

# คูฉบับ



คปก.

สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย  
การประกอบธุรกิจประกันภัย(คปภ.)

ประกาศสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย  
เรื่อง หลักเกณฑ์ วิธีการ และเงื่อนไขการขึ้นทะเบียนกิจกรรมทางอิเล็กทรอนิกส์  
การขอรับความเห็นชอบการใช้บริการบุคคลภายนอก และการรับรองระบบสารสนเทศ  
พ.ศ. ๒๕๖๐

อาศัยอำนาจตามความในข้อ ๑๘ (๒)(๓) และข้อ ๑๙ (๒) (๔) แห่งประกาศคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง หลักเกณฑ์ วิธีการออกกรมธรรม์ประกันภัย การเสนอขายกรมธรรม์ประกันภัย และการชดใช้เงินตามสัญญาประกันชีวิต โดยใช้วิธีการทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๖๐ สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง หลักเกณฑ์ วิธีการ และเงื่อนไขการขึ้นทะเบียนกิจกรรมทางอิเล็กทรอนิกส์ การขอรับความเห็นชอบการใช้บริการบุคคลภายนอก และการรับรองระบบสารสนเทศ พ.ศ. ๒๕๖๐”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันประกาศเป็นต้นไป

ข้อ ๓ ในประกาศนี้

“สำนักงาน” หมายความว่า สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย

“บริษัท” หมายความว่า บริษัทประกันชีวิตตามกฎหมายว่าด้วยการประกันชีวิต

“นายหน้าประกันชีวิต” หมายความว่า นายหน้าประกันชีวิตตามกฎหมายว่าด้วยการประกันชีวิต ไม่รวมถึงธนาคาร

“ธนาคาร” หมายความว่า ธนาคารที่ได้รับใบอนุญาตเป็นนายหน้าประกันชีวิตตามกฎหมายว่าด้วยการประกันชีวิต

“ผู้ให้บริการซึ่งเป็นบุคคลภายนอก” หมายความว่า ผู้ซึ่งมีระบบสารสนเทศไว้ให้บริการในการเสนอขายกรมธรรม์ประกันภัยผ่านทางอิเล็กทรอนิกส์ การใช้วิธีการทางอิเล็กทรอนิกส์ประกอบการเสนอขายกรมธรรม์ประกันภัย การออกกรมธรรม์ประกันภัย หรือการชดใช้เงินตามสัญญาประกันชีวิต ตามประกาศคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัยว่าด้วยหลักเกณฑ์ วิธีการออกกรมธรรม์ประกันภัย การเสนอขายกรมธรรม์ประกันภัย และการชดใช้เงินตามสัญญาประกันชีวิต โดยใช้วิธีการทางอิเล็กทรอนิกส์

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

Information Security Management หรือโดยหน่วยงานรับรองระบบสารสนเทศ (Certified Body)

“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) และสำนักงานมาตรฐานผลิตภัณฑ์อุตสาหกรรม (สมอ.) หรือหน่วยรับรองระบบงานอื่นที่สำนักงานยอมรับ

ข้อ ๔ ให้บริษัทที่ประสงค์จะขอขึ้นทะเบียนยื่นคำขอต่อสำนักงานตามแบบ อช. ๑ ที่แนบท้ายประกาศนี้ พร้อมเอกสารหลักฐานประกอบคำขอ ดังต่อไปนี้เป็นอย่างน้อย

- (๑) เอกสารแสดงกิจกรรมและรายละเอียดที่ต้องการใช้วิธีการทางอิเล็กทรอนิกส์
- (๒) แผนผัง (Flow chart) และขั้นตอนของกิจกรรมที่ใช้วิธีการทางอิเล็กทรอนิกส์
- (๓) เอกสารแสดงระบบสารสนเทศและวิธีการทางอิเล็กทรอนิกส์ที่ใช้เพื่อรองรับกิจกรรมที่ใช้วิธีการทางอิเล็กทรอนิกส์
- (๔) แนวนโยบายและแนวปฏิบัติด้านการบริหารจัดการความเป็นส่วนตัวและข้อมูลส่วนบุคคล

(๕) หนังสือรับรองการตรวจรับรองการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศในระดับเครื่องครัดสำหรับกิจกรรมตาม (๑) โดยผู้ตรวจสอบอิสระตามหนังสือรับรองตามแบบ อช. ๓ ที่แนบท้ายประกาศนี้ หรือประกาศนียบัตรที่ออกโดยหน่วยงานรับรองระบบสารสนเทศ ทั้งนี้ บริษัทต้องแสดงข้อมูลแก่สำนักงานจนเป็นที่พอใจได้ว่าระบบสารสนเทศที่ได้รับการรับรองตามประกาศนียบัตรดังกล่าว มีความมั่นคงปลอดภัยของระบบสารสนเทศในระดับเครื่องครัดสำหรับกิจกรรมตาม (๑)

ข้อ ๕ ให้นายหน้าประกันชีวิต หรือธนาคารที่ประสงค์จะขอขึ้นทะเบียนยื่นคำขอต่อสำนักงานตามแบบ อช. ๒ ที่แนบท้ายประกาศนี้ พร้อมเอกสารหลักฐานประกอบคำขอ ดังต่อไปนี้เป็นอย่างน้อย

- (๑) เอกสารแสดงกิจกรรมและรายละเอียดที่ต้องการใช้วิธีการทางอิเล็กทรอนิกส์
- (๒) แผนผัง (Flow chart) และขั้นตอนของกิจกรรมที่ใช้วิธีการทางอิเล็กทรอนิกส์
- (๓) เอกสารแสดงระบบสารสนเทศและวิธีการทางอิเล็กทรอนิกส์ที่ใช้เพื่อรองรับกิจกรรมที่ใช้วิธีการทางอิเล็กทรอนิกส์
- (๔) แนวนโยบายและแนวปฏิบัติด้านการบริหารจัดการความเป็นส่วนตัวและข้อมูลส่วนบุคคล

(๕) หนังสือรับรองการตรวจรับรองการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของบริษัท และนายหน้าประกันชีวิต หรือธนาคาร ในระดับเครื่องครัดสำหรับกิจกรรมตาม (๑) โดยผู้ตรวจสอบอิสระตามหนังสือรับรองตามแบบ อช. ๓ ที่แนบท้ายประกาศนี้ หรือประกาศนียบัตรที่ออกโดยหน่วยงานรับรองระบบสารสนเทศ ทั้งนี้ บริษัท และนายหน้าประกันชีวิต หรือธนาคาร ต้องแสดงข้อมูลแก่สำนักงานจนเป็นที่พอใจได้ว่าระบบสารสนเทศที่ได้รับการรับรองตามประกาศนียบัตรดังกล่าว มีความมั่นคงปลอดภัยของระบบสารสนเทศในระดับเครื่องครัดสำหรับกิจกรรมตาม (๑)

ข้อ ๖ ในการขอขึ้นทะเบียนและขอรับความเห็นชอบการใช้บริการบุคคลภายนอก ให้บริษัทดำเนินการหรือจัดการให้นายหน้าประกันชีวิต หรือธนาคาร ดำเนินการยื่นคำขอต่อ สำนักงานตามแบบ อช. ๔ ที่แนบท้ายประกาศนี้ พร้อมเอกสารหลักฐานประกอบคำขอ ดังต่อไปนี้ เป็นอย่างน้อย

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

(๔) หนังสือรับรองการตรวจรับรองการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของผู้ให้บริการซึ่งเป็นบุคคลภายนอก และของบริษัท นายหน้าประกันชีวิต หรือธนาคารในระดับเครื่องครัดสำหรับกิจกรรมตาม (๑) โดยผู้ตรวจสอบอิสระตามหนังสือรับรองตามแบบ อช. ๓ ที่แนบท้ายประกาศนี้ หรือประกาศนียบัตรที่ออกโดยหน่วยงานรับรองระบบสารสนเทศ ทั้งนี้ บริษัท นายหน้าประกันชีวิต หรือธนาคาร ต้องแสดงข้อมูลแก่สำนักงานจนเป็นที่พอใจได้ว่าระบบสารสนเทศที่ได้รับการรับรองตามประกาศนียบัตรดังกล่าว มีความมั่นคงปลอดภัยของระบบสารสนเทศในระดับเครื่องครัดสำหรับกิจกรรมตาม (๑)

