



ประกาศสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจแพ่งกันภัย  
เรื่อง หลักเกณฑ์ วิธีการ และเงื่อนไขการขึ้นทะเบียนกิจกรรมทางอิเล็กทรอนิกส์  
การขอรับความเห็นชอบการใช้บริการบุคคลภายนอก และการรับรองระบบสารสนเทศ  
สำหรับธุรกิจแพ่งกันภัย  
พ.ศ. ๒๕๖๖

อาศัยอำนาจตามความในข้อ ๒๒ และข้อ ๒๓ แห่งประกาศคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจแพ่งกันภัย เรื่อง หลักเกณฑ์ วิธีการออก และเสนอขายกรมธรรม์แพ่งกันภัย และการชดใช้เงิน หรือค่าสินไหมทดแทนตามสัญญาแพ่งกันภัย โดยใช้วิธีการทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๖๖ สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจแพ่งกันภัย จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจแพ่งกันภัย เรื่อง หลักเกณฑ์ วิธีการ และ เงื่อนไขการขึ้นทะเบียนกิจกรรมทางอิเล็กทรอนิกส์ การขอรับความเห็นชอบการใช้บริการบุคคลภายนอก และการรับรองระบบสารสนเทศ สำหรับธุรกิจแพ่งกันภัย พ.ศ. ๒๕๖๖”

ข้อ ๒ ให้ยกเลิกประกาศสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจแพ่งกันภัยเรื่อง หลักเกณฑ์ วิธีการและเงื่อนไขการขึ้นทะเบียนกิจกรรมทางอิเล็กทรอนิกส์ การขอรับความเห็นชอบการใช้บริการบุคคลภายนอก และการรับรองระบบสารสนเทศ พ.ศ. ๒๕๖๐

ข้อ ๓ ประกาศนี้ให้ใช้บังคับตั้งแต่วันประกาศเป็นต้นไป

ข้อ ๔ ในประกาศนี้

“บริษัท” หมายความว่า บริษัทที่ได้รับใบอนุญาตประกอบธุรกิจแพ่งกันภัยตามกฎหมายว่าด้วยการแพ่งกันภัย และหมายความรวมถึงสาขาของบริษัทแพ่งกันภัยต่างประเทศที่ได้รับใบอนุญาตประกอบธุรกิจแพ่งกันภัยในราชอาณาจักรตามกฎหมายว่าด้วยการแพ่งกันภัย

“นายหน้าแพ่งกันภัย” หมายความว่า นายหน้าแพ่งกันภัยตามกฎหมายว่าด้วยการแพ่งกันภัย ไม่รวมถึงธนาคาร

“ธนาคาร” หมายความว่า ธนาคารที่ได้รับใบอนุญาตเป็นนายหน้าแพ่งกันภัยตามกฎหมายว่าด้วยการแพ่งกันภัย

“ผู้ให้บริการซึ่งเป็นบุคคลภายนอก” หมายความว่า ผู้ซึ่งมีระบบสารสนเทศไว้ให้บริการในการเสนอขายกรมธรรม์แพ่งกันภัยผ่านทางอิเล็กทรอนิกส์ (Online) การเสนอขาย

กรรมธรรม์ประกันภัยโดยใช้เครื่องมือทางอิเล็กทรอนิกส์ประกอบ การออกกรรมธรรม์ประกันภัยโดยใช้วิธีการทางอิเล็กทรอนิกส์ และการชดใช้เงินตามสัญญาประกันภัยโดยใช้วิธีการทางอิเล็กทรอนิกส์ ตามประกาศคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัยว่าด้วย หลักเกณฑ์ วิธีการออกและเสนอขายกรรมธรรม์ประกันภัย และการชดใช้เงินตามสัญญาประกันภัยโดยใช้วิธีการทางอิเล็กทรอนิกส์

“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 ที่เป็นอิสระจากหน่วยงานที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศที่ได้รับประกาศนียบัตร Certified Information System Auditor (CISA), Certified Information Security Manager (CISM), Certified Information System Security Professional (CISSP), ISO ๒๗๐๐๑ Lead Auditor

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

“สำนักงาน” หมายความว่า สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย

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

ข้อ ๖ ให้บริษัทที่ประสงค์จะขอขึ้นทะเบียนยื่นคำขอต่อสำนักงานตามแบบ อว. ๑ ที่แนบท้ายประกาศนี้ พร้อมเอกสารหลักฐานประกอบคำขอ ดังต่อไปนี้เป็นอย่างน้อย

(๑) เอกสารแสดงกิจกรรมและรายละเอียดที่ต้องการใช้วิธีการทางอิเล็กทรอนิกส์  
(๒) แผนผัง (Flow chart) และขั้นตอนของกิจกรรมที่ใช้วิธีการทางอิเล็กทรอนิกส์  
(๓) เอกสารแสดงระบบสารสนเทศและวิธีการทางอิเล็กทรอนิกส์ที่ใช้เพื่อรองรับกิจกรรมที่ใช้วิธีการทางอิเล็กทรอนิกส์

(๔) หนังสือรับรองการตรวจรับรองการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศในระดับเครื่องครัดสำหรับกิจกรรมตาม (๑) โดยผู้ตรวจสอบอิสระตามหนังสือรับรองตามแบบ อว. ๓ ที่แนบท้ายประกาศนี้ หรือประกาศนียบัตรที่ออกโดยหน่วยงานรับรองระบบสารสนเทศ ทั้งนี้ บริษัทต้องแสดงข้อมูลแก่สำนักงานจนเป็นที่พอใจได้ว่าระบบสารสนเทศที่ได้รับการรับรองตามประกาศนียบัตรดังกล่าว มีความมั่นคงปลอดภัยของระบบสารสนเทศในระดับเครื่องครัดสำหรับกิจกรรมตาม (๑)

(๕) เอกสารแนวทางการประเมินมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับเครื่องครัดตามหลักเกณฑ์ที่กำหนดในเอกสารแนบท้ายประกาศ (กรณีมีการตรวจรับรองจากผู้ตรวจสอบอิสระตามหนังสือรับรองตามแบบ อว. ๓)

ข้อ ๗ ให้นายหน้าประกันวินาศภัย หรือธนาคารที่ประสงค์จะขอขึ้นทะเบียนกิจกรรมทางอิเล็กทรอนิกส์ ยื่นคำขอต่อสำนักงานตามแบบ อว. ๒ ที่แนบท้ายประกาศนี้ พร้อมเอกสารหลักฐานประกอบคำขอ ดังต่อไปนี้เป็นอย่างน้อย

(๑) เอกสารแสดงกิจกรรมและรายละเอียดที่ต้องการใช้วิธีการทางอิเล็กทรอนิกส์

(๒) แผนผัง (Flow chart) และขั้นตอนของกิจกรรมที่ใช้วิธีการทางอิเล็กทรอนิกส์

(๓) เอกสารแสดงระบบสารสนเทศและวิธีการทางอิเล็กทรอนิกส์ที่ใช้เพื่อรองรับกิจกรรมที่ใช้วิธีการทางอิเล็กทรอนิกส์

(๔) หนังสือรับรองการตรวจรับรองการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของบริษัท และนายหน้าประกันวินาศภัย หรือธนาคาร ในระดับเครื่องครัดสำหรับกิจกรรม ตาม (๑) โดยผู้ตรวจสอบอิสระตามหนังสือรับรองตามแบบ อว. ๓ ที่แนบท้ายประกาศนี้ หรือ ประกาศนียบัตรที่ออกโดยหน่วยงานรับรองระบบสารสนเทศ ทั้งนี้ นายหน้าประกันวินาศภัย หรือธนาคาร ต้องแสดงข้อมูลแก่สำนักงานจนเป็นที่พอใจได้ว่าระบบสารสนเทศที่ได้รับการรับรองตามประกาศนียบัตรดังกล่าว มีความมั่นคงปลอดภัยของระบบสารสนเทศในระดับเครื่องครัด สำหรับกิจกรรมตาม (๑)

(๕) เอกสารแนวทางการประเมินมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับเครื่องครัดตามหลักเกณฑ์ที่กำหนดในเอกสารแนบท้ายประกาศ (กรณีมีการตรวจรับรองจากผู้ตรวจสอบอิสระตามหนังสือรับรองตามแบบ อว. ๓)

(๖) หนังสือยินยอมของบริษัทให้เสนอขายกรมธรรม์ประกันภัยผ่านทางอิเล็กทรอนิกส์ (Online)

ข้อ ๘ ในการขอขึ้นทะเบียนและขอรับความเห็นชอบการผู้ให้บริการซึ่งเป็นบุคคลภายนอก ให้บริษัท หรือนายหน้าประกันวินาศภัย หรือธนาคาร ดำเนินการยื่นคำขอต่อสำนักงานตามแบบ อว. ๔ ที่แนบท้ายประกาศนี้ พร้อมเอกสารหลักฐานประกอบคำขอ ดังต่อไปนี้เป็นอย่างน้อย

(๑) เอกสารแสดงกิจกรรมและรายละเอียดที่ต้องการใช้วิธีการทางอิเล็กทรอนิกส์

(๒) แผนผัง (Flow chart) และขั้นตอนของกิจกรรมที่ใช้วิธีการทางอิเล็กทรอนิกส์

(๓) เอกสารแสดงระบบสารสนเทศและวิธีการทางอิเล็กทรอนิกส์ที่ใช้เพื่อรองรับกิจกรรมที่ใช้วิธีการทางอิเล็กทรอนิกส์

(๔) หนังสือรับรองการตรวจรับรองการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของผู้ให้บริการซึ่งเป็นบุคคลภายนอก และของบริษัท นายหน้าประกันวินาศภัย หรือธนาคาร ในระดับเครื่องครัดสำหรับกิจกรรมตาม (๑) โดยผู้ตรวจสอบอิสระตามหนังสือรับรองตามแบบ อว. ๓ ที่แนบท้ายประกาศนี้ หรือประกาศนียบัตรที่ออกโดยหน่วยงานรับรองระบบสารสนเทศ ทั้งนี้ บริษัท นายหน้าประกันวินาศภัย หรือธนาคาร ต้องแสดงข้อมูลแก่สำนักงานจนเป็นที่พอใจได้ว่า ระบบสารสนเทศที่ได้รับการรับรอง

ตามประกาศนียบัตรดังกล่าว มีความมั่นคงปลอดภัยของระบบสารสนเทศในระดับเครื่องครัดสำหรับกิจกรรมตาม (๑)

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

(๖) สำเนาสัญญาใช้บริการระบบสารสนเทศระหว่างผู้ให้บริการซึ่งเป็นบุคคลภายนอก และบริษัท นายหน้าประกันวินาศภัย หรือธนาคาร แล้วแต่กรณี ซึ่งครอบคลุมเงื่อนไข ดังต่อไปนี้

(ก) มาตรการรักษาความมั่นคงปลอดภัยเพื่อคุ้มครองข้อมูลส่วนบุคคล ให้เป็นไปตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

(ข) การป้องกันการใช้หรือเปิดเผยโดยมิชอบ

(ค) การรายงานถึงความผิดปกติและการรายงานถึงการละเมิดข้อมูลส่วนบุคคล

(ง) ความรับผิดชอบในการแจ้งช่วงของผู้ให้บริการซึ่งเป็นบุคคลภายนอก โดยต้องกำหนดความรับผิดชอบของผู้ให้บริการซึ่งเป็นบุคคลภายนอกเสมือนหนึ่งเป็นผู้ดำเนินการเองหากมีการแจ้งช่วงตามสัญญา

(จ) สิทธิการตรวจสอบโดยบริษัทและสำนักงาน

(ฉ) การคืน ทำลาย หรือลบข้อมูลส่วนบุคคล

(ช) ผลของการละเมิดเงื่อนไข

(๗) เอกสารแนวทางการประเมินมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับเครื่องครัดตามหลักเกณฑ์ที่กำหนดในเอกสารแนบท้ายประกาศ (กรณีมีการตรวจรับรองจากผู้ตรวจสอบอิสระตามหนังสือรับรองตามแบบ อว. ๓)

(๘) หนังสือรับรองนิติบุคคลจากกรมพัฒนาธุรกิจการค้ากรณีผู้ให้บริการซึ่งเป็นบุคคลภายนอกเป็นนิติบุคคล

ข้อ ๙ ในกรณีที่บริษัท นายหน้าประกันวินาศภัย หรือธนาคาร ยื่นคำขอขึ้นทะเบียนกิจกรรมทางอิเล็กทรอนิกส์หรือคำขอรับความเห็นชอบการใช้บริการผู้ให้บริการซึ่งเป็นบุคคลภายนอกพร้อมเอกสารหลักฐานประกอบคำขอไม่ถูกต้องครบถ้วน สำนักงานจะแจ้งให้บริษัท นายหน้าประกันวินาศภัย หรือธนาคาร ดำเนินการแก้ไข หรือยื่นเอกสารหลักฐานประกอบคำขอเพิ่มเติม ภายในระยะเวลาที่สำนักงานกำหนด

หากไม่ดำเนินการแก้ไข หรือยื่นเอกสารหลักฐานประกอบคำขอเพิ่มเติมให้ถูกต้องครบถ้วนภายในระยะเวลาดังกล่าว โดยปราศจากเหตุอันสมควร สำนักงานมีสิทธิปฏิเสธการพิจารณาคำขอดังกล่าวได้

ข้อ ๑๐ ในการพิจารณาคำขอขึ้นทะเบียนกิจกรรมทางอิเล็กทรอนิกส์ หรือคำขอรับความเห็นชอบการใช้บริการผู้ให้บริการซึ่งเป็นบุคคลภายนอก สำนักงานจะพิจารณาคำขอให้แล้วเสร็จภายในสามสิบวันนับแต่วันที่รับคำขอพร้อมเอกสารประกอบคำขอครบถ้วนแล้ว หรือภายในสามสิบวันนับแต่วันที่บริษัทได้นำส่งคำขอและเอกสารประกอบคำขอที่มีการแก้ไขเพิ่มเติม ตามที่สำนักงานได้มี



