ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

เรื่อง รายชื่อหน่วยงานหรือองค์กร หรือส่วนงานของหน่วยงานหรือองค์กรที่ถือเป็นโครงสร้างพื้นฐานสำคัญของประเทศซึ่งต้องกระทำตามวิธีการแบบปลอดภัยในระดับเคร่งครัด พ.ศ. ๒๕๕๙

โดยที่พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓ กำหนดให้คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ประกาศกำหนดรายชื่อหน่วยงานหรือองค์กรหรือส่วนงานของหน่วยงานหรือองค์กรที่ถือเป็นโครงสร้างพื้นฐานสำคัญของประเทศ เพื่อให้ดำเนินการตามวิธีการแบบปลอดภัยในระดับเคร่งครัด ระดับกลาง หรือระดับพื้นฐาน แล้วแต่กรณี

อาศัยอำนาจตามความในมาตรา ๖ วรรคสอง แห่งพระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓ คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์จึงออกประกาศไว้ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า "ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง รายชื่อหน่วยงานหรือองค์กร หรือส่วนงานของหน่วยงานหรือองค์กรที่ถือเป็นโครงสร้างพื้นฐานสำคัญของประเทศซึ่งต้องกระทำตามวิธีการแบบปลอดภัยในระดับเคร่งครัด พ.ศ. ๒๕๕๙"

ข้อ ๒ ประกาศนี้ให้ใช้บังคับเมื่อพ้นกำหนดสามร้อยหกสิบวันนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ให้หน่วยงานหรือองค์กร หรือส่วนงานของหน่วยงานหรือองค์กรที่มีรายชื่อแนบท้ายประกาศฉบับนี้ ถือเป็นโครงสร้างพื้นฐานสำคัญของประเทศซึ่งต้องกระทำตามวิธีการแบบปลอดภัยในระดับเคร่งครัดตามพระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓

ประกาศ ณ วันที่ ๒๘ กรกฎาคม พ.ศ. ๒๕๕๙
อุตตม สาวนายน
รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
ประธานกรรมการธุรกรรมทางอิเล็กทรอนิกส์

แนบท้าย ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
เรื่อง รายชื่อหน่วยงานหรือองค์กร หรือส่วนงานของหน่วยงานหรือองค์กรที่ถือเป็น
โครงสร้างพื้นฐานสำคัญของประเทศซึ่งต้องกระทำตามวิธีการแบบปลอดภัยในระดับเคร่งครัด
พ.ศ. ๒๕๕๙
ว่าด้วยรายชื่อหน่วยงานหรือองค์กร หรือส่วนงานของหน่วยงานหรือองค์กร

<u>ส่วนราชการ</u>

๑. **สำนักนายกรัฐมนตรี** เฉพาะ

(๑) สำนักงานปลัดสำนักนายกรัฐมนตรี

(๒) กรมประชาสัมพันธ์

(๓) สำนักข่าวกรองแห่งชาติ

(๔) สำนักงบประมาณ

(๕) สำนักงานคณะกรรมการข้าราชการพลเรือน

(๖) สำนักงานคณะกรรมการส่งเสริมการลงทุน

๒. **กระทรวงกลาโหม** เฉพาะ

(๑) สำนักงานปลัดกระทรวงกลาโหม

(๒) กองบัญชาการกองทัพไทย

(๓) กองทัพบก

(๔) กองทัพเรือ

(๕) กองทัพอากาศ

๓. **กระทรวงการคลัง** เฉพาะ

(๑) กรมธนารักษ์

(๒) กรมบัญชีกลาง

(๓) กรมศุลกากร

(๔) กรมสรรพสามิต

(๕) กรมสรรพากร

(๖) สำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ

(๗) สำนักงานบริหารหนี้สาธารณะ

๔. **กระทรวงการต่างประเทศ**

๕. **กระทรวงเกษตรและสหกรณ์** เฉพาะ

(๑) กรมชลประทาน

(๒) กรมประมง

(๓) กรมปศุสัตว์

(๔) กรมวิชาการเกษตร

(๕) กรมส่งเสริมสหกรณ์

๖. กระทรวงคมนาคม เฉพาะ

(๑) กรมเจ้าท่า

(๒) กรมการขนส่งทางบก

(๓) กรมท่าอากาศยาน

(๔) กรมทางหลวง

(๕) กรมทางหลวงชนบท

(๖) สำนักงานนโยบายและแผนการขนส่งและจราจร

๗. กระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม เฉพาะ

(๑) กรมควบคุมมลพิษ

๘. กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เฉพาะ

(๑) สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

(๒) กรมอุตุนิยมวิทยา

๙. กระทรวงพลังงาน เฉพาะ

(๑) กรมเชื้อเพลิงธรรมชาติ

(๒) กรมธุรกิจพลังงาน

๑๐.กระทรวงพาณิชย์ เฉพาะ

(๑) กรมการค้าภายใน

(๒) กรมพัฒนาธุรกิจการค้า

๑๑.กระทรวงมหาดไทย เฉพาะ

(๑) กรมการปกครอง

(๒) กรมที่ดิน

(๓) กรมป้องกันและบรรเทาสาธารณภัย

(๔) กรมโยธาธิการและผังเมือง

๑๒.กระทรวงยุติธรรม เฉพาะ

(๑) กรมบังคับคดี

(๒) กรมราชทัณฑ์

(๓) กรมสอบสวนคดีพิเศษ

(๔) สถาบันนิติวิทยาศาสตร์

(๕) สำนักงานคณะกรรมการป้องกันและปราบปรามยาเสพติด

(๖) สำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตในภาครัฐ

๑๓.กระทรวงแรงงาน เฉพาะ

(๑) กรมสวัสดิการและคุ้มครองแรงงาน

(๒) สำนักงานประกันสังคม

๑๔.กระทรวงวิทยาศาสตร์และเทคโนโลยี เฉพาะ

(๑) สำนักงานปรมาณูเพื่อสันติ

๑๕.กระทรวงศึกษาธิการ เฉพาะ

(๑) มหาวิทยาลัยขอนแก่น

(๒) มหาวิทยาลัยเชียงใหม่

(๓) มหาวิทยาลัยธรรมศาสตร์

(๔) มหาวิทยาลัยนเรศวร

(๕) มหาวิทยาลัยมหิดล

(๖) มหาวิทยาลัยศรีนครินทรวิโรฒ

(๗) มหาวิทยาลัยสงขลานครินทร์

๑๖.กระทรวงสาธารณสุข เฉพาะ

(๑) สำนักงานปลัดกระทรวงสาธารณสุข

(๒) กรมการแพทย์

(๓) กรมควบคุมโรค

(๔) กรมวิทยาศาสตร์การแพทย์

(๕) กรมอนามัย

(๖) สำนักงานคณะกรรมการอาหารและยา

๑๗.กระทรวงอุตสาหกรรม เฉพาะ

(๑) กรมโรงงานอุตสาหกรรม

(๒) สำนักงานคณะกรรมการอ้อยและน้ำตาลทราย

๑๘.ส่วนราชการไม่สังกัดสำนักนายกรัฐมนตรี กระทรวงหรือทบวง เฉพาะ

(๑) สำนักงานตำรวจแห่งชาติ

<u>องค์กรตามรัฐธรรมนูญ</u>

๑. สำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตแห่งชาติ

๒. สำนักงานอัยการสูงสุด

<u>รัฐวิสาหกิจ</u>

๑. การเคหะแห่งชาติ

๒. การทางพิเศษแห่งประเทศไทย

๓. การท่าเรือแห่งประเทศไทย

๔. การประปาส่วนภูมิภาค

๕. การประปานครหลวง

๖. การไฟฟ้านครหลวง

๗. การไฟฟ้าฝ่ายผลิตแห่งประเทศไทย

๘. การไฟฟ้าส่วนภูมิภาค

๙. การยางแห่งประเทศไทย

๑๐. การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย

๑๑. การรถไฟแห่งประเทศไทย

๑๒. ธนาคารกรุงไทย จำกัด (มหาชน)

๑๓. ธนาคารพัฒนาวิสาหกิจขนาดกลางและขนาดย่อมแห่งประเทศไทย

๑๔. ธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร

๑๕. ธนาคารเพื่อการส่งออกและนำเข้าแห่งประเทศไทย

๑๖. ธนาคารออมสิน

๑๗. ธนาคารอาคารสงเคราะห์

๑๘. ธนาคารอิสลามแห่งประเทศไทย

๑๙. บรรษัทตลาดรองสินเชื่อที่อยู่อาศัย

๒๐. บรรษัทประกันสินเชื่ออุตสาหกรรมขนาดย่อม

๒๑. บริษัท กสท โทรคมนาคม จำกัด (มหาชน)

๒๒. บริษัท การบินไทย จำกัด (มหาชน)

๒๓. บริษัท ขนส่ง จำกัด

๒๔. บริษัท ท่าอากาศยานไทย จำกัด (มหาชน)

๒๕. บริษัท ทีโอที จำกัด (มหาชน)

๒๖. บริษัท ปตท จำกัด (มหาชน)

๒๗. บริษัท ไปรษณีย์ไทย จำกัด

๒๘. บริษัท วิทยุการบินแห่งประเทศไทย จำกัด

๒๙. บริษัท อสมท จำกัด (มหาชน)

๓๐. องค์การเภสัชกรรม

๓๑. องค์การคลังสินค้า

๓๒. องค์การจัดการน้ำเสีย

๓๓. องค์การอุตสาหกรรมป่าไม้

๓๔. องค์การขนส่งมวลชนกรุงเทพ

๓๕. บริษัทบริหารสินทรัพย์ กรุงเทพพาณิชย์ จำกัด (มหาชน)

หน่วยงานอื่นของรัฐ

๑. กองทุนเงินให้กู้ยืมเงินเพื่อการศึกษา

๒. กองทุนบำเหน็จบำนาญข้าราชการ

๓. ตลาดหลักทรัพย์แห่งประเทศไทย

๔. ธนาคารแห่งประเทศไทย

๕. สถาบันการแพทย์ฉุกเฉินแห่งชาติ

๖. สภากาชาดไทย

๗. สำนักงานคณะกรรมการกำกับกิจการพลังงาน

๘. สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย

๙. สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์

องค์การมหาชน

๑. โรงพยาบาลบ้านแพ้ว (องค์การมหาชน)