(๕) เอกสารแสดงเหตุผลและข้อมูลเกี่ยวกับการกำหนดนโยบาย กระบวนการ และวิธีปฏิบัติที่ชัดเจน เช่น ระบบการประเมินความเสี่ยง การบริหารความเสี่ยง ขั้นตอนของการบริการ การควบคุมภายใน การรักษาความมั่นคงปลอดภัย และแผนรองรับกรณีที่บุคคลภายนอกไม่สามารถให้บริการได้

(๖) สำเนาสัญญาใช้บริการระบบสารสนเทศระหว่างผู้ให้บริการซึ่งเป็นบุคคลภายนอก และบริษัท นายหน้าประกันชีวิต หรือธนาคาร แล้วแต่กรณี ซึ่งครอบคลุมเงื่อนไข ดังต่อไปนี้

- (ก) มาตรการรักษาความมั่นคงปลอดภัยเพื่อคุ้มครองข้อมูลส่วนบุคคล
- (ข) การป้องกันการใช้หรือเปิดเผยโดยมิชอบ
- (ค) การรายงานถึงความผิดปกติและการรายงานถึงการละเมิดข้อมูลส่วนบุคคล
- (ง) การป้องกันการจ้างช่วง
- (จ) สิทธิการตรวจสอบโดยบริษัทและสำนักงาน
- (ฉ) การคืน ทำลาย หรือลบข้อมูลส่วนบุคคล
- (ช) ผลของการละเมิดเงื่อนไข

ข้อ ๗ ในกรณีที่ บริษัท นายหน้าประกันชีวิต หรือธนาคารยื่นคำขอขึ้นทะเบียน หรือคำขอรับความเห็นชอบการใช้บริการบุคคลภายนอก พร้อมเอกสารหลักฐานประกอบคำขอ ไม่ถูกต้องครบถ้วน สำนักงานจะแจ้งให้บริษัท นายหน้าประกันชีวิต หรือธนาคารดำเนินการแก้ไข หรือยื่นเอกสารหลักฐานประกอบคำขอเพิ่มเติม ภายในระยะเวลาที่สำนักงานกำหนด

หากไม่ดำเนินการแก้ไข หรือยื่นเอกสารหลักฐานประกอบคำขอเพิ่มเติมให้ถูกต้อง ครบถ้วนภายในระยะเวลาดังกล่าว โดยปราศจากเหตุอันสมควร สำนักงานมีสิทธิปฏิเสธการพิจารณา คำขอดังกล่าวได้

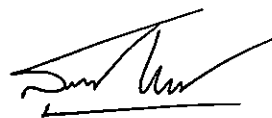
ข้อ ๘ ในการพิจารณาคำขอขึ้นทะเบียน หรือคำขอรับความเห็นชอบการใช้บริการบุคคลภายนอก สำนักงานจะพิจารณาคำขอให้แล้วเสร็จภายในสามสิบวันนับแต่วันที่รับคำขอ

พร้อมเอกสารประกอบคำขอครบถ้วนแล้ว เว้นแต่กรณีจำเป็นหรือมีเหตุอันสมควร สำนักงานอาจขยายระยะเวลาออกไปก็ได้ ทั้งนี้ ไม่เกินสองครั้ง และครั้งละไม่เกินสิบห้าวัน และเมื่อได้รับความเห็นชอบแล้ว บริษัท นายหน้าประกันชีวิต หรือธนาคาร แล้วแต่กรณี ต้องดำเนินการให้เป็นไปตามที่ยื่นขอขึ้นทะเบียนหรือขอรับความเห็นชอบไว้ตลอดเวลา

ในกรณีมีการแก้ไขเพิ่มเติม หรือเปลี่ยนแปลงข้อมูลที่เคยได้รับความเห็นชอบให้บริษัท นายหน้าประกันชีวิต หรือธนาคาร แล้วแต่กรณี ขอความเห็นชอบแก้ไขเพิ่มเติมหรือเปลี่ยนแปลงข้อมูลเป็นลายลักษณ์อักษร ทั้งนี้ หากเป็นการแก้ไขเพิ่มเติม หรือเปลี่ยนแปลงข้อมูลเกี่ยวกับกิจกรรมที่ใช้วิธีการทางอิเล็กทรอนิกส์ หรือระบบสารสนเทศที่ใช้กับกิจกรรม ให้บริษัท นายหน้าประกันชีวิต หรือธนาคาร ยื่นคำขอขึ้นทะเบียนหรือขอรับความเห็นชอบตามแบบ อช. ๑ อช. ๒ หรืออช. ๔ ฉบับใหม่ พร้อมเอกสารหลักฐานประกอบคำขอด้วย

บริษัท นายหน้าประกันชีวิต หรือธนาคารใด ยื่นคำขอขึ้นทะเบียน หรือ คำขอรับความเห็นชอบการใช้บริการบุคคลภายนอก พร้อมเอกสารหลักฐานประกอบคำขอกับสำนักงานภายในหนึ่งร้อยแปดสิบวันนับแต่วันที่ประกาศนี้ใช้บังคับ ให้บริษัท นายหน้าประกันชีวิต หรือธนาคารนั้น สามารถดำเนินการตามที่ได้ยื่นคำขอไปพลางก่อนได้ จนกว่าสำนักงานจะแจ้งผลการพิจารณาเป็นอย่างอื่นเป็นลายลักษณ์อักษร ทั้งนี้ ภายในระยะเวลาไม่เกินเก้าสิบวันนับแต่วันที่สำนักงานได้รับคำขอพร้อมเอกสารประกอบคำขอครบถ้วนแล้ว

ประกาศ ณ วันที่ ๒๕ พฤษภาคม พ.ศ. ๒๕๖๐



(นายสุทธิพล ทวีชัยการ)

เลขาธิการ

คณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย

หมายเหตุ :- เพื่อกำหนดหลักเกณฑ์และเงื่อนไขการขึ้นทะเบียน และการขอรับความเห็นชอบการ  
รับรองระบบสารสนเทศ และกำหนดระดับมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบ  
สารสนเทศ สำหรับการออกกรรมธรรม์ประกันภัย การเสนอขายกรรมธรรม์ประกันภัย และการชดใช้เงิน  
ตามสัญญาประกันชีวิต โดยการใช้วิธีการทางอิเล็กทรอนิกส์

ณัฐนิชา/ร่าง/พิมพ์  
/ทาน

คำขอขึ้นทะเบียนกิจกรรมทางอิเล็กทรอนิกส์และการรับรองระบบสารสนเทศ  
(กรณีบริษัทประกันชีวิต)

เขียนที่ .....

วันที่ ..... เดือน..... พ.ศ. ....

๑. บริษัท ..... มีความประสงค์  
ขอขึ้นทะเบียนกิจกรรมทางอิเล็กทรอนิกส์ เพื่อใช้วิธีการทางอิเล็กทรอนิกส์ในเรื่อง

- (....) การเสนอขายกรมธรรม์ประกันภัยผ่านทางอิเล็กทรอนิกส์ (Online)
- (....) การใช้วิธีการทางอิเล็กทรอนิกส์ประกอบการเสนอขายกรมธรรม์ประกันภัย
- (....) การออกกรมธรรม์ประกันภัย
- (....) การชดใช้เงินตามสัญญาประกันภัย

๒. บริษัทได้มอบหมายให้ นาย/นาง/นางสาว .....เป็นผู้บริหารซึ่งมีหน้าที่ดูแลรับผิดชอบงานด้านสารสนเทศที่เกี่ยวข้องตามที่ยื่นขอขึ้นทะเบียนหรือขอรับความเห็นชอบในครั้งนี้

๓. บริษัทขอรับรองว่าระบบสารสนเทศของบริษัทมีมาตรฐานความมั่นคงและปลอดภัยในระดับ  
เครื่องครัดสำหรับกิจกรรมตามข้อ ๑. โดยได้รับการตรวจสอบและรับรองจากผู้ตรวจสอบอิสระตามหนังสือ  
รับรองตามแบบ อช. ๓ หรือตามประกาศนียบัตรที่ออกโดยหน่วยงานรับรองระบบสารสนเทศ