ความเห็นหรือข้อสังเกตให้ปรับปรุงแก้ไข เว้นแต่กรณีจำเป็นหรือมีเหตุอันสมควร สำนักงานอาจขยายระยะเวลาออกไปก็ได้ ทั้งนี้ ไม่เกินสองครั้ง และครั้งละไม่เกินสิบห้าวัน และเมื่อได้รับความเห็นชอบแล้ว บริษัท นายหน้าประกันวินาศภัย หรือธนาคาร แล้วแต่กรณี ต้องดำเนินการให้เป็นไปตามที่ยื่นขอขึ้นทะเบียนหรือขอรับความเห็นชอบไว้ตลอดเวลา

ในกรณีมีการแก้ไขเพิ่มเติม หรือเปลี่ยนแปลงข้อมูลที่เคยได้รับความเห็นชอบให้ดำเนินการดังต่อไปนี้

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

(๒) ในกรณีบริษัท นายหน้าประกันวินาศภัย หรือธนาคาร ได้รับการขึ้นทะเบียนกิจกรรมการเสนอขายกรมธรรม์ประกันภัยผ่านทางอิเล็กทรอนิกส์ (Online) แล้ว และมีความประสงค์จะขอเพิ่มเติมผลิตภัณฑ์ประกันภัยประเภทกลุ่ม และประเภทอุตสาหกรรม ที่จะเสนอขายกรมธรรม์ประกันภัยผ่านทางอิเล็กทรอนิกส์ (Online) ให้บริษัท นายหน้าประกันวินาศภัย หรือธนาคาร ยื่นคำขอขึ้นทะเบียนหรือขอรับความเห็นชอบตามแบบ ปว. ๑ ปว. ๒ หรือ ปว. ๔ ที่แนบท้ายประกาศนี้ พร้อมเอกสารหลักฐานประกอบคำขอต่อสำนักงาน ทั้งนี้ บริษัท หรือนายหน้าประกันวินาศภัย หรือธนาคาร จะสามารถดำเนินการตามที่ยื่นขอรับความเห็นชอบดังกล่าวได้ก็ต่อเมื่อได้รับความเห็นชอบจากนายทะเบียนแล้ว

ข้อ ๑๑ ในการเสนอขายกรมธรรม์ประกันภัยผ่านทางอิเล็กทรอนิกส์ (Online) การเสนอขายกรมธรรม์ประกันภัยโดยใช้เครื่องมือทางอิเล็กทรอนิกส์ประกอบ การออกกรมธรรม์ประกันภัยโดยใช้วิธีการทางอิเล็กทรอนิกส์ หรือการชดใช้เงินตามสัญญาประกันภัยโดยใช้วิธีการทางอิเล็กทรอนิกส์ ให้บริษัท นายหน้าประกันวินาศภัย หรือธนาคาร แล้วแต่กรณี ต้องจัดให้มีการตรวจรับรองระบบสารสนเทศตามหลักเกณฑ์ ดังต่อไปนี้

(๑) จัดให้มีการตรวจรับรองระบบสารสนเทศเป็นประจำทุกปี ซึ่งเป็นการตรวจที่มีระยะเวลาห่างกันไม่เกินหนึ่งปี โดยต้องจัดให้มีการตรวจรับรองระบบสารสนเทศโดยผู้ตรวจสอบอิสระ หรือผู้ตรวจสอบภายในองค์กร หรือหน่วยงานรับรองระบบสารสนเทศ

(๒) จัดให้มีการตรวจรับรองระบบสารสนเทศทุกกรอบสามปี ซึ่งเป็นการตรวจที่มีระยะเวลาห่างกันไม่เกินสามปี โดยต้องจัดให้มีการตรวจรับรองระบบสารสนเทศโดยผู้ตรวจสอบอิสระ หรือหน่วยงานรับรองระบบสารสนเทศ

(๓) ในกรณีที่เป็นการขอขึ้นทะเบียนการทำธุรกรรมอิเล็กทรอนิกส์เป็นครั้งแรก หรือกรณีที่มีการแก้ไขระบบที่ได้มีการขึ้นทะเบียนธุรกรรมอย่างมีนัยสำคัญ หรือกรณีที่มีเหตุจำเป็นอย่างมีนัยสำคัญที่ต้องมีการตรวจรับรองระบบสารสนเทศเพิ่มเติม ต้องจัดให้มีการตรวจรับรองระบบสารสนเทศโดยผู้ตรวจสอบอิสระ หรือหน่วยงานรับรองระบบสารสนเทศ

ทั้งนี้ ให้บริษัท นายหน้าประกันวินาศภัย หรือธนาคาร แล้วแต่กรณี ส่งผลการตรวจภายในสามสิบวัน นับจากวันที่ได้รับการตรวจรับรองระบบสารสนเทศ และดำเนินการส่งหนังสือรับรองการตรวจรับรองการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศในระดับเคร่งครัด ที่จัดทำโดยผู้ตรวจสอบที่มีการตรวจรับรองระบบตามประเภทของการตรวจสอบในวรรคหนึ่ง ตามหนังสือรับรองตามแบบ อว. ๓ ที่แนบท้ายประกาศนี้ หรือส่งประกาศนียบัตรที่ออกโดยหน่วยงานรับรองระบบสารสนเทศต่อสำนักงาน

ประกาศ ณ วันที่ ๒๐ มิถุนายน พ.ศ. ๒๕๖๖



(นายสุทธิพล ทวีชัยการ)

เลขาธิการ

คณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย

**หมายเหตุ :-** เพื่อกำหนดหลักเกณฑ์และเงื่อนไขการขึ้นทะเบียน และการขอรับความเห็นชอบการรับรองระบบสารสนเทศ และกำหนดระดับมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ สำหรับการออกกรมธรรม์ประกันภัย การเสนอขายกรมธรรม์ประกันภัย การให้กู้ยืมเงิน และการชดใช้เงินตามสัญญาประกันภัย โดยใช้วิธีการทางอิเล็กทรอนิกส์

คำขอขึ้นทะเบียนกิจกรรมทางอิเล็กทรอนิกส์และการรับรองระบบสารสนเทศ  
(กรณีบริษัทประกันวินาศภัย)

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

๑. บริษัท ..... มีความประสงค์  
ขอขึ้นทะเบียนกิจกรรมทางอิเล็กทรอนิกส์ เพื่อใช้วิธีการทางอิเล็กทรอนิกส์ในเรื่อง
- (....) การเสนอขายกรมธรรม์ประกันภัยผ่านทางอิเล็กทรอนิกส์ (Online)
  - (....) การเสนอขายกรมธรรม์ประกันภัยโดยใช้เครื่องมือทางอิเล็กทรอนิกส์ประกอบ
  - (....) การออกกรมธรรม์ประกันภัยโดยใช้วิธีการทางอิเล็กทรอนิกส์
  - (....) การชดใช้เงิน หรือค่าสินไหมทดแทนตามสัญญาประกันภัยโดยใช้วิธีการทางอิเล็กทรอนิกส์

๒. บริษัทได้มอบหมายให้ นาย/นาง/นางสาว .....  
เป็นผู้ได้รับมอบหมายให้มีหน้าที่ดูแลรับผิดชอบงานด้านสารสนเทศที่เกี่ยวข้องตามที่ยื่นขอขึ้น  
ทะเบียนหรือขอรับความเห็นชอบในครั้งนี้ ติดต่อ โทร.....Email.....

๓. บริษัทขอรับรองว่าระบบสารสนเทศของบริษัทมีมาตรฐานความมั่นคงและปลอดภัยในระดับ  
เครื่องครัดสำหรับกิจกรรมตามข้อ ๑. โดยได้รับการตรวจสอบและรับรองจากผู้ตรวจสอบอิสระตามหนังสือ  
รับรองตามแบบ อว. ๓ หรือประกาศนียบัตรรับรองระบบบริหารจัดการความมั่นคงปลอดภัย  
สารสนเทศ ISO/IEC ๒๗๐๐๑ (ISMS : Information Security Management system)

๔. บริษัทได้แนบเอกสาร โดยมีรายการดังต่อไปนี้

- (....) เอกสารแสดงกิจกรรมและรายละเอียดที่ต้องการใช้วิธีการทางอิเล็กทรอนิกส์ (ตัวอย่าง  
หน้าจอ)
- (....) แผนผัง (Flow chart) และขั้นตอนของกิจกรรมที่ใช้วิธีการทางอิเล็กทรอนิกส์
- (....) เอกสารแสดงระบบสารสนเทศและวิธีการทางอิเล็กทรอนิกส์ที่ใช้เพื่อรองรับกิจกรรมที่ใช้  
วิธีการทางอิเล็กทรอนิกส์ (system architecture)
- (....) หนังสือรับรองการตรวจรับรองการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ  
โดยผู้ตรวจสอบอิสระตามแบบ อว. ๓ หรือประกาศนียบัตรที่ออกโดยหน่วยงานรับรองระบบ  
สารสนเทศ (ISO๒๗๐๐๑)
- (....) เอกสารแนวทางการประเมินมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตาม  
วิธีการแบบปลอดภัยในระดับเครื่องครัดตามหลักเกณฑ์ที่กำหนดในเอกสารแนบท้ายประกาศ (กรณีมี  
การตรวจรับรองจากผู้ตรวจสอบอิสระตามหนังสือรับรองตามแบบ อว. ๓)

บริษัท ..... ขอรับรองว่า ข้อความและ  
ข้อมูลในแบบ อว. ๑ นี้ ถูกต้องตรงตามความเป็นจริงทุกประการ

ประทับตรา (ถ้ามี)

ลงชื่อ .....  
(.....)

กรรมการผู้มีอำนาจ/ ผู้รับมอบอำนาจของบริษัท

คำขอขึ้นทะเบียนกิจกรรมทางอิเล็กทรอนิกส์และการรับรองระบบสารสนเทศ  
(กรณีนายหน้าประกันวินาศภัยหรือธนาคาร)

เขียนที่ .....

วันที่ ..... เดือน..... พ.ศ. ....

๑. ข้าพเจ้า .....ซึ่งมีใบอนุญาต  
เป็นนายหน้าประกันวินาศภัย เลขที่ ..... ใบอนุญาตหมดอายุ.....

มีความประสงค์ขอขึ้นทะเบียนกิจกรรมทางอิเล็กทรอนิกส์ เพื่อใช้วิธีการทางอิเล็กทรอนิกส์ในเรื่อง

(...) การเสนอขายกรมธรรม์ประกันภัยผ่านทางอิเล็กทรอนิกส์ (Online) ซึ่งได้รับความยินยอม  
จากบริษัท..... ในการทำกิจกรรม

(...) การเสนอขายกรมธรรม์ประกันภัยโดยใช้เครื่องมือทางอิเล็กทรอนิกส์ประกอบ

๒. ข้าพเจ้าได้มอบหมายให้ นาย/นาง/นางสาว .....เป็น  
ผู้ได้รับมอบหมายให้มีหน้าที่ดูแลรับผิดชอบงานด้านสารสนเทศที่เกี่ยวข้องตามที่ยื่นขอขึ้นทะเบียน  
หรือขอรับความเห็นชอบในครั้งนี้ ติดต่อ โทร.....Email.....

๓. ข้าพเจ้าขอรับรองว่าระบบสารสนเทศของข้าพเจ้ามีมาตรฐานความมั่นคงและปลอดภัยในระดับ  
เครื่องครัดสำหรับกิจกรรมตามข้อ ๑. ตามหลักเกณฑ์ที่กำหนดในเอกสารแนบท้ายประกาศนี้ โดยได้รับ  
การตรวจสอบและรับรองจากผู้ตรวจสอบอิสระตามหนังสือรับรองตามแบบ อว. ๓ หรือประกาศนียบัตร  
รับรองระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ISO/IEC ๒๗๐๐๑ (ISMS : Information  
Security Management system)

๔. ข้าพเจ้าได้แนบเอกสาร โดยมีรายการดังต่อไปนี้

(...) เอกสารแสดงกิจกรรมและรายละเอียดที่ต้องการใช้วิธีการทางอิเล็กทรอนิกส์ (ตัวอย่าง  
หน้าจอ)

(...) แผนผัง (Flow chart) และขั้นตอนของกิจกรรมที่ใช้วิธีการทางอิเล็กทรอนิกส์

(...) เอกสารแสดงระบบสารสนเทศและวิธีการทางอิเล็กทรอนิกส์ที่ใช้เพื่อรองรับกิจกรรมที่ใช้  
วิธีการทางอิเล็กทรอนิกส์ (system architecture)

(...) หนังสือรับรองการตรวจรับรองการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของ  
ข้าพเจ้าโดยผู้ตรวจสอบอิสระตามแบบ อว. ๓ หรือประกาศนียบัตรที่ออกโดยหน่วยงานรับรองระบบ  
สารสนเทศ (ISO๒๗๐๐๑)

(...) เอกสารแนวทางการประเมินมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ  
ตามวิธีการแบบปลอดภัยในระดับเครื่องครัดตามหลักเกณฑ์ที่กำหนดในเอกสารแนบท้ายประกาศ  
(กรณีมีการตรวจรับรองจากผู้ตรวจสอบอิสระตามหนังสือรับรองตามแบบ อว. ๓)

(...) หนังสือยินยอมของบริษัทให้เสนอขายกรมธรรม์ประกันภัยผ่านทางอิเล็กทรอนิกส์ (Online)

ข้าพเจ้า..... ขอรับรองว่าข้อความ  
และข้อมูลในแบบ อว. ๒ นี้ ถูกต้องตรงตามความเป็นจริงทุกประการ

ประทับตรา (ถ้ามี)

ลงชื่อ .....

