายนอกโดยผู้ตรวจสอบอิสระตามแบบ อช. ๓ หรือตามประกาศนียบัตรที่ออกโดยหน่วยงานรับรองระบบสารสนเทศ (ISO๒๗๐๐๑)

(....) หนังสือรับรองการตรวจรับรองการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของข้าพเจ้าโดยผู้ตรวจสอบอิสระตามแบบ อช. ๓ หรือตามประกาศนียบัตรที่ออกโดยหน่วยงานรับรองระบบสารสนเทศ (ISO๒๗๐๐๑)

(....) เอกสารแนวทางการประเมินมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับเคร่งครัดตามหลักเกณฑ์ที่กำหนดในเอกสารแนบท้ายประกาศ (กรณีมีการตรวจรับรองจากผู้ตรวจสอบอิสระตามหนังสือรับรองตามแบบ อช. ๓)

(....) สำเนาสัญญาใช้บริการระบบสารสนเทศระหว่างข้าพเจ้ากับผู้ให้บริการซึ่งเป็นบุคคลภายนอก

(....) หนังสือยินยอมของบริษัทให้เสนอขายกรมธรรม์ประกันภัยผ่านทางอิเล็กทรอนิกส์ (Online)

☐ บริษัท ☐ นายหน้าประกันชีวิตหรือธนาคาร .....

ขอรับรองว่า ข้อความและข้อมูลในแบบ อช. ๔ นี้ ถูกต้องตรงตามความเป็นจริงทุกประการ

ประทับตรา (ถ้ามี) ลงชื่อ .....

(.....)

กรรมการผู้มีอำนาจ/ผู้รับมอบอำนาจ*

*กรรมการผู้มีอำนาจ/ผู้รับมอบอำนาจของบริษัท/นายหน้าประกันชีวิตหรือธนาคาร แล้วแต่กรณี

แบบการแจ้งเปลี่ยนแปลงและการรับรองระบบสารสนเทศ
(กรณีบริษัทประกันชีวิต)

เขียนที่ .....
วันที่ ..... เดือน..... พ.ศ. .....

๑. บริษัท ..... มีความประสงค์แจ้งเปลี่ยนแปลงการขึ้นทะเบียนกิจกรรมทางอิเล็กทรอนิกส์ ในเรื่อง

(....) การเสนอขายกรมธรรม์ประกันภัยผ่านทางอิเล็กทรอนิกส์ (Online)

(....) การเสนอขายกรมธรรม์ประกันภัยโดยใช้เครื่องมือทางอิเล็กทรอนิกส์ประกอบ

(....) การออกกรมธรรม์ประกันภัยโดยใช้วิธีการทางอิเล็กทรอนิกส์

(....) การให้กู้ยืมเงินโดยมีกรมธรรม์ประกันภัยเป็นประกัน และการชดใช้เงินตามสัญญาประกันชีวิตโดยใช้วิธีการทางอิเล็กทรอนิกส์

รายละเอียดที่เปลี่ยนแปลง.....
.....

๒. บริษัทได้มอบหมายให้ นาย/นาง/นางสาว .....เป็นผู้ได้รับมอบหมายให้มีหน้าที่ดูแลรับผิดชอบงานด้านสารสนเทศที่เกี่ยวข้องตามที่ยื่นขอขึ้นทะเบียนหรือขอรับความเห็นชอบในครั้งนี้ ติดต่อ โทร.....Email.....

๓. บริษัทขอรับรองว่าระบบสารสนเทศของบริษัทมีมาตรฐานความมั่นคงและปลอดภัยในระดับเคร่งครัดสำหรับกิจกรรมตามข้อ ๑. โดยได้รับการตรวจสอบและรับรองจากผู้ตรวจสอบอิสระตามหนังสือรับรองตามแบบ อช. ๓ หรือตามประกาศนียบัตรที่ออกโดยหน่วยงานรับรองระบบสารสนเทศ (ISO๒๗๐๐๑)

๔. บริษัทได้แนบเอกสาร โดยมีรายการดังต่อไปนี้ (เฉพาะที่มีการแก้ไข)

(....) เอกสารแสดงกิจกรรมและรายละเอียดที่ต้องการใช้วิธีการทางอิเล็กทรอนิกส์ (ตัวอย่างหน้าจอ)

(....) แผนผัง (Flow chart) และขั้นตอนของกิจกรรมที่ใช้วิธีการทางอิเล็กทรอนิกส์

(....) เอกสารแสดงระบบสารสนเทศและวิธีการทางอิเล็กทรอนิกส์ที่ใช้เพื่อรองรับกิจกรรมที่ใช้วิธีการทางอิเล็กทรอนิกส์ (system architecture)

(....) หนังสือรับรองการตรวจรับรองการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศโดยผู้ตรวจสอบอิสระตามแบบ อช. ๓ หรือประกาศนียบัตรที่ออกโดยหน่วยงานรับรองระบบสารสนเทศ (ISO๒๗๐๐๑)

(....) เอกสารแนวทางการประเมินมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับเคร่งครัดตามหลักเกณฑ์ที่กำหนดในเอกสารแนบท้ายประกาศ (กรณีมีการตรวจรับรองจากผู้ตรวจสอบอิสระตามหนังสือรับรองตามแบบ อช. ๓)

บริษัท ..... ขอรับรองว่า ข้อความและข้อมูลในแบบ ปช. ๑ นี้ ถูกต้องตรงตามความเป็นจริงทุกประการ

ประทับตรา (ถ้ามี)

ลงชื่อ .....
(.....)
กรรมการผู้มีอำนาจ/
ผู้รับมอบอำนาจของบริษัท

แบบการแจ้งเปลี่ยนแปลงและการรับรองระบบสารสนเทศ
(กรณีนายหน้าประกันชีวิตหรือธนาคาร)

เขียนที่ .....
วันที่ ..... เดือน..... พ.ศ. .....

๑. ข้าพเจ้า .....ซึ่งมีใบอนุญาตเป็นนายหน้าประกันชีวิต เลขที่ ..... ใบอนุญาตหมดอายุ..... มีความประสงค์แจ้งเปลี่ยนแปลงการขึ้นทะเบียนกิจกรรมทางอิเล็กทรอนิกส์ ในเรื่อง

(....) การเสนอขายกรมธรรม์ประกันภัยผ่านทางอิเล็กทรอนิกส์ (Online) ซึ่งได้รับความยินยอมจากบริษัท..... ในการทำกิจกรรม

(....) การเสนอขายกรมธรรม์ประกันภัยโดยใช้เครื่องมือทางอิเล็กทรอนิกส์ประกอบ
รายละเอียดที่เปลี่ยนแปลง.....
.....

๒. ข้าพเจ้าได้มอบหมายให้ นาย/นาง/นางสาว ..... เป็นผู้ได้รับมอบหมายให้มีหน้าที่ดูแลรับผิดชอบงานด้านสารสนเทศที่เกี่ยวข้องตามที่แจ้งเปลี่ยนแปลงการขึ้นทะเบียนหรือขอรับความเห็นชอบในครั้งนี้ ติดต่อ โทร.....Email.....

๓. ข้าพเจ้าขอรับรองว่าระบบสารสนเทศของข้าพเจ้ามีมาตรฐานความมั่นคงและปลอดภัยในระดับเคร่งครัดสำหรับกิจกรรมตามข้อ ๑. ตามหลักเกณฑ์ที่กำหนดในเอกสารแนบท้ายประกาศนี้ โดยได้รับการตรวจสอบและรับรองจากผู้ตรวจสอบอิสระตามหนังสือรับรองตามแบบ อช. ๓ หรือตามประกาศนียบัตรที่ออกโดยหน่วยงานรับรองระบบสารสนเทศ (ISO๒๗๐๐๑)

๔. ข้าพเจ้าได้แนบเอกสาร โดยมีรายการดังต่อไปนี้ (เฉพาะที่แก้ไข)

(....) เอกสารแสดงกิจกรรมและรายละเอียดที่ต้องการใช้วิธีการทางอิเล็กทรอนิกส์ (ตัวอย่างหน้าจอ)

(....) แผนผัง (Flow chart) และขั้นตอนของกิจกรรมที่ใช้วิธีการทางอิเล็กทรอนิกส์

(....) เอกสารแสดงระบบสารสนเทศและวิธีการทางอิเล็กทรอนิกส์ที่ใช้เพื่อรองรับกิจกรรมที่ใช้วิธีการทางอิเล็กทรอนิกส์ (system architecture)