๔. บริษัทได้แนบเอกสาร โดยมีรายการดังต่อไปนี้

- (....) เอกสารแสดงกิจกรรมและรายละเอียดที่ต้องการใช้วิธีการทางอิเล็กทรอนิกส์
- (....) แผนผัง (Flow chart) และขั้นตอนของกิจกรรมที่ใช้วิธีการทางอิเล็กทรอนิกส์
- (....) เอกสารแสดงระบบสารสนเทศและวิธีการทางอิเล็กทรอนิกส์ที่ใช้เพื่อรองรับกิจกรรมที่ใช้  
วิธีการทางอิเล็กทรอนิกส์

(....) นโยบายและแนวปฏิบัติด้านการบริหารจัดการความเป็นส่วนตัวและข้อมูลส่วนบุคคล

(....) หนังสือรับรองการตรวจรับรองการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

โดยผู้ตรวจสอบอิสระตามแบบ อช. ๓ หรือประกาศนียบัตรที่ออกโดยหน่วยงานรับรองระบบ  
สารสนเทศ

(....) เอกสารแนวทางการประเมินมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการ  
แบบปลอดภัยในระดับเครื่องครัดตามหลักเกณฑ์ที่กำหนดในเอกสารแนบท้ายประกาศ (กรณีมีการตรวจ  
รับรองจากผู้ตรวจสอบอิสระตามหนังสือรับรองตามแบบ อช. ๓)

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

ประทับตรา (ถ้ามี)

ลงชื่อ .....

(.....)

กรรมการผู้มีอำนาจ/  
ผู้รับมอบอำนาจของบริษัท

คำขอขึ้นทะเบียนกิจกรรมทางอิเล็กทรอนิกส์และการรับรองระบบสารสนเทศ  
(กรณีนายหน้าประกันชีวิตหรือธนาคาร)

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

๑. ข้าพเจ้า ..... ซึ่งมีใบอนุญาต  
เป็นนายหน้าประกันชีวิต เลขที่ ..... ใบอนุญาตหมดอายุ.....  
มีความประสงค์ขอขึ้นทะเบียนกิจกรรมทางอิเล็กทรอนิกส์ เพื่อใช้วิธีการทางอิเล็กทรอนิกส์ในเรื่อง  
(...) การเสนอขายกรมธรรม์ประกันภัยผ่านทางอิเล็กทรอนิกส์ (Online) ซึ่งได้รับความยินยอม  
จากบริษัท..... ในการทำกิจกรรม  
(...) การใช้วิธีการทางอิเล็กทรอนิกส์ประกอบการเสนอขายกรมธรรม์ประกันภัย  
และบริษัทได้รับรองระบบสารสนเทศของบริษัทที่เกี่ยวข้องกับระบบสารสนเทศสำหรับ  
กิจกรรมตามข้อ ๑. ว่ามีมาตรฐานความมั่นคงและปลอดภัยในระดับเครื่องครัดตามหลักเกณฑ์ที่กำหนด  
ในเอกสารแนบท้ายประกาศนี้ และมอบหมายให้นาย/นาง/นางสาว.....  
เป็นผู้บริหารซึ่งมีหน้าที่ดูแลรับผิดชอบงานด้านสารสนเทศที่เกี่ยวข้องของบริษัท
๒. ข้าพเจ้าได้มอบหมายให้ นาย/นาง/นางสาว ..... เป็น  
ผู้บริหารซึ่งมีหน้าที่ดูแลรับผิดชอบงานด้านสารสนเทศที่เกี่ยวข้องตามที่ยื่นขอขึ้นทะเบียนหรือขอรับ  
ความเห็นชอบในครั้งนี้
๓. ข้าพเจ้าขอรับรองว่าระบบสารสนเทศของข้าพเจ้ามีมาตรฐานความมั่นคงและปลอดภัยในระดับ  
เครื่องครัดสำหรับกิจกรรมตามข้อ ๑. ตามหลักเกณฑ์ที่กำหนดในเอกสารแนบท้ายประกาศนี้ โดยได้รับ  
การตรวจสอบและรับรองจากผู้ตรวจสอบอิสระตามหนังสือรับรองตามแบบ อช. ๓ หรือตาม  
ประกาศนียบัตรที่ออกโดยหน่วยงานรับรองระบบสารสนเทศ
๔. ข้าพเจ้าได้แนบเอกสาร โดยมีรายการดังต่อไปนี้
- (...) เอกสารแสดงกิจกรรมและรายละเอียดที่ต้องการใช้วิธีการทางอิเล็กทรอนิกส์
  - (...) แผนผัง (Flow chart) และขั้นตอนของกิจกรรมที่ใช้วิธีการทางอิเล็กทรอนิกส์
  - (...) เอกสารแสดงระบบสารสนเทศและวิธีการทางอิเล็กทรอนิกส์ที่ใช้เพื่อรองรับกิจกรรมที่ใช้  
วิธีการทางอิเล็กทรอนิกส์
  - (...) นโยบายและแนวปฏิบัติด้านการบริหารจัดการความเป็นส่วนตัวและข้อมูลส่วนบุคคล
  - (...) หนังสือรับรองการตรวจรับรองการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของ  
ข้าพเจ้าโดยผู้ตรวจสอบอิสระตามแบบ อช. ๓ หรือประกาศนียบัตรที่ออกโดยหน่วยงานรับรองระบบ  
สารสนเทศ
  - (...) หนังสือรับรองการตรวจรับรองการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของบริษัท  
โดยผู้ตรวจสอบอิสระตามแบบ อช. ๓ หรือประกาศนียบัตรที่ออกโดยหน่วยงานรับรองระบบ  
สารสนเทศ
  - (...) เอกสารแนวทางการประเมินมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ  
ตามวิธีการแบบปลอดภัยในระดับเครื่องครัดตามหลักเกณฑ์ที่กำหนดในเอกสารแนบท้ายประกาศ  
(กรณีมีการตรวจรับรองจากผู้ตรวจสอบอิสระตามหนังสือรับรองตามแบบ อช. ๓)

(....) หนังสือรับรองระบบสารสนเทศของบริษัทว่ามีมาตรฐานความมั่นคงและปลอดภัยของบริษัท  
ในระดับเครื่องครัดลงนามโดยกรรมการผู้มีอำนาจลงนามหรือผู้รับมอบอำนาจของบริษัท

(....) หนังสือยินยอมของบริษัทให้เสนอขายกรรมธรรม์ประกันภัยผ่านทางอิเล็กทรอนิกส์ (Online)

ข้าพเจ้า..... ขอรับรองว่าข้อความ  
และข้อมูลในแบบ อช. ๒ นี้ ถูกต้องตรงตามความเป็นจริงทุกประการ

ประทับตรา (ถ้ามี)

ลงชื่อ .....

(.....)

กรรมการผู้มีอำนาจ/

ผู้รับมอบอำนาจของนายหน้าประกันชีวิตหรือธนาคาร



หนังสือรับรอง

การตรวจรับรองการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศโดยผู้ตรวจสอบอิสระ

เขียนที่ .....

วันที่ ..... เดือน..... พ.ศ. ....

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

(...) หน่วยงานรับรองระบบสารสนเทศ.....เป็นหน่วยงานรับรองระบบ  
สารสนเทศ ที่ไม่อยู่ระหว่างการถูกระงับหรือเพิกถอนการขึ้นทะเบียน และได้รับการขึ้นทะเบียนจาก  
หน่วยงาน..... และได้แนบสำเนา  
เอกสารการขึ้นทะเบียนมาด้วยพร้อมกันนี้

๒. ข้าพเจ้าขอรับรองว่าได้ตรวจสอบระบบสารสนเทศของ

(...) บริษัท .....

(...) นายหน้าประกันชีวิตหรือธนาคาร .....

(...) ผู้ให้บริการซึ่งเป็นบุคคลภายนอก.....

