Electronic Transactions Commission

MINISTRY OF ICT
Smart Thailand

รวมกฎหมาย เกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ และกฎหมายที่เกี่ยวข้อง

สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
รวบรวมและจัดพิมพ์ พ.ศ. ๒๕๕๖

Electronic Transactions Commission

MINISTRY OF ICT
Smart Thailand

รวมกฎหมาย
เกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์
และกฎหมายที่เกี่ยวข้อง

สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
รวบรวมและจัดพิมพ์ พ.ศ. ๒๕๕๖

ชื่อหนังสือ **รวมกฎหมายเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์และกฎหมายที่เกี่ยวข้อง**

หน่วยงานที่เผยแพร่ สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
๑๒๐ หมู่ ๓ ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา
อาคารรัฐประศาสนภักดี ชั้น ๖ ถนนแจ้งวัฒนะ เขตหลักสี่
กรุงเทพมหานคร ๑๐๒๑๐
โทรศัพท์ ๐ ๒๑๔๑ ๖๙๘๕-๙๙
โทรสาร ๐ ๒๑๔๓ ๘๐๓๖-๓๗
เว็บไซต์กระทรวงฯ : http://www.mict.go.th
เว็บไซต์คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ :
http://www.etcommission.go.th

ISBN : ๙๗๘-๙๗๔-๙๗๖๕-๕๑-๗

พิมพ์ครั้งที่ ๑	พ.ศ. ๒๕๕๓	๘,๐๐๐	เล่ม
พิมพ์ครั้งที่ ๒	พ.ศ. ๒๕๕๔	๕๐๐	เล่ม
พิมพ์ครั้งที่ ๓	พ.ศ. ๒๕๕๔	๒,๒๐๐	เล่ม
พิมพ์ครั้งที่ ๔	พ.ศ. ๒๕๕๖	๕๐๐	เล่ม
พิมพ์ครั้งที่ ๕	พ.ศ. ๒๕๕๖	๗๐๐	เล่ม
พิมพ์ครั้งที่ ๖	พ.ศ. ๒๕๕๗	๖๐๐	เล่ม
พิมพ์ครั้งที่ ๗	พ.ศ. ๒๕๕๘	๖๐๐	เล่ม

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

คำนำ

ในการดำรงชีวิตประจำวันของเราทุกคนต้องอยู่ภายใต้หลักเกณฑ์ของกฎหมายที่รัฐได้ตราขึ้น เพื่อความสงบเรียบร้อยของสังคมทั้งทางตรงและทางอ้อม กฎหมายที่ออกมาบังคับใช้ในปัจจุบันมีมากมายหลายฉบับยากที่จะจดจำได้ทั้งหมด แต่ผู้ปฏิบัติงานจำเป็นอย่างยิ่งที่จะต้องรู้และเข้าใจอย่างถ่องแท้ในเนื้อหาสาระของกฎหมายที่เกี่ยวข้อง เพื่อให้งานหรือกิจการนั้นๆ บรรลุวัตถุประสงค์ตามเป้าหมายอย่างมีประสิทธิภาพและประสิทธิผล

หนังสือเล่มนี้เป็นการรวบรวมกฎหมายที่เกี่ยวข้องกับธุรกรรมทางอิเล็กทรอนิกส์และเทคโนโลยีสารสนเทศไว้เพื่อประโยชน์ในการศึกษาอ้างอิงและการปฏิบัติงานของบุคคลที่เกี่ยวข้อง ซึ่งหวังเป็นอย่างยิ่งว่าจะเป็นประโยชน์ต่อทุกท่าน

คณะผู้จัดทำ

สารบัญ

พระราชบัญญัติว่าด้วยธุรกรรม
ทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔

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 ผู้รับข้อมูลมีสิทธิถือว่าข้อมูลอิเล็กทรอนิกส์ที่ได้รับนั้นถูกต้องตามเจตนาของผู้ส่งข้อมูลและสามารถดำเนินการไปตามข้อมูลอิเล็กทรอนิกส์นั้นได้ 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) ผู้ส่งข้อมูลอาจส่งคำบอกกล่าวไปยังผู้รับข้อมูลว่าตนยังมิได้รับการตอบแจ้งการรับและกำหนดระยะเวลาอันสมควรให้ผู้รับข้อมูลตอบแจ้งการรับ 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[๑] 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

---

[๑] 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

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
เรื่อง แนวทางการจัดทำแนวนโยบาย
(Certificate Policy) และ
แนวปฏิบัติ (Certification Practice Statement)
ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์
(Certification Authority)
พ.ศ. ๒๕๕๒

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

เรื่อง แนวทางการจัดทำแนวนโยบาย (Certificate Policy) และ
แนวปฏิบัติ (Certification Practice Statement)
ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Certification Authority)
พ.ศ. ๒๕๕๒

เพื่อให้การให้บริการของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์มีความน่าเชื่อถือ ตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากล คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ จึงเห็นควรกำหนดแนวทางในการจัดทำแนวนโยบาย (Certificate Policy) และแนวปฏิบัติ (Certification Practice Statement) ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Certification Authority)

อาศัยอำนาจตามความในมาตรา ๒๘ (๖) มาตรา ๒๙ (๗) และมาตรา ๓๗ (๔) แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ให้ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Certification Authority) จัดทำแนวนโยบาย (Certificate Policy) และแนวปฏิบัติ (Certification Practice Statement) ตามแนวทางการจัดทำแนวนโยบาย (Certificate Policy) และแนวปฏิบัติ (Certification Practice Statement) ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Certification Authority) ท้ายประกาศนี้

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ประกาศ ณ วันที่ ๘ ตุลาคม พ.ศ. ๒๕๕๒
ร้อยตรีหญิง ระนองรักษ์ สุวรรณฉวี
รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
ประธานกรรมการธุรกรรมทางอิเล็กทรอนิกส์

แนวทางการจัดทำแนวนโยบาย (Certificate Policy) และ
แนวปฏิบัติ (Certification Practice Statement)
ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Certification Authority)

๑. บทนำ

ในการนำใบรับรองอิเล็กทรอนิกส์ (Electronic Certificate) ที่ออกโดยผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Certification Authority) เพื่อให้ผู้ใช้บริการสามารถนำไปใช้ในการรับรองตัวบุคคลผู้ถือใบรับรองสำหรับใช้ในการสร้างลายมือชื่อดิจิทัล (Digital Signature) อันเป็นลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้ประเภทหนึ่ง หรือสำหรับการรับรองความมีตัวตนของนิติบุคคล หรือรับรองเครื่องให้บริการหรือเซิร์ฟเวอร์ (Server) หรือเอนทิตี (Entity) อื่นใดก็ตาม ด้วยการประยุกต์ใช้เทคโนโลยีโครงสร้างพื้นฐานกุญแจสาธารณะ (Public Key Infrastructure หรือเทคโนโลยี PKI) นั้น ความน่าเชื่อถือของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ นับว่ามีส่วนสำคัญยิ่งต่อการใช้บริการและก่อให้เกิดผลผูกพันทางกฎหมายในธุรกรรมต่าง ๆ ที่ทำขึ้นโดยมีการนำใบรับรองอิเล็กทรอนิกส์ไปใช้ยืนยันหรือรับรองตัวบุคคล นิติบุคคล เครื่องให้บริการหรือเซิร์ฟเวอร์ หรือเอนทิตีใดก็ตาม ในการทำธุรกรรมแต่ละครั้ง

เพื่อให้การให้บริการของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ มีความน่าเชื่อถือ หน่วยงานที่ชื่อว่า Internet Engineering Task Force หรือ IETF ซึ่งทำการพัฒนาสถาปัตยกรรมทางอินเทอร์เน็ต (Internet Architecture) จึงได้กำหนดกรอบหรือแนวทางในการทำแนวนโยบายและแนวปฏิบัติของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ขึ้น เรียกว่า Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC 3647) อันเป็นมาตรฐานที่ได้รับการยอมรับในระดับสากล จึงได้นำมาใช้เป็นแนวทางในการจัดทำประกาศฉบับนี้สำหรับใช้ปฏิบัติในการจัดทำแนวนโยบายและแนวปฏิบัติของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ในประเทศไทย เพื่อให้สอดคล้องตามมาตรฐานสากล

๒. คำนิยาม (Definition) และคำย่อ (Acronym)

ในส่วนนี้แสดงถึงคำนิยามและคำย่อเพื่อให้ความหมายกับคำที่ถูกใช้ในเอกสารนี้อย่างเข้าใจได้ถูกต้องตรงกัน

คำ/คำย่อ	คำนิยาม
RFC	“The Internet Request For Comments” เป็นชุดเอกสารที่เขียนเพื่อนิยามหรือบรรยายตามความเป็นจริงปัจจุบันและแนะนำแนวปฏิบัติเกี่ยวกับเกณฑ์วิธี (Protocol) และนโยบายของอินเทอร์เน็ต เป็นต้น

คำ/คำย่อ	คำนิยาม
บุคคล	บุคคลธรรมดา หรือนิติบุคคล
เอนทิตี	บุคคลและรวมถึงเครื่องให้บริการ (Server) หรือเว็บไซต์ หรือหน่วยปฏิบัติงาน (Operating Unit/Site) หรือเครื่องมืออื่นใด (Device) ที่อยู่ภายใต้การควบคุมของบุคคล
Certificate Revocation List (CRL)	รายการเพิกถอนใบรับรองอิเล็กทรอนิกส์ คือ รายการใบรับรองอิเล็กทรอนิกส์ที่ถูกเพิกถอนการใช้งาน
Online Certificate Status Protocol (OCSP)	เกณฑ์วิธี (Protocol) สำหรับตรวจสอบสถานะของการเพิกถอนใบรับรอง หรือวันเวลาที่เริ่มต้นและสิ้นสุดการใช้ใบรับรอง
Object Identifier (OID)	ค่าสัมพันธ์ซึ่งบ่งบอกถึงข้อมูลสารสนเทศของวัตถุ (Information Object) ใดๆ โดยเป็นค่าที่สามารถบ่งชี้ได้ถึงความเป็นหนึ่งเดียวของ Object นั้นๆ
กุญแจสาธารณะ Public Key	กุญแจที่ใช้ในการตรวจสอบลายมือชื่อดิจิทัล และสามารถนำไปใช้ในการเข้ารหัสลับข้อมูลอิเล็กทรอนิกส์ เพื่อมิให้สามารถเข้าใจความหมายของข้อมูลอิเล็กทรอนิกส์ที่มีการเข้ารหัสลับนั้นได้ เพื่อประโยชน์ในการรักษาความลับของข้อมูลอิเล็กทรอนิกส์นั้น
กุญแจส่วนตัว Private Key	กุญแจที่ใช้ในการสร้างลายมือชื่อดิจิทัล และสามารถนำไปใช้ในการถอดรหัสลับเมื่อมีการเข้ารหัสลับข้อมูลอิเล็กทรอนิกส์ เพื่อให้สามารถเข้าใจความหมายของข้อมูลอิเล็กทรอนิกส์ที่มีการเข้ารหัสลับนั้นได้
คู่กุญแจ Key Pair	กุญแจส่วนตัวและกุญแจสาธารณะในระบบการเข้ารหัสลับแบบอสมมาตรที่ได้สร้างขึ้นโดยวิธีการที่ทำให้กุญแจส่วนตัวมีความสัมพันธ์ในทางคณิตศาสตร์กับกุญแจสาธารณะในลักษณะที่สามารถใช้กุญแจสาธารณะตรวจสอบได้ว่าลายมือชื่อดิจิทัลได้สร้างขึ้นโดยใช้กุญแจส่วนตัวนั้นหรือไม่ และสามารถนำกุญแจสาธารณะไปใช้ในการเข้ารหัสลับข้อมูลอิเล็กทรอนิกส์ ทำให้ไม่สามารถเข้าใจความหมายของข้อมูลอิเล็กทรอนิกส์ได้เพื่อประโยชน์ในการรักษาความลับของข้อมูลอิเล็กทรอนิกส์ เว้นแต่บุคคลที่ถือกุญแจส่วนตัวซึ่งสามารถนำกุญแจส่วนตัวของตนใช้ในการถอดรหัสลับของข้อมูลอิเล็กทรอนิกส์ เพื่อให้เจ้าของกุญแจส่วนตัวสามารถอ่านหรือเข้าใจความหมายของข้อมูลอิเล็กทรอนิกส์นั้นได้

คำ/คำย่อ	คำนิยาม
เจ้าหน้าที่รับลงทะเบียน Registration Authority (RA)	ผู้ซึ่งทำหน้าที่รับลงทะเบียนเมื่อมีการยื่นคำขอใช้บริการ แจ้งเพิกถอนใบรับรองอิเล็กทรอนิกส์ หรือต่ออายุใบรับรองอิเล็กทรอนิกส์ โดยทำการตรวจสอบและยืนยันความถูกต้องของข้อมูลที่ผู้ใช้บริการให้ไว้
พฤติการณ์ที่กระทบต่อความมั่นคงปลอดภัยของข้อมูล (Compromise)	หมายถึง การที่ข้อมูลสูญหาย ถูกทำลาย ถูกแก้ไข ถูกเปิดเผยโดยมิชอบ หรือถูกล่วงรู้โดยไม่สอดคล้องกับวัตถุประสงค์ของการเก็บรักษาข้อมูลนั้น รวมทั้งกรณีที่มีเหตุอันควรสงสัยว่าจะมีพฤติการณ์ดังกล่าว

๓. หัวข้อที่ต้องกำหนดไว้ในแนวนโยบาย และ แนวปฏิบัติ

บทที่ ๑ บทนำ (Introduction)

บทที่ ๒ ความรับผิดชอบในการเผยแพร่ข้อมูลและการเก็บรักษาข้อมูล (Publication and Repository Responsibilities)

บทที่ ๓ การระบุและการยืนยันตัวบุคคล (Identification and Authentication)

บทที่ ๔ ข้อกำหนดเกี่ยวกับการดำเนินการตลอดอายุของใบรับรองอิเล็กทรอนิกส์ (Certificate Life-Cycle Operation Requirements)

บทที่ ๕ การควบคุมความมั่นคงปลอดภัยของเครื่องมืออุปกรณ์ การบริหารจัดการ และการดำเนินงาน (Facility, Management, and Operational Controls)

บทที่ ๖ การควบคุมความมั่นคงปลอดภัยด้านเทคนิค (Technical Security Controls)

บทที่ ๗ การกำหนดรูปแบบของใบรับรองอิเล็กทรอนิกส์ รายการเพิกถอน และสถานะของใบรับรองอิเล็กทรอนิกส์ (Certificate, CRL, and OCSP Profiles)

บทที่ ๘ การตรวจสอบการปฏิบัติตามกฎข้อบังคับต่างๆ และการประเมินความเสี่ยงอื่นๆ (Compliance Audit and Other Assessment)

บทที่ ๙ ข้อกำหนดอื่นๆ และประเด็นกฎหมาย (Other Business and Legal Matters)

๔. เนื้อหาที่ต้องกำหนดไว้ในแนวนโยบาย และแนวปฏิบัติ

บทที่ ๑ บทนำ (Introduction)

เนื้อหาในบทนี้ จะกล่าวถึงประเภทของบุคคลหรือเอนทิตีที่เกี่ยวข้องและการนำแนวนโยบายหรือแนวปฏิบัติไปใช้งาน

๑. ข้อมูลเบื้องต้นทั่วไป (Overview)

สาระสำคัญของเนื้อหาในข้อนี้ คือ การกล่าวถึงแนวนโยบายและแนวปฏิบัติ โดยทั่วๆ ไป และการนำแนวนโยบายและแนวปฏิบัติที่จัดทำขึ้นไปปรับใช้เมื่อมีการประยุกต์ใช้ PKI เช่น กรณีที่มีการกำหนดระดับความน่าเชื่อถือของใบรับรองอิเล็กทรอนิกส์ที่แตกต่างกัน ใบรับรองซึ่งแตกต่างกันนั้นอาจมีความซับซ้อนหรืออาจมีการกำหนดขอบเขตการใช้ PKI ที่แตกต่างกัน ดังนั้น การแสดงข้อมูลเกี่ยวกับโครงสร้างของ PKI จึงมีประโยชน์ต่อการทำความเข้าใจเนื้อหาในส่วนนี้

๒. ชื่อเอกสาร (Document Name and Identification)

เนื้อหาในส่วนนี้จะกำหนดเกี่ยวกับ “ชื่อ” สำหรับใช้เรียกแนวนโยบายและแนวปฏิบัติ หรือเรียกสิ่งหนึ่งสิ่งใด (Other Identifier) ทั้งนี้ รวมถึงการเรียกชื่อเอกสารหรือสิ่งที่ระบุถึงเช่นว่านั้นในทางเทคนิคด้วย กล่าวคือ จำเป็นต้องมีการจดทะเบียนเลข OID ซึ่งมีชื่อเรียกอย่างเป็นทางการว่า “ASN.1 Object Identifier ” ในทางปฏิบัติการกำหนดเลข OID ของแนวนโยบายและแนวปฏิบัติ หรือสิ่งหนึ่งสิ่งใดนั้นก็เพื่อให้สามารถตรวจสอบได้ว่าแนวนโยบายและแนวปฏิบัติ หรือสิ่งอื่นที่ถูกระบุถึงและกำกับด้วยเลข OID นั้น มีอยู่จริง เนื่องจากเลข OID จะเป็นตัวเลขซึ่งมีความสัมพันธ์หรือเชื่อมโยงถึง Information Object ใดๆ ลักษณะการกำหนดเลข OID จะมีการจัดเรียงลำดับตัวเลขกันและคั่นตัวเลขด้วยจุด โดยมีหน่วยงานรับจดทะเบียนเลข OID จำนวนหลายหน่วยงานด้วยกัน ได้แก่ American National Standard Institute (ANSI) สหรัฐอเมริกา, ISO เป็นต้น

๓. บุคคลที่เกี่ยวข้อง (PKI Participants)

เนื้อหาในบทนี้ควรจะกำหนดลักษณะ (Identity) ประเภทของบุคคลหรือเอนทิตี (Entity) ที่เกี่ยวข้อง รวมทั้งกำหนดบทบาทและหน้าที่ของบุคคลหรือเอนทิตีเหล่านั้นด้วย

๓.๑ ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Certification Authority)

คือ ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ ซึ่งสร้างและออกใบรับรองอิเล็กทรอนิกส์เพื่อรับรองกุญแจสาธารณะให้กับผู้ใช้บริการ

๓.๒ เจ้าหน้าที่รับลงทะเบียน (Registration Authority)

คือ บุคคลหรือเอนทิตี ที่ทำหน้าที่ในการตรวจสอบตัวบุคคลผู้สมัครขอใช้บริการ ทั้งในขั้นตอนที่มีการระบุตัวบุคคลผู้สมัครขอใช้บริการ (Identification) ว่าผู้สมัครขอใช้บริการเป็นใคร หรือเอนทิตีใดและขั้นตอนการยืนยันหรือพิสูจน์ตัวบุคคล (Authentication) ว่า ผู้สมัครขอใช้บริการหรือเอนทีตีอื่นใด

เป็นบุคคลหรือเอนทิตีนั้นจริง นอกจากนั้นผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ หรือเจ้าหน้าที่รับลงทะเบียน จะทำหน้าที่ทำนองเดียวกันในการเพิกถอนใบรับรอง หรือต่ออายุใบรับรอง โดยทำการตรวจสอบและยืนยันความถูกต้องของข้อมูลที่ผู้สมัครขอใช้บริการได้ให้ไว้ในขั้นตอนต่างๆ หลังจากตรวจสอบความถูกต้องของข้อมูลผู้สมัครขอใช้บริการเรียบร้อยแล้ว จึงแจ้งให้ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ ออกใบรับรองให้กับผู้สมัครขอใช้บริการต่อไป ทั้งนี้เจ้าหน้าที่รับลงทะเบียน อาจเป็นบุคลากรของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ หรืออาจเป็นบุคลากรของผู้สมัครขอใช้บริการ หรืออาจเป็นหน่วยงานหรือเอนทิตีอื่นที่ได้ทำข้อตกลงกับเจ้าหน้าที่รับลงทะเบียน เพื่อทำหน้าที่ดังกล่าว

๓.๓ ผู้ใช้บริการ (Subscriber)

คือ บุคคล หรือเอนทิตีใดๆ ที่ได้รับใบรับรองจากผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์

๓.๔ คู่กรณีที่เกี่ยวข้อง (Relying Party)

คือ บุคคล หรือเอนทิตีอื่นใดที่เชื่อถือลายมือชื่อดิจิทัล อันเป็นลายมือชื่ออิเล็กทรอนิกส์ชนิดหนึ่ง หรือเชื่อถือใบรับรองอิเล็กทรอนิกส์ ดังนั้น คู่กรณีที่เกี่ยวข้องอาจเป็นผู้ใช้บริการจากผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ หรืออาจไม่ใช่ผู้ใช้บริการจากผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ก็ได้ แต่เป็นผู้ซึ่งกระทำการหรืองดเว้นกระทำการใดๆ เพราะเชื่อถือใบรับรองอิเล็กทรอนิกส์หรือลายมือชื่อดิจิทัล โดยการใช้กุญแจสาธารณะที่อยู่ในใบรับรองนั้นในการตรวจสอบตัวตนที่แท้จริงของผู้ขอใช้บริการซึ่งเป็นเจ้าของลายมือชื่อดิจิทัลและมีชื่อปรากฏอยู่ในใบรับรองอิเล็กทรอนิกส์

๓.๕ บุคคลซึ่งเกี่ยวข้องอื่นๆ (Other Participants)

คือ บุคคล หรือเอนทิตีอื่น นอกจากที่กล่าวถึงข้างต้น เช่น ผู้ให้บริการในการเก็บรักษาข้อมูล (Providers of Repository Services) หรือผู้ได้รับการว่าจ้างโดยการ Outsource ให้เป็นผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ เป็นต้น

๓.๖ การใช้ใบรับรองอิเล็กทรอนิกส์ (Certificate Usage)

เนื้อหาในส่วนนี้ควรกำหนดเกี่ยวกับลักษณะหรือประเภทของใบรับรองอิเล็กทรอนิกส์ที่มีการนำไปใช้ในทางปฏิบัติ เช่น ใบรับรองอิเล็กทรอนิกส์เพื่อรับรองตัวบุคคล ใบรับรองอิเล็กทรอนิกส์เพื่อรับรองตัวนิติบุคคล ใบรับรองอิเล็กทรอนิกส์เพื่อรับรองเว็บไซต์ ใบรับรองอิเล็กทรอนิกส์เพื่อรับรองเครื่องให้บริการหรือเซิร์ฟเวอร์ ใบรับรองอิเล็กทรอนิกส์เพื่อใช้กับจดหมายอิเล็กทรอนิกส์หรืออีเมล์ ใบรับรองอิเล็กทรอนิกส์สำหรับใช้กับสัญญาหรือการทำข้อตกลง เป็นต้น

ทั้งนี้ ในกรณีที่มีข้อจำกัดการใช้งาน หรือกรณีที่มีการจัดระดับความน่าเชื่อถือของใบรับรองอิเล็กทรอนิกส์ ก็ควรระบุไว้ให้ชัดเจนด้วย และหากลักษณะการใช้งานหรือชนิดของใบรับรองอิเล็กทรอนิกส์มีความแตกต่างกันจนจำเป็นต้องจัดทำแนวนโยบายหรือแนวปฏิบัติสำหรับการใช้งานแต่ละลักษณะหรือตามชนิดของใบรับรอง ก็จำเป็นต้องให้ข้อมูลในเรื่องดังกล่าวเอาไว้ชัดเจนด้วยเช่นกัน

๓.๗ การบริหารจัดการเกี่ยวกับแนวนโยบายและแนวปฏิบัติ (Policy Administration)

เนื้อหาในส่วนนี้ควรกล่าวถึงชื่อ ที่อยู่ของหน่วยงานที่ยกร่าง จดทะเบียน ดูแลและปรับปรุงเอกสารแนวนโยบายและแนวปฏิบัติ นอกจากนั้นยังรวมถึง ชื่อ ที่อยู่ของจดหมายอิเล็กทรอนิกส์ หมายเลขโทรศัพท์ หมายเลขโทรสารของผู้ที่สามารถติดต่อได้ ทั้งนี้ โดยอาจกำหนดเป็นตำแหน่งที่รับผิดชอบในการตอบข้อซักถามหรือติดต่อกับผู้ใช้บริการของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ ก็ได้

นอกจากนั้น เพื่อสร้างความน่าเชื่อถือให้กับการให้บริการของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์เอง ในกรณีที่ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ ได้จัดทำแนวนโยบายและแนวปฏิบัติ ตามแนวทางที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ประกาศกำหนดแล้ว ควรระบุถึงคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ และที่อยู่ของหน่วยงานธุรการของคณะกรรมการไว้ในข้อนี้ด้วย

๓.๘ คำนิยามและคำย่อ (Definitions and Acronyms)

โดยที่ในการจัดทำแนวนโยบายและแนวปฏิบัติ จำเป็นต้องมีการกล่าวถึงคำศัพท์ และคำย่อเป็นจำนวนมาก ดังนั้น ในบทนี้จึงควรมีการให้ความหมายของคำศัพท์หรือคำย่อเหล่านั้นไว้ด้วย เช่น การให้ความหมายของคำว่าผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ เจ้าหน้าที่รับลงทะเบียนผู้ใช้บริการ แนวนโยบายและแนวปฏิบัติ ลายมือชื่อดิจิทัล ใบรับรองอิเล็กทรอนิกส์ คู่กุญแจ กุญแจส่วนตัว กุญแจสาธารณะ เอนทิตี เป็นต้น เพื่อเป็นข้อมูลให้กับผู้ใช้บริการต่อไป

บทที่ ๒ ความรับผิดชอบในการเผยแพร่ข้อมูลและการเก็บรักษาข้อมูล (Publication and Repository Responsibilities)

สำหรับเนื้อหาในส่วนนี้ ควรจะต้องระบุเกี่ยวกับบุคคลซึ่งทำหน้าที่ในการเก็บรักษาข้อมูล (Repository) ในการให้บริการของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ ไม่ว่าผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์จะทำหน้าที่ดังกล่าวนั้นเอง หรือเป็นการใช้บริการจากผู้ให้บริการรายอื่น และความรับผิดชอบของบุคคลหรือหน่วยงานที่ทำหน้าที่ในการเผยแพร่ข้อมูลเกี่ยวกับแนวนโยบาย และแนวปฏิบัติ รวมทั้งเนื้อหาที่จะมีการเผยแพร่ เช่น การควบคุมมาตรการในการรักษาความมั่นคงปลอดภัย (Security Controls) การรักษาความลับทางการค้า (Trade Secret) สำหรับข้อมูลสำคัญที่มีความอ่อนไหว เป็นต้น

นอกจากนั้น ควรให้ข้อมูลเกี่ยวกับความถี่หรือความบ่อยในการเผยแพร่ข้อมูล การควบคุมการเข้าถึงข้อมูลที่มีการเผยแพร่นั้น (Access Control) รวมทั้งแนวนโยบายและแนวปฏิบัติใบรับรองอิเล็กทรอนิกส์ หรือสถานะของใบรับรองอิเล็กทรอนิกส์ รวมทั้งการเพิกถอนใบรับรองอิเล็กทรอนิกส์

บทที่ ๓ การระบุและการยืนยันตัวบุคคล ((Identification and Authentication (I&A))

สำหรับเนื้อหาในบทนี้ควรให้ข้อมูลเกี่ยวกับขั้นตอนในการยืนยันหรือพิสูจน์ตัวบุคคล หรือเอนทิตีของผู้สมัครขอใช้บริการกับผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ หรือเจ้าหน้าที่รับลงทะเบียนก่อนที่จะมีการออกใบรับรองอิเล็กทรอนิกส์ รวมทั้งกำหนดขั้นตอนในการยืนยันหรือพิสูจน์บุคคลของ

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ หรือเจ้าหน้าที่รับลงทะเบียน หรือเอนทิตีที่เกี่ยวข้องกับการให้บริการหรือร่วมให้บริการกับผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ นอกจากนั้น อาจให้ข้อมูลเกี่ยวกับการออกใบรับรองอิเล็กทรอนิกส์ใหม่ การต่ออายุใบรับรองอิเล็กทรอนิกส์ หรือการเพิกถอนใบรับรองอิเล็กทรอนิกส์ไปพร้อมกันด้วย อย่างไรก็ตาม เนื้อหาที่พึงกำหนดไว้ในบทนี้นอกจากที่กล่าวถึงข้างต้น มีดังต่อไปนี้

๑. การกำหนดรูปแบบของชื่อ (Naming)

สำหรับการกำหนดรูปแบบของชื่อที่ใช้ (Naming Convention) เพื่อระบุถึงผู้ใช้บริการนั้น ควรกำหนด ดังนี้

๑.๑ รูปแบบของชื่อ เช่น X.500 Distinguished Name หรือ RFC 822 Names สำหรับจดหมายอิเล็กทรอนิกส์หรืออีเมล์ (e-mail) และ X.400 สำหรับชื่อ

๑.๒ ชื่อนั้น จะมีความหมายหรือไม่มีก็ได้

๑.๓ การกำหนดชื่อของผู้ใช้บริการในกรณีที่มีการใช้ชื่อนิรนามหรือนามแฝงหรือปิดบังชื่อที่แท้จริง (Anonymous or Pseudonymous)

๑.๔ กฎในการแปลงชื่อในรูปแบบต่างๆ เช่น มาตรฐาน X.500 และ RFC 822 เป็นต้น

๑.๕ ชื่อนั้นจะต้องมีลักษณะเฉพาะ (Unique Name)

๒. ความสมบูรณ์ในการระบุตัวบุคคล (Initial Identity Validation)

ข้อมูลในส่วนนี้ ควรจะกำหนดเกี่ยวกับวิธีการระบุตัวบุคคล (Identification) และยืนยันหรือพิสูจน์ตัวบุคคล (Authentication) เมื่อแรกเริ่มลงทะเบียนกับผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ เจ้าหน้าที่รับลงทะเบียน ผู้ใช้บริการ หรือคู่กรณีที่เกี่ยวข้องอื่นๆ ทั้งนี้ โดย

๒.๑ การยืนยันหรือพิสูจน์ความสัมพันธ์ของกุญแจส่วนตัวกับกุญแจสาธารณะที่ถือหรือครอบครองอยู่โดยผู้ใช้บริการ เช่น การใช้ในการพิสูจน์ลายมือชื่อดิจิทัลที่ปรากฏในใบรับรองอิเล็กทรอนิกส์ด้วยการใช้ลายมือชื่อดิจิทัลในการส่ง Certificate Request Message มายังผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ เป็นต้น

๒.๒ การยืนยันหรือพิสูจน์เงื่อนไขสำหรับการตรวจสอบความมีอยู่ขององค์กรหรือหน่วยงาน เช่น การตรวจสอบจากหนังสือรับรองของบริษัทหรือนิติบุคคลที่ออกโดยกรมพัฒนาธุรกิจการค้า กระทรวงพาณิชย์ เป็นต้น

๒.๓ การยืนยันหรือพิสูจน์เงื่อนไขสำหรับการตรวจสอบข้อมูลของบุคคลซึ่งกระทำการในนามขององค์กรหรือหน่วยงาน เช่น การตรวจสอบจากหนังสือมอบอำนาจ เป็นต้น

๓. การระบุและยืนยันหรือพิสูจน์ตัวบุคคลเมื่อมีการขอออกกุญแจใหม่ (Identification and Authentication for Re-key Requests)

สำหรับขั้นตอนนี้ จะครอบคลุมทั้งในขั้นตอนที่ใบรับรองอิเล็กทรอนิกส์หมดอายุลงและกรณีมีการเพิกถอนการใช้ใบรับรองอิเล็กทรอนิกส์ ดังนั้น จึงควรจะเป็นขั้นตอนที่มีรูปแบบการทำงานทำนองเดียวกันกับการระบุและยืนยันหรือพิสูจน์ตัวบุคคลเหมือนกับขั้นตอนแรกที่ได้มีการขอใช้บริการ

๔. การระบุและยืนยันหรือพิสูจน์ตัวบุคคลเมื่อมีการขอเพิกถอนใบรับรองอิเล็กทรอนิกส์ (Identification and Authentication for Revocation Requests)

เพื่อระบุประเภทของบุคคลที่สามารถทำการร้องขอเพิกถอนใบรับรองอิเล็กทรอนิกส์และขั้นตอนในการยืนยันหรือพิสูจน์ข้อมูลที่แสดงตัวตนของบุคคลดังกล่าวรวมทั้งสิทธิของบุคคลนั้น

บทที่ ๔ ข้อกำหนดเกี่ยวกับการดำเนินการตลอดอายุของใบรับรองอิเล็กทรอนิกส์ (Certificate Life-Cycle Operation Requirements)

ข้อมูลในส่วนนี้ใช้ในการระบุข้อกำหนดในการดำเนินการเกี่ยวกับใบรับรองอิเล็กทรอนิกส์สำหรับผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ เจ้าหน้าที่รับลงทะเบียน ผู้ใช้บริการ และบุคคลที่เกี่ยวข้องอื่นๆ ให้สอดคล้องกับบทบาทและหน้าที่ของตน

๑. การยื่นคำขอใบรับรองอิเล็กทรอนิกส์ (Certificate Application)

ส่วนนี้ควรระบุข้อกำหนดเกี่ยวกับการสมัครขอใบรับรองอิเล็กทรอนิกส์ดังต่อไปนี้

๑.๑ บุคคลที่สามารถสมัครขอใบรับรองอิเล็กทรอนิกส์ได้ เช่น ผู้ที่จะมีชื่อในใบรับรองอิเล็กทรอนิกส์ (Certificate Subject) หรือ RA เป็นต้น

๑.๒ กระบวนการยื่นคำขอใบรับรองอิเล็กทรอนิกส์ และภาระหน้าที่ที่เกี่ยวข้อง ตัวอย่างของกระบวนการยื่นขอใบรับรองอิเล็กทรอนิกส์ อาจเป็นดังต่อไปนี้

(๑) ผู้ส่งคำขอใบรับรองสร้างคู่กุญแจและส่งคำขอใบรับรองอิเล็กทรอนิกส์ให้เจ้าหน้าที่รับลงทะเบียน โดยผู้ส่งคำขอใบรับรองต้องให้ข้อมูลที่ครบถ้วนและถูกต้องตามระเบียบการขอใบรับรองอิเล็กทรอนิกส์ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์

(๒) เจ้าหน้าที่รับลงทะเบียนตรวจคำขอ และลงลายมือชื่อกำกับคำขอที่ผ่านการตรวจสอบแล้วไปให้ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ เจ้าหน้าที่รับลงทะเบียน และผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ ต้องกำหนดหลักการและวิธีการขอใบรับรองอิเล็กทรอนิกส์

๒. การพิจารณาคำขอใบรับรองอิเล็กทรอนิกส์ (Certificate Application Processing)

เนื้อหาส่วนนี้ควรให้ข้อมูลเกี่ยวกับกระบวนการพิจารณาคำขอใบรับรองอิเล็กทรอนิกส์ ตัวอย่างกระบวนการ เช่น

๒.๑ ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์และเจ้าหน้าที่รับลงทะเบียนจะดำเนินการตรวจสอบความถูกต้องของผู้สมัคร เพื่อการระบุและยืนยันตัวบุคคล

๒.๒ ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์และเจ้าหน้าที่รับลงทะเบียนจะพิจารณาว่าจะอนุมัติหรือไม่อนุมัติการสมัครขอใช้บริการใบรับรองอิเล็กทรอนิกส์

๒.๓ การกำหนดระยะเวลาที่ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ และเจ้าหน้าที่รับลงทะเบียนใช้ในการพิจารณาการยื่นคำขอใบรับรองอิเล็กทรอนิกส์

๓. การออกใบรับรองอิเล็กทรอนิกส์ (Certificate Issuance)

เนื้อหาส่วนนี้ควรให้ข้อมูลเกี่ยวกับกระบวนการออกใบรับรองอิเล็กทรอนิกส์ในประเด็นต่างๆ ดังต่อไปนี้

๓.๑ ข้อปฏิบัติของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ ในการออกใบรับรองอิเล็กทรอนิกส์ เช่น การตรวจลายมือชื่อและอำนาจกระทำการของ เจ้าหน้าที่รับลงทะเบียน ตลอดจนการสร้างใบรับรองอิเล็กทรอนิกส์

๓.๒ วิธีการแจ้งผลการออกใบรับรองอิเล็กทรอนิกส์แก่ผู้ใช้บริการ เช่น การแจ้งทางจดหมายอิเล็กทรอนิกส์

๔. การยอมรับใบรับรองอิเล็กทรอนิกส์ (Certificate Acceptance)