๒. สำนักงานพัฒนาเทคโนโลยีอวกาศและภูมิสารสนเทศ (องค์การมหาชน)

๓. สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

๔. สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน)

องค์กรปกครองส่วนท้องถิ่น

๑. กรุงเทพมหานคร

<u>หน่วยงานภาคเอกชน</u>

๑. บริษัท ข้อมูลเครดิตแห่งชาติ จำกัด

๒. บริษัท สำนักหักบัญชี (ประเทศไทย) จำกัด

๓. บริษัท ศูนย์รับฝากหลักทรัพย์ (ประเทศไทย) จำกัด

๔. สมาคมตลาดตราสารหนี้ไทย

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕

โดยที่พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓ กำหนดให้คณะกรรมการประกาศกำหนดมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในแต่ละระดับ เพื่อให้การทำธุรกรรมทางอิเล็กทรอนิกส์ใดที่ได้กระทำตามวิธีการแบบปลอดภัยที่คณะกรรมการกำหนดเป็นวิธีการที่เชื่อถือได้

อาศัยอำนาจตามความในมาตรา ๗ แห่งพระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓ คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์จึงออกประกาศไว้ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า "ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕"

ข้อ ๒ ในกรณีที่จะต้องปฏิบัติให้เป็นไปตามมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับเคร่งครัด ระดับกลาง หรือระดับพื้นฐาน ให้หน่วยงานหรือองค์กร หรือส่วนงานของหน่วยงานหรือองค์กรปฏิบัติตามมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามหลักเกณฑ์ที่กำหนดในแนบท้ายประกาศฉบับนี้

ข้อ ๓ ประกาศนี้ให้ใช้บังคับเมื่อพ้นกำหนดสามร้อยหกสิบวันนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ประกาศ ณ วันที่ ๑๓ พฤศจิกายน พ.ศ. ๒๕๕๕
นาวาอากาศเอก อนุติษฐ์ นาครทรรพ
รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
ประธานกรรมการธุรกรรมทางอิเล็กทรอนิกส์

บัญชีแนบท้ายประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕

มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศเป็นมาตรการสำหรับใช้ในการควบคุมให้ระบบสารสนเทศมีความมั่นคงปลอดภัย ซึ่งครอบคลุมการรักษาความลับ (Confidentiality) การรักษาความครบถ้วน (Integrity) และการรักษาสภาพพร้อมใช้งาน (Availability) ของระบบสารสนเทศและสารสนเทศในระบบ นั้น โดยการทำธุรกรรมทางอิเล็กทรอนิกส์ด้วยระบบสารสนเทศ ต้องดำเนินการตามมาตรการที่เกี่ยวข้องตามบัญชีแนบท้ายนี้ และต้องพิจารณาให้สอดคล้องกับระดับความเสี่ยงที่ได้จากการประเมิน ทั้งนี้ มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ แบ่งออกเป็น ๑๑ ข้อ ได้แก่

๑. การสร้างความมั่นคงปลอดภัยด้านบริหารจัดการ
๒. การจัดโครงสร้างด้านความมั่นคงปลอดภัยของระบบสารสนเทศในส่วนการบริหารจัดการด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ทั้งภายในและภายนอกหน่วยงานหรือองค์กร
๓. การบริหารจัดการทรัพย์สินสารสนเทศ
๔. การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร
๕. การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม
๖. การบริหารจัดการด้านการสื่อสารและการดำเนินงานของระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ
๗. การควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์
๘. การจัดหาหรือจัดให้มีการพัฒนา และการบำรุงรักษาระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ
๙. การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด
๑๐. การบริหารจัดการด้านการบริการหรือการดำเนินงานของหน่วยงานหรือองค์กรเพื่อให้มีความต่อเนื่อง
๑๑. การตรวจสอบและการประเมินผลการปฏิบัติตามนโยบาย มาตรการ หลักเกณฑ์ หรือกระบวนการใด ๆ รวมทั้งข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

๑. มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับพื้นฐาน

การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับพื้นฐานต้องปฏิบัติดังนี้

ข้อ ๑. การสร้างความมั่นคงปลอดภัยด้านบริหารจัดการหน่วยงานต้องกำหนดนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยผ่านการอนุมัติและผลักดันโดยผู้บริหารระดับสูง และมีการประกาศนโยบายดังกล่าวให้พนักงานและบุคคลภายนอกที่เกี่ยวข้องรับทราบโดยทั่วกัน

ข้อ ๒. การจัดโครงสร้างด้านความมั่นคงปลอดภัยของระบบสารสนเทศในส่วนการบริหารจัดการด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ทั้งภายในและภายนอกหน่วยงานหรือองค์กร

๒.๑ ผู้บริหารระดับสูงของหน่วยงานมีหน้าที่ดูแลรับผิดชอบงานด้านสารสนเทศของหน่วยงานให้การสนับสนุน และกำหนดทิศทางการดำเนินงานเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศที่ชัดเจน รวมทั้งมีการมอบหมายงานที่เกี่ยวข้องให้กับผู้ปฏิบัติงานอย่างชัดเจน ตลอดจนรับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกับระบบสารสนเทศไม่ว่ากรณีใด ๆ

๒.๒ สำหรับระบบสารสนเทศใหม่ มีการกำหนดขั้นตอนการพิจารณาทบทวน เพื่ออนุมัติการสร้าง การติดตั้ง หรือการใช้งานในแง่มุมต่าง ๆ เช่น การบริหารจัดการผู้ใช้งานระบบ หรือความสามารถในการทำงานร่วมกันได้ระหว่างระบบเดิมและระบบใหม่

๒.๓ มีการกำหนดสัญญาการรักษาข้อมูลที่เป็นความลับ (Confidentiality agreement หรือ Non-Disclosure agreement) ที่สอดคล้องกับสถานการณ์และความต้องการของหน่วยงานในการปกป้องข้อมูลสารสนเทศ

๒.๔ มีข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศสำหรับการอนุญาตให้ผู้ใช้บริการที่เป็นบุคคลภายนอกเข้าถึงระบบสารสนเทศ หรือใช้ข้อมูลสารสนเทศของหน่วยงาน

๒.๕ สำหรับข้อตกลงเพื่ออนุญาตให้บุคคลภายนอกเข้าถึงระบบสารสนเทศ หรือใช้ข้อมูลสารสนเทศของหน่วยงาน เพื่อการอ่าน การประมวลผล การบริหารจัดการระบบสารสนเทศ หรือการพัฒนาระบบสารสนเทศ ควรมีข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศระบุไว้ในข้อตกลง

ข้อ ๓. การบริหารจัดการทรัพย์สินสารสนเทศมีการเก็บบันทึกข้อมูลทรัพย์สินสารสนเทศ โดยข้อมูลที่จัดเก็บต้องประกอบด้วยข้อมูลที่จำเป็นในการค้นหาเพื่อการใช้งานในภายหลัง

ข้อ ๔. การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร

๔.๑ กำหนดหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยด้านสารสนเทศของพนักงาน หรือหน่วยงานหรือบุคคลภายนอกที่ว่าจ้าง โดยให้สอดคล้องกับความมั่นคงปลอดภัยด้านสารสนเทศและนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่หน่วยงานประกาศใช้

๔.๒ ผู้บริหารระดับสูงของหน่วยงานต้องกำหนดให้พนักงาน หน่วยงานหรือบุคคลภายนอกที่ว่าจ้างปฏิบัติงานตามนโยบายหรือระเบียบปฏิบัติด้านความมั่นคงปลอดภัยที่หน่วยงานประกาศใช้

๔.๓ กำหนดให้มีขั้นตอนการลงโทษพนักงานที่ฝ่าฝืนนโยบายหรือระเบียบปฏิบัติเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศในหน่วยงาน

๔.๔ กำหนดหน้าที่ความรับผิดชอบในการยุติการจ้าง หรือการเปลี่ยนแปลงสถานะการจ้างให้ชัดเจน และมอบหมายให้มีผู้รับผิดชอบอย่างชัดเจน

๔.๕ พนักงาน หน่วยงานหรือบุคคลภายนอกที่ว่าจ้างต้องส่งคืนทรัพย์สินสารสนเทศของหน่วยงานเมื่อสิ้นสุดสถานะการเป็นพนักงาน หรือสิ้นสุดสัญญาหรือข้อตกลงการปฏิบัติงานให้กับหน่วยงาน

๔.๖ ให้ยกเลิกสิทธิของพนักงาน หน่วยงานหรือบุคคลภายนอกในการเข้าใช้งานระบบสารสนเทศ เมื่อสิ้นสุดสถานะการเป็นพนักงาน หรือสิ้นสุดสัญญาหรือข้อตกลงการปฏิบัติงาน และให้ปรับเปลี่ยนระดับสิทธิในการเข้าใช้งานระบบสารสนเทศให้เหมาะสมเมื่อมีการเปลี่ยนแปลงหน้าที่ความรับผิดชอบใด ๆ เกิดขึ้น

ข้อ ๕. การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม

๕.๑ ให้มีการป้องกันขอบเขตพื้นที่ตั้งของหน่วยงาน (Security perimeter) ที่มีการติดตั้ง จัดเก็บ หรือใช้งาน ระบบสารสนเทศและข้อมูลสารสนเทศ

๕.๒ มีการออกแบบและติดตั้งการป้องกันความมั่นคงปลอดภัยด้านกายภาพ เพื่อป้องกันภัยจากภายนอกภัยในระดับหายนะทั้งที่ก่อโดยมนุษย์หรือภัยธรรมชาติ เช่น อัคคีภัย อุทกภัย แผ่นดินไหว ระเบิด การก่อจลาจล เป็นต้น

๕.๓ จัดวางและป้องกันอุปกรณ์สารสนเทศ เพื่อลดความเสี่ยงจากภัยธรรมชาติหรืออันตรายต่าง ๆ และเพื่อป้องกันการเข้าถึงโดยมิได้รับอนุญาต

