คู่มือการจัดทำนโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ตามข้อกำหนดภายใต้
ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย
ด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓

เมษายน ๒๕๕๗

สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
คู่มือการจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อมูลทางบรรณนุกรมของสำนักหอสมุดแห่งชาติ
National Library of Thailand Cataloging in Publication Data
สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
คู่มือการจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
- กรุงเทพฯ : กลุ่มงานผลักดันธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ
สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
๒๕๕๗
๑๐๔ หน้า.
ISBN 978-974-9765-58-6

เลขมาตรฐานสากลประจำหนังสือ ๙๗๘-๙๗๔-๙๗๖๕-๕๘-๖

พิมพ์ครั้งที่ ๑ เมษายน ๒๕๕๗
จำนวนพิมพ์ ๕๐๐ เล่ม

จัดพิมพ์โดย สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
๑๒๐ หมู่ ๓ ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษาฯ
อาคารรัฐประศาสนภักดี ชั้น ๖ ถนนแจ้งวัฒนะ เขตหลักสี่
กรุงเทพมหานคร ๑๐๒๑๐
โทรศัพท์ ๐ ๒๑๔๑ ๖๙๘๘, ๐ ๒๑๔๑ ๖๙๘๙, ๐ ๒๑๔๑ ๖๕๙๔
โทรสาร ๐ ๒๑๔๓ ๘๐๓๖-๓๗
เว็บไซต์กระทรวงฯ : http://www.mict.go.th
เว็บไซต์คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ :
http://www.etcommission.go.th

พิมพ์ที่ บริษัท ศูนย์การพิมพ์แก่นจันทร์ จำกัด
เลขที่ ๘๘/๕ วัฒนานิเวศน์ ซอย ๕ ถนนสุทธิสาร แขวงสามเสนนอก
เขตห้วยขวาง กรุงเทพมหานคร ๑๐๓๑๐
โทรศัพท์ ๐ ๒๒๗๖ ๖๕๔๕, ๐ ๒๒๗๖ ๖๗๑๓, ๐ ๒๒๗๖ ๖๗๒๑
โทรสาร ๐ ๒๒๗๗ ๘๑๓๗

สารบัญ

<u>ภาคผนวก</u>

คำนำ

คู่มือการจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเป็นเอกสารที่จัดทำขึ้นเพื่อเป็นเครื่องมือหนึ่งที่ช่วยในการจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ ให้เป็นไปตามมาตรฐานขั้นต่ำที่ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์กำหนดไว้ โดยที่การดำเนินงานดังกล่าว จะเป็นมาตรการหนึ่งที่ช่วยยกระดับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของหน่วยงานของรัฐ ให้อยู่ในระดับมาตรฐานสากล โดยอ้างอิงการดำเนินงานตามกรอบมาตรฐานสากล ISO/IEC 27001 ภายใต้แนวทางที่เป็นมาตรฐานขั้นต่ำซึ่งเพียงพอต่อการดำเนินงาน และไม่สร้างภาระให้หน่วยงานมากเกินความจำเป็น

การจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ จะช่วยให้หน่วยงานสามารถลดผลกระทบจากสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่คาดคิด ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือถูกโจมตี และความมั่นคงปลอดภัยถูกคุกคาม ตลอดจนช่วยให้สามารถฟื้นฟูระบบอย่างรวดเร็วหลังจากการโจมตีสิ้นสุดลงแล้ว

ทั้งนี้ ในการจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐจะต้องคำนึงถึงสถานการณ์ปัจจุบันและการวิเคราะห์ความเสี่ยงที่เกี่ยวข้อง ซึ่งอาจเกิดผลกระทบต่อภาคประชาชน ภาคเอกชน และภาครัฐบาล ดังนั้นจึงจำเป็นอย่างยิ่งที่จะต้องมีเครื่องมือเพื่อช่วยในการวางแผนและกำหนดรายละเอียดที่เหมาะสม คณะผู้จัดทำจึงหวังเป็นอย่างยิ่งว่า คู่มือฉบับนี้จะเป็นเครื่องมือหนึ่งที่ช่วยให้หน่วยงานสามารถจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศได้ตามมาตรฐานขั้นต่ำตามที่ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์กำหนดไว้

สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
เมษายน ๒๕๕๗

บทที่ ๑
ความเป็นมา / เหตุผลความจำเป็น

๑. ความเป็นมา

๑.๑ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ (แก้ไขเพิ่มเติม ฉบับที่ ๒ พ.ศ. ๒๕๕๑) ภายใต้มาตรา ๓๕ กำหนดให้ “คำขอ การอนุญาต การจดทะเบียน คำสั่งทางปกครอง การชำระเงิน การประกาศ หรือการดำเนินการใด ๆ ตามกฎหมายกับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐ ถ้าได้กระทำในรูปของข้อมูลอิเล็กทรอนิกส์ตามหลักเกณฑ์และวิธีการที่กำหนดโดยพระราชกฤษฎีกา ให้นำพระราชบัญญัตินี้มาใช้บังคับและให้ถือว่ามีผล โดยชอบด้วยกฎหมายเช่นเดียวกับการดำเนินการตามหลักเกณฑ์และวิธีการที่กฎหมายในเรื่องนั้นกำหนด ทั้งนี้ ในพระราชกฤษฎีกาอาจกำหนดให้บุคคลที่เกี่ยวข้องต้องกระทำหรืองดเว้นกระทำการใด ๆ หรือให้หน่วยงานของรัฐออกระเบียบเพื่อกำหนดรายละเอียดในบางกรณีด้วยก็ได้”

๑.๒ อาศัยอำนาจตามความในมาตรา ๓๕ แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ จึงได้มีการตราพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๔๙ ขึ้น ซึ่งมีข้อกำหนดที่เกี่ยวข้อง ๓ มาตรา ดังนี้

๑.๒.๑ มาตรา ๕ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐ หรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้

แนวนโยบายและแนวปฏิบัติอย่างน้อยต้องประกอบด้วยเนื้อหา ดังต่อไปนี้

(๑) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

(๒) การจัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งาน และจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

(๓) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

๑.๒.๒ มาตรา ๗ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเป็นประกาศ และต้องได้รับความเห็นชอบจากคณะกรรมการหรือหน่วยงานที่คณะกรรมการมอบหมาย จึงมีผลใช้บังคับได้

หน่วยงานของรัฐต้องปฏิบัติตามแนวนโยบายและแนวปฏิบัติที่ได้แสดงไว้ และให้จัดให้มีการตรวจสอบการปฏิบัติตามแนวนโยบายและแนวปฏิบัติที่กำหนดไว้อย่างสม่ำเสมอ

๑.๒.๓ มาตรา ๘ กำหนดให้คณะกรรมการหรือหน่วยงานที่คณะกรรมการมอบหมายจัดทำแนวนโยบายและแนวปฏิบัติหรือการอื่นอันเกี่ยวกับการดำเนินการตามพระราชกฤษฎีกานี้ ไว้เป็นตัวอย่างเบื้องต้น สำหรับการดำเนินการของหน่วยงานของรัฐในการปฏิบัติตามพระราชกฤษฎีกานี้ และหากหน่วยงานของรัฐแห่งใดมีการปฏิบัติงานตามกฎหมายที่แตกต่างเป็นการเฉพาะแล้ว หน่วยงานของรัฐแห่งนั้นอาจเพิ่มเติมรายละเอียดการปฏิบัติงานตามกฎหมายที่แตกต่างนั้นได้โดยออกเป็นระเบียบ ทั้งนี้ โดยให้คำนึงถึงความถูกต้องครบถ้วน ความน่าเชื่อถือ สภาพความพร้อมใช้งาน และความมั่นคงปลอดภัยของระบบและข้อมูลอิเล็กทรอนิกส์

๑.๓ อาศัยอำนาจตามความในมาตรา ๕ มาตรา ๗ และมาตรา ๘ แห่งพระราชกฤษฎีกา กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๔๙ คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์จึงได้จัดทำประกาศ เรื่อง แนวโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ เพื่อเป็นแนวทางเบื้องต้นให้หน่วยงานของรัฐใช้ในการกำหนดนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ซึ่งได้ประกาศในราชกิจจานุเบกษาแล้ว เมื่อวันที่ ๒๓ มิถุนายน ๒๕๕๓ และมีผลใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

๑.๔ คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ได้มีประกาศ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ (ฉบับที่ ๒) พ.ศ. ๒๕๕๖ ซึ่งเน้นการแสดงความรับผิดชอบของผู้บริหารระดับสูง โดยระบุให้ “หน่วยงานของรัฐต้องกำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ทั้งนี้ ให้ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Office : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น” โดยได้มีการประกาศในราชกิจจานุเบกษาแล้ว เมื่อวันที่ ๑๔ กุมภาพันธ์ ๒๕๕๖ และมีผลใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

๒. วัตถุประสงค์

๒.๑ เพื่อเป็นเครื่องมือช่วยในการจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ซึ่งมีความสำคัญเป็นอย่างยิ่งในการบริหารจัดการ และแก้ไขปัญหาความเสี่ยงที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศและการสื่อสาร อีกทั้งยังมีความสำคัญต่อการพัฒนาศักยภาพของระบบรักษาความมั่นคงปลอดภัยของข้อมูล ส่งผลให้เกิดประโยชน์สูงสุดโดยตรงต่อนโยบายและจุดประสงค์หลักด้านเทคโนโลยีสารสนเทศขององค์กร

๒.๒ เพื่อเป็นคู่มือในการกำหนดแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ซึ่งควรคำนึงถึงความถูกต้องครบถ้วน ความน่าเชื่อถือ สภาพความพร้อมใช้งาน และความมั่นคงปลอดภัยของระบบและข้อมูลอิเล็กทรอนิกส์ รวมทั้งครอบคลุมการควบคุมการเข้าถึง การกำหนดขั้นตอนและกระบวนการที่เหมาะสม ตามหลักมาตรฐานสากล เพื่อสร้างความมั่นคงปลอดภัยให้กับองค์กรได้อย่างเหมาะสมและมีความน่าเชื่อถือ

บทที่ ๒
ขั้นตอนการดำเนินงาน

ขั้นตอนปฏิบัติในการจัดส่งนโยบายและแนวปฏิบัติ ตามความในมาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ แบ่งเป็น ๔ กระบวนการ คือ

๑. การประเมินด้วยตนเอง (self-assessment)

๒. การพิจารณาให้ความเห็นเบื้องต้น โดยสำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

๓. การพิจารณาให้ความเห็น โดยคณะอนุกรรมการความมั่นคงปลอดภัย

๔. การพิจารณาให้ความเห็นชอบ โดยคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

โดยมีรายละเอียดการพิจารณาในแต่ละขั้นตอนดังนี้

<u>ขั้นตอนที่ ๑ การประเมินด้วยตนเอง (self-assessment)</u>

๑. ติดต่อขอรับแบบประเมินประกอบการพิจารณาการดำเนินงานตามแนวนโยบายและแนวปฏิบัติตามมาตรา ๗ ในพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ จากสำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ (ธอ.) สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร หรือดาวน์โหลดจาก <u>http://www.etcommission.go.th/</u> หรือ <u>http://www.mict.go.th/</u> “หัวข้อ download”

๒. ตรวจสอบการดำเนินงานของหน่วยงานว่ามีการดำเนินงานครบถ้วนตามข้อกำหนดในประกาศหรือไม่ โดยใช้แบบประเมินฯ เป็น Checklist เบื้องต้น

๓. ดำเนินการปรับปรุงแก้ไขการปฏิบัติงานด้านสารสนเทศขององค์กร ให้สอดคล้องกับข้อกำหนดตามประกาศของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ โดยหน่วยงานอาจมีกระบวนการกลั่นกรอง หรือกระบวนการบริหารจัดการภายในองค์กร เช่น การแต่งตั้งคณะกรรมการ หรือคณะทำงานที่เกี่ยวข้อง เพื่อทำหน้าที่ในการตรวจสอบรายละเอียดการดำเนินงานให้มีความครบถ้วนตามประกาศดังกล่าว ทั้งนี้ หากหน่วยงานมีคณะกรรมการหรือคณะทำงานที่เกี่ยวข้องแล้ว ไม่ต้องแต่งตั้งใหม่ แต่อาจให้คณะดังกล่าวทำการทบทวนความครบถ้วนอีกครั้ง

๔. เมื่อหน่วยงานพร้อมที่จะขอรับความเห็นชอบจากคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ **<u>ให้นำเสนอแบบประเมินตนเอง ต่อ “ผู้บริหารสูงสุด หรือผู้ที่ได้รับมอบอำนาจ”ของหน่วยงาน เพื่อลงนามท้ายแบบประเมินดังกล่าว</u>** ก่อนนำส่งแบบประเมินพร้อมเอกสารอ้างอิงให้สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ในฐานะฝ่ายเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ พิจารณาให้ความเห็นเบื้องต้นก่อน ทั้งนี้ ให้จัดส่งเอกสารตามที่อยู่ด้านล่างนี้

เรียน คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
<u>ที่อยู่ในการจัดส่ง</u> : สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษาฯ
อาคารรัฐประศาสนภักดี ถนนแจ้งวัฒนะ
เขตหลักสี่ กรุงเทพฯ ๑๐๒๑๐

ขั้นตอนที่ ๒ การพิจารณาให้ความเห็นเบื้องต้น โดยสำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

๑. สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ในฐานะฝ่ายเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ตรวจสอบรายละเอียดแบบประเมิน และให้ความเห็นเบื้องต้น

๒. หากไม่เห็นด้วยกับการประเมินตนเองของหน่วยงาน จะประสานให้ปรับแก้ไข และให้หน่วยงานนำเสนออีกครั้ง

๓. หากเห็นด้วย จะนำเสนอคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์เพื่อพิจารณา ผ่านคณะอนุกรรมการความมั่นคงปลอดภัย ซึ่งได้รับมอบหมายจากคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ให้เป็นผู้พิจารณากลั่นกรองตามความเห็นเบื้องต้นของสำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

ขั้นตอนที่ ๓ การพิจารณาให้ความเห็น โดยคณะอนุกรรมการความมั่นคงปลอดภัย

๑. หากคณะอนุกรรมการความมั่นคงปลอดภัย พบประเด็นที่เป็นข้อสังเกต จะประสานแจ้งหน่วยงานให้ชี้แจง เพิ่มเติม หรือปรับปรุงแก้ไข และให้นำเสนอต่อคณะอนุกรรมการฯ พิจารณาอีกครั้ง

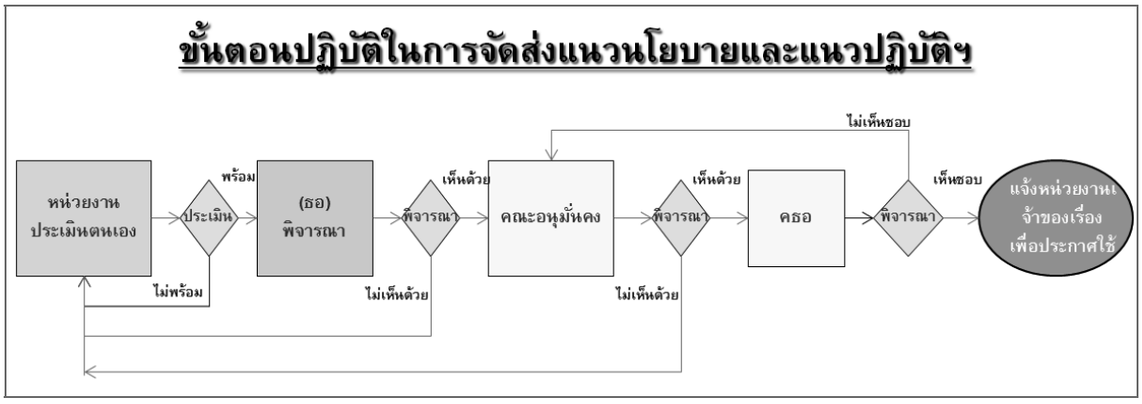
๒. หากคณะอนุกรรมการความมั่นคงปลอดภัย ไม่พบประเด็นที่เป็นข้อสังเกต จะนำเสนอความเห็นต่อคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เพื่อพิจารณาให้ความเห็นชอบ ต่อไป

ขั้นตอนที่ ๔ การพิจารณาให้ความเห็นชอบ โดยคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ (คธอ.)

๑. เมื่อคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์พิจารณาให้ความเห็นชอบ สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ จะแจ้งหน่วยงานเจ้าของเรื่องทราบ เพื่อประกาศใช้ต่อไป

๒. หากคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์พิจารณาแล้วไม่เห็นชอบ สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ จะนำส่งคืนให้คณะอนุกรรมการความมั่นคงปลอดภัยพิจารณาเพิ่มเติมอีกครั้ง

ผังแสดงกระบวนการพิจารณากลั่นกรอง



ติดต่อสอบถามข้อมูลเพิ่มเติม

กลุ่มงานผลักดันธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ

๑. นางสาวรัตนา จรูญศักดิ์สิทธิ์ หมายเลข ๐๒-๑๔๑-๖๙๘๘

๒. นายทวีสิทธิ์ เพ็ญรัศมีพูนสุข หมายเลข ๐๒-๑๔๑-๖๕๙๔

๓. นายธวัชชัย ศิริกุล หมายเลข ๐๒-๑๔๑-๖๙๘๙

บทที่ ๓
เอกสารสำคัญตามมาตรฐานขั้นต่ำ

ตามความในมาตรา ๕ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐ หรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ ซึ่งต้องประกอบด้วยเนื้อหาอย่างน้อย ๓ ประการ ดังนี้

(๑) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

(๒) การจัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งาน และจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

(๓) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

ดังนั้น ในการจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของหน่วยงานของรัฐ จึงควรมีเอกสารซึ่งครอบคลุมเนื้อหาดังกล่าว อย่างน้อย ๕ รายการ ต่อไปนี้

๑. ประกาศนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ซึ่งลงนามโดยผู้บริหารสูงสุดของหน่วยงาน เพื่อให้มีผลใช้บังคับในองค์กร โดยมีเนื้อหาสาระเชิงหลักการกว้าง ๆ ให้ครอบคลุมตามที่ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์กำหนด

๒. ขั้นตอนปฏิบัติในการรักษาความมั่นคงที่มีลักษณะเฉพาะเจาะจงและสามารถปฏิบัติได้จริง

๓. แผนสำรองระบบสารสนเทศ

๔. แผนเตรียมความพร้อมกรณีฉุกเฉิน

๕. คำสั่งแต่งตั้งผู้มีหน้าที่รับผิดชอบในด้านต่าง ๆ ภายใต้นโยบายและแนวปฏิบัติฯ อาทิ

๕.๑ ผู้รับผิดชอบต่อนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย รวมทั้งการจัดทำ และการทบทวนแก้ไขให้มีความทันสมัยอยู่เสมอ

๕.๒ ผู้รับผิดชอบต่อแผนเตรียมความพร้อมฉุกเฉิน และแผนสำรอง

๕.๓ ผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ทั้งนี้ การระบุรายละเอียดในการปฏิบัติ ควรมีความเชื่อมโยงที่ชัดเจน ทั้งตัวบุคคล ตำแหน่ง อำนาจหน้าที่ภายในโครงสร้างองค์กร และกฎระเบียบที่เกี่ยวข้อง เพื่อให้การรักษาความมั่นคงปลอดภัยมีความสอดคล้องกับสิทธิต่าง ๆ ที่เกี่ยวข้องอย่างเหมาะสม

บทที่ ๔
แนวทางการจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ (ฉบับที่ ๒) พ.ศ. ๒๕๕๖ ประกอบด้วย ข้อกำหนดหลักจำนวน ๑๔ ข้อ และมีข้อปฏิบัติย่อย รวมทั้งสิ้น ๕๒ ข้อย่อย ทั้งนี้ มีแนวทางการจัดทำรายละเอียดของเอกสาร “นโยบายและแนวปฏิบัติ” ในแต่ละประเด็น ดังต่อไปนี้

ข้อ	แนวนโยบาย / และแนวปฏิบัติ (ประกาศของคณะกรรมการ)	ข้อแนะนำในการเขียนข้อปฏิบัติของหน่วยงาน
๑	**กำหนดคำนิยาม**	**อาจอ้างอิงตามประกาศ หรือ อธิบายขอบเขตที่สอดคล้องกับประกาศ**
	(๑) ผู้ใช้งาน	ผู้ใช้งานในองค์กร หมายถึงใครบ้าง ควรระบุให้ชัดเจนว่า มีความเกี่ยวข้องอย่างไร
	(๒) สิทธิของผู้ใช้งาน	สิทธิในการใช้งานมีอะไรบ้าง ผู้ใช้งานในองค์กร มีสิทธิใดบ้าง
	(๓) สินทรัพย์	สินทรัพย์ที่เกี่ยวข้องหมายรวมถึงอะไรบ้าง
	(๔) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ	การเข้าถึง หรือควบคุมการใช้งานสารสนเทศ หมายรวมถึงอะไรบ้าง
	(๕) ความมั่นคงปลอดภัยด้านสารสนเทศ	ความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร หมายรวมถึงอะไรบ้าง
	(๖) เหตุการณ์ด้านความมั่นคงปลอดภัย	เหตุการณ์ที่เกิดขึ้นแล้ว หรือ เหตุการณ์ที่เคยเกิดขึ้นจริงและมีการดำเนินงานแล้ว
	(๗) สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด	สถานการณ์ที่อาจยังไม่เกิดขึ้นจริง หรือ คาดว่าจะเกิดขึ้น และมีมาตรการเตรียมรองรับเพื่อป้องกันและแก้ไขปัญหาที่จะเกิดขึ้น
	(๘) คำนิยามอื่น ๆ ตามความต้องการขององค์กร	นิยามอื่น ๆ ที่องค์กรเห็นสมควร
๒	**หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร ซึ่งอย่างน้อยต้องประกอบด้วยเนื้อหา ดังต่อไปนี้**	
	(๑) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ	ต้องมีการจัดทำนโยบายเพื่อควบคุมการเข้าถึงและการใช้งานสารสนเทศที่เป็นเป้าหมาย **<u>อย่างน้อย</u>**ต้องครอบคลุม ๔ เรื่อง ดังนี้

ข้อ	แนวนโยบาย / และแนวปฏิบัติ (ประกาศของคณะกรรมการ)	ข้อแนะนำในการเขียนข้อปฏิบัติของหน่วยงาน
		(๑) การเข้าถึงระบบสารสนเทศ (๒) การเข้าถึงระบบเครือข่าย (๓) การเข้าถึงระบบปฏิบัติการ (๔) การเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ
	(๒) จัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งานและจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง	ต้องมีการจัดทำนโยบายเกี่ยวกับการสำรองข้อมูลเพื่อให้สารสนเทศอยู่ในสภาพพร้อมใช้งาน และการจัดทำแผนเตรียมความพร้อม
	(๓) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ	ต้องมีการจัดทำนโยบายเกี่ยวกับการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ
๓	**หน่วยงานของรัฐต้องจัดให้มีข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน ซึ่งอย่างน้อยต้องประกอบด้วยกระบวนการ ดังต่อไปนี้**	
	(๑) หน่วยงานของรัฐต้องจัดทำข้อปฏิบัติที่สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน	ระบุให้ชัดเจนว่า มีการจัดทำข้อปฏิบัติที่สอดคล้องกับนโยบายในข้อ ๒ ทุกข้อ
	(๒) หน่วยงานของรัฐต้องประกาศนโยบายและข้อปฏิบัติดังกล่าว ให้ผู้เกี่ยวข้องทั้งหมดทราบ เพื่อให้สามารถเข้าถึง เข้าใจ และปฏิบัติตามนโยบายและข้อปฏิบัติได้	- ต้องมีการประกาศนโยบาย ซึ่งลงนามโดยผู้บริหารของหน่วยงาน พร้อมทั้งให้ระบุวิธีการประกาศและควรระบุไว้เป็นส่วนหนึ่งของนโยบาย - กรณีหน่วยงานมี “ผู้รับบริการทางอิเล็กทรอนิกส์” ต้องประกาศนโยบายและแนวปฏิบัติฯ ให้ผู้รับบริการทราบด้วย - หากหน่วยงานเห็นว่า “นโยบายและแนวปฏิบัติฯ” เป็นเรื่องลับ ไม่สามารถเปิดเผยได้ทั้งหมด ให้จัดทำเอกสาร “นโยบายและแนวปฏิบัติฯ (ฉบับผู้รับบริการ)” แยกส่วนที่สามารถเปิดเผยได้ขึ้นอีกฉบับ เพื่อแจ้งให้ผู้รับบริการทราบด้วย
	(๓) หน่วยงานของรัฐต้องกำหนดผู้รับผิดชอบตามนโยบายและข้อปฏิบัติดังกล่าวให้ชัดเจน	ต้องมีการกำหนดผู้รับผิดชอบตามนโยบายและข้อปฏิบัติที่กำหนดไว้อย่างชัดเจน โดยเชื่อมโยงทั้งตัวบุคคล ตำแหน่ง และภารกิจที่รับผิดชอบ