๔.๑ ข้อปฏิบัติของผู้สมัครขอใบรับรองอิเล็กทรอนิกส์ที่ถือเป็นการยอมรับใบรับรองอิเล็กทรอนิกส์ เช่น ผู้สมัครขอใบรับรองอิเล็กทรอนิกส์ยอมรับใบรับรองอิเล็กทรอนิกส์ที่ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ ออกให้ในกรณีที่

(๑) ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ มิได้รับการแจ้งการใดๆ จากผู้สมัครขอใบรับรองอิเล็กทรอนิกส์ภายในเวลาที่กำหนด

(๒) ผู้ใช้บริการลงลายมือชื่อกำกับข้อความแจ้งการยอมรับหรือไม่ยอมรับใบรับรองอิเล็กทรอนิกส์

๔.๒ การเผยแพร่ใบรับรองอิเล็กทรอนิกส์ที่ได้ยอมรับโดยผู้สมัครขอใบรับรองอิเล็กทรอนิกส์แล้ว ซึ่งอาจเผยแพร่โดยผ่านทาง X.500 Directory หรือ LDAP repository

๔.๓ การแจ้งให้บุคคลอื่นทราบถึงใบรับรองอิเล็กทรอนิกส์ที่ได้ออกให้ผู้สมัครขอใบรับรองอิเล็กทรอนิกส์ เช่น ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ อาจส่งใบรับรองอิเล็กทรอนิกส์ที่ออกให้ผู้สมัครขอใบรับรองอิเล็กทรอนิกส์ แก่เจ้าหน้าที่รับลงทะเบียน เป็นต้น

๕. การใช้คู่กุญแจ และใบรับรองอิเล็กทรอนิกส์ (Key Pair and Certificate Usage)

๕.๑ ความรับผิดชอบของผู้ใช้บริการในการใช้คู่กุญแจและใบรับรองอิเล็กทรอนิกส์ เช่น ผู้ใช้บริการจะต้องใช้กุญแจส่วนตัว (Private Key) และใบรับรองอิเล็กทรอนิกส์ตามนโยบายที่กำหนดในแนวนโยบาย และสัญญาระหว่างผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์กับผู้ใช้บริการ โดยผู้ใช้บริการสามารถใช้กุญแจส่วนตัวหลังจากที่ผู้ใช้บริการได้ยอมรับใบรับรองอิเล็กทรอนิกส์นั้นแล้ว และไม่สามารถใช้งานกุญแจส่วนตัวและใบรับรองอิเล็กทรอนิกส์ได้หลังจากใบรับรองอิเล็กทรอนิกส์ดังกล่าวหมดอายุลงหรือถูกเพิกถอน

๕.๒ ความรับผิดชอบของคู่กรณีที่เกี่ยวข้องในการใช้กุญแจสาธารณะ หรือใบรับรองอิเล็กทรอนิกส์ของผู้ใช้บริการ เช่น คู่กรณีที่เกี่ยวข้องจะต้องใช้ใบรับรองอิเล็กทรอนิกส์ตามนโยบายที่กำหนดในแนวนโยบาย และต้องตรวจสอบสถานะของใบรับรองอิเล็กทรอนิกส์ตามวิธีที่ระบุใน แนวนโยบายภายใต้เงื่อนไขเกี่ยวกับคู่กรณีที่เกี่ยวข้อง

๖. การต่ออายุใบรับรองอิเล็กทรอนิกส์ (Certificate Renewal)

การต่ออายุใบรับรองอิเล็กทรอนิกส์ หมายถึง การออกใบรับรองอิเล็กทรอนิกส์ใหม่ให้ผู้ใช้บริการโดยไม่มีการเปลี่ยนแปลงกุญแจสาธารณะของผู้ใช้บริการ หรือข้อมูลอื่นใดที่ปรากฏในใบรับรองอิเล็กทรอนิกส์ การต่ออายุใบรับรองอิเล็กทรอนิกส์ควรคำนึงถึงประเด็นต่างๆ ดังต่อไปนี้

๖.๑ กรณีต่างๆ ที่อนุญาตให้มีการต่ออายุใบรับรองอิเล็กทรอนิกส์ เช่น ใบรับรองอิเล็กทรอนิกส์หมดอายุแต่นโยบายอนุญาตให้ใช้คู่กุญแจเดิมต่อไปได้ ให้สามารถต่ออายุใบรับรองอิเล็กทรอนิกส์ได้

๖.๒ บุคคลที่สามารถขอต่ออายุใบรับรองอิเล็กทรอนิกส์ได้ เช่น ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ อาจอนุญาตให้เจ้าหน้าที่รับลงทะเบียน ขอต่ออายุแทนผู้ใช้บริการได้ หรือผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ อาจต่ออายุใบรับรองอิเล็กทรอนิกส์ให้ผู้ใช้บริการโดยอัตโนมัติเมื่อใบรับรองดังกล่าวหมดอายุลง

๖.๓ ควรมีการระบุกระบวนการในการขอต่ออายุใบรับรองอิเล็กทรอนิกส์ที่ชัดเจน เช่น การใช้รหัสผ่าน (Password) ในการยืนยันตัวบุคคลอีกครั้งก่อนการต่ออายุใบรับรองอิเล็กทรอนิกส์

๖.๔ ควรมีวิธีการแจ้งว่าได้ต่ออายุใบรับรองอิเล็กทรอนิกส์ให้ผู้ใช้บริการแล้ว

๖.๕ ควรระบุวิธีการยอมรับใบรับรองอิเล็กทรอนิกส์ที่ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ต่ออายุให้แก่ผู้ใช้บริการใบรับรองอิเล็กทรอนิกส์

๖.๖ ควรอธิบายเกี่ยวกับการเผยแพร่ใบรับรองอิเล็กทรอนิกส์ตลอดจนวิธีการแจ้งบุคคลที่เกี่ยวข้องให้ทราบถึงการต่ออายุใบรับรองอิเล็กทรอนิกส์

๗. การรับรองคู่กุญแจใหม่ (Certificate Re-key)

เนื้อหาส่วนนี้ควรให้ข้อมูลเกี่ยวกับการสร้างคู่กุญแจใหม่ รวมถึงการออกใบรับรองอิเล็กทรอนิกส์ใหม่เพื่อรองรับคู่กุญแจใหม่ โดยผู้ใช้บริการหรือบุคคลอื่น

๗.๑ กรณีต่างๆ ที่ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์สามารถหรือต้องสร้างคู่กุญแจ และออกใบรับรองอิเล็กทรอนิกส์เพื่อรองรับคู่กุญแจใหม่นี้ เช่น กรณีของการเพิกถอนใบรับรองอิเล็กทรอนิกส์ หรือการหมดอายุการใช้งานของคู่กุญแจ

๗.๒ การกำหนดให้บุคคลใดสามารถขอใบรับรองอิเล็กทรอนิกส์เพื่อรองรับคู่กุญแจใหม่

๗.๓ ควรมีวิธีการแจ้งการออกใบรับรองอิเล็กทรอนิกส์ใหม่ให้ผู้ใช้บริการทราบ

๗.๔ ควรระบุวิธีการยอมรับใบรับรองอิเล็กทรอนิกส์ที่ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์เพื่อรองรับคู่กุญแจใหม่

๗.๕ ควรอธิบายเกี่ยวกับการเผยแพร่ใบรับรองอิเล็กทรอนิกส์ตลอดจนวิธีการแจ้งบุคคลที่เกี่ยวข้องให้ทราบถึงการออกใบรับรองอิเล็กทรอนิกส์เพื่อรองรับคู่กุญแจใหม่

๘. การแก้ไขเปลี่ยนแปลงใบรับรองอิเล็กทรอนิกส์ (Certificate Modification)

เนื้อหาส่วนนี้ควรให้ข้อมูลเกี่ยวกับการออกใบรับรองอิเล็กทรอนิกส์ใหม่อันเนื่องมาจากการแก้ไขเปลี่ยนแปลงข้อมูลในใบรับรองอิเล็กทรอนิกส์ที่ไม่ใช่กุญแจสาธารณะของผู้ใช้บริการ เช่น

๘.๑ กรณีต่างๆ ที่ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์อนุญาตให้ผู้ใช้บริการสามารถแก้ไขเปลี่ยนแปลงข้อมูลในใบรับรองอิเล็กทรอนิกส์ได้ เช่น การเปลี่ยนชื่อ การเปลี่ยนแปลง Distinguished Name และการเปลี่ยนบทบาทภาระหน้าที่ในที่ทำงาน

๘.๒ การกำหนดให้บุคคลใดสามารถขอแก้ไขเปลี่ยนแปลงใบรับรองอิเล็กทรอนิกส์ได้ เช่น ผู้ใช้บริการ เจ้าหน้าที่ฝ่ายบุคคล หรือเจ้าหน้าที่รับลงทะเบียน เป็นต้น

๘.๓ ควรมีวิธีการแจ้งการออกใบรับรองอิเล็กทรอนิกส์ใหม่ให้ผู้ใช้บริการทราบ

๘.๔ ควรระบุวิธีการยอมรับใบรับรองอิเล็กทรอนิกส์ที่ผู้ให้บริการออกให้ใหม่

๘.๕ ควรอธิบายเกี่ยวกับการเผยแพร่ใบรับรองอิเล็กทรอนิกส์ตลอดจนวิธีการแจ้งบุคคลที่เกี่ยวข้องให้ทราบถึงการออกใบรับรองอิเล็กทรอนิกส์ใหม่

๙. การเพิกถอนและพักใช้ใบรับรองอิเล็กทรอนิกส์ (Certificate Revocation and Suspension)

เนื้อหาส่วนนี้ควรให้ข้อมูลเกี่ยวกับการเพิกถอนและการพักใช้ใบรับรองอิเล็กทรอนิกส์

๙.๑ กรณีต่างๆผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ ให้มีการพักใช้หรือเพิกถอนใบรับรองอิเล็กทรอนิกส์ เช่น การเลิกจ้างงานผู้ใช้บริการ การสูญหายของอุปกรณ์เข้ารหัสลับ หรือมีเหตุอันควรสงสัยว่ามีการล่วงรู้กุญแจส่วนตัวโดยมิชอบ เป็นต้น

๙.๒ การกำหนดให้บุคคลใดสามารถขอเพิกถอนและพักใช้ใบรับรองอิเล็กทรอนิกส์ของผู้ใช้บริการได้ เช่น ผู้ใช้บริการ และเจ้าหน้าที่รับลงทะเบียน เป็นต้น

๙.๓ ควรมีการระบุกระบวนการขอเพิกถอนและพักใช้ใบรับรองอิเล็กทรอนิกส์ เช่น การกำหนดให้เจ้าหน้าที่รับลงทะเบียน หรือผู้ใช้บริการต้องลงลายมือชื่อกำกับคำขอเพิกถอนใบรับรองอิเล็กทรอนิกส์ เป็นต้น

๙.๔ ควรมีการกำหนดระยะเวลาที่ผู้ใช้บริการสามารถขอเพิกถอนใบรับรองอิเล็กทรอนิกส์ได้

๙.๕ ควรมีการกำหนดวิธีการที่คู่กรณีที่เกี่ยวข้องสามารถตรวจสอบสถานะของใบรับรองอิเล็กทรอนิกส์ได้

๙.๖ ในกรณีที่มีการใช้ Certificate Revocation List (CRL) ในการเผยแพร่ใบรับรองอิเล็กทรอนิกส์ที่ได้เพิกถอนและพักใช้ ควรมีการกำหนดความถี่ของการเผยแพร่ข้อมูลดังกล่าว ระยะเวลาระหว่างการสร้าง CRL และเวลาที่เผยแพร่ CRL ให้สาธารณะทราบ และถ้ามีการให้บริการตรวจสอบสถานะของใบรับรองอิเล็กทรอนิกส์แบบออนไลน์ ก็ควรแจ้งให้สาธารณะทราบถึงวิธีการใช้งาน เงื่อนไข และข้อกำหนดที่เกี่ยวข้องด้วย

๙.๗ ควรกำหนดระยะเวลาการพักใช้ใบรับรองอิเล็กทรอนิกส์

๑๐. บริการตรวจสอบสถานะของใบรับรองอิเล็กทรอนิกส์ (Certificate Status Services)

ข้อมูลส่วนนี้กล่าวถึงบริการตรวจสอบสถานะของใบรับรองอิเล็กทรอนิกส์สำหรับคู่กรณีที่เกี่ยวข้อง และควรมีประเด็นดังต่อไปนี้

๑๐.๑ ลักษณะของบริการตรวจสอบสถานะของใบรับรองอิเล็กทรอนิกส์ และสภาพพร้อมใช้งานของระบบบริการ รวมถึงนโยบายรองรับกรณีที่ระบบไม่สามารถให้บริการได้

๑๐.๒ ลักษณะของบริการอื่นที่เกี่ยวข้อง

๑๑. การเลิกใช้บริการใบรับรองอิเล็กทรอนิกส์ (End of Subscription)

ข้อมูลส่วนนี้กล่าวถึงขั้นตอนที่ผู้ใช้บริการปฏิบัติในการเลิกใช้ใบรับรองอิเล็กทรอนิกส์ซึ่งอาจมีสาเหตุมาจากการหมดอายุของใบรับรองอิเล็กทรอนิกส์ หรือการเลิกให้บริการโดยผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์

๑๒. การเก็บรักษาและการกู้คืนกุญแจ (Key Escrow and Recovery)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ควรระบุนโยบายเกี่ยวกับการเก็บรักษาและการกู้คืนกุญแจส่วนตัว และการป้องกัน Session Key (Session Key Encapsulation)

บทที่ ๕ การควบคุมความมั่นคงปลอดภัยของเครื่องมืออุปกรณ์ การบริหารจัดการ และการดำเนินงาน (Facility, Management, and Operational Controls)

สำหรับเนื้อหาในบทนี้จะครอบคลุมการควบคุมและการรักษาความมั่นคงปลอดภัยทางกายภาพสำหรับกรณีที่ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ต้องใช้ในการสร้างกุญแจ (Key Generation) การยืนยันตัวบุคคล (Subject Authentication) การออกใบรับรองอิเล็กทรอนิกส์ (Certificate Issuance) การเพิกถอนใบรับรองอิเล็กทรอนิกส์ (Certificate Revocation) การตรวจสอบระบบและเก็บรักษาข้อมูล (Auditing and Archiving) ให้มั่นคงปลอดภัย

ดังนั้น จึงควรมีการกำหนดวิธีการในการรักษาความมั่นคงปลอดภัยของบุคคลที่เกี่ยวข้องเพื่อสร้างความเชื่อมั่นในการใช้งานใบรับรองอิเล็กทรอนิกส์ และป้องกันมิให้มีการบุกรุก หรือเข้าถึงระบบหรือล่วงรู้ข้อมูลในระบบการให้บริการของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ รวมทั้งป้องกันมิให้เกิดความผิดพลาดในข้อมูลที่ใช้ในการสร้างใบรับรองอิเล็กทรอนิกส์ หรือรายการเพิกถอนใบรับรองอิเล็กทรอนิกส์กรณีที่มีการล่วงรู้กุญแจส่วนตัวของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์โดยมิชอบ

ทั้งนี้ ความมั่นคงปลอดภัยทางกายภาพ (Physical Security Controls) นั้น ครอบคลุมในเรื่องดังต่อไปนี้

๑. สถานที่ตั้งหรือการก่อสร้างสำนักงานในการให้บริการ (Site Location and Construction)

เนื้อหาในส่วนนี้ควรมีการกำหนดพื้นที่ที่มีการรักษาความมั่นคงปลอดภัยเป็นพิเศษ (High Security Zone) หรือการใช้ห้องและตู้นิรภัย การติดตั้งระบบโทรทัศน์วงจรปิด และระบบตรวจจับการบุกรุกทางกายภาพ เป็นต้น

๒. การเข้าถึงทางกายภาพ (Physical Access)

ควรกำหนดเกี่ยวกับการเข้าออกระหว่างพื้นที่สำนักงานกับพื้นที่ที่มีการรักษาความมั่นคงปลอดภัยเป็นพิเศษ การเคลื่อนย้ายจากพื้นที่หนึ่งไปยังอีกพื้นที่หนึ่ง ให้มีการป้องกันการเข้าถึงทางกายภาพ เช่น การพิสูจน์ตัวบุคคลก่อนอนุญาตให้เข้าถึงระบบให้บริการได้ อาจทำได้โดยการใช้บัตรแถบแม่เหล็ก และการตรวจสอบลายนิ้วมือ เป็นต้น นอกจากนี้ ยังควรมีการคำนึงถึงการบริหารจัดการระบบไฟฟ้าและระบบปรับอากาศ การป้องกันภัยจากน้ำ การจัดเก็บ Backup Media ไว้ในสถานที่อื่น ที่ได้รับการป้องกันการเข้าถึง ป้องกันภัยจากไฟและน้ำ

๓. การควบคุมความมั่นคงปลอดภัยด้านกายภาพ (Physical Security Controls)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ควรบรรยายวิธีการควบคุมด้านกายภาพของสถานที่ประกอบการในหัวข้อดังต่อไปนี้

๓.๑ สถานที่ตั้งของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ และการจัดแบ่งพื้นที่ตามระดับของความมั่นคงปลอดภัยที่ต้องการ

๓.๒ การควบคุมการเข้าถึงพื้นที่ที่ต้องการระดับความมั่นคงปลอดภัยที่ต่างกัน

๓.๓ การดูแลเรื่องพลังงานไฟฟ้า การไหลเวียนของน้ำ การควบคุมสภาพอากาศ อุณหภูมิและความชื้นสัมพัทธ์ การป้องกันการเกิดอัคคีภัย เพื่อป้องกันการหยุดชะงักของการให้บริการจากเหตุเหล่านี้

๓.๔ การเก็บรักษาสื่อที่ใช้เก็บข้อมูลของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ให้มั่นคงปลอดภัย ตลอดจนการกำหนดให้มีการสำรองข้อมูลนอกสถานที่ประกอบการเพื่อป้องกันการสูญเสีย หรือสูญหายของข้อมูล

๔. การควบคุมกระบวนการต่าง ๆ ในการดำเนินการ (Procedural Controls)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ควรมีการจัดบทบาทและหน้าที่ของบุคลากรในองค์กรให้เหมาะสม และกำหนดนโยบายเกี่ยวกับการทำงานของบุคลากรในแต่ละบทบาท เช่น วิธีการระบุและยืนยันตัวบุคคล หรือวิธีการเข้าถึงข้อมูลสำคัญโดยบุคคลในบทบาทต่าง ๆ โดยการแบ่งแยกหน้าที่ซึ่งไม่อนุญาตให้บุคคลหนึ่งรับหน้าที่ในหลายบทบาทด้วยเหตุผลด้านความมั่นคงปลอดภัยของข้อมูล

๕. การกู้คืนระบบอันเกิดจากพฤติการณ์ที่กระทบต่อความมั่นคงปลอดภัยของข้อมูลและภัยพิบัติอันเกิดแก่ระบบ (Compromise and Disaster Recovery)

ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ควรมีนโยบายในการกู้คืนระบบอันเกิดจากพฤติการณ์ที่กระทบต่อความมั่นคงปลอดภัยของข้อมูลและภัยพิบัติอันเกิดแก่ระบบ เช่น ข้อมูลถูกทำลายอันเนื่องมาจากอุบัติเหตุหรือสาเหตุอื่นใด เพื่อให้การให้บริการไม่หยุดชะงัก

๖. การเลิกกิจการของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์และเจ้าหน้าที่รับลงทะเบียน (CA or RA Termination)

ในกรณีที่ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์หรือเจ้าหน้าที่รับลงทะเบียนเลิกกิจการจะต้องมีการแจ้งให้บุคคลที่เกี่ยวข้องทราบ รวมถึงผู้ที่รับผิดชอบข้อมูลของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์และเจ้าหน้าที่รับลงทะเบียนเพื่อให้เกิดผลกระทบต่อผู้ใช้บริการน้อยที่สุด

บทที่ ๖ การควบคุมความมั่นคงปลอดภัยด้านเทคนิค (Technical Security Controls)

สำหรับเนื้อหาในส่วนนี้เป็นการกำหนดมาตรการด้านการรักษาความมั่นคงปลอดภัยของกุญแจและข้อมูลสำหรับอนุญาตให้ใช้กุญแจ เช่น PIN และ Password และประเด็นต่าง ๆ ที่เกี่ยวกับการบริหารจัดการกุญแจ

๑. การสร้างและติดตั้งคู่กุญแจ (Key Pair Generation and Installation)

การสร้างและการติดตั้งคู่กุญแจมีประเด็นที่ต้องพิจารณาและกำหนดเป็นนโยบาย ดังต่อไปนี้

๑.๑ ใครเป็นผู้สร้างคู่กุญแจให้ผู้ใช้บริการ และสร้างโดยซอฟต์แวร์หรือฮาร์ดแวร์

๑.๒ วิธีการที่ผู้ใช้บริการจะได้รับกุญแจส่วนตัวของตนแบบมั่นคงปลอดภัยเป็นไปได้อย่างไรบ้าง

๑.๓ วิธีการที่ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์จะได้รับกุญแจสาธารณะของผู้ใช้บริการแบบมั่นคงปลอดภัยเป็นไปได้อย่างไรบ้าง

๑.๔ คู่กรณีที่เกี่ยวข้องจะได้รับกุญแจสาธารณะของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์แบบมั่นคงปลอดภัยเป็นไปได้อย่างไรบ้าง

๑.๕ ความยาวของคู่กุญแจเป็นเท่าใด เช่น กุญแจอาจมีความยาว 1,024 บิต RSA และ 1,024 บิต DSA

๑.๖ ใครเป็นผู้ที่กำหนดพารามิเตอร์ของกุญแจสาธารณะ และมีการตรวจสอบคุณภาพของพารามิเตอร์ระหว่างการสร้างกุญแจหรือไม่

๑.๗ วัตถุประสงค์ที่อาจจะนำคู่กุญแจไปใช้ หรือวัตถุประสงค์ที่ควรจำกัดการใช้คู่กุญแจคืออะไร สำหรับใบรับรองตาม X.509 นั้นวัตถุประสงค์เหล่านี้ควรจะสอดคล้องกับการใช้งานกุญแจตามมาตรฐาน X.509 เวอร์ชั่น 3

๒. การป้องกันกุญแจส่วนตัว (Private Key Protection) และการจัดการควบคุมชิ้นส่วนสำหรับการเข้ารหัสลับ (Cryptographic Module Engineering Control)

ในส่วนนี้ควรกำหนดวิธีการป้องกันกุญแจส่วนตัวและการใช้งานชิ้นส่วนสำหรับการเข้ารหัสลับของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ เจ้าหน้าที่รับลงทะเบียน ผู้ใช้บริการ และผู้ให้บริการเก็บข้อมูล โดยคำนึงถึงความมั่นคงปลอดภัยและความเสียหายอันเกิดจากการเก็บรักษากุญแจส่วนตัว การสำรองกุญแจส่วนตัว และการบันทึกถาวรกุญแจส่วนตัว ทั้งนี้ ให้พิจารณาคำถาม ดังต่อไปนี้

๒.๑ ถ้ามีการใช้งานชิ้นส่วนสำหรับการเข้ารหัสลับ (อาจเป็นซอฟต์แวร์ ฮาร์ดแวร์ และ หรือ เฟิร์มแวร์) ควรจะอ้างอิงตามมาตรฐานใด

๒.๒ จำเป็นต้องมีการควบคุมการเข้าถึงกุญแจส่วนตัว โดยผู้มีสิทธิมากกว่า ๑ คนหรือไม่ (แบบ m out of n)

๒.๓ มีนโยบายในการเก็บรักษากุญแจส่วนตัวหรือไม่ (Key Escrow)

๒.๔ มีนโยบายในการสำรองกุญแจส่วนตัวหรือไม่ (Private Key Backup)

๒.๕ มีนโยบายในการบันทึกถาวรกุญแจส่วนตัวหรือไม่ (Private Key Archival)

๒.๖ ในกรณีใดบ้างที่จะมีการถ่ายโอนกุญแจส่วนตัวเข้าไปในหรือออกจากชิ้นส่วนสำหรับเข้ารหัสลับ

๒.๗ การจัดเก็บกุญแจส่วนตัวในชิ้นส่วนสำหรับเข้ารหัสลับ (Private Key Storage in Cryptographic Module) จะทำด้วยวิธีใด เช่น เก็บในรูปแบบข้อมูลธรรมดาที่อ่านเข้าใจได้ (Plaintext) รูปแบบของข้อมูลที่มีการเข้ารหัสลับ (Encrypted) หรือการแยกกุญแจ (Split Key) เป็นต้น

๒.๘ ใครเป็นผู้ที่มีสิทธิในการใช้งานกุญแจส่วนตัว ด้วยวิธีอย่างไร

๒.๙ ใครเป็นผู้มีสิทธิในการยกเลิกการใช้งานกุญแจส่วนตัว ด้วยวิธีอย่างไร

๒.๑๐ ใครมีสิทธิทำลายกุญแจส่วนตัว ด้วยวิธีอย่างไร

๒.๑๑ รายละเอียดความสามารถของชิ้นส่วนสำหรับเข้ารหัสลับ เป็นอย่างไร (อาจอ้างถึงมาตรฐานที่เกี่ยวข้อง เช่น FIPS 140-1

๓. รายละเอียดอื่นเกี่ยวกับการจัดการและบริหารคู่กุญแจ (Other Aspects of Key Pair Management)

ในส่วนนี้ควรกำหนดวิธีการในการจัดการและบริหารคู่กุญแจของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ เจ้าหน้าที่รับลงทะเบียน ผู้ใช้บริการ และผู้ให้บริการเก็บข้อมูล โดยพิจารณาคำถามดังต่อไปนี้

๓.๑ ควรมีการเก็บบันทึกถาวรของกุญแจสาธารณะ (Public Key Archival) หรือไม่ ถ้ามีใครจะเป็นผู้ทำหน้าที่เก็บบันทึกถาวร และการควบคุมความมั่นคงปลอดภัยของระบบเก็บบันทึกถาวร ทั้งในเรื่องความจำเป็นในการปกป้องซอฟต์แวร์ และฮาร์ดแวร์ที่เกี่ยวข้องกับการใช้งานกุญแจสาธารณะอยู่ตลอดเวลา

๓.๒ ระยะเวลาใช้งานของใบรับรองอิเล็กทรอนิกส์ และคู่กุญแจของผู้ใช้บริการเป็นเท่าใด

๔. ข้อมูลที่ใช้ในการติดตั้งใบรับรองของผู้ใช้บริการ (Activation Data)

เนื้อหาในส่วนนี้ควรกำหนดวิธีการป้องกันข้อมูลที่จำเป็นต้องใช้ในการติดตั้งใบรับรองของผู้ใช้บริการ (Activation Data) ซึ่งอาจหมายถึง รหัสอ้างอิง (Reference Code) และรหัสติดตั้ง (Installation Code) เพื่อใช้ในการยืนยันตัวผู้ใช้บริการในขั้นตอนการติดตั้งใบรับรอง ซึ่งเป็นข้อมูลที่ผู้ใช้บริการได้รับจากผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์โดยตรงหรือจากเจ้าหน้าที่รับลงทะเบียน

๕. การควบคุมความมั่นคงปลอดภัยของระบบคอมพิวเตอร์ (Computer Security Controls)

เนื้อหาในส่วนนี้ควรอธิบายการควบคุมความมั่นคงปลอดภัยของระบบคอมพิวเตอร์ เพื่อให้เกิดความน่าเชื่อถือของระบบผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ โดยมีการควบคุมการเข้าถึง (Access Control) มีการตรวจสอบ (Audit) ระบบของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ การยืนยันตัวบุคคล (Identification และ Authentication) การทดสอบระบบความมั่นคงปลอดภัย (Security testing) และทดสอบการบุกรุกระบบ (Penetration Testing) โดยที่ระบบการควบคุมความมั่นคงปลอดภัยนั้นต้องได้รับการประเมินตามมาตรฐานสากล เช่น The Trusted System Evaluation Criteria (TCSEC)

๖. การควบคุมทางเทคนิคของระบบให้บริการ (Life Cycle Technical Controls)

เนื้อหาในส่วนนี้ควรจะกล่าวถึงการควบคุมการพัฒนาระบบและการควบคุมการบริหารจัดการด้านความมั่นคงปลอดภัย การควบคุมการพัฒนาระบบนั้นรวมความถึงความมั่นคงปลอดภัยของสภาพแวดล้อมในการพัฒนาระบบ บุคลากรที่พัฒนาระบบ และการออกแบบระบบ เป็นต้น

การควบคุมการบริหารจัดการด้านความมั่นคงปลอดภัย หมายความถึง การใช้เครื่องมืออุปกรณ์ (Tools) และกระบวนการ (procedure) เพื่อให้เกิดความมั่นใจด้านความมั่นคงปลอดภัยของระบบปฏิบัติการ (Operational Systems) และระบบเครือข่าย (Networks)

๗. การควบคุมความมั่นคงปลอดภัยทางเครือข่าย (Network Security Controls)

เนื้อหาในส่วนนี้ระบุการควบคุมความมั่นคงปลอดภัยทางเครือข่ายของระบบผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ โดยป้องกันมิให้เข้าถึงระบบได้โดยมิชอบด้วยกลไกของอุปกรณ์รักษาความมั่นคงปลอดภัยหลายส่วนหลายลำดับชั้น ได้แก่ อุปกรณ์เลือกเส้นทาง (Router) ตัวป้องกันการบุกรุก (Firewall) ระบบตรวจสอบผู้บุกรุก (Intrusion Detection System: IDS)

๘. ข้อกำหนดสำหรับการประทับเวลาในบันทึกต่าง ๆ (Time-stamping)

หากกำหนดให้มีการประทับเวลาในบันทึกต่างๆ ควรระบุไว้ในส่วนนี้ และกล่าวถึงแหล่งที่มาของเวลาและความน่าเชื่อถือประกอบด้วย

บทที่ ๗ การกำหนดรูปแบบของใบรับรองอิเล็กทรอนิกส์ รายการเพิกถอน และสถานะของใบรับรองอิเล็กทรอนิกส์ (Certificate, CRL, and OCSP Profiles)

๑. รูปแบบของใบรับรองอิเล็กทรอนิกส์ (Certificate Profile)

เนื้อหาในส่วนนี้กำหนดรายละเอียดเกี่ยวกับประเด็นดังต่อไปนี้ (อ้างอิงตาม IETF RFC 3280)

๑.๑ เวอร์ชั่นของใบรับรองอิเล็กทรอนิกส์ที่สนับสนุน

๑.๒ ข้อมูลใน Certificate Extensions และความสำคัญ (Criticality) ของข้อมูลดังกล่าว OID ของขั้นตอนวิธีการเข้ารหัสลับ (Cryptographic Algorithm Object Identifiers)

๑.๓ รูปแบบชื่อของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ เจ้าหน้าที่รับลงทะเบียน และผู้ใช้บริการ

๑.๔ OID ของแนวนโยบายที่เกี่ยวข้อง

๒. รูปแบบรายการเพิกถอนใบรับรอง (Certification Revocation List Profile)

๒.๑ เนื้อหาในส่วนนี้กำหนดรายละเอียดเกี่ยวกับประเด็นดังต่อไปนี้ (อ้างอิงตาม IETF RFC 3280) เวอร์ชั่นของรายการเพิกถอนใบรับรองที่สนับสนุน และ

๒.๒ รายการเพิกถอนใบรับรอง และข้อมูลใน CRL Entry Extensions และความสำคัญของข้อมูลดังกล่าว (Criticality)

๓. รูปแบบโปรโตคอล OCSP (OCSP Profile)

ในส่วนนี้แสดงถึงเนื้อหาและรูปแบบของข้อมูลที่ใช้ในการตรวจสอบสถานะของใบรับรองโดยใช้โปรโตคอล OCSP (Online Certificate Status Protocol) รวมทั้งข้อมูลอื่นๆ เช่น เวอรชั่นของ OCSP และข้อมูลเพิ่มเติมที่สามารถระบุลงไปใน OCSP (อ้างอิงตาม IETF RFC 2560)

บทที่ ๘ การตรวจสอบการปฏิบัติตามกฎข้อบังคับต่าง ๆ และการประเมินความเสี่ยงอื่น ๆ (Compliance Audit and Other Assessment)

สำหรับเนื้อหาในส่วนนี้จะต้องกำหนดเกี่ยวกับรายการที่ต้องมีการประเมินความเสี่ยง หรือระเบียบวิธี (Methodology) ที่ใช้ในการประเมินความเสี่ยง เช่น การประเมินความเสี่ยงตามแนวทางของ WebTrust เป็นต้น

นอกจากนั้น ก็อาจกำหนดความถี่ของการตรวจสอบหรือประเมินความเสี่ยง ทั้งนี้ ในการประเมินนั้น ก็ต้องประเมินตามแนวนโยบายและแนวปฏิบัติ และประเมินทั้งก่อนมีการให้บริการ เมื่อมีการให้บริการ และการตรวจสอบกรณีมีความเป็นไปได้ที่จะมีการล่วงรู้โดยมิชอบอันเป็นการกระทบถึงความมั่นคงปลอดภัย

ทั้งนี้ จำเป็นต้องระบุคุณสมบัติของบุคลากรที่ทำหน้าที่ตรวจสอบและประเมินความเสี่ยง การดำเนินการเกี่ยวกับผลการประเมิน เช่น การระงับการดำเนินการชั่วคราว หรือการเพิกถอนใบรับรองที่ออก เป็นต้น

บทที่ ๙ ข้อกำหนดอื่น ๆ และประเด็นกฎหมาย (Other Business and Legal Matters)

สำหรับเนื้อหาในส่วนนี้ จะกำหนดเกี่ยวกับการจัดเก็บค่าธรรมเนียม (Fees) ความรับผิดชอบทางการเงิน (Financial Responsibility) ทั้งในส่วนที่เกี่ยวกับการดำเนินการหรือกรณีมีการเรียกร้องค่าเสียหายจากการให้บริการเกิดขึ้น รวมทั้งประเด็นข้อกฎหมายต่าง ๆ

อย่างไรก็ตาม ในการจัดทำแนวนโยบายและแนวปฏิบัติ นั้น หากผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ ต้องการให้เอกสารฉบับดังกล่าวถือเป็นสัญญาฉบับหนึ่งหรือเป็นส่วนหนึ่งของสัญญาในการให้บริการ ก็อาจจำเป็นต้องพิจารณาเพิ่มเติมเนื้อหาเกี่ยวกับข้อจำกัดความรับผิด (Limitation of Liability) ไว้ในแนวนโยบายหรือแนวปฏิบัติ ด้วย แต่หากไม่ประสงค์ให้แนวนโยบายและแนวปฏิบัติเป็นสัญญาหรือส่วนหนึ่งของสัญญาในการให้บริการ ก็อาจจำเป็นต้องมีการจัดทำสัญญาในการให้บริการผู้ใช้บริการ หรือคู่กรณีที่เกี่ยวข้องซึ่งมีข้อความกำหนดเกี่ยวกับข้อจำกัดความรับผิดของบุคคลดังกล่าวในการให้บริการเอาไว้ด้วย

๑. ค่าธรรมเนียม (Fees)

สำหรับค่าธรรมเนียมในการให้บริการนั้น อาจกำหนดให้ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ซึ่งให้บริการออกใบรับรองอิเล็กทรอนิกส์ ผู้ให้บริการเก็บรักษาข้อมูล หรือผู้ให้บริการในฐานะเจ้าหน้าที่รับลงทะเบียน จัดเก็บค่าธรรมเนียมได้จากกรณีที่มีการออกใบรับรองอิเล็กทรอนิกส์ หรือต่ออายุใบรับรองดังกล่าว (Certificate Issuance or Renewal Fees) ค่าธรรมเนียมในการเข้าถึงใบรับรอง (Certificate Access Fees) การเข้าถึงข้อมูลเกี่ยวกับการเพิกถอนหรือสถานะล่าสุดของใบรับรองอิเล็กทรอนิกส์ ค่าธรรมเนียมสำหรับบริการอื่นๆ เช่น การเข้าถึงแนวนโยบายหรือแนวปฏิบัติ ทั้งนี้ ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ อาจจัดทำนโยบายในการคืนค่าธรรมเนียม (Refund Policy) ไว้ด้วย

๒. ความรับผิดชอบทางการเงิน (Financial Responsibility)