(.....)

กรรมการผู้มีอำนาจ/

ผู้รับมอบอำนาจของนายหน้าประกันวินาศภัยหรือธนาคาร

หนังสือรับรอง

การตรวจรับรองการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศโดยผู้ตรวจสอบอิสระ

เขียนที่ .....

วันที่ ..... เดือน..... พ.ศ. ....

๑. (...) ข้าพเจ้า .....ได้รับประกาศนียบัตรหลักสูตร  
..... (CISA, CISM , CISSP แล้วแต่กรณี)..... ประกาศนียบัตร  
หมดอายุ..... และได้แนบสำเนาประกาศนียบัตรมาพร้อมนี้ (กรณีบุคคล  
ธรรมดา)

(...) หน่วยงานรับรองระบบสารสนเทศ (ชื่อ).....เป็นหน่วยงานรับรอง  
ระบบสารสนเทศ ที่ไม่อยู่ระหว่างการถูกระงับหรือเพิกถอนการขึ้นทะเบียน และได้รับการขึ้นทะเบียน  
จากหน่วยงาน..... และได้แนบ  
สำเนาเอกสารการขึ้นทะเบียนมาด้วยพร้อมกันนี้

๒. ข้าพเจ้าขอรับรองว่าได้ตรวจสอบระบบสารสนเทศของ

(...) บริษัท .....

(...) นายหน้าประกันวินาศภัยหรือธนาคาร.....

(...) ผู้ให้บริการซึ่งเป็นบุคคลภายนอก.....

เพื่อใช้วิธีการทางอิเล็กทรอนิกส์ในเรื่อง

(....) การเสนอขายกรมธรรม์ประกันภัยผ่านทางอิเล็กทรอนิกส์ (Online)

(....) การเสนอขายกรมธรรม์ประกันภัยใช้เครื่องมือทางอิเล็กทรอนิกส์ประกอบ

(....) การออกกรมธรรม์ประกันภัยโดยใช้วิธีการทางอิเล็กทรอนิกส์

(....) การชดใช้เงิน หรือค่าสินไหมทดแทนตามสัญญาประกันภัยโดยใช้วิธีการทางอิเล็กทรอนิกส์

มีมาตรฐานความมั่นคงและปลอดภัยตามแนวทางการประเมินมาตรฐานการรักษาความมั่นคง  
ปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับเคร่งครัดที่แนบท้ายประกาศนี้

๓. ข้าพเจ้าได้ตรวจสอบระบบสารสนเทศเป็นที่เรียบร้อยแล้วตามหลักวิชาชีพและตามมาตรฐานที่  
อ้างอิงตามประกาศสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง  
หลักเกณฑ์ วิธีการ และเงื่อนไขการขึ้นทะเบียนกิจกรรมทางอิเล็กทรอนิกส์ การขอรับความเห็นชอบ  
การใช้บริการบุคคลภายนอก และการรับรองระบบสารสนเทศ พ.ศ. ๒๕๖๕ และยินยอมให้สำนักงาน  
สามารถตรวจสอบความถูกต้องของข้อมูลประกาศนียบัตรกับหน่วยงานออกประกาศนียบัตรหรือ  
เอกสารการขึ้นทะเบียนหน่วยงานรับรองระบบสารสนเทศกับหน่วยงานขึ้นทะเบียนตามข้อ ๑. ได้  
ข้าพเจ้าจึงลงลายมือชื่อไว้เป็นหลักฐาน

ประทับตรา (ถ้ามี)

ลงชื่อ .....

(.....)

ผู้ตรวจสอบอิสระ/หน่วยงานรับรองระบบสารสนเทศ

๔. ข้าพเจ้าซึ่งเป็นบุคคลตามข้อ ๒. ขอรับรองว่าข้อมูลที่ได้ให้แก่ผู้ตรวจสอบอิสระเพื่อใช้ตรวจรับรองการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศเป็นข้อมูลที่ถูกต้องตรงตามความเป็นจริงทุกประการ จึงได้ลงลายมือชื่อไว้เป็นหลักฐาน

ประทับตรา (ถ้ามี)

ลงชื่อ .....

(.....)

กรรมการผู้มีอำนาจ/ผู้รับมอบอำนาจ\*

\*กรรมการผู้มีอำนาจ/ผู้รับมอบอำนาจของบริษัท/นายหน้าประกันวินาศภัยหรือธนาคาร หรือผู้ให้บริการซึ่งเป็นบุคคลภายนอก แล้วแต่กรณี

คำขอรับความเห็นชอบการใช้บริการบุคคลภายนอก และการรับรองระบบสารสนเทศ

## ส่วนที่ ๑ กรณีบริษัทใช้บริการบุคคลภายนอก

๑. บริษัท .....

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

(....) การเสนอขายกรมธรรม์ประกันภัยผ่านทางอิเล็กทรอนิกส์ (Online)

(....) การเสนอขายกรมธรรม์ประกันภัยโดยใช้เครื่องมือทางอิเล็กทรอนิกส์ประกอบ

(....) การออกกรมธรรม์ประกันภัยโดยใช้วิธีการทางอิเล็กทรอนิกส์

(....) การชดใช้เงิน หรือค่าสินไหมทดแทนตามสัญญาประกันภัยโดยใช้วิธีการทางอิเล็กทรอนิกส์

๒. บริษัทขอรับรองว่า

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

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

๒.๒ ได้กำหนดนโยบาย กระบวนการและวิธีปฏิบัติที่ชัดเจน เช่น ระบบการประเมินความเสี่ยง การบริหารความเสี่ยง ขั้นตอนของการบริการ การควบคุมภายใน การรักษาความปลอดภัย และแผนรองรับกรณีบุคคลภายนอกไม่สามารถให้บริการได้

๒.๓ สัญญาใช้บริการระบบสารสนเทศระหว่างบริษัทกับผู้ให้บริการซึ่งเป็นบุคคลภายนอกครอบคลุมเงื่อนไข ดังต่อไปนี้

(ก) มาตรการรักษาความมั่นคงปลอดภัยเพื่อคุ้มครองข้อมูลส่วนบุคคล ให้เป็นไปตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

(ข) การป้องกันการใช้หรือเปิดเผยโดยมิชอบ

(ค) การรายงานถึงความผิดปกติและการรายงานถึงการละเมิดข้อมูลส่วนบุคคล

(ง) ความรับผิดชอบในการแจ้งช่วงของผู้ให้บริการภายนอก โดยต้องกำหนดความรับผิดชอบของผู้ให้บริการบุคคลภายนอกเสมือนหนึ่งเป็นผู้ดำเนินการเอง หากมีการแจ้งช่วงตามสัญญา

(จ) สิทธิการตรวจสอบโดยบริษัทและสำนักงาน

(ฉ) การคืน ทำลาย หรือลบข้อมูลส่วนบุคคล

(ช) ผลของการละเมิดเงื่อนไข

๓. บริษัทได้แนบเอกสาร โดยมีรายการดังต่อไปนี้
- (....) หนังสือรับรองนิติบุคคลจากกรมพัฒนาธุรกิจการค้ากรณีผู้ให้บริการซึ่งเป็นบุคคลภายนอกเป็นนิติบุคคล
  - (....) เอกสารแสดงกิจกรรมและรายละเอียดที่ต้องการใช้วิธีการทางอิเล็กทรอนิกส์ (ตัวอย่าง หน้าจอ)
  - (....) แผนผัง (Flow chart) และขั้นตอนของกิจกรรมที่ใช้วิธีการทางอิเล็กทรอนิกส์
  - (....) เอกสารแสดงระบบสารสนเทศและวิธีการทางอิเล็กทรอนิกส์ที่ใช้เพื่อรองรับกิจกรรมที่ใช้วิธีการทางอิเล็กทรอนิกส์ (system architecture)
  - (....) หนังสือรับรองการตรวจรับรองการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของผู้ให้บริการซึ่งเป็นบุคคลภายนอกโดยผู้ตรวจสอบอิสระตามแบบ อว. ๓ หรือประกาศนียบัตรที่ออกโดยหน่วยงานรับรองระบบสารสนเทศ (ISO๒๗๐๐๑)
  - (....) หนังสือรับรองการตรวจรับรองการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของบริษัท โดยผู้ตรวจสอบอิสระตามแบบ อว. ๓ หรือประกาศนียบัตรที่ออกโดยหน่วยงานรับรองระบบสารสนเทศ (ISO๒๗๐๐๑)
  - (....) เอกสารแนวทางการประเมินมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับเครื่องครัดตามหลักเกณฑ์ที่กำหนดในเอกสารแนบท้ายประกาศ (กรณีมีการตรวจรับรองจากผู้ตรวจสอบอิสระตามหนังสือรับรองตามแบบ อว. ๓)
  - (....) สำเนาสัญญาให้บริการระบบสารสนเทศระหว่างบริษัทกับผู้ให้บริการซึ่งเป็นบุคคลภายนอก

## ส่วนที่ ๒ กรณีนายหน้าประกันวินาศภัยหรือธนาคารให้บริการบุคคลภายนอก

๔. ข้าพเจ้า .....ซึ่งมีใบอนุญาตเป็นนายหน้าประกันวินาศภัย เลขที่ ..... ใบอนุญาตหมดอายุ.....มีความประสงค์ขอขึ้นทะเบียนกิจกรรมทางอิเล็กทรอนิกส์และขอรับความเห็นชอบในการให้บริการระบบสารสนเทศของผู้ให้บริการซึ่งเป็นบุคคลภายนอก.....(ระบุชื่อผู้ให้บริการ).....เพื่อใช้วิธีการทางอิเล็กทรอนิกส์ในเรื่อง
- (....) การเสนอขายกรมธรรม์ประกันภัยผ่านทางอิเล็กทรอนิกส์ (Online) ซึ่งได้รับความยินยอมจากบริษัท..... ในการทำงานกิจกรรม
  - (....) การเสนอขายกรมธรรม์ประกันภัยโดยใช้เครื่องมือทางอิเล็กทรอนิกส์ประกอบ และได้รับความยินยอมจากบริษัท.....ในกิจกรรมข้างต้น
๕. ข้าพเจ้าขอรับรองว่า

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

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



๕.๒ ได้กำหนดนโยบาย กระบวนการและวิธีปฏิบัติที่ชัดเจน เช่น ระบบการประเมินความเสี่ยง การบริหารความเสี่ยง ขั้นตอนของการบริการ การควบคุมภายใน การรักษาความปลอดภัย และแผนรองรับกรณีที่เกิดบุคคลภายนอกไม่สามารถให้บริการได้

๕.๓ สัญญาให้บริการระบบสารสนเทศระหว่างข้าพเจ้ากับผู้ให้บริการซึ่งเป็นบุคคลภายนอก ครอบคลุมเงื่อนไข ดังต่อไปนี้

(ก) มาตรการรักษาความมั่นคงปลอดภัยเพื่อคุ้มครองข้อมูลส่วนบุคคล ให้เป็นไปตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

(ข) การป้องกันการใช้หรือเปิดเผยโดยมิชอบ

(ค) การรายงานถึงความผิดปกติและการรายงานถึงการละเมิดข้อมูลส่วนบุคคล

(ง) ความรับผิดชอบในการแจ้งช่วงของผู้ให้บริการภายนอก โดยต้องกำหนดความรับผิดชอบของผู้ให้บริการบุคคลภายนอกเสมือนหนึ่งเป็นผู้ดำเนินการเอง หากมีการแจ้งช่วงตามสัญญา

(จ) สิทธิการตรวจสอบโดยบริษัทและสำนักงาน

(ฉ) การคืน ทำลาย หรือลบข้อมูลส่วนบุคคล

(ช) ผลของการละเมิดเงื่อนไข

๖. ข้าพเจ้าได้แนบเอกสาร โดยมีรายการดังต่อไปนี้

(...) หนังสือรับรองนิติบุคคลจากกรมพัฒนาธุรกิจการค้ากรณีผู้ให้บริการซึ่งเป็นบุคคลภายนอกเป็นนิติบุคคล

(...) เอกสารแสดงกิจกรรมและรายละเอียดที่ต้องการใช้วิธีการทางอิเล็กทรอนิกส์ (ตัวอย่าง หน้าจอ)

(...) แผนผัง (Flow chart) และขั้นตอนของกิจกรรมที่ใช้วิธีการทางอิเล็กทรอนิกส์

(...) เอกสารแสดงระบบสารสนเทศและวิธีการทางอิเล็กทรอนิกส์ที่ใช้เพื่อรองรับกิจกรรมที่ใช้วิธีการทางอิเล็กทรอนิกส์ (system architecture)

(...) หนังสือรับรองการตรวจรับรองการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของผู้ให้บริการซึ่งเป็นบุคคลภายนอกโดยผู้ตรวจสอบอิสระตามแบบ อว. ๓ หรือตามประกาศนียบัตรที่ออกโดยหน่วยงานรับรองระบบสารสนเทศ (ISO๒๗๐๐๑)

(...) หนังสือรับรองการตรวจรับรองการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของข้าพเจ้าโดยผู้ตรวจสอบอิสระตามแบบ อว. ๓ หรือตามประกาศนียบัตรที่ออกโดยหน่วยงานรับรองระบบสารสนเทศ (ISO๒๗๐๐๑)

(...) เอกสารแนวทางการประเมินมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับเครื่องครัดตามหลักเกณฑ์ที่กำหนดในเอกสารแนบท้ายประกาศ (กรณีมีการตรวจรับรองจากผู้ตรวจสอบอิสระตามหนังสือรับรองตามแบบ อว. ๓)

(...) สำเนาสัญญาให้บริการระบบสารสนเทศระหว่างข้าพเจ้ากับผู้ให้บริการซึ่งเป็นบุคคลภายนอก

(...) หนังสือยินยอมของบริษัทให้เสนอขายกรรมธรรม์ประกันภัยผ่านทางอิเล็กทรอนิกส์ (Online)

บริษัท  นายหน้าประกันวินาศภัยหรือธนาคาร .....