ข้อ	แนวนโยบาย / และแนวปฏิบัติ (ประกาศของคณะกรรมการ)	ข้อแนะนำในการเขียนข้อปฏิบัติของหน่วยงาน
	(๔) หน่วยงานของรัฐต้องทบทวนปรับปรุงนโยบายและข้อปฏิบัติให้เป็นปัจจุบันอยู่เสมอ	ต้องมีการกำหนดระยะเวลาในการทบทวนปรับปรุงนโยบายและข้อปฏิบัติให้เป็นปัจจุบัน ระบุว่ามีความถี่อย่างไร
๔	**ข้อปฏิบัติในด้านการรักษาความมั่นคงปลอดภัย ต้องมีเนื้อหาอย่างน้อยครอบคลุมตามข้อ ๕ – ๑๕**	ระบุชื่อเอกสารที่ใช้เป็นแนวปฏิบัติทั้งหมดที่เกี่ยวข้อง
๕	**ให้มีข้อกำหนดการเข้าถึงและควบคุมการใช้งานสารสนเทศ (access control) ซึ่งต้องมีเนื้อหาอย่างน้อย ดังนี้**	
	(๑) หน่วยงานของรัฐต้องมีการควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย	ต้องมีขั้นตอนปฏิบัติที่แสดงถึงการควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล
	(๒) ในการกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง ต้องกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจของหน่วยงานของรัฐนั้น ๆ	ต้องมีขั้นตอนปฏิบัติที่แสดงถึงการกำหนดสิทธิ เช่น มีสิทธิอย่างไร มีการอนุญาตอย่างไร หรือมีการมอบอำนาจในเรื่องใดบ้าง
	(๓) หน่วยงานของรัฐต้องกำหนดเกี่ยวกับ - ประเภทของข้อมูล - ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล - ระดับชั้นการเข้าถึง - เวลาที่ได้เข้าถึง - ช่องทางการเข้าถึง	ต้องมีรายละเอียดที่แสดงถึงการกำหนดในเรื่องต่อไปนี้ครบทุกประเด็น - ระบุประเภทของข้อมูลให้ชัดเจน - ระบุการจัดลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูลให้ชัดเจน - ระบุระดับชั้นการเข้าถึงว่าใครเป็นผู้มีสิทธิหรือไม่มีสิทธิในการเข้าถึงข้อมูล - ระบุวัน เวลา หากมีการกำหนดเป็นช่วงวันเวลาที่สามารถเข้าถึงได้ - รวมถึงระบุช่องทางที่สามารถเข้าถึงข้อมูลได้
๖	**ให้มีข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (business requirements for access control) โดยแบ่งการจัดทำข้อปฏิบัติเป็น ๒ ส่วนคือ การควบคุมการเข้าถึงสารสนเทศ และ การปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความ**	ต้องมีข้อกำหนดสำหรับควบคุมการเข้าถึงสารสนเทศ ซึ่งแสดงให้เห็นขั้นตอนปฏิบัติ ๒ ส่วน ดังนี้ - การควบคุมการเข้าถึงสารสนเทศ - การปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

ข้อ	แนวนโยบาย / และแนวปฏิบัติ (ประกาศของคณะกรรมการ)	ข้อแนะนำในการเขียนข้อปฏิบัติของหน่วยงาน
	มั่นคงปลอดภัย	
๗	**ให้มีการบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว และผ่านการฝึกอบรม หลักสูตรการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (information security awareness training) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต โดยต้องมีเนื้อหาอย่างน้อย ดังนี้**	ต้องมีการกำหนดขั้นตอนปฏิบัติ ๒ เรื่อง ดังนี้ - บริหารจัดการการเข้าถึงของผู้ใช้งาน - การฝึกอบรม หลักสูตรการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (information security awareness training)
	(๑) สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม	ต้องมีการกำหนด หลักสูตรฝึกอบรมเกี่ยวกับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (information security awareness training)
	(๒) การลงทะเบียนผู้ใช้งาน (user registration) ต้องกำหนดให้มีขั้นตอนทางปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานเมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว	- ต้องแสดงขั้นตอนปฏิบัติในการลงทะเบียนผู้ใช้งาน - ต้องแสดงข้อปฏิบัติ/หลักเกณฑ์ในการอนุญาตให้เข้าถึงระบบสารสนเทศ - ต้องแสดงข้อปฏิบัติ/หลักเกณฑ์ในการยกเลิกเพิกถอนการอนุญาตให้เข้าถึงระบบสารสนเทศ
	(๓) การบริหารจัดการสิทธิของผู้ใช้งาน (user management) ต้องจัดให้มีการควบคุมและจำกัดสิทธิเพื่อเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่น ๆ ที่เกี่ยวข้องกับการเข้าถึง	- ต้องมีรายละเอียดแสดงถึงการควบคุมและจำกัดสิทธิการใช้งาน (การเข้าถึงข้อมูลและระบบเทคโนโลยีสารสนเทศ) - ต้องแสดงกระบวนการในการมอบหมายหรือกำหนดสิทธิการใช้งานให้แก่ผู้ใช้งาน - ต้องมีการกำหนดระดับสิทธิในการเข้าถึงระบบงานที่เหมาะสมตามหน้าที่ความรับผิดชอบ และตามความจำเป็นในการใช้งาน
	(๔) การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน(user password management) ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม	- ต้องมีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน

ข้อ	แนวนโยบาย / และแนวปฏิบัติ (ประกาศของคณะกรรมการ)	ข้อแนะนำในการเขียนข้อปฏิบัติของหน่วยงาน
	(๕) การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (review of user access rights) ต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศตามระยะเวลาที่กำหนดไว้	- ต้องมีการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศตามระยะเวลาที่กำหนด
๘	**ให้มีการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ โดยต้องมีเนื้อหาอย่างน้อย ดังนี้**	ต้องมีการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งานให้ครอบคลุมเรื่องดังนี้ - ป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต - การเปิดเผย การล่วงรู้ - การลักลอบทำสำเนาข้อมูลสารสนเทศ - การลักขโมยอุปกรณ์ประมวลผลสารสนเทศ
	(๑) การใช้งานรหัสผ่าน (password use) ต้องกำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ	ต้องกำหนดวิธีปฏิบัติในการเลือกและใช้งานรหัสผ่าน รวมทั้งกำหนดวิธีปฏิบัติในการเปลี่ยนรหัสผ่านที่มีคุณภาพ
	(๒) การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ ต้องกำหนดข้อปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล	- ต้องกำหนดวิธีปฏิบัติในการป้องกันอุปกรณ์ขององค์กรในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ - ต้องสร้างความตระหนักให้พนักงานเข้าใจในมาตรการป้องกัน
	(๓) การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (clear desk and clear screen policy) ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์ หรือสารสนเทศ อยู่ในภาวะซึ่งเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน	- ต้องมีวิธีปฏิบัติในการควบคุมไม่ให้มีการทิ้งหรือปล่อยสินทรัพย์สารสนเทศที่สำคัญ ให้อยู่ในสถานที่ที่ไม่ปลอดภัย - ต้องมีวิธีปฏิบัติในการทำลายสื่อบันทึกข้อมูล ทำลายข้อมูลอิเล็กทรอนิกส์ และแฟ้มข้อมูลในสื่ออิเล็กทรอนิกส์ที่เป็นมาตรฐาน และไม่สามารถกู้คืนกลับมาใช้ใหม่ได้
	(๔) ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ.๒๕๔๔	- ต้องมีวิธีปฏิบัติเกี่ยวกับการนำวิธีการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ หรือข้อมูลที่สำคัญยิ่งยวด - ทั้งนี้ให้สอดคล้องกับการกำหนดประเภทข้อมูลในประกาศฯ ข้อ ๕(๓)

ข้อ	แนวนโยบาย / และแนวปฏิบัติ (ประกาศของคณะกรรมการ)	ข้อแนะนำในการเขียนข้อปฏิบัติของหน่วยงาน
๙	**ให้มีการควบคุมการเข้าถึงเครือข่าย (network access control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต โดยต้องมีเนื้อหาอย่างน้อย ดังนี้**	ต้องมีข้อปฏิบัติ/หลักเกณฑ์ที่เกี่ยวข้องกับการป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต
	(๑) การใช้งานบริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น	- ต้องกำหนดระบบสารสนเทศที่จำเป็นต้องมีการควบคุมการเข้าถึง - ต้องมีข้อปฏิบัติที่กำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น
	(๒) การยืนยันตัวบุคคลสำหรับผู้ใช้ที่อยู่ภายนอกองค์กร (user authentication for external connections) ต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกองค์กรสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศขององค์กรได้	ต้องมีข้อปฏิบัติ/กระบวนการที่ช่วยยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกองค์กรสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศขององค์กรได้ - ระบุมาตรการทางเทคนิคที่ชัดเจน
	(๓) การระบุอุปกรณ์บนเครือข่าย (equipment identification in networks) ต้องมีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และควรใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน	ต้องมีวิธีการ/กระบวนการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ โดยสามารถใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยันการเข้าถึง - ระบุมาตรการทางเทคนิคที่ชัดเจน
	(๔) การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (remote diagnostic and configuration port protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ ทั้งการเข้าถึงทางกายภาพและทางเครือข่าย	ต้องมีแนวปฏิบัติในการควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ ดังนี้ - การเข้าถึงทางกายภาพ - การเข้าถึงทางเครือข่าย
	(๕) การแบ่งแยกเครือข่าย (segregation in networks) ต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ	ต้องมีการแบ่งแยกเครือข่าย สำหรับกลุ่มต่าง ๆ เช่น - กลุ่มของบริการสารสนเทศ - กลุ่มผู้ใช้งาน - กลุ่มของระบบสารสนเทศ
	(๖) การควบคุมการเชื่อมต่อทางเครือข่าย (network connection control) ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่	ต้องมีแนวปฏิบัติในการควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างหน่วยงานให้สอดคล้องกับข้อปฏิบัติการควบคุมการ

ข้อ	แนวนโยบาย / และแนวปฏิบัติ (ประกาศของคณะกรรมการ)	ข้อแนะนำในการเขียนข้อปฏิบัติของหน่วยงาน
	มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างหน่วยงานให้สอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึง	เข้าถึงในแต่ละกลุ่มที่เกี่ยวข้อง
	(๗) การควบคุมการจัดเส้นทางบนเครือข่าย (network routing control) ต้องควบคุมการจัดเส้นทางบนเครือข่าย เพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ	ต้องมีแนวปฏิบัติในการจัดเส้นทางบนเครือข่าย ดังนี้ - ให้มีการเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศ - ต้องมีความสอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ
๑๐	**ให้มีการควบคุมการเข้าถึงระบบปฏิบัติการ (operating system access control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต โดยต้องมีเนื้อหาอย่างน้อย ดังนี้**	ต้องมีแนวปฏิบัติในการป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต
	(๑) การกำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย	ต้องมีขั้นตอนปฏิบัติในเรื่องดังนี้ - การเข้าใช้งานที่มั่นคงปลอดภัย - การเข้าถึงระบบปฏิบัติการ - ต้องมีวิธีการยืนยันตัวตน
	(๒) การระบุและยืนยันตัวตนของผู้ใช้งาน (user identification and authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง	ต้องมีการกำหนดข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน - ระบุมาตรการทางเทคนิคที่ชัดเจน
	(๓) การบริหารจัดการรหัสผ่าน (password management system) ต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ	ต้องมีการบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ หรือ อัตโนมัติ

ข้อ	แนวนโยบาย / และแนวปฏิบัติ (ประกาศของคณะกรรมการ)	ข้อแนะนำในการเขียนข้อปฏิบัติของหน่วยงาน
	(๔) การใช้งานโปรแกรมอรรถประโยชน์ (use of system utilities) ควรจำกัดและควบคุมการใช้งานโปรแกรมประเภทอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว	ต้องมีข้อปฏิบัติในการใช้งานโปรแกรมอรรถประโยชน์ โดยครอบคลุมเรื่องดังนี้ - ป้องกันการละเมิด - หลีกเลี่ยงมาตรการความมั่นคงปลอดภัย
	(๕) เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (session time-out)	ต้องมีข้อปฏิบัติในการกำหนดให้ยุติการใช้งานระบบสารสนเทศ เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่ง - ระบุระยะเวลาที่ชัดเจน
	(๖) การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (limitation of connection time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือแอพพลิเคชั่นที่มีความเสี่ยงหรือมีความสำคัญสูง	ต้องมีข้อปฏิบัติในการกำหนดให้จำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ สำหรับระบบสารสนเทศหรือแอพพลิเคชั่นที่มีความเสี่ยงหรือมีความสำคัญสูง - ระบุระยะเวลาที่ชัดเจน
๑๑	**ให้มีการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (application and information access control) โดยต้องมีการควบคุม ดังนี้**	ต้องมีข้อปฏิบัติในการป้องกันการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ
	(๑) การจำกัดการเข้าถึงสารสนเทศ (information access restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้าใช้งานในการเข้าถึงสารสนเทศและฟังก์ชัน (functions) ต่างๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น ทั้งนี้โดยให้สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้	ต้องมีข้อปฏิบัติในการจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งาน หรือบุคลากร โดยให้สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้ ต้องมีมาตรการควบคุม outsource กรณีมีการจ้างเหมาดำเนินการเกี่ยวกับระบบสารสนเทศของหน่วยงาน
	(๒) ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อองค์กร ต้องได้รับการแยกออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมของตนเอง	ต้องมีข้อปฏิบัติในการดูแลระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อองค์กร ซึ่งครอบคลุมในเรื่องต่อไปนี้ - การแยกระบบดังกล่าวออกจากระบบอื่น ๆ

ข้อ	แนวนโยบาย / และแนวปฏิบัติ (ประกาศของคณะกรรมการ)	ข้อแนะนำในการเขียนข้อปฏิบัติของหน่วยงาน
	โดยเฉพาะ ให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกองค์กร (mobile computing and teleworking)	- การควบคุมสภาพแวดล้อมของระบบดังกล่าวโดยเฉพาะ - การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกองค์กร (mobile computing and teleworking) ที่เกี่ยวข้องกับระบบดังกล่าว
	(๓) การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องกำหนดข้อปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่	ต้องมีข้อปฏิบัติในการควบคุมการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่
	(๔) การปฏิบัติงานจากภายนอกสำนักงาน (teleworking) ต้องกำหนดข้อปฏิบัติ แผนงาน และขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานขององค์กรจากภายนอกสำนักงาน	ต้องมีข้อปฏิบัติ/แผนงาน และขั้นตอนปฏิบัติ สำหรับการปฏิบัติงานขององค์กรจากภายนอกสำนักงาน
๑๒	**หน่วยงานของรัฐที่มีระบบสารสนเทศต้องจัดทำระบบสำรอง ตามแนวทางต่อไปนี้**	ต้องมีการจัดทำระบบสำรองสำหรับระบบสารสนเทศที่กำหนดไว้
	(๑) ต้องพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม	- ต้องมีการคัดเลือกระบบสารสนเทศ - ต้องมีการจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน
	(๒) ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ	- ต้องมีแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ - ต้องมีการปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ
	(๓) ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถ	ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรในเรื่องต่อไปนี้ - ระบบสารสนเทศ - ระบบสำรอง - การจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่

ข้อ	แนวนโยบาย / และแนวปฏิบัติ (ประกาศของคณะกรรมการ)	ข้อแนะนำในการเขียนข้อปฏิบัติของหน่วยงาน
	ดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์	สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ ทั้งนี้ ต้องสามารถเชื่อมโยงทั้งตัวบุคคล ตำแหน่ง และภารกิจที่รับผิดชอบ
	(๔) ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ (โปรดระบุความถี่)	ต้องมีความถี่ในการทดสอบสภาพพร้อมใช้งานในเรื่องดังต่อไปนี้ - ระบบสารสนเทศ - ระบบสำรอง - ระบบแผนเตรียมพร้อมกรณีฉุกเฉิน
	(๕) สำหรับความถี่ของการปฏิบัติในแต่ละข้อ ควรมีการปฏิบัติที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน	ระบุความถี่อื่น ๆ ในการปฏิบัติ ตามข้อ (๑) – (๓)
๑๓	**หน่วยงานของรัฐต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศโดยต้องมีเนื้อหาอย่างน้อย ดังนี้**	ต้องมีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ
	(๑) หน่วยงานของรัฐต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (information security audit and assessment) อย่างน้อยปีละ ๑ ครั้ง	- ต้องมีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (information security audit and assessment) - ต้องกำหนดความถี่ในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง
	(๒) ในการตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการ โดยผู้ตรวจสอบภายในหน่วยงานของรัฐ (internal auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (external auditor) เพื่อให้หน่วยงานของรัฐได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน	ต้องมีการตรวจสอบและประเมินความเสี่ยงโดยบุคลากร ดังนี้ - ผู้ตรวจสอบภายในหน่วยงานของรัฐ (internal auditor) **<u>หรือ</u>** - ผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (external auditor)
๑๔	**หน่วยงานของรัฐต้องกำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติใน**	ต้องกำหนดให้ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Office : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

ข้อ	แนวนโยบาย / และแนวปฏิบัติ (ประกาศของคณะกรรมการ)	ข้อแนะนำในการเขียนข้อปฏิบัติของหน่วยงาน
	การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ทั้งนี้ ให้ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Office : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น	

ข้อแนะนำทั่วไปในการจัดทำแนวปฏิบัติ

๑. ระบุให้ชัดเจนว่า ในแต่ละประเด็นเกี่ยวข้องกับผู้ใด ต้องปฏิบัติอย่างไร เช่น ผู้บริหาร ผู้ดูแลระบบ ผู้ใช้งาน

๒. หลีกเลี่ยงคำว่า “กำหนดให้มี” “ต้องกำหนดให้” “กำหนดขั้นตอนปฏิบัติ” “แสดงหลักฐาน” หรือคำอื่นใดที่ไม่แสดงถึงแนวปฏิบัติที่ชัดเจน เนื่องจากเป็นข้อความเชิงนโยบาย ดังนั้น ควรกำหนดรายละเอียดแนวปฏิบัติที่ชัดเจน

๓. หลีกเลี่ยงคำว่า “เช่น” เนื่องจาก “แนวปฏิบัติ” เป็นเอกสารที่กำหนดให้มีการปฏิบัติ ดังนั้น จึงไม่ใช่ “การยกตัวอย่าง”

๔. หลีกเลี่ยงคำว่า “ควร” เนื่องจาก “แนวปฏิบัติ” เป็นเอกสารที่กำหนดให้มีการปฏิบัติ ดังนั้น จึงไม่ใช่ “การแนะนำ”

๕. หลีกเลี่ยงคำว่า “มี” เนื่องจากเป็น ประโยคบอกเล่า ในลักษณะการรายงาน ควรใช้คำว่า “ต้อง” เพื่อเป็นประโยคคำสั่งให้ปฏิบัติ

หมายเหตุ : ทั้งนี้ ขอให้หน่วยงานพิจารณาการใช้ถ้อยคำในเอกสารตามความเหมาะสมด้วย

บทที่ ๕
รูปแบบเอกสารที่เหมาะสม

เอกสาร “นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ” ไม่มีรูปแบบตายตัว ขึ้นอยู่กับความต้องการของหน่วยงานว่าจะจัดทำในลักษณะใด ทั้งนี้ จากข้อกำหนดที่ปรากฏตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ พบว่า หน่วยงานควรจัดทำเอกสารแยกเป็น ๒ ฉบับ คือ

๑. เอกสาร “นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ” ควรจัดทำในรูปประกาศของหน่วยงาน ลงนามโดยผู้บริหารสูงสุดของหน่วยงาน เนื้อหาสาระควรประกอบด้วย คำนำ ข้ออ้างอิงตามกฎหมาย ระบุวัตถุประสงค์ของนโยบาย ขอบเขตของนโยบายสำคัญด้านเทคโนโลยีสารสนเทศอย่างกว้างๆ และควรมีเนื้อหาสาระสำคัญอย่างน้อยตามมาตรฐานขั้นต่ำที่ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์กำหนดไว้ คือ

๑.๑ การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

๑.๒ การจัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งาน และจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

๑.๓ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

นอกจากนี้ ยังควรระบุสาระสำคัญด้านอื่น ๆ ในเชิงนโยบาย เพิ่มเติม เช่น

๑.๔ การบริหารจัดการด้านเทคโนโลยีสารสนเทศ

๑.๕ การใช้งานคอมพิวเตอร์ ระบบเครือข่าย ระบบสารสนเทศ และฐานข้อมูล

๑.๖ การบริหารจัดการด้านบุคลากรที่เกี่ยวข้องกับการใช้งาน

๑.๗ การเผยแพร่ข้อมูลข่าวสารด้านเทคโนโลยีสารสนเทศภายในองค์กร

๑.๘ การประกาศนโยบายและข้อปฏิบัติดังกล่าว ให้ผู้เกี่ยวข้องทั้งหมดทราบ เพื่อให้สามารถเข้าถึง เข้าใจ และปฏิบัติตามนโยบายและข้อปฏิบัติได้

๑.๙ การกำหนดผู้รับผิดชอบตามนโยบายและข้อปฏิบัติฯ ที่ชัดเจน

๑.๑๐ การทบทวนปรับปรุงนโยบายและข้อปฏิบัติให้เป็นปัจจุบันอยู่เสมอ

พร้อมทั้งระบุให้มีการจัดทำข้อปฏิบัติที่สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่ระบุไว้ข้างต้น โดยอาจจัดทำเป็นเอกสารแนบท้ายประกาศ

หมายเหตุ : สาระสำคัญที่ปรากฏในนโยบายควรสอดคล้องกับประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ ข้อ ๒ ข้อ ๓ และข้อ ๑๔

ตัวอย่างเอกสาร ประกาศ “นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ”

ประกาศ (ระบุชื่อหน่วยงาน)

เรื่อง

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

คำนำ (ระบุเหตุผลความจำเป็น และข้ออ้างอิงตามกฎหมาย)

วัตถุประสงค์ของนโยบาย .....

ขอบเขตสำคัญของนโยบาย

.....

.....

.....

ระบุผู้รับผิดชอบตามนโยบายและข้อปฏิบัติฯ ที่ชัดเจน

ระบุการทบทวนปรับปรุงนโยบายและข้อปฏิบัติให้เป็นปัจจุบันอยู่เสมอ

ระบุการจัดทำรายละเอียดแนวปฏิบัติเป็นเอกสารแนบท้ายประกาศ

ระบุวันที่มีผลใช้บังคับ

ระบุ .....(ผู้ลงนาม).....

ระบุ (ตำแหน่งผู้ลงนาม)

๒. เอกสาร “แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ” ควรจัดทำเป็นเอกสารแนบท้ายประกาศ โดยมีสาระสำคัญสอดคล้องกับประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ ตั้งแต่ ข้อ ๕ – ๑๓ รวมทั้งให้ระบุคำนิยามตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ และคำนิยามอื่น ๆ ที่ได้มีการอ้างอิงถึง ทั้งนี้ ควรแบ่งเนื้อหาสาระเป็นส่วน ๆ ตามขอบเขตนโยบายที่กำหนดไว้ในประกาศข้างต้น ซึ่งแต่ละส่วนควรประกอบด้วยหัวข้อต่อไปนี้

๒.๑ วัตถุประสงค์ของนโยบายในแต่ละส่วน

๒.๒ ผู้รับผิดชอบนโยบายในแต่ละส่วน

๒.๓ การอ้างอิงมาตรฐานสากลที่เกี่ยวข้องและสอดคล้อง

๒.๔ แนวปฏิบัติภายใต้นโยบายในแต่ละส่วน

โดยมีรูปแบบตัวอย่างดังนี้

เอกสารแนบท้ายประกาศ
เรื่อง.....

ว่าด้วยคำนิยาม

ระบุรายการคำนิยามที่เกี่ยวข้องทั้งหมด

ผู้ใช้งาน .....

สิทธิ์ของผู้ใช้งาน.....

สินทรัพย์.....

และคำนิยามอื่น ๆ

เอกสารแนบท้ายประกาศ
เรื่อง.....

ส่วนที่ ๑
นโยบาย.....

วัตถุประสงค์

ผู้รับผิดชอบ

อ้างอิงมาตรฐาน

ข้อปฏิบัติ
๑).....
๑.๑).....