เนื้อหาในส่วนนี้ควรกำหนดขึ้นเกี่ยวกับความรับผิดในการดำเนินการที่เกิดขึ้น (Operational PKI Responsibilities) การรักษาสถานะของผู้ให้บริการให้สามารถชำระหนี้และจ่ายค่าเสียหายในกรณีที่ต้องรับผิดได้ (to Remain Solvent and Pay Damages) ทั้งนี้ อาจมีการเพิ่มเติมเนื้อหาที่เกี่ยวกับวงเงินประกันความเสียหายที่คุ้มครองความรับผิดที่เกิดขึ้น (Insurance Coverage for Liabilities) และความรับผิดในอนาคต (Contingencies) สินทรัพย์ที่ปรากฏในงบดุล (Assets on The Balance Sheet) หนังสือค้ำประกัน (Surety Bond) เล็ตเตอร์ อ๊อฟ เครดิต (Letter of Credit) ค่าสินไหมทดแทน (Indemnity) และอาจให้ความคุ้มครองเพิ่มเติมด้วยการกำหนดเกี่ยวกับการประกันภัย (Insurance) หรือการให้คำรับรอง (Warranty)

๓. การรักษาความลับของข้อมูลทางธุรกิจ (Confidentiality of Business Information)

ด้วยข้อมูลบางประเภทเป็นความลับทางธุรกิจที่จำเป็นต้องเก็บไว้เป็นความลับ เช่น แผนทางธุรกิจ (Business Plan) ข้อมูลการขาย (Sales Information) ความลับทางการค้า (Trade Secrets) และข้อมูลที่ได้จากบุคคลที่สามภายใต้ข้อตกลงไม่เปิดเผยความลับ (Nondisclosure Agreement) จึงจำเป็นต้องกำหนดขอบเขตในการรักษาความลับ ข้อมูลที่อยู่นอกเหนือจากข้อตกลงว่าด้วยการรักษาความลับ และความรับผิดของบุคคลที่เกี่ยวข้องซึ่งได้รับข้อมูลลับนั้น ทั้งนี้ อาจต้องมีกลไกทำให้เกิดความเชื่อมั่นว่าจะมีการปกป้องมิให้เกิดพฤติการณ์ที่กระทบต่อความมั่นคงปลอดภัยของข้อมูล (Compromise)

๔. นโยบายในการรักษาความเป็นส่วนตัวหรือข้อมูลส่วนบุคคล (Privacy of Personal Information)

ในการให้บริการของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ เจ้าหน้าที่รับลงทะเบียน หรือบุคคลอื่นๆ ซึ่งให้บริการที่เกี่ยวข้องนั้น จำเป็นต้องให้ความสำคัญสำหรับการรักษาความเป็นส่วนตัวหรือเก็บข้อมูลส่วนบุคคลของผู้ใช้บริการไว้เป็นความลับ จะเปิดเผยได้เพียงข้อมูลบางอย่างเท่านั้น เช่น ข้อมูลที่ต้องเผยแพร่โดยการบันทึกไว้ในใบรับรองอิเล็กทรอนิกส์ ได้แก่ ชื่อ ชื่อสกุล ของผู้ใช้บริการ เป็นต้น

ดังนั้น การดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลจึงต้องดำเนินการตามกฎหมายว่าด้วยการนั้น หรือกรณีที่ยังไม่มีการใช้บังคับกฎหมายเช่นว่านั้น ก็อาจจำเป็นต้องดำเนินการตามหลักเกณฑ์ในการให้ความคุ้มครองในเรื่องดังกล่าวตามมาตรฐานสากล เช่น ตามแนวทางของ OECD Guidelines

ด้วยเหตุนี้ ในการดำเนินการใดๆ เกี่ยวกับข้อมูลส่วนบุคคล จึงควรได้รับความยินยอมจากผู้ใช้บริการ ก่อนจะมีการเปิดเผยข้อมูลส่วนบุคคลดังกล่าว ทั้งนี้ จะต้องกำหนดข้อยกเว้นกรณีที่จำเป็นต้องมีการเปิดเผยข้อมูลส่วนบุคคลในกรณีที่ต้องดำเนินการตามกฎหมายฉบับต่างๆ หรือเมื่อมีคำสั่งศาล หรือเมื่อมีคำสั่งทางปกครอง เป็นต้น ไว้ด้วย

๕. ทรัพย์สินทางปัญญา (Intellectual Property Rights)

ให้กำหนดเรื่องทรัพย์สินทางปัญญา อันได้แก่ ลิขสิทธิ์ สิทธิบัตร เครื่องหมายการค้า หรือความลับทางการค้าซึ่งบุคคลที่เกี่ยวข้องอาจมีหรือใช้สิทธิเรียกร้องตามที่กำหนดไว้ในแนวนโยบาย

แนวปฏิบัติ ใบรับรองอิเล็กทรอนิกส์ ชื่อ กุญแจ หรือภายใต้การอนุญาตหรือที่กำหนดไว้ในข้อตกลงใดๆ กับบุคคลที่เกี่ยวข้อง

๖. คำรับรอง (Representations and Warranties)

ในส่วนนี้จะกำหนดให้บุคคลที่เกี่ยวข้องทำคำรับรองในเรื่องต่างๆ ที่กำหนดไว้ในแนวนโยบายหรือแนวปฏิบัติ เช่น การกำหนดให้ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ ต้องให้การรับรองว่า ข้อมูลหรือข้อเท็จจริงที่บันทึกไว้ในใบรับรองอิเล็กทรอนิกส์นั้นถูกต้อง ตามที่ได้มีการกำหนดให้แนวปฏิบัติเป็นข้อตกลงในการให้บริการ รวมทั้งกรณีมีการกำหนดให้มีการให้คำรับรองที่กำหนดไว้ในสัญญาหรือข้อตกลงอื่นๆ เช่น ข้อตกลงในการให้บริการกับผู้ใช้บริการ (Subscriber Agreement) และข้อตกลงในการให้บริการกับคู่กรณีที่เกี่ยวข้อง (Relying Party Agreement)

๗. การปฏิเสธความรับผิดตามคำรับรอง (Disclaimers of Warranties)

ในเนื้อหาของแนวนโยบายหรือแนวปฏิบัตินั้น ให้มีการกำหนดเกี่ยวกับการปฏิเสธความรับผิดตามคำรับรองหรือกำหนดเนื้อหาเกี่ยวกับเรื่องดังกล่าวไว้ในสัญญาในการให้บริการฉบับต่าง ๆ

๘. ข้อจำกัดความรับผิด (Limitations of Liability)

ในการให้บริการนั้น อาจมีการกำหนดเกี่ยวกับข้อจำกัดความรับผิดไว้ด้วยก็ได้ โดยอาจพิจารณาจากลักษณะของการจำกัดความรับผิด และจำนวนเงินค่าเสียหายที่จำกัดความรับผิด เช่น ค่าเสียหายอันเนื่องมาจากการผิดสัญญา (Incidental Damages) ค่าเสียหายจากการสูญเสียกำไรในอนาคต (Consequential Damages)

๙. ค่าสินไหมทดแทน (Indemnities)

สำหรับการชดใช้ค่าสินไหมทดแทนนั้น อาจมีการกำหนดให้คู่สัญญาฝ่ายใดต้องรับผิด ทั้งนี้โดยอาจมีการกำหนดไว้ในแนวนโยบาย แนวปฏิบัติ หรือสัญญา หรือข้อตกลงต่างๆ เช่น การกำหนดให้ผู้ใช้บริการต้องรับผิดในการชดใช้ค่าสินไหมทดแทนกรณีที่ผู้ใช้บริการได้แถลงข้อมูลหรือข้อเท็จจริงของตนที่ต้องบันทึกไว้ในใบรับรองอิเล็กทรอนิกส์เป็นเท็จหรือไม่ตรงกับความจริง หรือกรณีที่คู่กรณีที่เกี่ยวข้องต้องรับผิดชดใช้ค่าสินไหมทดแทนที่เกิดขึ้นกับผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ในกรณีที่ไม่ตรวจสอบการเพิกถอนใบรับรองอิเล็กทรอนิกส์

สำหรับในบทที่ ๙ นี้ นอกจากหัวข้อข้างต้นแล้ว อาจมีการกำหนดเนื้อหาเกี่ยวกับการเลิกสัญญา การติดต่อสื่อสารระหว่างผู้ให้บริการและผู้ใช้บริการ การแก้ไขปรับปรุงแนวนโยบาย หรือแนวปฏิบัติ การระงับข้อพิพาท กฎหมายที่ใช้บังคับ รวมทั้งเนื้อหาอื่นๆ ที่ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ประสงค์จะกำหนดเพิ่มเติมได้อีกด้วย

<u>เอกสารอ้างอิง</u>

Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC 3647)

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง หลักเกณฑ์และวิธีการในการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

เรื่อง หลักเกณฑ์และวิธีการในการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓

โดยที่พัฒนาการทางเทคโนโลยีในปัจจุบันทำให้รูปแบบและวิธีการในการติดต่อสื่อสาร การรับส่งเอกสารและข้อมูล ตลอดจนการทำธุรกรรมปรับเปลี่ยนไปเป็นรูปแบบของธุรกรรมทางอิเล็กทรอนิกส์มากขึ้น รวมถึงเอกสารหรือข้อความที่ได้มีการจัดทำหรือแปลงให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ในภายหลัง และโดยที่กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์กำหนดให้การจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์กำหนด

อาศัยอำนาจตามความในมาตรา ๑๒/๑ วรรคสอง แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ ๒) พ.ศ. ๒๕๕๑ คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง หลักเกณฑ์และวิธีการในการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓”

ข้อ ๒ ในประกาศนี้

“การจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์” หมายความว่า การจัดทำหรือแปลงเอกสารและข้อความตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ฉบับนี้

“ผู้จัดทำหรือแปลง” หมายความว่า บุคคลผู้จัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ และให้หมายความรวมถึง บุคคลผู้จัดทำหรือแปลงข้อความเสียง หรือวีดิทัศน์ให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์

“เอกสาร” หมายความว่า กระดาษหรือวัตถุอื่นใดซึ่งได้ทำให้ปรากฏความหมายด้วยตัวอักษร ตัวเลข ผัง หรือแผนแบบอย่างอื่นจะเป็นโดยวิธีพิมพ์ ถ่ายภาพหรือวิธีอื่นอันเป็นหลักฐานแห่งความหมายนั้น

“เมตาดาตา” (Metadata) หมายความว่า ข้อมูลที่ใช้กำกับและอธิบายข้อมูลอื่น

ข้อ ๓ การจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ให้เป็นไปตามหลักเกณฑ์และวิธีการดังต่อไปนี้

(๑) ข้อมูลอิเล็กทรอนิกส์ที่จัดทำหรือแปลงต้องมีความหมายหรือรูปแบบเหมือนกับเอกสารและข้อความเดิมซึ่งนำมาจัดทำหรือแปลงให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ โดยผู้จัดทำหรือแปลงจะต้องตรวจสอบและรับรองว่าข้อมูลอิเล็กทรอนิกส์นั้น มีความหมายหรือรูปแบบเหมือนกับเอกสารและข้อความเดิม

(๒) ข้อมูลอิเล็กทรอนิกส์ต้องจัดทำหรือแปลงขึ้นด้วยวิธีการที่เชื่อถือได้ในการระบุตัวตนผู้จัดทำหรือแปลงที่รับผิดชอบในการจัดทำหรือแปลงนั้น

(๓) ข้อมูลอิเล็กทรอนิกส์ต้องจัดทำหรือแปลงโดยมีเทคโนโลยีและมาตรการป้องกันมิให้มีการเปลี่ยนแปลงหรือแก้ไขเกิดขึ้นกับข้อมูลนั้น เว้นแต่การรับรองหรือบันทึกเพิ่มเติม ซึ่งไม่มีผลต่อความหมายของข้อมูลอิเล็กทรอนิกส์

รายละเอียดของวิธีการในการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ให้เป็นไปตามที่กำหนดไว้ในข้อ ๔ ถึงข้อ ๙

ข้อ ๔ การจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ให้มีกระบวนการในการจัดทำหรือแปลงเอกสารและข้อความอย่างน้อย ดังนี้

(๑) กระบวนการจัดทำหรือแปลงเอกสารและข้อความให้เป็นข้อมูลอิเล็กทรอนิกส์ด้วยวิธีการทางอิเล็กทรอนิกส์

(๒) กระบวนการตรวจสอบและรับรองว่าข้อมูลอิเล็กทรอนิกส์ที่จัดทำหรือแปลงนั้นมีความหมายเหมือนกับเอกสารและข้อความเดิม

(๓) กระบวนการบันทึกหลักฐานการดำเนินงานการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์

(๔) กระบวนการบันทึกเมตาดาตาในรูปแบบอิเล็กทรอนิกส์ที่เป็นข้อความบรรยายสาระสำคัญของเอกสารและข้อความ ซึ่งต้องครอบคลุมให้สามารถสืบค้นเอกสารและข้อความนั้นได้ถูกต้อง

ข้อ ๕ การจัดทำหรือแปลงเอกสารและข้อความด้วยวิธีการทางอิเล็กทรอนิกส์ ให้มีผู้รับผิดชอบดำเนินงานในการจัดทำหรือแปลงในเรื่องของวิธีการดังกล่าวอย่างน้อยดังต่อไปนี้

(๑) จัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์

(๒) ตรวจสอบและรับรองความถูกต้องและครบถ้วนของข้อมูลอิเล็กทรอนิกส์ที่ได้จากการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ ว่าข้อมูลอิเล็กทรอนิกส์มีความหมายหรือรูปแบบเหมือนกับเอกสารและข้อความเดิม

(๓) ตรวจสอบกระบวนการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ให้เป็นไปตามที่กำหนดไว้

(๔) ตรวจสอบและรับรองความถูกต้องและครบถ้วนของเมตาดาตา ตามข้อ ๔ (๔)

ข้อ ๖ การจัดทำหรือแปลงเอกสารและข้อความด้วยวิธีการทางอิเล็กทรอนิกส์ ให้มีการกำหนดมาตรการเกี่ยวกับการรักษาความมั่นคงปลอดภัยของข้อมูลอิเล็กทรอนิกส์ ซึ่งเป็นวิธีการที่เชื่อถือได้อย่างน้อยต้องครอบคลุมหัวข้อต่อไปนี้

(๑) การระบุตัวตน (Identification)

(๒) การยืนยันตัวตน (Authentication)

(๓) อนุญาตเฉพาะผู้มีสิทธิเข้าถึง (Authorization)

(๔) ความรับผิดชอบต่อผลของการกระทำ (Accountability)

ทั้งนี้ เพื่อให้สามารถยืนยันได้ว่า ข้อมูลอิเล็กทรอนิกส์ที่มีการจัดทำหรือแปลงได้ดำเนินการโดยผู้มีสิทธิในการเข้าถึงเท่านั้น ผู้มีสิทธิในการเข้าถึงดังกล่าวให้หมายความรวมถึงผู้รับผิดชอบดำเนินงานจัดทำหรือแปลงและผู้ที่มีสิทธิตรวจสอบตามข้อ ๕ ด้วย ซึ่งจะเป็นบุคคลเดียวกันหรือไม่ก็ได้

ข้อ ๗ การจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์นั้น ให้ข้อมูลอิเล็กทรอนิกส์มีความละเอียดและความชัดเจนของเอกสารและข้อความเดิม

ข้อ ๘ ให้ผู้จัดทำหรือแปลง มีหน้าที่รักษาและดำรงสภาพของระบบการจัดทำหรือแปลงเอกสารไว้ให้สมบูรณ์เพื่อให้มีการกำกับดูแลหรือการตรวจสอบได้ตลอดเวลาจากคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์หรือหน่วยงานอื่นที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์มอบหมายหรือหน่วยงานที่กำหนดไว้เป็นอย่างอื่นในประกาศฉบับนี้

ข้อ ๙ การดำเนินการตามข้อ ๔ ถึง ข้อ ๘ ให้ผู้จัดทำหรือแปลง จัดทำวิธีปฏิบัติที่สอดคล้องกับลักษณะงานองค์กรและประเภทของการทำธุรกรรมอย่างเหมาะสม โดยให้ใช้ข้อกำหนดวิธีปฏิบัติทั่วไปหรือตามข้อกำหนดวิธีปฏิบัติเฉพาะธุรกรรมบางประเภท ในการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ตามข้อกำหนดแนบท้ายประกาศนี้เป็นมาตรฐานขั้นต่ำในการดำเนินงานแล้วแต่กรณี

ข้อ ๑๐ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ประกาศ ณ วันที่ ๓๐ กันยายน พ.ศ. ๒๕๕๓
จุติ ไกรฤกษ์
รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
ประธานกรรมการธุรกรรมทางอิเล็กทรอนิกส์

ข้อกำหนดแนบท้ายประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
เรื่อง หลักเกณฑ์และวิธีการในการจัดทำหรือแปลงเอกสารและข้อความ
ให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓
ฉบับที่ ๑
ว่าด้วยข้อกำหนดวิธีปฏิบัติในการจัดทำหรือแปลงเอกสารและข้อความ
ให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์

หมวด ๑
บททั่วไป

ข้อ ๑ ในการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ ให้ผู้จัดทำหรือแปลงปฏิบัติตามข้อกำหนดนี้เป็นมาตรฐานขั้นต่ำ เว้นแต่มาตรฐานขั้นต่ำในบางเรื่องนั้นจะมิได้ถูกนำมาใช้

หมวด ๒
วิธีจัดทำหรือแปลงเอกสารและข้อความ

ข้อ ๒ ผู้จัดทำหรือแปลงต้องตรวจสอบเอกสารและข้อความที่จะนำไปจัดทำหรือแปลงให้เป็นข้อมูลอิเล็กทรอนิกส์ โดยพิจารณาความครบถ้วนของข้อความทั้งหมด จำนวนหน้า การจัดเรียงลำดับเนื้อหา รูปแบบของการนำเสนอเอกสารและข้อความ และต้องบันทึกแหล่งที่มาของเอกสารและข้อความนั้น ในกรณีที่เอกสารหรือข้อความที่จัดทำหรือแปลงนั้นเป็นเอกสารต้นฉบับ หรือสำเนา ก็ให้บันทึกและแสดงโดยชัดแจ้งถึงลักษณะเอกสารหรือข้อความนั้นด้วยว่าเป็นต้นฉบับหรือสำเนา

ข้อ ๓ มาตรฐานขั้นต่ำสำหรับความละเอียดของภาพ (Resolution) คือ

(๑) ภาพลายเส้น หรือภาพขาวดำ อย่างน้อย 150 จุดต่อนิ้ว (dot per inch หรือ dpi)

(๒) ภาพสีเทา อย่างน้อย 200 จุดต่อนิ้ว

(๓) ภาพสี อย่างน้อย 300 จุดต่อนิ้ว

(๔) ภาพสำหรับงานเว็บอย่างเดียว อย่างน้อย 72 จุดต่อนิ้ว

ข้อ ๔ มาตรฐานขั้นต่ำสำหรับความละเอียดของสี (Bit Depth) คือ

(๑) ภาพขาว-ดำ มีค่าความละเอียดของสีเท่ากับ 1 บิต (bit)

(๒) ภาพสีเทา (grayscale) มีค่าความละเอียดของสีเท่ากับ 8 บิต

(๓) ภาพสี มีค่าความละเอียดของสีเท่ากับ 24 บิต

ข้อ ๕ มาตรฐานขั้นต่ำสำหรับการแปลงสัญญาณอนาล็อกเป็นสัญญานดิจิทัล ในกรณีที่ข้อความเป็นเสียงต้องมีอัตราสุ่มข้อมูลสัญญาณเสียงขั้นต่ำที่ 44.1 กิโลเฮิร์ตซ (kHz) และจำนวนของข้อมูลสัญญาณเสียงที่สุ่มขั้นต่ำที่ 16 บิต

ข้อ ๖ มาตรฐานขั้นต่ำสำหรับการแปลงสัญญาณอนาล็อกเป็นสัญญานดิจิทัล ในกรณีที่ข้อความเป็นวีดิทัศน์ ต้องมีมาตรฐานขั้นต่ำ ดังนี้

(๑) อัตราการสุ่มข้อมูลตัวอย่างความสว่าง5ของแสง (Luminance) มีมาตรฐานขั้นต่ำที่ 13.5 เมกกะเฮิร์ตซ (MHz)

(๒) จำนวนข้อมูลตัวอย่างความสว่างของแสง มีมาตรฐานขั้นต่ำที่ 8 บิตต่อจุดภาพ (bits per pixel: bpp)

(๓) จำนวนข้อมูลตัวอย่างความเข้มของสี (Chrominance) มีมาตรฐานขั้นต่ำที่ 4 บิตต่อจุดภาพ (bits per pixel: bpp)

(๔) ค่าความสว่างของแสง (Luminance Resolution) เท่ากับ 720 จุดต่อภาพ (pixel) x 485 เส้น (active line)

(๕) ค่าความละเอียดของสี (Chrominance Resolution) เท่ากับ 360 จุดต่อภาพ (pixel) x 485 เส้น (active line)

ข้อ ๗ ผู้จัดทำหรือแปลงต้องตั้งชื่อไฟล์ข้อมูลอิเล็กทรอนิกส์ที่มีความหมายสื่อถึงเนื้อหาของข้อมูลเพื่อสามารถสืบค้นได้ ชื่อไฟล์ดังกล่าวจะต้องไม่ซ้ำกัน

ข้อ ๘ เมื่อดำเนินการแล้ว ผู้จัดทำหรือแปลงต้องตรวจทานความถูกต้อง ครบถ้วน ของข้อมูลอิเล็กทรอนิกส์ที่ได้จัดทำหรือแปลงด้วย

หมวด ๓
การตรวจสอบและรับรอง

ข้อ ๙ ผู้จัดทำหรือแปลงต้องจัดให้มีการตรวจสอบและการรับรองคุณภาพกระบวนการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ และการตรวจสอบและรับรองคุณภาพข้อมูลอิเล็กทรอนิกส์ และจัดให้มีการรายงานการตรวจสอบและรับรองคุณภาพ เพื่อใช้ในการยืนยันระบบการจัดการของตน

ข้อ ๑๐ การตรวจสอบและรับรองคุณภาพต้องครอบคลุมถึงเรื่อง ดังต่อไปนี้

(๑) คุณภาพของเครื่องมือและอุปกรณ์ที่ใช้ในการดำเนินการ

(๒) ขั้นตอนการดำเนินการ

(๓) คุณภาพและความถูกต้องของข้อมูลอิเล็กทรอนิกส์ที่ผ่านการจัดทำหรือแปลง

(๔) คุณภาพและความถูกต้องของข้อมูลอิเล็กทรอนิกส์ที่ใช้ในการระบุตัวตนของผู้จัดทำหรือแปลง

ข้อ ๑๑ ในกรณีการดำเนินการสำหรับข้อมูลอิเล็กทรอนิกส์ที่มีปริมาณมาก หรือการรวมข้อมูลจำนวนมากเป็นชุดเดียว การตรวจสอบและรับรองอาจใช้การสุ่มตัวอย่างในเชิงสถิติ เพื่อตรวจสอบได้

หมวด ๔
การบันทึก

ข้อ ๑๒ ผู้จัดทำหรือแปลงต้องจัดให้มีการบันทึกการดำเนินการไว้เป็นหลักฐาน โดยต้องบันทึกรายการ ดังต่อไปนี้

(๑) ชื่อหรือรายการข้อมูลอิเล็กทรอนิกส์ที่จัดทำหรือแปลง

(๒) ชื่อผู้จัดทำหรือแปลง

(๓) โปรแกรมและรูปแบบที่ใช้ในการจัดทำหรือแปลง

(๔) วัน เดือน ปี และเวลาที่จัดทำหรือแปลง

(๕) หลักฐานการตรวจสอบและรับรองคุณภาพและความถูกต้องของข้อมูลอิเล็กทรอนิกส์ว่ามีความหมายเหมือนกับเอกสารและข้อความเดิม

ข้อ ๑๓ ผู้จัดทำหรือแปลงต้องจัดให้มีการบันทึกเมตาดาตา (Metadata) ที่แสดงสาระสำคัญอันเป็นคุณลักษณะเฉพาะและรายละเอียดของข้อมูลอิเล็กทรอนิกส์นั้นๆ โดยจะต้องประกอบด้วยส่วนประกอบสำคัญของข้อมูลอิเล็กทรอนิกส์ ได้แก่ เนื้อหา (เช่น ชื่อเรื่อง หัวเรื่อง ต้นฉบับ/แหล่งที่มา ขอบเขต) บริบท (เช่น ทรัพย์สินทางปัญญาหรือสิทธิในงานนั้น ผู้สร้างสรรค์ผลงาน ผู้มีส่วนร่วมในผลงาน) และโครงสร้าง (เช่น วัน เดือน ปี ที่สร้างผลงาน ประเภทของเนื้อหา รูปแบบของการนำเสนอผลงาน ตัวบ่งชี้หรือตัวระบุถึงทรัพยากร) ซึ่งจะช่วยให้สามารถสืบค้นเอกสารและข้อความได้อย่างถูกต้องและมีประสิทธิภาพ

หมวด ๕
ผู้รับผิดชอบ

ข้อ ๑๔ ให้ผู้จัดทำหรือแปลงกำหนดตัวบุคคลผู้รับผิดชอบในเรื่องดังต่อไปนี้ ให้ชัดเจน

(๑) ผู้จัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์

(๒) ผู้ตรวจสอบคุณภาพของข้อมูลอิเล็กทรอนิกส์ที่ผ่านการจัดทำหรือแปลง

(๓) ผู้ตรวจสอบและรับรองกระบวนการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ ตามข้อ ๙

(๔) ผู้ตรวจสอบและรับรองความถูกต้องและครบถ้วนของเมตาดาตา ตามข้อ ๑๓

หมวด ๖
ความมั่นคงปลอดภัย

ข้อ ๑๕ ให้ผู้จัดทำหรือแปลงต้องกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลอิเล็กทรอนิกส์ ด้วยวิธีการที่เชื่อถือได้ โดยให้ครอบคลุมมาตรการเกี่ยวกับการรักษาความมั่นคงปลอดภัยของข้อมูลอิเล็กทรอนิกส์ อย่างน้อยต้องครอบคลุมหัวข้อต่อไปนี้

(๑) การลงทะเบียนผู้ใช้งาน (user registration) โดยต้องกำหนดให้มีขั้นตอนการปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานเพื่อแสดงตัวตนเพื่อรับการอนุญาตให้เข้าถึงข้อมูลอิเล็กทรอนิกส์ และการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว

(๒) การบริหารจัดการสิทธิของผู้ใช้งาน (user management) โดยต้องจัดให้มีการควบคุมและจำกัดสิทธิเพื่อเข้าถึงและใช้งานข้อมูลอิเล็กทรอนิกส์แต่ละชนิดตามความเหมาะสม

(๓) การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (user password management) โดยต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม

(๔) การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (review of user access rights) โดยต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานข้อมูลอิเล็กทรอนิกส์ตามระยะเวลาที่กำหนดไว้

(๕) การใช้รหัสผ่าน (password use) โดยต้องกำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ

(๖) การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ ต้องกำหนดข้อปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ในขณะที่ไม่มีผู้ดูแล

ข้อกำหนดแนบท้ายประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
เรื่อง หลักเกณฑ์และวิธีการในการจัดทำหรือแปลงเอกสารและข้อความ
ให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓
ฉบับที่ ๒
ว่าด้วยข้อกำหนดวิธีปฏิบัติในการจัดทำหรือแปลงเอกสารและข้อความ
ให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์
สำหรับระบบการหักบัญชีเช็คด้วยภาพเช็คและระบบการจัดเก็บภาพเช็ค

หมวด ๑
การจัดทำหรือแปลงเช็คต้นฉบับให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์

ข้อ ๑ ธนาคารผู้จัดทำหรือแปลงต้องตรวจสอบความสมบูรณ์ของตัวเช็คตามกฎหมาย และตรวจสอบการปลอมแปลงตัวเช็คโดยตรวจจากเนื้อกระดาษ ขนาดของตัวเช็ค และลายน้ำกลาง ก่อนที่จะนำเข้าระบบการจัดทำหรือแปลงเช็คต้นฉบับให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์

ข้อ ๒ เช็คที่จะนำเข้าระบบการจัดทำหรือแปลงเช็คต้นฉบับให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ต้องเป็นต้นฉบับเท่านั้น

ข้อ ๓ ข้อมูลอิเล็กทรอนิกส์ที่จะส่งเข้าระบบการหักบัญชีเช็คด้วยภาพเช็คและระบบการจัดเก็บภาพเช็คให้ประกอบด้วยข้อมูลเช็ค ภาพเช็ค และเมตาดาตา (Metadata) โดยต้องมีโครงสร้างและสาระสำคัญของธุรกรรมครบถ้วนถูกต้องตามระเบียบธนาคารแห่งประเทศไทยว่าด้วยระบบการหักบัญชีเช็คด้วยภาพเช็คและระบบการจัดเก็บภาพเช็ค

ทั้งนี้ เมตาดาตา (Metadata) ตามวรรคหนึ่ง ต้องสามารถแสดงสาระสำคัญที่เป็นคุณลักษณะและรายละเอียดตามลักษณะเฉพาะของข้อมูลอิเล็กทรอนิกส์นั้นๆ เช่น ค่าแสดงผลการตรวจสอบความสมบูรณ์ของเช็คต้นฉบับ (Physical Condition Tag) ค่าแสดงผลการตรวจสอบภาพเช็ค (IQA Tag)

ข้อ ๔ ธนาคารผู้จัดทำหรือแปลงต้องจัดให้มีระบบการจัดทำหรือแปลงเช็คต้นฉบับให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ เพื่อให้ได้ภาพเช็คตามมาตรฐานภาพเช็คตามระเบียบธนาคารแห่งประเทศไทยว่าด้วยระบบการหักบัญชีเช็คด้วยภาพเช็คและระบบการจัดเก็บภาพเช็ค ซึ่งอย่างน้อยมาตรฐานดังกล่าวต้องมีรูปแบบ ระดับสี และความละเอียด ดังนี้

ภาพที่ ๑ : ด้านหน้า กำหนดเป็น JPEG 8-bit Grayscale 100 dpi
ภาพที่ ๒ : ด้านหน้า กำหนดเป็น TIFF Black & White 200 dpi
ภาพที่ ๓ : ด้านหลัง กำหนดเป็น TIFF Black & White 200 dpi

ข้อ๕ ธนาคารผู้จัดทำหรือแปลงต้องบันทึกข้อมูลอิเล็กทรอนิกส์ที่ได้จากการจัดทำหรือแปลงไว้เป็นไฟล์ข้อมูลอิเล็กทรอนิกส์โดยตั้งชื่อไฟล์ข้อมูลอิเล็กทรอนิกส์ให้มีความหมายสื่อถึงเนื้อหาของข้อมูล มีรูปแบบและโครงสร้างของชื่อที่ช่วยให้สามารถติดตามหรือสืบค้นได้ง่าย และชื่อไฟล์จะต้องไม่ซ้ำกัน ทั้งนี้ ให้เป็นไปตามระเบียบธนาคารแห่งประเทศไทยว่าด้วยระบบการหักบัญชีเช็คด้วยภาพเช็คและระบบการจัดเก็บภาพเช็ค

หมวด ๒
การตรวจสอบและรับรองกระบวนการจัดทำหรือแปลงเช็คต้นฉบับให้อยู่ในรูปของ
ข้อมูลอิเล็กทรอนิกส์ และการรับรองคุณภาพข้อมูลอิเล็กทรอนิกส์

ข้อ ๖ ธนาคารผู้จัดทำหรือแปลงต้องจัดให้มีระบบการตรวจสอบและรับรองกระบวนการจัดทำหรือแปลงเช็คต้นฉบับให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ และการรับรองคุณภาพข้อมูลอิเล็กทรอนิกส์

ข้อ ๗ ธนาคารผู้จัดทำหรือแปลงต้องตรวจสอบคุณภาพของเครื่องมือหรืออุปกรณ์ที่ใช้ในกระบวนการจัดทำหรือแปลงเช็คต้นฉบับให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ เพื่อให้มั่นใจว่าเครื่องมือหรืออุปกรณ์ดังกล่าวสามารถจัดทำหรือแปลงเช็คต้นฉบับให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ได้อย่างมีประสิทธิภาพสม่ำเสมอ

ข้อ ๘ ธนาคารผู้จัดทำหรือแปลงต้องตรวจสอบกระบวนการจัดทำหรือแปลงเช็คต้นฉบับให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ ให้ดำเนินการไปตามขั้นตอนและกระบวนการปฏิบัติที่ได้กำหนดไว้ในคู่มือการทำงานที่ธนาคารผู้จัดทำหรือแปลงจัดทำขึ้น โดยจัดให้มีผู้ตรวจสอบและรับรองอย่างน้อยปีละหนึ่งครั้ง และรายงานผลการตรวจสอบและรับรองเสนอผู้บริหารของธนาคารผู้จัดทำหรือแปลงและธนาคารแห่งประเทศไทย

ข้อ ๙ ธนาคารผู้จัดทำหรือแปลงต้องตรวจสอบคุณภาพเพื่อดูว่าข้อมูลอิเล็กทรอนิกส์ที่ได้จากการจัดทำหรือแปลงนั้น สามารถอ่านได้ และมีความคมชัด ความสว่าง ขนาด รูปแบบ เป็นไปตามมาตรฐานภาพเช็คตามที่กำหนดในระเบียบธนาคารแห่งประเทศไทยว่าด้วยระบบการหักบัญชีเช็คด้วยภาพเช็คและระบบการจัดเก็บภาพเช็ค

ข้อ ๑๐ ธนาคารผู้จัดทำหรือแปลงต้องรับรองคุณภาพและความถูกต้องของข้อมูลอิเล็กทรอนิกส์ที่ได้จากการจัดทำหรือแปลง โดยลงลายมือชื่ออิเล็กทรอนิกส์ก่อนส่งข้อมูลอิเล็กทรอนิกส์ที่ได้จากการจัดทำหรือแปลงเข้าระบบการหักบัญชีเช็คด้วยภาพเช็คและระบบการจัดเก็บภาพเช็ค เพื่อให้สามารถยืนยันได้ว่า ข้อมูลอิเล็กทรอนิกส์ที่ได้จากการจัดทำหรือแปลงมีความหมายหรือรูปแบบเหมือนกับเช็คต้นฉบับ

หมวด ๓
การบันทึกหลักฐานการดำเนินงาน

ข้อ ๑๑ ธนาคารผู้จัดทำหรือแปลงต้องบันทึกหลักฐานการดำเนินงานจัดทำหรือแปลงเช็คต้นฉบับให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ เพื่อใช้อ้างอิงการดำเนินงานและสถานะการดำเนินงานที่เกิดขึ้น รวมทั้งเพื่อใช้ในการตรวจสอบประวัติการจัดทำหรือแปลงเช็คต้นฉบับให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ โดยอย่างน้อยต้องมีการบันทึกหลักฐานการดำเนินงาน ดังต่อไปนี้

(๑) ชื่อไฟล์ข้อมูลอิเล็กทรอนิกส์

(๒) ชื่อผู้ดำเนินงานในแต่ละขั้นตอนของระบบการจัดทำหรือแปลงเช็คต้นฉบับให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์

(๓) วัน เดือน ปีและเวลาที่ดำเนินงานในแต่ละขั้นตอนของระบบการจัดทำหรือแปลงเช็คต้นฉบับให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์

หมวด ๔
มาตรการเกี่ยวกับการรักษาความมั่นคงปลอดภัยของข้อมูลอิเล็กทรอนิกส์

ข้อ ๑๒ ธนาคารผู้จัดทำหรือแปลงต้องจัดให้มีมาตรการเกี่ยวกับการรักษาความมั่นคงปลอดภัยของข้อมูลอิเล็กทรอนิกส์ที่เชื่อถือได้ อย่างน้อยต้องครอบคลุมเรื่องดังต่อไปนี้

(๑) การระบุตัวตนผู้ดำเนินงาน (Identification) ในแต่ละขั้นตอนของระบบการจัดทำหรือแปลงเช็คต้นฉบับให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์

(๒) การยืนยันตัวตนผู้ดำเนินงาน (Authentication) ในแต่ละขั้นตอนของระบบการจัดทำหรือแปลงเช็คต้นฉบับให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์

(๓) การอนุญาตเฉพาะผู้มีสิทธิเข้าถึงระบบการจัดทำหรือแปลงเช็คต้นฉบับให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ (Authorization) รวมทั้งจัดให้มีระบบการรักษาความมั่นคงปลอดภัยทางกายภาพเพื่อป้องกันไม่ให้ผู้ที่ไม่มีหน้าที่เกี่ยวข้องเข้าถึงระบบการจัดทำหรือแปลงเช็คต้นฉบับให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์

(๔) ความรับผิดชอบต่อผลของการกระทำ (Accountability) โดยมีการบันทึกหลักฐานการดำเนินงานจัดทำหรือแปลงเช็คต้นฉบับให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ เพื่อป้องกันการปฏิเสธความรับผิด และใช้ในการตรวจสอบประวัติการจัดทำหรือแปลงเช็คต้นฉบับให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์