ขอรับรองว่า ข้อความและข้อมูลในแบบ อว. ๔ นี้ ถูกต้องตรงตามความเป็นจริงทุกประการ

ประทับตรา (ถ้ามี)

ลงชื่อ .....

(.....)

กรรมการผู้มีอำนาจ/ผู้รับมอบอำนาจ\*

\*กรรมการผู้มีอำนาจ/ผู้รับมอบอำนาจของบริษัท/นายหน้าประกันวินาศภัยหรือธนาคาร แล้วแต่กรณี

แบบการแจ้งเปลี่ยนแปลงและการรับรองระบบสารสนเทศ  
(กรณีบริษัทประกันวินาศภัย)

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

๑. บริษัท ..... มีความประสงค์  
แจ้งเปลี่ยนแปลงการขึ้นทะเบียนกิจกรรมทางอิเล็กทรอนิกส์ ในเรื่อง  
(....) การเสนอขายกรมธรรม์ประกันภัยผ่านทางอิเล็กทรอนิกส์ (Online)  
(....) การเสนอขายกรมธรรม์ประกันภัยโดยใช้เครื่องมือทางอิเล็กทรอนิกส์ประกอบ  
(....) การออกกรมธรรม์ประกันภัยโดยใช้วิธีการทางอิเล็กทรอนิกส์  
(....) การชดใช้เงิน หรือค่าสินไหมทดแทนตามสัญญาประกันภัยโดยใช้วิธีการทางอิเล็กทรอนิกส์  
รายละเอียดที่เปลี่ยนแปลง.....

๒. บริษัทได้มอบหมายให้ นาย/นาง/นางสาว .....เป็นผู้  
ได้รับมอบหมายให้มีหน้าที่ดูแลรับผิดชอบงานด้านสารสนเทศที่เกี่ยวข้องตามที่ยื่นขอขึ้นทะเบียน  
หรือขอรับความเห็นชอบในครั้งนี้ ติดต่อ โทร.....Email.....

๓. บริษัทขอรับรองว่าระบบสารสนเทศของบริษัทมีมาตรฐานความมั่นคงและปลอดภัยในระดับ  
เครื่องครัดสำหรับกิจกรรมตามข้อ ๑. โดยได้รับการตรวจสอบและรับรองจากผู้ตรวจสอบอิสระตามหนังสือ  
รับรองตามแบบ อว. ๓ หรือตามประกาศนียบัตรที่ออกโดยหน่วยงานรับรองระบบสารสนเทศ  
(ISO๒๗๐๐๑)

๔. บริษัทได้แนบเอกสาร โดยมีรายการดังต่อไปนี้ (เฉพาะที่มีการแก้ไข)  
(....) เอกสารแสดงกิจกรรมและรายละเอียดที่ต้องการใช้วิธีการทางอิเล็กทรอนิกส์ (ตัวอย่าง  
หน้าจอ)

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

(....) เอกสารแสดงระบบสารสนเทศและวิธีการทางอิเล็กทรอนิกส์ที่ใช้เพื่อรองรับกิจกรรมที่ใช้  
วิธีการทางอิเล็กทรอนิกส์ (system architecture)

(....) หนังสือรับรองการตรวจรับรองการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ  
โดยผู้ตรวจสอบอิสระตามแบบ อว. ๓ หรือประกาศนียบัตรที่ออกโดยหน่วยงานรับรองระบบ  
สารสนเทศ (ISO๒๗๐๐๑)

(....) เอกสารแนวทางการประเมินมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตาม  
วิธีการแบบปลอดภัยในระดับเครื่องครัดตามหลักเกณฑ์ที่กำหนดในเอกสารแนบท้ายประกาศ (กรณีมี  
การตรวจรับรองจากผู้ตรวจสอบอิสระตามหนังสือรับรองตามแบบ อว. ๓)

บริษัท ..... ขอรับรองว่า ข้อความและ  
ข้อมูลในแบบ ปว. ๑ นี้ ถูกต้องตรงตามความเป็นจริงทุกประการ

ประทับตรา (ถ้ามี)

ลงชื่อ .....  
(.....)

กรรมการผู้มีอำนาจ/  
ผู้รับมอบอำนาจของบริษัท

แบบการแจ้งเปลี่ยนแปลงและการรับรองระบบสารสนเทศ  
(กรณีนายหน้าประกันวินาศภัยหรือธนาคาร)

เขียนที่ .....

วันที่ ..... เดือน..... พ.ศ. ....

๑. ข้าพเจ้า .....ซึ่งมีใบอนุญาต  
เป็นนายหน้าประกันวินาศภัย เลขที่ ..... ใบอนุญาตหมดอายุ.....  
มีความประสงค์แจ้งเปลี่ยนแปลงการขึ้นทะเบียนกิจกรรมทางอิเล็กทรอนิกส์ ในเรื่อง  
(...) การเสนอขายกรมธรรม์ประกันภัยผ่านทางอิเล็กทรอนิกส์ (Online) ซึ่งได้รับความยินยอม  
จากบริษัท..... ในการทำกิจกรรม  
(...) การเสนอขายกรมธรรม์ประกันภัยโดยใช้เครื่องมือทางอิเล็กทรอนิกส์ประกอบ  
รายละเอียดที่เปลี่ยนแปลง.....

๒. ข้าพเจ้าได้มอบหมายให้ นาย/นาง/นางสาว .....เป็น  
ผู้ได้รับมอบหมายให้มีหน้าที่ดูแลรับผิดชอบงานด้านสารสนเทศที่เกี่ยวข้องตามที่แจ้งเปลี่ยนแปลงการ  
ขึ้นทะเบียนหรือขอรับความเห็นชอบในครั้งนี้ ติดต่อ โทร.....Email.....

๓. ข้าพเจ้าขอรับรองว่าระบบสารสนเทศของข้าพเจ้ามีมาตรฐานความมั่นคงและปลอดภัยในระดับ  
เครื่องครัดสำหรับกิจกรรมตามข้อ ๑. ตามหลักเกณฑ์ที่กำหนดในเอกสารแนบท้ายประกาศนี้ โดยได้รับ  
การตรวจสอบและรับรองจากผู้ตรวจสอบอิสระตามหนังสือรับรองตามแบบ อว. ๓ หรือตามประกาศนียบัตรที่  
ออกโดยหน่วยงานรับรองระบบสารสนเทศ (ISO๒๗๐๐๑)

๔. ข้าพเจ้าได้แนบเอกสาร โดยมีรายการดังต่อไปนี้ (เฉพาะที่แก้ไข)  
(...) เอกสารแสดงกิจกรรมและรายละเอียดที่ต้องการใช้วิธีการทางอิเล็กทรอนิกส์ (ตัวอย่าง  
หน้าจอ)

(...) แผนผัง (Flow chart) และขั้นตอนของกิจกรรมที่ใช้วิธีการทางอิเล็กทรอนิกส์  
(...) เอกสารแสดงระบบสารสนเทศและวิธีการทางอิเล็กทรอนิกส์ที่ใช้เพื่อรองรับกิจกรรมที่ใช้  
วิธีการทางอิเล็กทรอนิกส์ (system architecture)

(...) หนังสือรับรองการตรวจรับรองการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของ  
ข้าพเจ้าโดยผู้ตรวจสอบอิสระตามแบบ อว. ๓ หรือประกาศนียบัตรที่ออกโดยหน่วยงานรับรองระบบ  
สารสนเทศ (ISO๒๗๐๐๑)

(...) เอกสารแนวทางการประเมินมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ  
ตามวิธีการแบบปลอดภัยในระดับเครื่องครัดตามหลักเกณฑ์ที่กำหนดในเอกสารแนบท้ายประกาศ  
(กรณีมีการตรวจรับรองจากผู้ตรวจสอบอิสระตามหนังสือรับรองตามแบบ อว. ๓)

(...) หนังสือยินยอมของบริษัทให้เสนอขายกรมธรรม์ประกันภัยผ่านทางอิเล็กทรอนิกส์ (Online)

ข้าพเจ้า..... ขอรับรองว่าข้อความ  
และข้อมูลในแบบ ปว. ๒ นี้ ถูกต้องตรงตามความเป็นจริงทุกประการ

ประทับตรา (ถ้ามี)

ลงชื่อ .....

(.....)

กรรมการผู้มีอำนาจ/  
ผู้รับมอบอำนาจของนายหน้าประกันวินาศภัยหรือธนาคาร

## แบบการแจ้งเปลี่ยนแปลงและการรับรองระบบสารสนเทศ

## ส่วนที่ ๑ กรณีบริษัทให้บริการบุคคลภายนอก

๑. บริษัท .....

มีความประสงค์แจ้งเปลี่ยนแปลงการขึ้นทะเบียนกิจกรรมทางอิเล็กทรอนิกส์และการให้บริการระบบสารสนเทศของผู้ให้บริการซึ่งเป็นบุคคลภายนอก.....(ระบุชื่อผู้ให้บริการ).....ในเรื่อง

(....) การเสนอขายกรมธรรม์ประกันภัยผ่านทางอิเล็กทรอนิกส์ (Online)

(....) การเสนอขายกรมธรรม์ประกันภัยโดยใช้เครื่องมือทางอิเล็กทรอนิกส์ประกอบ

(....) การออกกรมธรรม์ประกันภัยโดยใช้วิธีการทางอิเล็กทรอนิกส์

(....) การขอใช้เงิน หรือค่าสินไหมทดแทนตามสัญญาประกันภัยโดยใช้วิธีการทางอิเล็กทรอนิกส์

รายละเอียดที่เปลี่ยนแปลง.....

๒. บริษัทขอรับรองว่า

๒.๑ ผู้ให้บริการซึ่งเป็นบุคคลภายนอกมีระบบสารสนเทศที่มีมาตรฐานความมั่นคงและปลอดภัยในระดับเครื่องครัดสำหรับกิจกรรมตามข้อ ๑. ตามหลักเกณฑ์ที่กำหนดในเอกสารแนบท้ายประกาศนี้ โดยได้รับการตรวจสอบและรับรองจากผู้ตรวจสอบอิสระตามหนังสือรับรองตามแบบ อว. ๓ หรือตามประกาศนียบัตรที่ออกโดยหน่วยงานรับรองระบบสารสนเทศ (ISO๒๗๐๐๑) และ

บริษัทมีระบบสารสนเทศที่มีมาตรฐานความมั่นคงและปลอดภัยในระดับเครื่องครัดสำหรับกิจกรรมตามข้อ ๑. ตามหลักเกณฑ์ที่กำหนดในเอกสารแนบท้ายประกาศนี้ โดยได้รับการตรวจสอบและรับรองจากผู้ตรวจสอบอิสระตามหนังสือรับรองตามแบบ อว. ๓ หรือตามประกาศนียบัตรที่ออกโดยหน่วยงานรับรองระบบสารสนเทศ (ISO๒๗๐๐๑)

๒.๒ ได้กำหนดนโยบาย กระบวนการและวิธีปฏิบัติที่ชัดเจน เช่น ระบบการประเมินความเสี่ยง การบริหารความเสี่ยง ขั้นตอนของการบริการ การควบคุมภายใน การรักษาความปลอดภัย และแผนรองรับกรณีบุคคลภายนอกไม่สามารถให้บริการได้

๒.๓ สัญญาให้บริการระบบสารสนเทศระหว่างบริษัทกับผู้ให้บริการซึ่งเป็นบุคคลภายนอกครอบคลุมเงื่อนไข ดังต่อไปนี้

(ก) มาตรการรักษาความมั่นคงปลอดภัยเพื่อคุ้มครองข้อมูลส่วนบุคคล ให้เป็นไปตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

(ข) การป้องกันการใช้หรือเปิดเผยโดยมิชอบ

(ค) การรายงานถึงความผิดปกติและการรายงานถึงการละเมิดข้อมูลส่วนบุคคล

(ง) ความรับผิดชอบในการแจ้งช่วงของผู้ให้บริการภายนอก โดยต้องกำหนดความรับผิดชอบของผู้ให้บริการบุคคลภายนอกเสมือนหนึ่งเป็นผู้ดำเนินการเอง หากมีการแจ้งช่วงตามสัญญา

(จ) สิทธิการตรวจสอบโดยบริษัทและสำนักงาน

(ฉ) การคืน ทำลาย หรือลบข้อมูลส่วนบุคคล

(ช) ผลของการละเมิดเงื่อนไข

๓. บริษัทได้แนบเอกสาร โดยมีรายการดังต่อไปนี้

(....) หนังสือรับรองนิติบุคคลจากกรมพัฒนาธุรกิจการค้ากรณีผู้ให้บริการซึ่งเป็นบุคคลภายนอกเป็นนิติบุคคล

(....) เอกสารแสดงกิจกรรมและรายละเอียดที่ต้องการใช้วิธีการทางอิเล็กทรอนิกส์ (ตัวอย่างหน้าจ่อ)

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

(....) เอกสารแสดงระบบสารสนเทศและวิธีการทางอิเล็กทรอนิกส์ที่ใช้เพื่อรองรับกิจกรรมที่ใช้วิธีการทางอิเล็กทรอนิกส์ (system architecture)

(....) หนังสือรับรองการตรวจรับรองการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของผู้ให้บริการซึ่งเป็นบุคคลภายนอกโดยผู้ตรวจสอบอิสระตามแบบ อว. ๓ หรือประกาศนียบัตรที่ออกโดยหน่วยงานรับรองระบบสารสนเทศ (ISO๒๗๐๐๑)

(....) หนังสือรับรองการตรวจรับรองการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของบริษัทโดยผู้ตรวจสอบอิสระตามแบบ อว. ๓ หรือประกาศนียบัตรที่ออกโดยหน่วยงานรับรองระบบสารสนเทศ (ISO๒๗๐๐๑)

(....) เอกสารแนวทางการประเมินมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับเครื่องครัดตามหลักเกณฑ์ที่กำหนดในเอกสารแนบท้ายประกาศ (กรณีมีการตรวจรับรองจากผู้ตรวจสอบอิสระตามหนังสือรับรองตามแบบ อว. ๓)

(....) สำเนาสัญญาให้บริการระบบสารสนเทศระหว่างบริษัทกับผู้ให้บริการซึ่งเป็นบุคคลภายนอก

## ส่วนที่ ๒ กรณีนายหน้าประกันวินาศภัยหรือธนาคารให้บริการบุคคลภายนอก

๔. ข้าพเจ้า .....ซึ่ง มีใบอนุญาตเป็นนายหน้าประกันวินาศภัย เลขที่ ..... ใบอนุญาตหมดอายุ.....มีความประสงค์แจ้งเปลี่ยนแปลงการขึ้นทะเบียนกิจกรรมทางอิเล็กทรอนิกส์และขอรับความเห็นชอบในการให้บริการระบบสารสนเทศของผู้ให้บริการซึ่งเป็นบุคคลภายนอก.....(ระบุชื่อผู้ให้บริการ).....ในเรื่อง

(....) การเสนอขายกรมธรรม์ประกันภัยผ่านทางอิเล็กทรอนิกส์ (Online) บริษัท..... ในการทำงาน

(....) การเสนอขายกรมธรรม์ประกันภัยโดยใช้เครื่องมือทางอิเล็กทรอนิกส์ประกอบรายละเอียดที่เปลี่ยนแปลง.....