๕.๔ มีการป้องกันอุปกรณ์สารสนเทศ ที่อาจเกิดจากไฟฟ้าขัดข้อง (Power failure) หรือที่อาจหยุดชะงักจากข้อผิดพลาดของโครงสร้างพื้นฐาน (Supporting utilities)

๕.๕ มีการดูแลอุปกรณ์สารสนเทศอย่างถูกวิธี เพื่อให้คงไว้ซึ่งความถูกต้องครบถ้วนและอยู่ในสภาพพร้อมใช้งานอยู่เสมอ

ข้อ ๖. การบริหารจัดการด้านการสื่อสารและการดำเนินงานของระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

๖.๑ มีการจัดทำ ปรับปรุง และดูแลเอกสารขั้นตอนการปฏิบัติงานที่อยู่ในสภาพพร้อมใช้งาน เพื่อให้พนักงานสามารถนำไปปฏิบัติได้

๖.๒ มีการดูแลให้บุคคลหรือหน่วยงานภายนอกที่ให้บริการแก่หน่วยงานตามที่ว่างจ้างปฏิบัติตามสัญญาหรือข้อตกลงให้บริการที่ระบุไว้ ซึ่งต้องครอบคลุมถึงงานด้านความมั่นคงปลอดภัย ลักษณะการให้บริการ และระดับการให้บริการ

๖.๓ มีการติดตามตรวจสอบรายงานหรือบันทึกการให้บริการของบุคคลหรือหน่วยงานภายนอกที่ให้บริการแก่หน่วยงานตามที่ว่าจ้างอย่างสม่ำเสมอ

๖.๔ จัดให้มีเกณฑ์การตรวจรับระบบสารสนเทศที่มีการปรับปรุง หรือที่มีเวอร์ชั่นใหม่ และควรมีการทดสอบระบบสารสนเทศทั้งในช่วงการพัฒนาระบบและก่อนการตรวจรับ

๖.๕ มีขั้นตอนควบคุมการตรวจสอบ ป้องกัน และกู้คืนในกรณีมีการใช้งานโปรแกรมไม่พึงประสงค์ และให้มีการสร้างความตระหนักรู้ให้กับผู้ใช้งานระบบสารสนเทศหรือข้อมูลสารสนเทศเกี่ยวกับโปรแกรมไม่พึงประสงค์

๖.๖ มีการสำรองข้อมูลสารสนเทศ และทดสอบการนำกลับมาใช้งาน โดยให้เป็นไปตามนโยบายการสำรองข้อมูลที่หน่วยงานประกาศใช้

๖.๗ มีการบริหารจัดการการควบคุมเครือข่ายคอมพิวเตอร์ เพื่อป้องกันภัยคุกคาม และมีการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและแอพพลิเคชั่นที่ทำงานบนเครือข่ายคอมพิวเตอร์ รวมทั้งข้อมูลสารสนเทศที่มีการแลกเปลี่ยนบนเครือข่ายดังกล่าว

๖.๘ มีการกำหนดรูปแบบการรักษาความมั่นคงปลอดภัย ระดับการให้บริการ ข้อกำหนดการบริหารจัดการในข้อตกลงการให้บริการด้านเครือข่ายคอมพิวเตอร์ ไม่ว่าเป็นการให้บริการโดยหน่วยงานเอง หรือจ้างช่วงไปยังผู้ให้บริการภายนอก

๖.๙ จัดให้มีนโยบายและขั้นตอนปฏิบัติงาน รวมทั้งควบคุมการแลกเปลี่ยนข้อมูลสารสนเทศผ่านช่องทางการสื่อสารในรูปแบบข้อมูลอิเล็กทรอนิกส์

๖.๑๐ จัดให้มีข้อตกลงในการแลกเปลี่ยนข้อมูลสารสนเทศหรือซอฟต์แวร์ระหว่างหน่วยงานกับบุคคลหรือหน่วยงานภายนอก

๖.๑๑ จัดให้มีนโยบายและขั้นตอนการปฏิบัติงาน เพื่อป้องกันข้อมูลสารสนเทศที่มีการสื่อสารหรือแลกเปลี่ยนผ่านระบบสารสนเทศที่มีการเชื่อมต่อกับระบบสารสนเทศต่าง ๆ

๖.๑๒ มีการป้องกันข้อมูลสารสนเทศที่มีการแลกเปลี่ยนในการทำพาณิชย์อิเล็กทรอนิกส์ (Electronic commerce) ผ่านเครือข่ายคอมพิวเตอร์สาธารณะ เพื่อมิให้มีการฉ้อโกง ละเมิดสัญญา หรือมีการรั่วไหลหรือข้อมูลสารสนเทศถูกแก้ไขโดยมิได้รับอนุญาต

๖.๑๓ มีการป้องกันข้อมูลสารสนเทศที่มีการสื่อสารหรือแลกเปลี่ยนในการทำธุรกรรมทางออนไลน์ (Online transaction) เพื่อมิให้มีการรับส่งข้อมูลที่ไม่สมบูรณ์ หรือส่งข้อมูลไปผิดที่ หรือมีการรั่วไหลของข้อมูล หรือข้อมูลถูกแก้ไขเปลี่ยนแปลง ถูกทำซ้ำใหม่ หรือถูกส่งซ้ำโดยมิได้รับอนุญาต

๖.๑๔ สำหรับข้อมูลสารสนเทศที่มีการเผยแพร่ต่อสาธารณชน ให้มีการป้องกันมิให้มีการแก้ไขเปลี่ยนแปลงโดยมิได้รับอนุญาต และเพื่อรักษาความถูกต้องครบถ้วนของข้อมูลสารสนเทศ

๖.๑๕ มีการเก็บบันทึกข้อมูล Audit log ซึ่งบันทึกข้อมูลกิจกรรมการใช้งานของผู้ใช้งานระบบสารสนเทศ และเหตุการณ์เกี่ยวกับความมั่นคงปลอดภัยต่าง ๆ เพื่อประโยชน์ในการสืบสวน สอบสวน ในอนาคต และเพื่อการติดตามการควบคุมการเข้าถึง

๖.๑๖ มีขั้นตอนการเฝ้าติดตามสังเกตการใช้งานระบบสารสนเทศ และมีการติดตามประเมินผลการติดตามสังเกตดังกล่าวอย่างสม่ำเสมอ

๖.๑๗ มีการป้องกันระบบสารสนเทศที่จัดเก็บ Log และข้อมูล Log เพื่อป้องกันการเข้าถึงหรือแก้ไขเปลี่ยนแปลงโดยมิได้รับอนุญาต

๖.๑๘ มีการจัดเก็บ Log ที่เกี่ยวข้องกับการดูแลระบบสารสนเทศโดยผู้ดูแลระบบ (System administrator หรือ System operator)

ข้อ ๗. การควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์

๗.๑ จัดให้มีนโยบายควบคุมการเข้าถึง โดยจัดทำเป็นเอกสาร และมีการติดตามทบทวนให้นโยบายดังกล่าวสอดคล้องกับข้อกำหนดหรือความต้องการด้านการดำเนินงานหรือการให้บริการ และด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

๗.๒ จัดให้มีการลงทะเบียนบัญชีผู้ใช้งานระบบสารสนเทศ และยกเลิกบัญชีผู้ใช้อย่างเป็นทางการเพื่อควบคุมการให้สิทธิและการยกเลิกสิทธิในการเข้าใช้งานระบบสารสนเทศใด ๆ ของหน่วยงาน

๗.๓ การกำหนดสิทธิในการเข้าถึงระดับสูง ให้ทำอย่างจำกัดและอยู่ภายใต้การควบคุม

๗.๔ ผู้ใช้งานต้องดูแลป้องกันอุปกรณ์สารสนเทศใดที่อยู่ภายใต้ความดูแลรับผิดชอบ ในระหว่างที่ไม่มีการใช้งาน

๗.๕ จำกัดการเข้าถึงเครือข่ายคอมพิวเตอร์ของหน่วยงานที่สามารถเข้าถึงได้จากภายนอก โดยให้สอดคล้องกับนโยบายควบคุมการเข้าถึง และข้อกำหนดการใช้งานแอพพลิเคชั่นเพื่อการดำเนินงาน

๗.๖ ให้ผู้ใช้งานทุกคนมีบัญชีผู้ใช้งานเป็นของตนเอง และให้ระบบสารสนเทศมีเทคนิคการตรวจสอบตัวตนที่เพียงพอ เพื่อให้สามารถระบุตัวตนของผู้เข้าใช้งานระบบสารสนเทศได้

๗.๗ ให้ยุติหรือปิดหน้าจอการใช้งานระบบสารสนเทศโดยอัตโนมัติ หากไม่มีการใช้งานเกินระยะเวลาสูงสุดที่กำหนดไว้

๗.๘ จำกัดการเข้าถึงข้อมูลสารสนเทศและฟังก์ชั่นต่าง ๆ ในแอพพลิเคชั่นของผู้ใช้งานและผู้ดูแลระบบสารสนเทศ โดยให้สอดคล้องกับนโยบายการเข้าถึงที่ได้กำหนดไว้

๗.๙ กำหนดนโยบายและแนวทางการจัดการด้านความมั่นคงปลอดภัย เพื่อลดความเสี่ยงในการใช้งานอุปกรณ์สารสนเทศหรืออุปกรณ์การสื่อสารที่เคลื่อนย้ายได้ เช่น แล็ปท็อปคอมพิวเตอร์ (Laptop Computer) หรือสมาร์ทโฟน (Smartphone) เป็นต้น

ข้อ ๘. การจัดหาหรือจัดให้มีการพัฒนา และการบำรุงรักษาระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

๘.๑ ในการจัดทำข้อกำหนดขั้นต่ำของระบบสารสนเทศใหม่ หรือการปรับปรุงระบบสารสนเทศเดิม ให้มีการระบุข้อกำหนดด้านการควบคุมความมั่นคงปลอดภัยด้านสารสนเทศไว้ด้วย

๘.๒ ให้ดูแล ควบคุม ติดตามตรวจสอบการทำงานในการจ้างช่วงพัฒนาซอฟต์แวร์

ข้อ ๙. การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิดให้มีการรายงานสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิดผ่าน ช่องทางการบริหารจัดการที่เหมาะสมโดยเร็วที่สุด