ทั้งนี้ เพื่อให้สามารถยืนยันได้ว่า ข้อมูลอิเล็กทรอนิกส์สำหรับระบบการหักบัญชีเช็คด้วยภาพเช็คและระบบการจัดเก็บภาพเช็คได้มีการจัดทำหรือแปลงที่ดำเนินการโดยผู้มีสิทธิในการเข้าถึงเท่านั้น

หมวด ๕
เบ็ดเตล็ด

ข้อ ๑๓ ให้ธนาคารแห่งประเทศไทยเป็นผู้ดูแลการดำเนินการตามข้อกำหนดวิธีปฏิบัตินี้ และให้จัดทำรายงานเสนอคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ทราบอย่างน้อยปีละหนึ่งครั้ง

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
เรื่อง การรับรองสิ่งพิมพ์ออก พ.ศ. ๒๕๕๕

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

เรื่อง การรับรองสิ่งพิมพ์ออก

พ.ศ. ๒๕๕๕

โดยที่กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์กำหนดให้มีหน่วยงานรับรองสิ่งพิมพ์ออกของข้อมูลอิเล็กทรอนิกส์ เพื่อให้สิ่งพิมพ์ออกสามารถใช้อ้างอิงแทนข้อมูลอิเล็กทรอนิกส์ และมีผลใช้แทนต้นฉบับได้

อาศัยอำนาจตามความในมาตรา ๑๐ วรรคสี่ แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ ๒) พ.ศ. ๒๕๕๑ คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง การรับรองสิ่งพิมพ์ออก พ.ศ. ๒๕๕๕”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ในประกาศนี้

“สิ่งพิมพ์ออก” หมายความว่า สิ่งพิมพ์ออกของข้อมูลอิเล็กทรอนิกส์ที่มีการนำเสนอหรือเก็บรักษาเป็นเอกสารต้นฉบับ

“ระบบการพิมพ์ออก” หมายความว่า ระบบที่ใช้ในการนำเข้าข้อมูลอิเล็กทรอนิกส์ที่เป็นต้นฉบับของสิ่งพิมพ์ออก และการจัดทำสิ่งพิมพ์ออกสำหรับใช้อ้างอิงข้อความของข้อมูลอิเล็กทรอนิกส์

“คณะกรรมการ” หมายความว่า คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

“หน่วยงานรับรองสิ่งพิมพ์ออก” หมายความว่า คณะกรรมการหรือหน่วยงานที่มีอำนาจรับรองสิ่งพิมพ์ออกตามที่คณะกรรมการประกาศกำหนด

ข้อ ๔ การจัดทำสิ่งพิมพ์ออกในกรณีดังต่อไปนี้ ให้ถือว่าได้มีการรับรองสิ่งพิมพ์ออกโดยหน่วยงานรับรองสิ่งพิมพ์ออกและมีผลใช้แทนต้นฉบับได้

(๑) เจ้าของข้อมูลอิเล็กทรอนิกส์ ผู้ควบคุมข้อมูลอิเล็กทรอนิกส์ หรือบุคคลภายใต้บังคับของเจ้าของข้อมูลอิเล็กทรอนิกส์หรือผู้ควบคุมข้อมูลอิเล็กทรอนิกส์ เป็นผู้จัดทำสิ่งพิมพ์ออกจากระบบการพิมพ์ออกที่อยู่ภายใต้การควบคุมดูแลของเจ้าของข้อมูลอิเล็กทรอนิกส์หรือผู้ควบคุมข้อมูลอิเล็กทรอนิกส์

(๒) หน่วยงานของรัฐที่มีอำนาจในการเก็บรักษาหรือควบคุมข้อมูลอิเล็กทรอนิกส์ของบุคคลอื่นหรือบุคคลภายใต้บังคับหน่วยงานของรัฐ เป็นผู้จัดทำสิ่งพิมพ์ออกจากระบบการพิมพ์ออกที่อยู่ภายใต้การควบคุมดูแลของหน่วยงานของรัฐนั้น

(๓) หน่วยงานของรัฐที่มีอำนาจตามกฎหมายในการกำกับหรือควบคุมดูแล หรือหน่วยงานที่อยู่ภายใต้การกำกับหรือควบคุมดูแลของหน่วยงานของรัฐ เป็นผู้จัดทำสิ่งพิมพ์ออกจากระบบการพิมพ์ออกที่มีมาตรฐานที่เทียบเท่าหรือมีความเหมาะสมกว่าหลักเกณฑ์และวิธีการที่กำหนดในประกาศนี้

หมวด ๑
หน่วยงานรับรองสิ่งพิมพ์ออก

ข้อ ๕ หน่วยงานรับรองสิ่งพิมพ์ออกต้องมีคุณสมบัติและไม่มีลักษณะต้องห้าม ดังต่อไปนี้

(๑) ต้องจัดให้มีบุคลากรซึ่งมีความรู้ ความเชี่ยวชาญและประสบการณ์ทางเทคนิคที่เหมาะสมสำหรับการปฏิบัติหน้าที่เป็นหน่วยงานรับรองสิ่งพิมพ์ออกในจำนวนที่เพียงพอ โดยอย่างน้อยต้องมีบุคลากรซึ่งมีความเชี่ยวชาญหรือประสบการณ์ในด้าน ดังต่อไปนี้

(ก) ด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

(ข) ด้านเทคโนโลยีการระบุตัวตน (Identification) และการยืนยันตัวตน (Authentication)

(ค) ด้านระบบเอกสารที่ทำในรูปของข้อมูลอิเล็กทรอนิกส์

(ง) ด้านการตรวจสอบและประเมินผลความมั่นคงปลอดภัยของระบบสารสนเทศ

(๒) ต้องจัดให้มีเครื่องมือหรือวิธีการที่เพียงพอและมีมาตรฐานสำหรับใช้ในการตรวจสอบว่าระบบการพิมพ์ออกและกระบวนการจัดทำสิ่งพิมพ์ออก มีความมั่นคงปลอดภัยและสามารถจัดทำสิ่งพิมพ์ออกที่มีข้อความถูกต้องครบถ้วนตรงกับข้อมูลอิเล็กทรอนิกส์

(๓) ไม่เคยถูกสั่งยกเลิกการเป็นหน่วยงานรับรองสิ่งพิมพ์ออกตามข้อ ๙ หรือเคยถูกสั่งยกเลิกแต่ยังไม่พ้นกำหนดห้าปีนับแต่วันที่ถูกสั่งยกเลิกการเป็นหน่วยงานรับรองสิ่งพิมพ์ออก

(๔) ต้องไม่มีส่วนได้เสียในกิจการของผู้ขอให้รับรองระบบการพิมพ์ออก และจะต้องไม่มีเหตุที่ทำให้หน่วยงานรับรองสิ่งพิมพ์ออกขาดความเป็นอิสระและความเป็นกลางในการดำเนินงาน

(๕) ต้องไม่มีส่วนได้เสียในกิจการของบุคคลหรือนิติบุคคลที่เป็นผู้พัฒนา ขาย จำหน่าย จัดทำ จัดซื้อ จัดหา หรือให้เช่าระบบฮาร์ดแวร์และซอฟต์แวร์ให้กับผู้ขอให้รับรองระบบการพิมพ์ออก

คณะกรรมการอาจออกประกาศกำหนดคุณสมบัติหรือลักษณะต้องห้ามประการอื่นของหน่วยงานรับรองสิ่งพิมพ์ออกเพิ่มเติมตามความเหมาะสมอีกก็ได้

ข้อ ๖ ในกรณีหน่วยงานรับรองสิ่งพิมพ์ออกเป็นนิติบุคคลประเภทห้างหุ้นส่วนจดทะเบียน ห้างหุ้นส่วนจำกัด บริษัทจำกัด หรือบริษัทมหาชนจำกัด กรรมการหรือผู้มีอำนาจจัดการแทนนิติบุคคลของหน่วยงานรับรองสิ่งพิมพ์ออกต้องมีคุณสมบัติและไม่มีลักษณะต้องห้าม ดังต่อไปนี้

(๑) มีอายุไม่ต่ำกว่ายี่สิบปีบริบูรณ์

(๒) มีภูมิลำเนาหรือถิ่นที่อยู่ในราชอาณาจักร

(๓) ไม่เป็นบุคคลล้มละลาย คนไร้ความสามารถ หรือคนเสมือนไร้ความสามารถ

(๔) ไม่เคยได้รับโทษจำคุกโดยคำพิพากษาถึงที่สุดให้จำคุก เว้นแต่เป็นโทษสำหรับความผิดที่ได้กระทำโดยประมาทหรือความผิดลหุโทษ

(๕) ไม่เป็นกรรมการหรือผู้ซึ่งมีอำนาจจัดการของหน่วยงานรับรองสิ่งพิมพ์ออกที่เคยถูกสั่งยกเลิกการเป็นหน่วยงานรับรองสิ่งพิมพ์ออก

คณะกรรมการอาจออกประกาศกำหนดคุณสมบัติหรือลักษณะต้องห้ามประการอื่นของหน่วยงานรับรองสิ่งพิมพ์ออกซึ่งเป็นนิติบุคคลตามวรรคหนึ่งเพิ่มเติมตามความเหมาะสมอีกก็ได้

ข้อ ๗ ผู้ประสงค์จะเป็นหน่วยงานรับรองสิ่งพิมพ์ออกให้ยื่นเอกสารหลักฐาน ดังต่อไปนี้ต่อคณะกรรมการหรือหน่วยงานที่คณะกรรมการมอบหมาย

(๑) คำขอให้ความเห็นชอบการเป็นหน่วยงานรับรองสิ่งพิมพ์ออก

(๒) นโยบายและมาตรการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ซึ่งอย่างน้อยต้องมีมาตรฐานที่เทียบเท่าหรือไม่ต่ำกว่าหลักเกณฑ์ตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓

(๓) กระบวนการรับรองระบบการพิมพ์ออก

(๔) นโยบาย มาตรฐานและมาตรการในการตรวจระบบการพิมพ์ออก

(๕) รายชื่อผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศ ด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ ด้านเทคโนโลยีการระบุตัวตน (Identification) และการยืนยันตัวตน (Authentication) ด้านระบบเอกสารที่ทำในรูปของข้อมูลอิเล็กทรอนิกส์ ด้านการตรวจสอบและประเมินผลความมั่นคงปลอดภัยของระบบสารสนเทศ รวมทั้งด้านอื่นที่เกี่ยวข้องตามที่คณะกรรมการประกาศกำหนด

(๖) เอกสารอื่นใดที่คณะกรรมการประกาศกำหนด

ข้อ ๘ คณะกรรมการจะประกาศให้ผู้ยื่นคำขอตามข้อ ๗ เป็นหน่วยงานรับรองสิ่งพิมพ์ออกเมื่อคณะกรรมการหรือหน่วยงานที่คณะกรรมการมอบหมายตรวจสอบและพิจารณาแล้วเห็นว่าผู้ยื่นคำขอมีคุณสมบัติและไม่มีลักษณะต้องห้ามตามข้อ ๕ และข้อ ๖ และได้ยื่นเอกสารหลักฐานตามข้อ ๗ ถูกต้องครบถ้วนแล้ว

คณะกรรมการอาจมอบหมายให้หน่วยงานใดทำหน้าที่ตรวจสอบกระบวนการรับรองระบบการพิมพ์ออกของผู้ยื่นคำขอเป็นหน่วยงานรับรองสิ่งพิมพ์ออกตามวรรคหนึ่งได้

ข้อ ๙ คณะกรรมการอาจยกเลิกการให้ความเห็นชอบการเป็นหน่วยงานรับรองสิ่งพิมพ์ออกเมื่อปรากฏว่าหน่วยงานรับรองสิ่งพิมพ์ออกกระทำการอย่างหนึ่งอย่างใด ดังต่อไปนี้

(๑) ขาดคุณสมบัติหรือมีลักษณะต้องห้ามตามข้อ ๕ หรือข้อ ๖

(๒) ฝ่าฝืนหรือไม่ปฏิบัติตามหลักเกณฑ์ที่กำหนดในประกาศนี้ รวมทั้งแนวปฏิบัติอื่นใดที่ออกโดยคณะกรรมการ

(๓) กระทำการใดจนเป็นเหตุให้เชื่อได้ว่าอาจส่งผลกระทบต่อความน่าเชื่อถือในการรับรองระบบการพิมพ์ออก

ข้อ ๑๐ เมื่อปรากฏเหตุแห่งการยกเลิกตามข้อ ๙ คณะกรรมการอาจสั่งให้หน่วยงานรับรองสิ่งพิมพ์ออกแก้ไขหรือดำเนินการอื่นใดตามที่คณะกรรมการมีคำสั่งภายในระยะเวลาที่กำหนด

ในกรณีที่หน่วยงานรับรองสิ่งพิมพ์ออกไม่ดำเนินการแก้ไขตามคำสั่งคณะกรรมการหรือกระทำการอันเป็นการฝ่าฝืนการกระทำนั้นอีก คณะกรรมการอาจยกเลิกการให้ความเห็นชอบการเป็นหน่วยงานรับรองสิ่งพิมพ์ออก

ข้อ ๑๑ ให้หน่วยงานรับรองสิ่งพิมพ์ออกมีหน้าที่ต้องรายงานผลการดำเนินงานในการรับรองระบบการพิมพ์ออก และรายงานการดำรงไว้ซึ่งคุณสมบัติหรือการเปลี่ยนแปลงใด ๆ ในคุณสมบัติอันเป็นเงื่อนไขในการเป็นหน่วยงานรับรองสิ่งพิมพ์ออกตามข้อ ๕ และข้อ ๖ ต่อคณะกรรมการหรือหน่วยงานที่คณะกรรมการมอบหมายทุกหนึ่งปีนับแต่วันที่ได้รับการประกาศให้เป็นหน่วยงานรับรองสิ่งพิมพ์ออก เว้นแต่คณะกรรมการจะกำหนดเป็นอย่างอื่น ทั้งนี้ ตามแบบรายงานที่คณะกรรมการหรือหน่วยงานที่คณะกรรมการมอบหมายกำหนด

หมวด ๒
การรับรอง

ข้อ ๑๒ หน่วยงานรับรองสิ่งพิมพ์ออกจะรับรองระบบการพิมพ์ออกของผู้ขอให้รับรองระบบการพิมพ์ออก เมื่อตรวจสอบพบว่าระบบการพิมพ์ออกเป็นไปตามหลักเกณฑ์และวิธีการที่กำหนดในหมวดนี้ โดยให้ถือเป็นมาตรฐานขั้นต่ำ เว้นแต่มาตรฐานขั้นต่ำในบางเรื่องนั้นจะมิได้ถูกนำมาใช้

ข้อ ๑๓ ให้หน่วยงานรับรองสิ่งพิมพ์ออกพิจารณารับรองระบบการพิมพ์ออก โดยคำนึงถึงหลักเกณฑ์ ดังต่อไปนี้

(๑) ระบบการพิมพ์ออกมีกระบวนการที่ทำให้มั่นใจได้ว่าสิ่งพิมพ์ออกมีข้อความถูกต้องครบถ้วนตรงกับข้อมูลอิเล็กทรอนิกส์ โดยผู้ขอให้รับรองระบบการพิมพ์ออกต้องจัดให้มีกระบวนการในการตรวจสอบและรับรองความถูกต้องและครบถ้วนของสิ่งพิมพ์ออก

(๒) คุณภาพและประสิทธิภาพของเครื่องมือและอุปกรณ์ที่ใช้ในระบบการพิมพ์ออก

(๓) วิธีการที่ใช้ในการระบุตัวตนผู้ที่เกี่ยวข้องกับระบบการพิมพ์ออก

(๔) การดำเนินการอื่นใดที่จำเป็นเพื่อรับรองว่าระบบการพิมพ์ออกมีความสอดคล้องตรงตามหลักเกณฑ์หรือมาตรฐานตามที่คณะกรรมการหรือหน่วยงานที่คณะกรรมการมอบหมายประกาศกำหนดไว้

ข้อ ๑๔ หน่วยงานรับรองสิ่งพิมพ์ออกจะรับรองระบบการพิมพ์ออก เมื่อระบบการพิมพ์ออกเป็นไปตามหลักเกณฑ์ ดังต่อไปนี้

(๑) มีกระบวนการที่มีความมั่นคงปลอดภัยด้านสารสนเทศ ซึ่งมีมาตรฐานไม่ต่ำกว่าหลักเกณฑ์ตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ หรือมาตรฐานอื่นที่เทียบเท่า

(๒) มีระบบสำรองข้อมูลอิเล็กทรอนิกส์ (Backup) และระบบการกู้คืนข้อมูล (Data recovery) ที่เหมาะสม

(๓) ได้จัดทำโดยมีเทคโนโลยีและมาตรการป้องกันมิให้มีการเปลี่ยนแปลงหรือแก้ไขข้อมูลอิเล็กทรอนิกส์ เว้นแต่เป็นการรับรองหรือบันทึกเพิ่มเติมโดยผู้ที่ได้รับอนุญาต ซึ่งไม่มีผลต่อความถูกต้องของข้อมูลอิเล็กทรอนิกส์

(๔) มีกระบวนการบันทึกหลักฐานการรับรองหรือบันทึกเพิ่มเติมข้อมูลอิเล็กทรอนิกส์

(๕) มีกระบวนการบันทึกหลักฐานการจัดทำสิ่งพิมพ์ออกเพื่อใช้ในการตรวจสอบประวัติการจัดทำสิ่งพิมพ์ออก

(๖) มีวิธีการที่เชื่อถือได้ในการระบุตัวตนผู้ที่เกี่ยวข้องกับระบบการพิมพ์ออก โดยอย่างน้อยต้องครอบคลุมเรื่องดังต่อไปนี้

(ก) การระบุตัวตน (Identification)

(ข) การยืนยันตัวตน (Authentication)

(ค) การอนุญาตเฉพาะผู้มีสิทธิเข้าถึง (Authorization)

(ง) ความรับผิดชอบต่อผลของการกระทำ (Accountability)

ทั้งนี้ เพื่อให้ยืนยันได้ว่าการจัดทำสิ่งพิมพ์ออกได้ดำเนินการโดยผู้มีสิทธิในการเข้าถึงเท่านั้น

(๗) มีระบบการจัดเก็บเอกสารที่ทำในรูปของข้อมูลอิเล็กทรอนิกส์ที่มีความมั่นคงปลอดภัยของระบบสารสนเทศ และสิ่งพิมพ์ออกสามารถแสดงหรืออ้างอิงข้อความเพื่อใช้ตรวจสอบในภายหลังได้ โดยมีรายละเอียดเกี่ยวกับข้อมูลที่ใช้ในการตรวจสอบความถูกต้องครบถ้วนตรงกับข้อมูลอิเล็กทรอนิกส์ เช่น วันเดือนปีที่มีการจัดทำสิ่งพิมพ์ออก เวลาที่มีการจัดทำสิ่งพิมพ์ออกซึ่งอ้างอิงตามเวลามาตรฐานประเทศไทย ตำแหน่งของเว็บเพจ เป็นต้น

ข้อ ๑๕ หน่วยงานรับรองสิ่งพิมพ์ออกอาจจัดให้มีเครื่องหมายหรือสัญลักษณ์อื่นใดที่ปรากฏในสิ่งพิมพ์ออก เพื่อยืนยันว่าสิ่งพิมพ์ออกได้จัดทำผ่านระบบการพิมพ์ออกที่ผ่านการรับรองโดยหน่วยงานรับรองสิ่งพิมพ์ออก

ข้อ ๑๖ สิ่งพิมพ์ออกที่ออกจากระบบการพิมพ์ออกซึ่งได้รับการรับรองโดยหน่วยงานรับรองสิ่งพิมพ์ออก เป็นสิ่งพิมพ์ออกที่สามารถใช้แทนต้นฉบับได้

ข้อ ๑๗ ให้ผู้จัดทำสิ่งพิมพ์ออกมีหน้าที่ ดังต่อไปนี้

(๑) ตรวจสอบคุณภาพเครื่องมือหรืออุปกรณ์ที่ใช้ในการจัดทำสิ่งพิมพ์ออก เพื่อให้มั่นใจได้ว่าเครื่องมือหรืออุปกรณ์ดังกล่าว สามารถจัดทำสิ่งพิมพ์ออกที่มีข้อความถูกต้องครบถ้วนตรงกับข้อมูลอิเล็กทรอนิกส์

(๒) ตรวจทานความถูกต้องครบถ้วนของสิ่งพิมพ์ออกที่ได้จัดทำกับข้อมูลอิเล็กทรอนิกส์ตามวิธีการที่ระบบการพิมพ์ออกกำหนดไว้

ข้อ ๑๘ เพื่อประโยชน์ในการควบคุมดูแลความน่าเชื่อถือของระบบการพิมพ์ออก หน่วยงานรับรองสิ่งพิมพ์ออกอาจเรียกให้ผู้ขอให้รับรองระบบการพิมพ์ออกมาให้ข้อมูลหรือส่งเอกสารใด ๆ ที่เกี่ยวข้องกับระบบการพิมพ์ออก รวมทั้งให้สามารถตรวจสอบระบบการพิมพ์ออกได้อย่างน้อยทุกสองปี

ข้อ ๑๙ หน่วยงานรับรองสิ่งพิมพ์ออกอาจยกเลิกการรับรองระบบการพิมพ์ออก เมื่อปรากฏว่าระบบการพิมพ์ออกไม่เป็นไปตามหลักเกณฑ์และวิธีการที่กำหนดในหมวดนี้

เมื่อปรากฏเหตุแห่งการยกเลิกตามวรรคหนึ่ง หน่วยงานรับรองสิ่งพิมพ์ออกอาจสั่งให้ผู้ที่ได้รับการรับรองระบบการพิมพ์ออกแก้ไขหรือดำเนินการอื่นใดตามที่หน่วยงานรับรองสิ่งพิมพ์ออกกำหนด

ในกรณีที่ผู้ที่ได้รับการรับรองระบบการพิมพ์ออกไม่ดำเนินการแก้ไขตามคำสั่งของหน่วยงานรับรองสิ่งพิมพ์ออกหรือกระทำการอันเป็นการฝ่าฝืนการกระทำนั้นอีก หน่วยงานรับรองสิ่งพิมพ์ออกอาจยกเลิกการรับรองระบบการพิมพ์ออกก็ได้

ประกาศ ณ วันที่ ๑๗ มกราคม พ.ศ. ๒๕๕๕
นาวาอากาศเอก อนุดิษฐ์ นาครทรรพ
รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
ประธานกรรมการธุรกรรมทางอิเล็กทรอนิกส์

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
เรื่อง หน่วยงานรับรองสิ่งพิมพ์ออก พ.ศ. ๒๕๕๕

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

เรื่อง หน่วยงานรับรองสิ่งพิมพ์ออก

พ.ศ. ๒๕๕๕

เพื่อให้มีหน่วยงานที่มีอำนาจในการรับรองสิ่งพิมพ์ออกของข้อมูลอิเล็กทรอนิกส์ ให้สามารถใช้อ้างอิงแทนข้อมูลอิเล็กทรอนิกส์ และมีผลใช้แทนต้นฉบับได้

อาศัยอำนาจตามความในมาตรา ๑๐ วรรคสี่ แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ ๒) พ.ศ. ๒๕๕๑ คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์จึงประกาศให้ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) เป็นหน่วยงานรับรองสิ่งพิมพ์ออก

ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ประกาศ ณ วันที่ ๑๗ มกราคม พ.ศ. ๒๕๕๕
นาวาอากาศเอก อนุดิษฐ์ นาครทรรพ
รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
ประธานกรรมการธุรกรรมทางอิเล็กทรอนิกส์

พระราชกฤษฎีกากำหนดประเภทธุรกรรมในทางแพ่งและพาณิชย์ที่ยกเว้นมิให้นำกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์มาใช้บังคับ

พ.ศ. ๒๕๔๙

พระราชกฤษฎีกา

กำหนดประเภทธุรกรรมในทางแพ่งและพาณิชย์ที่ยกเว้นมิให้นำ
กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์มาใช้บังคับ
พ.ศ. ๒๕๔๙

ภูมิพลอดุลยเดช ป.ร.

ให้ไว้ ณ วันที่ ๓ มีนาคม พ.ศ. ๒๕๔๙
เป็นปีที่ ๖๑ ในรัชกาลปัจจุบัน

พระบาทสมเด็จพระปรมินทรมหาภูมิพลอดุลยเดช มีพระบรมราชโองการโปรดเกล้า ฯ ให้ประกาศว่า

โดยที่เป็นการสมควรกำหนดประเภทธุรกรรมในทางแพ่งและพาณิชย์ที่ยกเว้นมิให้นำกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์มาใช้บังคับ

อาศัยอำนาจตามความในมาตรา ๒๒๑ ของรัฐธรรมนูญแห่งราชอาณาจักรไทย และมาตรา ๓ วรรคหนึ่ง แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ อันเป็นกฎหมายที่มีบทบัญญัติบางประการเกี่ยวกับการจำกัดสิทธิและเสรีภาพของบุคคล ซึ่งมาตรา ๒๙ ประกอบกับมาตรา ๕๐ ของรัฐธรรมนูญแห่งราชอาณาจักรไทย บัญญัติให้กระทำได้โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมาย จึงทรงพระกรุณาโปรดเกล้า ฯ ให้ตราพระราชกฤษฎีกาขึ้นไว้ ดังต่อไปนี้

มาตรา ๑ พระราชกฤษฎีกานี้เรียกว่า “พระราชกฤษฎีกากำหนดประเภทธุรกรรมในทางแพ่งและพาณิชย์ที่ยกเว้นมิให้นำกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์มาใช้บังคับ พ.ศ. ๒๕๔๙”

มาตรา ๒ พระราชกฤษฎีกานี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

มาตรา ๓ มิให้นำบทบัญญัติตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์มาใช้บังคับแก่ธุรกรรมดังต่อไปนี้

(๑) ธุรกรรมเกี่ยวกับครอบครัว

(๒) ธุรกรรมเกี่ยวกับมรดก

มาตรา ๔ ให้นายกรัฐมนตรีรักษาการตามพระราชกฤษฎีกานี้

ผู้รับสนองพระบรมราชโองการ
พันตำรวจโท ทักษิณ ชินวัตร
นายกรัฐมนตรี

หมายเหตุ :- เหตุผลในการประกาศใช้พระราชกฤษฎีกาฉบับนี้ คือ ปัจจุบัน แม้ว่าพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ ได้บัญญัติรับรองสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์และลายมือชื่ออิเล็กทรอนิกส์ให้เท่าเทียมกับธุรกรรมที่ทำบนกระดาษและการลงลายมือชื่อไว้แล้วก็ตาม แต่เนื่องจากการทำธุรกรรมบางประเภทยังไม่เหมาะสมที่จะให้กระทำได้ด้วยวิธีการทางอิเล็กทรอนิกส์ สมควรตราพระราชกฤษฎีกากำหนดประเภทธุรกรรมในทางแพ่งและพาณิชย์ที่ยกเว้นมิให้นำกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์มาใช้บังคับ จึงจำเป็นต้องตราพระราชกฤษฎีกานี้

พระราชกฤษฎีกา
กำหนดหลักเกณฑ์และวิธีการ
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 รวมทั้งมีวิธีการแจ้งสิทธิและหน้าที่ในกระบวนการพิจารณาทางปกครองตามความจำเป็นแก่กรณี ในกรณีที่กฎหมายกำหนดให้ต้องแจ้งให้คู่กรณีทราบ

(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

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
เรื่อง แนวนโยบายและแนวปฏิบัติ
ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของหน่วยงานของรัฐ
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) จัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งาน และจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

(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

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
เรื่อง แนวนโยบายและแนวปฏิบัติ
ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของหน่วยงานของรัฐ (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

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
เรื่อง แนวนโยบายและแนวปฏิบัติ
ในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ
พ.ศ. ๒๕๕๓

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ

พ.ศ. ๒๕๕๓

ข้อมูลส่วนบุคคลที่มีการรวบรวม จัดเก็บ ใช้หรือเผยแพร่ในรูปของข้อมูลอิเล็กทรอนิกส์เป็นสิทธิมนุษยชนขั้นพื้นฐานที่ได้รับความคุ้มครอง ซึ่งปัจจุบันมีการนำระบบสารสนเทศและการสื่อสารมาประยุกต์ใช้ประกอบการทำธุรกรรมทางอิเล็กทรอนิกส์อย่างแพร่หลาย และเพื่อให้การทำธุรกรรมทางอิเล็กทรอนิกส์ของหน่วยงานของรัฐมีความมั่นคงปลอดภัย ความน่าเชื่อถือ และมีการคุ้มครองข้อมูลส่วนบุคคล คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์เห็นสมควรกำหนดแนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐให้มีมาตรฐานเดียวกัน

อาศัยอำนาจตามความในมาตรา ๖ มาตรา ๗ และมาตรา ๘ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์จึงออกประกาศฉบับนี้ เพื่อเป็นแนวทางเบื้องต้น ให้หน่วยงานของรัฐใช้ในการกำหนดนโยบายและข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลสำหรับการทำธุรกรรมทางอิเล็กทรอนิกส์ดังต่อไปนี้

ข้อ ๑ ให้หน่วยงานของรัฐซึ่งรวบรวม จัดเก็บ ใช้ เผยแพร่ หรือดำเนินการอื่นใดเกี่ยวกับข้อมูลของผู้ใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ จัดทำนโยบายในการคุ้มครองข้อมูลส่วนบุคคลไว้เป็นลายลักษณ์อักษร โดยให้มีสาระสำคัญอย่างน้อย ดังนี้

(๑) การเก็บรวบรวมข้อมูลส่วนบุคคลอย่างจำกัด

การจัดเก็บรวบรวมข้อมูลส่วนบุคคลให้มีขอบเขตจำกัด และใช้วิธีการที่ชอบด้วยกฎหมายและเป็นธรรม และให้เจ้าของข้อมูลทราบหรือได้รับความยินยอมจากเจ้าของข้อมูลตามแต่กรณี

(๒) คุณภาพของข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคลที่รวบรวมและจัดเก็บให้เป็นไปตามอำนาจหน้าที่และวัตถุประสงค์ในการดำเนินงานของหน่วยงานของรัฐตามกฎหมาย

(๓) การระบุวัตถุประสงค์ในการเก็บรวบรวม

ให้บันทึกวัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลในขณะที่มีการรวบรวมและจัดเก็บ รวมถึงการนำข้อมูลนั้นไปใช้ในภายหลัง และหากมีการเปลี่ยนแปลงวัตถุประสงค์ของการเก็บรวบรวมข้อมูลให้จัดทำบันทึกแก้ไขเพิ่มเติมไว้เป็นหลักฐาน

(๔) ข้อจำกัดในการนำข้อมูลส่วนบุคคลไปใช้

ห้ามมิให้มีการเปิดเผย หรือแสดง หรือทำให้ปรากฏในลักษณะอื่นใดซึ่งข้อมูลส่วนบุคคลที่ไม่สอดคล้องกับวัตถุประสงค์ของการรวบรวมและจัดเก็บข้อมูล เว้นแต่จะได้รับความยินยอมจากเจ้าของข้อมูล หรือเป็นกรณีที่มีกฎหมายกำหนดให้กระทำได้

(๕) การรักษาความมั่นคงปลอดภัย

ให้มีมาตรการในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลอย่างเหมาะสม เพื่อป้องกันการสูญหาย การเข้าถึง ทำลาย ใช้ แปลง แก้ไขหรือเปิดเผยข้อมูลโดยมิชอบ

(๖) การเปิดเผยเกี่ยวกับการดำเนินการ แนวปฏิบัติ และนโยบายที่เกี่ยวกับข้อมูลส่วนบุคคล

ให้มีการเปิดเผยการดำเนินการ แนวปฏิบัติ และนโยบายที่เกี่ยวกับข้อมูลส่วนบุคคล และจัดให้มีวิธีการที่สามารถตรวจดูความมีอยู่ ลักษณะของข้อมูลส่วนบุคคลวัตถุประสงค์ของการนำข้อมูลไปใช้ ผู้ควบคุมและสถานที่ทำการของผู้ควบคุมข้อมูลส่วนบุคคล

(๗) การมีส่วนร่วมของเจ้าของข้อมูล

ให้ผู้ควบคุมข้อมูลส่วนบุคคลแจ้งถึงความมีอยู่ หรือรายละเอียดของข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลเมื่อได้รับคำร้องขอภายในระยะเวลาอันสมควรตามวิธีการในรูปแบบ รวมถึงค่าใช้จ่าย (ถ้ามี) ตามสมควร

ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลปฏิเสธที่จะให้คำชี้แจงหรือให้ข้อมูลแก่เจ้าของข้อมูล ผู้สืบสิทธิ์ ทายาท ผู้แทนโดยชอบธรรม หรือผู้พิทักษ์ ตามกฎหมาย

ให้ผู้ควบคุมข้อมูลจัดทำบันทึกคำคัดค้านการจัดเก็บ ความถูกต้อง หรือการกระทำใด ๆ เกี่ยวกับข้อมูลของเจ้าของข้อมูลไว้เป็นหลักฐาน

(๘) ความรับผิดชอบของบุคคลซึ่งทำหน้าที่ควบคุมข้อมูล

ให้ผู้ควบคุมข้อมูลส่วนบุคคลปฏิบัติตามมาตรการที่กำหนดไว้ข้างต้นเพื่อให้การดำเนินงานตามแนวนโยบายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลเป็นไปตามมาตรฐานของประกาศฉบับนี้

ข้อ ๒ ให้หน่วยงานของรัฐจัดทำข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของผู้ใช้บริการ และให้มีรายการอย่างน้อย ดังนี้

(๑) ข้อมูลเบื้องต้น ประกอบด้วย

(ก) ชื่อนโยบายการคุ้มครองข้อมูลส่วนบุคคลว่าเป็นของหน่วยงานใด

(ข) รายละเอียดขอบเขตของการบังคับใช้นโยบายการคุ้มครองข้อมูลส่วนบุคคลที่หน่วยงานของรัฐรวบรวม จัดเก็บ หรือการใช้ตามวัตถุประสงค์

(ค) ให้แจ้งการเปลี่ยนแปลงวัตถุประสงค์หรือนโยบายการคุ้มครองข้อมูลส่วนบุคคลให้เจ้าของข้อมูลทราบและขอความยินยอมก่อนทุกครั้งตามวิธีการและภายในกำหนดเวลาที่ประกาศ เช่น การแจ้งล่วงหน้าให้เจ้าของข้อมูลทราบก่อน ๑๕ วัน โดยการส่งทางจดหมายอิเล็กทรอนิกส์หรือประกาศไว้ในหน้าแรกของเว็บไซต์ เว้นแต่กฎหมายจะกำหนดไว้เป็นอย่างอื่น

การขอความยินยอมจากเจ้าของข้อมูลนั้น ให้มีความชัดเจนว่าหน่วยงานของรัฐขอรับความยินยอมเพื่อวัตถุประสงค์ใด

(๒) การเก็บรวบรวม จัดประเภท และการใช้ข้อมูลส่วนบุคคล

ให้หน่วยงานของรัฐที่ทำธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งเก็บรวบรวมข้อมูลผ่านทางเว็บไซต์หรือผ่านรูปแบบของการกรอกข้อความทางกระดาษแล้วนำมาแปลงข้อความเข้าระบบอิเล็กทรอนิกส์หรือจัดเก็บโดยวิธีอื่น ให้แสดงรายละเอียดของการรวบรวมข้อมูลเป็นชนิด ประเภท รวมถึงข้อมูลที่จะไม่จัดเก็บ และข้อมูลที่รวบรวมและจัดเก็บนั้นจะนำไปใช้ตามวัตถุประสงค์ใดโดยลักษณะหรือด้วยวิธีการที่ทำให้เจ้าของข้อมูลได้ทราบ ทั้งนี้ การรวบรวมและจัดเก็บข้อมูลนั้นให้ทำเป็นประกาศหรือแจ้งรายละเอียดให้เจ้าของข้อมูลทราบ

ให้หน่วยงานของรัฐที่จัดบริการผ่านทางเว็บไซต์ แสดงรายละเอียดของการรวบรวมข้อมูลผ่านทางเว็บไซต์ของหน่วยงานนั้น รวมถึงการใช้ข้อมูลซึ่งอย่างน้อยต้องระบุว่าอยู่ในส่วนใดของเว็บไซต์หรือในเว็บเพจใดที่มีการรวบรวมและจัดเก็บข้อมูล และให้มีรายละเอียดอย่างแจ้งชัดถึงวิธีการในการรวบรวมและจัดเก็บข้อมูล เช่น การจัดเก็บโดยให้มีการลงทะเบียน หรือการกรอกแบบสอบถาม เป็นต้น