และได้รับความยินยอมจากบริษัท.....ในกิจกรรมข้างต้น

๕. ข้าพเจ้าขอรับรองว่า

๕.๑ ระบบสารสนเทศของผู้ให้บริการซึ่งเป็นบุคคลภายนอกมีมาตรฐานความมั่นคงและปลอดภัยในระดับเครื่องครัดสำหรับกิจกรรมตามข้อ ๔. ตามหลักเกณฑ์ที่กำหนดในเอกสารแนบท้ายประกาศนี้ โดยได้รับการตรวจสอบและรับรองจากผู้ตรวจสอบอิสระตามหนังสือรับรองตามแบบ อว. ๓ หรือตามประกาศนียบัตรที่ออกโดยหน่วยงานรับรองระบบสารสนเทศ (ISO๒๗๐๐๑) และ

ข้าพเจ้ามีระบบสารสนเทศที่มีมาตรฐานความมั่นคงและปลอดภัยในระดับเครื่องครัดสำหรับกิจกรรมตามข้อ ๔. ตามหลักเกณฑ์ที่กำหนดในเอกสารแนบท้ายประกาศนี้ โดยได้รับการตรวจสอบและรับรองจากผู้ตรวจสอบอิสระตามหนังสือรับรองตามแบบ อว. ๓ หรือตามประกาศนียบัตรที่ออกโดยหน่วยงานรับรองระบบสารสนเทศ (ISO๒๗๐๐๑)

๕.๒ ได้กำหนดนโยบาย กระบวนการและวิธีปฏิบัติที่ชัดเจน เช่น ระบบการประเมินความเสี่ยง การบริหารความเสี่ยง ขั้นตอนของการบริการ การควบคุมภายใน การรักษาความปลอดภัย และแผนรองรับกรณีที่เกิดบุคคลภายนอกไม่สามารถให้บริการได้

๕.๓ สัญญาใช้บริการระบบสารสนเทศระหว่างข้าพเจ้ากับผู้ให้บริการซึ่งเป็นบุคคลภายนอก ครอบคลุมเงื่อนไข ดังต่อไปนี้

(ก) มาตรการรักษาความมั่นคงปลอดภัยเพื่อคุ้มครองข้อมูลส่วนบุคคล ให้เป็นไปตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

(ข) การป้องกันการใช้หรือเปิดเผยโดยมิชอบ

(ค) การรายงานถึงความผิดปกติและการรายงานถึงการละเมิดข้อมูลส่วนบุคคล

(ง) ความรับผิดชอบในการแจ้งช่วงของผู้ให้บริการภายนอก โดยต้องกำหนดความรับผิดชอบของผู้ให้บริการบุคคลภายนอกเสมือนหนึ่งเป็นผู้ดำเนินการเอง หากมีการแจ้งช่วงตามสัญญา

(จ) สิทธิการตรวจสอบโดยบริษัทและสำนักงาน

(ฉ) การคืน ทำลาย หรือลบข้อมูลส่วนบุคคล

(ช) ผลของการละเมิดเงื่อนไข

๖. ข้าพเจ้าได้แนบเอกสาร โดยมีรายการดังต่อไปนี้

(...) หนังสือรับรองนิติบุคคลจากกรมพัฒนาธุรกิจการค้ากรณีผู้ให้บริการซึ่งเป็นบุคคลภายนอกเป็นนิติบุคคล

(...) เอกสารแสดงกิจกรรมและรายละเอียดที่ต้องการใช้วิธีการทางอิเล็กทรอนิกส์ (ตัวอย่าง หน้าจอ)

(...) แผนผัง (Flow chart) และขั้นตอนของกิจกรรมที่ใช้วิธีการทางอิเล็กทรอนิกส์

(...) เอกสารแสดงระบบสารสนเทศและวิธีการทางอิเล็กทรอนิกส์ที่ใช้เพื่อรองรับกิจกรรมที่ใช้วิธีการทางอิเล็กทรอนิกส์ (system architecture)

(...) หนังสือรับรองการตรวจรับรองการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของผู้ให้บริการซึ่งเป็นบุคคลภายนอกโดยผู้ตรวจสอบอิสระตามแบบ อว. ๓ หรือตามประกาศนียบัตรที่ออกโดยหน่วยงานรับรองระบบสารสนเทศ (ISO๒๗๐๐๑)

(...) หนังสือรับรองการตรวจรับรองการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของข้าพเจ้าโดยผู้ตรวจสอบอิสระตามแบบ อว. ๓ หรือตามประกาศนียบัตรที่ออกโดยหน่วยงานรับรองระบบสารสนเทศ (ISO๒๗๐๐๑)

(...) เอกสารแนวทางการประเมินมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับเครื่องครัดตามหลักเกณฑ์ที่กำหนดในเอกสารแนบท้ายประกาศ (กรณีมีการตรวจรับรองจากผู้ตรวจสอบอิสระตามหนังสือรับรองตามแบบ อว. ๓)

(...) สำเนาสัญญาใช้บริการระบบสารสนเทศระหว่างข้าพเจ้ากับผู้ให้บริการซึ่งเป็นบุคคลภายนอก

(...) หนังสือยินยอมของบริษัทให้เสนอขายกรมธรรม์ประกันภัยผ่านทางอิเล็กทรอนิกส์ (Online)

บริษัท  นายหน้าประกันวินาศภัยหรือธนาคาร .....

ขอรับรองว่า ข้อความและข้อมูลในแบบ ปว. ๔ นี้ ถูกต้องตรงตามความเป็นจริงทุกประการ

ประทับตรา (ถ้ามี)

ลงชื่อ .....

(.....)

กรรมการผู้มีอำนาจ/ผู้รับมอบอำนาจ\*

\*กรรมการผู้มีอำนาจ/ผู้รับมอบอำนาจของบริษัท/นายหน้าประกันวินาศภัยหรือธนาคาร แล้วแต่กรณี

แนวทางการประเมินมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ  
ตามวิธีการแบบปลอดภัยในระดับเคร่งครัด

หัวข้อ	รายละเอียด
<p><b>๑. การสร้างความมั่นคงปลอดภัยด้านบริหารจัดการ</b></p>	
<p>๑.๑ กำหนดนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยผ่านการอนุมัติ และผลักดันโดยผู้บริหารระดับสูง และมีการประกาศนโยบายดังกล่าวให้พนักงานและบุคคลภายนอกที่เกี่ยวข้องรับทราบโดยทั่วกัน</p> <p>๑.๒ วางแผนการติดตามและประเมินผลการใช้งานความมั่นคงปลอดภัยด้านสารสนเทศ และนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างสม่ำเสมอ เพื่อปรับปรุงหากมีการเปลี่ยนแปลงใด ๆ ภายในหน่วยงาน ทั้งนี้เพื่อให้เหมาะสมกับสถานการณ์การใช้งาน และคงความมีประสิทธิภาพอยู่เสมอ</p>	
<p><b>๒. การจัดโครงสร้างด้านความมั่นคงปลอดภัยของระบบสารสนเทศในส่วนการบริหารจัดการด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ทั้งภายในและภายนอกหน่วยงานหรือองค์กร</b></p>	
<p>๒.๑ ผู้บริหารระดับสูงของหน่วยงานมีหน้าที่ดูแลรับผิดชอบงานด้านสารสนเทศของหน่วยงานให้การสนับสนุน และกำหนดทิศทางการดำเนินงานเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศที่ชัดเจน รวมทั้งมีการมอบหมายงานที่เกี่ยวข้องให้กับผู้ปฏิบัติงานอย่างชัดเจน ตลอดจนรับผิดชอบต่อความเสี่ยง ความเสียหาย หรือ อันตรายที่เกิดขึ้นกับระบบสารสนเทศไม่ว่ากรณีใด ๆ</p> <p>๒.๒ สำหรับระบบสารสนเทศใหม่มีการกำหนดขั้นตอนการพิจารณาทบทวน เพื่ออนุมัติการสร้าง การติดตั้ง หรือการใช้งานในแง่มุมต่าง ๆ เช่น การบริหารจัดการผู้ใช้งานระบบ หรือความสามารถในการทำงานร่วมกันได้ระหว่างระบบเดิมและระบบใหม่</p> <p>๒.๓ มีการกำหนดสัญญาการรักษาข้อมูลที่เป็นความลับ (Confidentiality agreement หรือ NonDisclosure agreement) ที่สอดคล้องกับสถานการณ์และความต้องการของหน่วยงานในการปกป้องข้อมูลสารสนเทศ</p> <p>๒.๔ มีข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศสำหรับการอนุญาตให้ผู้ใช้บริการที่เป็นบุคคลภายนอกเข้าถึงระบบสารสนเทศ หรือใช้ข้อมูลสารสนเทศของหน่วยงาน</p> <p>๒.๕ สำหรับข้อตกลงเพื่ออนุญาตให้บุคคลภายนอกเข้าถึงระบบสารสนเทศ หรือใช้ข้อมูลสารสนเทศของหน่วยงาน เพื่อการอ่าน การประมวลผล การบริหารจัดการระบบสารสนเทศ หรือการพัฒนาสารสนเทศ ควรมีข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศระบุไว้ในข้อตกลง</p> <p>๒.๖ มีการกำหนดเงื่อนไขหรือหน้าที่ความรับผิดชอบต่าง ๆ เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศไว้อย่างชัดเจน</p> <p>๒.๗ มีการกำหนดขั้นตอนและช่องทางในการติดต่อกับหน่วยงานภายนอกที่มีความเชี่ยวชาญเฉพาะด้าน หรือหน่วยงานที่มีความเชี่ยวชาญด้านความมั่นคงปลอดภัยด้านสารสนเทศภายใต้สถานการณ์ต่าง ๆ ไว้อย่างชัดเจน</p> <p>๒.๘ จัดให้มีการพิจารณาทบทวนแนวทางในการบริหารจัดการงานเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศอย่างสม่ำเสมอ หรือเมื่อมีการเปลี่ยนแปลงใด ๆ ในการดำเนินงาน ทั้งนี้ การพิจารณาทบทวนดังกล่าว ควรดำเนินการโดยผู้ไม่มีส่วนได้เสียกับงานที่มีการพิจารณาทบทวน</p> <p>๒.๙ มีการสร้างความร่วมมือระหว่างผู้ที่มีบทบาทเกี่ยวข้องกับความมั่นคงปลอดภัยด้าน</p>	