เพื่อใช้วิธีการทางอิเล็กทรอนิกส์ในเรื่อง

(...) การเสนอขายกรมธรรม์ประกันภัยผ่านทางอิเล็กทรอนิกส์ (Online)

(...) การใช้วิธีการทางอิเล็กทรอนิกส์ประกอบการเสนอขายกรมธรรม์ประกันภัย

(...) การออกกรมธรรม์ประกันภัย

(...) การชดใช้เงินตามสัญญาประกันภัย

มีมาตรฐานความมั่นคงและปลอดภัยตามแนวทางการประเมินมาตรฐานการรักษาความมั่นคง  
ปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับเคร่งครัดที่แนบท้ายประกาศนี้

๓. ข้าพเจ้าได้ตรวจสอบระบบสารสนเทศเป็นที่เรียบร้อยแล้วตามหลักวิชาชีพและตามมาตรฐานที่  
อ้างอิงตามประกาศสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง  
หลักเกณฑ์ วิธีการ และเงื่อนไขการขึ้นทะเบียนกิจกรรมทางอิเล็กทรอนิกส์ การขอรับความเห็นชอบ  
การใช้บริการบุคคลภายนอก และการรับรองระบบสารสนเทศ พ.ศ. ๒๕๖๐ และยินยอมให้สำนักงาน  
สามารถตรวจสอบความถูกต้องของข้อมูลประกาศนียบัตรกับหน่วยงานออกประกาศนียบัตรหรือ  
เอกสารการขึ้นทะเบียนหน่วยงานรับรองระบบสารสนเทศกับหน่วยงานขึ้นทะเบียนตามข้อ ๑. ได้  
ข้าพเจ้าจึงลงลายมือชื่อไว้เป็นหลักฐาน

ประทับตรา (ถ้ามี)

ลงชื่อ .....

(.....)

ผู้ตรวจสอบอิสระ/หน่วยงานรับรองระบบสารสนเทศ

๔. ข้าพเจ้าซึ่งเป็นบุคคลตามข้อ ๒. ขอรับรองว่าข้อมูลที่ได้ให้แก่ผู้ตรวจสอบอิสระเพื่อใช้ตรวจรับรองการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศเป็นข้อมูลที่ถูกต้องตรงตามความเป็นจริงทุกประการ จึงได้ลงลายมือชื่อไว้เป็นหลักฐาน

ประทับตรา (ถ้ามี)

ลงชื่อ .....

(.....)

กรรมการผู้มีอำนาจ/ผู้รับมอบอำนาจ\*

\*กรรมการผู้มีอำนาจ/ผู้รับมอบอำนาจของบริษัท/นายหน้าประกันชีวิตหรือธนาคาร หรือผู้ให้บริการ ซึ่งเป็นบุคคลภายนอก แล้วแต่กรณี

คำขอรับความเห็นชอบการใช้บริการบุคคลภายนอก และการรับรองระบบสารสนเทศ

ส่วนที่ ๑ กรณีบริษัทใช้บริการบุคคลภายนอก

๑. บริษัท .....

มีความประสงค์ขอขึ้นทะเบียนกิจกรรมทางอิเล็กทรอนิกส์และขอรับความเห็นชอบในการใช้  
บริการระบบสารสนเทศของผู้ให้บริการซึ่งเป็นบุคคลภายนอก.....(ระบุชื่อผู้ให้บริการ).....  
เพื่อใช้วิธีการทางอิเล็กทรอนิกส์ในเรื่อง

- (....) การเสนอขายกรมธรรม์ประกันภัยผ่านทางอิเล็กทรอนิกส์ (Online)
- (....) การใช้วิธีการทางอิเล็กทรอนิกส์ประกอบการเสนอขายกรมธรรม์ประกันภัย
- (....) การออกกรมธรรม์ประกันภัย
- (....) การชดใช้เงินตามสัญญาประกันภัย

๒. บริษัทขอรับรองว่า

๒.๑ ผู้ให้บริการซึ่งเป็นบุคคลภายนอกมีระบบสารสนเทศที่มีมาตรฐานความมั่นคงและปลอดภัยในระดับ  
เครื่องครัดสำหรับกิจกรรมตามข้อ ๑. ตามหลักเกณฑ์ที่กำหนดในเอกสารแนบท้ายประกาศนี้ โดยได้รับการ  
ตรวจสอบและรับรองจากผู้ตรวจสอบอิสระตามหนังสือรับรองตามแบบ อช. ๓ หรือตามประกาศนียบัตร  
ที่ออกโดยหน่วยงานรับรองระบบสารสนเทศ และ

บริษัทมีระบบสารสนเทศที่มีมาตรฐานความมั่นคงและปลอดภัยในระดับเครื่องครัดสำหรับกิจกรรมตาม  
ข้อ ๑. ตามหลักเกณฑ์ที่กำหนดในเอกสารแนบท้ายประกาศนี้ โดยได้รับการตรวจสอบและรับรองจาก  
ผู้ตรวจสอบอิสระตามหนังสือรับรองตามแบบ อช. ๓ หรือตามประกาศนียบัตรที่ออกโดยหน่วยงาน  
รับรองระบบสารสนเทศ

๒.๒ ได้กำหนดนโยบาย กระบวนการและวิธีปฏิบัติที่ชัดเจน เช่น ระบบการประเมินความเสี่ยง  
การบริหารความเสี่ยง ขั้นตอนของการบริการ การควบคุมภายใน การรักษาความปลอดภัย และแผน  
รองรับกรณีทีบุคคลภายนอกไม่สามารถให้บริการได้

๒.๓ สัญญาใช้บริการระบบสารสนเทศระหว่างบริษัทกับผู้ให้บริการซึ่งเป็นบุคคลภายนอก  
ครอบคลุมเงื่อนไข ดังต่อไปนี้

- (ก) มาตรการรักษาความมั่นคงปลอดภัยเพื่อคุ้มครองข้อมูลส่วนบุคคล
- (ข) การป้องกันการใช้หรือเปิดเผยโดยมิชอบ
- (ค) การรายงานถึงความผิดปกติและการรายงานถึงการละเมิดข้อมูลส่วนบุคคล
- (ง) การป้องกันการจ้างช่วง
- (จ) สิทธิการตรวจสอบโดยบริษัทและสำนักงาน
- (ฉ) การคืน ทำลาย หรือลบข้อมูลส่วนบุคคล
- (ช) ผลของการละเมิดเงื่อนไข

๓. บริษัทได้แนบเอกสาร โดยมีรายการดังต่อไปนี้

(....) หนังสือรับรองนิติบุคคลจากกรมพัฒนาธุรกิจการค้ากรณีผู้ให้บริการซึ่งเป็นบุคคลภายนอกเป็น  
นิติบุคคล

- (....) เอกสารแสดงกิจกรรมและรายละเอียดที่ต้องการใช้วิธีการทางอิเล็กทรอนิกส์
- (....) แผนผัง (Flow chart) และขั้นตอนของกิจกรรมที่ใช้วิธีการทางอิเล็กทรอนิกส์

(...) เอกสารแสดงระบบสารสนเทศและวิธีการทางอิเล็กทรอนิกส์ที่ใช้เพื่อรองรับกิจกรรมที่ใช้วิธีการทางอิเล็กทรอนิกส์

(...) หนังสือรับรองระบบสารสนเทศของผู้ให้บริการซึ่งเป็นบุคคลภายนอกว่ามีมาตรฐานความมั่นคงและปลอดภัย

(...) หนังสือรับรองการตรวจรับรองการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของผู้ให้บริการซึ่งเป็นบุคคลภายนอกโดยผู้ตรวจสอบอิสระตามแบบ อช. ๓ หรือประกาศนียบัตรที่ออกโดยหน่วยงานรับรองระบบสารสนเทศ

(...) หนังสือรับรองการตรวจรับรองการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของบริษัทโดยผู้ตรวจสอบอิสระตามแบบ อช. ๓ หรือประกาศนียบัตรที่ออกโดยหน่วยงานรับรองระบบสารสนเทศ

(...) เอกสารแนวทางการประเมินมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับเครื่องครัดตามหลักเกณฑ์ที่กำหนดในเอกสารแนบท้ายประกาศ (กรณีมีการตรวจรับรองจากผู้ตรวจสอบอิสระตามหนังสือรับรองตามแบบ อช. ๓)

(...) สำเนาสัญญาให้บริการระบบสารสนเทศระหว่างบริษัทกับผู้ให้บริการซึ่งเป็นบุคคลภายนอก

## ส่วนที่ ๒ กรณีนายหน้าประกันชีวิตหรือธนาคารใช้บริการบุคคลภายนอก

๔. ข้าพเจ้า ..... ซึ่งมีใบอนุญาตเป็นนายหน้าประกันชีวิต เลขที่ ..... ใบอนุญาตหมดอายุ.....