บทที่ ๖
การจัดทำรายละเอียดนโยบายและแนวปฏิบัติที่เกี่ยวข้อง

ในการจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน สิ่งที่ควรคำนึงถึงเป็นประการแรกคือ การประเมินสถานภาพการดำเนินงานด้านสารสนเทศของหน่วยงานเองว่า มีความพร้อมในเรื่องใด หรือมีความเสี่ยงมากน้อยเพียงใด ทั้งนี้ เพื่อให้การจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศมีความเหมาะสมและสอดคล้องกับภารกิจของหน่วยงานอย่างแท้จริง คณะผู้จัดทำฯ จึงได้แบ่งขั้นตอนการจัดทำรายละเอียดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เป็น ๒ กระบวนการ คือ

๑. การประเมินสถานภาพการดำเนินงานด้านสารสนเทศ

๒. การรวบรวมและจัดทำแนวปฏิบัติที่เหมาะสม

<u>การประเมินสถานภาพการดำเนินงานด้านสารสนเทศ</u>

ในการประเมินสถานภาพการดำเนินงานด้านสารสนเทศของหน่วยงาน ควรมีขอบเขตที่ชัดเจนและสอดคล้องตามมาตรฐานขั้นต่ำที่ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์กำหนดไว้ ในการนี้ คณะผู้จัดทำฯ จึงได้จัดเตรียมแบบประเมินสถานภาพการดำเนินงานด้านสารสนเทศ เพื่อให้หน่วยงานของรัฐใช้สำหรับทบทวนรายละเอียดการดำเนินงานของตนเอง โดยมีข้อแนะนำการใช้แบบประเมินสถานภาพด้านเทคโนโลยีสารสนเทศของตนเองดังนี้

๑. ศึกษาประเด็นด้านเทคโนโลยีสารสนเทศตามที่ระบุในแบบประเมิน (ด้านล่าง) พร้อมระบุสถานะปัจจุบันของหน่วยงานว่า “มี” หรือ “ไม่มี”

๒. หาก “มี” โปรดระบุสิ่งที่หน่วยงานของท่านได้ปฏิบัติแล้ว

๓. หาก “ไม่มี” โปรดระบุสิ่งที่ท่านคิดว่า หน่วยงานของท่านควรปฏิบัติ

๔. บันทึกสิ่งที่ได้ปฏิบัติแล้ว หรือสิ่งที่ควรต้องปฏิบัติเพิ่มเติมในช่อง “กระบวนงานที่ต้องปฏิบัติ”

๕. หากมีแนวปฏิบัติอื่น ๆ เพิ่มเติม นอกเหนือจากแบบประเมิน หน่วยงานสามารถระบุเพิ่มได้ตามความจำเป็น และความเหมาะสม

<u>การรวบรวมและจัดทำแนวปฏิบัติที่เหมาะสม</u>

หลังจากทำการประเมินสถานภาพการดำเนินงานด้านสารสนเทศ หน่วยงานสามารถนำประเด็นด้านเทคโนโลยีสารสนเทศมาเรียบเรียงเป็นเอกสาร “นโยบายและแนวปฏิบัติในการรักษาความปลอดภัยด้านสารสนเทศของหน่วยงาน” โดยมีข้อแนะนำดังนี้

๑. พิจารณาคัดแยกประเด็นด้านเทคโนโลยีสารสนเทศ ในส่วนที่เป็น “นโยบาย” และ “ส่วนที่เป็น “แนวปฏิบัติ”

๒. นำประเด็นด้านเทคโนโลยีสารสนเทศ ในส่วนที่เป็น “นโยบาย” บรรจุในเอกสาร “ประกาศนโยบาย” โดยให้สอดคล้องกับ “ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ” ข้อ ๒ ข้อ ๓ และ ข้อ ๑๔

๓. นำประเด็นด้านเทคโนโลยีสารสนเทศ ในส่วนที่เป็น “แนวปฏิบัติ” มาคัดแยกภายใต้หัวข้อที่สอดคล้องกับ “ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ” ข้อ ๕ – ๑๓

แบบประเมินสถานภาพการดำเนินงานด้านสารสนเทศ

หน่วยงาน..... ณ วันที่.....

ลำดับ	ประเด็นด้านเทคโนโลยีสารสนเทศ (ระบุว่ามีการดำเนินงานในเรื่องเหล่านี้หรือไม่)	สถานะปัจจุบัน		กระบวนงานที่ต้องปฏิบัติ	หมายเหตุ
		มี	ไม่มี		
๑.	**นโยบายความมั่นคงปลอดภัยด้านสารสนเทศ**				
	- มีเอกสารนโยบายในการรักษาความมั่นคงปลอดภัย อย่างเป็นลายลักษณ์อักษร			ระบุรูปแบบเอกสาร	
	- มีการประกาศใช้นโยบายในการรักษาความมั่นคงปลอดภัย			ระบุวิธีการประกาศ ระบุผู้มีอำนาจในการประกาศ	
	- มีการกำหนดหลักการ วัตถุประสงค์ และเป้าหมาย รวมทั้งข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยอย่างชัดเจน			ระบุหัวข้อสำคัญที่ปรากฏ	
	- มีการกำหนดความหมายของคำว่า “การรักษาความมั่นคงปลอดภัยสำหรับสารสนเทศ” (Information security) ที่ชัดเจน			ระบุความหมาย และความครอบคลุม	
	- มีผู้บริหารระดับสูงให้การสนับสนุนการดำเนินงานด้านเทคโนโลยีสารสนเทศ ในเชิงนโยบาย และการปฏิบัติ			ระบุผู้บริหารระดับสูงที่เกี่ยวข้อง	
	- มีเนื้อหาครอบคลุมการเข้าถึงหรือควบคุมการใช้งานสารสนเทศ			ระบุหัวข้อที่ควบคุมการเข้าถึง	
	- มีเนื้อหาครอบคลุมการจัดทำระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งาน			ระบุหัวข้อหลักที่เกี่ยวข้อง	
	- มีเนื้อหาครอบคลุมการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์			ระบุหัวข้อหลักที่เกี่ยวข้อง	
	- มีข้อกำหนดให้ทำการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ			ระบุข้อกำหนดเกี่ยวกับผู้ตรวจ และความถี่ในการดำเนินงาน	
	- มีรอบความถี่ในการทบทวนนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างสม่ำเสมอ			ระบุความถี่	
	- มีการกำหนดหน้าที่และความรับผิดชอบเกี่ยวกับการจัดทำนโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ รวมทั้งการทบทวน และการปรับปรุงแก้ไข			ระบุผู้รับผิดชอบ	
	- มีการกำหนดหน้าที่และความรับผิดชอบในการปฏิบัติ และการบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ			ระบุผู้เกี่ยวข้องทั้งในฐานะผู้ปฏิบัติ และผู้ใช้งาน	
	- มีการกำหนดหน้าที่และความรับผิดชอบเกี่ยวกับการรายงานเหตุการณ์ที่เสี่ยงต่อความมั่นคงปลอดภัยที่เกิดขึ้น			ระบุผู้เกี่ยวข้อง	
	- มีการอธิบาย ให้ความรู้และทำความเข้าใจเกี่ยวกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยกับบุคลากรในองค์กร			ระบุวิธีการ	
๒.	**การเข้าถึงข้อมูลและควบคุมการใช้งานสารสนเทศ**				
	- มีการควบคุมการเข้าถึงข้อมูล			ระบุประเด็นที่ควบคุม	
	- มีการควบคุมการเข้าถึงอุปกรณ์ในการประมวลผลข้อมูล			ระบุ สิทธิ การมอบอำนาจ การเข้า-ออก	

ลำดับ	ประเด็นด้านเทคโนโลยีสารสนเทศ (ระบุว่ามีการดำเนินงานในเรื่องเหล่านี้หรือไม่)	สถานะปัจจุบัน		กระบวนงานที่ต้องปฏิบัติ	หมายเหตุ
		มี	ไม่มี		
				พื้นที่ปฏิบัติงาน และอื่น ๆ	
	- มีแนวปฏิบัติในการอนุญาต ให้เข้าถึงระบบสารสนเทศ			ระบุหัวข้อสำคัญที่ปรากฏ	
	- มีแนวปฏิบัติในการกำหนดสิทธิ ให้เข้าถึงระบบสารสนเทศ			ระบุหัวข้อสำคัญที่ปรากฏ	
	- มีแนวปฏิบัติในการมอบอำนาจของหน่วยงานให้เข้าถึงระบบสารสนเทศ			ระบุหัวข้อสำคัญที่ปรากฏ	
	- มีการกำหนดประเภทของข้อมูล			ระบุกลุ่มข้อมูลที่มีภายในองค์กร เช่น การเงิน บุคลากร นโยบาย หรือผู้รับบริการ ฯลฯ	
	- มีการกำหนดลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูลแต่ละประเภท			ระบุข้อกำหนด	
	- มีการกำหนดระดับชั้นการเข้าถึงข้อมูลแต่ละประเภท			ระบุข้อกำหนด	
	- มีการกำหนดเวลาที่เข้าถึงได้			ระบุข้อกำหนด	
	- มีการกำหนดช่องทางที่เข้าถึง			ระบุข้อกำหนด	
	- มีข้อกำหนดให้นำการเข้ารหัสมาใช้กับข้อมูลที่สำคัญหรือข้อมูลลับแต่ละประเภท			ระบุข้อกำหนด	
	- มีการจัดทำข้อตกลงการรักษาความลับระหว่างหน่วยงานกับผู้ที่ได้รับการว่าจ้างหรือผู้ที่จำเป็นต้องเข้าถึงข้อมูล			ระบุข้อกำหนด	
๓.	**ข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ**				
	- มีข้อกำหนดการใช้งานตามภารกิจ			ระบุการตรวจสอบสิทธิและการอนุมัติให้กับผู้ใช้งาน	
	- มีข้อกำหนดด้านความมั่นคงปลอดภัย สำหรับแต่ละภารกิจ			ระบุเกณฑ์ที่เกี่ยวกับการตรวจสอบสิทธิและการอนุมัติให้กับผู้ใช้งาน	
๔.	**การบริหารจัดการการเข้าถึงและการใช้งานระบบสารสนเทศ**				
	- มีการสร้างความรู้ความเข้าใจกับผู้ใช้งาน เพื่อให้เกิดความตระหนักความเข้าใจถึงภัยและผลกระทบที่เกิดขึ้นจากการใช้ระบบสารสนเทศโดยไม่ระมัดระวัง			ระบุวิธีการ	
	- มีมาตรการเชิงป้องกันภัยและผลกระทบที่เกิดขึ้นจากการใช้ระบบสารสนเทศโดยไม่ระมัดระวังตามความเหมาะสม			ระบุมาตรการป้องกัน	
	- มีขั้นตอนปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานก่อนการอนุญาตให้เข้าถึง			ระบุขั้นตอนทางปฏิบัติ	
	- มีการตัดผู้ใช้งานออกจากทะเบียนเมื่อมีการเพิกถอนสิทธิ			ระบุกรณีที่มีการเพิกถอน	
	- มีการควบคุมและจำกัดสิทธิผู้ใช้งานเพื่อเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิด			ระบุการควบคุมและจำกัดสิทธิ	
	- มีการควบคุมและจำกัดสิทธิสำหรับสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่น ๆ ที่เกี่ยวข้องกับการเข้าถึง			ระบุการควบคุมและจำกัดสิทธิ	
	- มีข้อจำกัดไม่ให้ผู้ดูแลระบบใช้บัญชีผู้ใช้งานที่มีสิทธิในระดับสูง ในการปฏิบัติงานทั่วไป				

ลำดับ	ประเด็นด้านเทคโนโลยีสารสนเทศ (ระบุว่ามีการดำเนินงานในเรื่องเหล่านี้หรือไม่)	สถานะปัจจุบัน		กระบวนงานที่ต้องปฏิบัติ	หมายเหตุ
		มี	ไม่มี		
	- มีข้อมูลพื้นฐานที่ใช้ประกอบการควบคุมและจำกัดสิทธิสำหรับผู้ใช้งาน			ระบุหัวข้อ	
	- มีระยะเวลาการใช้งานของแต่ละสิทธิแตกต่างกัน			ระบุระยะเวลาที่แตกต่าง	
	- มีการเพิกถอนหรือระงับการใช้งานของแต่ละสิทธิแตกต่างกัน			ระบุการเพิกถอน	
	- มีการเปลี่ยนแปลงสิทธิการใช้งานระบบสารสนเทศ			ระบุกรณีที่มีการเปลี่ยนแปลงสิทธิ	
	- มีกระบวนการทบทวนสิทธิของผู้ใช้งาน			ระบุประเด็นทบทวน	
	- มีความถี่ในการทบทวนสิทธิของผู้ใช้งาน			ระบุรอบความถี่	
	- มีการตรวจสอบ ติดตามการใช้งานตามสิทธิที่ได้รับ			ระบุกระบวนการ	
๕.	**การบริหารจัดการรหัสผ่าน**				
	- มีกระบวนการจัดสรร หรือแจกจ่ายรหัสผ่านให้กับผู้ใช้งานอย่างรัดกุม			ระบุกระบวนการ	
	- มีข้อกำหนดให้ผู้ใช้งานเปลี่ยนรหัสผ่านหลังจากได้รับรหัสผ่านชั่วคราว			ระบุแนวปฏิบัติ	
	- มีแนวปฏิบัติสำหรับการตั้งหรือเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย			ระบุแนวปฏิบัติ	
	- มีคุณสมบัติพื้นฐานสำหรับรหัสผ่านที่ดี			ระบุคุณสมบัติพื้นฐาน	
	- มีระบบบริหารจัดการรหัสผ่าน ที่มีปฏิสัมพันธ์โต้ตอบกับผู้ใช้งาน			ระบุแนวปฏิบัติ	
	- มีการอนุญาตให้ผู้ใช้งานสามารถเปลี่ยนรหัสผ่านได้ด้วยตนเอง				
	- มีการจัดเก็บรหัสผ่านเดิมไว้เพื่อป้องกันการกลับไปใช้รหัสผ่านเดิมที่ได้เคยตั้งไปแล้ว				
	- มีการจัดเก็บไฟล์ข้อมูลรหัสผ่านของผู้ใช้งานแยกต่างหากจากข้อมูลของระบบงาน				
	- มีการเข้ารหัสข้อมูลกรณีที่ต้องมีการส่งรหัสผ่านไปในเครือข่าย				
๖	**การใช้งานรหัสผ่าน**				
	- มีรอบระยะเวลาการเปลี่ยนรหัสผ่านเพื่อความมั่นคงปลอดภัย				
	- มีข้อกำหนดให้ผู้ใช้งานยืนยันรหัสผ่านใหม่ที่ตั้งอีกครั้ง				
	- มีข้อระวังการใช้งานรหัสผ่านที่ปลอดภัย			ระบุข้อระวัง	
	- มีการเข้ารหัสข้อมูลป้องกันข้อมูลรหัสผ่านที่ได้มีการจัดเก็บไว้ในระบบ				
๗.	**การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์**				
	- มีการป้องกันอุปกรณ์หลังจากเลิกใช้งาน			ระบุแนวปฏิบัติ	
	- มีการป้องกันอุปกรณ์กรณีพักการใช้งานชั่วคราว			ระบุแนวปฏิบัติ	
	- มีการควบคุมการเข้า-ออกพื้นที่			ระบุแนวปฏิบัติ	
	- มีข้อกำหนดให้ผู้ใช้งานดูแล รักษา และป้องกันทรัพย์สินสารสนเทศที่เกี่ยวข้อง			ระบุข้อกำหนด	
๘.	**การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ ที่อยู่ในภาวะซึ่งเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ**				
	- มีการควบคุมเอกสาร			ระบุแนวปฏิบัติ	
	- มีการควบคุมสื่อบันทึกข้อมูล และแฟ้มข้อมูล			ระบุแนวปฏิบัติ	
	- มีการควบคุมเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง			ระบุแนวปฏิบัติ	
	- มีขั้นตอนปฏิบัติในการนำเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงออก			ระบุแนวปฏิบัติ	

ลำดับ	ประเด็นด้านเทคโนโลยีสารสนเทศ (ระบุว่ามีการดำเนินงานในเรื่องเหล่านี้หรือไม่)	สถานะปัจจุบัน		กระบวนงานที่ต้องปฏิบัติ	หมายเหตุ
		มี	ไม่มี		
	นอกสถานที่				
	- มีการควบคุมระบบสารสนเทศและข้อมูลสารสนเทศ			ระบุแนวปฏิบัติ	
	- มีการทำลาย เอกสาร สื่อบันทึกข้อมูล และแฟ้มข้อมูล เพื่อป้องกันการกู้คืน			ระบุแนวปฏิบัติ	
	- มีการควบคุมการเข้า-ออกพื้นที่			ระบุแนวปฏิบัติ	
	- มีข้อกำหนดให้ผู้ใช้งานดูแล รักษา และป้องกันทรัพย์สินสารสนเทศที่เกี่ยวข้อง			ระบุข้อกำหนด	
๙.	**การเข้ารหัส สำหรับข้อมูลที่เป็นความลับ**				
	- มีการนำวิธีการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ			ระบุแนวปฏิบัติ	
	- มีการแสดงชั้นความลับบนไฟล์ข้อมูลลับ			ระบุแนวปฏิบัติ	
	- มีการป้องกันไฟล์ข้อมูลลับที่จัดเก็บไว้ในเครื่องคอมพิวเตอร์			ระบุแนวปฏิบัติ	
	- มีการป้องกันสื่อบันทึกข้อมูลลับ			ระบุแนวปฏิบัติ	
	- มีการทำลายสื่อบันทึกข้อมูลลับ และแฟ้มข้อมูลลับ เพื่อป้องกันการกู้คืน			ระบุแนวปฏิบัติ	
๑๐	**การเข้าถึงระบบเครือข่าย**				
	- มีการแบ่งแยกเครือข่าย			ระบุการแยกประเภทเครือข่าย	
	- มีการจัดทำผังเครือข่าย			ระบุขอบเขตของเครือข่าย	
	- มีแนวปฏิบัติในการควบคุมให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น			ระบุข้อห้ามในการใช้งานระบบเครือข่าย	
	- มีการควบคุมการเข้าถึงทางกายภาพต่อเครือข่ายย่อยเพื่อป้องกันการเข้าถึงทางกายภาพต่อเครือข่ายย่อยและทำการเปลี่ยนแปลงแก้ไขสายสัญญาณ ดักแอบดูข้อมูลบนเครือข่าย หรืออื่นๆ โดยไม่ได้รับอนุญาต				
	- มีการจัดทำบัญชีผู้ใช้งานและสิทธิในการเข้าถึงบริการเครือข่ายต่างๆ				
๑๑.	**การยืนยันตัวบุคคล**				
	- มีการจัดเก็บข้อมูลพื้นฐานสำหรับบุคคลที่เข้าใช้งานระบบเครือข่ายทั้งผู้ใช้ที่อยู่ภายในองค์กรและผู้ใช้ที่อยู่ภายนอกองค์กร			ระบุข้อมูลที่จัดเก็บ	
	- มีการยืนยันตัวบุคคล สำหรับผู้ใช้ที่อยู่ภายในองค์กร			ระบุข้อมูลที่ใช้ในการยืนยัน	
	- มีการยืนยันตัวบุคคล สำหรับผู้ใช้ที่อยู่ภายนอกองค์กร			ระบุข้อมูลที่ใช้ในการยืนยัน	
	- มีวิธีการเชื่อมผ่านเข้าสู่ระบบเครือข่ายสำหรับผู้ใช้ที่อยู่ภายในองค์กร			ระบุวิธีการเชื่อมเข้าสู่ระบบ	
	- มีวิธีการเชื่อมผ่านเข้าสู่ระบบเครือข่ายสำหรับผู้ใช้ที่อยู่ภายนอกองค์กร			ระบุวิธีการเชื่อมเข้าสู่ระบบ	
	- มีการเก็บข้อมูลอุปกรณ์บนเครือข่าย			ระบุข้อมูลที่จัดเก็บ	
	- มีวิธีการระบุอุปกรณ์บนเครือข่าย			ระบุวิธีการ	
๑๒	**การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ**				
	- มีการป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ			ระบุแนวปฏิบัติ	

ลำดับ	ประเด็นด้านเทคโนโลยีสารสนเทศ (ระบุว่ามีการดำเนินงานในเรื่องเหล่านี้หรือไม่)	สถานะปัจจุบัน		กระบวนงานที่ต้องปฏิบัติ	หมายเหตุ
		มี	ไม่มี		
	- มีการรักษาความมั่นคงปลอดภัยทางกายภาพสำหรับอุปกรณ์คอมพิวเตอร์หรือเครือข่าย เพื่อป้องกันการเปลี่ยนแปลงแก้ไขหมายเลขระบุอุปกรณ์เหล่านั้น			ระบุความถี่ในการตรวจสอบ	
	- มีการตรวจสอบและปิดพอร์ต (Port) ของระบบหรืออุปกรณ์ที่ไม่มีความจำเป็นในการใช้งาน				
	- มีการกำหนดสิทธิบุคคลในการเข้า-ออกห้องเครื่องโดยเฉพาะบุคคลที่ปฏิบัติหน้าที่เกี่ยวข้องภายใน				
	- มีการบันทึก “ทะเบียนผู้มีสิทธิเข้า-ออกพื้นที่”				
	- มีข้อห้ามในการเข้า-ออก พื้นที่ห้องคอมพิวเตอร์แม่ข่าย				
๑๓	**การควบคุมการเชื่อมต่อทางเครือข่าย**				
	- มีอุปกรณ์ป้องกันการบุกรุก ซึ่งมีความสามารถในการตรวจจับโปรแกรมไม่ประสงค์ดี				
	- มีการป้องกันเลขที่อยู่ไอพี (IP Address) ภายในของระบบเครือข่ายมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้				
	- มีการบันทึกการทำงานของระบบเครือข่าย บันทึกการปฏิบัติงานของผู้ใช้บริการ บันทึกการบุกรุก บันทึกการเข้าออกระบบ บันทึกการใช้งาน และข้อมูลจราจรคอมพิวเตอร์				
	- มีการจำกัดการเชื่อมต่อทางเครือข่ายของผู้ใช้งานต่อระบบงานสำหรับการโอนย้ายไฟล์				
	- มีการจำกัดการเชื่อมต่อทางเครือข่ายของผู้ใช้งานต่อระบบงานสำหรับใช้งานภายในองค์กร				
	- มีการจำกัดการเชื่อมต่อการใช้งานอินเทอร์เน็ตและระบบงานต่างๆ				
	- มีการจำกัดการเชื่อมต่อทางเครือข่ายของผู้ใช้งานตามวันที่ เวลา หรือช่วงเวลาที่อนุญาตให้ใช้งาน				
๑๔	**การควบคุมการจัดเส้นทางบนเครือข่าย**				
	- มีอุปกรณ์เครือข่ายควบคุมการเชื่อมต่อทางเครือข่าย				
	- มีการปรับปรุงบัญชีผู้ใช้งานและสิทธิในการเข้าถึงบริการเครือข่ายต่างๆ				
	- มีเกตเวย์ เพื่อกรองข้อมูลที่ไหลเวียนในเครือข่าย				
	- มีการตรวจสอบไอพีแอดเดรสของทั้งต้นทางและปลายทาง				
	- มีการควบคุมการไหลของข้อมูลผ่านเครือข่าย				
	- มีการกำหนดเส้นทางการไหลของข้อมูลบนเครือข่ายที่สอดคล้องกับการควบคุมการเข้าถึงและการใช้งานบริการเครือข่าย				
	- มีการจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องแม่ข่าย เพื่อไม่อนุญาตให้ผู้ใช้บริการสามารถใช้เส้นทางอื่นๆ				
๑๕	**การเข้าถึงระบบปฏิบัติการ**				
	- มีขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย				
	- มีบัญชีผู้ใช้งานซึ่งแยกกันของแต่ละบุคคลที่ใช้พิสูจน์ตัวตน				
	- มีการตั้งชื่อบัญชีผู้ใช้งานในระบบงานให้แตกต่างกัน				
	- มีการพิสูจน์ตัวตนผู้ใช้งานก่อนเข้าใช้ระบบปฏิบัติการ				

ลำดับ	ประเด็นด้านเทคโนโลยีสารสนเทศ (ระบุว่ามีการดำเนินงานในเรื่องเหล่านี้หรือไม่)	สถานะปัจจุบัน		กระบวนงานที่ต้องปฏิบัติ	หมายเหตุ
		มี	ไม่มี		
	- มีการอนุมัติการใช้งานบัญชีผู้ใช้งานแบบกลุ่มอย่างเป็นลายลักษณ์อักษร				
	- มีการกำหนดลักษณะงานหรือกิจกรรมเฉพาะที่อนุญาตให้ใช้บัญชีแบบกลุ่ม				
	- มีมาตรการควบคุมและจำกัดการใช้บัญชีผู้ใช้งานแบบกลุ่ม				
	- มีมาตรการควบคุมการปฏิเสธความรับผิดชอบในการใช้บัญชีแบบกลุ่ม				
	- มีการใช้วิธีการทางเทคนิคสำหรับการพิสูจน์ตัวตนที่มีความมั่นคงปลอดภัยสูงกับระบบงานที่มีความสำคัญสูง				
	- มีข้อจำกัดหรือควบคุมในการใช้งานโปรแกรมยูทิลิตี้				
	- มีการป้องกันการละเมิดลิขสิทธิ์ในการใช้งานโปรแกรมยูทิลิตี้				
	- มีขั้นตอนปฏิบัติสำหรับการขออนุมัติการใช้งานโปรแกรมยูทิลิตี้ ตามระดับสิทธิ ในการใช้งาน				
	- มีการแยกจัดเก็บโปรแกรมยูทิลิตี้ออกจากซอฟต์แวร์สำหรับระบบงาน				
	- มีการจำกัดจำนวนผู้ที่สามารถใช้งานโปรแกรมยูทิลิตี้ และไม่อนุญาตให้ผู้ใช้งานทั่วไปสามารถใช้งานได้				
	- มีการบันทึกข้อมูลล็อกแสดงการใช้งานโปรแกรมยูทิลิตี้				
	- มีการควบคุมหรือยกเลิกหรือลบทิ้งโปรแกรมยูทิลิตี้ที่ไม่มีความจำเป็นในการใช้งาน				
	- มีการตัดการใช้งานของผู้ใช้งานออกจากระบบ หลังจากที่ไม่ได้ใช้งานเกินกว่าระยะเวลาหนึ่งที่ได้กำหนดไว้				
	- มีการจำกัดระยะเวลาเชื่อมต่อระบบสารสนเทศ เพื่อให้สามารถใช้งานได้เพียงช่วงเวลาหนึ่งที่ได้กำหนดไว้				
	- มีการตัดและหมดเวลาการใช้งานในระยะเวลาที่สั้นขึ้นสำหรับระบบเทคโนโลยีสารสนเทศที่มีความเสี่ยงสูง หรือมีการใช้งานในสถานที่ที่มีความเสี่ยง				
	- มีการพิสูจน์ตัวตนเพื่อเข้าใช้งานระบบเทคโนโลยีสารสนเทศอีกครั้งหลังจากที่ระบบได้ตัดการใช้งานนั้นไปแล้ว				
๑๖.	**การเข้าถึงระบบสารสนเทศและโปรแกรมประยุกต์**				
	- มีข้อจำกัดหรือควบคุมผู้ใช้งานในการเข้าถึงสารสนเทศและฟังก์ชัน (functions) ต่างๆ				
	- มีข้อจำกัดหรือควบคุมบุคลากรฝ่ายสนับสนุนในการเข้าถึงสารสนเทศและฟังก์ชัน (functions) ต่างๆ				
	- มีการลงทะเบียนผู้ใช้งานเพื่อควบคุม จำกัด หรือให้สิทธิการเข้าถึงข้อมูลและฟังก์ชันต่างๆ ของระบบงาน				
	- มีการควบคุมหรือจำกัดสิทธิการเข้าถึงระบบงานซึ่งถูกเข้าถึงจากอีกระบบงานหนึ่ง				
	- มีการควบคุมให้สามารถเข้าถึงได้เฉพาะข้อมูลและฟังก์ชันต่างๆ ที่จำเป็นต้องใช้งาน				
	- มีการควบคุมหรือจำกัดการนำข้อมูลออกจากระบบงานหนึ่ง เฉพาะที่เกี่ยวข้องและจำเป็นสำหรับการนำไปใช้งาน				