(....) หนังสือรับรองการตรวจรับรองการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของข้าพเจ้าโดยผู้ตรวจสอบอิสระตามแบบ อช. ๓ หรือประกาศนียบัตรที่ออกโดยหน่วยงานรับรองระบบสารสนเทศ (ISO๒๗๐๐๑)

(....) เอกสารแนวทางการประเมินมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับเคร่งครัดตามหลักเกณฑ์ที่กำหนดในเอกสารแนบท้ายประกาศ (กรณีมีการตรวจรับรองจากผู้ตรวจสอบอิสระตามหนังสือรับรองตามแบบ อช. ๓)

(....) หนังสือยินยอมของบริษัทให้เสนอขายกรมธรรม์ประกันภัยผ่านทางอิเล็กทรอนิกส์ (Online)

ข้าพเจ้า..... ขอรับรองว่าข้อความและข้อมูลในแบบ ปช. ๒ นี้ ถูกต้องตรงตามความเป็นจริงทุกประการ

ประทับตรา (ถ้ามี)

ลงชื่อ .....
(.....)
กรรมการผู้มีอำนาจ/
ผู้รับมอบอำนาจของนายหน้าประกันชีวิตหรือธนาคาร

แบบการแจ้งเปลี่ยนแปลงและการรับรองระบบสารสนเทศ

ส่วนที่ ๑ กรณีบริษัทใช้บริการบุคคลภายนอก

๑. บริษัท .....

มีความประสงค์แจ้งเปลี่ยนแปลงการขึ้นทะเบียนกิจกรรมทางอิเล็กทรอนิกส์และการใช้บริการระบบสารสนเทศของผู้ให้บริการซึ่งเป็นบุคคลภายนอก.....(ระบุชื่อผู้ให้บริการ).....ในเรื่อง

(....) การเสนอขายกรมธรรม์ประกันภัยผ่านทางอิเล็กทรอนิกส์ (Online)

(....) การเสนอขายกรมธรรม์ประกันภัยโดยใช้เครื่องมือทางอิเล็กทรอนิกส์ประกอบ

(....) การออกกรมธรรม์ประกันภัยโดยใช้วิธีการทางอิเล็กทรอนิกส์

(....) การให้กู้ยืมเงินโดยมีกรมธรรม์ประกันภัยเป็นประกัน และการชดใช้เงินตามสัญญาประกันชีวิตโดยใช้วิธีการทางอิเล็กทรอนิกส์

รายละเอียดที่เปลี่ยนแปลง.....

.....

๒.บริษัทขอรับรองว่า

๒.๑ ผู้ให้บริการซึ่งเป็นบุคคลภายนอกมีระบบสารสนเทศที่มีมาตรฐานความมั่นคงและปลอดภัยในระดับเคร่งครัดสำหรับกิจกรรมตามข้อ ๑. ตามหลักเกณฑ์ที่กำหนดในเอกสารแนบท้ายประกาศนี้ โดยได้รับการตรวจสอบและรับรองจากผู้ตรวจสอบอิสระตามหนังสือรับรองตามแบบ อช. ๓ หรือตามประกาศนียบัตรที่ออกโดยหน่วยงานรับรองระบบสารสนเทศ (ISO๒๗๐๐๑) และ

บริษัทมีระบบสารสนเทศที่มีมาตรฐานความมั่นคงและปลอดภัยในระดับเคร่งครัดสำหรับกิจกรรมตามข้อ ๑. ตามหลักเกณฑ์ที่กำหนดในเอกสารแนบท้ายประกาศนี้ โดยได้รับการตรวจสอบและรับรองจากผู้ตรวจสอบอิสระตามหนังสือรับรองตามแบบ อช. ๓ หรือตามประกาศนียบัตรที่ออกโดยหน่วยงานรับรองระบบสารสนเทศ (ISO๒๗๐๐๑)

๒.๒ ได้กำหนดนโยบาย กระบวนการและวิธีปฏิบัติที่ชัดเจน เช่น ระบบการประเมินความเสี่ยง การบริหารความเสี่ยง ขั้นตอนของการบริการ การควบคุมภายใน การรักษาความปลอดภัย และแผนรองรับกรณีที่บุคคลภายนอกไม่สามารถให้บริการได้

๒.๓ สัญญาใช้บริการระบบสารสนเทศระหว่างบริษัทกับผู้ให้บริการซึ่งเป็นบุคคลภายนอกครอบคลุมเงื่อนไข ดังต่อไปนี้

(ก) มาตรการรักษาความมั่นคงปลอดภัยเพื่อคุ้มครองข้อมูลส่วนบุคคล ให้เป็นไปตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

(ข) การป้องกันการใช้หรือเปิดเผยโดยมิชอบ

(ค) การรายงานถึงความผิดปกติและการรายงานถึงการละเมิดข้อมูลส่วนบุคคล

(ง) ความรับผิดในการจ้างช่วงของผู้ให้บริการภายนอก โดยต้องกำหนดความรับผิดชอบของผู้ให้บริการบุคคลภายนอกเสมือนหนึ่งเป็นผู้ดำเนินการเอง หากมีการจ้างช่วงตามสัญญา

(จ) สิทธิการตรวจสอบโดยบริษัทและสำนักงาน

(ฉ) การคืน ทำลาย หรือลบข้อมูลส่วนบุคคล

(ช) ผลของการละเมิดเงื่อนไข

๓. บริษัทได้แนบเอกสาร โดยมีรายการดังต่อไปนี้

(....) หนังสือรับรองนิติบุคคลจากกรมพัฒนาธุรกิจการค้ากรณีผู้ให้บริการซึ่งเป็นบุคคลภายนอกเป็นนิติบุคคล

(....) เอกสารแสดงกิจกรรมและรายละเอียดที่ต้องการใช้วิธีการทางอิเล็กทรอนิกส์ (ตัวอย่างหน้าจอ)

(....) แผนผัง (Flow chart) และขั้นตอนของกิจกรรมที่ใช้วิธีการทางอิเล็กทรอนิกส์

(....) เอกสารแสดงระบบสารสนเทศและวิธีการทางอิเล็กทรอนิกส์ที่ใช้เพื่อรองรับกิจกรรมที่ใช้วิธีการทางอิเล็กทรอนิกส์ (system architecture)

(....) หนังสือรับรองการตรวจรับรองการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของผู้ให้บริการซึ่งเป็นบุคคลภายนอกโดยผู้ตรวจสอบอิสระตามแบบ อช. ๓ หรือประกาศนียบัตรที่ออกโดยหน่วยงานรับรองระบบสารสนเทศ (ISO๒๗๐๐๑)

(....) หนังสือรับรองการตรวจรับรองการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของบริษัทโดยผู้ตรวจสอบอิสระตามแบบ อช. ๓ หรือประกาศนียบัตรที่ออกโดยหน่วยงานรับรองระบบสารสนเทศ (ISO๒๗๐๐๑)

(....) เอกสารแนวทางการประเมินมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับเคร่งครัดตามหลักเกณฑ์ที่กำหนดในเอกสารแนบท้ายประกาศ (กรณีมีการตรวจรับรองจากผู้ตรวจสอบอิสระตามหนังสือรับรองตามแบบ อช. ๓)

(....) สำเนาสัญญาใช้บริการระบบสารสนเทศระหว่างบริษัทกับผู้ให้บริการซึ่งเป็นบุคคลภายนอก

ส่วนที่ ๒ กรณีนายหน้าประกันชีวิตหรือธนาคารใช้บริการบุคคลภายนอก

๔. ข้าพเจ้า .....ซึ่งมีใบอนุญาตเป็นนายหน้าประกันชีวิต เลขที่ ..... ใบอนุญาตหมดอายุ..... มีความประสงค์แจ้งเปลี่ยนแปลงการขอรับความเห็นชอบในการใช้บริการระบบสารสนเทศของผู้ให้บริการซึ่งเป็นบุคคลภายนอก.....(ระบุชื่อผู้ให้บริการ).....เพื่อใช้วิธีการทางอิเล็กทรอนิกส์ในเรื่อง

(....) การเสนอขายกรมธรรม์ประกันภัยผ่านทางอิเล็กทรอนิกส์ (Online) ซึ่งได้รับความยินยอมจากบริษัท..... ในการทำกิจกรรม

(....) การเสนอขายกรมธรรม์ประกันภัยโดยใช้เครื่องมือทางอิเล็กทรอนิกส์ประกอบ

รายละเอียดที่เปลี่ยนแปลง.....

.....