มีความประสงค์ขอขึ้นทะเบียนกิจกรรมทางอิเล็กทรอนิกส์และขอรับความเห็นชอบในการใช้บริการระบบสารสนเทศของผู้ให้บริการซึ่งเป็นบุคคลภายนอก เพื่อใช้วิธีการทางอิเล็กทรอนิกส์ในเรื่อง

(...) การเสนอขายกรมธรรม์ประกันภัยผ่านทางอิเล็กทรอนิกส์ (Online) ซึ่งได้รับความยินยอมจากบริษัท..... ในการทำงาน

(...) การใช้วิธีการทางอิเล็กทรอนิกส์ประกอบการเสนอขายกรมธรรม์ประกันภัย

ได้รับความยินยอมจากบริษัท..... ในกิจกรรมข้างต้น และบริษัทได้รับรองระบบสารสนเทศของบริษัทที่เกี่ยวข้องกับระบบสารสนเทศสำหรับกิจกรรมตามข้อ ๔. ว่ามีมาตรฐานความมั่นคงและปลอดภัยในระดับเครื่องครัดตามหลักเกณฑ์ที่กำหนดในเอกสารแนบท้ายประกาศนี้ และมอบหมายให้นาย/นาง/นางสาว.....เป็นผู้บริหารซึ่งมีหน้าที่ดูแลรับผิดชอบงานด้านสารสนเทศที่เกี่ยวข้องของบริษัท

๕. ข้าพเจ้าขอรับรองว่า

๕.๑ ระบบสารสนเทศของผู้ให้บริการซึ่งเป็นบุคคลภายนอกมีมาตรฐานความมั่นคงและปลอดภัยในระดับเครื่องครัดสำหรับกิจกรรมตามข้อ ๔ ตามหลักเกณฑ์ที่กำหนดในเอกสารแนบท้ายประกาศนี้ โดยได้รับการตรวจสอบและรับรองจากผู้ตรวจสอบอิสระตามหนังสือรับรองตามแบบ อช. ๓ หรือตามประกาศนียบัตรที่ออกโดยหน่วยงานรับรองระบบสารสนเทศ และ

ข้าพเจ้ามีระบบสารสนเทศที่มีมาตรฐานความมั่นคงและปลอดภัยในระดับเครื่องครัดสำหรับกิจกรรมตามข้อ ๔. ตามหลักเกณฑ์ที่กำหนดในเอกสารแนบท้ายประกาศนี้ โดยได้รับการตรวจสอบและรับรองจากผู้ตรวจสอบอิสระตามหนังสือรับรองตามแบบ อช. ๓ หรือตามประกาศนียบัตรที่ออกโดยหน่วยงานรับรองระบบสารสนเทศ

๕.๒ ได้กำหนดนโยบาย กระบวนการและวิธีปฏิบัติที่ชัดเจน เช่น ระบบการประเมินความเสี่ยง การบริหารความเสี่ยง ขั้นตอนของการบริการ การควบคุมภายใน การรักษาความปลอดภัย และแผนรองรับกรณีที่บุคคลภายนอกไม่สามารถให้บริการได้

๕.๓ สัญญาใช้บริการระบบสารสนเทศระหว่างข้าพเจ้ากับผู้ให้บริการซึ่งเป็นบุคคลภายนอก  
ครอบคลุมเงื่อนไข ดังต่อไปนี้

- (ก) มาตรการรักษาความมั่นคงปลอดภัยเพื่อคุ้มครองข้อมูลส่วนบุคคล
- (ข) การป้องกันการใช้หรือเปิดเผยโดยมิชอบ
- (ค) การรายงานถึงความผิดปกติและการรายงานถึงการละเมิดข้อมูลส่วนบุคคล
- (ง) การป้องกันการจ้างช่วง
- (จ) สิทธิการตรวจสอบโดยบริษัทและสำนักงาน
- (ฉ) การคืน ทำลาย หรือลบข้อมูลส่วนบุคคล
- (ช) ผลของการละเมิดเงื่อนไข

๖. ข้าพเจ้าได้แนบเอกสาร โดยมีรายการดังต่อไปนี้

- (....) เอกสารแสดงกิจกรรมและรายละเอียดที่ต้องการใช้วิธีการทางอิเล็กทรอนิกส์
- (....) แผนผัง (Flow chart) และขั้นตอนของกิจกรรมที่ใช้วิธีการทางอิเล็กทรอนิกส์
- (....) เอกสารแสดงระบบสารสนเทศและวิธีการทางอิเล็กทรอนิกส์ที่ใช้เพื่อรองรับกิจกรรมที่ใช้  
วิธีการทางอิเล็กทรอนิกส์

(....) หนังสือรับรองระบบสารสนเทศของผู้ให้บริการซึ่งเป็นบุคคลภายนอกว่ามีมาตรฐานความ  
มั่นคงและปลอดภัย (ไม่ใช้กับกรณีบริษัทเป็นผู้ให้บริการซึ่งเป็นบุคคลภายนอก)

(....) หนังสือรับรองการตรวจรับรองการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของ  
ผู้ให้บริการซึ่งเป็นบุคคลภายนอกโดยผู้ตรวจสอบอิสระตามแบบ อช. ๓ หรือตามประกาศนียบัตรที่  
ออกโดยหน่วยงานรับรองระบบสารสนเทศ

(....) หนังสือรับรองการตรวจรับรองการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของ  
ข้าพเจ้าโดยผู้ตรวจสอบอิสระตามแบบ อช. ๓ หรือตามประกาศนียบัตรที่ออกโดยหน่วยงานรับรอง  
ระบบสารสนเทศ

(....) เอกสารแนวทางการประเมินมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ  
ตามวิธีการแบบปลอดภัยในระดับเคร่งครัดตามหลักเกณฑ์ที่กำหนดในเอกสารแนบท้ายประกาศ  
(กรณีมีการตรวจรับรองจากผู้ตรวจสอบอิสระตามหนังสือรับรองตามแบบ อช. ๓)

(....) สำเนาสัญญาใช้บริการระบบสารสนเทศระหว่างข้าพเจ้ากับผู้ให้บริการซึ่งเป็นบุคคลภายนอก

(....) หนังสือรับรองระบบสารสนเทศของบริษัทว่ามีมาตรฐานความมั่นคงและปลอดภัยของบริษัท  
ซึ่งลงนามโดยกรรมการผู้มีอำนาจลงนามหรือผู้รับมอบอำนาจของบริษัท

(....) หนังสือยินยอมของบริษัทให้เสนอขายกรรมธรรม์ประกันภัยผ่านทางอิเล็กทรอนิกส์ (Online)

(....) บริษัท .....

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

ขอรับรองว่า ข้อความและข้อมูลในแบบ อช. ๔ นี้ ถูกต้องตรงตามความเป็นจริงทุกประการ

ประทับตรา (ถ้ามี)

ลงชื่อ .....

(.....)