ให้หน่วยงานของรัฐรวบรวม จัดเก็บและใช้ข้อมูลส่วนบุคคลจัดทำรายละเอียด ดังต่อไปนี้

(ก) การติดต่อระหว่างหน่วยงานของรัฐ

ให้หน่วยงานของรัฐซึ่งจะติดต่อไปยังผู้ใช้บริการด้วยวิธีการทางอิเล็กทรอนิกส์บอกกล่าวให้ผู้ใช้บริการทราบล่วงหน้า ทั้งนี้ ผู้ใช้บริการอาจแจ้งความประสงค์ให้ติดต่อโดยวิธีการอื่นได้

(ข) การใช้คุกกี้ (Cookies)

ให้หน่วยงานของรัฐระบุบนเว็บไซต์สำหรับการใช้คุกกี้ที่เชื่อมโยงกับข้อมูลส่วนบุคคลว่าผู้ใช้บริการจะใช้คุกกี้เพื่อวัตถุประสงค์และประโยชน์ใด และให้สิทธิที่จะไม่รับการต่อเชื่อมคุกกี้ได้

(ค) การเก็บข้อมูลสถิติเกี่ยวกับประชากร (Demographic Information)

ให้หน่วยงานของรัฐมีเว็บไซต์สำหรับการเก็บรวบรวมข้อมูลสถิติเกี่ยวกับประชากร เช่น เพศ อายุ อาชีพ ที่สามารถเชื่อมโยงกับข้อมูลระบุตัวบุคคลได้ ระบุถึงวิธีการรวบรวมและจัดเก็บข้อมูลดังกล่าวไว้ในนโยบายการคุ้มครองข้อมูลส่วนบุคคลด้วย และให้ชี้แจงวัตถุประสงค์ของการใช้ข้อมูลดังกล่าว รวมถึงการให้บุคคลอื่นร่วมใช้ข้อมูลนั้นด้วย

(ง) บันทึกผู้เข้าชมเว็บ (Log Files)

ให้หน่วยงานของรัฐซึ่งจัดบริการเว็บไซต์ที่มีการเก็บบันทึกการเข้าออกโดยอัตโนมัติ เช่น หมายเลขไอพี (IP Address) เว็บไซต์ที่เข้าออกก่อนและหลัง และประเภทของโปรแกรมบราวเซอร์ (Browser) ที่สามารถเชื่อมโยงข้อมูลดังกล่าวกับข้อมูลซึ่งระบุตัวบุคคลได้ ระบุวิธีการรวบรวมและจัดเก็บข้อมูลดังกล่าวไว้ในนโยบายการคุ้มครองข้อมูลส่วนบุคคล และให้ชี้แจงวัตถุประสงค์ของการใช้ รวมถึงการให้บุคคลอื่นร่วมใช้ข้อมูลนั้นด้วย

(จ) ให้หน่วยงานของรัฐระบุข้อมูลที่มีการจัดเก็บผ่านทางเว็บไซต์ว่าเป็นข้อมูลที่ประชาชนมีสิทธิเลือกว่า “จะให้หรือไม่ให้” ก็ได้ และให้หน่วยงานของรัฐจัดเตรียมช่องทางอื่นในการติดต่อสื่อสารสำหรับผู้ใช้บริการที่ไม่ประสงค์จะให้ข้อมูลผ่านทางเว็บไซต์

(๓) การแสดงระบุความเชื่อมโยงให้ข้อมูลส่วนบุคคลกับหน่วยงานหรือองค์กรอื่น

การเก็บรวบรวมข้อมูลผ่านทางเว็บไซต์ของหน่วยงานของรัฐและเว็บไซต์ดังกล่าวที่มีการเชื่อมโยงให้ข้อมูลแก่หน่วยงานหรือองค์กรอื่น ให้หน่วยงานของรัฐแสดงไว้อย่างชัดเจนถึงชื่อผู้เก็บรวบรวมข้อมูลผ่านทางเว็บไซต์ หรือชื่อผู้มีสิทธิในข้อมูลที่ได้มีการเก็บรวบรวม (Data Subject) และชื่อเป็นผู้มีสิทธิเข้าถึงข้อมูลดังกล่าวทั้งหมด รวมถึงประเภทของข้อมูลที่จะใช้ร่วมกับหน่วยงานหรือองค์กรนั้น ๆ ตลอดจนชื่อผู้มีหน้าที่ปฏิบัติตามนโยบายการคุ้มครองข้อมูลส่วนบุคคลไว้ในนโยบายการคุ้มครองข้อมูลส่วนบุคคล เพื่อให้ผู้ใช้บริการทราบ

ให้หน่วยงานของรัฐแจ้งให้ผู้ใช้บริการทราบและให้ความยินยอมล่วงหน้าก่อนทำการเปลี่ยนแปลงการเชื่อมโยงข้อมูลตามวรรคแรกกับหน่วยงานหรือองค์กรอื่น

(๔) การรวมข้อมูลจากที่มาหลาย ๆ แห่ง

ให้หน่วยงานของรัฐที่ซึ่งได้รับข้อมูลมาจากผู้ใช้บริการเว็บไซต์ และจะนำไปรวมเข้ากับข้อมูลของบุคคลดังกล่าวที่ได้รับจากที่มาแห่งอื่น ระบุไว้ในนโยบายคุ้มครองข้อมูลส่วนบุคคลถึงเจตนารมณ์การรวมข้อมูลดังกล่าวด้วย เช่น เว็บไซต์ได้รับข้อมูลที่เป็นชื่อและที่อยู่ของการส่งจดหมายอิเล็กทรอนิกส์จากผู้ใช้บริการโดยการกรอกข้อมูลตามแบบสอบถามผ่านทางเว็บไซต์ และจะนำข้อมูลดังกล่าวไปรวมเข้ากับข้อมูลเกี่ยวกับประวัติของผู้ใช้บริการที่ได้รับจากที่มาแห่งอื่น

(๕) การให้บุคคลอื่นใช้หรือการเปิดเผยข้อมูลส่วนบุคคล

ให้หน่วยงานของรัฐระบุไว้ในนโยบายการคุ้มครองข้อมูลส่วนบุคคลด้วยว่ามีบุคคลอื่นที่จะเข้าถึงหรือใช้ข้อมูลที่หน่วยงานนั้นได้เก็บรวบรวมมาผ่านทางเว็บไซต์ด้วย และให้ระบุไว้ด้วยว่าการให้เข้าถึง ใช้ หรือเปิดเผยข้อมูลดังกล่าวสอดคล้องกับข้อกำหนดตามกฎหมายของหน่วยงานของรัฐที่ดำเนินการดังกล่าว

(๖) การรวบรวม จัดเก็บ ใช้ และการเปิดเผยข้อมูลเกี่ยวกับผู้ใช้บริการ

ให้หน่วยงานของรัฐซึ่งรวบรวม จัดเก็บ ใช้ และเปิดเผยข้อมูลส่วนบุคคลที่ประสงค์จะนำไปดำเนินการอื่นนอกเหนือไปจากวัตถุประสงค์ของการรวบรวมข้อมูลส่วนบุคคลตามที่ได้ระบุไว้ เช่น การรวบรวม จัดเก็บ ใช้ และเปิดเผยข้อมูลที่ไม่จำเป็น หรือการเปิดเผยข้อมูลส่วนบุคคลต่อบุคคลอื่น ระบุไว้ในนโยบายการคุ้มครองข้อมูลส่วนบุคคลถึงสิทธิของผู้ใช้บริการที่จะเลือกว่า จะให้หน่วยงานของรัฐรวบรวม จัดเก็บหรือไม่ให้จัดเก็บ ใช้หรือไม่ให้ใช้ และเปิดเผยหรือไม่เปิดเผยข้อมูลดังกล่าว

การให้ผู้ใช้บริการใช้สิทธิเลือกตามวรรคแรกให้รวมถึงการให้สิทธิเลือกแบบที่หน่วยงานของรัฐจะต้องขอความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคลนั้นก่อน และการให้สิทธิเลือกแบบที่ให้สิทธิแก่ผู้ใช้บริการในการปฏิเสธไม่ให้มีการใช้หรือการเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์อื่นนอกเหนือจากวัตถุประสงค์ที่เก็บรวบรวมข้อมูลส่วนบุคคลดังกล่าวข้างต้นแล้วเท่านั้น ทั้งนี้ การให้สิทธิเลือกต้องกระทำให้สมบูรณ์ก่อนที่เว็บไซต์จะทำการติดต่อกับผู้ใช้บริการในครั้งแรก และหากเป็นการใช้สิทธิเลือกแบบห้ามไม่ให้มีการใช้ข้อมูลส่วนบุคคลแตกต่างไปจากวัตถุประสงค์เดิม หน่วยงานเจ้าของเว็บไซต์ต้องระบุไว้ในนโยบายการคุ้มครองข้อมูลส่วนบุคคลให้ผู้ใช้บริการได้รับทราบถึงวิธีการของการส่งการติดต่อครั้งที่สองของเว็บไซต์ด้วย

(๗) การเข้าถึง การแก้ไขให้ถูกต้อง และการปรับปรุงให้เป็นปัจจุบัน

ให้หน่วยงานของรัฐกำหนดวิธีการที่ผู้ใช้บริการเว็บไซต์สามารถเข้าถึงและแก้ไขหรือปรับปรุงข้อมูลส่วนบุคคลเกี่ยวกับตนเองที่หน่วยงานของรัฐรวบรวมและจัดเก็บไว้ในเว็บไซต์ให้ถูกต้อง

(๘) การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

ให้หน่วยงานของรัฐซึ่งรวบรวมข้อมูลส่วนบุคคลผ่านทางจัดให้มีวิธีการรักษาความมั่นคงปลอดภัยสำหรับข้อมูลส่วนบุคคลที่รวบรวมและจัดเก็บไว้ให้เหมาะสมกับการรักษาความลับของข้อมูลส่วนบุคคล เพื่อป้องกันการเปลี่ยนแปลงแก้ไขข้อมูลดังกล่าวโดยมิชอบ รวมถึงการป้องกันการกระทำใดที่จะมีผลทำให้ข้อมูลไม่อยู่ในสภาพพร้อมใช้งาน ซึ่งหน่วยงานของรัฐพึงดำเนินการ ดังนี้

(ก) สร้างเสริมความสำนึกในการรับผิดชอบด้านความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลให้แก่บุคลากร พนักงาน หรือลูกจ้างของหน่วยงานด้วยการเผยแพร่ข้อมูลข่าวสาร ให้ความรู้ จัดสัมมนา หรือฝึกอบรมในเรื่องดังกล่าวให้แก่บุคลากรในองค์กรเป็นประจำ

(ข) กำหนดสิทธิและข้อจำกัดสิทธิในการเข้าถึงข้อมูลส่วนบุคคลของบุคลากร พนักงาน หรือลูกจ้างของตนในแต่ละลำดับชั้นให้ชัดเจน และให้มีการบันทึกรวมทั้งการทำสำรองข้อมูลของการเข้าถึงหรือการเข้าใช้งานข้อมูลส่วนบุคคลไว้ในระยะเวลาที่เหมาะสมหรือตามระยะเวลาที่กฎหมายกำหนด

(ค) ตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยของเว็บไซต์หรือของระบบสารสนเทศทั้งหมดอย่างน้อยปีละ ๑ ครั้ง

(ง) กำหนดให้มีการใช้มาตรการที่เหมาะสมและเป็นการเฉพาะสำหรับการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่มีความสำคัญยิ่งหรือเป็นข้อมูลที่อาจกระทบต่อความรู้สึก ความเชื่อ ความสงบเรียบร้อย และศีลธรรมอันดีของประชาชนซึ่งเป็นผู้ใช้บริการของหน่วยงานของรัฐ หรืออาจก่อให้เกิดความเสียหาย หรือมีผลกระทบต่อสิทธิเสรีภาพของผู้เป็นเจ้าของข้อมูลอย่างชัดเจน เช่น หมายเลขบัตรเดบิต หรือบัตรเครดิต หมายเลขประจำตัวประชาชน หรือหมายเลขประจำตัวบุคคล เชื้อชาติ ศาสนา ความเชื่อ ความคิดเห็นทางการเมือง สุขภาพ พฤติกรรมทางเพศ เป็นต้น

(จ) ควรจัดให้มีมาตรการที่รอบคอบในการรักษาความมั่นคงปลอดภัยสำหรับข้อมูลส่วนบุคคลของบุคคลซึ่งอายุไม่เกินสิบแปดปีโดยใช้วิธีการโดยเฉพาะและเหมาะสม

(๙) การติดต่อกับเว็บไซต์

เว็บไซต์ซึ่งให้ข้อมูลแก่ผู้ใช้บริการในการติดต่อกับหน่วยงานของรัฐ ต้องจัดให้มีทั้งข้อมูลติดต่อไปยังสถานที่ทำการงานปกติและข้อมูลติดต่อผ่านทางออนไลน์ด้วย ข้อมูลติดต่อที่หน่วยงานของรัฐควรจะระบุเอาไว้ อย่างน้อยต้องประกอบด้วยข้อมูลดังต่อไปนี้

(ก) ชื่อและที่อยู่

(ข) หมายเลขโทรศัพท์

(ค) หมายเลขโทรสาร

(ง) ที่อยู่จดหมายอิเล็กทรอนิกส์

ข้อ ๓ ให้หน่วยงานของรัฐจัดทำนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลภายใต้หลักการตามข้อ ๑ และข้อ ๒ สำหรับหน่วยงานของรัฐที่ได้รับทรัสต์มาร์คจากหน่วยงานหรือองค์กรอื่นที่ทำหน้าที่ออกทรัสต์มาร์ค (Trust Mark) ให้หน่วยงานของรัฐนั้นแสดงนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลที่ได้รับการรับรองจากหน่วยงานหรือองค์กรที่ออกหรือรับรองทรัสต์มาร์คดังกล่าวต่อคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ประกอบด้วย

ทรัสต์มาร์ค (Trust Mark) ตามความในวรรคแรกหมายถึง เครื่องหมายที่รับรองว่าหน่วยงานดังกล่าวมีมาตรฐานในการคุ้มครองข้อมูลส่วนบุคคลของประชาชนในการทำธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งออกโดยหน่วยงานหรือองค์กรที่จัดตั้งโดยชอบด้วยกฎหมายเพื่อทำหน้าที่ในการตรวจสอบและรับรองการออกทรัสต์มาร์คให้กับผู้ขอรับการรับรอง

ข้อ ๔ ให้หน่วยงานของรัฐกำหนดชื่อเรียกนโยบายการคุ้มครองข้อมูลส่วนบุคคลไว้ให้ชัดเจน และในกรณีที่มีการปรับปรุงนโยบาย ให้ระบุวัน เวลา และปี ซึ่งจะมีการปรับปรุงหรือเปลี่ยนแปลงนโยบายดังกล่าวไว้ด้วย

ข้อ ๕ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ประกาศ ณ วันที่ ๑ ตุลาคม พ.ศ. ๒๕๕๓
จุติ ไกรฤกษ์
รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
ประธานกรรมการธุรกรรมทางอิเล็กทรอนิกส์

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
เรื่อง แนวนโยบายและแนวปฏิบัติ
ในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ
พ.ศ. ๒๕๕๓ (แก้คำผิด)

แก้คำผิด

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ ซึ่งประกาศในราชกิจจานุเบกษา ฉบับประกาศและงานทั่วไป

เล่ม ๑๒๗ ตอนพิเศษ ๑๒๖ ง วันที่ ๑ พฤศจิกายน ๒๕๕๓

หน้า ๗๖ บรรทัดที่ ๒ คำว่า “ให้หน่วยงานของรัฐซึ่งรวบรวมข้อมูลส่วนบุคคลผ่านทางจัดให้มีวิธีการรักษาความมั่นคง” ให้แก้เป็น “ให้หน่วยงานของรัฐซึ่งรวบรวมข้อมูลส่วนบุคคลผ่านทางเว็บไซต์จัดให้มีวิธีการรักษาความมั่นคง”

พระราชกฤษฎีกา
ว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงิน ทางอิเล็กทรอนิกส์
พ.ศ. ๒๕๕๑

พระราชกฤษฎีกา

ว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์

พ.ศ. ๒๕๕๑

ภูมิพลอดุลยเดช ป.ร.

ให้ไว้ ณ วันที่ ๑๗ สิงหาคม พ.ศ. ๒๕๕๑

เป็นปีที่ ๖๓ ในรัชกาลปัจจุบัน

พระบาทสมเด็จพระปรมินทรมหาภูมิพลอดุลยเดช มีพระบรมราชโองการโปรดเกล้า ฯ ให้ประกาศว่า

โดยที่เป็นการสมควรควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์

อาศัยอำนาจตามความในมาตรา ๑๘๗ ของรัฐธรรมนูญแห่งราชอาณาจักรไทย และมาตรา ๓๒ วรรคหนึ่ง มาตรา ๓๓ วรรคสอง และมาตรา ๓๔ วรรคสอง แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ อันเป็นกฎหมายที่มีบทบัญญัติบางประการเกี่ยวกับการจำกัดสิทธิและเสรีภาพของบุคคล ซึ่งมาตรา ๒๙ ประกอบกับมาตรา ๔๓ ของรัฐธรรมนูญแห่งราชอาณาจักรไทย บัญญัติให้กระทำได้โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมาย จึงทรงพระกรุณาโปรดเกล้า ฯ ให้ตราพระราชกฤษฎีกาขึ้นไว้ ดังต่อไปนี้

มาตรา ๑ พระราชกฤษฎีกานี้เรียกว่า “พระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๑”

มาตรา ๒ พระราชกฤษฎีกานี้ให้ใช้บังคับเมื่อพ้นกำหนดหนึ่งร้อยยี่สิบวันนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

มาตรา ๓ ในพระราชกฤษฎีกานี้

“การชำระเงินทางอิเล็กทรอนิกส์” หมายความว่า การโอนสิทธิการถือครองเงินหรือการโอนสิทธิการถอนเงิน หรือหักเงินจากบัญชีเงินฝากของผู้ใช้บริการที่เปิดไว้กับผู้ให้บริการด้วยวิธีการทางอิเล็กทรอนิกส์ทั้งหมดหรือบางส่วน

“บัตรอิเล็กทรอนิกส์” หมายความว่า บัตรอิเล็กทรอนิกส์ตามประมวลกฎหมายอาญา

“บัตรเครดิต” หมายความว่า บัตรอิเล็กทรอนิกส์ที่ผู้ให้บริการออกให้แก่ผู้ใช้บริการเพื่อใช้ชำระค่าสินค้า ค่าบริการ หรือค่าอื่นใด แทนการชำระด้วยเงินสด หรือเพื่อใช้เบิก ถอน โอน หรือทำธุรกรรมอื่นใดที่เกี่ยวกับเงิน และผู้ให้บริการจะเรียกให้ผู้ใช้บริการชำระเงินในภายหลัง

“บัตรเดบิต” หมายความว่า บัตรอิเล็กทรอนิกส์ที่ผู้ให้บริการออกให้แก่ผู้ใช้บริการเพื่อใช้ชำระค่าสินค้า ค่าบริการ หรือค่าอื่นใด แทนการชำระด้วยเงินสด หรือเพื่อใช้เบิก ถอน โอน หรือทำธุรกรรมอื่นใดที่เกี่ยวกับเงิน ตามมูลค่าของเงินที่ผู้ใช้บริการได้ฝากไว้กับผู้ให้บริการ

“เงินอิเล็กทรอนิกส์” หมายความว่า บัตรอิเล็กทรอนิกส์ที่ผู้ให้บริการออกให้แก่ผู้ใช้บริการซึ่งจะระบุชื่อหรือไม่ก็ตาม โดยมีการชำระเงินให้แก่ผู้ให้บริการไว้ล่วงหน้า เพื่อนำไปใช้ชำระค่าสินค้า ค่าบริการ หรือค่าอื่นใดแทนการชำระด้วยเงินสด และได้มีการบันทึกมูลค่าหรือจำนวนเงินที่ชำระไว้ล่วงหน้า

“อีดีซี” (Electronic Data Capture : EDC) หมายความว่า อุปกรณ์หรือเครื่องมือสำหรับการรับส่งข้อมูลการชำระเงินทางอิเล็กทรอนิกส์จากบัตรเครดิต บัตรเดบิต เงินอิเล็กทรอนิกส์ หรือบัตรอิเล็กทรอนิกส์อื่นใด ไปยังผู้ให้บริการซึ่งออกบัตร

“เครือข่ายอีดีซี” (EDC Network) หมายความว่า เครือข่ายรับส่งข้อมูลอีดีซีที่มีศูนย์กลางหรือจุดเชื่อมต่อการรับส่งข้อมูลระหว่างผู้ใช้บริการเครือข่าย

“เครือข่ายบัตรเครดิต” หมายความว่า เครือข่ายการให้บริการรับส่งข้อมูลการชำระเงินทางอิเล็กทรอนิกส์จากบัตรเครดิตของผู้ถือบัตรไปยังผู้ให้บริการซึ่งออกบัตรเช่นว่านั้น เพื่ออนุมัติการใช้บัตรในการทำรายการแต่ละรายการ หรือรับส่งข้อมูลเรียกเก็บเงินอันเกิดจากการชำระเงินทางอิเล็กทรอนิกส์ ตลอดจนการหักทอนบัญชีระหว่างกัน

“บริการสวิตช์ชิ่งในการชำระเงิน” (Transaction Switching) หมายความว่า บริการเป็นศูนย์กลางหรือจุดเชื่อมต่อรับส่งข้อมูลรายการชำระเงินทางอิเล็กทรอนิกส์ให้แก่ผู้ให้บริการตามที่ตกลงกัน

“บริการรับชำระเงินแทน” หมายความว่า บริการรับชำระเงินทางอิเล็กทรอนิกส์แทนเจ้าหนี้

"บริการหักบัญชี" (Clearing) หมายความว่า บริการรับส่ง ตรวจสอบ และยืนยันข้อมูลตามคำสั่งการชำระเงินสำหรับนำไปคำนวณหายอดเงินแสดงความเป็นเจ้าหนี้ หรือลูกหนี้ของผู้ใช้บริการเพื่อใช้ข้อมูลดังกล่าวไปทำการชำระดุลระหว่างเจ้าหนี้และลูกหนี้ ทั้งนี้ รวมถึงการจัดการเพื่อให้กระบวนการชำระดุลสำเร็จลุล่วงด้วย

"บริการชำระดุล" (Settlement) หมายความว่า บริการระบบการชำระเงินที่ตกลงกันไว้ล่วงหน้าระหว่างผู้ใช้บริการกับผู้ให้บริการเพื่อให้ผู้ให้บริการปรับฐานะความเป็นเจ้าหนี้ หรือลูกหนี้ของผู้ใช้บริการโดยผู้ให้บริการจะทำการหักบัญชีเงินฝากของผู้ใช้บริการซึ่งมีฐานะเป็นลูกหนี้ หรือรับชำระหนี้โดยวิธีอื่นใดตามที่ตกลงกัน แล้วปรับบัญชีเงินฝากของผู้ใช้บริการซึ่งมีฐานะเป็นเจ้าหนี้ หรือชำระเงินด้วยวิธีอื่นใด เพื่อให้หนี้ดังกล่าวระงับไป

"ผู้ให้บริการ" หมายความว่า ผู้ประกอบธุรกิจให้บริการการชำระเงินทางอิเล็กทรอนิกส์ตามที่กำหนดไว้ในบัญชีท้ายพระราชกฤษฎีกานี้

"ธปท." หมายความว่า ธนาคารแห่งประเทศไทย ตามกฎหมายว่าด้วยธนาคารแห่งประเทศไทย

"ผู้ว่าการ" หมายความว่า ผู้ว่าการธนาคารแห่งประเทศไทย

"คณะกรรมการ" หมายความว่า คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

"พนักงานเจ้าหน้าที่" หมายความว่า ผู้ว่าการธนาคารแห่งประเทศไทยหรือผู้ซึ่งผู้ว่าการธนาคารแห่งประเทศไทยแต่งตั้งให้ปฏิบัติการตามพระราชกฤษฎีกานี้

มาตรา ๔ ให้ ธปท. เป็นผู้รับผิดชอบในการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ตามพระราชกฤษฎีกานี้

มาตรา ๕ พระราชกฤษฎีกานี้ไม่ใช้บังคับกับการให้บริการการชำระเงินทางอิเล็กทรอนิกส์ที่ ธปท. เป็นผู้ให้บริการ

มาตรา ๖ ให้นายกรัฐมนตรีรักษาการตามพระราชกฤษฎีกานี้

หมวด ๑
การประกอบธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์

มาตรา ๗ ธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ใดที่ผู้ให้บริการจะต้องแจ้งให้ทราบขึ้นทะเบียน หรือได้รับใบอนุญาต ให้เป็นไปตามบัญชีท้ายพระราชกฤษฎีกานี้

หลักเกณฑ์ วิธีการ และแบบการแจ้งให้ทราบ การขึ้นทะเบียน และการขอรับใบอนุญาต ให้เป็นไปตามที่คณะกรรมการประกาศกำหนด

มาตรา ๘ ผู้ประสงค์จะเป็นผู้ให้บริการตามบัญชี ก จะเป็นบุคคลธรรมดาหรือนิติบุคคล ตามมาตรา ๙ (๒) ก็ได้

ผู้ประสงค์จะเป็นผู้ให้บริการตามบัญชี ข หรือบัญชี ค ต้องเป็นนิติบุคคลตามมาตรา ๙ (๒)

มาตรา ๙ ผู้ประสงค์จะเป็นผู้ให้บริการต้องมีคุณสมบัติและไม่มีลักษณะต้องห้าม ดังต่อไปนี้

(๑) บุคคลธรรมดา

(ก) มีอายุไม่ต่ำกว่ายี่สิบปีบริบูรณ์

(ข) มีภูมิลำเนาหรือถิ่นที่อยู่ในราชอาณาจักร

(ค) ไม่อยู่ในระหว่างถูกพิทักษ์ทรัพย์ หรือไม่เป็นบุคคลล้มละลายหรือเคยเป็นบุคคล ล้มละลายและยังไม่พ้นกำหนดสองปีนับแต่วันที่มีคำสั่งยกเลิกการล้มละลายหรือปลดจากล้มละลาย

(ง) ไม่เป็นบุคคลวิกลจริต คนไร้ความสามารถ หรือคนเสมือนไร้ความสามารถ

(จ) ไม่เคยได้รับโทษจำคุกโดยคำพิพากษาถึงที่สุดให้จำคุกในความผิดเกี่ยวกับการปลอม และการแปลง ลักทรัพย์ วิ่งราวทรัพย์ กรรโชก รีดเอาทรัพย์ ชิงทรัพย์ ปล้นทรัพย์ ฉ้อโกง โกงเจ้าหนี้ ยักยอก หรือรับของโจร หรือความผิดเกี่ยวกับคอมพิวเตอร์ตามกฎหมายว่าด้วยการกระทำ ความผิดเกี่ยวกับคอมพิวเตอร์

(ฉ) ไม่เคยถูกสั่งห้ามประกอบธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์และยังไม่พ้น กำหนดห้าปีนับถึงวันแจ้งให้ทราบ

(ช) ไม่เป็นกรรมการหรือผู้ซึ่งมีอำนาจจัดการของนิติบุคคลที่เคยถูกสั่งห้ามประกอบ ธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์หรือเพิกถอนใบอนุญาตและยังไม่พ้นกำหนดห้าปีนับถึงวัน แจ้งให้ทราบ วันขอขึ้นทะเบียน หรือวันขอรับใบอนุญาต แล้วแต่กรณี

(๒) นิติบุคคล

(ก) เป็นนิติบุคคลประเภทห้างหุ้นส่วนจดทะเบียน ห้างหุ้นส่วนจำกัด บริษัทจำกัด หรือ บริษัทมหาชนจำกัด และมีวัตถุประสงค์เกี่ยวกับการประกอบธุรกิจบริการการชำระเงินทาง อิเล็กทรอนิกส์ตามที่กำหนดไว้ในบัญชีท้ายพระราชกฤษฎีกานี้ ในการนี้ คณะกรรมการจะประกาศ

กำหนดจำนวนทุนจดทะเบียนซึ่งชำระแล้วด้วยก็ได้ ทั้งนี้ ในกรณีผู้ที่ประสงค์จะเป็นผู้ให้บริการตามบัญชี ค ต้องมิใช่นิติบุคคลประเภทห้างหุ้นส่วนจดทะเบียน หรือห้างหุ้นส่วนจำกัด

(ข) กรรมการหรือผู้ซึ่งมีอำนาจจัดการของนิติบุคคลต้องมีคุณสมบัติและไม่มีลักษณะต้องห้ามตาม (๑)

(ค) ไม่อยู่ในระหว่างถูกพักใช้ใบอนุญาต

(ง) ไม่เคยถูกสั่งห้ามประกอบธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์หรือเพิกถอนใบอนุญาตและยังไม่พ้นกำหนดห้าปีนับถึงวันแจ้งให้ทราบ วันยื่นขอจดทะเบียน หรือวันขอรับใบอนุญาต แล้วแต่กรณี

คณะกรรมการอาจออกประกาศกำหนดคุณสมบัติหรือลักษณะต้องห้ามประการอื่นของผู้ให้บริการแต่ละบัญชีท้ายพระราชกฤษฎีกานี้เพิ่มเติมตามความเหมาะสมอีกก็ได้

มาตรา ๑๐ ผู้ประสงค์จะเป็นผู้ให้บริการให้ยื่นแบบการแจ้งให้ทราบ แบบการขอขึ้นทะเบียน หรือแบบการขอรับใบอนุญาต แล้วแต่กรณี พร้อมด้วยเอกสารที่มีรายการดังต่อไปนี้

(๑) ผู้ให้บริการตามบัญชี ก ได้แก่

(ก) แผนฉุกเฉินหรือระบบให้บริการสำรองเพื่อให้สามารถให้บริการได้อย่างต่อเนื่อง

(ข) นโยบายและมาตรการการรักษาความปลอดภัยทางระบบสารสนเทศซึ่งอย่างน้อยต้องมีมาตรฐานตามที่ ธปท. ประกาศกำหนด

(๒) ผู้ให้บริการตามบัญชี ข และบัญชี ค ได้แก่

(ก) เอกสารตาม (๑)

(ข) นโยบายและแผนการประกอบธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์

(ค) แผนปฏิบัติการเตรียมการรองรับการประกอบธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์

(ง) ระบบบริหารและจัดการความเสี่ยง

(จ) ระบบการควบคุมภายใน

(ฉ) ผลการศึกษาความเป็นไปได้และประเมินความเสี่ยงในการให้บริการ รวมทั้งแผนฉุกเฉินรองรับกรณีเกิดปัญหา

เพื่อประโยชน์ในการควบคุมดูแลการให้บริการของผู้ให้บริการแต่ละบัญชี ธปท. จะประกาศกำหนดให้ยื่นเอกสารที่มีรายการเพิ่มเติมจากที่กำหนดไว้ตามวรรคหนึ่งก็ได้

มาตรา ๑๑ ให้ผู้ประสงค์จะเป็นผู้ให้บริการตามบัญชี ก หรือบัญชี ข ยื่นแบบการแจ้งให้ทราบหรือแบบการขอขึ้นทะเบียน แล้วแต่กรณี พร้อมทั้งเอกสารตามมาตรา ๑๐ ต่อผู้ว่าการหรือพนักงานเจ้าหน้าที่ที่ผู้ว่าการมอบหมาย และหากปรากฏว่าผู้ประสงค์จะเป็นผู้ให้บริการนั้นยื่นเอกสารครบถ้วน รวมทั้งปฏิบัติตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนดตามมาตรา ๗ วรรคสองแล้ว ให้ออกใบรับแจ้งหรือใบรับการขึ้นทะเบียนให้ แล้วแต่กรณี

ในกรณีที่ตรวจสอบภายหลังพบว่าผู้ให้บริการตามบัญชี ก หรือบัญชี ข ผู้ใดยื่นเอกสารหรือหลักฐานใดไม่ถูกต้องหรือไม่ครบถ้วน หรือมีกรณีที่มิได้ปฏิบัติให้ถูกต้องตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด หรือขาดคุณสมบัติ หรือมีลักษณะต้องห้าม ให้ผู้ว่าการหรือพนักงานเจ้าหน้าที่ที่ผู้ว่าการมอบหมายแจ้งให้ผู้ให้บริการนั้นทราบ เพื่อดำเนินการแก้ไขให้ถูกต้อง หรือครบถ้วน แล้วแต่กรณี ภายในเจ็ดวันนับแต่วันที่ได้รับคำสั่ง

ในกรณีที่ผู้ให้บริการนั้นไม่ปฏิบัติตามคำสั่ง หรือไม่ปฏิบัติภายในระยะเวลาที่กำหนดไว้ตามวรรคสอง ให้ผู้ว่าการหรือพนักงานเจ้าหน้าที่ที่ผู้ว่าการมอบหมายรายงานต่อคณะกรรมการเพื่อพิจารณาดำเนินการตามมาตรา ๓๓ วรรคสี่ แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ และให้คณะกรรมการมีอำนาจสั่งให้ผู้ให้บริการนั้นดำเนินการแก้ไขให้ถูกต้อง หรือเหมาะสมก็ได้

ในกรณีที่ตรวจสอบภายหลังพบว่าผู้ให้บริการตามบัญชี ก หรือบัญชี ข ผู้ใดขาดคุณสมบัติหรือมีลักษณะต้องห้ามซึ่งไม่อาจจะแก้ไขได้ ให้คณะกรรมการมีคำสั่งห้ามผู้ให้บริการนั้นประกอบธุรกิจตามที่ได้แจ้งหรือขึ้นทะเบียน และเพิกถอนการแจ้งหรือการขึ้นทะเบียนของผู้ให้บริการนั้น แล้วแต่กรณี

มาตรา ๑๒ ในกรณีที่ผู้ประสงค์จะเป็นผู้ให้บริการตามบัญชี ค ได้ยื่นแบบการขอใบอนุญาตพร้อมทั้งเอกสารตามมาตรา ๑๐ (๒) แล้ว ให้ผู้ว่าการหรือพนักงานเจ้าหน้าที่ที่ผู้ว่าการมอบหมายตรวจสอบความครบถ้วนและถูกต้องของเอกสารตามมาตรา ๑๐ และการดำเนินการตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนดตามมาตรา ๗ วรรคสอง ในกรณีที่พบว่าเอกสารหรือหลักฐานใดไม่ครบถ้วนหรือไม่ถูกต้อง หรือยังมิได้ปฏิบัติให้ถูกต้องตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด ให้ผู้ว่าการหรือพนักงานเจ้าหน้าที่ที่ผู้ว่าการมอบหมายแจ้งให้ผู้ประสงค์จะเป็นผู้ให้บริการทราบ เพื่อดำเนินการแก้ไขให้ถูกต้อง หรือครบถ้วนก่อนเสนอคณะกรรมการเพื่อออกใบอนุญาต

ในกรณีที่ปรากฏว่าผู้ประสงค์จะเป็นผู้ให้บริการตามบัญชี ค ยื่นเอกสารครบถ้วนและถูกต้องและปฏิบัติตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนดตามมาตรา ๗ วรรคสอง หรือได้ดำเนินการแก้ไขให้ถูกต้องหรือครบถ้วนตามที่ผู้ว่าการหรือพนักงานเจ้าหน้าที่ที่ผู้ว่าการมอบหมายมีคำสั่งตามวรรคหนึ่งแล้ว ให้ผู้ว่าการหรือพนักงานเจ้าหน้าที่ที่ผู้ว่าการมอบหมายเสนอคณะกรรมการเพื่อพิจารณาออกใบอนุญาตต่อไป

มาตรา ๑๓ เพื่อประโยชน์ในการควบคุมดูแลการให้บริการของผู้ให้บริการแต่ละราย คณะกรรมการอาจกำหนดข้อปฏิบัติในการให้บริการของผู้ให้บริการตามบัญชี ก หรือบัญชี ข หรือจะกำหนดเงื่อนไขในการให้บริการไว้ในใบอนุญาตของผู้ให้บริการตามบัญชี ค ก็ได้

ข้อปฏิบัติและเงื่อนไขตามวรรคหนึ่งต้องไม่เป็นภาระหรืออุปสรรคเกินสมควรในการให้บริการของผู้ให้บริการ

มาตรา ๑๔ ใบอนุญาตของผู้ให้บริการตามบัญชี ค มีอายุสิบปี

ผู้ให้บริการตามบัญชี ค อาจยื่นขอต่ออายุใบอนุญาตภายในระยะเวลาเก้าสิบวันแต่ไม่น้อยกว่าหกสิบวันก่อนวันที่ใบอนุญาตนั้นสิ้นอายุ โดยยื่นคำขอต่ออายุใบอนุญาตต่อผู้ว่าการหรือพนักงานเจ้าหน้าที่ที่ผู้ว่าการมอบหมาย พร้อมทั้งเอกสารที่แสดงหลักฐานการได้รับใบอนุญาตเดิม

ให้คณะกรรมการพิจารณาการต่ออายุใบอนุญาตหรือการไม่ต่ออายุใบอนุญาตให้แล้วเสร็จภายในสามสิบวันนับแต่วันที่ได้รับคำขอต่ออายุใบอนุญาตตามวรรคสอง โดยแจ้งเป็นหนังสือให้แก่ผู้ให้บริการซึ่งยื่นคำขอต่ออายุใบอนุญาต

ในกรณีที่คณะกรรมการแจ้งการไม่ต่ออายุใบอนุญาตตามวรรคสอง และใบอนุญาตเดิมยังไม่สิ้นอายุ ให้ผู้ให้บริการนั้นยังคงให้บริการตามใบอนุญาตเดิมได้ต่อไปจนกว่าใบอนุญาตสิ้นอายุ ในการนี้คณะกรรมการจะสั่งให้ผู้ให้บริการต้องปฏิบัติการอย่างหนึ่งอย่างใดเพื่อคุ้มครองประโยชน์ของผู้ใช้บริการด้วยก็ได้

หลักเกณฑ์ วิธีการ และแบบในการขอต่ออายุใบอนุญาต ให้เป็นไปตามที่คณะกรรมการประกาศกำหนด

มาตรา ๑๕ ในกรณีที่ใบรับแจ้ง ใบรับขึ้นทะเบียน หรือใบอนุญาตเป็นผู้ให้บริการสูญหาย ถูกทำลาย หรือชำรุดเสียหายในสาระสำคัญ ให้ผู้ให้บริการยื่นคำขอรับใบแทนต่อผู้ว่าการ หรือพนักงานเจ้าหน้าที่ที่ผู้ว่าการมอบหมาย ทั้งนี้ ตามหลักเกณฑ์ วิธีการ และแบบที่คณะกรรมการประกาศกำหนด

หมวด ๒
การควบคุมดูแลการประกอบธุรกิจบริการ
การชำระเงินทางอิเล็กทรอนิกส์

มาตรา ๑๖ ให้คณะกรรมการมีอำนาจประกาศกำหนดหลักเกณฑ์ วิธีการ และเงื่อนไขการให้บริการการชำระเงินทางอิเล็กทรอนิกส์ตามความจำเป็นและเหมาะสมกับประเภทธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์แต่ละบัญชี โดยอาจประกอบด้วยเรื่องดังต่อไปนี้

(๑) การเก็บรักษาและการเปิดเผยข้อมูลส่วนบุคคลของผู้ใช้บริการ

(๒) การตรวจสอบและรักษาความมั่นคงปลอดภัยของระบบการให้บริการที่น่าเชื่อถืออย่างสม่ำเสมอ

(๓) การปฏิบัติตามแผน นโยบาย มาตรการและระบบต่าง ๆ ที่ผู้ให้บริการยื่นตามมาตรา ๑๐ แล้วแต่กรณี

(๔) การกำหนดค่าธรรมเนียมในการให้บริการอย่างชัดเจน

(๕) การรับคำร้องเมื่อมีการร้องเรียน หรือมีข้อโต้แย้งจากผู้ใช้บริการ และการดำเนินการรวมทั้งกรอบเวลาเพื่อหาข้อยุติ

(๖) การจัดทำบัญชีและรายงานการปฏิบัติการ

(๗) การส่งงบการเงินและผลการดำเนินงานต่อ ธปท.