หัวข้อ	รายละเอียด
<p>สารสนเทศของ หน่วยงาน ในงานหรือกิจกรรมใด ๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศ</p> <p>๒.๑๐ มีการกำหนดขั้นตอนและช่องทางในการติดต่อกับหน่วยงานภายนอกที่มีหน้าที่ในการกำกับดูแล หรือหน่วยงานที่เกี่ยวข้องกับการบังคับใช้กฎหมาย รวมทั้งหน่วยงานที่ควบคุมดูแลสถานการณ์ฉุกเฉินภายใต้สถานการณ์ต่าง ๆ ไว้อย่างชัดเจน</p> <p>๒.๑๑ ก่อนที่จะอนุญาตให้หน่วยงานหรือบุคคลภายนอกเข้าถึงระบบสารสนเทศหรือใช้ข้อมูลสารสนเทศของ หน่วยงาน ให้มีการระบุความเสี่ยงที่อาจเกิดขึ้นและกำหนดแนวทางป้องกันเพื่อลดความเสี่ยงนั้นก่อนการอนุญาต</p>	
<p><b>๓. การบริหารจัดการทรัพย์สินสารสนเทศ</b></p>	
<p>๓.๑ มีการเก็บบันทึกข้อมูลทรัพย์สินสารสนเทศ โดยข้อมูลที่จัดเก็บต้องประกอบด้วยข้อมูลที่จำเป็นในการค้นหาเพื่อการใช้งานในภายหลัง</p> <p>๓.๒ มีการกำหนดบุคคลผู้มีหน้าที่ดูแลควบคุมการใช้งานและรับผิดชอบทรัพย์สินสารสนเทศไว้ชัดเจน</p> <p>๓.๓ มีการกำหนดกฎระเบียบในการใช้งานทรัพย์สินสารสนเทศไว้อย่างชัดเจน โดยจัดทำเป็นเอกสาร และมีการประกาศใช้ในหน่วยงาน</p> <p>๓.๔ มีการจำแนกประเภทของข้อมูลสารสนเทศ โดยจำแนกตามมูลค่าของข้อมูล ข้อกำหนดทางกฎหมาย ระดับชั้นความลับและความสำคัญต่อหน่วยงาน</p> <p>๓.๕ มีการกำหนดและประกาศใช้ขั้นตอนที่เหมาะสมในการจำแนกประเภทของข้อมูลสารสนเทศ และจัดการข้อมูลสารสนเทศ โดยให้สอดคล้องกับแนวทางการจำแนกประเภทของข้อมูลสารสนเทศที่หน่วยงานประกาศใช้</p>	
<p><b>๔. การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร</b></p>	
<p>๔.๑ กำหนดหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยด้านสารสนเทศของพนักงานหรือหน่วยงาน หรือบุคคลภายนอกที่ว่าจ้าง โดยให้สอดคล้องกับความมั่นคงปลอดภัยด้านสารสนเทศและนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่หน่วยงานประกาศใช้</p> <p>๔.๒ ผู้บริหารระดับสูงของหน่วยงานต้องกำหนดให้พนักงาน หน่วยงานหรือบุคคลภายนอกที่ว่าจ้าง ปฏิบัติงานตามนโยบายหรือระเบียบปฏิบัติด้านความมั่นคงปลอดภัยที่หน่วยงานประกาศใช้</p> <p>๔.๓ กำหนดให้มีขั้นตอนการลงโทษพนักงานที่ฝ่าฝืนนโยบายหรือระเบียบปฏิบัติเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศในหน่วยงาน</p> <p>๔.๔ กำหนดหน้าที่ความรับผิดชอบในการยุติการจ้าง หรือการเปลี่ยนแปลงสถานะการจ้างให้ชัดเจน และมอบหมายให้ผู้ที่รับผิดชอบอย่างชัดเจน</p> <p>๔.๕ พนักงานหน่วยงานหรือบุคคลภายนอกที่ว่าจ้างต้องส่งคืนทรัพย์สินสารสนเทศของหน่วยงานเมื่อ สิ้นสุดสถานะการเป็นพนักงาน หรือสิ้นสุดสัญญาหรือข้อตกลงการปฏิบัติงานให้กับหน่วยงาน</p> <p>๔.๖ ให้ยกเลิกสิทธิของพนักงานหน่วยงานหรือบุคคลภายนอกในการเข้าใช้งานระบบสารสนเทศ เมื่อสิ้นสุดสถานะการเป็นพนักงาน หรือสิ้นสุดสัญญาหรือข้อตกลงการปฏิบัติงาน และให้ปรับเปลี่ยนระดับสิทธิในการเข้าใช้งานระบบสารสนเทศให้เหมาะสมเมื่อมีการเปลี่ยนแปลงหน้าที่ความรับผิดชอบใด ๆ เกิดขึ้น</p> <p>๔.๗ พนักงาน หน่วยงานหรือ บุคคลภายนอกต้องได้รับการอบรมเพื่อสร้างความตระหนักรู้เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศในส่วนที่ เกี่ยวข้องกับหน้าที่ความรับผิดชอบของตน และได้รับการสื่อสารให้ทราบถึงนโยบายหรือระเบียบปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ</p>	



หัวข้อ	รายละเอียด
<p>ที่หน่วยงานประกาศใช้อย่างสม่ำเสมอ หรือเมื่อมีการเปลี่ยนแปลง</p> <p>๔.๘ ในการพิจารณารับพนักงานเข้าทำงาน หรือการว่าจ้างหน่วยงานหรือบุคคลภายนอก ให้มีการตรวจสอบประวัติหรือคุณสมบัติเพื่อให้เป็นไปตามกฎหมาย กฎระเบียบและจริยธรรมที่เกี่ยวข้อง โดยให้คำนึงถึงระดับชั้นความลับของข้อมูลสารสนเทศที่จะให้เข้าถึง และระดับความเสี่ยงที่ได้ประเมิน</p> <p>๔.๙ ในสัญญาจ้างหรือข้อตกลงการปฏิบัติงานของพนักงาน หรือสัญญาว่าจ้างหน่วยงาน หรือ บุคคลภายนอก ให้ระบุหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยด้านสารสนเทศไว้ในสัญญา</p>	
<p><b>๕. การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม</b></p>	
<p>๕.๑ ให้มีการป้องกันขอบเขตพื้นที่ตั้งของหน่วยงาน (Security perimeter) ที่มีการติดตั้งจัดเก็บ หรือใช้งานระบบสารสนเทศและข้อมูลสารสนเทศ</p> <p>๕.๒ มีการออกแบบและติดตั้งการป้องกันความมั่นคงปลอดภัยด้านกายภาพ เพื่อป้องกันภัยจากภายนอก ภัยในระดับหายนะทั้งที่ก่อโดยมนุษย์หรือภัยธรรมชาติเช่น อัคคีภัย อุทกภัย แผ่นดินไหว ระเบิด การก่อจลาจล เป็นต้น</p> <p>๕.๓ จัดวางและป้องกันอุปกรณ์สารสนเทศ เพื่อลดความเสี่ยงจากภัยธรรมชาติหรืออันตรายต่าง ๆ และเพื่อป้องกันการเข้าถึงโดยมิได้รับอนุญาต</p> <p>๕.๔ มีการป้องกันอุปกรณ์สารสนเทศ ที่อาจเกิดจากไฟฟ้าขัดข้อง (Power failure) หรือที่อาจหยุดชะงัก จากข้อผิดพลาดของโครงสร้างพื้นฐาน (Supporting utilities)</p> <p>๕.๕ มีการดูแลอุปกรณ์สารสนเทศอย่างถูกวิธีเพื่อให้คงไว้ซึ่งความถูกต้องครบถ้วนและอยู่ในสภาพพร้อมใช้งานอยู่เสมอ</p> <p>๕.๖ มีการออกแบบและติดตั้งการป้องกันความมั่นคงปลอดภัยด้านกายภาพ เพื่อป้องกันพื้นที่หรือสถานที่ปฏิบัติงาน หรืออุปกรณ์สารสนเทศต่าง ๆ</p> <p>๕.๗ ไม่ควรรนำอุปกรณ์สารสนเทศ ข้อมูลสารสนเทศ หรือซอฟต์แวร์ออกจากสถานที่ปฏิบัติงานของหน่วยงานหากมิได้รับอนุญาต</p> <p>๕.๘ ในพื้นที่ที่ต้องมีการรักษาความมั่นคงปลอดภัยด้านกายภาพ (Secure area) ต้องมีการควบคุมการเข้าออก โดยให้เฉพาะผู้มีสิทธิที่สามารถเข้าออกได้</p> <p>๕.๙ มีการออกแบบแนวทางการป้องกันทางกายภาพสำหรับการทำงานในพื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัยด้านกายภาพ (Secure area) และกำหนดให้มีการนำไปใช้งาน</p> <p>๕.๑๐ มีการควบคุมบริเวณที่ผู้ไม่มีสิทธิเข้าถึงอาจสามารถเข้าถึงได้เช่น จุดรับส่งของ เป็นต้น หรือหากเป็นไปได้ให้แยกบริเวณดังกล่าวออกจากพื้นที่ที่มีการติดตั้ง จัดเก็บ หรือใช้งานระบบสารสนเทศและข้อมูลสารสนเทศเพื่อหลีกเลี่ยงการเข้าถึงโดยมิได้รับอนุญาต</p> <p>๕.๑๑ มีการป้องกันสายเคเบิลที่ใช้เพื่อการสื่อสาร หรือสายไฟ เพื่อมิให้มีการดักจับสัญญาณ (Interception) หรือมีความเสียหายเกิดขึ้น</p> <p>๕.๑๒ มีการรักษาความมั่นคงปลอดภัยให้กับอุปกรณ์สารสนเทศที่มีการนำไปใช้งานนอกสถานที่ปฏิบัติงานของหน่วยงาน โดยให้คำนึงถึงระดับความเสี่ยงที่แตกต่างกันจากการนำไปใช้งานในสถานที่ต่าง ๆ</p> <p>๕.๑๓ ก่อนการยกเลิกการใช้งานหรือจำหน่ายอุปกรณ์สารสนเทศที่ใช้ในการจัดเก็บข้อมูลสารสนเทศต้องมีการตรวจสอบอุปกรณ์สารสนเทศนั้นว่า ได้มีการลบ ย้าย หรือทำลายข้อมูลที่สำคัญหรือซอฟต์แวร์ที่จัดซื้อและติดตั้งไว้ด้วยวิธีการที่ทำให้ไม่สามารถกู้คืนได้อีก</p>	
<p><b>๖. การบริหารจัดการด้านการสื่อสารและการดำเนินงานของระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ระบบงานคอมพิวเตอร์และระบบสารสนเทศ</b></p>	

หัวข้อ	รายละเอียด
<p>๖.๑ มีการจัดทำ ปรับปรุง และดูแลเอกสารขั้นตอนการปฏิบัติงานที่อยู่ในสภาพพร้อมใช้งาน เพื่อให้พนักงานสามารถนำไปปฏิบัติได้</p> <p>๖.๒ มีการดูแลให้บุคคลหรือหน่วยงานภายนอกที่ให้บริการแก่หน่วยงานตามที่วางจ้าง ปฏิบัติตามสัญญา หรือข้อตกลงให้บริการที่ระบุไว้ซึ่งต้องครอบคลุมถึงงานด้านความมั่นคงปลอดภัย ลักษณะการให้บริการ และระดับการให้บริการ</p> <p>๖.๓ มีการติดตามตรวจสอบรายงานหรือบันทึกการให้บริการของบุคคลหรือหน่วยงานภายนอกที่ให้บริการแก่หน่วยงานตามที่วางจ้างอย่างสม่ำเสมอ</p> <p>๖.๔ จัดให้มีเกณฑ์การตรวจรับระบบสารสนเทศที่มีการปรับปรุงหรือที่มีเวอร์ชันใหม่ และควรมีการทดสอบระบบสารสนเทศทั้งในช่วงการพัฒนาระบบและก่อนการตรวจรับ</p> <p>๖.๕ มีขั้นตอนควบคุมการตรวจสอบ ป้องกัน และกักกันในกรณีมีการใช้งานโปรแกรมไม่พึงประสงค์และให้มีการสร้างความตระหนักรู้ให้กับผู้ใช้งานระบบสารสนเทศหรือข้อมูลสารสนเทศเกี่ยวกับโปรแกรมไม่พึงประสงค์</p> <p>๖.๖ มีการสำรองข้อมูลสารสนเทศ และทดสอบการนำกลับมาใช้งาน โดยให้เป็นไปตามนโยบายการสำรองข้อมูลที่หน่วยงานประกาศใช้</p> <p>๖.๗ มีการบริหารจัดการการควบคุมเครือข่ายคอมพิวเตอร์เพื่อป้องกันภัยคุกคาม และมีการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและแอปพลิเคชันที่ทำงานบนเครือข่ายคอมพิวเตอร์รวมทั้งข้อมูลสารสนเทศ ที่มีการแลกเปลี่ยนบนเครือข่ายดังกล่าว</p> <p>๖.๘ มีการกำหนดรูปแบบการรักษาความมั่นคงปลอดภัย ระดับการให้บริการ ข้อกำหนดการบริหารจัดการ ในข้อตกลงการให้บริการด้านเครือข่ายคอมพิวเตอร์ไม่ว่าเป็นการให้บริการโดยหน่วยงานเอง หรือจ้างช่วงไปยังผู้ให้บริการภายนอก</p> <p>๖.๙ จัดให้มีนโยบายและขั้นตอนปฏิบัติงาน รวมทั้งควบคุมการแลกเปลี่ยนข้อมูลสารสนเทศผ่านช่องทางการสื่อสารในรูปแบบข้อมูลอิเล็กทรอนิกส์</p> <p>๖.๑๐ จัดให้มีข้อตกลงในการแลกเปลี่ยนข้อมูลสารสนเทศหรือซอฟต์แวร์ระหว่างหน่วยงานกับบุคคลหรือหน่วยงานภายนอก</p> <p>๖.๑๑ จัดให้มีนโยบายและขั้นตอนการปฏิบัติงาน เพื่อป้องกันข้อมูลสารสนเทศที่มีการสื่อสารหรือ แลกเปลี่ยนผ่านระบบสารสนเทศที่มีการเชื่อมต่อกับระบบสารสนเทศต่าง ๆ</p> <p>๖.๑๒ มีการป้องกันข้อมูลสารสนเทศที่มีการแลกเปลี่ยนในการทำพาณิชย์อิเล็กทรอนิกส์ (Electronic commerce) ผ่านเครือข่ายคอมพิวเตอร์สาธารณะ เพื่อมิให้มีการฉ้อโกง ละเมิดสัญญา หรือมีการรั่วไหลหรือข้อมูลสารสนเทศถูกแก้ไขโดยมิได้รับอนุญาต</p> <p>๖.๑๓ มีการป้องกันข้อมูลสารสนเทศที่มีการสื่อสารหรือแลกเปลี่ยนในการทำธุรกรรมทางออนไลน์ (Online transaction) เพื่อมิให้มีการรับส่งข้อมูลที่ไม่สมบูรณ์หรือส่งข้อมูลไปผิดที่ หรือมีการรั่วไหลของข้อมูล หรือข้อมูลถูกแก้ไขเปลี่ยนแปลง ถูกทำซ้ำใหม่ หรือถูกส่งซ้ำโดยมิได้รับอนุญาต</p> <p>๖.๑๔ สำหรับข้อมูลสารสนเทศที่มีการเผยแพร่ต่อสาธารณชน ให้มีการป้องกันมิให้มีการแก้ไขเปลี่ยนแปลง โดยมิได้รับอนุญาต และเพื่อรักษาความถูกต้องครบถ้วนของข้อมูลสารสนเทศ</p> <p>๖.๑๕ มีการเก็บบันทึกข้อมูล Audit log ซึ่งบันทึกข้อมูลกิจกรรมการใช้งานของผู้ใช้งานระบบสารสนเทศ และเหตุการณ์เกี่ยวกับความมั่นคงปลอดภัยต่าง ๆ เพื่อประโยชน์ในการสืบสวน สอบสวนในอนาคต และเพื่อการติดตามการควบคุมการเข้าถึง</p> <p>๖.๑๖ มีขั้นตอนการเฝ้าติดตามสังเกตการใช้งานระบบสารสนเทศ และมีการติดตามประเมินผลการติดตามสังเกตดังกล่าวอย่างสม่ำเสมอ</p> <p>๖.๑๗ มีการป้องกันระบบสารสนเทศที่จัดเก็บ Log และข้อมูล Log เพื่อป้องกันการเข้าถึงหรือแก้ไข เปลี่ยนแปลงโดยมิได้รับอนุญาต</p> <p>๖.๑๘ มีการจัดเก็บ Log ที่เกี่ยวข้องกับการดูแลระบบสารสนเทศโดยผู้ดูแลระบบ</p>	