กรรมการผู้มีอำนาจ/ผู้รับมอบอำนาจ\*

\*กรรมการผู้มีอำนาจ/ผู้รับมอบอำนาจของบริษัท/นายหน้าประกันชีวิตหรือธนาคาร แล้วแต่กรณี

แนวทางการประเมินมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ  
ตามวิธีการแบบปลอดภัยในระดับเคร่งครัด

| หัวข้อ  | รายละเอียด |
|---|------------|
| <p>๑. การสร้างความมั่นคงปลอดภัยด้านการบริหารจัดการ</p>  |            |
| <p>๑.๑ กำหนดนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยผ่านการอนุมัติ และผลักดันโดยผู้บริหารระดับสูง และมีการประกาศ นโยบายดังกล่าวให้พนักงานและ บุคคลภายนอกที่เกี่ยวข้องรับทราบโดยทั่วกัน</p> <p>๑.๒ วางแผนการติดตามและประเมินผลการใช้งานความมั่นคงปลอดภัยด้านสารสนเทศ และ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างสม่ำเสมอ เพื่อปรับปรุงหากมีการ เปลี่ยนแปลงใด ๆ ภายในหน่วยงาน ทั้งนี้เพื่อให้เหมาะสมกับสถานการณ์การใช้งาน และคง ความมีประสิทธิภาพอยู่เสมอ</p>   |            |
| <p>๒. การจัดโครงสร้างด้านความมั่นคงปลอดภัยของระบบสารสนเทศในด้านการบริหารจัดการด้านความ มั่นคงปลอดภัยของระบบสารสนเทศ ทั้งภายในและภายนอกหน่วยงานหรือองค์กร</p>  |            |
| <p>๒.๑ ผู้บริหารระดับสูงของหน่วยงานมีหน้าที่ดูแลรับผิดชอบงานด้านสารสนเทศของ หน่วยงานให้การสนับสนุน และกำหนดทิศทางการดำเนินงานเกี่ยวกับความมั่นคงปลอดภัยด้าน สารสนเทศที่ชัดเจน รวมทั้งมีการมอบหมายงานที่เกี่ยวข้องให้กับผู้ปฏิบัติงานอย่างชัดเจน ตลอดจนรับผิดชอบต่อความเสี่ยง ความเสียหาย หรือ อันตรายที่เกิดขึ้นกับระบบสารสนเทศไม่ว่ากรณีใด ๆ</p> <p>๒.๒ สำหรับระบบสารสนเทศใหม่มีการกำหนดขั้นตอนการพิจารณาทบทวน เพื่ออนุมัติการ สร้าง การติดตั้ง หรือการใช้งานในแง่มุมต่าง ๆ เช่น การบริหารจัดการผู้ใช้งานระบบ หรือ ความสามารถในการทำงานร่วมกันได้ระหว่างระบบเดิมและระบบใหม่</p> <p>๒.๓ มีการกำหนดสัญญาการรักษาข้อมูลที่เป็นความลับ (Confidentiality agreement หรือ NonDisclosure agreement) ที่สอดคล้องกับสถานการณ์และความต้องการของ หน่วยงานในการปกป้องข้อมูลสารสนเทศ</p> <p>๒.๔ มีข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศสำหรับการอนุญาตให้ ผู้ใช้บริการที่เป็นบุคคลภายนอกเข้าถึงระบบสารสนเทศ หรือใช้ข้อมูลสารสนเทศของหน่วยงาน</p> <p>๒.๕ สำหรับข้อตกลงเพื่ออนุญาตให้บุคคลภายนอกเข้าถึงระบบสารสนเทศ หรือใช้ข้อมูล สารสนเทศของหน่วยงาน เพื่อการอ่าน การประมวลผล การบริหารจัดการระบบสารสนเทศ หรือการพัฒนาสารสนเทศ ควรมีข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ ระบุไว้ในข้อตกลง</p> <p>๒.๖ มีการกำหนดเงื่อนไขหรือหน้าที่ความรับผิดชอบต่าง ๆ เกี่ยวกับความมั่นคงปลอดภัย ด้านสารสนเทศไว้อย่างชัดเจน</p> <p>๒.๗ มีการกำหนดขั้นตอนและช่องทางในการติดต่อกับหน่วยงานภายนอกที่มีความ เชี่ยวชาญเฉพาะด้าน หรือหน่วยงานที่มีความเชี่ยวชาญด้านความมั่นคงปลอดภัยด้านสารสนเทศ ภายใต้สถานการณ์ต่าง ๆ ไว้อย่างชัดเจน</p> <p>๒.๘ จัดให้มีการพิจารณาทบทวนแนวทางในการบริหารจัดการงานเกี่ยวกับความมั่นคง ปลอดภัยด้าน สารสนเทศอย่างสม่ำเสมอ หรือเมื่อมีการเปลี่ยนแปลงใด ๆ ในการดำเนินงาน</p> |            |

| หัวข้อ  | รายละเอียด |
|---|------------|
| <p>ทั้งนี้ การพิจารณาบททวนดังกล่าว ควรดำเนินการโดยผู้ไม่มีส่วนได้เสียกับงานที่มีการพิจารณาบททวน</p> <p>๒.๙ มีการสร้างความร่วมมือระหว่างผู้ที่มีบทบาทเกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน ในงานหรือกิจกรรมใด ๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศ</p> <p>๒.๑๐ มีการกำหนดขั้นตอนและช่องทางในการติดต่อกับหน่วยงานภายนอกที่มีหน้าที่ในการกำกับดูแล หรือหน่วยงานที่เกี่ยวข้องกับการบังคับใช้กฎหมาย รวมทั้งหน่วยงานที่ควบคุมดูแลสถานการณ์ฉุกเฉินภายใต้สถานการณ์ ต่าง ๆ ไว้อย่างชัดเจน</p> <p>๒.๑๑ ก่อนที่จะอนุญาตให้หน่วยงานหรือบุคคลภายนอกเข้าถึงระบบสารสนเทศหรือใช้ข้อมูลสารสนเทศของหน่วยงาน 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 และมอบหมายให้มีผู้รับผิดชอบอย่างชัดเจน</p> <p>๔.๕ พนักงานหน่วยงานหรือบุคคลภายนอกที่ว่าจ้างต้องส่งคืนทรัพย์สินสารสนเทศของหน่วยงานเมื่อสิ้นสุดสถานะการเป็นพนักงาน หรือสิ้นสุดสัญญาหรือข้อตกลงการปฏิบัติงานให้กับหน่วยงาน</p> <p>๔.๖ ให้ยกเลิกสิทธิของพนักงานหน่วยงานหรือบุคคลภายนอกในการเข้าใช้งานระบบ</p> |            |

| หัวข้อ   | รายละเอียด |
|--|------------|
| <p>สารสนเทศ เมื่อสิ้นสุดสถานะการเป็นพนักงาน หรือสิ้นสุดสัญญาหรือข้อตกลงการปฏิบัติงาน และให้ปรับเปลี่ยนระดับสิทธิในการเข้าถึงงานระบบสารสนเทศให้เหมาะสมเมื่อมีการเปลี่ยนแปลงหน้าที่ความรับผิดชอบใด ๆ เกิดขึ้น</p> <p>๔.๗ พนักงาน หน่วยงานหรือบุคคลภายนอกต้องได้รับการอบรมเพื่อสร้างความตระหนักรู้เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศในส่วนที่ เกี่ยวข้องกับหน้าที่ความรับผิดชอบของตน และได้รับการสื่อสารให้ทราบถึงนโยบายหรือระเบียบปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศที่หน่วยงานประกาศใช้อย่างสม่ำเสมอ หรือเมื่อมีการเปลี่ยนแปลง</p> <p>๔.๘ ในการพิจารณารับพนักงานเข้าทำงาน หรือการว่าจ้างหน่วยงานหรือบุคคลภายนอก ให้มีการตรวจสอบประวัติหรือคุณสมบัติเพื่อให้เป็นไปตามกฎหมาย กฎระเบียบและจริยธรรมที่เกี่ยวข้อง โดยให้คำนึงถึงระดับชั้นความลับของข้อมูลสารสนเทศที่จะให้เข้าถึง และระดับความเสี่ยงที่ได้ประเมิน</p> <p>๔.๙ ในสัญญาจ้างหรือข้อตกลงการปฏิบัติงานของพนักงาน หรือสัญญาว่าจ้างหน่วยงานหรือบุคคลภายนอก 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> |            |