(๘) เรื่องอื่น ๆ ตามความเหมาะสมในการควบคุมดูแลการประกอบธุรกิจการให้บริการแต่ละประเภท

มาตรา ๑๗ เพื่อประโยชน์ในการควบคุมดูแลการประกอบธุรกิจของผู้ให้บริการแต่ละประเภท ธปท. จะกำหนดหลักเกณฑ์ วิธีการ และเงื่อนไขการให้บริการเพิ่มเติมที่จำเป็นให้เกิดความเรียบร้อย ในเรื่องดังต่อไปนี้ก็ได้

(๑) การออกหลักฐานการชำระเงิน

(๒) การเก็บรักษาเงินที่จะต้องส่งมอบ

(๓) การกำหนดผลสิ้นสุดของการโอนเงินซึ่งผู้รับสามารถใช้เงินได้ทันทีโดยปราศจากเงื่อนไข

(๔) การดำเนินการเพื่อรักษาสถานภาพทางการเงินของผู้ให้บริการ หรือ

(๕) การจัดให้มีผู้ตรวจสอบอิสระทางด้านความมั่นคงปลอดภัย

ผู้ตรวจสอบอิสระทางด้านความมั่นคงปลอดภัยตาม (๕) ให้เป็นไปตามรายชื่อที่คณะกรรมการประกาศกำหนด

มาตรา ๑๘ ให้ผู้ให้บริการตามบัญชี ข และบัญชี ค ต้องปฏิบัติในเรื่องดังต่อไปนี้

(๑) ในกรณีที่เกิดปัญหา หรือความบกพร่องในการให้บริการการชำระเงินทางอิเล็กทรอนิกส์ ให้แจ้ง ธปท. ทราบโดยเร็ว

(๒) จัดทำข้อมูลและรายละเอียดเกี่ยวกับการให้บริการตามพระราชกฤษฎีกานี้ไว้ให้พร้อมที่พนักงานเจ้าหน้าที่จะเข้าตรวจสอบได้ รวมทั้งอำนวยความสะดวกแก่พนักงานเจ้าหน้าที่ในการเข้าตรวจสอบการปฏิบัติตามพระราชกฤษฎีกานี้

(๓) ในกรณีที่มีการเปลี่ยนแปลงกรรมการ หรือผู้ซึ่งมีอำนาจจัดการของนิติบุคคล ให้แจ้งให้ ธปท. ทราบ โดยบุคคลดังกล่าวต้องมีคุณสมบัติและไม่มีลักษณะต้องห้ามตามมาตรา ๙ (๒) (ข) ในวันที่แจ้งการเปลี่ยนแปลงนั้น

มาตรา ๑๙ ในกรณีที่ผู้ให้บริการรายใดประสงค์จะเลิกการให้บริการ ให้ผู้ให้บริการรายนั้นแจ้งให้ ธปท. ทราบล่วงหน้าไม่น้อยกว่าหกสิบวันก่อนวันเลิกการให้บริการ และให้ส่งคืนใบรับแจ้ง ใบขึ้นทะเบียน หรือใบอนุญาต แล้วแต่กรณี ภายในสิบห้าวันนับแต่วันเลิกการให้บริการด้วย ทั้งนี้ หากผู้ประสงค์จะเลิกการให้บริการนั้นเป็นผู้ให้บริการตามบัญชี ข หรือบัญชี ค ให้ ธปท. ประกาศให้ทราบโดยทั่วกัน

ให้ ธปท. มีอำนาจสั่งให้ผู้ให้บริการที่ประสงค์จะเลิกการให้บริการตามวรรคหนึ่งต้องปฏิบัติอย่างหนึ่งอย่างใดเพื่อคุ้มครองประโยชน์ของผู้ใช้บริการก่อนเลิกการให้บริการก็ได้

ในกรณีที่ ธปท. ได้ดำเนินการตามวรรคหนึ่งแล้ว ให้รายงานให้คณะกรรมการทราบโดยเร็ว

มาตรา ๒๐ เพื่อประโยชน์ในการปฏิบัติการให้เป็นไปตามพระราชกฤษฎีกานี้ ให้พนักงานเจ้าหน้าที่มีอำนาจเรียกให้ผู้ให้บริการมาให้ข้อมูล หรือส่งเอกสารใด ๆ ในการควบคุมดูแลการประกอบธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์

มาตรา ๒๑ ในกรณีที่ผู้ให้บริการรายใดไม่ปฏิบัติตามหลักเกณฑ์ที่กำหนดไว้ในประกาศของ ธปท. ประกาศของคณะกรรมการ หรือพระราชกฤษฎีกานี้ ให้ ธปท. มีอำนาจสั่งให้แก้ไขหรือให้ปฏิบัติให้ถูกต้องภายในระยะเวลาที่กำหนดได้

หมวด ๓
การห้ามประกอบธุรกิจ การพักใช้ และเพิกถอนใบอนุญาต

มาตรา ๒๒ ในกรณีที่ผู้ให้บริการตามบัญชี ก หรือบัญชี ข ผู้ใดฝ่าฝืน หรือไม่ปฏิบัติตามประกาศของ ธปท. ประกาศของคณะกรรมการ หรือพระราชกฤษฎีกานี้ ให้ผู้ว่าการหรือพนักงานเจ้าหน้าที่ที่ผู้ว่าการมอบหมายรายงานต่อคณะกรรมการเพื่อดำเนินการตามบทบัญญัติในมาตรา ๓๓ วรรคสี่ วรรคห้า และวรรคหก แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ โดยเร็ว

มาตรา ๒๓ ในกรณีที่ผู้ให้บริการตามบัญชี ค ผู้ใดไม่ปฏิบัติตามหลักเกณฑ์ที่กำหนดไว้ในประกาศของ ธปท. ประกาศของคณะกรรมการ หรือพระราชกฤษฎีกานี้ จนเป็นเหตุให้เชื่อได้ว่าอาจส่งผลกระทบต่อระบบการชำระเงินโดยรวมของประเทศ หรือไม่ปฏิบัติตามคำสั่งของ ธปท. ที่สั่งให้แก้ไขให้ถูกต้องตามมาตรา ๒๑ ให้คณะกรรมการดำเนินการตามบทบัญญัติในมาตรา ๓๔ วรรคสี่ แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ และจะสั่งพักใช้ใบอนุญาตได้จนกว่าผู้ให้บริการผู้นั้นจะดำเนินการให้ถูกต้องภายในระยะเวลาที่คณะกรรมการกำหนดด้วยก็ได้

มาตรา ๒๔ ให้คณะกรรมการมีอำนาจสั่งเพิกถอนใบอนุญาตของผู้ให้บริการตามบัญชี ค เมื่อปรากฏว่าผู้ให้บริการตามบัญชี ค นั้น กระทำการอย่างหนึ่งอย่างใดดังต่อไปนี้

(๑) กระทำการตามที่บัญญัติไว้ในมาตรา ๓๔ วรรคห้า แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔

(๒) ขาดคุณสมบัติ หรือมีลักษณะต้องห้ามตามมาตรา ๘ และมาตรา ๙

(๓) ไม่ปฏิบัติตามหลักเกณฑ์ที่กำหนดไว้ในประกาศของ ธปท. ประกาศของคณะกรรมการหรือพระราชกฤษฎีกานี้ หรือกระทำความผิดตามมาตรา ๒๑ ซ้ำอีก จนเป็นเหตุให้เชื่อได้ว่าอาจส่งผลกระทบอย่างร้ายแรงต่อระบบการชำระเงินโดยรวมของประเทศ

บทเฉพาะกาล

มาตรา ๒๕ ผู้ซึ่งประกอบธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ตามพระราชกฤษฎีกานี้ในวันที่พระราชกฤษฎีกานี้ใช้บังคับ ให้ยังคงดำเนินการต่อไปได้เป็นระยะเวลาหนึ่งร้อยยี่สิบวันนับแต่วันที่พระราชกฤษฎีกานี้ใช้บังคับ

ในกรณีที่ผู้ให้บริการตามวรรคหนึ่งประสงค์จะประกอบธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ตามพระราชกฤษฎีกานี้ต่อไปภายหลังครบกำหนดระยะเวลาตามวรรคหนึ่ง ให้ผู้ให้บริการนั้นแจ้งให้ทราบ ขอขึ้นทะเบียน หรือขอรับใบอนุญาต แล้วแต่กรณี ภายในระยะเวลาเก้าสิบวัน แต่ไม่น้อยกว่าหกสิบวันก่อนครบกำหนดระยะเวลาตามวรรคหนึ่ง

ผู้รับสนองพระบรมราชโองการ
สมัคร สุนทรเวช
นายกรัฐมนตรี

บัญชีท้ายพระราชกฤษฎีกา
ว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ.๒๕๕๑

บัญชี ก

ธุรกิจบริการที่ต้องแจ้งให้ทราบก่อนให้บริการ

การให้บริการเงินอิเล็กทรอนิกส์ที่ใช้ซื้อสินค้าหรือรับบริการเฉพาะอย่างตามรายการที่กำหนดไว้ล่วงหน้า จากผู้ให้บริการเพียงรายเดียว ทั้งนี้ เว้นแต่การให้บริการเงินอิเล็กทรอนิกส์ที่ใช้จำกัดเพื่ออำนวยความสะดวกแก่ผู้บริโภคโดยมิได้แสวงหากำไรจากการออกบัตร ตามที่ ธปท. ประกาศกำหนดโดยความเห็นชอบของคณะกรรมการ

บัญชี ข

ธุรกิจบริการที่ต้องขอขึ้นทะเบียนก่อนให้บริการ

(๑) การให้บริการเครือข่ายบัตรเครดิต

(๒) การให้บริการเครือข่ายอีดีซี

(๓) การให้บริการสวิตช์ชิ่งในการชำระเงินระบบหนึ่งระบบใด

(๔) การให้บริการเงินอิเล็กทรอนิกส์ที่ใช้ซื้อสินค้า และหรือรับบริการเฉพาะอย่างตามรายการที่กำหนดไว้ล่วงหน้า จากผู้ให้บริการหลายราย ณ สถานที่ที่อยู่ภายใต้ระบบการจัดจำหน่ายและการให้บริการเดียวกัน

บัญชี ค

ธุรกิจบริการที่ต้องได้รับอนุญาตก่อนให้บริการ

(๑) การให้บริการหักบัญชี

(๒) การให้บริการชำระดุล

(๓) การให้บริการชำระเงินทางอิเล็กทรอนิกส์ผ่านอุปกรณ์อย่างหนึ่งอย่างใดหรือผ่านทางเครือข่าย

(๔) การให้บริการสวิตช์ชิ่งในการชำระเงินหลายระบบ

(๕) การให้บริการรับชำระเงินแทน

(๖) การให้บริการเงินอิเล็กทรอนิกส์ที่ใช้ซื้อสินค้า และหรือรับบริการเฉพาะอย่างตามรายการที่กำหนดไว้ล่วงหน้า จากผู้ให้บริการหลายราย โดยไม่จำกัดสถานที่และไม่อยู่ภายใต้ระบบการจัดจำหน่ายและการให้บริการเดียวกัน

หมายเหตุ :- เหตุผลในการประกาศใช้พระราชกฤษฎีกาฉบับนี้ คือ โดยที่ปัจจุบันเทคโนโลยีอิเล็กทรอนิกส์มีความก้าวหน้ามากขึ้น ซึ่งธุรกิจบริการเกี่ยวกับการชำระเงินทางอิเล็กทรอนิกส์เป็นธุรกิจที่ต้องใช้เทคโนโลยีอิเล็กทรอนิกส์ที่มีความซับซ้อนและหลากหลาย และเป็นธุรกิจที่มีมูลค่าโดยรวมทางเศรษฐกิจค่อนข้างสูงและมีการขยายตัวเพิ่มขึ้นอย่างรวดเร็ว นอกจากนี้ ผู้ให้บริการในธุรกิจการชำระเงินทางอิเล็กทรอนิกส์ในขณะนี้มิได้มีเพียงสถาบันการเงินเท่านั้นแต่ยังรวมถึงผู้ให้บริการที่มิได้มีกฎหมายใดควบคุมดูแล จึงอาจส่งผลกระทบต่อความมั่นคงทางการเงินและการพาณิชย์ ความน่าเชื่อถือและยอมรับในระบบข้อมูลอิเล็กทรอนิกส์ และอาจก่อให้เกิดความเสียหายต่อสาธารณชน ประกอบกับเพื่อบูรณาการกฎหมายที่เกี่ยวข้องกับธุรกิจบริการเกี่ยวกับการชำระเงินทางอิเล็กทรอนิกส์ให้เป็นฉบับเดียวกัน อันจะช่วยก่อให้เกิดประสิทธิภาพในการควบคุมดูแลและเป็นมาตรการสำคัญประการหนึ่งในการส่งเสริมการใช้บริการการชำระเงินทางอิเล็กทรอนิกส์มากขึ้นและเป็นการเพิ่มศักยภาพในการแข่งขันของภาคธุรกิจหรือการให้บริการภาครัฐ จึงจำเป็นต้องตราพระราชกฤษฎีกานี้

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง หลักเกณฑ์ วิธีการ และเงื่อนไข ในการประกอบธุรกิจบริการการชำระเงิน ทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๒

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

เรื่อง หลักเกณฑ์ วิธีการ และเงื่อนไขในการประกอบธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์

พ.ศ. ๒๕๕๒

อาศัยอำนาจตามความในมาตรา ๗ มาตรา ๙ มาตรา ๑๔ มาตรา ๑๕ และมาตรา ๑๖ แห่งพระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๑ คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์จึงกำหนดหลักเกณฑ์ วิธีการ และเงื่อนไขในการประกอบธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ ให้ผู้ให้บริการถือปฏิบัติ ดังนี้

ข้อ ๑ ในประกาศฉบับนี้

"ผู้ให้บริการ" หมายความว่า ผู้ประกอบธุรกิจให้บริการการชำระเงินทางอิเล็กทรอนิกส์ตามที่กำหนดไว้ในบัญชีท้ายพระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๑ ประกอบด้วยธุรกิจบริการที่ต้องแจ้งให้ทราบก่อนให้บริการ (บัญชี ก) ธุรกิจบริการที่ต้องขอขึ้นทะเบียนก่อนให้บริการ (บัญชี ข) และธุรกิจบริการที่ต้องได้รับอนุญาตก่อนให้บริการ (บัญชี ค)

"ธุรกิจบริการที่ต้องแจ้งให้ทราบก่อนให้บริการ" (บัญชี ก) ได้แก่ การให้บริการเงินอิเล็กทรอนิกส์ที่ใช้ซื้อสินค้าหรือรับบริการเฉพาะอย่างตามรายการที่กำหนดไว้ล่วงหน้าจากผู้ขายสินค้าหรือให้บริการเพียงรายเดียว ทั้งนี้ เว้นแต่การให้บริการเงินอิเล็กทรอนิกส์ที่ใช้จำกัดเพื่ออำนวยความสะดวกแก่ผู้บริโภคโดยมิได้แสวงหากำไรจากการออกบัตร ตามที่ธนาคารแห่งประเทศไทยประกาศกำหนดโดยความเห็นชอบของคณะกรรมการ (e-Money บัญชี ก)

"ธุรกิจบริการที่ต้องขอขึ้นทะเบียนก่อนให้บริการ" (บัญชี ข) ได้แก่

(๑) การให้บริการเครือข่ายบัตรเครดิต (Credit Card Network)

(๒) การให้บริการเครือข่ายอีดีซี (EDC Network)

(๓) การให้บริการสวิตช์ชิ่งในการชำระเงินระบบหนึ่งระบบใด (Transaction Switching บัญชี ข)

(๔) การให้บริการเงินอิเล็กทรอนิกส์ที่ใช้ซื้อสินค้า และหรือรับบริการเฉพาะอย่างตามรายการที่กำหนดไว้ล่วงหน้าจากผู้ขายสินค้าหรือให้บริการหลายราย ณ สถานที่ที่อยู่ภายใต้ระบบการจัดจำหน่ายและการให้บริการเดียวกัน (e-Money บัญชี ข)

"ธุรกิจบริการที่ต้องได้รับอนุญาตก่อนให้บริการ" (บัญชี ค) ได้แก่

(๑) การให้บริการหักบัญชี (Clearing)

(๒) การให้บริการชำระดุล (Settlement)

(๓) การให้บริการชำระเงินทางอิเล็กทรอนิกส์ผ่านอุปกรณ์อย่างหนึ่งอย่างใด หรือผ่านทางเครือข่าย

(๔) การให้บริการสวิตช์ชิ่งในการชำระเงินหลายระบบ (Transaction Switching บัญชี ค)

(๕) การให้บริการรับชำระเงินแทน

(๖) การให้บริการเงินอิเล็กทรอนิกส์ที่ใช้ซื้อสินค้า และหรือรับบริการเฉพาะอย่างตามรายการที่กำหนดไว้ล่วงหน้าจากผู้ขายสินค้าหรือให้บริการหลายราย โดยไม่จำกัดสถานที่และไม่อยู่ภายใต้ระบบการจัดจำหน่ายและการให้บริการเดียวกัน (e-Money บัญชี ค)

"ธปท." หมายความว่า ธนาคารแห่งประเทศไทยตามกฎหมายว่าด้วยธนาคารแห่งประเทศไทย

"ผู้ว่าการ" หมายความว่า ผู้ว่าการธนาคารแห่งประเทศไทย

"คณะกรรมการ" หมายความว่า คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

"พนักงานเจ้าหน้าที่" หมายความว่า ผู้ว่าการธนาคารแห่งประเทศไทย หรือผู้ซึ่งผู้ว่าการธนาคารแห่งประเทศไทยแต่งตั้งให้ปฏิบัติตามพระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๑

หมวด ๑

คุณสมบัติของผู้ให้บริการ การแจ้งให้ทราบ การขอขึ้นทะเบียน และการขอรับใบอนุญาต

ข้อ ๒ ผู้ประสงค์จะเป็นผู้ให้บริการตามบัญชี ก บัญชี ข หรือบัญชี ค ต้องมีคุณสมบัติตามที่กำหนดไว้ในมาตรา ๘ และมาตรา ๙ แห่งพระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๑

ข้อ ๓ ผู้ประสงค์จะเป็นผู้ให้บริการตามบัญชี ค ในแต่ละประเภทธุรกิจ ต้องมีทุนจดทะเบียนซึ่งชำระแล้ว ดังนี้

(๑) การให้บริการหักบัญชี (Clearing) ไม่ต่ำกว่า ๕๐ ล้านบาท

(๒) การให้บริการชำระดุล (Settlement) ไม่ต่ำกว่า ๒๐๐ ล้านบาท

(๓) การให้บริการชำระเงินทางอิเล็กทรอนิกส์ผ่านอุปกรณ์อย่างหนึ่งอย่างใด หรือผ่านทางเครือข่าย ไม่ต่ำกว่า ๕ ล้านบาท

(๔) การให้บริการสวิตช์ชิ่งในการชำระเงินหลายระบบ (Transaction Switching บัญชี ค) ไม่ต่ำกว่า ๕๐ ล้านบาท

(๕) การให้บริการรับชำระเงินแทน ไม่ต่ำกว่า ๕ ล้านบาท

(๖) การให้บริการเงินอิเล็กทรอนิกส์ที่ใช้ซื้อสินค้า และหรือรับบริการเฉพาะอย่างตามรายการที่กำหนดไว้ล่วงหน้าจากผู้ขายสินค้าหรือให้บริการหลายราย โดยไม่จำกัดสถานที่และไม่อยู่ภายใต้ระบบการจัดจำหน่ายและการให้บริการเดียวกัน (e-Money บัญชี ค) ไม่ต่ำกว่า ๒๐๐ ล้านบาท

ทั้งนี้ ผู้ประสงค์จะเป็นผู้ให้บริการมากกว่าหนึ่งประเภทธุรกิจ ต้องมีทุนจดทะเบียนซึ่งชำระแล้วไม่ต่ำกว่าจำนวนทุนจดทะเบียนซึ่งชำระแล้วของประเภทธุรกิจที่กำหนดไว้สูงสุด และเมื่อได้รับอนุญาตให้ประกอบธุรกิจแล้ว ห้ามผู้ให้บริการตามบัญชี ค ลดทุนก่อนได้รับอนุญาตจาก ธปท. เว้นแต่ผู้ให้บริการที่เป็นสถาบันการเงินตามพระราชบัญญัติธุรกิจสถาบันการเงิน พ.ศ. ๒๕๕๑ หรือผู้ให้บริการที่เป็นผู้ประกอบธุรกิจบัตรเงินอิเล็กทรอนิกส์หรือผู้ประกอบธุรกิจบัตรเครดิตหรือผู้ประกอบธุรกิจสินเชื่อส่วนบุคคลภายใต้การกำกับตามประกาศของคณะปฏิวัติ ฉบับที่ ๕๘ แล้วแต่กรณี ที่ได้รับอนุญาตตามหลักเกณฑ์ที่ออกภายใต้กฎหมายดังกล่าวแล้ว

ข้อ ๔ ผู้ประสงค์จะเป็นผู้ให้บริการตามบัญชี ก บัญชี ข หรือบัญชี ค ต้องยื่นแบบการแจ้งให้ทราบ แบบการขอขึ้นทะเบียน หรือแบบการขอรับใบอนุญาต พร้อมเอกสารหลักฐานแล้วแต่กรณี ตามแบบแนบท้ายประกาศฉบับนี้หรือตามแบบที่คณะกรรมการจะแก้ไขเพิ่มเติม ต่อผู้ว่าการหรือพนักงานเจ้าหน้าที่ที่ผู้ว่าการมอบหมาย

ทั้งนี้ กรณีที่ผู้ประสงค์จะประกอบธุรกิจเป็นผู้ให้บริการมากกว่าหนึ่งประเภทธุรกิจสามารถยื่นแบบการแจ้งให้ทราบ แบบการขอขึ้นทะเบียน หรือแบบการขอรับใบอนุญาต พร้อมเอกสารหลักฐานตามที่กำหนดในคราวเดียวกันได้

ข้อ ๕ ผู้ให้บริการที่ประสงค์จะประกอบธุรกิจต่อไปเมื่อใบอนุญาตครบกำหนด ให้ยื่นคำขอต่ออายุใบอนุญาต พร้อมเอกสารหลักฐานตามแบบที่คณะกรรมการกำหนด ต่อผู้ว่าการหรือพนักงานเจ้าหน้าที่ที่ผู้ว่าการมอบหมายภายในระยะเวลา ๙๐ วันแต่ไม่น้อยกว่า ๖๐ วันก่อนวันที่ใบอนุญาตเดิมสิ้นอายุ

ในกรณีที่คณะกรรมการพิจารณาไม่ต่อใบอนุญาต และสั่งให้ผู้ให้บริการต้องปฏิบัติการอย่างหนึ่งอย่างใดไปจนกว่าใบอนุญาตจะสิ้นอายุ พนักงานเจ้าหน้าที่จะแจ้งให้ผู้ให้บริการรายนั้นทราบเพื่อถือปฏิบัติต่อไป

ข้อ ๖ กรณีที่ใบรับแจ้ง ใบรับขึ้นทะเบียน หรือใบอนุญาต สูญหาย ถูกทำลาย หรือชำรุดเสียหายในสาระสำคัญ ให้ผู้ให้บริการยื่นคำขอรับใบแทนพร้อมเอกสารหลักฐานตามแบบแนบท้ายประกาศฉบับนี้หรือตามแบบที่คณะกรรมการจะแก้ไขเพิ่มเติม ต่อผู้ว่าการหรือพนักงานเจ้าหน้าที่ที่ผู้ว่าการมอบหมาย ภายในกำหนด ๓๐ วันนับตั้งแต่วันที่รู้ถึงการสูญหาย การถูกทำลาย หรือการชำรุดเสียหาย แล้วแต่กรณี ทั้งนี้ เมื่อพนักงานเจ้าหน้าที่ได้ตรวจสอบความครบถ้วนและถูกต้องของเอกสารหลักฐานแล้ว ให้พนักงานเจ้าหน้าที่ที่ผู้ว่าการมอบหมายออกใบแทนของใบรับแจ้ง ใบรับขึ้นทะเบียน หรือใบอนุญาต แล้วแต่กรณี

หมวด ๒
หลักเกณฑ์ วิธีการ และเงื่อนไขทั่วไปในการประกอบธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์

ข้อ ๗ ผู้ให้บริการตามบัญชี ก บัญชี ข และบัญชี ค ต้องประกอบธุรกิจโดยปฏิบัติตามแผน นโยบาย มาตรการ และระบบต่างๆ ตามที่ได้ยื่นแจ้งให้ทราบ ขึ้นทะเบียน หรือได้รับอนุญาต แล้วแต่กรณี

ข้อ ๘ กรณีผู้ให้บริการตามบัญชี ก บัญชี ข และบัญชี ค ได้มีการเปลี่ยนแปลงการดำเนินงานไปจากเอกสารที่ได้ยื่นประกอบการแจ้งให้ทราบ การขึ้นทะเบียน หรือการได้รับอนุญาต แล้วแต่กรณี ให้ผู้ให้บริการแต่ละรายยื่นขออนุญาตหรือแจ้งให้ ธปท. ทราบตามเงื่อนไข ดังต่อไปนี้

(๑) กรณีผู้ให้บริการตามบัญชี ข และบัญชี ค ย้ายสำนักงานใหญ่ หรือย้ายหรือปิดสำนักงานสาขา ให้ยื่นขออนุญาตจาก ธปท. ล่วงหน้าไม่น้อยกว่า ๓๐ วันก่อนเริ่มดำเนินการ ทั้งนี้ สำนักงานสาขาไม่รวมถึงจุดให้บริการชั่วคราว หรือสำนักงานหรือจุดให้บริการของตัวแทนที่ผู้ให้บริการแต่งตั้ง

(๒) กรณีดังต่อไปนี้ ให้ผู้ให้บริการแจ้ง ธปท. ทราบล่วงหน้าไม่น้อยกว่า ๑๕ วัน ก่อนเริ่มดำเนินการ

(ก) กรณีผู้ให้บริการตามบัญชี ก ย้ายสำนักงานใหญ่ หรือย้ายหรือปิดสำนักงานสาขา

(ข) กรณีผู้ให้บริการตามบัญชี ก บัญชี ข และบัญชี ค เปิดสำนักงานสาขาแห่งใหม่

(ค) กรณีผู้ให้บริการตามบัญชี ก บัญชี ข และบัญชี ค เปลี่ยนแปลงระบบสารสนเทศอย่างมีสาระสำคัญ หรือมีผลกระทบต่อการรักษาความมั่นคงปลอดภัยของระบบให้บริการ ให้แจ้ง ธปท. ทราบพร้อมทั้งแสดงแผนภาพของระบบสารสนเทศ

(ง) กรณีผู้ให้บริการตามบัญชี ข และบัญชี ค เพิ่มเติมการให้บริการอื่นที่เกี่ยวกับหรือเนื่องจากการให้บริการการชำระเงินทางอิเล็กทรอนิกส์จากที่ได้ขึ้นทะเบียนหรือได้รับอนุญาตไว้แล้วแต่กรณี

(๓) กรณีดังต่อไปนี้ ให้ผู้ให้บริการแจ้ง ธปท. ทราบภายใน ๑๕ วันนับจากวันที่มีการเปลี่ยนแปลง

(ก) กรณีผู้ให้บริการตามบัญชี ก บัญชี ข และบัญชี ค เปลี่ยนแปลงกรรมการหรือผู้ซึ่งมีอำนาจจัดการของนิติบุคคล

(ข) กรณีผู้ให้บริการตามบัญชี ข และบัญชี ค เปลี่ยนแปลงทุนจดทะเบียน

(ค) กรณีผู้ให้บริการตามบัญชี ข และบัญชี ค ปรับปรุงรูปแบบของการให้บริการตามที่ได้ขึ้นทะเบียนหรือได้รับอนุญาตไว้ แล้วแต่กรณี ให้แจ้ง ธปท. ทราบพร้อมทั้งแจ้งข้อมูลรายละเอียดของระบบสารสนเทศ (ถ้ามี)

เว้นแต่ การปฏิบัติตาม (๓) กรณีมีเหตุสุดวิสัย ผู้ให้บริการอาจขอผ่อนผันต่อ ธปท. พร้อมแจ้งเหตุผลและความจำเป็นไม่น้อยกว่า ๓ วันทำการก่อนครบระยะเวลาที่กำหนด โดย ธปท. อาจผ่อนผันระยะเวลาออกไปได้อีกไม่เกิน ๓๐ วัน และอาจกำหนดเงื่อนไขใด ๆ ไว้ด้วยก็ได้

ทั้งนี้ กรณีผู้ให้บริการที่เป็นสถาบันการเงินตามพระราชบัญญัติธุรกิจสถาบันการเงิน พ.ศ. ๒๕๕๑ หรือผู้ให้บริการที่เป็นผู้ประกอบธุรกิจบัตรเงินอิเล็กทรอนิกส์หรือผู้ประกอบธุรกิจบัตรเครดิตหรือผู้ประกอบธุรกิจสินเชื่อส่วนบุคคลภายใต้การกำกับตามประกาศของคณะปฏิวัติ ฉบับที่ ๕๘ ได้เปิด ย้าย หรือปิดสำนักงานสาขา และย้ายสำนักงานใหญ่ รวมถึงเปลี่ยนแปลงกรรมการหรือผู้ซึ่งมีอำนาจจัดการ และเปลี่ยนแปลงทุนจดทะเบียน โดยได้รับอนุญาตหรือแจ้งให้ ธปท. ทราบตามหลักเกณฑ์ที่ออกภายใต้พระราชบัญญัติธุรกิจสถาบันการเงิน พ.ศ. ๒๕๕๑ หรือประกาศของคณะปฏิวัติ ฉบับที่ ๕๘ แล้ว ให้ได้รับยกเว้นไม่ต้องปฏิบัติตาม (๑) (๒) (ก) (ข) หรือ (๓) (ก) (ข) อีกแล้วแต่กรณี

ข้อ ๙ ผู้ให้บริการตามบัญชี ก บัญชี ข และบัญชี ค ต้องกำหนดนโยบายในการเก็บรักษาข้อมูลของผู้ใช้บริการ การกำหนดชั้นความลับในการเข้าถึงข้อมูล และการระบุตัวบุคคลที่มีสิทธิเข้าถึง

ข้อมูลดังกล่าว พร้อมทั้งจัดให้มีระบบการจัดเก็บข้อมูลที่ถูกต้องเชื่อถือได้และป้องกันผู้ที่ไม่มีหน้าที่เกี่ยวข้องเข้าถึงหรือแก้ไขข้อมูลที่เก็บรักษา

ข้อ ๑๐ ผู้ให้บริการตามบัญชี ก บัญชี ข และบัญชี ค ต้องรักษาความลับข้อมูลส่วนบุคคลของผู้ใช้บริการ โดยจะไม่เปิดเผยข้อมูลเหล่านั้นตลอดระยะเวลาการใช้บริการและภายหลังที่เลิกใช้บริการแล้ว เว้นแต่กรณีต่อไปนี้

(๑) การเปิดเผยโดยได้รับความยินยอมเป็นหนังสือหรือวิธีการอื่นใดทางอิเล็กทรอนิกส์ตามที่ผู้ให้บริการกำหนดจากผู้ใช้บริการ

(๒) การเปิดเผยเพื่อประโยชน์แก่การสอบสวน หรือการพิจารณาคดี

(๓) การเปิดเผยแก่ผู้สอบบัญชีของผู้ให้บริการ

(๔) การเปิดเผยเพื่อประโยชน์ในการปฏิบัติตามกฎหมาย

(๕) การเปิดเผยเพื่อประโยชน์ในการกำกับดูแลระบบการชำระเงินของ ธปท.