หัวข้อ	รายละเอียด
<p>(System administrator หรือ System operator)</p> <p>๖.๑๙ มีการจัดการควบคุมการเปลี่ยนแปลงของระบบสารสนเทศ</p> <p>๖.๒๐ มีการติดตามผลการใช้งานทรัพยากรสารสนเทศ และวางแผนด้านทรัพยากรสารสนเทศให้รองรับการปฏิบัติงานในอนาคตอย่างเหมาะสม</p> <p>๖.๒๑ มีขั้นตอนการปฏิบัติงานในการจัดการและจัดเก็บข้อมูลสารสนเทศเพื่อมิให้ข้อมูลรั่วไหลหรือถูกนำไปใช้ผิดประเภท</p> <p>๖.๒๒ มีการจัดเก็บ Log ที่เกี่ยวข้องกับข้อผิดพลาดใด ๆ ของระบบสารสนเทศ มีการวิเคราะห์ Log ดังกล่าว อย่างสม่ำเสมอ และมีการจัดการแก้ไขข้อผิดพลาดที่ตรวจพบอย่างเหมาะสม</p> <p>๖.๒๓ ระบบเวลาของระบบสารสนเทศต่าง ๆ ที่ใช้ในหน่วยงานหรือในขอบเขตงานด้านความมั่นคงปลอดภัย (Security domain) ต้องมีความสอดคล้องกัน (Synchronization) โดยให้มีการตั้งค่าพร้อมกันกับเวลาจากแหล่งเวลา ที่เชื่อถือได้</p> <p>๖.๒๔ มีการแบ่งแยกหน้าที่และขอบเขตความรับผิดชอบอย่างชัดเจน เพื่อลดโอกาสความผิดพลาดในการเปลี่ยนแปลงหรือใช้งานระบบสารสนเทศหรือข้อมูลสารสนเทศที่ผิดประเภท</p> <p>๖.๒๕ มีการแยกระบบสารสนเทศสำหรับการพัฒนา ทดสอบ และใช้งานจริงออกจากกัน เพื่อลดความเสี่ยง ในการเข้าใช้งานหรือการเปลี่ยนแปลงระบบสารสนเทศโดยมิได้รับอนุญาต</p> <p>๖.๒๖ มีการบริหารจัดการการเปลี่ยนแปลงใด ๆ เกี่ยวกับการจัดเตรียมการให้บริการ และการดูแลปรับปรุงนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ขั้นตอนปฏิบัติงานหรือการควบคุมเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ โดยคำนึงถึงระดับความสำคัญของการดำเนินธุรกิจที่เกี่ยวข้องและการประเมินความเสี่ยงอย่างต่อเนื่อง</p> <p>๖.๒๗ หากหน่วยงานอนุญาตให้มีการใช้งาน Mobile code (เช่น Script บางอย่างของเว็บ แอปพลิเคชันที่มีการทำงานอัตโนมัติเมื่อเรียกดูเว็บ) ควรมีการตั้งค่าการทำงาน (Configuration) เพื่อให้มั่นใจได้ว่าการทำงานของ Mobile code นั้นเป็นไปตามความมั่นคงปลอดภัยด้านสารสนเทศและนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และห้ามโดยอัตโนมัติมิให้ Mobile code สามารถทำงานได้ในระบบสารสนเทศ หากในนโยบาย การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กำหนดห้ามมิให้ประเภทของ Mobile code ดังกล่าวทำงานได้</p> <p>๖.๒๘ มีขั้นตอนการปฏิบัติงานสำหรับการบริหารจัดการอุปกรณ์ที่ใช้ในการบันทึกข้อมูลอิเล็กทรอนิกส์ที่สามารถถอดหรือต่อพ่วงกับเครื่องคอมพิวเตอร์ได้ (Removable media)</p> <p>๖.๒๙ มีขั้นตอนการปฏิบัติงานในการทำลายอุปกรณ์ที่ใช้ในการบันทึกข้อมูลอิเล็กทรอนิกส์ที่สามารถถอด หรือต่อพ่วงกับเครื่องคอมพิวเตอร์ได้ (Removable media) อย่างมั่นคงปลอดภัย</p> <p>๖.๓๐ มีการป้องกันมิให้ข้อมูลหรือเอกสารเกี่ยวกับระบบสารสนเทศ (System documentation) ถูกเข้าถึง โดยมิได้รับอนุญาต</p> <p>๖.๓๑ ในกรณีที่มีการเคลื่อนย้ายอุปกรณ์ที่จัดเก็บข้อมูลสารสนเทศ ให้มีการป้องกันอุปกรณ์ที่ใช้จัดเก็บข้อมูลดังกล่าว เพื่อมิให้มีการเข้าถึงโดยมิได้รับอนุญาต หรือถูกนำไปใช้งานผิดประเภท หรืออุปกรณ์หรือข้อมูลสารสนเทศได้รับความเสียหาย</p> <p>๖.๓๒ ให้มีการป้องกันข้อมูลสารสนเทศที่มีการสื่อสารกันผ่านข้อมูลอิเล็กทรอนิกส์ (Electronic messaging) เช่น จดหมายอิเล็กทรอนิกส์ ( E - mail) EDI หรือ Instant messaging)</p>	
<p>๗. การควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์และข้อมูลคอมพิวเตอร์</p>	
<p>๗.๑ จัดให้มีนโยบายควบคุมการเข้าถึง โดยจัดทำเป็นเอกสาร และมีการติดตามทบทวนให้</p>	

หัวข้อ	รายละเอียด
<p>นโยบายดังกล่าว สอดคล้องกับข้อกำหนดหรือความต้องการด้านการดำเนินงานหรือการให้บริการ และด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ</p> <p>๗.๒ จัดให้มีการลงทะเบียนบัญชีผู้ใช้งานระบบสารสนเทศ และยกเลิกบัญชีผู้ใช้อย่างเป็นทางการ เพื่อควบคุมการให้สิทธิและการยกเลิกสิทธิในการเข้าใช้งานระบบสารสนเทศใด ๆ ของหน่วยงาน</p> <p>๗.๓ การกำหนดสิทธิในการเข้าถึงระดับสูง ให้ทำอย่างจำกัดและอยู่ภายใต้การควบคุม</p> <p>๗.๔ ผู้ใช้งานต้องดูแลป้องกันอุปกรณ์สารสนเทศที่อยู่ภายใต้ความดูแลรับผิดชอบ ในระหว่างที่ไม่มีการใช้งาน</p> <p>๗.๕ จำกัดการเข้าถึงเครือข่ายคอมพิวเตอร์ของหน่วยงานที่สามารถเข้าถึงได้จากภายนอก โดยให้สอดคล้องกับนโยบายควบคุมการเข้าถึง และข้อกำหนดการใช้งานแอปพลิเคชันเพื่อการดำเนินงาน</p> <p>๗.๖ ให้ผู้ใช้งานทุกคนมีบัญชีผู้ใช้งานเป็นของตนเอง และให้ระบบสารสนเทศมีเทคนิคการตรวจสอบตัวตนที่เพียงพอ เพื่อให้สามารถระบุตัวตนของผู้เข้าใช้งานระบบสารสนเทศได้</p> <p>๗.๗ ให้อัตโนมัติหรือปิดหน้าจอการใช้งานระบบสารสนเทศโดยอัตโนมัติหากไม่มีการใช้งานเกินระยะเวลาสูงสุดที่กำหนดไว้</p> <p>๗.๘ จำกัดการเข้าถึงข้อมูลสารสนเทศและฟังก์ชันต่าง ๆ ในแอปพลิเคชันของผู้ใช้งานและผู้ดูแลระบบสารสนเทศ โดยให้สอดคล้องกับนโยบายการเข้าถึงที่ได้กำหนดไว้</p> <p>๗.๙ กำหนดนโยบายและแนวทางการจัดการด้านความมั่นคงปลอดภัย เพื่อลดความเสี่ยงในการใช้งานอุปกรณ์สารสนเทศหรืออุปกรณ์การสื่อสารที่เคลื่อนย้ายได้เช่น แล็ปท็อปคอมพิวเตอร์ (Laptop Computer) หรือสมาร์ทโฟน (Smartphone) เป็นต้น</p> <p>๗.๑๐ มีข้อบังคับให้ผู้ใช้งานปฏิบัติตามขั้นตอนเพื่อการเลือกใช้รหัสผ่านอย่างมั่นคงปลอดภัยตามที่หน่วยงานกำหนด</p> <p>๗.๑๑ ผู้ใช้งานสามารถเข้าถึงเฉพาะบริการทางเครือข่ายคอมพิวเตอร์ที่ตนเองได้รับอนุญาตให้ใช้ได้เท่านั้น</p> <p>๗.๑๒ ให้มีการกำหนดวิธีการตรวจสอบตัวตนที่เหมาะสมเพื่อควบคุมการเข้าถึงระบบสารสนเทศของ หน่วยงานจากระยะไกล</p> <p>๗.๑๓ มีการควบคุมการเข้าถึงช่องทางการดูแลระบบสารสนเทศทั้งทางกายภาพและการเชื่อมต่อผ่าน คอมพิวเตอร์สำหรับระบบสารสนเทศที่สามารถเข้าถึงจากระยะไกลได้เช่น Remote diagnostic หรือ Configuration facility ของอุปกรณ์เครือข่ายคอมพิวเตอร์</p> <p>๗.๑๔ มีการจัดกลุ่มตามประเภทของข้อมูลสารสนเทศที่ให้บริการ ระบบสารสนเทศ กลุ่มผู้ใช้งานโดยมีการแบ่งแยกบนเครือข่ายคอมพิวเตอร์อย่างเป็นสัดส่วน</p> <p>๗.๑๕ กำหนดให้มีการควบคุมเส้นทางการไหลของข้อมูลสารสนเทศในระบบเครือข่ายคอมพิวเตอร์เพื่อไม่ให้ขัดแย้งกับนโยบายควบคุมการเข้าถึงของแอปพลิเคชัน</p> <p>๗.๑๖ กำหนดขั้นตอนการ Log-on เพื่อควบคุมการเข้าถึงระบบปฏิบัติการคอมพิวเตอร์</p> <p>๗.๑๗ ให้จัดทำหรือจัดให้มีระบบการบริหารจัดการรหัสผ่านที่สามารถทำงานแบบเชิงโต้ตอบกับผู้ใช้งาน (Interactive) และสามารถรองรับการใช้งานรหัสผ่านที่มีความมั่นคงปลอดภัย</p> <p>๗.๑๘ จัดให้มีขั้นตอนการบริหารจัดการเรื่องการกำหนดรหัสผ่านอย่างเป็นทางการ</p> <p>๗.๑๙ กำหนดให้ผู้บริหารติดตามทบทวนระดับสิทธิในการเข้าถึงของผู้ใช้งานอย่างเป็นทางการเป็นประจำ</p> <p>๗.๒๐ มีการกำหนดนโยบาย Clear desk สำหรับข้อมูลสารสนเทศในรูปแบบกระดาษและที่จัดเก็บใน อุปกรณ์บันทึกข้อมูลอิเล็กทรอนิกส์ที่สามารถถอดหรือต่อพ่วงกับเครื่องคอมพิวเตอร์ได้และนโยบาย Clear screen สำหรับระบบสารสนเทศ</p>	