และได้รับความยินยอมจากบริษัท.....ในกิจกรรมข้างต้น

๕. ข้าพเจ้าขอรับรองว่า

๕.๑ ระบบสารสนเทศของผู้ให้บริการซึ่งเป็นบุคคลภายนอกมีมาตรฐานความมั่นคงและปลอดภัยในระดับเคร่งครัดสำหรับกิจกรรมตามข้อ ๔. ตามหลักเกณฑ์ที่กำหนดในเอกสารแนบท้ายประกาศนี้ โดยได้รับการตรวจสอบและรับรองจากผู้ตรวจสอบอิสระตามหนังสือรับรองตามแบบ อช. ๓ หรือตามประกาศนียบัตรที่ออกโดยหน่วยงานรับรองระบบสารสนเทศ (ISO๒๗๐๐๑) และ

ข้าพเจ้ามีระบบสารสนเทศที่มีมาตรฐานความมั่นคงและปลอดภัยในระดับเคร่งครัดสำหรับกิจกรรมตามข้อ ๔. ตามหลักเกณฑ์ที่กำหนดในเอกสารแนบท้ายประกาศนี้ โดยได้รับการตรวจสอบและรับรองจากผู้ตรวจสอบอิสระตามหนังสือรับรองตามแบบ อช. ๓ หรือตามประกาศนียบัตรที่ออกโดยหน่วยงานรับรองระบบสารสนเทศ (ISO๒๗๐๐๑)

๕.๒ ได้กำหนดนโยบาย กระบวนการและวิธีปฏิบัติที่ชัดเจน เช่น ระบบการประเมินความเสี่ยง การบริหารความเสี่ยง ขั้นตอนของการบริการ การควบคุมภายใน การรักษาความปลอดภัย และแผนรองรับกรณีที่บุคคลภายนอกไม่สามารถให้บริการได้

๕.๓ สัญญาใช้บริการระบบสารสนเทศระหว่างข้าพเจ้ากับผู้ให้บริการซึ่งเป็นบุคคลภายนอกครอบคลุมเงื่อนไข ดังต่อไปนี้

(ก) มาตรการรักษาความมั่นคงปลอดภัยเพื่อคุ้มครองข้อมูลส่วนบุคคล ให้เป็นไปตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

(ข) การป้องกันการใช้หรือเปิดเผยโดยมิชอบ

(ค) การรายงานถึงความผิดปกติและการรายงานถึงการละเมิดข้อมูลส่วนบุคคล

(ง) ความรับผิดในการจ้างช่วงของผู้ให้บริการภายนอก โดยต้องกำหนดความรับผิดชอบของผู้ให้บริการบุคคลภายนอกเสมือนหนึ่งเป็นผู้ดำเนินการเอง หากมีการจ้างช่วงตามสัญญา

(จ) สิทธิการตรวจสอบโดยบริษัทและสำนักงาน

(ฉ) การคืน ทำลาย หรือลบข้อมูลส่วนบุคคล

(ช) ผลของการละเมิดเงื่อนไข

๖. ข้าพเจ้าได้แนบเอกสาร โดยมีรายการดังต่อไปนี้

(....) หนังสือรับรองนิติบุคคลจากกรมพัฒนาธุรกิจการค้ากรณีผู้ให้บริการซึ่งเป็นบุคคลภายนอกเป็นนิติบุคคล

(....) เอกสารแสดงกิจกรรมและรายละเอียดที่ต้องการใช้วิธีการทางอิเล็กทรอนิกส์ (ตัวอย่างหน้าจอ)

(....) แผนผัง (Flow chart) และขั้นตอนของกิจกรรมที่ใช้วิธีการทางอิเล็กทรอนิกส์

(....) เอกสารแสดงระบบสารสนเทศและวิธีการทางอิเล็กทรอนิกส์ที่ใช้เพื่อรองรับกิจกรรมที่ใช้วิธีการทางอิเล็กทรอนิกส์ (system architecture)

(....) หนังสือรับรองการตรวจรับรองการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของผู้ให้บริการซึ่งเป็นบุคคลภายนอกโดยผู้ตรวจสอบอิสระตามแบบ อช. ๓ หรือตามประกาศนียบัตรที่ออกโดยหน่วยงานรับรองระบบสารสนเทศ (ISO๒๗๐๐๑)

(....) หนังสือรับรองการตรวจรับรองการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของข้าพเจ้าโดยผู้ตรวจสอบอิสระตามแบบ อช. ๓ หรือตามประกาศนียบัตรที่ออกโดยหน่วยงานรับรองระบบสารสนเทศ (ISO๒๗๐๐๑)

(....) เอกสารแนวทางการประเมินมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับเคร่งครัดตามหลักเกณฑ์ที่กำหนดในเอกสารแนบท้ายประกาศ (กรณีมีการตรวจรับรองจากผู้ตรวจสอบอิสระตามหนังสือรับรองตามแบบ อช. ๓)

(....) สำเนาสัญญาใช้บริการระบบสารสนเทศระหว่างข้าพเจ้ากับผู้ให้บริการซึ่งเป็นบุคคลภายนอก

(....) หนังสือยินยอมของบริษัทให้เสนอขายกรมธรรม์ประกันภัยผ่านทางอิเล็กทรอนิกส์ (Online)

☐ บริษัท ☐ นายหน้าประกันชีวิตหรือธนาคาร .....

ขอรับรองว่า ข้อความและข้อมูลในแบบ ปช. ๔ นี้ ถูกต้องตรงตามความเป็นจริงทุกประการ

ประทับตรา (ถ้ามี) ลงชื่อ .....

(.....)

กรรมการผู้มีอำนาจ/ผู้รับมอบอำนาจ*

*กรรมการผู้มีอำนาจ/ผู้รับมอบอำนาจของบริษัท/นายหน้าประกันชีวิตหรือธนาคาร แล้วแต่กรณี

แนวทางการประเมินมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ
ตามวิธีการแบบปลอดภัยในระดับเคร่งครัด

หัวข้อ	รายละเอียด
๑. การสร้างความมั่นคงปลอดภัยด้านบริหารจัดการ	
๑.๑ กำหนดนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยผ่านการอนุมัติและผลักดันโดยผู้บริหารระดับสูง และมีการประกาศนโยบายดังกล่าวให้พนักงานและบุคคลภายนอกที่เกี่ยวข้องรับทราบโดยทั่วกัน ๑.๒ วางแผนการติดตามและประเมินผลการใช้งานความมั่นคงปลอดภัยด้านสารสนเทศ และนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างสม่ำเสมอ เพื่อปรับปรุงหากมีการเปลี่ยนแปลงใด ๆ ภายในหน่วยงาน ทั้งนี้เพื่อให้เหมาะสมกับสถานการณ์การใช้งาน และคงความมีประสิทธิผลอยู่เสมอ	
๒. การจัดโครงสร้างด้านความมั่นคงปลอดภัยของระบบสารสนเทศในส่วนการบริหารจัดการด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ทั้งภายในและภายนอกหน่วยงานหรือองค์กร	
๒.๑ ผู้บริหารระดับสูงของหน่วยงานมีหน้าที่ดูแลรับผิดชอบงานด้านสารสนเทศของหน่วยงานให้การสนับสนุน และกำหนดทิศทางการดำเนินงานเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศที่ชัดเจน รวมทั้งมีการมอบหมายงานที่เกี่ยวข้องให้กับผู้ปฏิบัติงานอย่างชัดเจน ตลอดจนรับผิดชอบต่อความเสี่ยง ความเสียหาย หรือ อันตรายที่เกิดขึ้นกับระบบสารสนเทศไม่ว่ากรณีใด ๆ ๒.๒ สำหรับระบบสารสนเทศใหม่มีการกำหนดขั้นตอนการพิจารณาทบทวน เพื่ออนุมัติการสร้าง การติดตั้ง หรือการใช้งานในแง่มุมต่าง ๆ เช่น การบริหารจัดการผู้ใช้งานระบบ หรือความสามารถในการทำงานร่วมกันได้ระหว่างระบบเดิมและระบบใหม่ ๒.๓ มีการกำหนดสัญญาการรักษาข้อมูลที่เป็นความลับ (Confidentiality agreement หรือ NonDisclosure agreement) ที่สอดคล้องกับสถานการณ์และความต้องการของหน่วยงานในการปกป้องข้อมูลสารสนเทศ ๒.๔ มีข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศสำหรับการอนุญาตให้ผู้ใช้บริการที่เป็นบุคคลภายนอกเข้าถึงระบบสารสนเทศ หรือใช้ข้อมูลสารสนเทศของหน่วยงาน ๒.๕ สำหรับข้อตกลงเพื่ออนุญาตให้บุคคลภายนอกเข้าถึงระบบสารสนเทศ หรือใช้ข้อมูลสารสนเทศของหน่วยงาน เพื่อการอ่าน การประมวลผล การบริหารจัดการระบบสารสนเทศ หรือการพัฒนาระบบสารสนเทศ ควรมีข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศระบุไว้ในข้อตกลง ๒.๖ มีการกำหนดเนื้องานหรือหน้าที่ความรับผิดชอบต่าง ๆ เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศไว้อย่างชัดเจน ๒.๗ มีการกำหนดขั้นตอนและช่องทางในการติดต่อกับหน่วยงานภายนอกที่มีความเชี่ยวชาญเฉพาะด้าน หรือหน่วยงานที่มีความเชี่ยวชาญด้านความมั่นคงปลอดภัยด้านสารสนเทศภายใต้สถานการณ์ต่าง ๆ ไว้อย่างชัดเจน ๒.๘ จัดให้มีการพิจารณาทบทวนแนวทางในการบริหารจัดการงานเกี่ยวกับความมั่นคงปลอดภัยด้าน สารสนเทศอย่างสม่ำเสมอ หรือเมื่อมีการเปลี่ยนแปลงใด ๆ ในการดำเนินงาน ทั้งนี้ การพิจารณาทบทวนดังกล่าว ควรดำเนินการโดยผู้ไม่มีส่วนได้เสียกับงานที่มีการพิจารณาทบทวน ๒.๙ มีการสร้างความร่วมมือระหว่างผู้ที่มีบทบาทเกี่ยวข้องกับความมั่นคงปลอดภัยด้าน	