ข้อ ๑๑ ผู้ให้บริการตามบัญชี ก บัญชี ข และบัญชี ค ต้องมีการกำหนดข้อตกลงในการให้บริการไว้เป็นลายลักษณ์อักษร และเปิดเผยให้ผู้ใช้บริการทราบอย่างชัดเจน ซึ่งอย่างน้อยต้องประกอบด้วย

(๑) สิทธิ หน้าที่ และความรับผิดของผู้ให้บริการและผู้ใช้บริการทั้งในกรณีปกติ และกรณีที่เกิดเหตุฉุกเฉิน

(๒) หลักเกณฑ์ เงื่อนไข และวิธีปฏิบัติในการให้บริการ

(๓) ความเสี่ยงทางการเงิน (Financial Risk) ที่อาจเกิดขึ้นจากการใช้บริการ (ถ้ามี)

ทั้งนี้ ผู้ให้บริการมีหน้าที่ติดตามดูแลให้ผู้ใช้บริการปฏิบัติตามหลักเกณฑ์ เงื่อนไขที่กำหนด และกรณีที่มีการเปลี่ยนแปลงซึ่งทำให้ผู้ใช้บริการเสียประโยชน์ ผู้ให้บริการต้องแจ้งให้ผู้ใช้บริการทราบล่วงหน้า โดยประกาศไว้ ณ สถานที่ทำการทุกแห่ง หรือด้วยวิธีการอื่นใดให้ผู้ใช้บริการสามารถทราบได้

ข้อ ๑๒ ผู้ให้บริการตามบัญชี ก บัญชี ข และบัญชี ค ต้องดำเนินการเกี่ยวกับการเปิดเผยค่าธรรมเนียมดังต่อไปนี้

(๑) เปิดเผยรายละเอียดของค่าธรรมเนียมที่จะเรียกเก็บจากผู้ใช้บริการ โดยประกาศไว้ ณ สถานที่ทำการทุกแห่ง หรือด้วยวิธีการอื่นใดให้ผู้ใช้บริการสามารถทราบได้ ทั้งนี้ ในการกำหนดค่าธรรมเนียม ผู้ให้บริการต้องกำหนดให้เป็นไปตามกลไกตลาดเพื่อให้เกิดการแข่งขัน และต้องคำนึงถึงความเป็นธรรมต่อผู้ใช้บริการด้วย

(๒) เมื่อมีการเปลี่ยนแปลงค่าธรรมเนียม ผู้ให้บริการจะต้องประกาศรายละเอียดไว้ ณ สถานที่ทำการทุกแห่ง โดยในกรณีที่มีการเปลี่ยนแปลงที่ทำให้ผู้ใช้บริการเสียประโยชน์ ผู้ให้บริการต้องแจ้งด้วยวิธีการอื่นใด ให้ผู้ใช้บริการทราบล่วงหน้าไม่น้อยกว่า ๓๐ วันก่อนการเปลี่ยนแปลงจะมีผลใช้บังคับ

(๓) จัดส่งประกาศค่าธรรมเนียมให้ ธปท. ทราบโดยเร็วในรูปเอกสารอิเล็กทรอนิกส์ นับแต่วันที่ออกประกาศครั้งแรกและทุก ๆ ครั้งที่มีการเปลี่ยนแปลง

ข้อ ๑๓ ผู้ให้บริการตามบัญชี ก บัญชี ข และบัญชี ค ต้องดำเนินการเมื่อมีการร้องเรียนหรือมีข้อโต้แย้งจากผู้ใช้บริการ รวมทั้งกำหนดกรอบเวลาเพื่อหาข้อยุติ ดังนี้

(๑) จัดให้มีช่องทางและวิธีการสำหรับการรับข้อร้องเรียนจากผู้ใช้บริการ

(๒) กำหนดวิธีปฏิบัติเกี่ยวกับขั้นตอนและการดำเนินการเพื่อหาข้อยุติเป็นลายลักษณ์อักษร โดยผู้ให้บริการต้องดำเนินการตรวจสอบและแจ้งความคืบหน้า รวมทั้งชี้แจงขั้นตอนการดำเนินการพร้อมทั้งแจ้งกำหนดเวลาในการแก้ไขข้อร้องเรียนให้ผู้ร้องเรียนทราบภายใน ๗ วัน นับจากวันที่ได้รับแจ้งการร้องเรียน

(๓) ดำเนินการแก้ไขข้อร้องเรียนให้แล้วเสร็จและแจ้งผลการดำเนินการให้ผู้ร้องเรียนทราบโดยเร็ว

ข้อ ๑๔ ผู้ให้บริการตามบัญชี ก บัญชี ข และบัญชี ค ต้องจัดทำงบการเงินที่แสดงฐานะทางการเงินและผลการดำเนินงาน และจัดส่งให้ ธปท. ตามเงื่อนไขดังต่อไปนี้ โดยเริ่มตั้งแต่งวดแรกที่ได้ประกอบธุรกิจ

(๑) ให้ผู้ให้บริการตามบัญชี ก ที่เป็นบุคคลธรรมดาจัดส่งสำเนาแบบแสดงรายการเสียภาษีเงินได้บุคคลธรรมดาที่ได้ยื่นเสียภาษีเงินได้บุคคลธรรมดา มายัง ธปท. ภายใน ๓๐ วัน นับแต่วันที่ได้ยื่นเสียภาษีในแต่ละงวด

(๒) ให้ผู้ให้บริการตามบัญชี ก ที่เป็นนิติบุคคลจัดส่งงบการเงินประจำปีที่ผ่านการรับรองจากผู้สอบบัญชีรับอนุญาตหรือผู้สอบบัญชีภาษีอากร แล้วแต่กรณี มายัง ธปท. ภายใน ๙๐ วัน นับแต่วันสิ้นงวด

(๓) ให้ผู้ให้บริการตามบัญชี ข และบัญชี ค จัดส่งงบการเงินงวด ๖ เดือนแรก มายัง ธปท. ภายใน ๓๐ วันนับแต่วันสิ้นงวด และจัดส่งงบการเงินประจำปีที่ผ่านการรับรองของผู้สอบบัญชีรับอนุญาตหรือผู้สอบบัญชีภาษีอากร แล้วแต่กรณี มายัง ธปท. ภายใน ๙๐ วันนับแต่วันสิ้นงวด

เว้นแต่กรณีมีเหตุสุดวิสัย ผู้ให้บริการอาจขอผ่อนผันต่อ ธปท. พร้อมแจ้งเหตุผลและความจำเป็นไม่น้อยกว่า ๓ วันทำการก่อนครบระยะเวลาที่กำหนด โดย ธปท. อาจผ่อนผันระยะเวลาออกไปได้อีกไม่เกิน ๓๐ วันและอาจกำหนดเงื่อนไข ใด ๆ ไว้ด้วยก็ได้

ทั้งนี้ กรณีผู้ให้บริการที่เป็นสถาบันการเงินที่ได้จัดส่งงบการเงินให้กับ ธปท. ตามหลักเกณฑ์ที่ออกภายใต้พระราชบัญญัติธุรกิจสถาบันการเงิน พ.ศ. ๒๕๕๑ ให้ถือว่าได้จัดส่งงบการเงินตามวรรคหนึ่งแล้ว

ข้อ ๑๕ ผู้ให้บริการตามบัญชี ก บัญชี ข และบัญชี ค ต้องจัดทำรายงานที่เกี่ยวข้องตามแบบและกำหนดเวลาที่ ธปท. กำหนด และส่งมายัง ธปท. ภายใน ๓๐ วันนับจากวันสิ้นงวดที่กำหนดให้จัดทำรายงานนั้น โดยเริ่มตั้งแต่งวดระยะเวลาแรกที่ผู้ให้บริการเริ่มประกอบธุรกิจ

ทั้งนี้ กรณีผู้ให้บริการที่ได้จัดส่งแบบรายงานที่เกี่ยวข้องให้กับ ธปท. ตามหลักเกณฑ์ที่ออกภายใต้พระราชบัญญัติธุรกิจสถาบันการเงิน พ.ศ. ๒๕๕๑ หรือประกาศของคณะปฏิวัติ ฉบับที่ ๕๘ แล้วแต่กรณี ให้ถือว่าได้ยื่นรายงานตามวรรคหนึ่งแล้ว เว้นแต่ ประเภทธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ที่ยังไม่มีหลักเกณฑ์กำหนดแบบรายงาน ก็ให้ผู้ให้บริการถือปฏิบัติตามหลักเกณฑ์ที่กำหนดในวรรคหนึ่งด้วย

นอกจากนี้ ผู้ให้บริการตามบัญชี ก บัญชี ข และบัญชี ค ทุกประเภท อาจต้องจัดทำข้อมูลรายงานอื่นเพิ่มเติมตามที่ ธปท. กำหนดด้วย

ข้อ ๑๖ ผู้ให้บริการตามบัญชี ก บัญชี ข และบัญชี ค ต้องจัดให้มีระบบงานที่สามารถตรวจสอบรายการย้อนหลังได้

ข้อ ๑๗ กรณีผู้ให้บริการตามบัญชี ก บัญชี ข และบัญชี ค ให้ผู้ให้บริการรายอื่นหรือบุคคลอื่น (Outsourcing) มาดำเนินการแทนในงานระบบสารสนเทศ รวมถึงงานที่มีผลกระทบอย่างมีนัยสำคัญต่อธุรกิจ ผู้ให้บริการจะต้องดำเนินการดังต่อไปนี้

(๑) จัดให้มีกระบวนการบริหารความเสี่ยง รวมทั้งการคัดเลือก ติดตาม ประเมินผลและตรวจสอบการให้บริการของผู้ให้บริการรายอื่นหรือบุคคลอื่น (Outsourcing) อย่างเหมาะสม โดยประเมินความเสี่ยงของการใช้บริการจากผู้ให้บริการรายอื่นอย่างสม่ำเสมอ

(๒) จัดให้มีการทำสัญญาการให้บริการ ซึ่งระบุสิทธิของผู้ตรวจสอบภายใน ผู้ตรวจสอบภายนอก และ ธปท. ในการเข้าตรวจสอบการดำเนินงานและการควบคุมภายในของผู้ให้บริการรายอื่นหรือบุคคลอื่นนั้นได้

ทั้งนี้ ผู้ให้บริการยังคงมีความรับผิดต่อผู้ใช้บริการในการให้บริการที่ต่อเนื่อง ปลอดภัย น่าเชื่อถือ และความเสียหายใด ๆ ที่อาจเกิดขึ้น เสมือนกับการให้บริการโดยผู้ให้บริการเอง

ข้อ ๑๘ ผู้ให้บริการตามบัญชี ก บัญชี ข และบัญชี ค ต้องจัดให้มีการตรวจสอบระบบสารสนเทศอย่างน้อยปีละหนึ่งครั้ง โดยให้เป็นไปตามแนวนโยบายและมาตรการการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศตามที่ ธปท. กำหนด และจัดส่งสำเนาผลการตรวจสอบมายัง ธปท. ภายใน ๓๐ วันนับแต่วันที่ทำการตรวจสอบแล้วเสร็จ

ทั้งนี้ กรณีผู้ให้บริการที่เป็นสถาบันการเงินที่ได้มีการตรวจสอบระบบสารสนเทศตามหลักเกณฑ์ที่ออกภายใต้พระราชบัญญัติธุรกิจสถาบันการเงิน พ.ศ. ๒๕๕๑ ให้ถือว่าได้ดำเนินการตามวรรคหนึ่งแล้ว

ข้อ ๑๙ ผู้ให้บริการจะต้องถือปฏิบัติตามประกาศ ธปท. เรื่อง หลักเกณฑ์ วิธีการ และเงื่อนไขว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ และเรื่อง นโยบายและมาตรการการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศในการประกอบธุรกิจของผู้ให้บริการการชำระเงินทางอิเล็กทรอนิกส์ ด้วย

หมวด ๓
หลักเกณฑ์เฉพาะสำหรับธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์แต่ละประเภท

ส่วนที่ ๑
การให้บริการเงินอิเล็กทรอนิกส์ (e-Money)

ข้อ ๒๐ ผู้ให้บริการเงินอิเล็กทรอนิกส์บัญชี ก บัญชี ข และบัญชี ค ต้องให้บริการภายใต้เงื่อนไข ดังนี้

(๑) การให้บริการเงินอิเล็กทรอนิกส์ต้องเป็นเงินสกุลบาทและใช้ในประเทศเท่านั้น

(๒) การให้บริการเงินอิเล็กทรอนิกส์ต้องไม่มีลักษณะเป็นการให้สินเชื่อ

(๓) ผู้ให้บริการต้องเปิดเผยหลักเกณฑ์และเงื่อนไขในการขอแลกคืนเป็นเงินสดให้ผู้ใช้บริการทราบ

ทั้งนี้ หากการขอแลกคืนเป็นเงินสดเป็นไปตามหลักเกณฑ์และเงื่อนไขแล้ว ผู้ให้บริการตามบัญชี ค จะต้องจัดให้มีการคืนเงินภายใน ๑๕ วันนับจากวันที่ผู้ใช้บริการได้ดำเนินการ ขอแลกคืน

(๔) ผู้ให้บริการต้องจัดให้มีวิธีการที่ผู้ใช้บริการสามารถตรวจสอบยอดเงินคงเหลือวันหมดอายุ และแจ้งวิธีการดังกล่าวให้ผู้ใช้บริการทราบ

(๕) ผู้ให้บริการต้องจัดให้มีระบบงานที่สามารถป้องกันไม่ให้ผู้ใช้บริการโอนเงินระหว่างกันโดยไม่ผ่านระบบของผู้ให้บริการ

(๖) ผู้ให้บริการต้องกำหนดแนวปฏิบัติเกี่ยวกับการรู้จักลูกค้า (Know Your Customer: KYC) การตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้า (Customer Due Diligence: CDD) และการรายงานข้อมูลตามแนวทางของสำนักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.)

(๗) ผู้ให้บริการเงินอิเล็กทรอนิกส์บัญชี ข และบัญชี ค ต้องจัดทำบัญชีเงินรับล่วงหน้าที่ได้รับจากผู้ใช้บริการแยกไว้ต่างหากจากบัญชีอื่นของผู้ให้บริการ และแยกแสดงไว้ในงบการเงินต่างหากให้ชัดเจน

(๘) ผู้ให้บริการเงินอิเล็กทรอนิกส์บัญชี ค ที่มิได้เป็นสถาบันการเงินตามพระราชบัญญัติธุรกิจสถาบันการเงิน พ.ศ. ๒๕๕๑ จะต้องประกอบธุรกิจเฉพาะธุรกิจการให้บริการเงินอิเล็กทรอนิกส์หรือธุรกิจที่เกี่ยวกับหรือเนื่องจากการให้บริการเงินอิเล็กทรอนิกส์เท่านั้น โดยหากธุรกิจที่เกี่ยวกับหรือเนื่องจากการให้บริการเงินอิเล็กทรอนิกส์ดังกล่าว เป็นธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ประเภทอื่น ให้ดำเนินการแจ้งให้ทราบ ขึ้นทะเบียน หรือขอรับใบอนุญาต แล้วแต่กรณีด้วย และห้ามประกอบธุรกิจอื่น

ส่วนที่ ๒
การให้บริการเครือข่ายบัตรเครดิต (Credit Card Network) การให้บริการเครือข่ายอีดีซี (EDC Network) และ การให้บริการสวิตช์ชิ่งในการชำระเงิน (Transaction Switching)

ข้อ ๒๑ ผู้ให้บริการเครือข่ายบัตรเครดิต ผู้ให้บริการเครือข่ายอีดีซี และผู้ให้บริการสวิตช์ชิ่งในการชำระเงินระบบหนึ่งระบบใด หรือผู้ให้บริการสวิตช์ชิ่งในการชำระเงินหลายระบบ ต้องกำหนดวัตถุประสงค์ หลักเกณฑ์ เงื่อนไข และวิธีปฏิบัติในการเข้าร่วมและการออกจากระบบของผู้ใช้บริการ (Access and Exit Criteria) ไว้อย่างชัดเจนเป็นลายลักษณ์อักษร และเปิดเผยให้ผู้ใช้บริการทราบโดยทั่วถึง เพื่อให้มั่นใจว่าการรับผู้ใช้บริการรายใหม่เพิ่มเติม จะไม่ก่อให้เกิดความเสี่ยงและผลกระทบต่อการใช้บริการของผู้ใช้บริการรายเดิม

ส่วนที่ ๓
การให้บริการหักบัญชี (Clearing)

ข้อ ๒๒ ให้นำความในข้อ ๒๑ มาใช้บังคับกับผู้ให้บริการหักบัญชีด้วย

ข้อ ๒๓ ผู้ให้บริการหักบัญชีต้องจัดให้มีมาตรการจัดการความเสี่ยง เพื่อให้การชำระดุลระหว่างผู้ใช้บริการสำเร็จลุล่วง โดยมีการชำระเงินตามภาระผูกพันภายในเวลาที่กำหนด รวมทั้งวิธีปฏิบัติที่เหมาะสมเพื่อรองรับกรณีที่ผู้ใช้บริการรายใดรายหนึ่งไม่สามารถชำระดุลได้ และต้องเปิดเผยให้ผู้ใช้บริการทราบโดยทั่วถึง รวมทั้งมีหน้าที่ต้องติดตามดูแลให้ผู้ใช้บริการปฏิบัติตามมาตรการและวิธีปฏิบัติดังกล่าวด้วย

ทั้งนี้ ในกรณีที่มีการเปลี่ยนแปลงมาตรการจัดการความเสี่ยง ผู้ให้บริการหักบัญชีต้องแจ้งให้ผู้ใช้บริการทราบล่วงหน้า และแจ้ง ธปท. ล่วงหน้าไม่น้อยกว่า ๑๕ วันก่อนเริ่มดำเนินการ

ข้อ ๒๔ ผู้ให้บริการหักบัญชีต้องแจ้งให้ ธปท. ทราบด้วยวาจาหรือโดยวิธีอื่นใดโดยทันทีเมื่อมีเหตุดังนี้

(๑) กรณีที่ผู้ใช้บริการรายใดรายหนึ่งไม่สามารถชำระดุลได้ด้วยวิธีการปกติและตามเวลาที่กำหนด เช่น มีเงินไม่เพียงพอสำหรับการชำระดุล โดยต้องใช้มาตรการจัดการความเสี่ยงและวิธีปฏิบัติที่กำหนดเพื่อให้กระบวนการชำระดุลสำเร็จลุล่วง

(๒) กรณีที่ระบบของผู้ให้บริการขัดข้อง ทำให้ไม่สามารถคำนวณยอดเงินแสดงความเป็นเจ้าหนี้ หรือลูกหนี้ของผู้ใช้บริการ หรือไม่สามารถส่งข้อมูลดังกล่าวไปเพื่อทำการชำระดุลระหว่างเจ้าหนี้และลูกหนี้ได้ด้วยวิธีการปกติและตามเวลาที่กำหนด

ทั้งนี้ ผู้ให้บริการหักบัญชีต้องจัดส่งรายงานปัญหากรณีเกิดเหตุขัดข้องตามแบบที่ ธปท. กำหนด ให้ ธปท. ภายในวันทำการถัดจากวันเกิดเหตุ

ข้อ ๒๕ ในกรณีที่ผู้ให้บริการหักบัญชีมีการระงับการให้บริการกับผู้ใช้บริการรายใดรายหนึ่งเป็นการชั่วคราว ผู้ให้บริการต้องแจ้งให้ผู้ใช้บริการรายอื่นทราบโดยทันที และในกรณีที่มีการยกเลิกการให้บริการกับผู้ใช้บริการรายใดรายหนึ่ง ให้แจ้งผู้ใช้บริการรายอื่นทราบล่วงหน้าไม่น้อยกว่า ๑๕ วัน

ทั้งนี้ ผู้ให้บริการหักบัญชีต้องแจ้ง ธปท. ทราบภายใน ๑๕ วันนับจากวันที่มีการระงับหรือยกเลิกการให้บริการ แล้วแต่กรณี

ส่วนที่ ๔

การให้บริการชำระดุล (Settlement)

ข้อ ๒๖ ให้นำความในข้อ ๒๑ มาใช้บังคับกับผู้ให้บริการชำระดุลด้วย

ข้อ ๒๗ ผู้ให้บริการชำระดุลต้องจัดให้มีวิธีการชำระดุลเพื่อปรับฐานะความเป็นเจ้าหนี้หรือลูกหนี้ของผู้ใช้บริการที่เหมาะสม โดยคำนึงถึงความเสี่ยงจากการชำระดุล (Settlement Risk) ที่อาจทำให้ไม่สามารถชำระดุลได้สำเร็จลุล่วงและส่งผลกระทบต่อผู้ใช้บริการรายอื่น

ข้อ ๒๘ ในกรณีที่ผู้ให้บริการชำระดุลไม่สามารถดำเนินการปรับฐานะความเป็นเจ้าหนี้หรือลูกหนี้ของผู้ใช้บริการได้ด้วยวิธีการปกติและตามเวลาที่กำหนด ให้ผู้ให้บริการชำระดุลแจ้งให้ ธปท. ทราบด้วยวาจาหรือโดยวิธีอื่นใดโดยทันที และต้องจัดส่งรายงานปัญหากรณีเกิดเหตุขัดข้องตามแบบที่ ธปท. กำหนด ภายในวันทำการถัดจากวันเกิดเหตุ

ข้อ ๒๙ ในกรณีที่ผู้ให้บริการชำระดุลมีการระงับการให้บริการกับผู้ใช้บริการรายใดรายหนึ่งเป็นการชั่วคราว ผู้ให้บริการต้องแจ้งให้ผู้ใช้บริการรายอื่นทราบโดยทันที และในกรณีที่มีการยกเลิกการให้บริการกับผู้ใช้บริการรายใดรายหนึ่ง ให้แจ้งผู้ใช้บริการรายอื่นทราบล่วงหน้าไม่น้อยกว่า ๑๕ วัน

ทั้งนี้ ผู้ให้บริการชำระดุลต้องแจ้ง ธปท. ทราบภายใน ๑๕ วันนับจากวันที่มีการระงับหรือยกเลิกการให้บริการ แล้วแต่กรณี

ส่วนที่ ๕

การให้บริการชำระเงินทางอิเล็กทรอนิกส์ผ่านอุปกรณ์อย่างหนึ่งอย่างใด หรือผ่านทางเครือข่าย

ข้อ ๓๐ ผู้ให้บริการชำระเงินทางอิเล็กทรอนิกส์ผ่านอุปกรณ์อย่างหนึ่งอย่างใด หรือผ่านทางเครือข่าย ต้องกำหนดแนวปฏิบัติเกี่ยวกับการรู้จักลูกค้า (Know Your Customer: KYC) การตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้า (Customer Due Diligence: CDD) และการรายงานตามแนวทางของสำนักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.)

ส่วนที่ ๖

การให้บริการรับชำระเงินแทน

ข้อ ๓๑ ผู้ให้บริการรับชำระเงินแทนต้องออกข้อกำหนดและให้บริการภายใต้เงื่อนไขดังนี้

(๑) กำหนดหน้าที่และความรับผิดของผู้ให้บริการที่มีต่อเจ้าหนี้ซึ่งผู้ให้บริการรับชำระเงินแทน และผู้ใช้บริการ รวมถึงหน้าที่และความรับผิดของตัวแทนที่ผู้ให้บริการแต่งตั้งด้วย

(๒) กำหนดวิธีปฏิบัติในการส่งข้อมูลรายการรับชำระเงินให้แก่เจ้าหนี้

ประกาศนี้ให้ใช้บังคับนับแต่วันที่ประกาศในราชกิจจานุเบกษาเป็นต้นไป

ประกาศ ณ วันที่ ๓๐ มกราคม พ.ศ. ๒๕๕๒

ร้อยตรีหญิง ระนองรักษ์ สุวรรณฉวี

รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

ประธานกรรมการธุรกรรมทางอิเล็กทรอนิกส์

เลขที่ ..... / 25....

แบบการแจ้งให้ทราบ

การประกอบธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ (บัญชี ก)

วันที่ ..... เดือน ..... พ.ศ. .....

เรียน ผู้ว่าการธนาคารแห่งประเทศไทย

ข้าพเจ้า..... ..... โดยสะกดเป็นภาษา
(ชื่อภาษาไทย)
อังกฤษว่า .... ที่ตั้งสำนักงานใหญ่
(ชื่อภาษาอังกฤษ)
อยู่ที่ .....
โทรศัพท์..... โทรสาร..... และมีสาขาจำนวน.....แห่ง ดังรายละเอียดต่อไปนี้

1. สาขา ..... ตั้งอยู่ที่ .....
2. สาขา ..... ตั้งอยู่ที่ .....
3. สาขา ..... ตั้งอยู่ที่ .....
4. สาขา ..... ตั้งอยู่ที่ .....
5. สาขา ..... ตั้งอยู่ที่ .....

(หากมีสาขามากกว่า 5 แห่ง ให้แนบรายชื่อและสถานที่ตั้งเพิ่มเติมมาด้วย ทั้งนี้ สาขา หมายถึง สำนักงานใด ๆ ซึ่งแยกออกจากสำนักงานใหญ่ของผู้ให้บริการไปประกอบการอย่างใดอย่างหนึ่งเกี่ยวกับธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ แต่ไม่รวมถึงจุดให้บริการชั่วคราวเพื่อการดำเนินการใดเป็นการเฉพาะ หรือสำนักงาน หรือจุดให้บริการของตัวแทนที่ผู้ให้บริการแต่งตั้ง)

มีความประสงค์ขอแจ้งให้ทราบว่าจะประกอบธุรกิจการให้บริการเงินอิเล็กทรอนิกส์ที่ใช้ซื้อสินค้าหรือรับบริการเฉพาะอย่างตามรายการที่กำหนดไว้ล่วงหน้า จากผู้ขายสินค้าหรือให้บริการเพียงรายเดียว ที่กำหนดไว้ในบัญชี ก (e-Money บัญชี ก) ตามบัญชีท้ายพระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. 2551

บัดนี้ ข้าพเจ้าได้แนบเอกสารและรายละเอียดที่ได้มีการรับรองสำเนาถูกต้องโดยผู้มีอำนาจลงนาม มาพร้อมแบบการแจ้งให้ทราบ การประกอบธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์นี้ด้วยแล้ว ดังนี้

ก. <u>รายละเอียด หลักฐาน และข้อมูลเกี่ยวกับผู้ให้บริการ</u>

<u>กรณีบุคคลธรรมดา</u>

(1) สำเนาบัตรประชาชนและสำเนาทะเบียนบ้าน หากผู้ให้บริการเป็นคณะบุคคลให้แนบสำเนาบัตรประจำตัวผู้เสียภาษีอากรของคณะบุคคลด้วย

(2) หนังสือชี้แจงพร้อมแนบหลักฐานแสดงจำนวนเงินทุนที่นำมาใช้ในการประกอบธุรกิจการให้บริการเงินอิเล็กทรอนิกส์

<u>กรณีนิติบุคคลที่เป็นห้างหุ้นส่วนสามัญจดทะเบียน หรือห้างหุ้นส่วนจำกัด</u>

(1) สำเนาหนังสือรับรองการจดทะเบียนห้างหุ้นส่วน

(2) วัตถุประสงค์ของห้างหุ้นส่วนเกี่ยวกับการประกอบธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์

<u>กรณีนิติบุคคลที่เป็นบริษัทจำกัด หรือบริษัทมหาชนจำกัด</u>

(1) สำเนาหนังสือรับรองการจดทะเบียนบริษัท

(2) วัตถุประสงค์ของบริษัทเกี่ยวกับการประกอบธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์

(3) สำเนาหนังสือบริคณห์สนธิของบริษัท

(4) สำเนาข้อบังคับของบริษัท

(5) สำเนาทะเบียนผู้ถือหุ้นของบริษัท

6) ชื่อ ประวัติการทำงาน และคุณวุฒิของกรรมการ

ข. <u>รายละเอียดเกี่ยวกับการประกอบธุรกิจการให้บริการเงินอิเล็กทรอนิกส์</u>

(1) รายละเอียดเกี่ยวกับการให้บริการ

1.1 ชื่อและประเภทการให้บริการ

1.2 สาระสำคัญ เงื่อนไข และรูปแบบการให้บริการ รวมถึงวิธีการบริหารเงินที่ได้รับล่วงหน้าจากผู้ใช้บริการ ซึ่งอย่างน้อยประกอบด้วย

1.2.1 ช่องทางในการแลกเปลี่ยนเงินสดเป็นเงินอิเล็กทรอนิกส์ของผู้ใช้บริการ

1.2.2 วิธีการบันทึกบัญชี

1.2.3 วิธีการบริหารเงินที่ยังไม่มีการเรียกเก็บ การบริหารสภาพคล่องและนโยบายการลงทุน

1.2.4 ขั้นตอนและวิธีการชำระเงินระหว่างผู้ที่เกี่ยวข้อง

1.3 รายละเอียดขั้นตอน วิธีการในการให้บริการ รวมถึงรายละเอียดในเรื่องต่าง ๆ ดังต่อไปนี้

1.3.1 แผนภาพระบบงาน

1.3.2 คำอธิบายรายละเอียดเทคโนโลยีที่ใช้ในการให้บริการ และเทคโนโลยีที่ใช้เพื่อการรักษาความมั่นคงปลอดภัยของระบบการให้บริการ

1.3.3 แนวทางการเชื่อมโยงกับระบบงานอื่นๆ ที่เกี่ยวข้อง

1.4 ขอบเขตการให้บริการ เช่น กลุ่มผู้ใช้บริการ ประเภทสินค้า หรือสถานที่ที่ให้บริการ เป็นต้น

1.5 ผู้ที่เกี่ยวข้องในการให้บริการ โดยระบุถึงหน้าที่ ความรับผิดชอบ และความสัมพันธ์ระหว่างกัน (ถ้ามี)

1.6 รายละเอียดการใช้บริการระบบสารสนเทศจากผู้ให้บริการรายอื่นหรือบุคคลอื่น (Outsourcing) โดยระบุระยะเวลา ขอบเขตการใช้บริการ และหน้าที่ความรับผิดชอบของผู้เกี่ยวข้องในการให้บริการ

(2) แผนฉุกเฉินด้านระบบสารสนเทศ หรือระบบการให้บริการสำรองเพื่อให้สามารถให้บริการได้อย่างต่อเนื่อง

(3) นโยบายและมาตรการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศ ซึ่งอย่างน้อยต้องมีมาตรฐานตามที่ธนาคารแห่งประเทศไทยประกาศกำหนด

(4) โครงสร้างองค์กรด้านเทคโนโลยีสารสนเทศของผู้ให้บริการ หน่วยงาน หรือบุคลากรที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ รวมถึงหน้าที่ความรับผิดชอบ

ข้าพเจ้าขอรับรองว่า หากเอกสารหรือหลักฐานใดไม่ถูกต้องหรือไม่ครบถ้วน หรือมิได้ปฏิบัติให้ถูกต้องตามหลักเกณฑ์และวิธีการที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์กำหนดแล้ว ข้าพเจ้าจะดำเนินการแก้ไขให้ถูกต้อง หรือครบถ้วน แล้วแต่กรณี ภายในเจ็ดวันนับจากที่ได้รับคำสั่งจากธนาคารแห่งประเทศไทย และข้าพเจ้าตกลงจะปฏิบัติตามเงื่อนไขที่ธนาคารแห่งประเทศไทยกำหนดขึ้นหรือจะกำหนดในภายหน้าทุกประการ

ทั้งนี้ หากได้รับใบรับแจ้งแล้ว ข้าพเจ้ายินยอมให้ธนาคารแห่งประเทศไทยสามารถเข้าตรวจสอบกิจการได้ตามความจำเป็นเพื่อให้มีการปฏิบัติเป็นไปตามหลักเกณฑ์ที่กำหนดได้

ขอรับรองว่ารายละเอียดข้างต้นนี้ถูกต้อง ครบถ้วน และตรงต่อความเป็นจริง

ลงนาม.....

( )

ผู้มีอำนาจลงนาม

(ประทับตรา ถ้ามี)

เลขที่ ..... / 25....

แบบการขอขึ้นทะเบียน

การประกอบธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ (บัญชี ข)

วันที่ ..... เดือน ..... พ.ศ. .....

เรียน ผู้ว่าการธนาคารแห่งประเทศไทย

ข้าพเจ้า..... *(ชื่อภาษาไทย)* .....โดยสะกดเป็นภาษาอังกฤษว่า ..... *(ชื่อภาษาอังกฤษ)* ... . ที่ตั้งสำนักงานใหญ่อยู่ที่ .....

โทรศัพท์..... โทรสาร..... และมีสาขาจำนวน.....แห่ง ดังรายละเอียดต่อไปนี้

1. สาขา ..... ตั้งอยู่ที่ .....
2. สาขา ..... ตั้งอยู่ที่ .....
3. สาขา ..... ตั้งอยู่ที่ .....
4. สาขา ..... ตั้งอยู่ที่ .....
5. สาขา ..... ตั้งอยู่ที่ .....

(หากมีสาขามากกว่า 5 แห่ง ให้แนบรายชื่อและสถานที่ตั้งเพิ่มเติมมาด้วย ทั้งนี้ สาขา หมายถึง สำนักงานใด ๆ ซึ่งแยกออกจากสำนักงานใหญ่ของผู้ให้บริการไปประกอบการอย่างใดอย่างหนึ่งเกี่ยวกับธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ แต่ไม่รวมถึงจุดให้บริการชั่วคราวเพื่อการดำเนินการใดเป็นการเฉพาะ หรือสำนักงาน หรือจุดให้บริการของตัวแทนที่ผู้ให้บริการแต่งตั้ง)

มีความประสงค์ที่จะขอขึ้นทะเบียน การประกอบธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ที่กำหนดไว้ในบัญชี ข ตามบัญชีท้ายพระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. 2551 ดังนี้ (โปรดทำเครื่องหมาย ✓ ในช่อง ☐ หน้าประเภทธุรกิจบริการที่ประสงค์จะขอขึ้นทะเบียน)

☐ (1) การให้บริการเครือข่ายบัตรเครดิต (Credit Card Network)

☐ (2) การให้บริการเครือข่ายอีดีซี (EDC Network)

☐ (3) การให้บริการสวิตช์ชิ่งในการชำระเงินระบบหนึ่งระบบใด (Transaction Switching บัญชี ข)

☐ (4) การให้บริการเงินอิเล็กทรอนิกส์ที่ใช้ซื้อสินค้า และหรือรับบริการเฉพาะอย่างตามรายการที่กำหนดไว้ล่วงหน้าจากผู้ขายสินค้าหรือให้บริการหลายราย ณ สถานที่ที่อยู่ภายใต้ระบบการจัดจำหน่ายและการให้บริการเดียวกัน (e-Money บัญชี ข)

บัดนี้ ข้าพเจ้าได้แนบเอกสารและรายละเอียดที่ได้มีการรับรองสำเนาถูกต้องโดยผู้มีอำนาจลงนาม มาพร้อมแบบการขอขึ้นทะเบียน การประกอบธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์นี้ด้วยแล้ว ดังนี้

ก. <u>รายละเอียด หลักฐาน และข้อมูลเกี่ยวกับผู้ให้บริการ</u>

<u>กรณีนิติบุคคลที่เป็นห้างหุ้นส่วนสามัญจดทะเบียน หรือห้างหุ้นส่วนจำกัด</u>

(1) สำเนาหนังสือรับรองการจดทะเบียนห้างหุ้นส่วน

(2) วัตถุประสงค์ของห้างหุ้นส่วนเกี่ยวกับการประกอบธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์

<u>กรณีนิติบุคคลที่เป็นบริษัทจำกัด หรือบริษัทมหาชนจำกัด</u>

(1) สำเนาหนังสือรับรองการจดทะเบียนบริษัท

(2) วัตถุประสงค์ของบริษัทเกี่ยวกับการประกอบธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์

(3) สำเนาหนังสือบริคณห์สนธิของบริษัท

(4) สำเนาข้อบังคับของบริษัท

(5) สำเนาทะเบียนผู้ถือหุ้นของบริษัท

(6) ชื่อ ประวัติการทำงาน และคุณวุฒิของกรรมการ

ข. <u>รายละเอียดเกี่ยวกับการประกอบธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์</u>

(1) รายละเอียดเกี่ยวกับการให้บริการ

1.1 ชื่อและประเภทการให้บริการ

1.2 สาระสำคัญ เงื่อนไข และรูปแบบการให้บริการ

1.3 รายละเอียดขั้นตอน วิธีการในการให้บริการ รวมถึงรายละเอียดในเรื่องต่าง ๆ ดังต่อไปนี้

1.3.1 แผนภาพระบบงาน

1.3.2 คำอธิบายรายละเอียดเทคโนโลยีที่ใช้ในการให้บริการ และเทคโนโลยีที่ใช้เพื่อการรักษาความมั่นคงปลอดภัยของระบบให้บริการ

1.3.3 แนวทางการเชื่อมโยงกับระบบงานอื่น ๆ ที่เกี่ยวข้อง

1.4 ขอบเขตการให้บริการ เช่น กลุ่มผู้ใช้บริการ ประเภทสินค้า หรือสถานที่ที่ให้บริการ เป็นต้น

1.5 ผู้ที่เกี่ยวข้องในการให้บริการ โดยระบุถึงหน้าที่ ความรับผิดชอบ และความสัมพันธ์ระหว่างกัน (ถ้ามี)

1.6 รายละเอียดการใช้บริการด้านระบบสารสนเทศจากผู้ให้บริการรายอื่นหรือบุคคลอื่น (Outsourcing) โดยระบุระยะเวลา ขอบเขตการใช้บริการ และหน้าที่ความรับผิดชอบของผู้เกี่ยวข้องในการให้บริการ

(2) นโยบายและมาตรการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศ ซึ่งอย่างน้อยต้องมีมาตรฐานตามที่ธนาคารแห่งประเทศไทยประกาศกำหนด

(3) โครงสร้างองค์กรด้านเทคโนโลยีสารสนเทศของผู้ให้บริการ หน่วยงาน หรือเจ้าหน้าที่ที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศรวมถึงหน้าที่ความรับผิดชอบ

(4) นโยบายและแผนการประกอบธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์

(5) แผนปฏิบัติการเตรียมการรองรับการประกอบธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์

(6) แนวทางการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management: BCM) โดยผู้ให้บริการควรกำหนดรายละเอียดการบริหารความต่อเนื่องทางธุรกิจให้เหมาะสมกับประเภทและความซับซ้อนของธุรกิจตนเอง ซึ่งมีสาระสำคัญดังนี้

6.1 การกำหนดแนวนโยบายการบริหารความต่อเนื่องทางธุรกิจ

6.2 การระบุและประเมินความเสี่ยง ซึ่งรวมถึงระบบการบริหารและจัดการความเสี่ยงประเภทต่าง ๆ ที่สามารถบ่งชี้และสามารถวัด ควบคุม ติดตาม ระดับความเสี่ยงโดยรวมขององค์กรได้ โดยรวมถึง

6.2.1 ความเสี่ยงด้านกลยุทธ์ (Strategic Risk)

6.2.2 ความเสี่ยงด้านสภาพคล่อง (Liquidity Risk)

6.2.3 ความเสี่ยงด้านปฏิบัติการ (Operation Risk)

6.2.4 ความเสี่ยงด้านกฎหมาย (Legal Risk)

6.2.5 ความเสี่ยงด้านชื่อเสียง (Reputation Risk)

6.3 การจัดทำแผนฉุกเฉินหรือแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Planning: BCP)

6.4 แนวทางการติดตามและประเมินผล และแนวทางการทดสอบแผน BCP

(7) ระบบการควบคุมภายใน รวมถึง

7.1 การกำหนดหน้าที่ความรับผิดชอบของหน่วยงานที่เกี่ยวข้อง

7.2 แนวทางการใช้บริการจากผู้ให้บริการรายอื่นหรือบุคคลอื่น (Outsourcing) และรายละเอียดของผู้ให้บริการรายอื่นหรือบุคคลอื่น (เช่น ผู้ถือหุ้น ฐานะทางการเงิน ความรับผิดชอบต่อการให้บริการ เป็นต้น)

(8) ผลการศึกษาความเป็นไปได้ (Feasibility Study) และประเมินความเสี่ยงในการให้บริการ

(9) นโยบายและมาตรการป้องกันปราบปรามการฟอกเงินและการต่อต้านการสนับสนุนทางการเงินแก่การก่อการร้าย ซึ่งไม่น้อยกว่าหลักเกณฑ์ที่สำนักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.) กำหนด

(10) รายละเอียดเพิ่มเติมเฉพาะสำหรับธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ตามบัญชี ข (รายละเอียดตามแนบ)

ข้าพเจ้าขอรับรองว่า หากเอกสารหรือหลักฐานใดไม่ถูกต้องหรือไม่ครบถ้วน หรือมิได้ปฏิบัติให้ถูกต้องตามหลักเกณฑ์และวิธีการที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์กำหนดแล้ว ข้าพเจ้าจะดำเนินการแก้ไขให้ถูกต้อง หรือครบถ้วน แล้วแต่กรณี ภายในเจ็ดวันนับจากที่ได้รับคำสั่งจากธนาคารแห่งประเทศไทย และเมื่อได้รับการขึ้นทะเบียนแล้ว ตกลงจะปฏิบัติตามเงื่อนไขที่ธนาคารแห่งประเทศไทยกำหนดขึ้น หรือจะกำหนดในภายหน้าทุกประการ

ทั้งนี้ หากได้รับใบขึ้นทะเบียนแล้ว ข้าพเจ้ายินยอมให้ธนาคารแห่งประเทศไทยสามารถเข้าตรวจสอบกิจการได้ตามความจำเป็นเพื่อให้มีการปฏิบัติเป็นไปตามหลักเกณฑ์ที่กำหนดได้

ขอรับรองว่ารายละเอียดข้างต้นนี้ถูกต้อง ครบถ้วน และตรงต่อความเป็นจริง

ลงนาม.....