ข้อ ๑๐. การบริหารจัดการด้านการบริการหรือการดำเนินงานของหน่วยงานหรือองค์กรเพื่อให้มีความต่อเนื่อง ให้กำหนดแผนเพื่อรักษาไว้หรือกู้คืนการให้บริการสารสนเทศ หลังเกิดเหตุการณ์ที่ทำให้ การดำเนินงานหยุดชะงัก เพื่อให้ข้อมูลสารสนเทศอยู่ในสภาพพร้อมใช้งานตามระดับที่กำหนดไว้ ภายในระยะเวลาที่กำหนดไว้

ข้อ ๑๑. การตรวจสอบและการประเมินผลการปฏิบัติตามนโยบาย มาตรการ หลักเกณฑ์ หรือกระบวนการใด ๆ รวมทั้งข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

๑๑.๑ ให้มีการระบุไว้ให้ชัดเจนถึงแนวทางในการดำเนินงานของระบบสารสนเทศที่มีความสอดคล้องตามกฎหมายและข้อกำหนดตามสัญญาต่าง ๆ ของหน่วยงาน โดยต้องจัดทำเป็นเอกสาร และมีการปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๑๑.๒ ป้องกันมิให้มีการใช้งานระบบสารสนเทศผิดวัตถุประสงค์

๑๑.๓ พนักงานของหน่วยงานต้องดูแลให้งานที่เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศที่อยู่ในขอบเขตความรับผิดชอบได้ดำเนินการไปโดยสอดคล้องกับกฎหมายและข้อกำหนดตามสัญญาต่าง ๆ ของหน่วยงาน

๒. มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับกลาง

การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับกลาง ให้ปฏิบัติตามมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับพื้นฐาน และต้องปฏิบัติเพิ่มเติม ดังนี้

ข้อ ๑. การสร้างความมั่นคงปลอดภัยด้านบริหารจัดการ หน่วยงานต้องวางแผนการติดตามและประเมินผลการใช้งานความมั่นคงปลอดภัยด้านสารสนเทศ และนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างสม่ำเสมอ เพื่อปรับปรุงหากมีการเปลี่ยนแปลงใด ๆ ภายในหน่วยงาน ทั้งนี้ เพื่อให้เหมาะสมกับสถานการณ์การใช้งาน และคงความมีประสิทธิผลอยู่เสมอ

ข้อ ๒. การจัดโครงสร้างด้านความมั่นคงปลอดภัยของระบบสารสนเทศในส่วนการบริหารจัดการด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ทั้งภายในและภายนอกหน่วยงานหรือองค์กร

๒.๑ มีการกำหนดเนื้องานหรือหน้าที่ความรับผิดชอบต่าง ๆ เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศไว้อย่างชัดเจน

๒.๒ มีการกำหนดขั้นตอนและช่องทางในการติดต่อกับหน่วยงานภายนอกที่มีความเชี่ยวชาญเฉพาะด้านหรือหน่วยงานที่มีความเชี่ยวชาญด้านความมั่นคงปลอดภัยด้านสารสนเทศภายใต้สถานการณ์ต่าง ๆ ไว้อย่างชัดเจน

๒.๓ จัดให้มีการพิจารณาทบทวนแนวทางในการบริหารจัดการงานเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศอย่างสม่ำเสมอ หรือเมื่อมีการเปลี่ยนแปลงใด ๆ ในการดำเนินงาน ทั้งนี้ การพิจารณาทบทวนดังกล่าวควรดำเนินการโดยผู้ไม่มีส่วนได้เสียกับงานที่มีการพิจารณาทบทวน

ข้อ ๓. การบริหารจัดการทรัพย์สินสารสนเทศ

๓.๑ มีการกำหนดบุคคลผู้มีหน้าที่ดูแลควบคุมการใช้งานและรับผิดชอบทรัพย์สินสารสนเทศไว้ชัดเจน

๓.๒ มีการกำหนดกฎระเบียบในการใช้งานทรัพย์สินสารสนเทศไว้อย่างชัดเจน โดยจัดทำเป็นเอกสาร และมีการประกาศใช้ในหน่วยงาน

๓.๓ มีการจำแนกประเภทของข้อมูลสารสนเทศ โดยจำแนกตามมูลค่าของข้อมูล ข้อกำหนดทางกฎหมาย ระดับชั้นความลับและความสำคัญต่อหน่วยงาน

๓.๔ มีการกำหนดและประกาศใช้ขั้นตอนที่เหมาะสมในการจำแนกประเภทของข้อมูลสารสนเทศ และจัดการข้อมูลสารสนเทศ โดยให้สอดคล้องกับแนวทางการจำแนกประเภทของข้อมูลสารสนเทศที่หน่วยงานประกาศใช้

ข้อ ๔. การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร พนักงาน หน่วยงานหรือบุคคลภายนอกต้องได้รับการอบรมเพื่อสร้างความตระหนักรู้เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศในส่วนที่เกี่ยวข้องกับหน้าที่ความรับผิดชอบของตน และได้รับการสื่อสารให้ทราบถึงนโยบายหรือระเบียบปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศที่หน่วยงานประกาศใช้อย่างสม่ำเสมอ หรือเมื่อมีการเปลี่ยนแปลง

ข้อ ๕. การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม

๕.๑ มีการออกแบบและติดตั้งการป้องกันความมั่นคงปลอดภัยด้านกายภาพ เพื่อป้องกันพื้นที่หรือสถานที่ปฏิบัติงาน หรืออุปกรณ์สารสนเทศต่าง ๆ

๕.๒ ไม่ควรนำอุปกรณ์สารสนเทศ ข้อมูลสารสนเทศ หรือซอฟต์แวร์ออกจากสถานที่ปฏิบัติงานของหน่วยงานหากมิได้รับอนุญาต

ข้อ ๖. การบริหารจัดการด้านการสื่อสารและการดำเนินงานของระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

๖.๑ มีการจัดการควบคุมการเปลี่ยนแปลงของระบบสารสนเทศ

๖.๒ มีการติดตามผลการใช้งานทรัพยากรสารสนเทศ และวางแผนด้านทรัพยากรสารสนเทศให้รองรับการปฏิบัติงานในอนาคตอย่างเหมาะสม

๖.๓ มีขั้นตอนการปฏิบัติงานในการจัดการและจัดเก็บข้อมูลสารสนเทศเพื่อมิให้ข้อมูลรั่วไหลหรือถูกนำไปใช้ผิดประเภท

๖.๔ มีการจัดเก็บ Log ที่เกี่ยวข้องกับข้อผิดพลาดใด ๆ ของระบบสารสนเทศ มีการวิเคราะห์ Log ดังกล่าวอย่างสม่ำเสมอ และมีการจัดการแก้ไขข้อผิดพลาดที่ตรวจพบอย่างเหมาะสม

๖.๕ ระบบเวลาของระบบสารสนเทศต่าง ๆ ที่ใช้ในหน่วยงานหรือในขอบเขตงานด้านความมั่นคงปลอดภัย (Security domain) ต้องมีความสอดคล้องกัน (Synchronization) โดยให้มีการตั้งค่าพร้อมกับเวลาจากแหล่งเวลาที่เชื่อถือได้

ข้อ ๗. การควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์

๗.๑ มีข้อบังคับให้ผู้ใช้งานปฏิบัติตามขั้นตอนเพื่อการเลือกใช้รหัสผ่านอย่างมั่นคงปลอดภัยตามที่หน่วยงานกำหนด

๗.๒ ผู้ใช้งานสามารถเข้าถึงเฉพาะบริการทางเครือข่ายคอมพิวเตอร์ที่ตนเองได้รับอนุญาตให้ใช้ได้เท่านั้น

๗.๓ ให้มีการกำหนดวิธีการตรวจสอบตัวตนที่เหมาะสมเพื่อควบคุมการเข้าถึงระบบสารสนเทศของหน่วยงานจากระยะไกล

๗.๔ มีการควบคุมการเข้าถึงช่องทางการดูแลระบบสารสนเทศทั้งทางกายภาพและการเชื่อมต่อผ่านคอมพิวเตอร์ สำหรับระบบสารสนเทศที่สามารถเข้าถึงจากระยะไกลได้ เช่น Remote diagnostic หรือ Configuration facility ของอุปกรณ์เครือข่ายคอมพิวเตอร์

๗.๕ มีการจัดกลุ่มตามประเภทของข้อมูลสารสนเทศที่ให้บริการ ระบบสารสนเทศ กลุ่มผู้ใช้งานโดยมีการแบ่งแยกบนเครือข่ายคอมพิวเตอร์อย่างเป็นสัดส่วน

๗.๖ กำหนดให้มีการควบคุมเส้นทางการไหลของข้อมูลสารสนเทศในระบบเครือข่ายคอมพิวเตอร์เพื่อไม่ให้ขัดแย้งกับนโยบายควบคุมการเข้าถึงของแอพพลิเคชั่น

๗.๗ กำหนดขั้นตอนการ Log-on เพื่อควบคุมการเข้าถึงระบบปฏิบัติการคอมพิวเตอร์

๗.๘ ให้จัดทำหรือจัดให้มีระบบการบริหารจัดการรหัสผ่านที่สามารถทำงานแบบเชิงโต้ตอบกับผู้ใช้งาน (Interactive) และสามารถรองรับการใช้งานรหัสผ่านที่มีความมั่นคงปลอดภัย

ข้อ ๘. การจัดหาหรือจัดให้มีการพัฒนา และการบำรุงรักษาระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

๘.๑ ให้มีการตรวจสอบ (Validate) ข้อมูลใด ๆ ที่จะรับเข้าสู่แอพพลิเคชั่นก่อนเสมอ เพื่อให้มั่นใจได้ว่าข้อมูลมีความถูกต้องและมีรูปแบบเหมาะสม

๘.๒ ให้มีการตรวจสอบ (Validate) ข้อมูลใด ๆ อันเป็นผลจากการประมวลผลของแอพพลิเคชั่น เพื่อให้มั่นใจได้ว่า ข้อมูลที่ได้จากการประมวลผลถูกต้องและเหมาะสม