หัวข้อ	รายละเอียด
สารสนเทศของ หน่วยงาน ในงานหรือกิจกรรมใด ๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศ ๒.๑๐ มีการกำหนดขั้นตอนและช่องทางในการติดต่อกับหน่วยงานภายนอกที่มีหน้าที่ในการกำกับดูแล หรือหน่วยงานที่เกี่ยวข้องกับการบังคับใช้กฎหมาย รวมทั้งหน่วยงานที่ควบคุมดูแลสถานการณ์ฉุกเฉินภายใต้สถานการณ์ต่าง ๆ ไว้อย่างชัดเจน ๒.๑๑ ก่อนที่จะอนุญาตให้หน่วยงานหรือบุคคลภายนอกเข้าถึงระบบสารสนเทศหรือใช้ข้อมูลสารสนเทศของ หน่วยงาน ให้มีการระบุความเสี่ยงที่อาจเกิดขึ้นและกำหนดแนวทางป้องกันเพื่อลดความเสี่ยงนั้นก่อนการอนุญาต	
๓. การบริหารจัดการทรัพย์สินสารสนเทศ	
๓.๑ มีการเก็บบันทึกข้อมูลทรัพย์สินสารสนเทศ โดยข้อมูลที่จัดเก็บต้องประกอบด้วยข้อมูลที่จำเป็นในการค้นหาเพื่อการใช้งานในภายหลัง ๓.๒ มีการกำหนดบุคคลผู้มีหน้าที่ดูแลควบคุมการใช้งานและรับผิดชอบทรัพย์สินสารสนเทศไว้ชัดเจน ๓.๓ มีการกำหนดกฎระเบียบในการใช้งานทรัพย์สินสารสนเทศไว้อย่างชัดเจน โดยจัดทำเป็นเอกสาร และมีการประกาศใช้ในหน่วยงาน ๓.๔ มีการจำแนกประเภทของข้อมูลสารสนเทศ โดยจำแนกตามมูลค่าของข้อมูลข้อกำหนดทางกฎหมาย ระดับชั้นความลับและความสำคัญต่อหน่วยงาน ๓.๕ มีการกำหนดและประกาศใช้ขั้นตอนที่เหมาะสมในการจำแนกประเภทของข้อมูลสารสนเทศ และจัดการข้อมูลสารสนเทศ โดยให้สอดคล้องกับแนวทางการจำแนกประเภทของข้อมูลสารสนเทศที่หน่วยงานประกาศใช้	
๔. การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร	
๔.๑ กำหนดหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยด้านสารสนเทศของพนักงานหรือหน่วยงาน หรือบุคคลภายนอกที่ว่าจ้าง โดยให้สอดคล้องกับความมั่นคงปลอดภัยด้านสารสนเทศและนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่หน่วยงานประกาศใช้ ๔.๒ ผู้บริหารระดับสูงของหน่วยงานต้องกำหนดให้พนักงาน หน่วยงานหรือบุคคลภายนอกที่ว่าจ้าง ปฏิบัติงานตามนโยบายหรือระเบียบปฏิบัติด้านความมั่นคงปลอดภัยที่หน่วยงานประกาศใช้ ๔.๓ กำหนดให้มีขั้นตอนการลงโทษพนักงานที่ฝ่าฝืนนโยบายหรือระเบียบปฏิบัติเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศในหน่วยงาน ๔.๔ กำหนดหน้าที่ความรับผิดชอบในการยุติการจ้าง หรือการเปลี่ยนแปลงสถานะการจ้างให้ชัดเจน และมอบหมายให้มีผู้รับผิดชอบอย่างชัดเจน ๔.๕ พนักงานหน่วยงานหรือบุคคลภายนอกที่ว่าจ้างต้องส่งคืนทรัพย์สินสารสนเทศของหน่วยงานเมื่อ สิ้นสุดสถานะการเป็นพนักงาน หรือสิ้นสุดสัญญาหรือข้อตกลงการปฏิบัติงานให้กับหน่วยงาน ๔.๖ ให้ยกเลิกสิทธิของพนักงานหน่วยงานหรือบุคคลภายนอกในการเข้าใช้งานระบบสารสนเทศ เมื่อสิ้นสุดสถานะการเป็นพนักงาน หรือสิ้นสุดสัญญาหรือข้อตกลงการปฏิบัติงานและให้ปรับเปลี่ยนระดับสิทธิในการเข้าใช้งานระบบสารสนเทศให้เหมาะสมเมื่อมีการเปลี่ยนแปลงหน้าที่ความรับผิดชอบใด ๆ เกิดขึ้น ๔.๗ พนักงาน หน่วยงานหรือ บุคคลภายนอกต้องได้รับการอบรมเพื่อสร้างความตระหนักรู้เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศในส่วนที่ เกี่ยวข้องกับหน้าที่ความรับผิดชอบของตนและได้รับการสื่อสารให้ทราบถึงนโยบายหรือระเบียบปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศที่หน่วยงานประกาศใช้อย่างสม่ำเสมอ หรือเมื่อมีการเปลี่ยนแปลง	