ลำดับ	ประเด็นด้านเทคโนโลยีสารสนเทศ (ระบุว่ามีการดำเนินงานในเรื่องเหล่านี้หรือไม่)	สถานะปัจจุบัน		กระบวนงานที่ต้องปฏิบัติ	หมายเหตุ
		มี	ไม่มี		
	- มีการแสดงเฉพาะข้อมูลพื้นฐานเพื่อให้ผู้ใช้งานได้รับทราบที่จำเป็นเท่านั้น				
	- มีการแสดงรายละเอียดเท่าที่จำเป็นของระบบงาน หลังจากที่ล็อกอินเสร็จแล้ว				
	- มีข้อความแสดงเตือนห้ามผู้ไม่มีสิทธิเข้าถึงระบบงาน				
	- มีข้อจำกัดไม่ให้ระบบแสดงความช่วยเหลือใดๆ กรณีมีเหตุการณ์ไม่พึงประสงค์เกิดขึ้นกับระบบ				
	- มีการตรวจสอบข้อมูลการล็อกอินหลังจากที่ผู้ใช้งานใส่ข้อมูลทั้งหมดครบถ้วนแล้ว				
	- มีข้อจำกัดไม่ให้ระบบแสดงข้อความผิดพลาดจากการทำงานหรือการใช้งานในลักษณะที่เปิดเผยข้อมูลภายในของระบบงาน				
	- มีการจำกัดจำนวนครั้งที่ผู้ใช้งานสามารถใส่ข้อมูลการล็อกอินผิด				
	- มีการกำหนดการหน่วงระยะเวลาที่ผู้ใช้งานสามารถเชื่อมโยงกลับเข้ามายังระบบงานได้ภายหลังจากที่ใส่ข้อมูลการล็อกอินผิดเกินกว่าจำนวนครั้งที่กำหนด				
	- มีการส่งข้อความเตือนไปยังผู้ดูแลระบบให้ทราบว่ามีผู้ใช้งานพยายามล็อกอินแต่ผิดพลาดเป็นจำนวนหลายครั้ง				
	- มีการบันทึกข้อมูลการล็อกอินทั้งที่สำเร็จและไม่สำเร็จ			ระบุข้อมูลที่บันทึก	
	- มีการจำกัดช่วงระยะเวลาที่นานที่สุดที่ให้ผู้ใช้งานจะต้องล็อกอินเข้าใช้งานให้สำเร็จ				
	- มีการแสดงวัน/เวลาที่ล็อกอินครั้งที่แล้ว (ทั้งที่สำเร็จและไม่สำเร็จ)				
๑๗.	**ระบบที่ไวต่อการรบกวน**				
	- มีระบบที่มีผลกระทบและมีความสำคัญสูงต่อองค์กร				
	- มีการแยกระบบที่ไวต่อการรบกวน ออกจากระบบอื่น ๆ				
	- มีการประเมินความเสี่ยงสำหรับการใช้งานทรัพยากรร่วมกันระหว่างระบบงานที่มีความสำคัญสูงกับระบบงานอื่นๆ ที่มีความสำคัญน้อยกว่า				
	- มีการควบคุมสภาพแวดล้อมของระบบที่ไวต่อการรบกวน โดยเฉพาะ				
	- มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ สำหรับระบบที่ไวต่อการรบกวน				
	- มีการปฏิบัติงาน สำหรับระบบที่ไวต่อการรบกวน จากภายนอกองค์กร				
๑๘.	**การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่**				
	- มีการปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่				
	- มีการควบคุมหน่วยงานภายนอกที่นำอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานภายในหน่วยงานมาปฏิบัติงานที่ห้องเครื่อง				
	- มีการลงบันทึกรายการอุปกรณ์ เพื่อขออนุญาตเข้า-ออกพื้นที่				
	- มีการจัดทำแผนผังแสดงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร				

ลำดับ	ประเด็นด้านเทคโนโลยีสารสนเทศ (ระบุว่ามีการดำเนินงานในเรื่องเหล่านี้หรือไม่)	สถานะปัจจุบัน		กระบวนงานที่ต้องปฏิบัติ	หมายเหตุ
		มี	ไม่มี		
	- มีข้อปฏิบัติสำหรับการใช้งานอุปกรณ์คอมพิวเตอร์ประเภทพกพา				
	- มีการวิเคราะห์และประเมินความเสี่ยงลักษณะการใช้งานอุปกรณ์คอมพิวเตอร์ประเภทพกพาของหน่วยงาน				
	- มีการสร้างความตระหนักเพื่อให้พนักงานระมัดระวังและป้องกันการใช้อุปกรณ์คอมพิวเตอร์ประเภทพกพา				
	- มีการควบคุมการเชื่อมต่ออุปกรณ์คอมพิวเตอร์ประเภทพกพา ผ่านทางเครือข่ายสาธารณะภายนอกหน่วยงาน				
	- มีการป้องกันข้อมูลที่จัดเก็บไว้ในอุปกรณ์คอมพิวเตอร์ประเภทพกพาจากการถูกเข้าถึงโดยไม่ได้รับอนุญาต				
	- มีการสำรองข้อมูลสำคัญที่อยู่ในอุปกรณ์คอมพิวเตอร์ประเภทพกพาอย่างสม่ำเสมอ				
	- มีการจัดเตรียมอุปกรณ์ที่สามารถใช้ทำการสำรองข้อมูลออกมาจากอุปกรณ์คอมพิวเตอร์ประเภทพกพา				
	- มีการป้องกันข้อมูลที่ได้สำรองเก็บไว้ของอุปกรณ์คอมพิวเตอร์ประเภทพกพา				
	- มีการพิสูจน์ตัวตนสำหรับการเข้าถึงระบบงานจากระยะไกลโดยผ่านทางอุปกรณ์คอมพิวเตอร์ประเภทพกพา				
	- มีการป้องกันอุปกรณ์คอมพิวเตอร์ประเภทพกพาจากการถูกขโมยหรือสูญหาย				
	- มีการป้องกันอุปกรณ์คอมพิวเตอร์ประเภทพกพาสำหรับกรณีที่ต้องปล่อยอุปกรณ์นั้นทิ้งไว้โดยไม่มีผู้ดูแล				
	- มีการจัดการกับโปรแกรมไม่พึงประสงค์ในอุปกรณ์คอมพิวเตอร์ประเภทพกพา				
	- มีกระบวนการจัดการกรณีที่อุปกรณ์คอมพิวเตอร์ประเภทพกพาเกิดการสูญหายหรือถูกขโมย				
๑๙.	**การปฏิบัติงานจากภายนอกสำนักงาน (teleworking)**				
	- มีข้อปฏิบัติ แผนงาน และขั้นตอนปฏิบัติสำหรับการปฏิบัติงานจากภายนอกสำนักงาน				
	- มีการระบุชนิดของงานที่อนุญาตและไม่อนุญาตสำหรับการปฏิบัติงานจากระยะไกล				
	- มีขั้นตอนปฏิบัติในการขออนุมัติสำหรับการปฏิบัติงานจากภายนอกสำนักงาน				
	- มีขั้นตอนปฏิบัติในการยกเลิกสำหรับการปฏิบัติงานจากภายนอกสำนักงาน				
	- มีการจำกัดระยะเวลาการเข้าถึง สำหรับการปฏิบัติงานจากภายนอกสำนักงาน				
	- มีการพิสูจน์ตัวตนก่อนเข้าใช้งาน สำหรับการปฏิบัติงานจากภายนอกสำนักงาน				
	- มีการป้องกันการเปิดเผยข้อมูล และการเข้าถึงข้อมูลที่ไม่ได้รับอนุญาต สำหรับการปฏิบัติงานจากภายนอกสำนักงาน				

ลำดับ	ประเด็นด้านเทคโนโลยีสารสนเทศ (ระบุว่ามีการดำเนินงานในเรื่องเหล่านี้หรือไม่)	สถานะปัจจุบัน		กระบวนงานที่ต้องปฏิบัติ	หมายเหตุ
		มี	ไม่มี		
	- มีการจัดระดับความสำคัญของข้อมูลที่จะมีการรับส่งหรือสื่อสารกันสำหรับการปฏิบัติงานจากภายนอกสำนักงาน				
	- มีข้อกำหนดไม่อนุญาตให้ครอบครัวหรือเพื่อนเข้าถึงระบบเทคโนโลยีสารสนเทศและข้อมูลสำหรับการปฏิบัติงานจากภายนอกสำนักงาน				
	- มีการบำรุงรักษาและให้บริการสนับสนุนสำหรับซอฟต์แวร์และฮาร์ดแวร์ต่างๆ ที่ใช้งานจากระยะไกล				
	- มีการควบคุมสำหรับการใช้งานเครือข่ายจากที่บ้าน				
	- มีการป้องกันทรัพย์สินทางปัญญาที่เกิดขึ้นจากการปฏิบัติงานจากระยะไกล				
	- มีการจัดเตรียมอุปกรณ์ที่จำเป็นสำหรับการปฏิบัติงานจากระยะไกล ซึ่ง รวมถึงอุปกรณ์สำหรับการจัดเก็บข้อมูล และอุปกรณ์สื่อสาร				
	- มีข้อจำกัดไม่อนุญาตให้ใช้งานอุปกรณ์ที่เป็นของส่วนตัวเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศจากระยะไกล ถ้าอุปกรณ์ดังกล่าวไม่อยู่ภายใต้การควบคุมหรือดูแล				
	- มีการตรวจสอบความมั่นคงปลอดภัยของสถานที่ที่จะมีการปฏิบัติงานจากระยะไกล				
๒๐.	**การจัดทำระบบสำรอง**				
	- มีกระบวนการคัดเลือกและจัดทำระบบสำรองให้อยู่ในสภาพพร้อมใช้				
	- มีผู้รับผิดชอบในการคัดเลือกและจัดทำระบบสำรองให้อยู่ในสภาพพร้อมใช้				
	- มีขั้นตอนปฏิบัติสำหรับการสำรองข้อมูลที่ชัดเจน				
	- มีการกำหนดข้อมูลที่ต้องทำการสำรองเก็บไว้				
	- มีความถี่ในการสำรอง ที่สอดคล้องกับระยะเวลาที่ยอมรับได้หากข้อมูลนั้นจะไม่ได้รับการปรับปรุงให้เป็นข้อมูลล่าสุด				
	- มีผู้รับผิดชอบในการสำรองข้อมูล				
	- มีการจัดเก็บข้อมูลที่สำรองไว้นอกสถานที่				
	- มีมาตรการป้องกันทางกายภาพต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูลนอกสถานที่ เหมือนกับมาตรการที่ใช้กับหน่วยงานหลัก (Main site)				
	- มีการบันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล				
	- มีการจัดทำบันทึกการสำรองข้อมูล (Operator logs)				
	- มีการรายงานข้อผิดพลาด (Fault logging) บันทึกข้อผิดพลาดที่เกิดขึ้น				
	- มีการเข้ารหัสข้อมูลสำคัญในการสำรองข้อมูล (Encrypted backup)				
	- มีการใช้เทคโนโลยีการเข้ารหัส เพื่อป้องกันมิให้ข้อมูลสำรองถูกเปิดเผย				
๒๑.	**การจัดทำแผนเตรียมความพร้อมฉุกเฉิน**				
	- มีแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์				
	- มีการปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉิน ให้สามารถปรับใช้ได้อย่างสอดคล้องกับภารกิจ				

ลำดับ	ประเด็นด้านเทคโนโลยีสารสนเทศ (ระบุว่ามีการดำเนินงานในเรื่องเหล่านี้หรือไม่)	สถานะปัจจุบัน		กระบวนงานที่ต้องปฏิบัติ	หมายเหตุ
		มี	ไม่มี		
	- มีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศที่เพียงพอ				
	- มีการตรวจสอบหรือทดสอบระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ				
	- มีการใช้ระบบสำรองเพื่อป้องกันอุปกรณ์ไฟฟ้าเสียหายจากความไม่สม่ำเสมอของกระแสไฟฟ้า				
	- มีการจัดทำแผนฉุกเฉินสำหรับระบบกระแสไฟฟ้า เช่น ในกรณีที่ระบบกระแสไฟฟ้าเกิดการล้มเหลวหรือดับ				
	- มีการจัดหาเครื่องกำเนิดกระแสไฟฟ้าสำรองเพื่อจ่ายไฟสำรองให้ในกรณีที่กระแสไฟฟ้าหลักเกิดการหยุดชะงักหรือดับเป็นระยะเวลายาวนาน				
	- มีการจัดเตรียมเชื้อเพลิงสำรองเพียงพอสำหรับเครื่องกำเนิดกระแสไฟฟ้าสำรองในช่วงเกิดเหตุฉุกเฉิน				
	- มีแหล่งจ่ายกระแสไฟฟ้ามากกว่าหนึ่งแหล่ง เพื่อสนับสนุนกระบวนการทำงานของระบบสารสนเทศที่สำคัญ				
	- มีการจัดทำสวิตช์ฉุกเฉินไว้ใกล้กับบริเวณทางออกของห้องเครื่องเพื่อให้สามารถปิดสวิตช์ดับอุปกรณ์ทั้งหมดได้โดยทันทีทันใดและอย่างรวดเร็ว				
	- มีการจัดทำระบบไฟส่องสว่างฉุกเฉินเพื่อรองรับในกรณีที่กระแสไฟฟ้าหลักเกิดการขัดข้อง และต้องการแสงสว่างในพื้นที่หรือบริเวณต่าง ๆ				
	- มีระบบจ่ายน้ำที่เพียงพอสำหรับระบบปรับอากาศที่ต้องใช้น้ำในการทำงาน				
	- มีระบบจ่ายน้ำที่เพียงพอเพื่อสนับสนุนระบบดับเพลิงของอาคาร				
	- มีการติดตั้งระบบแจ้งเตือนในกรณีที่ระบบสนับสนุนการทำงานภายในห้องเครื่องทำงานผิดปกติหรือหยุดการทำงาน				
	- มีระบบสายสื่อสารสำรอง ซึ่งเชื่อมต่อไปยังผู้ให้บริการเครือข่าย และหรือผู้ให้บริการโทรคมนาคม เพื่อใช้เป็นเส้นทางสำรอง				
๒๒.	**การทดสอบและการกู้คืน**				
	- มีการทดสอบความเชื่อถือได้ของสื่อบันทึกข้อมูลสำรองอย่างสม่ำเสมอ				
	- มีการจัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้				
	- มีการทดสอบขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลนั้นอย่างสม่ำเสมอเพื่อดูว่าขั้นตอนที่กำหนดไว้ใช้ได้จริง				
	- มีขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลสำคัญ ซึ่งสามารถดำเนินการให้แล้วเสร็จได้ตามขั้นตอนภายในระยะเวลาเป้าหมายที่กำหนดไว้				
	- มีการเข้ารหัสข้อมูลกับข้อมูลลับที่ได้สำรองเก็บไว้				
	- มีการทดสอบข้อมูลที่ได้สำรองเก็บไว้ จากสื่อบันทึกข้อมูล เพื่อดูว่าข้อมูลเหล่านั้นยังสามารถใช้งานได้กับแผนสร้างความต่อเนื่องทางธุรกิจ				
	- มีการตรวจสอบว่าข้อมูลทั้งหมดของระบบงานสำคัญได้รับการสำรอง				

ลำดับ	ประเด็นด้านเทคโนโลยีสารสนเทศ (ระบุว่ามีการดำเนินงานในเรื่องเหล่านี้หรือไม่)	สถานะปัจจุบัน		กระบวนงานที่ต้องปฏิบัติ	หมายเหตุ
		มี	ไม่มี		
	ไว้อย่างครบถ้วน				
	- มีระยะเวลาสำหรับการจัดเก็บข้อมูลสำคัญแต่ละชนิด				
	- มีข้อกำหนดให้จัดเก็บข้อมูลสำคัญอย่างถาวร				
๒๓.	**การประเมินความเสี่ยงด้านสารสนเทศ**				
	- มีข้อกำหนดให้ดำเนินการการตรวจสอบระบบให้บริการ				
	- มีการอนุมัติให้ดำเนินการประเมินความเสี่ยงด้านสารสนเทศ			ระบุผู้บริหาร	
	- มีการวางแผนสำหรับการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย				
	- มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศอย่างสม่ำเสมอทุกปี			ระบุความถี่	
	- มีผู้ตรวจสอบภายใน(internal auditor) หรือโดยผู้ตรวจสอบภายนอก(external auditor) เป็นผู้ดำเนินการตรวจสอบและประเมินความเสี่ยง			ระบุผู้ทำหน้าที่ตรวจสอบ	
	- มีข้อตกลงร่วมกันสำหรับขอบเขตการตรวจสอบระหว่างผู้ตรวจสอบกับผู้รับการตรวจ				
	- มีข้อจำกัดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้ในลักษณะที่อ่านได้เพียงอย่างเดียว				
	- มีวิธีการที่ปลอดภัยสำหรับการอนุญาตให้ผู้ตรวจสามารถเข้าถึงข้อมูลชนิดที่สามารถเขียนหรือบันทึกข้อมูลได้				
	- มีการสร้างสำเนาข้อมูลเพื่อให้ผู้ตรวจสอบทำงานบนข้อมูลสำเนา				
	- มีการทำลายหรือลบข้อมูลที่ทำสำเนาทิ้งโดยทันทีที่ตรวจสอบเสร็จ				
	- มีวิธีการแบบปลอดภัยสำหรับจัดเก็บหลักฐานข้อมูลสำหรับอ้างอิงในการตรวจ				
	- มีการกำหนดหน้าที่ความรับผิดชอบของผู้ตรวจสอบและขั้นตอนปฏิบัติสำหรับการตรวจสอบ				
	- มีการกำหนดตัวบุคลากรผู้ทำหน้าที่เป็นผู้ตรวจสอบให้เป็นเอกเทศจากกิจกรรมหรือระบบเทคโนโลยีสารสนเทศที่จะดำเนินการตรวจสอบ (ผู้ตรวจสอบจะต้องไม่ตรวจสอบกิจกรรมหรือระบบเทคโนโลยีสารสนเทศที่ตนดูแลหรือรับผิดชอบ)				

คณะผู้จัดทำ

ที่ปรึกษา

๑. คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
๒. คณะอนุกรรมการความมั่นคงปลอดภัย

จัดทำโดย :

๑. นางสมใจ ประเสริฐจีรังกุล
ผู้อำนวยการสำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
๒. นางสาวรัตนา จรูญศักดิ์สิทธิ์
ผู้อำนวยการกลุ่มงานผลักดันธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ
๓. นายทวีสิทธิ์ เพ็ญรัศมีพูนสุข
นักวิชาการคอมพิวเตอร์ปฏิบัติการ
๔. นายธวัชชัย ศิริกุล
นักวิชาการคอมพิวเตอร์ปฏิบัติการ

ภาคผนวก

ภาคผนวก ๑

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔

(แก้ไขเพิ่มเติม ฉบับที่ ๒ พ.ศ. ๒๕๕๑)

พระราชบัญญัติ
ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์
พ.ศ. ๒๕๔๔

ภูมิพลอดุลยเดช ป.ร.
ให้ไว้ ณ วันที่ ๒ ธันวาคม พ.ศ. ๒๕๔๔
เป็นปีที่ ๕๖ ในรัชกาลปัจจุบัน

พระบาทสมเด็จพระปรมินทรมหาภูมิพลอดุลยเดช มีพระบรมราชโองการโปรดเกล้าฯ ให้ประกาศว่า

โดยที่เป็นการสมควรให้มีกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

พระราชบัญญัตินี้มีบทบัญญัติบางประการเกี่ยวกับการจำกัดสิทธิและเสรีภาพของบุคคล ซึ่งมาตรา ๒๙ ประกอบกับมาตรา ๕๐ ของรัฐธรรมนูญแห่งราชอาณาจักรไทย บัญญัติให้กระทำได้โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมาย

จึงทรงพระกรุณาโปรดเกล้าฯ ให้ตราพระราชบัญญัติขึ้นไว้โดยคำแนะนำและยินยอมของรัฐสภา ดังต่อไปนี้

มาตรา ๑ พระราชบัญญัตินี้เรียกว่า “พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔”

มาตรา ๒[๑] พระราชบัญญัตินี้ให้ใช้บังคับเมื่อพ้นกำหนดหนึ่งร้อยยี่สิบวันนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

มาตรา ๓ พระราชบัญญัตินี้ให้ใช้บังคับแก่ธุรกรรมในทางแพ่งและพาณิชย์ที่ดำเนินการโดยใช้ข้อมูลอิเล็กทรอนิกส์ เว้นแต่ธุรกรรมที่มีพระราชกฤษฎีกากำหนดมิให้นำพระราชบัญญัตินี้ทั้งหมดหรือแต่บางส่วนมาใช้บังคับ

ความในวรรคหนึ่งไม่มีผลกระทบกระเทือนถึงกฎหมายหรือกฎใดที่กำหนดขึ้นเพื่อคุ้มครองผู้บริโภค

พระราชบัญญัตินี้ให้ใช้บังคับแก่ธุรกรรมในการดำเนินงานของรัฐตามที่กำหนดในหมวด ๔

มาตรา ๔ ในพระราชบัญญัตินี้

“**ธุรกรรม**” หมายความว่า การกระทำใดๆ ที่เกี่ยวกับกิจกรรมในทางแพ่งและพาณิชย์ หรือในการดำเนินงานของรัฐตามที่กำหนดในหมวด ๔

---

[๑] ราชกิจจานุเบกษา เล่ม ๑๑๘/ตอนที่ ๑๑๒ ก/หน้า ๒๖/๔ ธันวาคม ๒๕๔๔

“**อิเล็กทรอนิกส์**” หมายความว่า การประยุกต์ใช้วิธีการทางอิเล็กตรอน ไฟฟ้า คลื่นแม่เหล็กไฟฟ้า หรือวิธีอื่นใดในลักษณะคล้ายกัน และให้หมายความรวมถึงการประยุกต์ใช้วิธีการทางแสง วิธีการทางแม่เหล็ก หรืออุปกรณ์ที่เกี่ยวข้องกับการประยุกต์ใช้วิธีต่างๆ เช่นว่านั้น

“**ธุรกรรมทางอิเล็กทรอนิกส์**” หมายความว่า ธุรกรรมที่กระทำขึ้นโดยใช้วิธีการทางอิเล็กทรอนิกส์ทั้งหมดหรือแต่บางส่วน

“**ข้อความ**” หมายความว่า เรื่องราวหรือข้อเท็จจริง ไม่ว่าจะปรากฏในรูปแบบของตัวอักษร ตัวเลข เสียง ภาพ หรือรูปแบบอื่นใดที่สื่อความหมายได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใดๆ

“**ข้อมูลอิเล็กทรอนิกส์**” หมายความว่า ข้อความที่ได้สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์ เช่น วิธีการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ จดหมายอิเล็กทรอนิกส์ โทรเลข โทรพิมพ์ หรือโทรสาร

“**ลายมือชื่ออิเล็กทรอนิกส์**” หมายความว่า อักษร อักขระ ตัวเลข เสียงหรือสัญลักษณ์อื่นใดที่สร้างขึ้นให้อยู่ในรูปแบบอิเล็กทรอนิกส์ซึ่งนำมาใช้ประกอบกับข้อมูลอิเล็กทรอนิกส์เพื่อแสดงความสัมพันธ์ระหว่างบุคคลกับข้อมูลอิเล็กทรอนิกส์ โดยมีวัตถุประสงค์เพื่อระบุตัวบุคคลผู้เป็นเจ้าของลายมือชื่ออิเล็กทรอนิกส์ที่เกี่ยวข้องกับข้อมูลอิเล็กทรอนิกส์นั้น และเพื่อแสดงว่าบุคคลดังกล่าวยอมรับข้อความในข้อมูลอิเล็กทรอนิกส์นั้น

“**ระบบข้อมูล**” หมายความว่า กระบวนการประมวลผลด้วยเครื่องมืออิเล็กทรอนิกส์สำหรับสร้าง ส่ง รับ เก็บรักษา หรือประมวลผลข้อมูลอิเล็กทรอนิกส์

“**การแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์**” หมายความว่า การส่งหรือรับข้อความด้วยวิธีการทางอิเล็กทรอนิกส์ระหว่างเครื่องคอมพิวเตอร์โดยใช้มาตรฐานที่กำหนดไว้ล่วงหน้า