๘.๓ จัดให้มีแนวทางการบริหารจัดการกุญแจ (Key) เพื่อรองรับการใช้งานเทคนิคที่เกี่ยวข้องกับการเข้ารหัสลับของหน่วยงาน

๘.๔ ให้เลือกชุดข้อมูลสารสนเทศที่จะนำไปใช้เพื่อการทดสอบในระบบสารสนเทศอย่างระมัดระวัง รวมทั้งมีแนวทางควบคุมและป้องกันข้อมูลรั่วไหล

๘.๕ ให้มีการจำกัดการเข้าถึงซอร์สโค้ด (Source code) ของโปรแกรม

๘.๖ หากมีการเปลี่ยนแปลงใด ๆ ในระบบปฏิบัติการคอมพิวเตอร์ ให้มีการตรวจสอบทบทวนการทำงานของโปรแกรมที่มีความสำคัญ และทดสอบการใช้งานเพื่อให้มั่นใจว่าผลของการเปลี่ยนแปลงดังกล่าว จะไม่ส่งผลกระทบใด ๆ ต่อความมั่นคงปลอดภัยของระบบสารสนเทศและการให้บริการของหน่วยงาน

ข้อ ๙. การบริหารจัดการด้านการบริการหรือการดำเนินงานของหน่วยงานหรือองค์กรเพื่อให้มีความต่อเนื่อง

๙.๑ จัดให้มีข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศที่จำเป็น โดยกำหนดให้เป็นส่วนหนึ่งของขั้นตอนการบริหารจัดการเพื่อการดำเนินงานอย่างต่อเนื่องในภาวะฉุกเฉิน

๙.๒ กำหนดให้มีกรอบงานหลักสำหรับการพัฒนาแผนการบริหารจัดการเพื่อการดำเนินงานอย่างต่อเนื่องในภาวะฉุกเฉิน เพื่อให้การพัฒนาแผนต่าง ๆ เป็นไปในทิศทางเดียวกัน รวมทั้งสอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัย ตลอดจนมีการจัดลำดับความสำคัญก่อนหลังในการทดสอบและการดูแล

๙.๓ ให้มีการทดสอบและปรับปรุงแผนการบริหารจัดการเพื่อการดำเนินงานอย่างต่อเนื่องในภาวะฉุกเฉินอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าแผนดังกล่าวเป็นปัจจุบันและมีประสิทธิผลอยู่เสมอ

ข้อ ๑๐. การตรวจสอบและการประเมินผลการปฏิบัติตามนโยบาย มาตรการ หลักเกณฑ์ หรือกระบวนการใด ๆ รวมทั้งข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

๑๐.๑ จัดให้มีการคุ้มครองข้อมูลส่วนบุคคลโดยให้สอดคล้องกับกฎหมายและข้อกำหนดตามสัญญาต่าง ๆ ของหน่วยงาน

๑๐.๒ ใช้เทคนิคการเข้ารหัสลับ ที่สอดคล้องกับกฎหมายและข้อกำหนดตามสัญญาต่าง ๆ ของหน่วยงาน

๑๐.๓ ให้มีการทบทวนตรวจสอบระบบสารสนเทศในด้านเทคนิคอย่างสม่ำเสมอเพื่อให้สอดคล้องกับมาตรฐานการพัฒนางานด้านความมั่นคงปลอดภัยด้านสารสนเทศ

๑๐.๔ วางแผนและจัดให้มีข้อกำหนดการตรวจสอบและกิจกรรมที่เกี่ยวข้องกับการตรวจสอบระบบสารสนเทศ เพื่อลดความเสี่ยงในการเกิดการหยุดชะงักของการให้บริการ

๑๐.๕ ป้องกันการเข้าใช้งานเครื่องมือที่ใช้เพื่อการตรวจสอบ เพื่อมิให้เกิดการใช้งานผิดประเภทหรือถูกละเมิดการใช้งาน (Compromise)

๓. มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับเคร่งครัด

การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับเคร่งครัด ให้ปฏิบัติตามมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับพื้นฐานและระดับกลาง และต้องปฏิบัติเพิ่มเติม ดังนี้

ข้อ ๑. การจัดโครงสร้างด้านความมั่นคงปลอดภัยของระบบสารสนเทศในส่วนการบริหารจัดการด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ทั้งภายในและภายนอกหน่วยงานหรือองค์กร

๑.๑ มีการสร้างความร่วมมือระหว่างผู้ที่มีบทบาทเกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน ในงานหรือกิจกรรมใด ๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศ

๑.๒ มีการกำหนดขั้นตอนและช่องทางในการติดต่อกับหน่วยงานภายนอกที่มีหน้าที่ในการกำกับดูแล หรือหน่วยงานที่เกี่ยวข้องกับการบังคับใช้กฎหมาย รวมทั้งหน่วยงานที่ควบคุมดูแลสถานการณ์ฉุกเฉินภายใต้สถานการณ์ต่าง ๆ ไว้อย่างชัดเจน

๑.๓ ก่อนที่จะอนุญาตให้หน่วยงานหรือบุคคลภายนอกเข้าถึงระบบสารสนเทศหรือใช้ข้อมูลสารสนเทศของหน่วยงาน ให้มีการระบุความเสี่ยงที่อาจเกิดขึ้นและกำหนดแนวทางป้องกันเพื่อลดความเสี่ยงนั้นก่อนการอนุญาต

ข้อ ๒. การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร

๒.๑ ในการพิจารณารับพนักงานเข้าทำงาน หรือการว่าจ้างหน่วยงานหรือบุคคลภายนอก ให้มีการตรวจสอบประวัติหรือคุณสมบัติเพื่อให้เป็นไปตามกฎหมาย กฎระเบียบและจริยธรรมที่เกี่ยวข้อง โดยให้คำนึงถึงระดับชั้นความลับของข้อมูลสารสนเทศที่จะให้เข้าถึง และระดับความเสี่ยงที่ได้ประเมิน

๒.๒ ในสัญญาจ้างหรือข้อตกลงการปฏิบัติงานของพนักงาน หรือสัญญาว่าจ้างหน่วยงานหรือบุคคลภายนอก ให้ระบุหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยด้านสารสนเทศไว้ในสัญญา

ข้อ ๓. การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม

๓.๑ ในพื้นที่ที่ต้องมีการรักษาความมั่นคงปลอดภัยด้านกายภาพ (Secure area) ต้องมีการควบคุมการเข้าออก โดยให้เฉพาะผู้มีสิทธิที่สามารถเข้าออกได้

๓.๒ มีการออกแบบแนวทางการป้องกันทางกายภาพสำหรับการทำงานในพื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัยด้านกายภาพ (Secure area) และกำหนดให้มีการนำไปใช้งาน

๓.๓ มีการควบคุมบริเวณที่ผู้ไม่มีสิทธิเข้าถึงอาจสามารถเข้าถึงได้ เช่น จุดรับส่งของ เป็นต้น หรือหากเป็นไปได้ให้แยกบริเวณดังกล่าวออกจากพื้นที่ที่มีการติดตั้ง จัดเก็บ หรือใช้งาน ระบบสารสนเทศและข้อมูลสารสนเทศเพื่อหลีกเลี่ยงการเข้าถึงโดยมิได้รับอนุญาต

๓.๔ มีการป้องกันสายเคเบิลที่ใช้เพื่อการสื่อสาร หรือสายไฟ เพื่อมิให้มีการดักรับสัญญาณ (Interception) หรือมีความเสียหายเกิดขึ้น

๓.๕ มีการรักษาความมั่นคงปลอดภัยให้กับอุปกรณ์สารสนเทศที่มีการนำไปใช้งานนอกสถานที่ปฏิบัติงานของหน่วยงาน โดยให้คำนึงถึงระดับความเสี่ยงที่แตกต่างกันจากการนำไปใช้งานในสถานที่ต่าง ๆ

๓.๖ ก่อนการยกเลิกการใช้งานหรือจำหน่ายอุปกรณ์สารสนเทศที่ใช้ในการจัดเก็บข้อมูลสารสนเทศต้องมีการตรวจสอบอุปกรณ์สารสนเทศนั้นว่า ได้มีการลบ ย้าย หรือทำลาย ข้อมูลที่สำคัญหรือซอฟต์แวร์ที่จัดซื้อและติดตั้งไว้ด้วยวิธีการที่ทำให้ไม่สามารถกู้คืนได้อีก

ข้อ ๔. การบริหารจัดการด้านการสื่อสารและการดำเนินงานของระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

๔.๑ มีการแบ่งแยกหน้าที่และขอบเขตความรับผิดชอบอย่างชัดเจน เพื่อลดโอกาสความผิดพลาดในการเปลี่ยนแปลงหรือใช้งานระบบสารสนเทศหรือข้อมูลสารสนเทศที่ผิดประเภท

๔.๒ มีการแยกระบบสารสนเทศสำหรับการพัฒนา ทดสอบ และใช้งานจริงออกจากกัน เพื่อลดความเสี่ยงในการเข้าใช้งานหรือการเปลี่ยนแปลงระบบสารสนเทศโดยมิได้รับอนุญาต

๔.๓ มีการบริหารจัดการการเปลี่ยนแปลงใด ๆ เกี่ยวกับการจัดเตรียมการให้บริการ และการดูแลปรับปรุงนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ขั้นตอนปฏิบัติงาน หรือการควบคุมเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ โดยคำนึงถึงระดับความสำคัญของการดำเนินธุรกิจที่เกี่ยวข้องและการประเมินความเสี่ยงอย่างต่อเนื่อง

๔.๔ หากหน่วยงานอนุญาตให้มีการใช้งาน Mobile code (เช่น Script บางอย่างของเว็บแอพพลิเคชั่นที่มีการทำงานอัตโนมัติเมื่อเรียกดูเว็บ) ควรมีการตั้งค่าการทำงาน (Configuration) เพื่อให้มั่นใจได้ว่าการทำงานของ Mobile code นั้นเป็นไปตามความมั่นคงปลอดภัยด้านสารสนเทศและนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และห้ามโดยอัตโนมัติมิให้ Mobile code สามารถทำงานได้ในระบบสารสนเทศ หากในนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กำหนดห้ามมิให้ประเภทของ Mobile code ดังกล่าวทำงานได้