หัวข้อ	รายละเอียด
๔.๘ ในการพิจารณารับพนักงานเข้าทำงาน หรือการว่าจ้างหน่วยงานหรือบุคคลภายนอก ให้มีการตรวจสอบประวัติหรือคุณสมบัติเพื่อให้เป็นไปตามกฎหมาย กฎระเบียบและจริยธรรมที่เกี่ยวข้อง โดยให้คำนึงถึงระดับชั้นความลับของข้อมูลสารสนเทศที่จะให้เข้าถึง และระดับความเสี่ยงที่ได้ประเมิน ๔.๙ ในสัญญาจ้างหรือข้อตกลงการปฏิบัติงานของพนักงาน หรือสัญญาว่าจ้างหน่วยงานหรือ บุคคลภายนอก ให้ระบุหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยด้านสารสนเทศไว้ในสัญญา	
๕. การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม	
๕.๑ ให้มีการป้องกันขอบเขตพื้นที่ตั้งของหน่วยงาน (Security perimeter) ที่มีการติดตั้ง จัดเก็บ หรือใช้งานระบบสารสนเทศและข้อมูลสารสนเทศ ๕.๒ มีการออกแบบและติดตั้งการป้องกันความมั่นคงปลอดภัยด้านกายภาพ เพื่อป้องกันภัยจากภายนอก ภัยในระดับหายนะทั้งที่ก่อโดยมนุษย์หรือภัยธรรมชาติเช่น อัคคีภัย อุทกภัย แผ่นดินไหว ระเบิด การก่อจลาจล เป็นต้น ๕.๓ จัดวางและป้องกันอุปกรณ์สารสนเทศ เพื่อลดความเสี่ยงจากภัยธรรมชาติหรืออันตรายต่าง ๆ และเพื่อป้องกันการเข้าถึงโดยมิได้รับอนุญาต ๕.๔ มีการป้องกันอุปกรณ์สารสนเทศ ที่อาจเกิดจากไฟฟ้าขัดข้อง (Power failure) หรือที่อาจหยุดชะงัก จากข้อผิดพลาดของโครงสร้างพื้นฐาน (Supporting utilities) ๕.๕ มีการดูแลอุปกรณ์สารสนเทศอย่างถูกวิธีเพื่อให้คงไว้ซึ่งความถูกต้องครบถ้วนและอยู่ในสภาพพร้อมใช้งานอยู่เสมอ ๕.๖ มีการออกแบบและติดตั้งการป้องกันความมั่นคงปลอดภัยด้านกายภาพ เพื่อป้องกันพื้นที่หรือสถานที่ปฏิบัติงาน หรืออุปกรณ์สารสนเทศต่าง ๆ ๕.๗ ไม่ควรนำอุปกรณ์สารสนเทศ ข้อมูลสารสนเทศ หรือซอฟต์แวร์ออกจากสถานที่ปฏิบัติงานของหน่วยงานหากมิได้รับอนุญาต ๕.๘ ในพื้นที่ที่ต้องมีการรักษาความมั่นคงปลอดภัยด้านกายภาพ (Secure area) ต้องมีการควบคุมการเข้าออก โดยให้เฉพาะผู้มีสิทธิที่สามารถเข้าออกได้ ๕.๙ มีการออกแบบแนวทางการป้องกันทางกายภาพสำหรับการทำงานในพื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัยด้านกายภาพ (Secure area) และกำหนดให้มีการนำไปใช้งาน ๕.๑๐ มีการควบคุมบริเวณที่ผู้ไม่มีสิทธิเข้าถึงอาจสามารถเข้าถึงได้เช่น จุดรับส่งของ เป็นต้น หรือหากเป็นไปได้ให้แยกบริเวณดังกล่าวออกจากพื้นที่ที่มีการติดตั้ง จัดเก็บ หรือใช้งานระบบสารสนเทศและข้อมูลสารสนเทศเพื่อหลีกเลี่ยงการเข้าถึงโดยมิได้รับอนุญาต ๕.๑๑ มีการป้องกันสายเคเบิลที่ใช้เพื่อการสื่อสาร หรือสายไฟ เพื่อมิให้มีการดักรับสัญญาณ (Interception) หรือมีความเสียหายเกิดขึ้น ๕.๑๒ มีการรักษาความมั่นคงปลอดภัยให้กับอุปกรณ์สารสนเทศที่มีการนำไปใช้งานนอกสถานที่ปฏิบัติงานของหน่วยงาน โดยให้คำนึงถึงระดับความเสี่ยงที่แตกต่างกันจากการนำไปใช้งานในสถานที่ต่าง ๆ ๕.๑๓ ก่อนการยกเลิกการใช้งานหรือจำหน่ายอุปกรณ์สารสนเทศที่ใช้ในการจัดเก็บข้อมูลสารสนเทศต้องมีการตรวจสอบอุปกรณ์สารสนเทศนั้นว่า ได้มีการลบ ย้าย หรือทำลายข้อมูลที่สำคัญหรือซอฟต์แวร์ที่จัดซื้อและติดตั้งไว้ด้วยวิธีการที่ทำให้ไม่สามารถกู้คืนได้อีก	
๖. การบริหารจัดการด้านการสื่อสารและการดำเนินงานของระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์และระบบสารสนเทศ	
๖.๑ มีการจัดทำ ปรับปรุง และดูแลเอกสารขั้นตอนการปฏิบัติงานที่อยู่ในสภาพพร้อมใช้งาน เพื่อให้พนักงานสามารถนำไปปฏิบัติได้	

หัวข้อ	รายละเอียด
๖.๒ มีการดูแลให้บุคคลหรือหน่วยงานภายนอกที่ให้บริการแก่หน่วยงานตามที่ว่าจ้างปฏิบัติตามสัญญา หรือข้อตกลงให้บริการที่ระบุไว้ซึ่งต้องครอบคลุมถึงงานด้านความมั่นคงปลอดภัย ลักษณะการให้บริการ และระดับการให้บริการ ๖.๓ มีการติดตามตรวจสอบรายงานหรือบันทึกการให้บริการของบุคคลหรือหน่วยงานภายนอกที่ให้บริการแก่หน่วยงานตามที่ว่าจ้างอย่างสม่ำเสมอ ๖.๔ จัดให้มีเกณฑ์การตรวจรับระบบสารสนเทศที่มีการปรับปรุงหรือที่มีเวอร์ชั่นใหม่ และควรมีการทดสอบระบบสารสนเทศทั้งในช่วงการพัฒนาระบบและก่อนการตรวจรับ ๖.๕ มีขั้นตอนควบคุมการตรวจสอบ ป้องกัน และกู้คืนในกรณีมีการใช้งานโปรแกรมไม่พึงประสงค์และให้มีการสร้างความตระหนักรู้ให้กับผู้ใช้งานระบบสารสนเทศหรือข้อมูลสารสนเทศเกี่ยวกับโปรแกรมไม่พึงประสงค์ ๖.๖ มีการสำรองข้อมูลสารสนเทศ และทดสอบการนำกลับมาใช้งาน โดยให้เป็นไปตามนโยบายการสำรองข้อมูลที่หน่วยงานประกาศใช้ ๖.๗ มีการบริหารจัดการการควบคุมเครือข่ายคอมพิวเตอร์เพื่อป้องกันภัยคุกคาม และมีการรักษาความ มั่นคงปลอดภัยของระบบสารสนเทศและแอพพลิเคชั่นที่ทำงานบนเครือข่ายคอมพิวเตอร์รวมทั้งข้อมูลสารสนเทศ ที่มีการแลกเปลี่ยนบนเครือข่ายดังกล่าว ๖.๘ มีการกำหนดรูปแบบการรักษาความมั่นคงปลอดภัย ระดับการให้บริการ ข้อกำหนดการบริหารจัดการ ในข้อตกลงการให้บริการด้านเครือข่ายคอมพิวเตอร์ไม่ว่าเป็นการให้บริการโดยหน่วยงานเอง หรือจ้างช่วงไปยังผู้ให้บริการภายนอก ๖.๙ จัดให้มีนโยบายและขั้นตอนปฏิบัติงาน รวมทั้งควบคุมการแลกเปลี่ยนข้อมูลสารสนเทศผ่านช่องทางการสื่อสารในรูปแบบข้อมูลอิเล็กทรอนิกส์ ๖.๑๐ จัดให้มีข้อตกลงในการแลกเปลี่ยนข้อมูลสารสนเทศหรือซอฟต์แวร์ระหว่างหน่วยงานกับบุคคลหรือหน่วยงานภายนอก ๖.๑๑ จัดให้มีนโยบายและขั้นตอนการปฏิบัติงาน เพื่อป้องกันข้อมูลสารสนเทศที่มีการสื่อสารหรือ แลกเปลี่ยนผ่านระบบสารสนเทศที่มีการเชื่อมต่อกับระบบสารสนเทศต่าง ๆ ๖.๑๒ มีการป้องกันข้อมูลสารสนเทศที่มีการแลกเปลี่ยนในการทำพาณิชย์อิเล็กทรอนิกส์ (Electronic commerce) ผ่านเครือข่ายคอมพิวเตอร์สาธารณะ เพื่อมิให้มีการฉ้อโกง ละเมิดสัญญา หรือมีการรั่วไหลหรือข้อมูลสารสนเทศถูกแก้ไขโดยมิได้รับอนุญาต ๖.๑๓ มีการป้องกันข้อมูลสารสนเทศที่มีการสื่อสารหรือแลกเปลี่ยนในการทำธุรกรรมทางออนไลน์ (Online transaction) เพื่อมิให้มีการรับส่งข้อมูลที่ไม่สมบูรณ์หรือส่งข้อมูลไปผิดที่ หรือมีการรั่วไหลของข้อมูล หรือข้อมูลถูกแก้ไขเปลี่ยนแปลง ถูกทำซ้ำใหม่ หรือถูกส่งซ้ำโดยมิได้รับอนุญาต ๖.๑๔ สำหรับข้อมูลสารสนเทศที่มีการเผยแพร่ต่อสาธารณชน ให้มีการป้องกันมิให้มีการแก้ไขเปลี่ยนแปลง โดยมิได้รับอนุญาต และเพื่อรักษาความถูกต้องครบถ้วนของข้อมูลสารสนเทศ ๖.๑๕ มีการเก็บบันทึกข้อมูล Audit log ซึ่งบันทึกข้อมูลกิจกรรมการใช้งานของผู้ใช้งานระบบสารสนเทศ และเหตุการณ์เกี่ยวกับความมั่นคงปลอดภัยต่าง ๆ เพื่อประโยชน์ในการสืบสวน สอบสวนในอนาคต และเพื่อการติดตามการควบคุมการเข้าถึง ๖.๑๖ มีขั้นตอนการเฝ้าติดตามสังเกตการใช้งานระบบสารสนเทศ และมีการติดตามประเมินผลการติดตามสังเกตดังกล่าวอย่างสม่ำเสมอ ๖.๑๗ มีการป้องกันระบบสารสนเทศที่จัดเก็บ Log และข้อมูล Log เพื่อป้องกันการเข้าถึงหรือแก้ไข เปลี่ยนแปลงโดยมิได้รับอนุญาต ๖.๑๘ มีการจัดเก็บ Log ที่เกี่ยวข้องกับการดูแลระบบสารสนเทศโดยผู้ดูแลระบบ (System administrator หรือ System operator) ๖.๑๙ มีการจัดการควบคุมการเปลี่ยนแปลงของระบบสารสนเทศ ๖.๒๐ มีการติดตามผลการใช้งานทรัพยากรสารสนเทศ และวางแผนด้านทรัพยากร	