“**ผู้ส่งข้อมูล**” หมายความว่า บุคคลซึ่งเป็นผู้ส่งหรือสร้างข้อมูลอิเล็กทรอนิกส์ก่อนจะมีการเก็บรักษาข้อมูลเพื่อส่งไปตามวิธีการที่ผู้นั้นกำหนด โดยบุคคลนั้นอาจจะส่งหรือสร้างข้อมูลอิเล็กทรอนิกส์ด้วยตนเอง หรือมีการส่งหรือสร้างข้อมูลอิเล็กทรอนิกส์ในนามหรือแทนบุคคลนั้นก็ได้ ทั้งนี้ ไม่รวมถึงบุคคลที่เป็นสื่อกลางสำหรับข้อมูลอิเล็กทรอนิกส์นั้น

“**ผู้รับข้อมูล**” หมายความว่า บุคคลซึ่งผู้ส่งข้อมูลประสงค์จะส่งข้อมูลอิเล็กทรอนิกส์ให้และได้รับข้อมูลอิเล็กทรอนิกส์นั้น ทั้งนี้ ไม่รวมถึงบุคคลที่เป็นสื่อกลางสำหรับข้อมูลอิเล็กทรอนิกส์นั้น

“**บุคคลที่เป็นสื่อกลาง**” หมายความว่า บุคคลซึ่งกระทำการในนามผู้อื่นในการส่ง รับ หรือเก็บรักษาข้อมูลอิเล็กทรอนิกส์อันใดอันหนึ่งโดยเฉพาะ รวมถึงให้บริการอื่นที่เกี่ยวกับข้อมูลอิเล็กทรอนิกส์นั้น

“**ใบรับรอง**” หมายความว่า ข้อมูลอิเล็กทรอนิกส์หรือการบันทึกอื่นใด ซึ่งยืนยันความเชื่อมโยงระหว่างเจ้าของลายมือชื่อกับข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์

“**เจ้าของลายมือชื่อ**” หมายความว่า ผู้ซึ่งถือข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์และสร้างลายมือชื่ออิเล็กทรอนิกส์นั้นในนามตนเองหรือแทนบุคคลอื่น

“**คู่กรณีที่เกี่ยวข้อง**” หมายความว่า ผู้ซึ่งอาจกระทำการใดๆ โดยขึ้นอยู่กับใบรับรองหรือลายมือชื่ออิเล็กทรอนิกส์

“**หน่วยงานของรัฐ**” หมายความว่า กระทรวง ทบวง กรม ส่วนราชการที่เรียกชื่ออย่างอื่นและมีฐานะเป็นกรม ราชการส่วนภูมิภาค ราชการส่วนท้องถิ่น รัฐวิสาหกิจที่ตั้งขึ้นโดยพระราชบัญญัติหรือพระราชกฤษฎีกา และให้หมายความรวมถึงนิติบุคคล คณะบุคคล หรือบุคคลซึ่งมีอำนาจหน้าที่ดำเนินงานของรัฐไม่ว่าในการใดๆ

“**คณะกรรมการ**” หมายความว่า คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

“**รัฐมนตรี**” หมายความว่า รัฐมนตรีผู้รักษาการตามพระราชบัญญัตินี้

มาตรา ๕ บทบัญญัติมาตรา ๑๓ ถึงมาตรา ๒๔ และบทบัญญัติมาตรา ๒๖ ถึงมาตรา ๓๑ จะตกลงกันเป็นอย่างอื่นก็ได้

มาตรา ๖ ให้นายกรัฐมนตรีรักษาการตามพระราชบัญญัตินี้

หมวด ๑
ธุรกรรมทางอิเล็กทรอนิกส์

มาตรา ๗ ห้ามมิให้ปฏิเสธความมีผลผูกพันและการบังคับใช้ทางกฎหมายของข้อความใดเพียงเพราะเหตุที่ข้อความนั้นอยู่ในรูปของข้อมูลอิเล็กทรอนิกส์

มาตรา ๘ ภายใต้บังคับบทบัญญัติแห่งมาตรา ๙ ในกรณีที่กฎหมายกำหนดให้การใดต้องทำเป็นหนังสือ มีหลักฐานเป็นหนังสือ หรือมีเอกสารมาแสดง ถ้าได้มีการจัดทำข้อความขึ้นเป็นข้อมูลอิเล็กทรอนิกส์ที่สามารถเข้าถึงและนำกลับมาใช้ได้โดยความหมายไม่เปลี่ยนแปลง ให้ถือว่าข้อความนั้นได้ทำเป็นหนังสือ มีหลักฐานเป็นหนังสือ หรือมีเอกสารมาแสดงแล้ว

ในกรณีที่กฎหมายกำหนดให้ต้องมีการปิดอากรแสตมป์ หากได้มีการชำระเงินแทนหรือดำเนินการอื่นใดด้วยวิธีการทางอิเล็กทรอนิกส์ตามหลักเกณฑ์และวิธีการที่หน่วยงานของรัฐซึ่งเกี่ยวข้องประกาศกำหนด ให้ถือว่าหนังสือ หลักฐานเป็นหนังสือ หรือเอกสาร ซึ่งมีลักษณะเป็นตราสารนั้นได้มีการปิดอากรแสตมป์และขีดฆ่าตามกฎหมายนั้นแล้ว ในการนี้ในการกำหนดหลักเกณฑ์และวิธีการของหน่วยงานของรัฐดังกล่าว คณะกรรมการจะกำหนดกรอบและแนวทางเพื่อเป็นมาตรฐานทั่วไปไว้ด้วยก็ได้[๒]

[๒] มาตรา ๘ วรรคสอง เพิ่มโดยพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ ๒) พ.ศ. ๒๕๕๑

มาตรา ๙ ในกรณีที่บุคคลพึงลงลายมือชื่อในหนังสือ ให้ถือว่าข้อมูลอิเล็กทรอนิกส์นั้นมีการลงลายมือชื่อแล้ว ถ้า

(๑) ใช้วิธีการที่สามารถระบุตัวเจ้าของลายมือชื่อ และสามารถแสดงได้ว่าเจ้าของลายมือชื่อรับรองข้อความในข้อมูลอิเล็กทรอนิกส์นั้นว่าเป็นของตน และ

(๒) วิธีการดังกล่าวเป็นวิธีการที่เชื่อถือได้โดยเหมาะสมกับวัตถุประสงค์ของการสร้างหรือส่งข้อมูลอิเล็กทรอนิกส์ โดยคำนึงถึงพฤติการณ์แวดล้อมหรือข้อตกลงของคู่กรณี

วิธีการที่เชื่อถือได้ตาม (๒) ให้คำนึงถึง

ก. ความมั่นคงและรัดกุมของการใช้วิธีการหรืออุปกรณ์ในการระบุตัวบุคคล สภาพพร้อมใช้งานของทางเลือกในการระบุตัวบุคคล กฎเกณฑ์เกี่ยวกับลายมือชื่อที่กำหนดไว้ในกฎหมายระดับความมั่นคงปลอดภัยของการใช้ลายมือชื่ออิเล็กทรอนิกส์ การปฏิบัติตามกระบวนการในการระบุตัวบุคคลผู้เป็นสื่อกลาง ระดับของการยอมรับหรือไม่ยอมรับ วิธีการที่ใช้ในการระบุตัวบุคคลในการทำธุรกรรม วิธีการระบุตัวบุคคล ณ ช่วงเวลาที่มีการทำธุรกรรมและติดต่อสื่อสาร

ข. ลักษณะ ประเภท หรือขนาดของธุรกรรมที่ทำ จำนวนครั้งหรือความสม่ำเสมอในการทำธุรกรรม ประเพณีทางการค้าหรือทางปฏิบัติ ความสำคัญ มูลค่าของธุรกรรมที่ทำ หรือ

ค. ความรัดกุมของระบบการติดต่อสื่อสาร[๓]

ให้นำความในวรรคหนึ่งมาใช้บังคับกับการประทับตราของนิติบุคคลด้วยวิธีการทางอิเล็กทรอนิกส์ ด้วยโดยอนุโลม[๔]

มาตรา ๑๐ ในกรณีที่กฎหมายกำหนดให้นำเสนอหรือเก็บรักษาข้อความใดในสภาพที่เป็นมาแต่เดิมอย่างเอกสารต้นฉบับ ถ้าได้นำเสนอหรือเก็บรักษาในรูปข้อมูลอิเล็กทรอนิกส์ตามหลักเกณฑ์ดังต่อไปนี้ ให้ถือว่าได้มีการนำเสนอหรือเก็บรักษาเป็นเอกสารต้นฉบับตามกฎหมายแล้ว

(๑) ข้อมูลอิเล็กทรอนิกส์ได้ใช้วิธีการที่เชื่อถือได้ในการรักษาความถูกต้องของข้อความตั้งแต่การสร้างข้อความเสร็จสมบูรณ์ และ

(๒) สามารถแสดงข้อความนั้นในภายหลังได้

ความถูกต้องของข้อความตาม (๑) ให้พิจารณาถึงความครบถ้วนและไม่มีการเปลี่ยนแปลงใดของข้อความ เว้นแต่การรับรองหรือบันทึกเพิ่มเติม หรือการเปลี่ยนแปลงใดๆ ที่อาจจะเกิดขึ้นได้ตามปกติในการติดต่อสื่อสาร การเก็บรักษา หรือการแสดงข้อความซึ่งไม่มีผลต่อความถูกต้องของข้อความนั้น

---

[๓] มาตรา ๙ วรรคสอง เพิ่มโดยพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ ๒) พ.ศ. ๒๕๕๑

[๔] มาตรา ๙ วรรคสาม เพิ่มโดยพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ ๒) พ.ศ. ๒๕๕๑

ในการวินิจฉัยความน่าเชื่อถือของวิธีการรักษาความถูกต้องของข้อความตาม (๑) ให้พิเคราะห์ถึงพฤติการณ์ที่เกี่ยวข้องทั้งปวง รวมทั้งวัตถุประสงค์ของการสร้างข้อความนั้น

ในกรณีที่มีการทำสิ่งพิมพ์ออกของข้อมูลอิเล็กทรอนิกส์ตามวรรคหนึ่งสำหรับใช้อ้างอิงข้อความของข้อมูลอิเล็กทรอนิกส์ หากสิ่งพิมพ์ออกนั้นมีข้อความถูกต้องครบถ้วนตรงกับข้อมูลอิเล็กทรอนิกส์ และมีการรับรองสิ่งพิมพ์ออกโดยหน่วยงานที่มีอำนาจตามที่คณะกรรมการประกาศกำหนดแล้ว ให้ถือว่าสิ่งพิมพ์ออกดังกล่าวใช้แทนต้นฉบับได้[๕]

มาตรา ๑๑[๖] ห้ามมิให้ปฏิเสธการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานในกระบวนการพิจารณาตามกฎหมายทั้งในคดีแพ่ง คดีอาญา หรือคดีอื่นใด เพียงเพราะเหตุว่าเป็นข้อมูลอิเล็กทรอนิกส์

ในการชั่งน้ำหนักพยานหลักฐานว่าข้อมูลอิเล็กทรอนิกส์จะเชื่อถือได้หรือไม่เพียงใดนั้น ให้พิเคราะห์ถึงความน่าเชื่อถือของลักษณะหรือวิธีการที่ใช้สร้าง เก็บรักษา หรือสื่อสารข้อมูลอิเล็กทรอนิกส์ ลักษณะหรือวิธีการเก็บรักษา ความครบถ้วน และไม่มีการเปลี่ยนแปลงของข้อความ ลักษณะ หรือวิธีการที่ใช้ในการระบุหรือแสดงตัวผู้ส่งข้อมูล รวมทั้งพฤติการณ์ที่เกี่ยวข้องทั้งปวง

ให้นำความในวรรคหนึ่งมาใช้บังคับกับสิ่งพิมพ์ออกของข้อมูลอิเล็กทรอนิกส์ด้วย

มาตรา ๑๒ ภายใต้บังคับบทบัญญัติมาตรา ๑๐ ในกรณีที่กฎหมายกำหนดให้เก็บรักษาเอกสารหรือข้อความใด ถ้าได้เก็บรักษาในรูปข้อมูลอิเล็กทรอนิกส์ตามหลักเกณฑ์ดังต่อไปนี้ ให้ถือว่าได้มีการเก็บรักษาเอกสารหรือข้อความตามที่กฎหมายต้องการแล้ว

(๑) ข้อมูลอิเล็กทรอนิกส์นั้นสามารถเข้าถึงและนำกลับมาใช้ได้โดยความหมายไม่เปลี่ยนแปลง

(๒) ได้เก็บรักษาข้อมูลอิเล็กทรอนิกส์นั้นให้อยู่ในรูปแบบที่เป็นอยู่ในขณะที่สร้าง ส่ง หรือได้รับข้อมูลอิเล็กทรอนิกส์นั้น หรืออยู่ในรูปแบบที่สามารถแสดงข้อความที่สร้าง ส่ง หรือได้รับให้ปรากฏอย่างถูกต้องได้ และ

(๓) ได้เก็บรักษาข้อความส่วนที่ระบุถึงแหล่งกำเนิด ต้นทาง และปลายทางของข้อมูลอิเล็กทรอนิกส์ ตลอดจนวันและเวลาที่ส่งหรือได้รับข้อความดังกล่าว ถ้ามี

ความในวรรคหนึ่ง มิให้ใช้บังคับกับข้อความที่ใช้เพียงเพื่อวัตถุประสงค์ในการส่งหรือรับข้อมูลอิเล็กทรอนิกส์

หน่วยงานของรัฐที่รับผิดชอบในการเก็บรักษาเอกสารหรือข้อความใด อาจกำหนดหลักเกณฑ์รายละเอียดเพิ่มเติมเกี่ยวกับการเก็บรักษาเอกสารหรือข้อความนั้นได้ เท่าที่ไม่ขัดหรือแย้งกับบทบัญญัติในมาตรานี้

---

[๕] มาตรา ๑๐ วรรคสี่ เพิ่มโดยพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ ๒) พ.ศ. ๒๕๕๑

[๖] มาตรา ๑๑ แก้ไขเพิ่มเติมโดยพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ ๒) พ.ศ. ๒๕๕๑

มาตรา ๑๒/๑[๗] ให้นำบทบัญญัติในมาตรา ๑๐ มาตรา ๑๑ และมาตรา ๑๒ มาใช้บังคับกับเอกสารหรือข้อความที่ได้มีการจัดทำหรือแปลงให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ในภายหลังด้วยวิธีการทางอิเล็กทรอนิกส์ และการเก็บรักษาเอกสารและข้อความดังกล่าวด้วยโดยอนุโลม

การจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ตามวรรคหนึ่งให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการกำหนด

มาตรา ๑๓ คำเสนอหรือคำสนองในการทำสัญญาอาจทำเป็นข้อมูลอิเล็กทรอนิกส์ก็ได้ และห้ามมิให้ปฏิเสธการมีผลทางกฎหมายของสัญญาเพียงเพราะเหตุที่สัญญานั้นได้ทำคำเสนอหรือคำสนองเป็นข้อมูลอิเล็กทรอนิกส์

มาตรา ๑๔ ในระหว่างผู้ส่งข้อมูลและผู้รับข้อมูล การแสดงเจตนาหรือคำบอกกล่าวอาจทำเป็นข้อมูลอิเล็กทรอนิกส์ก็ได้

มาตรา ๑๕ บุคคลใดเป็นผู้ส่งข้อมูลไม่ว่าจะเป็นการส่งโดยวิธีใด ให้ถือว่าข้อมูลอิเล็กทรอนิกส์เป็นของผู้นั้น

ในระหว่างผู้ส่งข้อมูลและผู้รับข้อมูล ให้ถือว่าเป็นข้อมูลอิเล็กทรอนิกส์ของผู้ส่งข้อมูล หากข้อมูลอิเล็กทรอนิกส์นั้นได้ส่งโดย

(๑) บุคคลผู้มีอำนาจกระทำการแทนผู้ส่งข้อมูลเกี่ยวกับข้อมูลอิเล็กทรอนิกส์นั้น หรือ

(๒) ระบบข้อมูลที่ผู้ส่งข้อมูลหรือบุคคลผู้มีอำนาจกระทำการแทนผู้ส่งข้อมูลได้กำหนดไว้ล่วงหน้าให้สามารถทำงานได้โดยอัตโนมัติ

มาตรา ๑๖ ผู้รับข้อมูลชอบที่จะถือว่าข้อมูลอิเล็กทรอนิกส์เป็นของผู้ส่งข้อมูลและชอบที่จะดำเนินการไปตามข้อมูลอิเล็กทรอนิกส์นั้นได้ ถ้า

(๑) ผู้รับข้อมูลได้ตรวจสอบโดยสมควรตามวิธีการที่ได้ตกลงกับผู้ส่งข้อมูลว่าข้อมูลอิเล็กทรอนิกส์เป็นของผู้ส่งข้อมูล หรือ

(๒) ข้อมูลอิเล็กทรอนิกส์ที่ผู้รับข้อมูลได้รับนั้นเกิดจากการกระทำของบุคคลซึ่งใช้วิธีการที่ผู้ส่งข้อมูลใช้ในการแสดงว่าข้อมูลอิเล็กทรอนิกส์นั้นเป็นของผู้ส่งข้อมูล ซึ่งบุคคลนั้นได้ล่วงรู้โดยอาศัยความสัมพันธ์ระหว่างบุคคลนั้นกับผู้ส่งข้อมูลหรือผู้มีอำนาจกระทำการแทนผู้ส่งข้อมูล

ความในวรรคหนึ่งมิให้ใช้บังคับ ถ้า

(๑) ในขณะนั้นผู้รับข้อมูลได้รับแจ้งจากผู้ส่งข้อมูลว่าข้อมูลอิเล็กทรอนิกส์ที่ผู้รับข้อมูลได้รับนั้นมิใช่ของผู้ส่งข้อมูล และในขณะเดียวกันผู้รับข้อมูลมีเวลาพอสมควรที่จะตรวจสอบข้อเท็จจริงตามที่ได้รับแจ้งนั้น หรือ

---

[๗] มาตรา ๑๒/๑ เพิ่มโดยพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ ๒) พ.ศ. ๒๕๕๑

(๒) กรณีตามวรรคหนึ่ง (๒) เมื่อผู้รับข้อมูลได้รู้หรือควรจะได้รู้ว่าข้อมูลอิเล็กทรอนิกส์นั้นไม่ใช่ของผู้ส่งข้อมูล หากผู้รับข้อมูลได้ใช้ความระมัดระวังตามสมควร หรือดำเนินการตามวิธีการที่ได้ตกลงกันไว้ก่อนแล้ว

มาตรา ๑๗ ในกรณีตามมาตรา ๑๕ หรือมาตรา ๑๖ วรรคหนึ่ง ในระหว่างผู้ส่งข้อมูลและผู้รับข้อมูล ผู้รับข้อมูลมีสิทธิถือว่าข้อมูลอิเล็กทรอนิกส์ที่ได้รับนั้นถูกต้องตามเจตนาของผู้ส่งข้อมูล และสามารถดำเนินการไปตามข้อมูลอิเล็กทรอนิกส์นั้นได้ เว้นแต่ผู้รับข้อมูลได้รู้หรือควรจะได้รู้ว่าข้อมูลอิเล็กทรอนิกส์ที่ได้รับนั้นมีข้อผิดพลาดอันเกิดจากการส่ง หากผู้รับข้อมูลได้ใช้ความระมัดระวังตามสมควรหรือดำเนินการตามวิธีการที่ได้ตกลงกันไว้ก่อนแล้ว

มาตรา ๑๘ ผู้รับข้อมูลชอบที่จะถือว่าข้อมูลอิเล็กทรอนิกส์ที่ได้รับแต่ละชุดเป็นข้อมูลที่แยกจากกัน และสามารถดำเนินการไปตามข้อมูลอิเล็กทรอนิกส์แต่ละชุดนั้นได้ เว้นแต่ข้อมูลอิเล็กทรอนิกส์ชุดนั้นจะซ้ำกับข้อมูลอิเล็กทรอนิกส์อีกชุดหนึ่ง และผู้รับข้อมูลได้รู้หรือควรจะได้รู้ว่าข้อมูลอิเล็กทรอนิกส์นั้นเป็นข้อมูลอิเล็กทรอนิกส์ซ้ำ หากผู้รับข้อมูลได้ใช้ความระมัดระวังตามสมควรหรือดำเนินการตามวิธีการที่ได้ตกลงกันไว้ก่อนแล้ว

มาตรา ๑๙ ในกรณีที่ต้องมีการตอบแจ้งการรับข้อมูลอิเล็กทรอนิกส์ ไม่ว่าผู้ส่งข้อมูลได้ร้องขอหรือตกลงกับผู้รับข้อมูลไว้ก่อนหรือขณะที่ส่งข้อมูลอิเล็กทรอนิกส์หรือปรากฏในข้อมูลอิเล็กทรอนิกส์ ให้เป็นไปตามหลักเกณฑ์ดังต่อไปนี้

(๑) ในกรณีที่ผู้ส่งข้อมูลมิได้ตกลงให้ตอบแจ้งการรับข้อมูลอิเล็กทรอนิกส์ในรูปแบบหรือวิธีการใดโดยเฉพาะ การตอบแจ้งการรับอาจทำได้ด้วยการติดต่อสื่อสารจากผู้รับข้อมูล ไม่ว่าโดยระบบข้อมูลที่ทำงานโดยอัตโนมัติหรือโดยวิธีอื่นใด หรือด้วยการกระทำใดๆ ของผู้รับข้อมูลซึ่งเพียงพอจะแสดงต่อผู้ส่งข้อมูลว่าผู้รับข้อมูลได้รับข้อมูลอิเล็กทรอนิกส์นั้นแล้ว

(๒) ในกรณีที่ผู้ส่งข้อมูลกำหนดเงื่อนไขว่าจะถือว่ามีการส่งข้อมูลอิเล็กทรอนิกส์ต่อเมื่อได้รับการตอบแจ้งการรับจากผู้รับข้อมูล ให้ถือว่ายังไม่มีการส่งข้อมูลอิเล็กทรอนิกส์จนกว่าผู้ส่งข้อมูลจะได้รับการตอบแจ้งการรับแล้ว

(๓) ในกรณีที่ผู้ส่งข้อมูลมิได้กำหนดเงื่อนไขตามความใน (๒) และผู้ส่งข้อมูลมิได้รับการตอบแจ้งการรับนั้นภายในเวลาที่กำหนดหรือตกลงกัน หรือภายในระยะเวลาอันสมควรในกรณีที่มิได้กำหนดหรือตกลงเวลาไว้

(ก) ผู้ส่งข้อมูลอาจส่งคำบอกกล่าวไปยังผู้รับข้อมูลว่าตนยังมิได้รับการตอบแจ้งการรับ และกำหนดระยะเวลาอันสมควรให้ผู้รับข้อมูลตอบแจ้งการรับ และ

(ข) หากผู้ส่งข้อมูลมิได้รับการตอบแจ้งการรับภายในระยะเวลาตาม (ก) เมื่อผู้ส่งข้อมูลบอกกล่าวแก่ผู้รับข้อมูลแล้ว ผู้ส่งข้อมูลชอบที่จะถือว่าข้อมูลอิเล็กทรอนิกส์นั้นมิได้มีการส่งเลยหรือผู้ส่งข้อมูลอาจใช้สิทธิอื่นใดที่ผู้ส่งข้อมูลมีอยู่ได้

มาตรา ๒๐ ในกรณีที่ผู้ส่งข้อมูลได้รับการตอบแจ้งการรับจากผู้รับข้อมูล ให้สันนิษฐานว่าผู้รับข้อมูลได้รับข้อมูลอิเล็กทรอนิกส์ที่เกี่ยวข้องแล้ว แต่ข้อสันนิษฐานดังกล่าวมิให้ถือว่าข้อมูลอิเล็กทรอนิกส์ที่ผู้รับข้อมูลได้รับนั้นถูกต้องตรงกันกับข้อมูลอิเล็กทรอนิกส์ที่ผู้ส่งข้อมูลได้ส่งมา

มาตรา ๒๑ ในกรณีที่ปรากฏในการตอบแจ้งการรับข้อมูลอิเล็กทรอนิกส์นั้นเองว่าข้อมูลอิเล็กทรอนิกส์ที่ผู้รับข้อมูลได้รับเป็นไปตามข้อกำหนดทางเทคนิคที่ผู้ส่งข้อมูลและผู้รับข้อมูลได้ตกลงหรือระบุไว้ในมาตรฐานซึ่งใช้บังคับอยู่ ให้สันนิษฐานว่าข้อมูลอิเล็กทรอนิกส์ที่ส่งไปนั้นได้เป็นไปตามข้อกำหนดทางเทคนิคทั้งหมดแล้ว

มาตรา ๒๒ การส่งข้อมูลอิเล็กทรอนิกส์ให้ถือว่าได้มีการส่งเมื่อ ข้อมูลอิเล็กทรอนิกส์นั้นได้เข้าสู่ระบบข้อมูลที่อยู่นอกเหนือการควบคุมของผู้ส่งข้อมูล

มาตรา ๒๓ การรับข้อมูลอิเล็กทรอนิกส์ให้ถือว่ามีผลนับแต่เวลาที่ข้อมูลอิเล็กทรอนิกส์นั้นได้เข้าสู่ระบบข้อมูลของผู้รับข้อมูล