หัวข้อ	รายละเอียด
<p>๗.๒๑ ให้มีการระบุอุปกรณ์ที่เชื่อมต่อเข้ากับระบบสารสนเทศโดยอัตโนมัติ (Automatic equipment identification) เพื่อตรวจสอบการเชื่อมต่อของอุปกรณ์ดังกล่าวว่ามาจากอุปกรณ์ดังกล่าวจริง หรือจากสถานที่ที่กำหนดไว้เท่านั้น ทั้งนี้จำเป็นสำหรับการที่ระบบสารสนเทศจะรับการเชื่อมต่อจากเฉพาะอุปกรณ์ที่ได้รับอนุญาต หรือมาจากเฉพาะสถานที่ที่ได้รับอนุญาต</p> <p>๗.๒๒ ให้จำกัดการเข้าถึงการใช้งานโปรแกรมมัลติโพรโทคอลต่าง ๆ อย่างเข้มงวด เนื่องจากโปรแกรมดังกล่าวอาจมีความสามารถควบคุมดูแลและเปลี่ยนแปลงการทำงานของระบบสารสนเทศได้</p> <p>๗.๒๓ จำกัดระยะเวลาการเชื่อมต่อกับระบบสารสนเทศที่มีระดับความเสี่ยงสูง เพื่อเพิ่มระดับการรักษาความมั่นคงปลอดภัย</p> <p>๗.๒๔ สำหรับระบบสารสนเทศที่มีความสำคัญสูง ต้องจัดให้ระบบสารสนเทศทำงานในสภาพแวดล้อมที่แยกออกมาต่างหาก โดยไม่ใช่ปะปนกับระบบสารสนเทศอื่น</p> <p>๗.๒๕ กำหนดให้มีนโยบาย แผนงานและขั้นตอนการปฏิบัติงานที่เกี่ยวข้องกับกิจกรรมใด ๆ ที่มีการปฏิบัติงานจากภายนอกหน่วยงาน (Teleworking)</p>	
<p><b>๘. การจัดหาหรือจัดให้มีการพัฒนา และการบำรุงรักษาระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์และระบบสารสนเทศ</b></p>	
<p>๘.๑ ในการจัดทำข้อกำหนดขั้นต่ำของระบบสารสนเทศใหม่ หรือการปรับปรุงระบบสารสนเทศเดิม ให้มีการระบุข้อกำหนดด้านการควบคุมความมั่นคงปลอดภัยด้านสารสนเทศไว้ด้วย</p> <p>๘.๒ ให้ดูแล ควบคุม ติดตามตรวจสอบการทำงานในการจ้างช่วงพัฒนาซอฟต์แวร์</p> <p>๘.๓ ให้มีการตรวจสอบ (Validate) ข้อมูลใด ๆ ที่จะรับเข้าสู่แอปพลิเคชันก่อนเสมอ เพื่อให้มั่นใจได้ว่า ข้อมูลมีความถูกต้องและมีรูปแบบเหมาะสม</p> <p>๘.๔ ให้มีการตรวจสอบ (Validate) ข้อมูลใด ๆ อันเป็นผลจากการประมวลผลของแอปพลิเคชัน เพื่อให้มั่นใจได้ว่า ข้อมูลที่ได้จากการประมวลผลถูกต้องและเหมาะสม</p> <p>๘.๕ จัดให้มีแนวทางการบริหารจัดการกุญแจ (Key) เพื่อรองรับการใช้งานเทคนิคที่เกี่ยวข้องกับการเข้ารหัสลับของหน่วยงาน</p> <p>๘.๖ ให้เลือกชุดข้อมูลสารสนเทศที่จะนำไปใช้เพื่อทดสอบในระบบสารสนเทศอย่างระมัดระวัง รวมทั้งมีแนวทางควบคุมและป้องกันข้อมูลรั่วไหล</p> <p>๘.๗ ให้มีการจำกัดการเข้าถึงซอร์สโค้ด (Source code) ของโปรแกรม</p> <p>๘.๘ หากมีการเปลี่ยนแปลงใด ๆ ในระบบปฏิบัติการคอมพิวเตอร์ให้มีการตรวจสอบ ทบทวนการทำงานของโปรแกรมที่มีความสำคัญ และทดสอบการใช้งานเพื่อให้มั่นใจว่าผลของการเปลี่ยนแปลงดังกล่าว จะไม่ส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ และการให้บริการของหน่วยงาน</p> <p>๘.๙ ให้มีการตรวจสอบ (Validate) การทำงานของแอปพลิเคชันเพื่อตรวจสอบหาข้อผิดพลาดของข้อมูลที่เกิดจากการทำงานหรือการประมวลผลที่ผิดพลาด</p> <p>๘.๑๐ ให้มีข้อกำหนดขั้นต่ำสำหรับการรักษาความถูกต้องแท้จริง (Authenticity) และความถูกต้องครบถ้วน (Integrity) ของข้อมูลในแอปพลิเคชัน รวมทั้งมีการระบุและปฏิบัติตามวิธีการป้องกันที่เหมาะสม</p> <p>๘.๑๑ จัดให้มีนโยบายในการใช้งานเทคนิคที่เกี่ยวข้องกับการเข้ารหัสลับ</p> <p>๘.๑๒ กำหนดให้มีขั้นตอนการปฏิบัติงานเพื่อควบคุมการติดตั้งซอฟต์แวร์บนระบบสารสนเทศที่ให้บริการ</p> <p>๘.๑๓ ให้มีการควบคุมการเปลี่ยนแปลงต่าง ๆ ในการพัฒนาระบบสารสนเทศ โดยมีขั้นตอนการควบคุมที่เป็นทางการ</p>	

หัวข้อ	รายละเอียด
<p>๘.๑๔ ให้จำกัดการเปลี่ยนแปลงใด ๆ ต่อซอฟต์แวร์ที่ใช้งาน (Software package) โดยให้เปลี่ยนแปลงเฉพาะเท่าที่จำเป็น และควบคุมทุก ๆ การเปลี่ยนแปลงอย่างเข้มงวด</p> <p>๘.๑๕ มีมาตรการป้องกันเพื่อลดโอกาสที่เกิดการรั่วไหลของข้อมูลสารสนเทศ</p>	
<p><b>๙. การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด</b></p>	
<p>๙.๑ ให้มีการรายงานสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดผ่าน ช่องทางการบริหารจัดการที่เหมาะสมโดยเร็วที่สุด</p> <p>๙.๒ กำหนดให้พนักงานหรือผู้ใช้งานที่เป็นบุคคลภายนอก มีการบันทึกและรายงานจุดอ่อนใด ๆ ที่อาจสังเกตพบระหว่างการใช้งานระบบสารสนเทศ</p> <p>๙.๓ กำหนดขอบเขตความรับผิดชอบของผู้บริหารและขั้นตอนการปฏิบัติงาน เพื่อตอบสนองต่อสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด อย่างรวดเร็ว มีระเบียบ และมีประสิทธิผล</p> <p>๙.๔ หากในขั้นตอนการติดตามผลกับบุคคลหรือหน่วยงานภายหลังจากเกิดสถานการณ์ด้านความมั่นคง ปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ซึ่งเกี่ยวข้องกับการดำเนินการทางกฎหมาย (ไม่ว่าทางแพ่งหรือทาง อาญา) ให้มีการรวบรวม จัดเก็บ และนำเสนอหลักฐาน ให้สอดคล้องกับหลักเกณฑ์ของกฎหมายที่ใช้บังคับ</p>	
<p><b>๑๐. การบริหารจัดการด้านการบริการหรือการดำเนินงานของหน่วยงานหรือองค์กรเพื่อให้มีความต่อเนื่อง</b></p>	
<p>๑๐.๑ ให้กำหนดแผนเพื่อรักษาไว้หรือกู้คืนการให้บริการสารสนเทศ หลังเกิดเหตุการณ์ที่ทำให้ การดำเนินงานหยุดชะงัก เพื่อให้ข้อมูลสารสนเทศอยู่ในสภาพพร้อมใช้งานตามระดับที่กำหนดไว้ภายในระยะเวลาที่กำหนดไว้</p> <p>๑๐.๒ จัดให้มีข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศที่จำเป็น โดยกำหนดให้เป็นส่วนหนึ่งของขั้นตอนการบริหารจัดการเพื่อการดำเนินงานอย่างต่อเนื่องในภาวะฉุกเฉิน</p> <p>๑๐.๓ กำหนดให้มีกรอบงานหลักสำหรับการพัฒนาแผนการบริหารจัดการเพื่อการดำเนินงานอย่างต่อเนื่องในภาวะฉุกเฉิน เพื่อให้การพัฒนาแผนต่าง ๆ เป็นไปในทิศทางเดียวกัน รวมทั้งสอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัย ตลอดจนมีการจัดลำดับความสำคัญ ก่อนหลังในการทดสอบและการดูแล</p> <p>๑๐.๔ ให้มีการทดสอบและปรับปรุงแผนการบริหารจัดการเพื่อการดำเนินงานอย่างต่อเนื่องในภาวะฉุกเฉินอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าแผนดังกล่าวเป็นปัจจุบันและมีประสิทธิผลอยู่เสมอ</p> <p>๑๐.๕ ให้มีการระบุเหตุการณ์ใด ๆ ที่อาจส่งผลให้การดำเนินงานหยุดชะงัก และความ เป็นไปได้ในการเกิดผลกระทบ ตลอดจนผลต่อเนื่องจากการหยุดชะงักนั้นในแง่ของความมั่นคง ปลอดภัยด้านสารสนเทศ</p>	
<p><b>๑๑. การตรวจสอบและการประเมินผลการปฏิบัติตามนโยบาย มาตรการ หลักเกณฑ์หรือกระบวนการใด ๆ รวมทั้งข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศ</b></p>	
<p>๑๑.๑ ให้มีการระบุไว้ให้ชัดเจนถึงแนวทางในการดำเนินงานของระบบสารสนเทศที่มีความ สอดคล้องตาม กฎหมายและข้อกำหนดตามสัญญาต่าง ๆ ของหน่วยงาน โดยต้องจัดทำเป็น เอกสาร และมีการปรับปรุงให้เป็นปัจจุบันอยู่เสมอ</p> <p>๑๑.๒ ป้องกันมิให้มีการใช้งานระบบสารสนเทศผิดวัตถุประสงค์</p> <p>๑๑.๓ พนักงานของหน่วยงานต้องดูแลให้งานที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้าน</p>	

หัวข้อ	รายละเอียด
<p>สารสนเทศที่อยู่ใน ขอบเขตความรับผิดชอบได้ดำเนินการไปโดยสอดคล้องกับกฎหมายและข้อกำหนดตามสัญญาต่าง ๆ ของหน่วยงาน</p> <p>๑๑.๔ จัดให้มีการคุ้มครองข้อมูลส่วนบุคคลโดยให้สอดคล้องกับกฎหมายและข้อกำหนดตามสัญญาต่าง ๆ ของหน่วยงาน</p> <p>๑๑.๕ ใช้เทคนิคการเข้ารหัสลับ ที่สอดคล้องกับกฎหมายและข้อกำหนดตามสัญญาต่าง ๆ ของหน่วยงาน</p> <p>๑๑.๖ ให้มีการทบทวนตรวจสอบระบบสารสนเทศในด้านเทคนิคอย่างสม่ำเสมอ เพื่อให้สอดคล้องกับมาตรฐานการพัฒนางานด้านความมั่นคงปลอดภัยด้านสารสนเทศ</p> <p>๑๑.๗ วางแผนและจัดให้มีข้อกำหนดการตรวจสอบและกิจกรรมที่เกี่ยวข้องกับการตรวจสอบระบบสารสนเทศ เพื่อลดความเสี่ยงในการเกิดการหยุดชะงักของการให้บริการ</p> <p>๑๑.๘ ป้องกันการเข้าใช้งานเครื่องมือที่ใช้เพื่อการตรวจสอบ เพื่อมิให้เกิดการใช้งานผิดประเภทหรือถูกละเมิดการใช้งาน (Compromise)</p> <p>๑๑.๙ กำหนดขั้นตอนปฏิบัติงานเพื่อให้มั่นใจว่าในการใช้งานข้อมูลนี้อาจถือเป็นทรัพย์สินทางปัญญาหรือการใช้งานซอฟต์แวร์มีความสอดคล้องกับกฎหมายและข้อกำหนดตามสัญญาต่าง ๆ</p> <p>๑๑.๑๐ ป้องกันมิให้ข้อมูลสารสนเทศที่สำคัญเกิดความเสียหาย สูญหายหรือถูกปลอมแปลง โดยให้สอดคล้องกับกฎหมาย ข้อกำหนดตามสัญญาต่าง ๆ ของหน่วยงาน และข้อกำหนดการให้บริการ</p>	

(...) บริษัท .....

(...) นายหน้าประกันวินาศภัยหรือธนาคาร .....

(...) ผู้ให้บริการซึ่งเป็นบุคคลภายนอก.....

ขอรับรองว่าข้อความและข้อมูลตามหลักเกณฑ์ที่กำหนดในเอกสารฉบับนี้ถูกต้องตรงตามความเป็นจริงทุกประการ และยินดีต้อนรับข้อมูลที่เกี่ยวข้องกับการตรวจสอบมาตรฐานของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

ประทับตรา (ถ้ามี)

ลงชื่อ .....

(.....)

กรรมการผู้มีอำนาจ/ผู้รับมอบอำนาจ\*

\*กรรมการผู้มีอำนาจ/ผู้รับมอบอำนาจของบริษัท/นายหน้าประกันวินาศภัยหรือธนาคาร หรือผู้ให้บริการซึ่งเป็นบุคคลภายนอก แล้วแต่กรณี

**หมายเหตุ:** หลักเกณฑ์ตามแนวทางทางการประเมินมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับเครื่องครัดฉบับนี้เป็นการเทียบเคียงหลักเกณฑ์ตามบัญชีแนบท้ายประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕ และในกรณีที่หลักเกณฑ์ตามบัญชีแนบท้ายประกาศฯ ดังกล่าวมีการปรับแก้ไขเพิ่มเติม ให้หลักเกณฑ์ตามแนวทางทางการประเมินมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับเครื่องครัดฉบับนี้ ปรับแก้ไขเพิ่มเติมและใช้บังคับโดยเป็นไปตามหลักเกณฑ์ที่ได้มีการปรับแก้ไขเพิ่มเติมดังกล่าว