หัวข้อ	รายละเอียด
สารสนเทศให้รองรับการปฏิบัติงานในอนาคตอย่างเหมาะสม ๖.๒๑ มีขั้นตอนการปฏิบัติงานในการจัดการและจัดเก็บข้อมูลสารสนเทศเพื่อมิให้ข้อมูลรั่วไหลหรือถูกนำไปใช้ผิดประเภท ๖.๒๒ มีการจัดเก็บ Log ที่เกี่ยวข้องกับข้อผิดพลาดใด ๆ ของระบบสารสนเทศ มีการวิเคราะห์ Log ดังกล่าว อย่างสม่ำเสมอ และมีการจัดการแก้ไขข้อผิดพลาดที่ตรวจพบอย่างเหมาะสม ๖.๒๓ ระบบเวลาของระบบสารสนเทศต่าง ๆ ที่ใช้ในหน่วยงานหรือในขอบเขตงานด้านความมั่นคงปลอดภัย (Security domain) ต้องมีความสอดคล้องกัน (Synchronization) โดยให้มีการตั้งค่าพร้อมกับเวลาจากแหล่งเวลา ที่เชื่อถือได้ ๖.๒๔ มีการแบ่งแยกหน้าที่และขอบเขตความรับผิดชอบอย่างชัดเจน เพื่อลดโอกาสความผิดพลาดในการเปลี่ยนแปลงหรือใช้งานระบบสารสนเทศหรือข้อมูลสารสนเทศที่ผิดประเภท ๖.๒๕ มีการแยกระบบสารสนเทศสำหรับการพัฒนา ทดสอบ และใช้งานจริงออกจากกัน เพื่อลดความเสี่ยง ในการเข้าใช้งานหรือการเปลี่ยนแปลงระบบสารสนเทศโดยมิได้รับอนุญาต ๖.๒๖ มีการบริหารจัดการการเปลี่ยนแปลงใด ๆ เกี่ยวกับการจัดเตรียมการให้บริการ และการดูแลปรับปรุงนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ขั้นตอนปฏิบัติงานหรือการควบคุมเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ โดยคำนึงถึงระดับความสำคัญของการดำเนินธุรกิจที่เกี่ยวข้องและการประเมินความเสี่ยงอย่างต่อเนื่อง ๖.๒๗ หากหน่วยงานอนุญาตให้มีการใช้งาน Mobile code (เช่น Script บางอย่างของเว็บแอพพลิเคชั่นที่มีการทำงานอัตโนมัติเมื่อเรียกดูเว็บ) ควรมีการตั้งค่าการทำงาน (Configuration) เพื่อให้มั่นใจได้ว่าการทำงานของ Mobile code นั้นเป็นไปตามความมั่นคงปลอดภัยด้านสารสนเทศและนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และห้ามโดยอัตโนมัติมิให้ Mobile code สามารถทำงานได้ในระบบสารสนเทศ หากในนโยบาย การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กำหนดห้ามมิให้ประเภทของ Mobile code ดังกล่าวทำงานได้ ๖.๒๘ มีขั้นตอนการปฏิบัติงานสำหรับการบริหารจัดการอุปกรณ์ที่ใช้ในการบันทึกข้อมูลอิเล็กทรอนิกส์ที่สามารถถอดหรือต่อพ่วงกับเครื่องคอมพิวเตอร์ได้ (Removable media) ๖.๒๙ มีขั้นตอนการปฏิบัติงานในการทำลายอุปกรณ์ที่ใช้ในการบันทึกข้อมูลอิเล็กทรอนิกส์ที่สามารถถอด หรือต่อพ่วงกับเครื่องคอมพิวเตอร์ได้ (Removable media) อย่างมั่นคงปลอดภัย ๖.๓๐ มีการป้องกันมิให้ข้อมูลหรือเอกสารเกี่ยวกับระบบสารสนเทศ (System documentation) ถูกเข้าถึง โดยมิได้รับอนุญาต ๖.๓๑ ในกรณีที่มีการเคลื่อนย้ายอุปกรณ์ที่จัดเก็บข้อมูลสารสนเทศ ให้มีการป้องกันอุปกรณ์ที่ใช้จัดเก็บข้อมูลดังกล่าว เพื่อมิให้มีการเข้าถึงโดยมิได้รับอนุญาต หรือถูกนำไปใช้งานผิดประเภท หรืออุปกรณ์หรือข้อมูลสารสนเทศได้รับความเสียหาย ๖.๓๒ ให้มีการป้องกันข้อมูลสารสนเทศที่มีการสื่อสารกันผ่านข้อมูลอิเล็กทรอนิกส์ (Electronic messaging) เช่น จดหมายอิเล็กทรอนิกส์ (E - mail) EDI หรือ Instant messaging)	
๗. การควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์และข้อมูลคอมพิวเตอร์	
๗.๑ จัดให้มีนโยบายควบคุมการเข้าถึง โดยจัดทำเป็นเอกสาร และมีการติดตามทบทวนให้นโยบายดังกล่าว สอดคล้องกับข้อกำหนดหรือความต้องการด้านการดำเนินงานหรือการให้บริการ และด้านการรักษาความมั่นคง ปลอดภัยระบบสารสนเทศ ๗.๒ จัดให้มีการลงทะเบียนบัญชีผู้ใช้งานระบบสารสนเทศ และยกเลิกบัญชีผู้ใช้อย่างเป็นทางการ เพื่อควบคุมการให้สิทธิและการยกเลิกสิทธิในการเข้าใช้งานระบบสารสนเทศใด ๆ ของ	