หากผู้รับข้อมูลได้กำหนดระบบข้อมูลที่ประสงค์จะใช้ในการรับข้อมูลอิเล็กทรอนิกส์ไว้โดยเฉพาะ ให้ถือว่าการรับข้อมูลอิเล็กทรอนิกส์มีผลนับแต่เวลาที่ข้อมูลอิเล็กทรอนิกส์นั้นได้เข้าสู่ระบบข้อมูลที่ผู้รับข้อมูลได้กำหนดไว้นั้น แต่ถ้าข้อมูลอิเล็กทรอนิกส์ดังกล่าวได้ส่งไปยังระบบข้อมูลอื่นของผู้รับข้อมูลซึ่งมิใช่ระบบข้อมูลที่ผู้รับข้อมูลกำหนดไว้ ให้ถือว่าการรับข้อมูลอิเล็กทรอนิกส์มีผลนับแต่เวลาที่ได้เรียกข้อมูลอิเล็กทรอนิกส์จากระบบข้อมูลนั้น

ความในมาตรานี้ให้ใช้บังคับแม้ระบบข้อมูลของผู้รับข้อมูลตั้งอยู่ในสถานที่อีกแห่งหนึ่งต่างหากจากสถานที่ที่ถือว่าผู้รับข้อมูลได้รับข้อมูลอิเล็กทรอนิกส์ตามมาตรา ๒๔

มาตรา ๒๔ การส่งหรือการรับข้อมูลอิเล็กทรอนิกส์ ให้ถือว่า ได้ส่ง ณ ที่ทำการงานของผู้ส่งข้อมูล หรือได้รับ ณ ที่ทำการงานของผู้รับข้อมูล แล้วแต่กรณี

ในกรณีที่ผู้ส่งข้อมูลหรือผู้รับข้อมูลมีที่ทำการงานหลายแห่ง ให้ถือเอาที่ทำการงานที่เกี่ยวข้องมากที่สุดกับธุรกรรมนั้นเป็นที่ทำการงานเพื่อประโยชน์ตามวรรคหนึ่ง แต่ถ้าไม่สามารถกำหนดได้ว่าธุรกรรมนั้นเกี่ยวข้องกับที่ทำการงานแห่งใดมากที่สุด ให้ถือเอาสำนักงานใหญ่เป็นสถานที่ที่ได้รับหรือส่งข้อมูลอิเล็กทรอนิกส์นั้น

ในกรณีที่ไม่ปรากฏที่ทำการงานของผู้ส่งข้อมูลหรือผู้รับข้อมูล ให้ถือเอาถิ่นที่อยู่ปกติเป็นสถานที่ที่ส่งหรือได้รับข้อมูลอิเล็กทรอนิกส์

ความในมาตรานี้มิให้ใช้บังคับกับการส่งและการรับข้อมูลอิเล็กทรอนิกส์โดยวิธีการทางโทรเลขและโทรพิมพ์ หรือวิธีการสื่อสารอื่นตามที่กำหนดในพระราชกฤษฎีกา

มาตรา ๒๕ ธุรกรรมทางอิเล็กทรอนิกส์ใดที่ได้กระทำตามวิธีการแบบปลอดภัยที่กำหนดในพระราชกฤษฎีกา ให้สันนิษฐานว่าเป็นวิธีการที่เชื่อถือได้

หมวด ๒
ลายมือชื่ออิเล็กทรอนิกส์

มาตรา ๒๖ ลายมือชื่ออิเล็กทรอนิกส์ที่มีลักษณะดังต่อไปนี้ให้ถือว่าเป็นลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้

(๑) ข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์นั้นได้เชื่อมโยงไปยังเจ้าของลายมือชื่อโดยไม่เชื่อมโยงไปยังบุคคลอื่นภายใต้สภาพที่นำมาใช้

(๒) ในขณะสร้างลายมือชื่ออิเล็กทรอนิกส์นั้น ข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์อยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่น

(๓) การเปลี่ยนแปลงใดๆ ที่เกิดแก่ลายมือชื่ออิเล็กทรอนิกส์ นับแต่เวลาที่ได้สร้างขึ้นสามารถจะตรวจพบได้ และ

(๔) ในกรณีที่กฎหมายกำหนดให้การลงลายมือชื่ออิเล็กทรอนิกส์เป็นไปเพื่อรับรองความครบถ้วนและไม่มีการเปลี่ยนแปลงของข้อความ การเปลี่ยนแปลงใดแก่ข้อความนั้นสามารถตรวจพบได้นับแต่เวลาที่ลงลายมือชื่ออิเล็กทรอนิกส์

บทบัญญัติในวรรคหนึ่ง ไม่เป็นการจำกัดว่าไม่มีวิธีการอื่นใดที่แสดงได้ว่าเป็นลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้ หรือการแสดงพยานหลักฐานใดเกี่ยวกับความไม่น่าเชื่อถือของลายมือชื่ออิเล็กทรอนิกส์

มาตรา ๒๗ ในกรณีมีการใช้ข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์เพื่อสร้างลายมือชื่ออิเล็กทรอนิกส์ที่จะมีผลตามกฎหมาย เจ้าของลายมือชื่อต้องดำเนินการดังต่อไปนี้

(๑) ใช้ความระมัดระวังตามสมควรเพื่อมิให้มีการใช้ข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์โดยไม่ได้รับอนุญาต

(๒) แจ้งให้บุคคลที่คาดหมายได้โดยมีเหตุอันควรเชื่อว่าจะกระทำการใดโดยขึ้นอยู่กับลายมือชื่ออิเล็กทรอนิกส์หรือให้บริการเกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์ ทราบโดยมิชักช้า เมื่อ

(ก) เจ้าของลายมือชื่อรู้หรือควรได้รู้ว่าข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์นั้นสูญหาย ถูกทำลาย ถูกแก้ไข ถูกเปิดเผยโดยมิชอบ หรือถูกล่วงรู้โดยไม่สอดคล้องกับวัตถุประสงค์

(ข) เจ้าของลายมือชื่อรู้จากสภาพการณ์ที่ปรากฏว่ากรณีมีความเสี่ยงมากพอที่ข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์ สูญหาย ถูกทำลาย ถูกแก้ไข ถูกเปิดเผยโดยมิชอบ หรือถูกล่วงรู้โดยไม่สอดคล้องกับวัตถุประสงค์

(๓) ในกรณีมีการออกใบรับรองสนับสนุนการใช้ลายมือชื่ออิเล็กทรอนิกส์ จะต้องใช้ความระมัดระวังตามสมควรให้แน่ใจในความถูกต้องและสมบูรณ์ของการแสดงสาระสำคัญทั้งหมด ซึ่งกระทำโดยเจ้าของลายมือชื่อเกี่ยวกับใบรับรองนั้นตลอดอายุใบรับรอง หรือตามที่มีการกำหนดในใบรับรอง

มาตรา ๒๘ ในกรณีมีการให้บริการออกใบรับรองเพื่อสนับสนุนลายมือชื่ออิเล็กทรอนิกส์ให้มีผลทางกฎหมายเสมือนหนึ่งลงลายมือชื่อผู้ให้บริการออกใบรับรองต้องดำเนินการ ดังต่อไปนี้

(๑) ปฏิบัติตามแนวนโยบายและแนวปฏิบัติที่ตนได้แสดงไว้

(๒) ใช้ความระมัดระวังตามสมควรให้แน่ใจในความถูกต้องและความสมบูรณ์ของการแสดงสาระสำคัญทั้งหมดที่ตนได้กระทำเกี่ยวกับใบรับรองนั้นตลอดอายุใบรับรอง หรือตามที่มีการกำหนดในใบรับรอง

(๓) จัดให้มีวิธีการในการเข้าถึงโดยสมควร ให้คู่กรณีที่เกี่ยวข้องสามารถตรวจสอบข้อเท็จจริงในการแสดงสาระสำคัญทั้งหมดจากใบรับรองได้ ในเรื่องดังต่อไปนี้

(ก) การระบุผู้ให้บริการออกใบรับรอง

(ข) เจ้าของลายมือชื่อซึ่งระบุในใบรับรองได้ควบคุมข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์ในขณะมีการออกใบรับรอง

(ค) ข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์มีผล ใช้ได้ในขณะหรือก่อนที่มีการออกใบรับรอง

(๔) จัดให้มีวิธีการเข้าถึงโดยสมควร ให้คู่กรณีที่เกี่ยวข้องสามารถตรวจสอบกรณีดังต่อไปนี้จากใบรับรองหรือจากวิธีอื่น

(ก) วิธีการที่ใช้ในการระบุตัวเจ้าของลายมือชื่อ

(ข) ข้อจำกัดเกี่ยวกับวัตถุประสงค์และคุณค่าที่มีการนำข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์หรือใบรับรอง

(ค) ข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์มีผลสมบูรณ์ใช้ได้และไม่สูญหาย ถูกทำลาย ถูกแก้ไข ถูกเปิดเผยโดยมิชอบ หรือถูกล่วงรู้โดยไม่สอดคล้องกับวัตถุประสงค์

(ง) ข้อจำกัดเกี่ยวกับขอบเขตความรับผิดที่ผู้ให้บริการออกใบรับรองได้ระบุไว้

(จ) การมีวิธีการให้เจ้าของลายมือชื่อส่งคำบอกกล่าวเมื่อมีเหตุตามมาตรา ๒๗ (๒)

(ฉ) การมีบริการเกี่ยวกับการเพิกถอนใบรับรองที่ทันการ

(๕) ในกรณีที่มีบริการตาม (๔) (จ) บริการนั้นต้องมีวิธีการที่ให้เจ้าของลายมือชื่อสามารถแจ้งได้ตามหลักเกณฑ์ที่กำหนดตามมาตรา ๒๗ (๒) และในกรณีที่มีบริการตาม (๔) (ฉ) บริการนั้นต้องสามารถเพิกถอนใบรับรองได้ทันการ

(๖) ใช้ระบบ วิธีการ และบุคลากรที่เชื่อถือได้ในการให้บริการ

มาตรา ๒๙ ในการพิจารณาความเชื่อถือได้ของระบบ วิธีการ และบุคลากรตามมาตรา ๒๘ (๖) ให้คำนึงถึงกรณีดังต่อไปนี้

(๑) สถานภาพทางการเงิน บุคลากร และสินทรัพย์ที่มีอยู่

(๒) คุณภาพของระบบฮาร์ดแวร์และซอฟต์แวร์

(๓) วิธีการออกใบรับรอง การขอใบรับรอง และการเก็บรักษาข้อมูลการให้บริการนั้น

(๔) การจัดให้มีข้อมูลข่าวสารเกี่ยวกับเจ้าของลายมือชื่อที่ระบุในใบรับรอง และผู้ที่อาจคาดหมายได้ว่าจะเป็นคู่กรณีที่เกี่ยวข้อง

(๕) ความสม่ำเสมอและขอบเขตในการตรวจสอบโดยผู้ตรวจสอบอิสระ

(๖) องค์กรที่ให้การรับรองหรือให้บริการออกใบรับรองเกี่ยวกับการปฏิบัติหรือการมีอยู่ของสิ่งที่กล่าวมาใน (๑) ถึง (๕)

(๗) กรณีใดๆ ที่คณะกรรมการประกาศกำหนด

มาตรา ๓๐ คู่กรณีที่เกี่ยวข้องต้องดำเนินการ ดังต่อไปนี้

(๑) ดำเนินการตามสมควรในการตรวจสอบความน่าเชื่อถือของลายมือชื่ออิเล็กทรอนิกส์

(๒) ในกรณีลายมือชื่ออิเล็กทรอนิกส์มีใบรับรอง ต้องมีการดำเนินการตามสมควร ดังนี้

(ก) ตรวจสอบความสมบูรณ์ของใบรับรอง การพักใช้ หรือการเพิกถอนใบรับรอง และ

(ข) ปฏิบัติตามข้อจำกัดใดๆ ที่เกี่ยวกับใบรับรอง

มาตรา ๓๑ ใบรับรองหรือลายมือชื่ออิเล็กทรอนิกส์ให้ถือว่ามีผลทางกฎหมายโดยไม่ต้องคำนึงถึง

(๑) สถานที่ออกใบรับรองหรือสถานที่สร้างหรือใช้ลายมือชื่ออิเล็กทรอนิกส์ หรือ

(๒) สถานที่ทำการงานของผู้ออกใบรับรองหรือเจ้าของลายมือชื่ออิเล็กทรอนิกส์

ใบรับรองที่ออกในต่างประเทศให้มีผลตามกฎหมายในประเทศเช่นเดียวกับใบรับรองที่ออกในประเทศ หากการออกใบรับรองดังกล่าวได้ใช้ระบบที่เชื่อถือได้ไม่น้อยกว่าระบบที่เชื่อถือได้ตามพระราชบัญญัตินี้

ลายมือชื่ออิเล็กทรอนิกส์ที่สร้างหรือใช้ในต่างประเทศให้ถือว่ามีผลตามกฎหมายในประเทศเช่นเดียวกับลายมือชื่ออิเล็กทรอนิกส์ที่สร้างหรือใช้ในประเทศ หากการสร้างหรือใช้ลายมือชื่ออิเล็กทรอนิกส์ดังกล่าวได้ใช้ระบบที่เชื่อถือได้ไม่น้อยกว่าระบบที่เชื่อถือได้ตามพระราชบัญญัตินี้

ในการพิจารณาว่าใบรับรองหรือลายมือชื่ออิเล็กทรอนิกส์ใดมีความเชื่อถือได้ตามวรรคสองหรือวรรคสาม ให้คำนึงถึงมาตรฐานระหว่างประเทศและปัจจัยอื่นๆ ที่เกี่ยวข้องประกอบด้วย

หมวด ๓

ธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์

มาตรา ๓๒ บุคคลย่อมมีสิทธิประกอบธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ แต่ในกรณีที่จำเป็นเพื่อรักษาความมั่นคงทางการเงินและการพาณิชย์ หรือเพื่อประโยชน์ในการเสริมสร้างความเชื่อถือและยอมรับในระบบข้อมูลอิเล็กทรอนิกส์ หรือเพื่อป้องกันความเสียหายต่อสาธารณชน ให้มีการตราพระราชกฤษฎีกากำหนดให้การประกอบธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ใดเป็นกิจการที่ต้องแจ้งให้ทราบ ต้องขึ้นทะเบียน หรือต้องได้รับใบอนุญาตก่อนก็ได้

ในการกำหนดให้กรณีใดต้องแจ้งให้ทราบ ต้องขึ้นทะเบียน หรือต้องได้รับใบอนุญาตตามวรรคหนึ่ง ให้กำหนดโดยพิจารณาจากความเหมาะสมในการป้องกันความเสียหายตามระดับความรุนแรงของผลกระทบที่อาจเกิดขึ้นจากการประกอบธุรกิจนั้น

ในการนี้ จะกำหนดให้หน่วยงานของรัฐแห่งหนึ่งแห่งใดเป็นผู้รับผิดชอบในการควบคุมดูแลในพระราชกฤษฎีกาดังกล่าวก็ได้

ก่อนเสนอให้ตราพระราชกฤษฎีกาตามวรรคหนึ่ง ต้องจัดให้มีการรับฟังความคิดเห็นของประชาชนตามความเหมาะสม และนำข้อมูลที่ได้รับมาประกอบการพิจารณา

มาตรา ๓๓ ในกรณีที่มีพระราชกฤษฎีกากำหนดให้การประกอบธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ใดเป็นกิจการที่ต้องแจ้งให้ทราบ หรือต้องขึ้นทะเบียน ให้ผู้ที่ประสงค์จะประกอบธุรกิจดังกล่าวต้องแจ้งหรือขึ้นทะเบียนต่อพนักงานเจ้าหน้าที่ตามที่กำหนดในพระราชกฤษฎีกาก่อนเริ่มประกอบธุรกิจนั้น

หลักเกณฑ์และวิธีการแจ้งหรือขึ้นทะเบียนตามวรรคหนึ่ง ให้เป็นไปตามที่กำหนดในพระราชกฤษฎีกา และเมื่อพนักงานเจ้าหน้าที่ตามที่กำหนดในพระราชกฤษฎีกาได้รับแจ้งหรือรับขึ้นทะเบียนให้ออกใบรับแจ้งหรือใบรับขึ้นทะเบียนเพื่อเป็นหลักฐานการแจ้งหรือการขึ้นทะเบียนในวันที่ได้รับแจ้งหรือรับขึ้นทะเบียน และให้ผู้แจ้งหรือผู้ขึ้นทะเบียนประกอบธุรกิจนั้นได้ตั้งแต่วันที่ได้รับแจ้งหรือรับขึ้นทะเบียน แต่ถ้าพนักงานเจ้าหน้าที่ตามที่กำหนดในพระราชกฤษฎีกาตรวจพบในภายหลังว่าการแจ้งหรือขึ้นทะเบียนไม่ถูกต้องหรือไม่ครบถ้วน ให้มีอำนาจสั่งผู้แจ้งหรือผู้ขึ้นทะเบียนแก้ไขให้ถูกต้องหรือครบถ้วนภายในเจ็ดวันนับแต่วันที่ได้รับคำสั่งดังกล่าว

ในการประกอบธุรกิจ ผู้แจ้งหรือผู้ขึ้นทะเบียนตามวรรคหนึ่งต้องปฏิบัติตามหลักเกณฑ์ที่กำหนดในพระราชกฤษฎีกาและตามที่คณะกรรมการประกาศกำหนด

ถ้าผู้แจ้งหรือผู้ขึ้นทะเบียนตามวรรคหนึ่งไม่แก้ไขการแจ้งหรือขึ้นทะเบียนให้ถูกต้องหรือครบถ้วนตามวรรคสอง หรือฝ่าฝืนหรือไม่ปฏิบัติตามหลักเกณฑ์การประกอบธุรกิจตามวรรคสาม ให้คณะกรรมการพิจารณามีคำสั่งลงโทษปรับทางปกครองไม่เกินหนึ่งล้านบาท โดยคำนึงถึงความร้ายแรงแห่งพฤติกรรมที่กระทำผิด และในกรณีที่เห็นสมควรคณะกรรมการอาจมีคำสั่งให้ผู้นั้นดำเนินการใดๆ เพื่อแก้ไขให้ถูกต้องหรือเหมาะสมได้

หลักเกณฑ์ในการพิจารณาลงโทษปรับทางปกครองให้เป็นไปตามที่คณะกรรมการกำหนด และถ้าผู้ถูกลงโทษปรับทางปกครองไม่ยอมชำระค่าปรับทางปกครอง ให้นำบทบัญญัติเกี่ยวกับการบังคับทางปกครองตามกฎหมายว่าด้วยวิธีปฏิบัติราชการทางปกครองมาใช้บังคับโดยอนุโลม และในกรณีไม่มีเจ้าหน้าที่ดำเนินการบังคับตามคำสั่ง ให้คณะกรรมการมีอำนาจฟ้องคดีต่อศาลปกครองเพื่อบังคับชำระค่าปรับ ในการนี้ ถ้าศาลปกครองเห็นว่าคำสั่งให้ชำระค่าปรับนั้นชอบด้วยกฎหมายก็ให้ศาลปกครองมีอำนาจพิจารณาพิพากษาและบังคับให้มีการยึดหรืออายัดทรัพย์สินขายทอดตลาดเพื่อชำระค่าปรับได้

ในกรณีผู้กระทำผิดตามวรรคสี่ไม่ดำเนินการแก้ไขตามคำสั่งของคณะกรรมการหรือกระทำความผิดซ้ำอีก ให้คณะกรรมการมีอำนาจออกคำสั่งห้ามมิให้ผู้นั้นประกอบธุรกิจตามที่ได้แจ้งหรือขึ้นทะเบียนอีกต่อไป

มาตรา ๓๔ ในกรณีที่มีพระราชกฤษฎีกากำหนดให้การประกอบธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์กรณีใดเป็นกิจการที่ต้องได้รับใบอนุญาต ให้ผู้ที่ประสงค์จะประกอบธุรกิจดังกล่าวยื่นคำขอรับใบอนุญาตต่อพนักงานเจ้าหน้าที่ตามที่กำหนดในพระราชกฤษฎีกา

คุณสมบัติของผู้ขอรับใบอนุญาต หลักเกณฑ์และวิธีการขออนุญาต การออกใบอนุญาต การต่ออายุใบอนุญาต การคืนใบอนุญาต และการสั่งพักใช้หรือเพิกถอนใบอนุญาต ให้เป็นไปตามหลักเกณฑ์ที่กำหนดในพระราชกฤษฎีกา

ในการประกอบธุรกิจ ผู้ได้รับใบอนุญาตตามวรรคหนึ่ง ต้องปฏิบัติตามหลักเกณฑ์ที่กำหนดในพระราชกฤษฎีกา ประกาศที่คณะกรรมการกำหนดหรือเงื่อนไขในใบอนุญาต

ในกรณีที่ผู้ได้รับใบอนุญาตฝ่าฝืนหรือปฏิบัติไม่ถูกต้องตามหลักเกณฑ์การประกอบธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ตามวรรคสาม ให้คณะกรรมการพิจารณามีคำสั่งลงโทษปรับทางปกครองไม่เกินสองล้านบาท โดยคำนึงถึงความร้ายแรงแห่งพฤติกรรมที่กระทำผิด และในกรณีที่เห็นสมควร คณะกรรมการอาจมีคำสั่งให้ผู้นั้นดำเนินการใดๆ เพื่อแก้ไขให้ถูกต้องหรือเหมาะสมได้ ทั้งนี้ ให้นำความในมาตรา ๓๓ วรรคห้า มาใช้บังคับโดยอนุโลม

ถ้าผู้กระทำความผิดตามวรรคสี่ไม่ดำเนินการแก้ไขตามคำสั่งของคณะกรรมการหรือกระทำความผิดซ้ำอีก ให้คณะกรรมการมีอำนาจออกคำสั่งเพิกถอนใบอนุญาต

หมวด ๔
ธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ

มาตรา ๓๕ คำขอ การอนุญาต การจดทะเบียน คำสั่งทางปกครอง การชำระเงิน การประกาศ หรือการดำเนินการใดๆ ตามกฎหมายกับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐ ถ้าได้กระทำในรูปของข้อมูลอิเล็กทรอนิกส์ตามหลักเกณฑ์และวิธีการที่กำหนดโดยพระราชกฤษฎีกา ให้นำพระราชบัญญัตินี้มาใช้บังคับและให้ถือว่ามีผล โดยชอบด้วยกฎหมายเช่นเดียวกับการดำเนินการตาม

หลักเกณฑ์และวิธีการที่กฎหมายในเรื่องนั้นกำหนด ทั้งนี้ ในพระราชกฤษฎีกาอาจกำหนดให้บุคคลที่เกี่ยวข้องต้องกระทำหรืองดเว้นกระทำการใดๆ หรือให้หน่วยงานของรัฐออกระเบียบเพื่อกำหนดรายละเอียดในบางกรณีด้วยก็ได้

ในการออกพระราชกฤษฎีกาตามวรรคหนึ่ง พระราชกฤษฎีกาดังกล่าวอาจกำหนดให้ผู้ประกอบธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ต้องแจ้งให้ทราบ ต้องขึ้นทะเบียน หรือต้องได้รับใบอนุญาต แล้วแต่กรณี ก่อนประกอบกิจการก็ได้ ในกรณีนี้ ให้นำบทบัญญัติในหมวด ๓ และบทกำหนดโทษที่เกี่ยวข้องมาใช้บังคับโดยอนุโลม

หมวด ๕
คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

มาตรา ๓๖[๕] ให้มีคณะกรรมการคณะหนึ่ง เรียกว่า “คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์” ประกอบด้วย รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เป็นประธานกรรมการ ปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เป็นรองประธานกรรมการ และกรรมการอื่นอีกจำนวนสิบสองคนซึ่งคณะรัฐมนตรีแต่งตั้งจากผู้ทรงคุณวุฒิด้านการเงิน ด้านการพาณิชย์อิเล็กทรอนิกส์ ด้านนิติศาสตร์ ด้านวิทยาการคอมพิวเตอร์ ด้านวิทยาศาสตร์หรือวิศวกรรมศาสตร์และด้านสังคมศาสตร์ ที่ได้รับการสรรหาด้านละสองคน ทั้งนี้ ผู้ทรงคุณวุฒิคนหนึ่งของแต่ละด้านต้องมาจากภาคเอกชน และให้หัวหน้าสำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์เป็นกรรมการและเลขานุการ

หลักเกณฑ์และวิธีการสรรหาและการเสนอชื่อบุคคลที่เห็นสมควรต่อคณะรัฐมนตรีเพื่อพิจารณาแต่งตั้งเป็นคณะกรรมการตามวรรคหนึ่ง ให้เป็นไปตามระเบียบที่รัฐมนตรีประกาศกำหนด

ให้เลขานุการแต่งตั้งผู้ช่วยเลขานุการอีกไม่เกินสองคน

มาตรา ๓๗ ให้คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ มีอำนาจหน้าที่ดังต่อไปนี้

(๑) เสนอแนะต่อคณะรัฐมนตรีเพื่อวางนโยบายการส่งเสริมและพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ ตลอดจนการแก้ไขปัญหาและอุปสรรคที่เกี่ยวข้อง

(๒) ติดตามดูแลการประกอบธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์

(๓) เสนอแนะหรือให้คำปรึกษาต่อรัฐมนตรีเพื่อการตราพระราชกฤษฎีกาตามพระราชบัญญัตินี้

(๔) ออกระเบียบหรือประกาศเกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์เพื่อให้เป็นไปตามพระราชบัญญัตินี้ หรือตามพระราชกฤษฎีกาที่ออกตามพระราชบัญญัตินี้

---

[๕] มาตรา ๓๖ วรรคหนึ่ง แก้ไขเพิ่มเติมโดยพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ ๒) พ.ศ. ๒๕๕๑