๔.๕ มีขั้นตอนการปฏิบัติงานสำหรับการบริหารจัดการอุปกรณ์ที่ใช้ในการบันทึกข้อมูลอิเล็กทรอนิกส์ที่สามารถถอดหรือต่อพ่วงกับเครื่องคอมพิวเตอร์ได้ (Removable media)

๔.๖ มีขั้นตอนการปฏิบัติงานในการทำลายอุปกรณ์ที่ใช้ในการบันทึกข้อมูลอิเล็กทรอนิกส์ที่สามารถถอดหรือต่อพ่วงกับเครื่องคอมพิวเตอร์ได้ (Removable media) อย่างมั่นคงปลอดภัย

๔.๗ มีการป้องกันมิให้ข้อมูลหรือเอกสารเกี่ยวกับระบบสารสนเทศ (System documentation) ถูกเข้าถึงโดยมิได้รับอนุญาต

๔.๘ ในกรณีที่มีการเคลื่อนย้ายอุปกรณ์ที่จัดเก็บข้อมูลสารสนเทศ ให้มีการป้องกันอุปกรณ์ที่ใช้จัดเก็บข้อมูลดังกล่าว เพื่อมิให้มีการเข้าถึงโดยมิได้รับอนุญาต หรือถูกนำไปใช้งานผิดประเภท หรืออุปกรณ์หรือข้อมูลสารสนเทศได้รับความเสียหาย

๔.๙ ให้มีการป้องกันข้อมูลสารสนเทศที่มีการสื่อสารกันผ่านข้อมูลอิเล็กทรอนิกส์ (Electronic messaging) เช่น จดหมายอิเล็กทรอนิกส์ (E - mail) EDI หรือ Instant messaging)

ข้อ ๕. การควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์

๕.๑ จัดให้มีขั้นตอนการบริหารจัดการเรื่องการกำหนดรหัสผ่านอย่างเป็นทางการ

๕.๒ กำหนดให้ผู้บริหารติดตามทบทวนระดับสิทธิในการเข้าถึงของผู้ใช้งานอย่างเป็นทางการเป็นประจำ

๕.๓ มีการกำหนดนโยบาย Clear desk สำหรับข้อมูลสารสนเทศในรูปแบบกระดาษและที่จัดเก็บในอุปกรณ์บันทึกข้อมูลอิเล็กทรอนิกส์ที่สามารถถอดหรือต่อพ่วงกับเครื่องคอมพิวเตอร์ได้ และนโยบาย Clear screen สำหรับระบบสารสนเทศ

๕.๔ ให้มีการระบุอุปกรณ์ที่เชื่อมต่อเข้ากับระบบสารสนเทศโดยอัตโนมัติ (Automatic equipment identification) เพื่อตรวจสอบการเชื่อมต่อของอุปกรณ์ดังกล่าวว่ามาจากอุปกรณ์ดังกล่าวจริง หรือจากสถานที่ที่กำหนดไว้เท่านั้น ทั้งนี้ จำเป็นสำหรับการที่ระบบสารสนเทศจะรับการเชื่อมต่อจากเฉพาะอุปกรณ์ที่ได้รับอนุญาต หรือมาจากเฉพาะสถานที่ที่ได้รับอนุญาต

๕.๕ ให้จำกัดการเข้าถึงการใช้งานโปรแกรมอรรถประโยชน์ต่าง ๆ อย่างเข้มงวด เนื่องจากโปรแกรมดังกล่าวอาจมีความสามารถควบคุมดูแลและเปลี่ยนแปลงการทำงานของระบบสารสนเทศได้

๕.๖ จำกัดระยะเวลาการเชื่อมต่อกับระบบสารสนเทศที่มีระดับความเสี่ยงสูง เพื่อเพิ่มระดับการรักษาความมั่นคงปลอดภัย

๕.๗ สำหรับระบบสารสนเทศที่มีความสำคัญสูง ต้องจัดให้ระบบสารสนเทศทำงานในสภาพแวดล้อมที่แยกออกมาต่างหาก โดยไม่ใช้ปะปนกับระบบสารสนเทศอื่น

๕.๘ กำหนดให้มีนโยบาย แผนงานและขั้นตอนการปฏิบัติงานที่เกี่ยวข้องกับกิจกรรมใด ๆ ที่มีการปฏิบัติงานจากภายนอกหน่วยงาน (Teleworking)

ข้อ ๖. การจัดหาหรือจัดให้มีการพัฒนา และการบำรุงรักษาระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

๖.๑ ให้มีการตรวจสอบ (Validate) การทำงานของแอพพลิเคชั่นเพื่อตรวจหาข้อผิดพลาดของข้อมูลที่อาจเกิดจากการทำงานหรือการประมวลผลที่ผิดพลาด

๖.๒ ให้มีข้อกำหนดขั้นต่ำสำหรับการรักษาความถูกต้องแท้จริง (Authenticity) และความถูกต้องครบถ้วน (Integrity) ของข้อมูลในแอพพลิเคชั่น รวมทั้งมีการระบุและปฏิบัติตามวิธีการป้องกันที่เหมาะสม

๖.๓ จัดให้มีนโยบายในการใช้งานเทคนิคที่เกี่ยวข้องกับการเข้ารหัสลับ

๖.๔ กำหนดให้มีขั้นตอนการปฏิบัติงานเพื่อควบคุมการติดตั้งซอฟต์แวร์บนระบบสารสนเทศที่ให้บริการ

๖.๕ ให้มีการควบคุมการเปลี่ยนแปลงต่าง ๆ ในการพัฒนาระบบสารสนเทศ โดยมีขั้นตอนการควบคุมที่เป็นทางการ

๖.๗ ให้จำกัดการเปลี่ยนแปลงใด ๆ ต่อซอฟต์แวร์ที่ใช้งาน (Software package) โดยให้เปลี่ยนแปลงเฉพาะเท่าที่จำเป็น และควบคุมทุก ๆ การเปลี่ยนแปลงอย่างเข้มงวด

๖.๘ มีมาตรการป้องกันเพื่อลดโอกาสที่เกิดการรั่วไหลของข้อมูลสารสนเทศ

ข้อ ๗. การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด

๗.๑ กำหนดให้พนักงานหรือผู้ใช้งานที่เป็นบุคคลภายนอก มีการบันทึกและรายงานจุดอ่อนใด ๆ ที่อาจสังเกตพบระหว่างการใช้งานระบบสารสนเทศ

๗.๒ กำหนดขอบเขตความรับผิดชอบของผู้บริหารและขั้นตอนการปฏิบัติงาน เพื่อตอบสนองต่อสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด อย่างรวดเร็ว มีระเบียบ และมีประสิทธิผล

๗.๓ หากในขั้นตอนการติดตามผลกับบุคคลหรือหน่วยงานภายหลังจากเกิดสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด ซึ่งเกี่ยวข้องกับการดำเนินการทางกฎหมาย (ไม่ว่าทางแพ่งหรือทางอาญา) ให้มีการรวบรวม จัดเก็บ และนำเสนอหลักฐาน ให้สอดคล้องกับหลักเกณฑ์ของกฎหมายที่ใช้บังคับ

ข้อ ๘. การบริหารจัดการด้านการบริการหรือการดำเนินงานของหน่วยงานหรือองค์กรเพื่อให้มีความต่อเนื่อง ให้มีการระบุเหตุการณ์ใด ๆ ที่อาจส่งผลให้การดำเนินงานหยุดชะงัก และความเป็นไปได้ในการเกิดผลกระทบ ตลอดจนผลต่อเนื่องจากการหยุดชะงักนั้นในแง่ของความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ ๙. การตรวจสอบและการประเมินผลการปฏิบัติตามนโยบาย มาตรการ หลักเกณฑ์ หรือกระบวนการใด ๆ รวมทั้งข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

๙.๑ กำหนดขั้นตอนปฏิบัติงานเพื่อให้มั่นใจว่าในการใช้งานข้อมูลที่อาจถือเป็นทรัพย์สินทางปัญญาหรือการใช้งานซอฟต์แวร์มีความสอดคล้องกับกฎหมายและข้อกำหนดตามสัญญาต่าง ๆ

๙.๒ ป้องกันมิให้ข้อมูลสารสนเทศที่สำคัญเกิดความเสียหาย สูญหายหรือถูกปลอมแปลง โดยให้สอดคล้องกับกฎหมาย ข้อกำหนดตามสัญญาต่าง ๆ ของหน่วยงาน และข้อกำหนดการให้บริการ

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

เรื่อง ประเภทของธุรกรรมทางอิเล็กทรอนิกส์ และหลักเกณฑ์การประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ตามวิธีการแบบปลอดภัย

พ.ศ. ๒๕๕๕

โดยที่พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓ กำหนดให้คณะกรรมการประกาศกำหนดประเภทของธุรกรรมทางอิเล็กทรอนิกส์ หรือหลักเกณฑ์การประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ เพื่อให้การทำธุรกรรมทางอิเล็กทรอนิกส์ใดที่ได้กระทำตามวิธีการแบบปลอดภัยที่คณะกรรมการกำหนดเป็นวิธีการที่เชื่อถือได้

อาศัยอำนาจตามความในมาตรา ๖ วรรคหนึ่ง แห่งพระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓ คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์จึงออกประกาศเพื่อกำหนดประเภทของธุรกรรมทางอิเล็กทรอนิกส์ และหลักเกณฑ์การประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ตามวิธีการแบบปลอดภัยไว้ ดังนี้

ข้อ ๑ ประกาศนี้เรียกว่า "ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง ประเภทของธุรกรรมทางอิเล็กทรอนิกส์ และหลักเกณฑ์การประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕"

ข้อ ๒ ให้ธุรกรรมทางอิเล็กทรอนิกส์ในประเภทดังต่อไปนี้ ใช้วิธีการแบบปลอดภัยในระดับเคร่งครัด

(๑) ธุรกรรมทางอิเล็กทรอนิกส์ด้านการชำระเงินทางอิเล็กทรอนิกส์ตามพระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๑

(๒) ธุรกรรมทางอิเล็กทรอนิกส์ด้านการเงินของธนาคารพาณิชย์ตามกฎหมายว่าด้วยธุรกิจสถาบันการเงิน