หัวข้อ	รายละเอียด
หน่วยงาน ๗.๓ การกำหนดสิทธิในการเข้าถึงระดับสูง ให้ทำอย่างจำกัดและอยู่ภายใต้การควบคุม ๗.๔ ผู้ใช้งานต้องดูแลป้องกันอุปกรณ์สารสนเทศใดที่อยู่ภายใต้ความดูแลรับผิดชอบ ในระหว่างที่ไม่มีการใช้งาน ๗.๕ จำกัดการเข้าถึงเครือข่ายคอมพิวเตอร์ของหน่วยงานที่สามารถเข้าถึงได้จากภายนอก โดยให้สอดคล้องกับนโยบายควบคุมการเข้าถึง และข้อกำหนดการใช้งานแอพพลิเคชั่นเพื่อการดำเนินงาน ๗.๖ ให้ผู้ใช้งานทุกคนมีบัญชีผู้ใช้งานเป็นของตนเอง และให้ระบบสารสนเทศมีเทคนิคการตรวจสอบตัวตนที่เพียงพอ เพื่อให้สามารถระบุตัวตนของผู้เข้าใช้งานระบบสารสนเทศได้ ๗.๗ ให้ยุติหรือปิดหน้าจอการใช้งานระบบสารสนเทศโดยอัตโนมัติหากไม่มีการใช้งานเกินระยะเวลาสูงสุดที่กำหนดไว้ ๗.๘ จำกัดการเข้าถึงข้อมูลสารสนเทศและฟังก์ชั่นต่าง ๆ ในแอพพลิเคชั่นของผู้ใช้งานและผู้ดูแลระบบสารสนเทศ โดยให้สอดคล้องกับนโยบายการเข้าถึงที่ได้กำหนดไว้ ๗.๙ กำหนดนโยบายและแนวทางการจัดการด้านความมั่นคงปลอดภัย เพื่อลดความเสี่ยงในการใช้งานอุปกรณ์สารสนเทศหรืออุปกรณ์การสื่อสารที่เคลื่อนย้ายได้เช่น แล็ปท็อปคอมพิวเตอร์ (Laptop Computer) หรือสมาร์ทโฟน (Smartphone) เป็นต้น ๗.๑๐ มีข้อบังคับให้ผู้ใช้งานปฏิบัติตามขั้นตอนเพื่อการเลือกใช้รหัสผ่านอย่างมั่นคงปลอดภัยตามที่หน่วยงานกำหนด ๗.๑๑ ผู้ใช้งานสามารถเข้าถึงเฉพาะบริการทางเครือข่ายคอมพิวเตอร์ที่ตนเองได้รับอนุญาตให้ใช้ได้เท่านั้น ๗.๑๒ ให้มีการกำหนดวิธีการตรวจสอบตัวตนที่เหมาะสมเพื่อควบคุมการเข้าถึงระบบสารสนเทศของ หน่วยงานจากระยะไกล ๗.๑๓ มีการควบคุมการเข้าถึงช่องทางการดูแลระบบสารสนเทศทั้งทางกายภาพและการเชื่อมต่อผ่าน คอมพิวเตอร์สำหรับระบบสารสนเทศที่สามารถเข้าถึงจากระยะไกลได้เช่น Remote diagnostic หรือ Configuration facility ของอุปกรณ์เครือข่ายคอมพิวเตอร์ ๗.๑๔ มีการจัดกลุ่มตามประเภทของข้อมูลสารสนเทศที่ให้บริการ ระบบสารสนเทศ กลุ่มผู้ใช้งานโดยมีการแบ่งแยกบนเครือข่ายคอมพิวเตอร์อย่างเป็นสัดส่วน ๗.๑๕ กำหนดให้มีการควบคุมเส้นทางการไหลของข้อมูลสารสนเทศในระบบเครือข่ายคอมพิวเตอร์เพื่อไม่ให้ขัดแย้งกับนโยบายควบคุมการเข้าถึงของแอพพลิเคชั่น ๗.๑๖ กำหนดขั้นตอนการ Log-on เพื่อควบคุมการเข้าถึงระบบปฏิบัติการคอมพิวเตอร์ ๗.๑๗ ให้จัดทำหรือจัดให้มีระบบการบริหารจัดการรหัสผ่านที่สามารถทำงานแบบเชิงโต้ตอบกับผู้ใช้งาน (Interactive) และสามารถรองรับการใช้งานรหัสผ่านที่มีความมั่นคงปลอดภัย ๗.๑๘ จัดให้มีขั้นตอนการบริหารจัดการเรื่องการกำหนดรหัสผ่านอย่างเป็นทางการ ๗.๑๙ กำหนดให้ผู้บริหารติดตามทบทวนระดับสิทธิในการเข้าถึงของผู้ใช้งานอย่างเป็นทางการเป็นประจำ ๗.๒๐ มีการกำหนดนโยบาย Clear desk สำหรับข้อมูลสารสนเทศในรูปแบบกระดาษและที่จัดเก็บใน อุปกรณ์บันทึกข้อมูลอิเล็กทรอนิกส์ที่สามารถถอดหรือต่อพ่วงกับเครื่องคอมพิวเตอร์ได้และนโยบาย Clear screen สำหรับระบบสารสนเทศ ๗.๒๑ ให้มีการระบุอุปกรณ์ที่เชื่อมต่อเข้ากับระบบสารสนเทศโดยอัตโนมัติ (Automatic equipment identification) เพื่อตรวจสอบการเชื่อมต่อของอุปกรณ์ดังกล่าวว่ามาจากอุปกรณ์ดังกล่าวจริง หรือจากสถานที่ที่กำหนดไว้เท่านั้น ทั้งนี้จำเป็นสำหรับการที่ระบบสารสนเทศจะรับการเชื่อมต่อจากเฉพาะอุปกรณ์ที่ได้รับอนุญาต หรือมาจากเฉพาะสถานที่ที่ได้รับอนุญาต ๗.๒๒ ให้จำกัดการเข้าถึงการใช้งานโปรแกรมอรรถประโยชน์ต่าง ๆ อย่างเข้มงวด เนื่องจาก	

หัวข้อ	รายละเอียด
โปรแกรมดังกล่าวอาจมีความสามารถควบคุมดูแลและเปลี่ยนแปลงการทำงานของระบบสารสนเทศได้ ๗.๒๓ จำกัดระยะเวลาการเชื่อมต่อกับระบบสารสนเทศที่มีระดับความเสี่ยงสูง เพื่อเพิ่มระดับการรักษาความมั่นคงปลอดภัย ๗.๒๔ สำหรับระบบสารสนเทศที่มีความสำคัญสูง ต้องจัดให้ระบบสารสนเทศทำงานในสภาพแวดล้อมที่แยกออกมาต่างหาก โดยไม่ใช้ปะปนกับระบบสารสนเทศอื่น ๗.๒๕ กำหนดให้มีนโยบาย แผนงานและขั้นตอนการปฏิบัติงานที่เกี่ยวข้องกับกิจกรรมใด ๆ ที่มีการปฏิบัติงานจากภายนอกหน่วยงาน (Teleworking)	
๘. การจัดหาหรือจัดให้มีการพัฒนา และการบำรุงรักษาระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์และระบบสารสนเทศ	
๘.๑ ในการจัดทำข้อกำหนดขั้นต่ำของระบบสารสนเทศใหม่ หรือการปรับปรุงระบบสารสนเทศเดิม ให้มีการระบุข้อกำหนดด้านการควบคุมความมั่นคงปลอดภัยด้านสารสนเทศไว้ด้วย ๘.๒ ให้ดูแล ควบคุม ติดตามตรวจสอบการทำงานในการจ้างช่วงพัฒนาซอฟต์แวร์ ๘.๓ ให้มีการตรวจสอบ (Validate) ข้อมูลใด ๆ ที่จะรับเข้าสู่แอพพลิเคชั่นก่อนเสมอ เพื่อให้มั่นใจได้ว่า ข้อมูลมีความถูกต้องและมีรูปแบบเหมาะสม ๘.๔ ให้มีการตรวจสอบ (Validate) ข้อมูลใด ๆ อันเป็นผลจากการประมวลผลของแอพพลิเคชั่น เพื่อให้มั่นใจได้ว่า ข้อมูลที่ได้จากการประมวลผลถูกต้องและเหมาะสม ๘.๕ จัดให้มีแนวทางการบริหารจัดการกุญแจ (Key) เพื่อรองรับการใช้งานเทคนิคที่เกี่ยวข้องกับการเข้ารหัสลับของหน่วยงาน ๘.๖ ให้เลือกชุดข้อมูลสารสนเทศที่จะนำไปใช้เพื่อการทดสอบในระบบสารสนเทศอย่างระมัดระวัง รวมทั้งมีแนวทางควบคุมและป้องกันข้อมูลรั่วไหล ๘.๗ ให้มีการจำกัดการเข้าถึงซอร์สโค้ด (Source code) ของโปรแกรม ๘.๘ หากมีการเปลี่ยนแปลงใด ๆ ในระบบปฏิบัติการคอมพิวเตอร์ให้มีการตรวจสอบทบทวนการทำงานของโปรแกรมที่มีความสำคัญ และทดสอบการใช้งานเพื่อให้มั่นใจว่าผลของการเปลี่ยนแปลงดังกล่าว จะไม่ส่งผลกระทบใด ๆ ต่อความมั่นคงปลอดภัยของระบบสารสนเทศและการให้บริการของหน่วยงาน ๘.๙ ให้มีการตรวจสอบ (Validate) การทำงานของแอพพลิเคชั่นเพื่อตรวจหาข้อผิดพลาดของข้อมูลที่อาจเกิดจากการทำงานหรือการประมวลผลที่ผิดพลาด ๘.๑๐ ให้มีข้อกำหนดขั้นต่ำสำหรับการรักษาความถูกต้องแท้จริง (Authenticity) และความถูกต้องครบถ้วน (Integrity) ของข้อมูลในแอพพลิเคชั่น รวมทั้งมีการระบุและปฏิบัติตามวิธีการป้องกันที่เหมาะสม ๘.๑๑ จัดให้มีนโยบายในการใช้งานเทคนิคที่เกี่ยวข้องกับการเข้ารหัสลับ ๘.๑๒ กำหนดให้มีขั้นตอนการปฏิบัติงานเพื่อควบคุมการติดตั้งซอฟต์แวร์บนระบบสารสนเทศที่ให้บริการ ๘.๑๓ ให้มีการควบคุมการเปลี่ยนแปลงต่าง ๆ ในการพัฒนาระบบสารสนเทศ โดยมีขั้นตอนการควบคุมที่เป็นทางการ ๘.๑๔ ให้จำกัดการเปลี่ยนแปลงใด ๆ ต่อซอฟต์แวร์ที่ใช้งาน (Software package) โดยให้เปลี่ยนแปลงเฉพาะเท่าที่จำเป็น และควบคุมทุก ๆ การเปลี่ยนแปลงอย่างเข้มงวด ๘.๑๕ มีมาตรการป้องกันเพื่อลดโอกาสที่เกิดการรั่วไหลของข้อมูลสารสนเทศ	
๙. การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด	
๙.๑ ให้มีการรายงานสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดผ่าน ช่องทางการบริหารจัดการที่เหมาะสมโดยเร็วที่สุด	