(๕) ปฏิบัติการอื่นใดเพื่อให้เป็นไปตามพระราชบัญญัตินี้ หรือกฎหมายอื่น

ในการปฏิบัติการตามพระราชบัญญัตินี้ให้คณะกรรมการเป็นเจ้าพนักงานตามประมวลกฎหมายอาญา

มาตรา ๓๘ กรรมการผู้ทรงคุณวุฒิมีวาระการดำรงตำแหน่งสามปี

กรรมการซึ่งพ้นจากตำแหน่งอาจได้รับแต่งตั้งอีกได้ แต่ไม่เกินสองวาระติดต่อกัน

มาตรา ๓๙ นอกจากการพ้นจากตำแหน่งตามวาระตามมาตรา ๓๘ กรรมการผู้ทรงคุณวุฒิพ้นจากตำแหน่ง เมื่อ

(๑) ตาย

(๒) ลาออก

(๓) คณะรัฐมนตรีให้ออกเพราะมีความประพฤติเสื่อมเสีย บกพร่อง หรือไม่สุจริตต่อหน้าที่ หรือหย่อนความสามารถ

(๔) เป็นคนไร้ความสามารถหรือคนเสมือนไร้ความสามารถ

(๕) ได้รับโทษจำคุกโดยต้องคำพิพากษาถึงที่สุดให้จำคุก เว้นแต่เป็นโทษสำหรับความผิดที่ได้กระทำโดยประมาทหรือความผิดลหุโทษ

มาตรา ๔๐ ในกรณีที่กรรมการผู้ทรงคุณวุฒิพ้นจากตำแหน่งตามมาตรา ๓๙ ให้ถือว่าคณะกรรมการประกอบด้วยกรรมการเท่าที่เหลืออยู่ และให้ดำเนินการแต่งตั้งกรรมการใหม่แทนภายในหกสิบวันนับแต่วันที่กรรมการพ้นจากตำแหน่ง

ให้กรรมการซึ่งได้รับแต่งตั้งแทนอยู่ในตำแหน่งเท่ากับวาระที่เหลืออยู่ของผู้ซึ่งตนแทน

มาตรา ๔๑ การประชุมของคณะกรรมการต้องมีกรรมการมาประชุมไม่น้อยกว่ากึ่งหนึ่งของจำนวนกรรมการทั้งหมดจึงเป็นองค์ประชุม

ถ้าประธานกรรมการไม่มาประชุมหรือไม่อาจปฏิบัติหน้าที่ได้ ให้คณะกรรมการเลือกกรรมการคนหนึ่งทำหน้าที่ประธานในที่ประชุม

การวินิจฉัยชี้ขาดของที่ประชุมให้ถือเสียงข้างมาก กรรมการคนหนึ่งให้มีเสียงหนึ่งในการลงคะแนน ถ้าคะแนนเสียงเท่ากันให้ประธานออกเสียงเพิ่มขึ้นอีกเสียงหนึ่งเป็นเสียงชี้ขาด

มาตรา ๔๒ คณะกรรมการมีอำนาจแต่งตั้งคณะอนุกรรมการเพื่อพิจารณาหรือปฏิบัติการอย่างหนึ่งอย่างใดแทนคณะกรรมการก็ได้

ให้นำความในมาตรา ๔๑ มาใช้บังคับแก่การประชุมของคณะอนุกรรมการโดยอนุโลม

มาตรา ๔๒/๑[๙] ให้คณะกรรมการได้รับเบี้ยประชุมและประโยชน์ตอบแทนอื่นตามหลักเกณฑ์ที่คณะรัฐมนตรีกำหนด

คณะอนุกรรมการที่คณะกรรมการแต่งตั้งตามมาตรา ๔๒ ให้ได้รับเบี้ยประชุมและประโยชน์ตอบแทนอื่นตามหลักเกณฑ์ที่คณะกรรมการกำหนด

มาตรา ๔๓[๑๐] ให้จัดตั้งสำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์เป็นส่วนราชการในสำนักงานปลัดกระทรวง กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ทำหน้าที่เป็นหน่วยงานธุรการของคณะกรรมการ

หมวด ๖
บทกำหนดโทษ

มาตรา ๔๔ ผู้ใดประกอบธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์โดยไม่แจ้งหรือขึ้นทะเบียนต่อพนักงานเจ้าหน้าที่ตามที่กำหนดในพระราชกฤษฎีกาตามมาตรา ๓๓ วรรคหนึ่ง หรือโดยฝ่าฝืน คำสั่งห้ามการประกอบธุรกิจของคณะกรรมการตามมาตรา ๓๓ วรรคหก ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

มาตรา ๔๕ ผู้ใดประกอบธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์โดยไม่ได้รับใบอนุญาตตามมาตรา ๓๔ ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสองแสนบาท หรือทั้งจำทั้งปรับ

มาตรา ๔๖ บรรดาความผิดตามพระราชบัญญัตินี้ที่กระทำโดยนิติบุคคล ผู้จัดการหรือผู้แทนนิติบุคคลหรือผู้ซึ่งมีส่วนร่วมในการดำเนินงานของนิติบุคคล ต้องรับผิดในความผิดนั้นด้วย เว้นแต่พิสูจน์ได้ว่าตนมิได้รู้เห็นหรือมีส่วนร่วมในการกระทำความผิดนั้น

ผู้รับสนองพระบรมราชโองการ

พันตำรวจโท ทักษิณ ชินวัตร
นายกรัฐมนตรี

---

[๙] มาตรา ๔๒/๑ เพิ่มโดยพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ ๒) พ.ศ. ๒๕๕๑

[๑๐] มาตรา ๔๓ แก้ไขเพิ่มเติมโดยพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ ๒) พ.ศ. ๒๕๕๑

หมายเหตุ :- เหตุผลในการประกาศใช้พระราชบัญญัติฉบับนี้ คือ โดยที่การทำธุรกรรมในปัจจุบันมีแนวโน้มที่จะปรับเปลี่ยนวิธีการในการติดต่อสื่อสารที่อาศัยการพัฒนาการเทคโนโลยีทางอิเล็กทรอนิกส์ซึ่งมีความสะดวก รวดเร็วและมีประสิทธิภาพ แต่เนื่องจากการทำธุรกรรมทางอิเล็กทรอนิกส์ดังกล่าวมีความแตกต่างจากวิธีการทำธุรกรรมซึ่งมีกฎหมายรองรับอยู่ในปัจจุบันเป็นอย่างมาก อันส่งผลให้ต้องมีการรองรับสถานะทางกฎหมายของข้อมูลทางอิเล็กทรอนิกส์ให้เสมอกับการทำเป็นหนังสือ หรือหลักฐานเป็นหนังสือ การรับรองวิธีการส่งและรับข้อมูลอิเล็กทรอนิกส์ การใช้ลายมือชื่ออิเล็กทรอนิกส์ ตลอดจนการรับฟังพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ เพื่อเป็นการส่งเสริมการทำธุรกรรมทางอิเล็กทรอนิกส์ให้น่าเชื่อถือ และมีผลในทางกฎหมายเช่นเดียวกับการทำธุรกรรมโดยวิธีการทั่วไปที่เคยปฏิบัติอยู่เดิมควรกำหนดให้มีคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ทำหน้าที่วางนโยบายกำหนดหลักเกณฑ์เพื่อส่งเสริมการทำธุรกรรมทางอิเล็กทรอนิกส์ ติดตามดูแลการประกอบธุรกิจเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ รวมทั้งมีหน้าที่ในการส่งเสริมการพัฒนาการทางเทคโนโลยีเพื่อติดตามความก้าวหน้าของเทคโนโลยี ซึ่งมีการเปลี่ยนแปลงและพัฒนาศักยภาพตลอดเวลาให้มีมาตรฐานน่าเชื่อถือ ตลอดจนเสนอแนะแนวทางแก้ไขปัญหาและอุปสรรคที่เกี่ยวข้องอันจะเป็นการส่งเสริมการใช้ธุรกรรมทางอิเล็กทรอนิกส์ทั้งภายในประเทศและระหว่างประเทศ ด้วยการมีกฎหมายรองรับในลักษณะที่เป็นเอกรูป และสอดคล้องกับมาตรฐานที่นานาประเทศยอมรับ จึงจำเป็นต้องตราพระราชบัญญัตินี้

*พระราชกฤษฎีกาแก้ไขบทบัญญัติให้สอดคล้องกับการโอนอำนาจหน้าที่ของส่วนราชการให้เป็นไปตามพระราชบัญญัติปรับปรุงกระทรวง ทบวง กรม พ.ศ. ๒๕๔๕ พ.ศ. ๒๕๔๕[๑๑]

มาตรา ๑๐๒ ในพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ ให้แก้ไขคำว่า “รัฐมนตรีว่าการกระทรวงวิทยาศาสตร์ เทคโนโลยีและสิ่งแวดล้อม” เป็น “รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร”

หมายเหตุ :- เหตุผลในการประกาศใช้พระราชกฤษฎีกาฉบับนี้ คือ โดยที่พระราชบัญญัติปรับปรุงกระทรวง ทบวง กรม พ.ศ. ๒๕๔๕ ได้บัญญัติให้จัดตั้งส่วนราชการขึ้นใหม่โดยมีภารกิจใหม่ ซึ่งได้มีการตราพระราชกฤษฎีกาโอนกิจการบริหารและอำนาจหน้าที่ของส่วนราชการให้เป็นไปตามพระราชบัญญัติปรับปรุงกระทรวง ทบวง กรม นั้นแล้ว และเนื่องจากพระราชบัญญัติดังกล่าวได้บัญญัติให้โอนอำนาจหน้าที่ของส่วนราชการ รัฐมนตรีผู้ดำรงตำแหน่งหรือผู้ซึ่งปฏิบัติหน้าที่ในส่วนราชการเดิมมาเป็นของส่วนราชการใหม่ โดยให้มีการแก้ไขบทบัญญัติต่างๆ ให้สอดคล้องกับอำนาจหน้าที่ที่โอนไปด้วย ฉะนั้น เพื่ออนุวัติให้เป็นไปตามหลักการที่ปรากฏในพระราชบัญญัติและพระราชกฤษฎีกาดังกล่าว จึงสมควรแก้ไขบทบัญญัติของกฎหมายให้สอดคล้องกับการโอนส่วนราชการ เพื่อให้ผู้เกี่ยวข้องมีความชัดเจนในการใช้กฎหมายโดยไม่ต้องไปค้นหาในกฎหมายโอนอำนาจหน้าที่ว่า

---

[๑๑] ราชกิจจานุเบกษา เล่ม ๑๑๙/ตอนที่ ๑๐๒ ก/หน้า ๖๖/๘ ตุลาคม ๒๕๔๕

ตามกฎหมายใดได้มีการโอนภารกิจของส่วนราชการหรือผู้รับผิดชอบตามกฎหมายนั้นไปเป็นของหน่วยงานใดหรือผู้ใดแล้ว โดยแก้ไขบทบัญญัติของกฎหมายให้มีการเปลี่ยนชื่อส่วนราชการ รัฐมนตรี ผู้ดำรงตำแหน่งหรือผู้ซึ่งปฏิบัติหน้าที่ของส่วนราชการให้ตรงกับการโอนอำนาจหน้าที่ และเพิ่มผู้แทนส่วนราชการในคณะกรรมการให้ตรงตามภารกิจที่มีการตัดโอนจากส่วนราชการเดิมมาเป็นของส่วนราชการใหม่รวมทั้งตัดส่วนราชการเดิมที่มีการยุบเลิกแล้ว ซึ่งเป็นการแก้ไขให้ตรงตามพระราชบัญญัติและพระราชกฤษฎีกาดังกล่าว จึงจำเป็นต้องตราพระราชกฤษฎีกานี้

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ ๒) พ.ศ. ๒๕๕๑[๑๒]

มาตรา ๑๑ ในระหว่างที่จัดตั้งสำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ตามมาตรา ๔๓ แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัตินี้ยังไม่แล้วเสร็จ ให้สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารรับผิดชอบทำหน้าที่หน่วยงานธุรการของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ไปพลางก่อน

ให้ปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารแต่งตั้งข้าราชการซึ่งดำรงตำแหน่งไม่ต่ำกว่าระดับแปดหรือเทียบเท่าในสังกัดสำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ทำหน้าที่เป็นหัวหน้าสำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ไปพลางก่อนจนกว่าการจัดตั้งสำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์จะแล้วเสร็จ

เพื่อประโยชน์ในการปฏิบัติงานตามวรรคหนึ่ง รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารจะสั่งให้ข้าราชการในสังกัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารมาปฏิบัติงานชั่วคราวในสำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารตามความจำเป็นก็ได้

มาตรา ๑๒ ให้นายกรัฐมนตรีและรัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารรักษาการตามพระราชบัญญัตินี้

หมายเหตุ :- เหตุผลในการประกาศใช้พระราชบัญญัติฉบับนี้ คือ เนื่องจากปัจจุบันกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ยังไม่มีบทบัญญัติรองรับในเรื่องตราประทับอิเล็กทรอนิกส์ ซึ่งเป็นสิ่งที่สามารถระบุถึงตัวผู้ทำธุรกรรมทางอิเล็กทรอนิกส์ได้เช่นเดียวกับลายมือชื่ออิเล็กทรอนิกส์ ทำให้เป็นอุปสรรคต่อการทำธุรกรรมทางอิเล็กทรอนิกส์ที่ต้องมีการประทับตราในหนังสือเป็นสำคัญ รวมทั้งยังไม่มีบทบัญญัติที่กำหนดให้สามารถนำเอกสารซึ่งเป็นสิ่งพิมพ์ออกของข้อมูลอิเล็กทรอนิกส์มาใช้แทนต้นฉบับหรือให้เป็นพยานหลักฐานในศาลได้ และโดยที่ได้มีการปรับปรุงโครงสร้างระบบราชการตามพระราชบัญญัติปรับปรุง กระทรวง ทบวง กรม พ.ศ. ๒๕๔๕ และกำหนดให้กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารเป็นหน่วยงานที่มีอำนาจหน้าที่เกี่ยวกับการวางแผน ส่งเสริม พัฒนา และ

[๑๒] ราชกิจจานุเบกษา เล่ม ๑๒๕/ตอนที่ ๓๓ ก/หน้า ๘๑/๑๓ กุมภาพันธ์ ๒๕๕๑

ดำเนินกิจการเกี่ยวกับเทคโนโลยีสารสนเทศและการสื่อสารประกอบกับปัจจุบันธุรกรรมทางอิเล็กทรอนิกส์ได้มีการใช้อย่างแพร่หลาย จำเป็นที่จะต้องมีหน่วยงานธุรการเพื่อทำหน้าที่กำกับดูแลเพื่อให้เป็นไปตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์และเป็นฝ่ายเลขานุการของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ โดยสมควรจัดตั้งสำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ สังกัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารขึ้นทำหน้าที่แทนศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ อันจะเป็นการส่งเสริมความเชื่อมั่นในการทำธุรกรรมทางอิเล็กทรอนิกส์ และเสริมสร้างศักยภาพการแข่งขันในเวทีการค้าระหว่างประเทศ สมควรแก้ไขเพิ่มเติมกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์เพื่อให้สอดคล้องกับหลักการดังกล่าว จึงจำเป็นต้องตราพระราชบัญญัตินี้

ภาคผนวก ๒

พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการ

ในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙

พระราชกฤษฎีกา

กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ

พ.ศ. ๒๕๔๙

ภูมิพลอดุลยเดช ป.ร.

ให้ไว้ ณ วันที่ ๒๖ พฤศจิกายน พ.ศ. ๒๕๔๙

เป็นปีที่ ๖๑ ในรัชกาลปัจจุบัน

พระบาทสมเด็จพระปรมินทรมหาภูมิพลอดุลยเดช มีพระบรมราชโองการโปรดเกล้า ฯ ให้ประกาศว่า

โดยที่เป็นการสมควรกำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ

อาศัยอำนาจตามความในมาตรา ๑๖ ของรัฐธรรมนูญแห่งราชอาณาจักรไทย (ฉบับชั่วคราว) พุทธศักราช ๒๕๔๙ และมาตรา ๓๕ วรรคหนึ่ง แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ จึงทรงพระกรุณาโปรดเกล้า ฯ ให้ตราพระราชกฤษฎีกาขึ้นไว้ ดังต่อไปนี้

มาตรา ๑ พระราชกฤษฎีกานี้เรียกว่า “พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙”

มาตรา ๒ พระราชกฤษฎีกานี้ให้ใช้บังคับตั้งแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

มาตรา ๓ ในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ หน่วยงานของรัฐต้องจัดให้มีระบบเอกสารที่ทำในรูปของข้อมูลอิเล็กทรอนิกส์ในลักษณะ ดังต่อไปนี้

(๑) เอกสารที่ทำในรูปของข้อมูลอิเล็กทรอนิกส์นั้นต้องอยู่ในรูปแบบที่เหมาะสม โดยสามารถแสดงหรืออ้างอิงเพื่อใช้ในภายหลังและยังคงความครบถ้วนของข้อความในรูปแบบของข้อมูลอิเล็กทรอนิกส์

(๒) ต้องกำหนดระยะเวลาเริ่มต้นและสิ้นสุดในการยื่นเอกสารที่ทำในรูปของข้อมูลอิเล็กทรอนิกส์ โดยปกติให้ยึดถือวันเวลาของการปฏิบัติงานหน่วยงานของรัฐนั้นเป็นหลัก และอาจกำหนดระยะเวลาในการดำเนินการพิจารณาของหน่วยงานของรัฐด้วยวิธีการทางอิเล็กทรอนิกส์ไว้ด้วยก็ได้ เว้นแต่จะมีกฎหมายในเรื่องนั้นกำหนดไว้เป็นอย่างอื่น

(๓) ต้องกำหนดวิธีการที่ทำให้สามารถระบุตัวเจ้าของลายมือชื่อ ประเภท ลักษณะหรือรูปแบบของลายมือชื่ออิเล็กทรอนิกส์ และสามารถแสดงได้ว่าเจ้าของลายมือชื่อรับรองข้อความในข้อมูลอิเล็กทรอนิกส์

(๔) ต้องกำหนดวิธีการแจ้งการตอบรับด้วยวิธีการทางอิเล็กทรอนิกส์หรือด้วยวิธีการอื่นใดเพื่อเป็นหลักฐานว่าได้มีการดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ไปยังอีกฝ่ายหนึ่งแล้ว

มาตรา ๔ นอกจากที่บัญญัติไว้ในมาตรา ๓ ในกรณีที่หน่วยงานของรัฐจัดทำกระบวนการพิจารณาทางปกครองโดยวิธีการทางอิเล็กทรอนิกส์ ระบบเอกสารที่ทำในรูปของข้อมูลอิเล็กทรอนิกส์ต้องมีลักษณะดังต่อไปนี้ด้วย เว้นแต่จะมีกฎหมายในเรื่องนั้นกำหนดไว้เป็นอย่างอื่น

(๑) มีวิธีการสื่อสารกับผู้ยื่นคำขอในกรณีที่เอกสารมีข้อบกพร่องหรือมีข้อความที่ผิดหลงอันเห็นได้ชัดว่าเกิดจากความไม่รู้หรือความเลินเล่อของผู้ยื่นคำขอ หรือการขอข้อเท็จจริงเพิ่มเติม รวมทั้งมีวิธีการแจ้งสิทธิและหน้าที่ในกระบวนการพิจารณาทางปกครองตามความจำเป็นแก่กรณีในกรณีที่กฎหมายกำหนดให้ต้องแจ้งให้คู่กรณีทราบ

(๒) ในกรณีมีความจำเป็นตามลักษณะเฉพาะของธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐใด หน่วยงานของรัฐนั้นอาจกำหนดเงื่อนไขว่าคู่กรณียินยอมตกลงและยอมรับการดำเนินการพิจารณาทางปกครองของหน่วยงานของรัฐโดยวิธีการทางอิเล็กทรอนิกส์

มาตรา ๕ หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้

แนวนโยบายและแนวปฏิบัติอย่างน้อยต้องประกอบด้วยเนื้อหา ดังต่อไปนี้

(๑) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

(๒) การจัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งาน และจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

(๓) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

มาตรา ๖ ในกรณีที่มีการรวบรวม จัดเก็บ ใช้ หรือเผยแพร่ข้อมูล หรือข้อเท็จจริงที่ทำให้สามารถระบุตัวบุคคล ไม่ว่าโดยตรงหรือโดยอ้อม ให้หน่วยงานของรัฐจัดทำแนวนโยบายและแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลด้วย

มาตรา ๗ แนวนโยบายและแนวปฏิบัติตามมาตรา ๕ และมาตรา ๖ ให้หน่วยงานของรัฐจัดทำเป็นประกาศ และต้องได้รับความเห็นชอบจากคณะกรรมการหรือหน่วยงานที่คณะกรรมการมอบหมาย จึงมีผลใช้บังคับได้

หน่วยงานของรัฐต้องปฏิบัติตามแนวนโยบายและแนวปฏิบัติที่ได้แสดงไว้ และให้จัดให้มีการตรวจสอบการปฏิบัติตามแนวนโยบายและแนวปฏิบัติที่กำหนดไว้อย่างสม่ำเสมอ

มาตรา ๘ ให้คณะกรรมการหรือหน่วยงานที่คณะกรรมการมอบหมายจัดทำแนวนโยบายและแนวปฏิบัติหรือการอื่นอันเกี่ยวกับการดำเนินการตามพระราชกฤษฎีกานี้ ไว้เป็นตัวอย่างเบื้องต้นสำหรับการดำเนินการของหน่วยงานของรัฐในการปฏิบัติตามพระราชกฤษฎีกานี้ และหากหน่วยงานของรัฐแห่งใดมีการปฏิบัติงานตามกฎหมายที่แตกต่างเป็นการเฉพาะแล้ว หน่วยงานของรัฐแห่งนั้นอาจเพิ่มเติมรายละเอียดการปฏิบัติงานตามกฎหมายที่แตกต่างนั้นได้โดยออกเป็นระเบียบ ทั้งนี้ โดยให้คำนึงถึงความถูกต้องครบถ้วน ความน่าเชื่อถือ สภาพความพร้อมใช้งาน และความมั่นคงปลอดภัยของระบบและข้อมูลอิเล็กทรอนิกส์

มาตรา ๙ การทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐตามหลักเกณฑ์และวิธีการตามพระราชกฤษฎีกานี้ ไม่มีผลเป็นการยกเว้นกฎหมายหรือหลักเกณฑ์และวิธีการที่กฎหมายในเรื่องนั้นกำหนดไว้เพื่อการอนุญาต อนุมัติ การให้ความเห็นชอบ หรือการวินิจฉัย

มาตรา ๑๐ ให้นายกรัฐมนตรีรักษาการตามพระราชกฤษฎีกานี้

ผู้รับสนองพระบรมราชโองการ
พลเอก สุรยุทธ์ จุลานนท์
นายกรัฐมนตรี

หมายเหตุ :- เหตุผลในการประกาศใช้พระราชกฤษฎีกาฉบับนี้ คือ เนื่องจากประเทศไทยได้เริ่มเข้าสู่ยุคสังคมสารสนเทศ ซึ่งมีการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐมากขึ้น สมควรสนับสนุนให้หน่วยงานของรัฐมีระบบการบริการของตน โดยการประยุกต์ใช้เทคโนโลยีสารสนเทศเพื่อให้สามารถบริการประชาชนได้อย่างทั่วถึง สะดวก และรวดเร็ว อันเป็นการเพิ่มประสิทธิภาพและประสิทธิผลของหน่วยงานของรัฐ พร้อมกับให้หน่วยงานของรัฐสามารถพัฒนาการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐภายใต้มาตรฐานและเป็นไปในทิศทางเดียวกัน และสร้างความเชื่อมั่นของประชาชนต่อการดำเนินกิจกรรมของรัฐด้วยวิธีการทางอิเล็กทรอนิกส์ ประกอบกับมาตรา ๓๕ วรรคหนึ่ง แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ บัญญัติว่า คำขอ การอนุญาต การจดทะเบียน คำสั่งทางปกครอง การชำระเงิน การประกาศหรือการดำเนินการใด ๆ ตามกฎหมายกับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐ ถ้าได้กระทำในรูปของข้อมูลอิเล็กทรอนิกส์ตามหลักเกณฑ์และวิธีการที่กำหนดโดยพระราชกฤษฎีกาแล้ว ให้ถือว่ามีผลโดยชอบด้วยกฎหมายเช่นเดียวกับการดำเนินการตามหลักเกณฑ์และวิธีการที่กฎหมายในเรื่องนั้นกำหนด จึงจำเป็นต้องตราพระราชกฤษฎีกานี้

ภาคผนวก ๓

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

เรื่อง

แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย

ด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ

พ.ศ. ๒๕๕๓

ด้วยปัญหาด้านการรักษาความมั่นคงปลอดภัยให้กับสารสนเทศมีความรุนแรงเพิ่มขึ้นทั้งในประเทศและต่างประเทศ อีกทั้งยังมีแนวโน้มที่จะส่งผลกระทบต่อภาครัฐและภาคธุรกิจมากขึ้น ทำให้ผู้ประกอบการ ตลอดจนองค์กร ภาครัฐ และภาคเอกชนที่มีการดำเนินงานใด ๆ ในรูปของข้อมูลอิเล็กทรอนิกส์ผ่านระบบสารสนเทศขององค์กร ขาดความเชื่อมั่นต่อการทำธุรกรรมทางอิเล็กทรอนิกส์ในทุกรูปแบบ ประกอบกับคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ตระหนักถึงความจำเป็นที่จะส่งเสริมและผลักดันให้ประเทศสามารถยกระดับการแข่งขันกับประเทศอื่น ๆ โดยการนำระบบสารสนเทศและการสื่อสารมาประยุกต์ใช้ประกอบการทำธุรกรรมทางอิเล็กทรอนิกส์อย่างแพร่หลาย จึงเห็นความสำคัญที่จะนำกฎหมาย ข้อบังคับต่าง ๆ มาบังคับใช้กับการทำธุรกรรมทางอิเล็กทรอนิกส์ทั้งในส่วนที่ต้องกระทำและในส่วนที่ต้องงดเว้นการกระทำ เพื่อช่วยให้การทำธุรกรรมทางอิเล็กทรอนิกส์ของหน่วยงานของรัฐมีความมั่นคงปลอดภัยและมีความน่าเชื่อถือ

เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐ หรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ ตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากล คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ จึงเห็นควรกำหนดแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ

อาศัยอำนาจตามความในมาตรา ๕ มาตรา ๗ และมาตรา ๘ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์จึงได้จัดทำประกาศฉบับนี้ เพื่อเป็นแนวทางเบื้องต้นให้หน่วยงานของรัฐใช้ในการกำหนดนโยบาย และข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ซึ่งอย่างน้อยต้องประกอบด้วยสาระสำคัญ ดังต่อไปนี้

ข้อ ๑ ในประกาศนี้

(๑) ผู้ใช้งาน หมายความว่า ข้าราชการ เจ้าหน้าที่ พนักงานของรัฐ ลูกจ้าง ผู้ดูแลระบบ ผู้บริหารขององค์กร ผู้รับบริการ ผู้ใช้งานทั่วไป

(๒) สิทธิของผู้ใช้งาน หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน

(๓) สินทรัพย์ (asset) หมายความว่า สิ่งใดก็ตามที่มีคุณค่าสำหรับองค์กร

(๔) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายความว่า การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

(๕) ความมั่นคงปลอดภัยด้านสารสนเทศ (information security) หมายความว่า การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability)

(๖) เหตุการณ์ด้านความมั่นคงปลอดภัย (information security event) หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

(๗) สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (information security incident) หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (unwanted or unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

ข้อ ๒ หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร ซึ่งอย่างน้อยต้องประกอบด้วยเนื้อหา ดังต่อไปนี้

(๑) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

(๒) จัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งานและจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

(๓) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

ข้อ ๓ หน่วยงานของรัฐต้องจัดให้มีข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน ซึ่งอย่างน้อยต้องประกอบด้วยกระบวนการ ดังต่อไปนี้

(๑) หน่วยงานของรัฐต้องจัดทำข้อปฏิบัติที่สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

(๒) หน่วยงานของรัฐต้องประกาศนโยบายและข้อปฏิบัติดังกล่าว ให้ผู้เกี่ยวข้องทั้งหมดทราบเพื่อให้สามารถเข้าถึง เข้าใจ และปฏิบัติตามนโยบายและข้อปฏิบัติได้

(๓) หน่วยงานของรัฐต้องกำหนดผู้รับผิดชอบตามนโยบายและข้อปฏิบัติดังกล่าวให้ชัดเจน

(๔) หน่วยงานของรัฐต้องทบทวนปรับปรุงนโยบายและข้อปฏิบัติให้เป็นปัจจุบันอยู่เสมอ

ข้อ ๔ ข้อปฏิบัติในด้านการรักษาความมั่นคงปลอดภัย ต้องมีเนื้อหาอย่างน้อยครอบคลุมตามข้อ ๕ - ๑๕

ข้อ ๕ ให้มีข้อกำหนดการเข้าถึงและควบคุมการใช้งานสารสนเทศ (access control) ซึ่งต้องมีเนื้อหาอย่างน้อย ดังนี้

(๑) หน่วยงานของรัฐต้องมีการควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

(๒) ในการกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง ต้องกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจของหน่วยงานของรัฐนั้น ๆ

(๓) หน่วยงานของรัฐต้องกำหนดเกี่ยวกับประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

ข้อ ๖ ให้มีข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (business requirements for access control) โดยแบ่งการจัดทำข้อปฏิบัติเป็น ๒ ส่วนคือ การควบคุมการเข้าถึงสารสนเทศ และการปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

ข้อ ๗ ให้มีการบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว และผ่านการฝึกอบรม หลักสูตรการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (information security awareness training) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต โดยต้องมีเนื้อหาอย่างน้อย ดังนี้

(๑) สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

(๒) การลงทะเบียนผู้ใช้งาน (user registration) ต้องกำหนดให้มีขั้นตอนทางปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานเมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว

(๓) การบริหารจัดการสิทธิของผู้ใช้งาน (user management) ต้องจัดให้มีการควบคุมและจำกัดสิทธิเพื่อเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่น ๆ ที่เกี่ยวข้องกับการเข้าถึง

(๔) การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (user password management) ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม

(๕) การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (review of user access rights) ต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศตามระยะเวลาที่กำหนดไว้

ข้อ ๘ ให้มีการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ โดยต้องมีเนื้อหาอย่างน้อย ดังนี้

(๑) การใช้งานรหัสผ่าน (password use) ต้องกำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ

(๒) การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ ต้องกำหนดข้อปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล

(๓) การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (clear desk and clear screen policy) ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูลคอมพิวเตอร์ หรือสารสนเทศ อยู่ในภาวะซึ่งเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

(๔) ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

ข้อ ๙ ให้มีการควบคุมการเข้าถึงเครือข่าย (network access control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต โดยต้องมีเนื้อหาอย่างน้อย ดังนี้

(๑) การใช้งานบริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(๒) การยืนยันตัวบุคคลสำหรับผู้ใช้ที่อยู่ภายนอกองค์กร (user authentication for external connections) ต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกองค์กรสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศขององค์กรได้

(๓) การระบุอุปกรณ์บนเครือข่าย (equipment identification in networks) ต้องมีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และควรใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน

(๔) การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (remote diagnostic and configuration port protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

(๕) การแบ่งแยกเครือข่าย (segregation in networks) ต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ

(๖) การควบคุมการเชื่อมต่อทางเครือข่าย (network connection control) ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างหน่วยงานให้สอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึง

(๗) การควบคุมการจัดเส้นทางบนเครือข่าย (network routing control) ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

ข้อ ๑๐ ให้มีการควบคุมการเข้าถึงระบบปฏิบัติการ (operating system access control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต โดยต้องมีเนื้อหาอย่างน้อย ดังนี้

(๑) การกำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

(๒) การระบุและยืนยันตัวตนของผู้ใช้งาน (user identification and authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง

(๓) การบริหารจัดการรหัสผ่าน (password management system) ต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ

(๔) การใช้งานโปรแกรมอรรถประโยชน์ (use of system utilities) ควรจำกัดและควบคุมการใช้งานโปรแกรมประเภทอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว

(๕) เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (session time-out)

(๖) การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (limitation of connection time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือแอพพลิเคชั่นที่มีความเสี่ยงหรือมีความสำคัญสูง

ข้อ ๑๑ ให้มีการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (application and information access control) โดยต้องมีการควบคุม ดังนี้

(๑) การจำกัดการเข้าถึงสารสนเทศ (information access restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้าใช้งานในการเข้าถึงสารสนเทศและฟังก์ชัน (functions) ต่าง ๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น ทั้งนี้โดยให้สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

(๒) ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อองค์กร ต้องได้รับการแยกออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ ให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกองค์กร (mobile computing and teleworking)

(๓) การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องกำหนดข้อปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

(๔) การปฏิบัติงานจากภายนอกสำนักงาน (teleworking) ต้องกำหนดข้อปฏิบัติ แผนงาน และขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานขององค์กรจากภายนอกสำนักงาน

ข้อ ๑๒ หน่วยงานของรัฐที่มีระบบสารสนเทศต้องจัดทำระบบสำรอง ตามแนวทางต่อไปนี้

(๑) ต้องพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม

(๒) ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

(๓) ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

(๔) ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองและระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ

(๕) สำหรับความถี่ของการปฏิบัติในแต่ละข้อ ควรมีการปฏิบัติที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน

ข้อ ๑๓ หน่วยงานของรัฐต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยต้องมีเนื้อหาอย่างน้อย ดังนี้

(๑) หน่วยงานของรัฐต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (information security audit and assessment) อย่างน้อยปีละ ๑ ครั้ง

(๒) ในการตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการ โดยผู้ตรวจสอบภายในหน่วยงานของรัฐ (internal auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (external auditor) เพื่อให้หน่วยงานของรัฐได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน

ข้อ ๑๔ หน่วยงานของรัฐต้องกำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจาก

ความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้ผู้บริหารระดับสูง ซึ่งมีหน้าที่ดูแลรับผิดชอบด้านสารสนเทศของหน่วยงานของรัฐเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

ข้อ ๑๕ หน่วยงานของรัฐสามารถเลือกใช้ข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ที่ต่างไปจากประกาศฉบับนี้ได้ หากแสดงให้เห็นว่า ข้อปฏิบัติที่เลือกใช้มีความเหมาะสมกว่า หรือเทียบเท่า

ข้อ ๑๖ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ประกาศ ณ วันที่ ๓๑ พฤษภาคม พ.ศ. ๒๕๕๓
ร้อยตรีหญิง ระนองรักษ์ สุวรรณฉวี
รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
ประธานกรรมการธุรกรรมทางอิเล็กทรอนิกส์

ภาคผนวก ๔

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

เรื่อง

แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย

ด้านสารสนเทศของหน่วยงานของรัฐ (ฉบับที่ ๒) พ.ศ. ๒๕๕๖

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย
ด้านสารสนเทศของหน่วยงานของรัฐ (ฉบับที่ ๒)
พ.ศ. ๒๕๕๖

โดยที่เป็นการสมควรปรับปรุงแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐให้สอดคล้องกับมาตรฐานสากล

อาศัยอำนาจตามความในมาตรา ๕ มาตรา ๗ และมาตรา ๘ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๙ คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ (ฉบับที่ ๒) พ.ศ. ๒๕๕๖”

ข้อ ๒ ให้ยกเลิกความในข้อ ๑๔ ของประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ และให้ใช้ความต่อไปนี้แทน

“ข้อ ๑๔ หน่วยงานของรัฐต้องกำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่องละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ทั้งนี้ ให้ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น”

ข้อ ๓ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ประกาศ ณ วันที่ ๒๕ มกราคม พ.ศ. ๒๕๕๖
นาวาอากาศเอก อนุดิษฐ์ นาครทรรพ
รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
ประธานกรรมการธุรกรรมทางอิเล็กทรอนิกส์

ภาคผนวก ๕

แบบประเมินประกอบการพิจารณาการดำเนินงานตาม แนวนโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัย ของหน่วยงานของรัฐ

แบบประเมินประกอบการพิจารณาการดำเนินงานตาม
แนวนโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัย ของหน่วยงานของรัฐ
ตามมาตรา ๗ ใน พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙

ชื่อหน่วยงานผู้นำเสนอ .....

เอกสารประกอบการพิจารณา .....**(สามารถแนบเพิ่มเติมได้)**

.....

หมายเหตุ : กรณีที่กรรมการธุรกรรมทางอิเล็กทรอนิกส์ หรืออนุกรรมการมีความเกี่ยวข้องกับข้อเสนอที่กำลังพิจารณา จะต้องแสดงตนและไม่เข้าร่วมในการพิจารณาให้ข้อคิดเห็นหรือมีส่วนร่วมในการประเมิน เพื่อหลีกเลี่ยงปัญหาการมีผลประโยชน์ทับซ้อน (Conflicts of Interest)

ข้อ	แนวนโยบาย / และแนวปฏิบัติ (ประกาศของคณะกรรมการ)	หน่วยงานประเมินตนเอง		ความเห็นจาก ธอ. เห็นด้วย/ไม่เห็นด้วย	ความเห็นจากอนุกรรมการความมั่นคงฯ
		ผ่าน/ไม่ผ่าน	อ้างอิงหน้า... / ระบุเหตุผล (ถ้ามี)		
๑	**กำหนดคำนิยาม**				
	(๑) ผู้ใช้งาน				
	(๒) สิทธิของผู้ใช้งาน				
	(๓) สินทรัพย์				
	(๔) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ				
	(๕) ความมั่นคงปลอดภัยด้านสารสนเทศ				
	(๖) เหตุการณ์ด้านความมั่นคงปลอดภัย				
	(๗) สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด				
	(๘) คำนิยามอื่น ๆ ตามความต้องการขององค์กร				
๒	**หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร ซึ่งอย่างน้อยต้องประกอบด้วยเนื้อหาดังต่อไปนี้**				
	(๑) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ				
	(๒) จัดให้มีระบบสารสนเทศและระบบสำรองของ				

ข้อ	แนวนโยบาย / และแนวปฏิบัติ (ประกาศของคณะกรรมการ)	หน่วยงานประเมินตนเอง		ความเห็นจาก ธอ. เห็นด้วย/ไม่เห็นด้วย	ความเห็นจากอนุกรรมการความมั่นคงฯ
		ผ่าน/ไม่ผ่าน	อ้างอิงหน้า... / ระบุเหตุผล (ถ้ามี)		
	สารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งานและจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่าง ต่อเนื่อง				
	(๓) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ				
๓	**หน่วยงานของรัฐต้องจัดให้มีข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน ซึ่งอย่างน้อยต้องประกอบด้วยกระบวนการ ดังต่อไปนี้**				
	(๑) หน่วยงานของรัฐต้องจัดทำข้อปฏิบัติที่สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน				
	(๒) หน่วยงานของรัฐต้องประกาศนโยบายและข้อปฏิบัติดังกล่าว ให้ผู้เกี่ยวข้องทั้งหมดทราบ เพื่อให้สามารถเข้าถึง เข้าใจ และปฏิบัติตามนโยบายและข้อปฏิบัติได้				
	(๓) หน่วยงานของรัฐต้องกำหนดผู้รับผิดชอบตามนโยบายและข้อปฏิบัติดังกล่าวให้ชัดเจน				
	(๔) หน่วยงานของรัฐต้องทบทวนปรับปรุงนโยบายและข้อปฏิบัติให้เป็นปัจจุบันอยู่เสมอ				
๔	**ข้อปฏิบัติในด้านการรักษาความมั่นคงปลอดภัย ต้องมีเนื้อหา อย่างน้อยครอบคลุมตามข้อ ๕ – ๑๕**				
๕	**ให้มีข้อกำหนดการเข้าถึงและควบคุมการใช้งานสารสนเทศ (access control) ซึ่งต้องมีเนื้อหาอย่างน้อย ดังนี้**				
	(๑) หน่วยงานของรัฐต้องมีการควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย				

ข้อ	แนวนโยบาย / และแนวปฏิบัต (ประกาศของคณะกรรมการ)	หน่วยงานประเมินตนเอง		ความเห็นจาก ธอ. เห็นด้วย/ไม่เห็นด้วย	ความเห็นจากอนุกรรมการ ความมั่นคงฯ
		ผ่าน/ไม่ผ่าน	อ้างอิงหน้า... / ระบุเหตุผล (ถ้ามี)		
	(๒) ในการกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง ต้องกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจของหน่วยงานของรัฐนั้น ๆ				
	(๓) หน่วยงานของรัฐต้องกำหนดเกี่ยวกับ - ประเภทของข้อมูล - ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล - รวมทั้งระดับชั้นการเข้าถึง - เวลาที่ได้เข้าถึง - และช่องทางการเข้าถึง				
๖	**ให้มีข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (business requirements for access control) โดยแบ่งการจัดทำข้อปฏิบัติเป็น 2 ส่วนคือ การควบคุมการเข้าถึงสารสนเทศ และ การปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย**				
๗	**ให้มีการบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว และผ่านการฝึกอบรม หลักสูตรการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (information security awareness training) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต โดยต้องมีเนื้อหาอย่างน้อย ดังนี้**				
	(๑) สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม				

ข้อ	แนวนโยบาย / และแนวปฏิบัติ (ประกาศของคณะกรรมการ)	หน่วยงานประเมินตนเอง		ความเห็นจาก ธอ. เห็นด้วย/ไม่เห็นด้วย	ความเห็นจากอนุกรรมการความมั่นคงฯ
		ผ่าน/ไม่ผ่าน	อ้างอิงหน้า... / ระบุเหตุผล (ถ้ามี)		
	(๒) การลงทะเบียนผู้ใช้งาน (user registration) ต้องกำหนดให้มีขั้นตอนทางปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานเมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว				
	(๓) การบริหารจัดการสิทธิของผู้ใช้งาน (user management) ต้องจัดให้มีการควบคุมและจำกัดสิทธิเพื่อเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่น ๆ ที่เกี่ยวข้องกับการเข้าถึง				
	(๔) การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (user password management) ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม				
	(๕) การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (review of user access rights) ต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศตามระยะเวลาที่กำหนดไว้				
๘	**ให้มีการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ โดยต้องมีเนื้อหาอย่างน้อย ดังนี้**				
	(๑) การใช้งานรหัสผ่าน (password use) ต้องกำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ				

ข้อ	แนวนโยบาย / และแนวปฏิบัติ (ประกาศของคณะกรรมการ)	หน่วยงานประเมินตนเอง		ความเห็นจาก ธอ. เห็นด้วย/ไม่เห็นด้วย	ความเห็นจากอนุกรรมการความมั่นคงฯ
		ผ่าน/ไม่ผ่าน	อ้างอิงหน้า... / ระบุเหตุผล (ถ้ามี)		
	(๒) การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ต้องกำหนดข้อปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล				
	(๓) การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (clear desk and clear screen policy) ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์ หรือสารสนเทศ อยู่ในภาวะซึ่งเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน				
	(๔) ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ.๒๕๔๔				
๙	**ให้มีการควบคุมการเข้าถึงเครือข่าย (network access control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต โดยต้องมีเนื้อหาอย่างน้อย ดังนี้**				
	(๑) การใช้งานบริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น				
	(๒) การยืนยันตัวบุคคลสำหรับผู้ใช้ที่อยู่ภายนอกองค์กร (user authentication for external connections) ต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกองค์กรสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศขององค์กรได้				

ข้อ	แนวนโยบาย / และแนวปฏิบัติ (ประกาศของคณะกรรมการ)	หน่วยงานประเมินตนเอง		ความเห็นจาก ธอ. เห็นด้วย/ไม่เห็นด้วย	ความเห็นจากอนุกรรมการ ความมั่นคงฯ
		ผ่าน/ไม่ผ่าน	อ้างอิงหน้า... / ระบุเหตุผล (ถ้ามี)		
	(๓) การระบุอุปกรณ์บนเครือข่าย (equipment identification in networks) ต้องมีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และควรใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน				
	(๔) การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (remote diagnostic and configuration port protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ ทั้งการเข้าถึงทางกายภาพและทางเครือข่าย				
	(๕) การแบ่งแยกเครือข่าย (segregation in networks) ต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ				
	(๖) การควบคุมการเชื่อมต่อทางเครือข่าย (network connection control) ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างหน่วยงานให้สอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึง				
	(๗) การควบคุมการจัดเส้นทางบนเครือข่าย (network routing control) ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ				
๑๐	**ให้มีการควบคุมการเข้าถึงระบบปฏิบัติการ (operating system access control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต โดยต้องมีเนื้อหาอย่างน้อย ดังนี้**				

ข้อ	แนวนโยบาย / และแนวปฏิบัติ (ประกาศของคณะกรรมการ)	หน่วยงานประเมินตนเอง		ความเห็นจาก ธอ. เห็นด้วย/ไม่เห็นด้วย	ความเห็นจากอนุกรรมการความมั่นคงฯ
		ผ่าน/ไม่ผ่าน	อ้างอิงหน้า... / ระบุเหตุผล (ถ้ามี)		
	(๑) การกำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย				
	(๒) การระบุและยืนยันตัวตนของผู้ใช้งาน (user identification and authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง				
	(๓) การบริหารจัดการรหัสผ่าน (password management system) ต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ				
	(๔) การใช้งานโปรแกรมอรรถประโยชน์ (use of system utilities) ควรจำกัดและควบคุมการใช้งานโปรแกรมประเภทอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว				
	(๕) เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (session time-out)				
	(๖) การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (limitation of connection time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือแอพพลิเคชั่นที่มีความเสี่ยงหรือมีความสำคัญสูง				

ข้อ	แนวนโยบาย / และแนวปฏิบัต (ประกาศของคณะกรรมการ)	หน่วยงานประเมินตนเอง		ความเห็นจาก ธอ. เห็นด้วย/ไม่เห็นด้วย	ความเห็นจากอนุกรรมการ ความมั่นคงฯ
		ผ่าน/ไม่ผ่าน	อ้างอิงหน้า... / ระบุเหตุผล (ถ้ามี)		
๑๑	**ให้มีการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (application and information access control) โดยต้องมีการควบคุมดังนี้**				
	(๑) การจำกัดการเข้าถึงสารสนเทศ (information access restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้าใช้งานในการเข้าถึงสารสนเทศและฟังก์ชัน (functions) ต่างๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น ทั้งนี้โดยให้สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้				
	(๒) ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อองค์กร ต้องได้รับการแยกออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ ให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกองค์กร (mobile computing and teleworking)				
	(๓) การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ต้องกำหนดข้อปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่				
	(๔) การปฏิบัติงานจากภายนอกสำนักงาน (teleworking) ต้องกำหนดข้อปฏิบัติ แผนงาน และขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานขององค์กรจากภายนอกสำนักงาน				

ข้อ	แนวนโยบาย / และแนวปฏิบัติ (ประกาศของคณะกรรมการ)	หน่วยงานประเมินตนเอง		ความเห็นจาก ธอ. เห็นด้วย/ไม่เห็นด้วย	ความเห็นจากอนุกรรมการความมั่นคงฯ
		ผ่าน/ไม่ผ่าน	อ้างอิงหน้า... / ระบุเหตุผล (ถ้ามี)		
๑๒	**หน่วยงานของรัฐที่มีระบบสารสนเทศต้องจัดทำระบบสำรอง ตามแนวทางต่อไปนี้**				
	(๑) ต้องพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม				
	(๒) ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ				
	(๓) ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์				
	(๔) ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ (โปรดระบุความถี่)				
	(๕) สำหรับความถี่ของการปฏิบัติในแต่ละข้อ ควรมีการปฏิบัติที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน				
๑๓	**หน่วยงานของรัฐต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศโดยต้องมีเนื้อหาอย่างน้อย ดังนี้**				
	(๑) หน่วยงานของรัฐต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (information security audit and assessment) อย่างน้อยปีละ ๑ ครั้ง				

ข้อ	แนวนโยบาย / และแนวปฏิบัติ (ประกาศของคณะกรรมการ)	หน่วยงานประเมินตนเอง		ความเห็นจาก ธอ. เห็นด้วย/ไม่เห็นด้วย	ความเห็นจากอนุกรรมการความมั่นคงฯ
		ผ่าน/ไม่ผ่าน	อ้างอิงหน้า... / ระบุเหตุผล (ถ้ามี)		
	(๒) ในการตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการ โดยผู้ตรวจสอบภายในหน่วยงานของรัฐ (internal auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (external auditor) เพื่อให้หน่วยงานของรัฐได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน				
๑๔	**หน่วยงานของรัฐต้องกำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิด ความเสียหายหรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ** ทั้งนี้ให้ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Office : CEO) **เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น**				

โปรดระบุเพื่อรับทราบ ☐ กรณีหน่วยงานมีเอกสารที่เป็นความลับ ไม่จำเป็นต้องจัดส่งเอกสาร แต่ให้นำมาชี้แจงประกอบการพิจารณาของคณะกรรมการ

ขอรับรองว่าข้อความที่แจ้งไว้ในแบบฟอร์มนี้ถูกต้อง เป็นความจริงทุกประการ และสอดคล้องตามแนวนโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัย ของหน่วยงานภาครัฐ ตามมาตรา ๗ ใน พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙

ลงชื่อ ..... (ผู้บริหารสูงสุด/ผู้ที่ได้รับมอบอำนาจ)
(.....)
ตำแหน่ง .....
ลงวันที่ .....

เรียน ผู้อำนวยการสำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

ความเห็นของผู้ประเมินเบื้องต้น ☐ เห็นสมควรให้ความเห็นชอบ ☐ เห็นสมควรให้มีการปรับแก้ (ระบุรายละเอียด)

.....

.....

.....

ลงชื่อ .....

(.....)

ตำแหน่ง ผู้อำนวยการกลุ่มงานผลักดันธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ

ลงวันที่ .....

เรียน คณะอนุกรรมการความมั่นคงปลอดภัย

ความเห็นของผู้อำนวยการสำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ☐ เห็นสมควรให้ความเห็นชอบ ☐ เห็นสมควรให้มีการปรับแก้ (ระบุรายละเอียด)

.....

.....

.....

ลงชื่อ .....

(.....)

ตำแหน่ง ผู้อำนวยการสำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

ลงวันที่ .....

เรียน คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

ความเห็นของคณะอนุกรรมการความมั่นคงปลอดภัย ☐ เห็นสมควรให้ความเห็นชอบ ☐ เห็นสมควรให้มีการปรับแก้ (ระบุรายละเอียด)

.....

.....

.....

ลงชื่อ .....

(.....)

ตำแหน่ง ประธานคณะอนุกรรมการความมั่นคงปลอดภัย

ลงวันที่ .....

บันทึก

บันทึก

บันทึก

บันทึก