| หัวข้อ  | รายละเอียด |
|---|------------|
| <p>๕.๑๒ มีการรักษาความมั่นคงปลอดภัยให้กับอุปกรณ์สารสนเทศที่มีการนำไปใช้งานนอกสถานที่ปฏิบัติงานของหน่วยงาน โดยให้คำนึงถึงระดับความเสี่ยงที่แตกต่างกันจากการนำไปใช้งานในสถานที่ต่าง ๆ</p> <p>๕.๑๓ ก่อนการยกเลิกการใช้งานหรือจำหน่ายอุปกรณ์สารสนเทศที่ใช้ในการจัดเก็บข้อมูลสารสนเทศต้องมีการตรวจสอบอุปกรณ์สารสนเทศนั้นว่า ได้มีการลบ ย้าย หรือทำลายข้อมูลที่สำคัญหรือซอฟต์แวร์ที่จัดซื้อและติดตั้งไว้ด้วยวิธีการที่ทำให้ไม่สามารถกู้คืนได้อีก</p>  |            |
| <p><b>๖. การบริหารจัดการด้านการสื่อสารและการดำเนินงานของระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์และระบบสารสนเทศ</b></p>  |            |
| <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 จัดให้มีเกณฑ์การตรวจรับระบบสารสนเทศที่มีการปรับปรุง หรือที่มีเวอร์ชันใหม่ และควรมีการทดสอบระบบสารสนเทศทั้งในช่วงการพัฒนาระบบและก่อนการตรวจรับ</p> <p>๖.๕ มีขั้นตอนควบคุมการตรวจสอบ ป้องกัน และกู้คืนในกรณีมีการใช้งานโปรแกรมไม่พึงประสงค์และให้มีการสร้างความตระหนักรู้ให้กับผู้ใช้งานระบบสารสนเทศหรือข้อมูลสารสนเทศเกี่ยวกับโปรแกรมไม่พึงประสงค์</p> <p>๖.๖ มีการสำรองข้อมูลสารสนเทศ และทดสอบการนำกลับมาใช้งาน โดยให้เป็นไปตามนโยบายการสำรองข้อมูลที่หน่วยงานประกาศใช้</p> <p>๖.๗ มีการบริหารจัดการการควบคุมเครือข่ายคอมพิวเตอร์เพื่อป้องกันภัยคุกคาม และมีการรักษาความ มั่นคงปลอดภัยของระบบสารสนเทศและแอปพลิเคชันที่ทำงานบนเครือข่ายคอมพิวเตอร์รวมทั้งข้อมูลสารสนเทศ 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</p> |            |

| หัวข้อ   | รายละเอียด |
|--|------------|
| <p>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 (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 ขั้นตอนปฏิบัติงาน หรือการควบคุมเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ โดยคำนึงถึงระดับความสำคัญของการดำเนินธุรกิจที่เกี่ยวข้องและการประเมินความเสี่ยงอย่างต่อเนื่อง</p> <p>๖.๒๗ หากหน่วยงานอนุญาตให้มีการใช้งาน Mobile code (เช่น Script บางอย่างของเว็บ แอปพลิเคชันที่มีการทำงานอัตโนมัติเมื่อเรียกดูเว็บ) ควรมีการตั้งค่าการทำงาน (Configuration) เพื่อให้มั่นใจได้ว่าการทำงานของ Mobile code นั้นเป็นไปตามความมั่นคงปลอดภัยด้านสารสนเทศและนโยบายในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศ และห้ามโดยอัตโนมัติมิให้ Mobile code สามารถทำงานได้ในระบบสารสนเทศ หากในนโยบาย การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กำหนดห้ามมิให้ประเภทของ Mobile code ดังกล่าวทำงานได้</p> <p>๖.๒๘ มีขั้นตอนการปฏิบัติงานสำหรับการบริหารจัดการอุปกรณ์ที่ใช้ในการบันทึกข้อมูล อิเล็กทรอนิกส์ที่สามารถถอดหรือต่อพ่วงกับเครื่องคอมพิวเตอร์ได้ (Removable media)</p> |            |

| หัวข้อ  | รายละเอียด |
|---|------------|
| <p>๖.๒๙ มีขั้นตอนการปฏิบัติงานในการทำลายอุปกรณ์ที่ใช้ในการบันทึกข้อมูลอิเล็กทรอนิกส์ที่สามารถถอด หรือต่อพ่วงกับเครื่องคอมพิวเตอร์ได้ (Removable media) อย่างมั่นคงปลอดภัย</p> <p>๖.๓๐ มีการป้องกันมิให้ข้อมูลหรือเอกสารเกี่ยวกับระบบสารสนเทศ (System documentation) ถูกเข้าถึง โดยมีได้รับอนุญาต</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 และมีการติดตามทบทวนให้นโยบายดังกล่าว 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 ให้อุบัติหรือปิดหน้าจอการใช้งานระบบสารสนเทศโดยอัตโนมัติหากไม่มีการใช้งานเกินระยะเวลาสูงสุด ที่กำหนดไว้</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 ให้มีการกำหนดวิธีการตรวจสอบตัวตนที่เหมาะสมเพื่อควบคุมการเข้าถึงระบบ</p> |            |

| หัวข้อ   | รายละเอียด |
|--|------------|
| <p>สารสนเทศของ 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> <p>๗.๒๑ ให้มีการระบุอุปกรณ์ที่เชื่อมต่อเข้ากับระบบสารสนเทศโดยอัตโนมัติ (Automatic equipment identification) เพื่อตรวจสอบการเชื่อมต่อของอุปกรณ์ดังกล่าวว่ามาจากอุปกรณ์ดังกล่าวจริง หรือจากสถานที่ที่กำหนดไว้เท่านั้น ทั้งนี้จำเป็นสำหรับการที่ระบบสารสนเทศจะรับการเชื่อมต่อจากเฉพาะอุปกรณ์ที่ได้รับอนุญาต หรือมาจากเฉพาะสถานที่ที่ได้รับอนุญาต</p> <p>๗.๒๒ ให้จำกัดการเข้าถึงการใช้งานโปรแกรมมัลติมีเดียต่าง 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>๘. การจัดหาหรือจัดให้มีการพัฒนา และการบำรุงรักษาระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ระบบงานคอมพิวเตอร์และระบบสารสนเทศ</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>  |            |