หัวข้อ	รายละเอียด
๙.๒ กำหนดให้พนักงานหรือผู้ใช้งานที่เป็นบุคคลภายนอก มีการบันทึกและรายงานจุดอ่อนใด ๆ ที่อาจสังเกตพบระหว่างการใช้งานระบบสารสนเทศ ๙.๓ กำหนดขอบเขตความรับผิดชอบของผู้บริหารและขั้นตอนการปฏิบัติงาน เพื่อตอบสนองต่อสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด อย่างรวดเร็ว มีระเบียบ และมีประสิทธิผล ๙.๔ หากในขั้นตอนการติดตามผลกับบุคคลหรือหน่วยงานภายหลังจากเกิดสถานการณ์ด้านความมั่นคง ปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ซึ่งเกี่ยวข้องกับการดำเนินการทางกฎหมาย (ไม่ว่าทางแพ่งหรือทาง อาญา) ให้มีการรวบรวม จัดเก็บ และนำเสนอหลักฐาน ให้สอดคล้องกับหลักเกณฑ์ของกฎหมายที่ใช้บังคับ	
๑๐. การบริหารจัดการด้านการบริการหรือการดำเนินงานของหน่วยงานหรือองค์กรเพื่อให้มีความต่อเนื่อง	
๑๐.๑ ให้กำหนดแผนเพื่อรักษาไว้หรือกู้คืนการให้บริการสารสนเทศ หลังเกิดเหตุการณ์ที่ทำให้ การดำเนินงานหยุดชะงัก เพื่อให้ข้อมูลสารสนเทศอยู่ในสภาพพร้อมใช้งานตามระดับที่กำหนดไว้ภายในระยะเวลาที่กำหนดไว้ ๑๐.๒ จัดให้มีข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศที่จำเป็น โดยกำหนดให้เป็นส่วนหนึ่งของขั้นตอนการบริหารจัดการเพื่อการดำเนินงานอย่างต่อเนื่องในภาวะฉุกเฉิน ๑๐.๓ กำหนดให้มีกรอบงานหลักสำหรับการพัฒนาแผนการบริหารจัดการเพื่อการดำเนินงานอย่างต่อเนื่องในภาวะฉุกเฉิน เพื่อให้การพัฒนาแผนต่าง ๆ เป็นไปในทิศทางเดียวกัน รวมทั้งสอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัย ตลอดจนมีการจัดลำดับความสำคัญก่อนหลังในการทดสอบและการดูแล ๑๐.๔ ให้มีการทดสอบและปรับปรุงแผนการบริหารจัดการเพื่อการดำเนินงานอย่างต่อเนื่องในภาวะฉุกเฉินอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าแผนดังกล่าวเป็นปัจจุบันและมีประสิทธิผลอยู่เสมอ ๑๐.๕ ให้มีการระบุเหตุการณ์ใด ๆ ที่อาจส่งผลให้การดำเนินงานหยุดชะงัก และความเป็นไปได้ในการเกิดผลกระทบ ตลอดจนผลต่อเนื่องจากการหยุดชะงักนั้นในแง่ของความมั่นคงปลอดภัยด้านสารสนเทศ	
๑๑. การตรวจสอบและการประเมินผลการปฏิบัติตามนโยบาย มาตรการ หลักเกณฑ์หรือกระบวนการใดๆ รวมทั้งข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศ	
๑๑.๑ ให้มีการระบุไว้ให้ชัดเจนถึงแนวทางในการดำเนินงานของระบบสารสนเทศที่มีความสอดคล้องตาม กฎหมายและข้อกำหนดตามสัญญาต่าง ๆ ของหน่วยงาน โดยต้องจัดทำเป็นเอกสาร และมีการปรับปรุงให้เป็นปัจจุบันอยู่เสมอ ๑๑.๒ ป้องกันมิให้มีการใช้งานระบบสารสนเทศผิดวัตถุประสงค์ ๑๑.๓ พนักงานของหน่วยงานต้องดูแลให้งานที่เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศที่อยู่ใน ขอบเขตความรับผิดชอบได้ดำเนินการไปโดยสอดคล้องกับกฎหมายและข้อกำหนดตามสัญญาต่าง ๆ ของหน่วยงาน ๑๑.๔ จัดให้มีการคุ้มครองข้อมูลส่วนบุคคลโดยให้สอดคล้องกับกฎหมายและข้อกำหนดตามสัญญาต่าง ๆ ของหน่วยงาน ๑๑.๕ ใช้เทคนิคการเข้ารหัสลับ ที่สอดคล้องกับกฎหมายและข้อกำหนดตามสัญญาต่าง ๆ ของหน่วยงาน ๑๑.๖ ให้มีการทบทวนตรวจสอบระบบสารสนเทศในด้านเทคนิคอย่างสม่ำเสมอ เพื่อให้สอดคล้องกับมาตรฐานการพัฒนางานด้านความมั่นคงปลอดภัยด้านสารสนเทศ ๑๑.๗ วางแผนและจัดให้มีข้อกำหนดการตรวจสอบและกิจกรรมที่เกี่ยวข้องกับการ	

หัวข้อ	รายละเอียด
ตรวจสอบระบบสารสนเทศ เพื่อลดความเสี่ยงในการเกิดการหยุดชะงักของการให้บริการ ๑๑.๘ ป้องกันการเข้าใช้งานเครื่องมือที่ใช้เพื่อการตรวจสอบ เพื่อมิให้เกิดการใช้งานผิดประเภทหรือถูกละเมิดการใช้งาน (Compromise) ๑๑.๙ กำหนดขั้นตอนปฏิบัติงานเพื่อให้มั่นใจว่าในการใช้งานข้อมูลที่อาจถือเป็นทรัพย์สินทางปัญญาหรือการใช้งานซอฟต์แวร์มีความสอดคล้องกับกฎหมายและข้อกำหนดตามสัญญาต่าง ๆ ๑๑.๑๐ ป้องกันมิให้ข้อมูลสารสนเทศที่สำคัญเกิดความเสียหาย สูญหายหรือถูกปลอมแปลง โดยให้สอดคล้องกับกฎหมาย ข้อกำหนดตามสัญญาต่าง ๆ ของหน่วยงาน และข้อกำหนดการให้บริการ	

(....) บริษัท .....

(....) นายหน้าประกันชีวิตหรือธนาคาร .....

(....) ผู้ให้บริการซึ่งเป็นบุคคลภายนอก.....

ขอรับรองว่าข้อความและข้อมูลตามหลักเกณฑ์ที่กำหนดในเอกสารฉบับนี้ถูกต้องตรงตามความเป็นจริงทุกประการ และยินดีนำส่งข้อมูลที่เกี่ยวข้องกับการตรวจสอบมาตรฐานของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

ประทับตรา (ถ้ามี)

ลงชื่อ .....

(.....)

กรรมการผู้มีอำนาจ/ผู้รับมอบอำนาจ*

*กรรมการผู้มีอำนาจ/ผู้รับมอบอำนาจของบริษัท/นายหน้าประกันชีวิตหรือธนาคาร หรือผู้ให้บริการซึ่งเป็นบุคคลภายนอก แล้วแต่กรณี

หมายเหตุ: หลักเกณฑ์ตามแนวทางทางการประเมินมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับเคร่งครัดฉบับนี้เป็นการเทียบเคียงหลักเกณฑ์ตามบัญชีแนบท้ายประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕ และในกรณีที่หลักเกณฑ์ตามบัญชีแนบท้ายประกาศฯ ดังกล่าวมีการปรับแก้ไขเพิ่มเติม ให้หลักเกณฑ์ตามแนวทางทางการประเมินมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับเคร่งครัดฉบับนี้ ปรับแก้ไขเพิ่มเติมและใช้บังคับโดยเป็นไปตามหลักเกณฑ์ที่ได้มีการปรับแก้ไขเพิ่มเติมดังกล่าว