(๓) ธุรกรรมทางอิเล็กทรอนิกส์ด้านประกันภัยตามกฎหมายว่าด้วยประกันชีวิตและประกันวินาศภัย

(๔) ธุรกรรมทางอิเล็กทรอนิกส์ด้านหลักทรัพย์ของผู้ประกอบธุรกิจหลักทรัพย์ตามกฎหมายว่าด้วยหลักทรัพย์และตลาดหลักทรัพย์

(๕) ธุรกรรมทางอิเล็กทรอนิกส์ที่จัดเก็บ รวบรวม และให้บริการข้อมูลของบุคคลหรือทรัพย์สินหรือทะเบียนต่าง ๆ ที่เป็นเอกสารมหาชนหรือที่เป็นข้อมูลสาธารณะ

(๖) ธุรกรรมทางอิเล็กทรอนิกส์ในการให้บริการด้านสาธารณูปโภคและบริการสาธารณะที่ต้องดำเนินการอย่างต่อเนื่องตลอดเวลา

ข้อ ๓ ในการประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ ให้หน่วยงานหรือองค์กรยึดถือหลักการประเมินความเสี่ยงของระบบเทคโนโลยีสารสนเทศซึ่งเป็นที่ยอมรับเป็นการทั่วไปว่าเชื่อถือได้เป็นแนวทางในการประเมินระดับผลกระทบ

ข้อ ๔ การประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ จะต้องประเมินผลกระทบในด้านต่อไปนี้ด้วย

(๑) ผลกระทบด้านมูลค่าความเสียหายทางการเงิน

(๒) ผลกระทบต่อจำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับอันตรายต่อชีวิต ร่างกายหรืออนามัย

(๓) ผลกระทบต่อจำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับความเสียหายอื่นใดนอกจาก (๒)

(๔) ผลกระทบด้านความมั่นคงของรัฐ

ข้อ ๕ ในการประเมินผลกระทบด้านมูลค่าความเสียหายทางการเงิน ให้จัดเป็นสามระดับ โดยมีเกณฑ์ในการประเมิน ดังนี้

(๑) ในกรณีมูลค่าความเสียหายทางการเงินไม่เกินหนึ่งล้านบาท ให้จัดเป็นผลกระทบระดับต่ำ

(๒) ในกรณีมูลค่าความเสียหายทางการเงินเกินกว่าหนึ่งล้านบาทแต่ไม่เกินหนึ่งร้อยล้านบาท ให้จัดเป็นผลกระทบระดับกลาง

(๓) ในกรณีมูลค่าความเสียหายทางการเงินเกินกว่าหนึ่งร้อยล้านบาทขึ้นไป ให้จัดเป็นผลกระทบระดับสูง

ในการประเมินมูลค่าความเสียหายทางการเงินตามวรรคหนึ่ง ให้คำนวณจากความเสียหายที่จะเกิดขึ้นในหนึ่งวันและคำนวณความเสียหายโดยตรงเท่านั้น

ข้อ ๖ ในการประเมินผลกระทบต่อจำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับอันตรายต่อชีวิต ร่างกายหรืออนามัย ให้จัดเป็นสามระดับ โดยมีเกณฑ์ในการประเมิน ดังนี้

(๑) ในกรณีที่ไม่มีผู้ใช้บริการหรือผู้มีส่วนได้เสียได้รับผลกระทบต่อชีวิต ร่างกายหรืออนามัย ให้จัดเป็นผลกระทบระดับต่ำ

(๒) ในกรณีจำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียได้รับผลกระทบต่อร่างกายหรืออนามัยตั้งแต่หนึ่งคน แต่ไม่เกินหนึ่งพันคน ให้จัดเป็นผลกระทบระดับกลาง

(๓) ในกรณีจำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียได้รับผลกระทบต่อร่างกายหรืออนามัยเกินกว่าหนึ่งพันคน หรือต่อชีวิตตั้งแต่หนึ่งคน ให้จัดเป็นผลกระทบระดับสูง

ในการประเมินผลกระทบต่อจำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับอันตรายต่อชีวิต ร่างกายหรืออนามัยตามวรรคหนึ่ง ให้คำนวณจากจำนวนของบุคคลดังกล่าวที่ได้รับผลกระทบในหนึ่งวัน

ข้อ ๗ ในการประเมินผลกระทบต่อจำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับความเสียหายอื่นนอกจากข้อ ๔ (๒) ให้จัดเป็นสามระดับ โดยมีเกณฑ์ในการประเมิน ดังนี้

(๑) ในกรณีจำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับผลกระทบไม่เกินหนึ่งหมื่นคน ให้จัดเป็นผลกระทบระดับต่ำ

(๒) ในกรณีจำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับผลกระทบเกินกว่าหนึ่งหมื่นคน แต่ไม่เกินหนึ่งแสนคน ให้จัดเป็นผลกระทบระดับกลาง

(๓) ในกรณีจำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับผลกระทบเกินกว่าหนึ่งแสนคน ให้จัดเป็นผลกระทบระดับสูง

ในการประเมินผลกระทบต่อจำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับความเสียหายตามวรรคหนึ่ง ให้คำนวณจากจำนวนของบุคคลดังกล่าวที่ได้รับผลกระทบ ในหนึ่งวันและคำนวณความเสียหายโดยตรงเท่านั้น

ข้อ ๘ ในการประเมินผลกระทบด้านความมั่นคงของรัฐ ให้จัดเป็นสองระดับ โดยมีเกณฑ์ในการประเมิน ดังนี้

(๑) ในกรณีไม่มีผลกระทบต่อความมั่นคงของรัฐ ให้จัดเป็นผลกระทบระดับต่ำ

(๒) ในกรณีมีผลกระทบต่อความมั่นคงของรัฐ ให้จัดเป็นผลกระทบระดับสูง

ข้อ ๙ หากปรากฏว่ามีผลประเมินที่เป็นผลกระทบในระดับสูงด้านหนึ่งด้านใดให้ธุรกรรมทางอิเล็กทรอนิกส์นั้นต้องใช้วิธีการแบบปลอดภัยในระดับเคร่งครัด และหากมีผลกระทบในระดับกลางอย่างน้อยสองด้านขึ้นไปให้ใช้วิธีการแบบปลอดภัยในระดับกลางขึ้นไป

ในกรณีที่ไม่เป็นไปตามวรรคหนึ่ง ให้ธุรกรรมทางอิเล็กทรอนิกส์ใช้วิธีการแบบปลอดภัยในระดับไม่ต่ำกว่าระดับพื้นฐาน

ข้อ ๑๐ ประกาศนี้ให้ใช้บังคับเมื่อพ้นกำหนดสามร้อยหกสิบวัน นับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ประกาศ ณ วันที่ ๑๓ พฤศจิกายน พ.ศ. ๒๕๕๕
นาวาอากาศเอก อนุดิษฐ์ นาครทรรพ
รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
ประธานกรรมการธุรกรรมทางอิเล็กทรอนิกส์

พระราชกฤษฎีกา

ว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์

พ.ศ. ๒๕๕๓

ภูมิพลอดุลยเดช ป.ร.

ให้ไว้ ณ วันที่ ๒๓ สิงหาคม พ.ศ. ๒๕๕๓

เป็นปีที่ ๖๕ ในรัชกาลปัจจุบัน

พระบาทสมเด็จพระปรมินทรมหาภูมิพลอดุลยเดช มีพระบรมราชโองการโปรดเกล้า ฯ ให้ประกาศว่า

โดยที่เป็นการสมควรกำหนดวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์

อาศัยอำนาจตามความในมาตรา ๑๘๗ ของรัฐธรรมนูญแห่งราชอาณาจักรไทย และมาตรา ๒๕ แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ อันเป็นกฎหมายที่มีบทบัญญัติบางประการเกี่ยวกับการจำกัดสิทธิและเสรีภาพของบุคคล ซึ่งมาตรา ๒๕ ประกอบกับมาตรา ๔๓ ของรัฐธรรมนูญแห่งราชอาณาจักรไทย บัญญัติให้กระทำได้โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมาย จึงทรงพระกรุณาโปรดเกล้า ฯ ให้ตราพระราชกฤษฎีกาขึ้นไว้ ดังต่อไปนี้

มาตรา ๑ พระราชกฤษฎีกานี้เรียกว่า "พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓"

มาตรา ๒ พระราชกฤษฎีกานี้ให้ใช้บังคับเมื่อพ้นกำหนดหนึ่งร้อยแปดสิบวันนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

มาตรา ๓ ในพระราชกฤษฎีกานี้

"วิธีการแบบปลอดภัย" หมายความว่า วิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์

"ทรัพย์สินสารสนเทศ" หมายความว่า

(๑) ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

(๒) ตัวเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล และอุปกรณ์อื่นใด

(๓) ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์

"ความมั่นคงปลอดภัยของระบบสารสนเทศ" (information security) หมายความว่า การป้องกันทรัพย์สินสารสนเทศจากการเข้าถึง ใช้ เปิดเผย ขัดขวาง เปลี่ยนแปลงแก้ไข ทำให้สูญหาย ทำให้เสียหาย ถูกทำลาย หรือล่วงรู้โดยมิชอบ

"ความมั่นคงปลอดภัยด้านบริหารจัดการ" (administrative security) หมายความว่า การกระทำในระดับบริหารโดยการจัดให้มีนโยบาย มาตรการ หลักเกณฑ์ หรือกระบวนการใด ๆ เพื่อนำมาใช้ในกระบวนการคัดเลือก การพัฒนา การนำไปใช้ หรือการบำรุงรักษาทรัพย์สินสารสนเทศให้มีความมั่นคงปลอดภัย

"ความมั่นคงปลอดภัยด้านกายภาพ" (physical security) หมายความว่า การจัดให้มีนโยบาย มาตรการ หลักเกณฑ์ หรือกระบวนการใด ๆ เพื่อนำมาใช้ในการป้องกันทรัพย์สินสารสนเทศ สิ่งปลูกสร้าง หรือทรัพย์สินอื่นใดจากการคุกคามของบุคคล ภัยธรรมชาติ อุบัติภัย หรือภัยทางกายภาพอื่น