| หัวข้อ   | รายละเอียด |
|--|------------|
| <p>๘.๔ ให้มีการตรวจสอบ (Validate) ข้อมูลใด ๆ อันเป็นผลจากการประมวลผลของ แอปพลิเคชัน เพื่อให้มั่นใจได้ว่า ข้อมูลที่ได้จากการประมวลผลถูกต้องและเหมาะสม</p> <p>๘.๕ จัดให้มีแนวทางการบริหารจัดการกุญแจ (Key) เพื่อรองรับการใช้งานเทคนิคที่เกี่ยวข้องกับการเข้ารหัสลับของหน่วยงาน</p> <p>๘.๖ ให้เลือกชุดข้อมูลสารสนเทศที่จะนำไปใช้เพื่อการทดสอบในระบบสารสนเทศอย่าง ะมัดระวัง รวมทั้งมีแนวทางควบคุมและป้องกันข้อมูลรั่วไหล</p> <p>๘.๗ ให้มีการจำกัดการเข้าถึงซอร์สโค้ด (Source code) ของโปรแกรม</p> <p>๘.๘ หากมีการเปลี่ยนแปลงใด ๆ ในระบบปฏิบัติการคอมพิวเตอร์ให้มีการตรวจสอบ ทบทวนการทำงานของโปรแกรมที่มีความสำคัญ และทดสอบการใช้งานเพื่อให้มั่นใจว่าผลของ การเปลี่ยนแปลงดังกล่าว จะไม่ส่งผลกระทบต่อ ความมั่นคงปลอดภัยของระบบสารสนเทศ และการให้บริการของหน่วยงาน</p> <p>๘.๙ ให้มีการตรวจสอบ (Validate) การทำงานของแอปพลิเคชันเพื่อตรวจหาข้อผิดพลาด ของข้อมูลนี้อาจเกิดจากการทำงานหรือการประมวลผลที่ผิดพลาด</p> <p>๘.๑๐ ให้มีข้อกำหนดขั้นต่ำสำหรับการรักษาความถูกต้องแท้จริง (Authenticity) และ ความถูกต้องครบถ้วน (Integrity) ของข้อมูลในแอปพลิเคชัน รวมทั้งมีการระบุและปฏิบัติตาม วิธีการป้องกันที่เหมาะสม</p> <p>๘.๑๑ จัดให้มีนโยบายในการใช้งานเทคนิคที่เกี่ยวข้องกับการเข้ารหัสลับ</p> <p>๘.๑๒ กำหนดให้มีขั้นตอนการปฏิบัติงานเพื่อควบคุมการติดตั้งซอฟต์แวร์บนระบบ สารสนเทศที่ให้บริการ</p> <p>๘.๑๓ ให้มีการควบคุมการเปลี่ยนแปลงต่าง ๆ ในการพัฒนาระบบสารสนเทศ โดยมีขั้นตอน การควบคุมที่เป็นทางการ</p> <p>๘.๑๔ ให้จำกัดการเปลี่ยนแปลงใด ๆ ต่อซอฟต์แวร์ที่ใช้งาน (Software package) โดยให้ เปลี่ยนแปลงเฉพาะเท่าที่จำเป็น และควบคุมทุก ๆ การเปลี่ยนแปลงอย่างเข้มงวด</p> <p>๘.๑๕ มีมาตรการป้องกันเพื่อลดโอกาสที่เกิดการรั่วไหลของข้อมูลสารสนเทศ</p> |            |
| <p>๙. การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด</p>  |            |
| <p>๙.๑ ให้มีการรายงานสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจ คาดคิดผ่าน ช่องทางการบริหารจัดการที่เหมาะสมโดยเร็วที่สุด</p> <p>๙.๒ กำหนดให้พนักงานหรือผู้ใช้งานที่เป็นบุคคลภายนอก มีการบันทึกและรายงานจุดอ่อน ใด ๆ ที่อาจสังเกตพบระหว่างการใช้งานระบบสารสนเทศ</p> <p>๙.๓ กำหนดขอบเขตความรับผิดชอบของผู้บริหารและขั้นตอนการปฏิบัติงาน เพื่อ ตอบสนองต่อสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด อย่าง รวดเร็ว มีระเบียบ และมีประสิทธิผล</p> <p>๙.๔ หากในขั้นตอนการติดตามผลกับบุคคลหรือหน่วยงานภายหลังจากเกิดสถานการณ์ด้าน ความมั่นคง ปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ซึ่งเกี่ยวข้องกับการดำเนินการทาง กฎหมาย (ไม่ว่าทางแพ่งหรือทาง อาญา) ให้มีการรวบรวม จัดเก็บ และนำเสนอหลักฐาน ให้ สอดคล้องกับหลักเกณฑ์ของกฎหมายที่ใช้บังคับ</p>  |            |

| หัวข้อ  | รายละเอียด |
|---|------------|
| <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 ให้มีการทดสอบและปรับปรุงแผนการบริหารจัดการเพื่อการดำเนินงานอย่างต่อเนื่อง ในภาวะฉุกเฉินอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าแผนดังกล่าวเป็นปัจจุบันและมีประสิทธิผลอยู่เสมอ</p> <p>๑๐.๕ ให้มีการระบุเหตุการณ์ใด ๆ ที่อาจส่งผลให้การดำเนินงานหยุดชะงัก และความเป็นไปได้ในการเกิดผลกระทบ ตลอดจนผลต่อเนื่องจากการหยุดชะงักนั้นในแง่ของความมั่นคง ปลอดภัยด้านสารสนเทศ</p>  |            |
| <p><b>๑๑. การตรวจสอบและการประเมินผลการปฏิบัติตามนโยบาย มาตรการ หลักเกณฑ์หรือกระบวนการใด ๆ รวมทั้งข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศ</b></p>   |            |
| <p>๑๑.๑ ให้มีการระบุไว้ให้ชัดเจนถึงแนวทางในการดำเนินงานของระบบสารสนเทศที่มีความสอดคล้องตาม กฎหมายและข้อกำหนดตามสัญญาต่าง ๆ ของหน่วยงาน โดยต้องจัดทำเป็น เอกสาร และมีการปรับปรุงให้เป็นปัจจุบันอยู่เสมอ</p> <p>๑๑.๒ ป้องกันมิให้มีการใช้งานระบบสารสนเทศผิดวัตถุประสงค์</p> <p>๑๑.๓ พนักงานของหน่วยงานต้องดูแลให้งานที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศที่อยู่ในขอบเขตความรับผิดชอบได้ดำเนินการไปโดยสอดคล้องกับกฎหมายและ ข้อกำหนดตามสัญญาต่าง ๆ ของหน่วยงาน</p> <p>๑๑.๔ จัดให้มีการคุ้มครองข้อมูลส่วนบุคคลโดยให้สอดคล้องกับกฎหมายและข้อกำหนด ตามสัญญาต่าง ๆ ของหน่วยงาน</p> <p>๑๑.๕ ใช้เทคนิคการเข้ารหัสลับ ที่สอดคล้องกับกฎหมายและข้อกำหนดตามสัญญาต่าง ๆ ของหน่วยงาน</p> <p>๑๑.๖ ให้มีการทบทวนตรวจสอบระบบสารสนเทศในด้านเทคนิคอย่างสม่ำเสมอ เพื่อให้ สอดคล้องกับมาตรฐานการพัฒนางานด้านความมั่นคงปลอดภัยด้านสารสนเทศ</p> <p>๑๑.๗ วางแผนและจัดให้มีข้อกำหนดการตรวจสอบและกิจกรรมที่เกี่ยวข้องกับการ ตรวจสอบระบบสารสนเทศ เพื่อลดความเสี่ยงในการเกิดการหยุดชะงักของการให้บริการ</p> <p>๑๑.๘ ป้องกันการเข้าใช้งานเครื่องมือที่ใช้เพื่อการตรวจสอบ เพื่อมิให้เกิดการใช้งานผิด ประเภทหรือถูกละเมิดการใช้งาน (Compromise)</p> <p>๑๑.๙ กำหนดขั้นตอนปฏิบัติงานเพื่อให้มั่นใจว่าในการใช้งานข้อมูลนี้อาจถือเป็นทรัพย์สิน ทางปัญญาหรือการใช้งานซอฟต์แวร์มีความสอดคล้องกับกฎหมายและข้อกำหนดตามสัญญาต่าง ๆ</p> |            |

| หัวข้อ   | รายละเอียด |
|--|------------|
| ๑๑.๑๐ ป้องกันมิให้ข้อมูลสารสนเทศที่สำคัญเกิดความเสียหาย สูญหายหรือถูกปลอมแปลง โดยให้สอดคล้องกับกฎหมาย ข้อกำหนดตามสัญญาต่าง ๆ ของหน่วยงาน และข้อกำหนดการให้บริการ |            |

(...) บริษัท .....

(...) นายหน้าประกันชีวิตหรือธนาคาร .....

(...) ผู้ให้บริการซึ่งเป็นบุคคลภายนอก.....

ขอรับรองว่าข้อความและข้อมูลตามหลักเกณฑ์ที่กำหนดในเอกสารฉบับนี้ถูกต้องตรงตามความเป็นจริงทุกประการ และยินดีนำส่งข้อมูลที่เกี่ยวข้องกับการตรวจสอบมาตรฐานของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

ประทับตรา (ถ้ามี)

ลงชื่อ .....

(.....)

กรรมการผู้มีอำนาจ/ผู้รับมอบอำนาจ\*

\*กรรมการผู้มีอำนาจ/ผู้รับมอบอำนาจของบริษัท/นายหน้าประกันชีวิตหรือธนาคาร หรือผู้ให้บริการ ซึ่งเป็นบุคคลภายนอก แล้วแต่กรณี

หมายเหตุ: หลักเกณฑ์ตามแนวทางการประเมินมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับเคร่งครัดฉบับนี้เป็นการเทียบเคียงหลักเกณฑ์ตามบัญชีแนบท้ายประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕ และในกรณีที่หลักเกณฑ์ตามบัญชีแนบท้ายประกาศฯ ดังกล่าวมีการปรับแก้ไขเพิ่มเติม ให้หลักเกณฑ์ตามแนวทางการประเมินมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับเคร่งครัดฉบับนี้ ปรับแก้ไขเพิ่มเติมและใช้บังคับโดยเป็นไปตามหลักเกณฑ์ที่ได้มีการปรับแก้ไขเพิ่มเติมดังกล่าว