"การรักษาความลับ" (confidentiality) หมายความว่า การรักษาหรือสงวนไว้เพื่อป้องกันระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ หรือข้อมูลคอมพิวเตอร์จากการเข้าถึง ใช้ หรือเปิดเผยโดยบุคคลซึ่งไม่ได้รับอนุญาต

"การรักษาความครบถ้วน" (integrity) หมายความว่า การดำเนินการเพื่อให้ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ หรือข้อมูลคอมพิวเตอร์อยู่ในสภาพสมบูรณ์ขณะที่มีการใช้งาน ประมวลผล โอน หรือเก็บรักษา เพื่อมิให้มีการเปลี่ยนแปลงแก้ไข ทำให้สูญหาย ทำให้เสียหาย หรือถูกทำลายโดยไม่ได้รับอนุญาตหรือโดยมิชอบ

"การรักษาสภาพพร้อมใช้งาน" (availability) หมายความว่า การจัดทำให้ทรัพย์สินสารสนเทศสามารถทำงาน เข้าถึง หรือใช้งานได้ในเวลาที่ต้องการ

"โครงสร้างพื้นฐานสำคัญของประเทศ" (critical infrastructure) หมายความว่า บรรดาหน่วยงานหรือองค์กร หรือส่วนงานหนึ่งส่วนงานใดของหน่วยงานหรือองค์กร ซึ่งธุรกรรมทางอิเล็กทรอนิกส์ของหน่วยงานหรือองค์กร หรือส่วนงานของหน่วยงานหรือองค์กรนั้น มีผลเกี่ยวเนื่องสำคัญต่อความมั่นคงหรือความสงบเรียบร้อยของประเทศ หรือต่อสาธารณชน

มาตรา ๔ วิธีการแบบปลอดภัยมีสามระดับ ดังต่อไปนี้

(๑) ระดับเคร่งครัด

(๒) ระดับกลาง

(๓) ระดับพื้นฐาน

มาตรา ๕ วิธีการแบบปลอดภัยตามมาตรา ๔ ให้ใช้สำหรับการทำธุรกรรมทางอิเล็กทรอนิกส์ดังต่อไปนี้

(๑) ธุรกรรมทางอิเล็กทรอนิกส์ซึ่งมีผลกระทบต่อความมั่นคงหรือความสงบเรียบร้อยของประเทศ หรือต่อสาธารณชน

(๒) ธุรกรรมทางอิเล็กทรอนิกส์ของหน่วยงานหรือองค์กร หรือส่วนงานของหน่วยงานหรือองค์กรที่ถือเป็นโครงสร้างพื้นฐานสำคัญของประเทศ

มาตรา ๖ ให้คณะกรรมการประกาศกำหนดประเภทของธุรกรรมทางอิเล็กทรอนิกส์หรือหลักเกณฑ์การประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ตามมาตรา ๕ (๑) ซึ่งต้องกระทำตามวิธีการแบบปลอดภัยในระดับเคร่งครัด ระดับกลาง หรือระดับพื้นฐาน แล้วแต่กรณี ทั้งนี้ โดยให้คำนึงถึงระดับความเสี่ยงต่อความมั่นคงปลอดภัยของระบบสารสนเทศ ผลกระทบต่อมูลค่าและความเสียหายที่ผู้ใช้บริการอาจได้รับ รวมทั้งผลกระทบต่อเศรษฐกิจและสังคมของประเทศ

ให้คณะกรรมการประกาศกำหนดรายชื่อหรือประเภทของหน่วยงานหรือองค์กร หรือส่วนงานของหน่วยงานหรือองค์กรที่ถือเป็นโครงสร้างพื้นฐานสำคัญของประเทศตามมาตรา ๕ (๒) ซึ่งต้องกระทำตามวิธีการแบบปลอดภัยในระดับเคร่งครัด ระดับกลาง หรือระดับพื้นฐาน แล้วแต่กรณี

มาตรา ๗ วิธีการแบบปลอดภัยตามมาตรา ๔ ในแต่ละระดับ ให้มีมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามหลักเกณฑ์ที่คณะกรรมการประกาศกำหนด

โดยมาตรฐานดังกล่าวสำหรับวิธีการแบบปลอดภัยในแต่ละระดับนั้น อาจมีการกำหนดหลักเกณฑ์ที่แตกต่างกันตามความจำเป็น แต่อย่างน้อยต้องมีการกำหนดเกี่ยวกับหลักเกณฑ์ ดังต่อไปนี้

(๑) การสร้างความมั่นคงปลอดภัยด้านบริหารจัดการ

(๒) การจัดโครงสร้างด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ในส่วนการบริหารจัดการด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ทั้งภายในและภายนอกหน่วยงานหรือองค์กร

(๓) การบริหารจัดการทรัพย์สินสารสนเทศ

(๔) การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร

(๕) การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม

(๖) การบริหารจัดการด้านการสื่อสารและการดำเนินงานของระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

(๗) การควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์

(๘) การจัดหาหรือจัดให้มี การพัฒนา และการบำรุงรักษาระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

(๙) การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด

(๑๐) การบริหารจัดการด้านการบริการหรือการดำเนินงานของหน่วยงานหรือองค์กรเพื่อให้มีความต่อเนื่อง

(๑๑) การตรวจสอบและการประเมินผลการปฏิบัติตามนโยบาย มาตรการ หลักเกณฑ์ หรือกระบวนการใด ๆ รวมทั้งข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

มาตรา ๘ เพื่อประโยชน์ในการเป็นแนวทางสำหรับการจัดทำนโยบายหรือแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของหน่วยงานหรือองค์กร คณะกรรมการอาจระบุหรือแสดงตัวอย่างมาตรฐานทางเทคโนโลยีซึ่งเป็นที่ยอมรับเป็นการทั่วไปว่าเป็นมาตรฐานทางเทคโนโลยีที่เชื่อถือได้ไว้ในประกาศตามมาตรา ๗ ด้วยก็ได้

มาตรา ๙ ธุรกรรมทางอิเล็กทรอนิกส์ใดได้กระทำโดยวิธีการที่มีการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศในระดับที่เทียบเท่าหรือไม่ต่ำกว่ามาตรฐานความมั่นคงปลอดภัยของระบบสารสนเทศตามประกาศตามมาตรา ๗ ซึ่งได้กำหนดไว้สำหรับระดับของวิธีการแบบปลอดภัยในการทำ

ธุรกรรมทางอิเล็กทรอนิกส์นั้น ให้ถือว่าธุรกรรมทางอิเล็กทรอนิกส์ดังกล่าวได้กระทำตามวิธีการที่เชื่อถือได้ตามมาตรา ๒๕ แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔

มาตรา ๑๐ ในการทำธุรกรรมทางอิเล็กทรอนิกส์ตามวิธีการแบบปลอดภัยตามพระราชกฤษฎีกานี้ ผู้กระทำต้องคำนึงถึงหลักการพื้นฐานของการรักษาความลับ การรักษาความครบถ้วน และการรักษาสภาพพร้อมใช้งาน รวมทั้งต้องปฏิบัติตามนโยบายและแนวปฏิบัติในการควบคุมการปฏิบัติงานและการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของหน่วยงานหรือองค์กรนั้นด้วย

มาตรา ๑๑ ในกรณีที่คณะกรรมการเห็นว่าหน่วยงานหรือองค์กรใด หรือส่วนงานหนึ่งส่วนงานใดของหน่วยงานหรือองค์กรใด มีการจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศโดยสอดคล้องกับวิธีการแบบปลอดภัยตามพระราชกฤษฎีกานี้ คณะกรรมการอาจประกาศเผยแพร่รายชื่อหน่วยงานหรือองค์กร หรือส่วนงานของหน่วยงานหรือองค์กรนั้นเพื่อให้สาธารณชนทราบเป็นการทั่วไปก็ได้

มาตรา ๑๒ ให้คณะกรรมการพิจารณาทบทวนหลักเกณฑ์เกี่ยวกับวิธีการแบบปลอดภัยตามพระราชกฤษฎีกานี้และประกาศที่ออกตามพระราชกฤษฎีกานี้ รวมทั้งกฎหมายอื่นที่เกี่ยวข้อง อย่างน้อยทุกรอบระยะเวลาสองปีนับแต่วันที่พระราชกฤษฎีกานี้ใช้บังคับ ทั้งนี้ โดยพิจารณาถึงความเหมาะสมและความสอดคล้องกับเทคโนโลยีที่ได้มีการพัฒนาหรือเปลี่ยนแปลงไป และจัดทำเป็นรายงานเสนอต่อคณะรัฐมนตรีเพื่อทราบต่อไป

มาตรา ๑๓ ให้นายกรัฐมนตรีรักษาการตามพระราชกฤษฎีกานี้

ผู้รับสนองพระบรมราชโองการ
อภิสิทธิ์ เวชชาชีวะ
นายกรัฐมนตรี

หมายเหตุ :- เหตุผลในการประกาศใช้พระราชกฤษฎีกาฉบับนี้ คือ เนื่องจากในปัจจุบันเทคโนโลยีสารสนเทศและการสื่อสารได้เข้ามามีบทบาทสำคัญต่อการดำเนินการของทั้งภาครัฐและภาคเอกชน โดยมีการทำธุรกรรมทางอิเล็กทรอนิกส์กันอย่างแพร่หลาย จึงสมควรส่งเสริมให้มีการบริหารจัดการและรักษาความมั่นคงปลอดภัยของทรัพย์สินสารสนเทศในการทำธุรกรรมทางอิเล็กทรอนิกส์ เพื่อให้มีการยอมรับและเชื่อมั่นในข้อมูลอิเล็กทรอนิกส์มากยิ่งขึ้น ประกอบกับมาตรา ๒๕ แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ บัญญัติให้ธุรกรรมทางอิเล็กทรอนิกส์ใดที่ได้กระทำตามวิธีการแบบปลอดภัยที่กำหนดในพระราชกฤษฎีกาแล้ว ให้สันนิษฐานว่าเป็นวิธีการที่เชื่อถือได้ จึงจำเป็นต้องตราพระราชกฤษฎีกานี้