( )

ผู้มีอำนาจลงนาม

(ประทับตรา ถ้ามี)

<u>รายละเอียดเพิ่มเติมเฉพาะสำหรับการให้บริการเงินอิเล็กทรอนิกส์ตามบัญชี ข (e-Money บัญชี ข)</u>

1. <u>รายละเอียดและวิธีการบริหารเงินที่ได้รับล่วงหน้าจากผู้ใช้บริการ</u>

1.1 ช่องทางในการแลกเปลี่ยนเงินสดเป็นเงินอิเล็กทรอนิกส์ของผู้ใช้บริการ

1.2 วิธีการบันทึกบัญชี

1.3 วิธีการบริหารเงินที่ยังไม่มีการเรียกเก็บ การบริหารสภาพคล่อง และนโยบายการลงทุน

1.4 ขั้นตอนและวิธีการชำระเงินระหว่างผู้ใช้บริการ ผู้ให้บริการ และร้านค้า รวมถึงผู้เกี่ยวข้องอื่น ๆ (ถ้ามี)

2. <u>รายละเอียดการควบคุมภายใน (เพิ่มเติม)</u>

2.1 วิธีการ และการควบคุมการดำเนินการสร้างหรือเปลี่ยนแปลงมูลค่าของเงินอิเล็กทรอนิกส์ เช่น วิธีการบันทึกมูลค่าเงินอิเล็กทรอนิกส์ หรือการเติมเงินอิเล็กทรอนิกส์ เป็นต้น

2.2 วิธีการเก็บรักษาและจำหน่ายเงินอิเล็กทรอนิกส์

2.3 การกำหนดวงเงินของเงินอิเล็กทรอนิกส์

2.4 การกำหนดอายุของเงินอิเล็กทรอนิกส์

3 <u>แนวทางการคุ้มครองผู้ใช้บริการ</u>

3.1 ข้อตกลงหรือสัญญา ระบุวิธีการ สิทธิ ความรับผิดชอบ และเงื่อนไขของการใช้บริการ

3.2 การปฏิบัติและจัดการเกี่ยวกับข้อมูลผู้ใช้บริการ

3.3 แนวทางและวิธีการเปิดเผยข้อมูลให้แก่ผู้ใช้บริการในเรื่องต่าง ๆ เช่น

- เงื่อนไขในการใช้บริการ เช่น สถานที่ใช้บริการ วงเงิน อายุของเงินอิเล็กทรอนิกส์ การคืนเงิน ค่าธรรมเนียม เป็นต้น
- ช่องทางการแจ้งปัญหา และแนวทางการแก้ไขปัญหา
- วิธีการ สิทธิ ความรับผิดชอบ และเงื่อนไข ในกรณีปัญหาต่างๆ เช่น บัตรถูกขโมยหรือสูญหาย ความผิดพลาดของมูลค่าเงินที่บันทึกไว้ บัตรชำรุด บัตรปลอม การใช้บัตรโดยไม่ได้รับอนุญาต เป็นต้น
- วิธีการตรวจสอบรายการการใช้เงินอิเล็กทรอนิกส์ของผู้ใช้บริการ
- วิธีการแจ้งข้อมูลหรือเงื่อนไขของการให้บริการที่เปลี่ยนแปลงแก่ผู้ใช้บริการ
- นโยบายในการแลกเปลี่ยนมูลค่าของเงินอิเล็กทรอนิกส์คืนเป็นเงินสด
- ค่าธรรมเนียมใด ๆ เกี่ยวกับการใช้เงินอิเล็กทรอนิกส์
- แนวทางการปฏิบัติเมื่อมีข้อร้องเรียน หรือข้อโต้แย้งเกี่ยวกับมูลค่าของเงินอิเล็กทรอนิกส์

เลขที่ ..... / 25....

แบบการขอรับใบอนุญาต

การประกอบธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ (บัญชี ค)

วันที่ ..... เดือน ..... พ.ศ. .....

เรียน ผู้ว่าการธนาคารแห่งประเทศไทย

ข้าพเจ้า..... *(ชื่อภาษาไทย)* .....โดยสะกดเป็นภาษาอังกฤษว่า ..... *(ชื่อภาษาอังกฤษ)* ..... ที่ตั้งสำนักงานใหญ่อยู่ที่ .....

โทรศัพท์..... โทรสาร..... และมีสาขาจำนวน.....แห่ง ดังรายละเอียดต่อไปนี้

1. สาขา ..... ตั้งอยู่ที่ .....
2. สาขา ..... ตั้งอยู่ที่ .....
3. สาขา ..... ตั้งอยู่ที่ .....
4. สาขา ..... ตั้งอยู่ที่ .....
5. สาขา ..... ตั้งอยู่ที่ .....

(หากมีสาขามากกว่า 5 แห่ง ให้แนบรายชื่อและสถานที่ตั้งเพิ่มเติมมาด้วย ทั้งนี้ สาขา หมายถึง สำนักงานใด ๆ ซึ่งแยกออกจากสำนักงานใหญ่ของผู้ให้บริการไปประกอบการอย่างใดอย่างหนึ่งเกี่ยวกับธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ แต่ไม่รวมถึงจุดให้บริการชั่วคราวเพื่อการดำเนินการใดเป็นการเฉพาะ หรือสำนักงาน หรือจุดให้บริการของตัวแทนที่ผู้ให้บริการแต่งตั้ง)

มีความประสงค์ที่จะขอรับใบอนุญาต การประกอบธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ ที่กำหนดไว้ในบัญชี ค ตามบัญชีท้ายพระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. 2551 (โปรดทำเครื่องหมาย ✓ ในช่อง ☐ หน้าประเภทธุรกิจบริการที่ประสงค์จะขอรับใบอนุญาต)

☐ (1) การให้บริการหักบัญชี (Clearing)

☐ (2) การให้บริการชำระดุล (Settlement)

☐ (3) การให้บริการชำระเงินทางอิเล็กทรอนิกส์ผ่านอุปกรณ์อย่างหนึ่งอย่างใดหรือผ่านทางเครือข่าย

☐ (4) การให้บริการสวิตช์ชิ่งในการชำระเงินหลายระบบ (Transaction Switching บัญชี ค)

☐ (5) การให้บริการรับชำระเงินแทน

☐ (6) การให้บริการเงินอิเล็กทรอนิกส์ที่ใช้ซื้อสินค้า และหรือรับบริการเฉพาะอย่างตามรายการที่กำหนดไว้ล่วงหน้า จากผู้ขายสินค้าหรือให้บริการหลายราย โดยไม่จำกัดสถานที่และไม่อยู่ภายใต้ระบบการจัดจำหน่ายและการให้บริการเดียวกัน (e-Money บัญชี ค)

บัดนี้ ข้าพเจ้าได้แนบเอกสารและรายละเอียดที่ได้มีการรับรองสำเนาถูกต้องโดยผู้มีอำนาจลงนาม มาพร้อมแบบการขอรับใบอนุญาต การประกอบธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์นี้ด้วยแล้ว ดังนี้

ก. <u>รายละเอียด หลักฐาน และข้อมูลเกี่ยวกับผู้ให้บริการ</u>

(1) สำเนาหนังสือรับรองการจดทะเบียนบริษัท

(2) วัตถุประสงค์ของบริษัทเกี่ยวกับการประกอบธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์

(3) สำเนาหนังสือบริคณห์สนธิของบริษัท

(4) สำเนาข้อบังคับของบริษัท

(5) สำเนาทะเบียนผู้ถือหุ้นของบริษัท

(6) ชื่อ ประวัติการทำงาน และคุณวุฒิของกรรมการ

ข. <u>รายละเอียดเกี่ยวกับการประกอบธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์</u>

(1) รายละเอียดเกี่ยวกับการให้บริการ

1.1 ชื่อและประเภทการให้บริการ

1.2 สาระสำคัญ เงื่อนไข และรูปแบบการให้บริการ

1.3 รายละเอียดขั้นตอน วิธีการในการให้บริการ รวมถึงรายละเอียดในเรื่องต่าง ๆ ดังต่อไปนี้

1.3.1 แผนภาพระบบงาน

1.3.2 คำอธิบายรายละเอียดเทคโนโลยีที่ใช้ในการให้บริการ และเทคโนโลยีที่ใช้เพื่อการรักษาความมั่นคงปลอดภัยของระบบให้บริการ

1.3.3 แนวทางการเชื่อมโยงกับระบบงานอื่น ๆ ที่เกี่ยวข้อง

1.4 ขอบเขตการให้บริการ เช่น กลุ่มผู้ใช้บริการ ประเภทสินค้า สถานที่ที่ให้บริการ เจ้าหนี้ซึ่งผู้ให้บริการรับชำระเงินแทน เป็นต้น

1.5 ผู้ที่เกี่ยวข้องในการให้บริการ โดยระบุถึงหน้าที่ ความรับผิดชอบ และความสัมพันธ์ระหว่างกัน (ถ้ามี)

1.6 รายละเอียดการใช้บริการระบบสารสนเทศจากผู้ให้บริการรายอื่นหรือบุคคลอื่น (Outsourcing) โดยระบุระยะเวลา ขอบเขตการใช้บริการ และหน้าที่ความรับผิดชอบของผู้เกี่ยวข้องในการให้บริการ

(2) นโยบายและมาตรการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศ ซึ่งอย่างน้อยต้องมีมาตรฐานตามที่ธนาคารแห่งประเทศไทยประกาศกำหนด

(3) โครงสร้างองค์กรด้านเทคโนโลยีสารสนเทศของผู้ให้บริการ หน่วยงาน หรือเจ้าหน้าที่ที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศรวมถึงหน้าที่ความรับผิดชอบ

(4) นโยบายและแผนการประกอบธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ในระยะเวลา 3 ปี โดยรวมถึงเงินลงทุน รายได้ ค่าใช้จ่าย ปริมาณธุรกรรม และบริการที่จะเพิ่มเติม เป็นต้น

(5) แผนปฏิบัติการเตรียมการรองรับการประกอบธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์

(6) แนวทางการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management: BCM) โดยผู้ให้บริการควรกำหนดรายละเอียดการบริหารความต่อเนื่องทางธุรกิจให้เหมาะสมกับประเภทและความซับซ้อนของธุรกิจตนเอง ซึ่งมีสาระสำคัญดังนี้

6.1 การกำหนดแนวนโยบายการบริหารความต่อเนื่องทางธุรกิจ

6.2 การระบุและประเมินความเสี่ยง ซึ่งรวมถึงระบบการบริหารและจัดการความเสี่ยงประเภทต่าง ๆ ที่สามารถบ่งชี้และสามารถวัด ควบคุม ติดตาม ระดับความเสี่ยงโดยรวมขององค์กรได้ โดยรวมถึง

6.2.1 ความเสี่ยงด้านกลยุทธ์ (Strategic Risk)

6.2.2 ความเสี่ยงด้านสภาพคล่อง (Liquidity Risk)

6.2.3 ความเสี่ยงด้านปฏิบัติการ (Operation Risk)

6.2.4 ความเสี่ยงด้านกฎหมาย (Legal Risk)

6.2.5 ความเสี่ยงด้านชื่อเสียง (Reputation Risk)

6.3 การจัดทำแผนฉุกเฉินหรือแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Planning: BCP)

6.4 แนวทางการติดตามและประเมินผล และแนวทางการทดสอบแผน BCP

(7) ระบบการควบคุมภายใน รวมถึง

7.1 การกำหนดหน้าที่ความรับผิดชอบของหน่วยงานที่เกี่ยวข้อง

7.2 แนวทางการใช้บริการจากผู้ให้บริการรายอื่นหรือบุคคลอื่น (Outsourcing) และรายละเอียดของผู้ให้บริการรายอื่นหรือบุคคลอื่น (เช่น ผู้ถือหุ้น ฐานะทางการเงิน ความรับผิดชอบต่อการให้บริการ เป็นต้น)

(8) ผลการศึกษาความเป็นไปได้ (Feasibility Study) และประเมินความเสี่ยงในการให้บริการ

(9) นโยบายและมาตรการป้องกันปราบปรามการฟอกเงินและการต่อต้านการสนับสนุนทางการเงินแก่การก่อการร้าย ซึ่งไม่น้อยกว่าหลักเกณฑ์ที่สำนักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.) กำหนด

(10) รายละเอียดเพิ่มเติมเฉพาะสำหรับธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ตามบัญชี ค (รายละเอียดตามแนบ)

ข้าพเจ้าขอรับรองว่า หากเอกสารหรือหลักฐานใดไม่ถูกต้องหรือไม่ครบถ้วน หรือมิได้ปฏิบัติให้ถูกต้องตามหลักเกณฑ์และวิธีการที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์กำหนดแล้ว ข้าพเจ้าจะรีบดำเนินการแก้ไขให้ถูกต้อง หรือครบถ้วน แล้วแต่กรณี ตามที่ได้รับคำสั่งจากธนาคารแห่งประเทศไทยภายในเวลาที่กำหนด และเมื่อได้รับใบอนุญาตแล้ว ข้าพเจ้าตกลงจะปฏิบัติตามเงื่อนไขที่ธนาคารแห่งประเทศไทยกำหนดขึ้น หรือจะกำหนดในภายหน้าทุกประการ

ทั้งนี้ หากได้รับใบอนุญาตแล้ว ข้าพเจ้ายินยอมให้ธนาคารแห่งประเทศไทยสามารถเข้าตรวจสอบกิจการได้ตามความจำเป็นเพื่อให้มีการปฏิบัติเป็นไปตามหลักเกณฑ์ที่กำหนดได้

ขอรับรองว่ารายละเอียดข้างต้นนี้ถูกต้อง ครบถ้วน และตรงต่อความเป็นจริง

ลงนาม.....

( )

ผู้มีอำนาจลงนาม

(ประทับตรา ถ้ามี)

รายละเอียดเพิ่มเติมเฉพาะสำหรับธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ตามบัญชี ค

1. <u>การให้บริการเงินอิเล็กทรอนิกส์ตามบัญชี ค (e-Money บัญชี ค)</u>

1.1 <u>รายละเอียดและวิธีการบริหารเงินที่ได้รับล่วงหน้าจากผู้ใช้บริการ</u>

1.1.1 ช่องทางในการแลกเปลี่ยนเงินสดเป็นเงินอิเล็กทรอนิกส์ของผู้ใช้บริการ

1.1.2 วิธีการบันทึกบัญชี

1.1.3 วิธีการบริหารเงินที่ยังไม่มีการเรียกเก็บ การบริหารสภาพคล่อง และนโยบายการลงทุน

1.1.4 ขั้นตอนและวิธีการชำระเงินระหว่างผู้ใช้บริการ ผู้ให้บริการ และร้านค้า รวมถึงผู้เกี่ยวข้องอื่น ๆ (ถ้ามี)

1.2 <u>รายละเอียดการควบคุมภายใน (เพิ่มเติม)</u>

1.2.1 วิธีการ และการควบคุมการดำเนินการสร้างหรือเปลี่ยนแปลงมูลค่าของเงินอิเล็กทรอนิกส์ เช่น วิธีการบันทึกมูลค่าเงินอิเล็กทรอนิกส์ หรือการเติมเงินอิเล็กทรอนิกส์ เป็นต้น

1.2.2 วิธีการเก็บรักษาและจำหน่ายเงินอิเล็กทรอนิกส์

1.2.3 การกำหนดวงเงินของเงินอิเล็กทรอนิกส์

1.2.4 การกำหนดอายุของเงินอิเล็กทรอนิกส์

1.3 <u>แนวทางการคุ้มครองผู้ใช้บริการ</u>

1.3.1 ข้อตกลงหรือสัญญา ระบุวิธีการ สิทธิ ความรับผิดชอบ และเงื่อนไขของการใช้บริการ

1.3.2 การปฏิบัติและจัดการเกี่ยวกับข้อมูลผู้ใช้บริการ

1.3.3 แนวทางและวิธีการเปิดเผยข้อมูลให้แก่ผู้ใช้บริการในเรื่องต่าง ๆ เช่น

- เงื่อนไขในการใช้บริการ เช่น สถานที่ใช้บริการ วงเงิน อายุของเงินอิเล็กทรอนิกส์ การคืนเงิน ค่าธรรมเนียม เป็นต้น
- ช่องทางการแจ้งปัญหา และแนวทางการแก้ไขปัญหา
- วิธีการ สิทธิ ความรับผิดชอบ และเงื่อนไข ในกรณีปัญหาต่างๆ เช่น บัตรถูกขโมยหรือสูญหาย ความผิดพลาดของมูลค่าเงินที่บันทึกไว้ บัตรชำรุด บัตรปลอม การใช้บัตรโดยไม่ได้รับอนุญาต เป็นต้น
- วิธีการตรวจสอบรายการการใช้เงินอิเล็กทรอนิกส์ของผู้ใช้บริการ
- วิธีการแจ้งข้อมูลหรือเงื่อนไขของการให้บริการที่เปลี่ยนแปลงแก่ผู้ใช้บริการ
- นโยบายในการแลกเปลี่ยนมูลค่าของเงินอิเล็กทรอนิกส์คืนเป็นเงินสด
- ค่าธรรมเนียมใด ๆ เกี่ยวกับการใช้เงินอิเล็กทรอนิกส์
- แนวทางการปฏิบัติเมื่อมีข้อร้องเรียน หรือข้อโต้แย้งเกี่ยวกับมูลค่าของเงินอิเล็กทรอนิกส์

2. <u>การให้บริการหักบัญชี (Clearing)</u>

2.1 วัตถุประสงค์ หลักเกณฑ์ เงื่อนไข และวิธีปฏิบัติในการเข้าร่วมและออกจากระบบของผู้ใช้บริการ

2.2 ข้อตกลง หลักเกณฑ์ เงื่อนไข และวิธีปฏิบัติในการดำเนินงาน ระหว่างผู้ให้บริการกับผู้ใช้บริการ

2.3 มาตรการจัดการความเสี่ยง เพื่อให้การชำระดุลระหว่างผู้ใช้บริการสำเร็จลุล่วง

2.4 จำนวนและรายชื่อผู้ใช้บริการ (ถ้ามี)

3. <u>การให้บริการชำระดุล (Settlement)</u>

3.1 วัตถุประสงค์ หลักเกณฑ์ เงื่อนไข และวิธีปฏิบัติในการเข้าร่วมและออกจากระบบของผู้ใช้บริการ

3.2 ข้อตกลง หลักเกณฑ์ เงื่อนไข และวิธีปฏิบัติในการดำเนินงาน ระหว่างผู้ให้บริการกับผู้ใช้บริการ

3.3 หลักเกณฑ์และเงื่อนไขที่กำหนดผลสิ้นสุดสมบูรณ์ของการโอนเงิน (Finality) ซึ่งผู้รับสามารถใช้เงินได้ทันทีโดยปราศจากเงื่อนไข และไม่สามารถเพิกถอนได้ (Irrevocable)

3.4 จำนวนและรายชื่อผู้ใช้บริการ (ถ้ามี)

4. <u>การให้บริการสวิตช์ชิ่งในการชำระเงินหลายระบบ (Transaction switching บัญชี ค)</u>

4.1 วัตถุประสงค์ หลักเกณฑ์ เงื่อนไข และวิธีปฏิบัติในการเข้าร่วมและออกจากระบบของผู้ใช้บริการ

4.2 ข้อตกลง หลักเกณฑ์ เงื่อนไข และวิธีปฏิบัติในการดำเนินงาน ระหว่างผู้ให้บริการกับผู้ใช้บริการ

4.3 จำนวนและรายชื่อผู้ใช้บริการ (ถ้ามี)

5. <u>การให้บริการรับชำระเงินแทน</u>

แนวทางการคุ้มครองผู้ใช้บริการ

5.1 ข้อตกลงกับผู้ใช้บริการ โดยมีรายละเอียดเกี่ยวกับกำหนดหน้าที่และความรับผิดชอบของผู้ให้บริการต่อผู้ใช้บริการ

5.2 การปฏิบัติและจัดการเกี่ยวกับข้อมูลผู้ใช้บริการ

5.3 กำหนดผลสิ้นสุดของการชำระเงินเมื่อผู้ใช้บริการได้ชำระเงินให้กับผู้ให้บริการแล้ว

เลขที่ ..... / 25....

แบบการขอรับใบแทน

กรณีที่ใบรับแจ้ง ใบรับการขึ้นทะเบียน หรือใบอนุญาต การประกอบธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ สูญหาย ถูกทำลาย หรือชำรุดเสียหายในสาระสำคัญ

วันที่ ..... เดือน ..... พ.ศ. .....

เรียน ผู้ว่าการธนาคารแห่งประเทศไทย

ข้าพเจ้า..... *(ชื่อภาษาไทย)* .....โดยสะกดเป็นภาษาอังกฤษ ว่า ..... *(ชื่อภาษาอังกฤษ)* ..... ที่ตั้งสำนักงานใหญ่อยู่ที่ .....

โทรศัพท์..... โทรสาร.....

มีความประสงค์ที่จะขอรับใบแทน กรณีที่ใบรับแจ้ง ใบรับการขึ้นทะเบียน หรือใบอนุญาต ที่เคยได้รับ เกิด ☐ สูญหาย ☐ ถูกทำลาย หรือ ☐ ชำรุดเสียหายในสาระสำคัญ ในการประกอบธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์กรณีดังต่อไปนี้

☐ **ใบรับแจ้ง (บัญชี ก)** การประกอบธุรกิจการให้บริการเงินอิเล็กทรอนิกส์ที่ใช้ซื้อสินค้าหรือรับบริการเฉพาะอย่างตามรายการที่กำหนดไว้ล่วงหน้า จากผู้ขายสินค้าหรือให้บริการเพียงรายเดียว ที่กำหนดไว้ในบัญชี ก (e-Money บัญชี ก) เลขที่ ..... ลงวันที่ .....

☐ **ใบรับขึ้นทะเบียน (บัญชี ข)** เลขที่ ..... ลงวันที่ .....

- ☐ (1) การให้บริการเครือข่ายบัตรเครดิต (Credit card network)
- ☐ (2) การให้บริการเครือข่ายอีดีซี (EDC network)
- ☐ (3) การให้บริการสวิตช์ชิ่งในการชำระเงินระบบหนึ่งระบบใด (Transaction Switching บัญชี ข)
- ☐ (4) การให้บริการเงินอิเล็กทรอนิกส์ที่ใช้ซื้อสินค้า และหรือรับบริการเฉพาะอย่างตามรายการที่กำหนดไว้ล่วงหน้าจากผู้ขายสินค้าหรือให้บริการหลายราย ณ สถานที่ที่อยู่ภายใต้ระบบการจัดจำหน่ายและการให้บริการเดียวกัน (e-Money บัญชี ข)

☐ **ใบอนุญาต (บัญชี ค)** เลขที่ ..... ลงวันที่ .....

☐ (1) การให้บริการหักบัญชี (Clearing)

☐ (2) การให้บริการชำระดุล (Settlement)

☐ (3) การให้บริการชำระเงินทางอิเล็กทรอนิกส์ผ่านอุปกรณ์อย่างหนึ่งอย่างใดหรือผ่านทางเครือข่าย

☐ (4) การให้บริการสวิตช์ชิ่งในการชำระเงินหลายระบบ (Transaction Switching บัญชี ค)

☐ (5) การให้บริการรับชำระเงินแทน

☐ (6) การให้บริการเงินอิเล็กทรอนิกส์ที่ใช้ซื้อสินค้า และหรือรับบริการเฉพาะอย่างตามรายการที่กำหนดไว้ล่วงหน้า จากผู้ขายสินค้าหรือให้บริการหลายราย โดยไม่จำกัดสถานที่และไม่อยู่ภายใต้ระบบการจัดจำหน่ายและการให้บริการเดียวกัน (e-Money บัญชี ค)

ลงนาม.....

( )

ผู้มีอำนาจลงนาม

(ประทับตรา ถ้ามี)

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง หลักเกณฑ์ วิธีการ และเงื่อนไข ในการประกอบธุรกิจบริการการชำระเงิน ทางอิเล็กทรอนิกส์ (ฉบับที่ ๒) พ.ศ. ๒๕๕๕

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

เรื่อง หลักเกณฑ์ วิธีการ และเงื่อนไขในการประกอบธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ (ฉบับที่ ๒) พ.ศ. ๒๕๕๕

เพื่อรักษาความมั่นคงทางการเงิน และลดต้นทุนในการให้บริการการชำระเงินทางอิเล็กทรอนิกส์ตลอดจนเพื่อประโยชน์ต่อการเข้าไปกำกับดูแลของธนาคารแห่งประเทศไทย

อาศัยอำนาจตามความในมาตรา ๑๖ (๘) แห่งพระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๑ คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์จึงออกประกาศไว้ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง หลักเกณฑ์ วิธีการ และเงื่อนไขในการประกอบธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ (ฉบับที่ ๒) พ.ศ. ๒๕๕๕ ”

ข้อ ๒ ให้เพิ่มความต่อไปนี้เป็นส่วนที่ ๗ ในหมวด ๓ แห่งประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง หลักเกณฑ์ วิธีการ และเงื่อนไขในการประกอบธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๒

“ส่วนที่ ๗
การให้บริการที่เกี่ยวข้องกับบัตรเดบิตที่ออกและมีการใช้จ่ายภายในประเทศ

ข้อ ๓๒ ในส่วนนี้

“ผู้ออกบัตร” (Issuer) หมายความว่า สถาบันการเงินที่ตกลงและยินยอมออกบัตรเดบิตให้แก่บุคคลที่ผูกพันตนตามสัญญาบัตรเดบิต

“ผู้ให้บริการแก่ผู้รับบัตร” (Acquirer) หมายความว่า ผู้ที่ทำหน้าที่ให้บริการรับส่งข้อมูลการชำระเงินทางอิเล็กทรอนิกส์จากบัตรเดบิตไปยังผู้ออกบัตร และจะจ่ายเงินค่าสินค้าหรือค่าบริการให้แก่ผู้ประกอบกิจการขายสินค้าหรือให้บริการซึ่งมีสัญญาระหว่างกันว่าจะรับชำระราคาสินค้าหรือบริการด้วยบัตรเดบิตตามเงื่อนไขที่ตกลงกัน

ผู้ให้บริการ หมายความว่า

(๑) ผู้ให้บริการการชำระเงินทางอิเล็กทรอนิกส์ผ่านอุปกรณ์อย่างหนึ่งอย่างใดหรือผ่านทางเครือข่ายตามบัญชี ค (๓) ที่เป็นผู้ออกบัตร (Issuer) และผู้ให้บริการแก่ผู้รับบัตร (Acquirer)

(๒) ผู้ให้บริการสวิตช์ชิ่งในการชำระเงินระบบหนึ่งระบบใดตามบัญชี ข (๓) หรือผู้ให้บริการสวิตช์ชิ่งในการชำระเงินหลายระบบตามบัญชี ค (๔)

(๓) ผู้ให้บริการหักบัญชีตามบัญชี ค (๑)

(๔) ผู้ให้บริการชำระดุลตามบัญชี ค (๒)

ข้อ ๓๓ ในการให้บริการที่เกี่ยวข้องกับบัตรเดบิตที่ออกและมีการใช้จ่ายภายในประเทศ ผู้ให้บริการต้องดำเนินการเหล่านี้ภายในประเทศเท่านั้น

(๑) การรับส่งข้อมูลการใช้บัตรเดบิตระหว่างผู้ให้บริการแก่ผู้รับบัตร (Acquirer) และผู้ออกบัตร (Issuer)

(๒) การให้บริการสวิตช์ชิ่งในการชำระเงิน (Transaction Switching)

(๓) การให้บริการหักบัญชี (Clearing)

(๔) การให้บริการชำระดุล (Settlement)

ข้อ ๓๔ ในกรณีที่ผู้ให้บริการ จะให้ผู้ให้บริการรายอื่นหรือบุคคลอื่นมาดำเนินการแทนในงานระบบสารสนเทศ (IT Outsourcing) ผู้ให้บริการจะต้องได้รับอนุญาตจาก ธปท. ก่อนการดำเนินการ”

ข้อ ๓ ผู้ให้บริการตามประกาศนี้ที่ได้รับอนุญาตหรือได้ขึ้นทะเบียนไว้อยู่ก่อนวันที่ประกาศนี้ใช้บังคับ ให้สามารถให้บริการต่อไปได้ แต่จะต้องดำเนินการให้เป็นไปตามหลักเกณฑ์ วิธีการ และเงื่อนไขตามที่กำหนดไว้ในประกาศนี้ภายในหนึ่งปี นับแต่วันที่ประกาศนี้ใช้บังคับ

ในกรณีที่ผู้ให้บริการตามวรรคหนึ่งเห็นว่าไม่สามารถดำเนินการให้เป็นไปตามหลักเกณฑ์ วิธีการ และเงื่อนไขที่กำหนดตามประกาศนี้ภายในระยะเวลาตามวรรคหนึ่ง ให้ขออนุญาตพร้อมชี้แจงเหตุผลและความจำเป็นต่อ ธปท. เป็นรายกรณี ก่อนครบระยะเวลาตามวรรคหนึ่ง

ข้อ ๔ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ประกาศ ณ วันที่ ๑๕ สิงหาคม พ.ศ. ๒๕๕๕
นาวาอากาศเอก อนุดิษฐ์ นาครทรรพ
รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
ประธานกรรมการธุรกรรมทางอิเล็กทรอนิกส์

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง หลักเกณฑ์การพิจารณาลงโทษปรับทางปกครอง สำหรับผู้ประกอบธุรกิจให้บริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๔

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

เรื่อง หลักเกณฑ์การพิจารณาลงโทษปรับทางปกครอง
สำหรับผู้ประกอบธุรกิจให้บริการการชำระเงินทางอิเล็กทรอนิกส์
พ.ศ. ๒๕๕๔

อาศัยอำนาจตามความในมาตรา ๓๓ มาตรา ๓๔ แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ ประกอบมาตรา ๒๒ และมาตรา ๒๓ แห่งพระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๑ คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ได้กำหนดหลักเกณฑ์ วิธีการและเงื่อนไขในการพิจารณาลงโทษปรับทางปกครอง ดังนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง หลักเกณฑ์การพิจารณาลงโทษปรับทางปกครองสำหรับผู้ประกอบธุรกิจให้บริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๔”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับนับแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ให้ประธานกรรมการธุรกรรมทางอิเล็กทรอนิกส์เป็นผู้รักษาการตามประกาศนี้

หมวด ๑
บททั่วไป

ข้อ ๔ ในประกาศนี้

“การพิจารณาลงโทษปรับทางปกครอง” หมายความว่า การดำเนินการที่เกี่ยวกับการพิจารณาลงโทษปรับทางปกครองสำหรับผู้ประกอบธุรกิจให้บริการการชำระเงินทางอิเล็กทรอนิกส์

“คณะกรรมการ” หมายความว่า คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

“พนักงานเจ้าหน้าที่” หมายความว่า ผู้ว่าการธนาคารแห่งประเทศไทยหรือผู้ซึ่งผู้ว่าการธนาคารแห่งประเทศไทยแต่งตั้งให้ปฏิบัติการตามพระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๑

“ผู้ถูกกล่าวหา” หมายความว่า ผู้ให้บริการตามที่กำหนดไว้ในพระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๑ ซึ่งพนักงานเจ้าหน้าที่พิจารณาในเบื้องต้นแล้วเห็นว่ามีการกระทำที่มีมูลเข้าข่ายเป็นการกระทำผิดที่มีโทษปรับทางปกครอง

“ผู้ถูกสั่งปรับ” หมายความว่า ผู้กระทำการฝ่าฝืนพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ ที่คณะกรรมการมีคำสั่งปรับ

“ค่าปรับ” หมายความว่า เงินค่าปรับทางปกครองที่คณะกรรมการกำหนดให้ผู้กระทำการฝ่าฝืนพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ ชำระให้แก่คณะกรรมการ

“ยึด” หมายความว่า การกระทำใด ๆ ต่อทรัพย์สินของผู้ถูกสั่งปรับ เพื่อให้ทรัพย์สินนั้นได้เข้ามาอยู่ในความควบคุมหรือครอบครองของเจ้าหน้าที่บังคับโทษปรับทางปกครอง

“อายัด” หมายความว่า การสั่งให้ผู้ถูกสั่งปรับและหรือบุคคลภายนอกมิให้จำหน่าย จ่าย โอนหรือกระทำนิติกรรมใด ๆ เกี่ยวกับทรัพย์สิน หรือสิทธิเรียกร้องที่ได้สั่งอายัดไว้ รวมตลอดถึงการสั่งให้บุคคลภายนอกมิให้นำส่งมอบทรัพย์สิน หรือชำระหนี้แก่ผู้ถูกสั่งปรับ แต่ให้ส่งมอบทรัพย์สินหรือชำระหนี้ต่อเจ้าหน้าที่บังคับโทษปรับทางปกครอง ณ ที่ซึ่งเจ้าหน้าที่บังคับโทษปรับทางปกครองกำหนด

“การขายทอดตลาด” หมายความว่า การนำเอาทรัพย์สินของผู้ถูกสั่งปรับออกขายโดยวิธีให้สู้ราคากันโดยเปิดเผย

“เจ้าหน้าที่บังคับโทษปรับทางปกครอง” หมายความว่า บุคคลผู้ซึ่งคณะกรรมการมอบหมายให้ดำเนินการบังคับตามคำสั่งลงโทษปรับทางปกครองหรือคำสั่งอื่นใดที่เกี่ยวข้อง

ข้อ ๕ ในการพิจารณาและมีคำสั่งลงโทษปรับทางปกครอง และการพิจารณาอุทธรณ์คำสั่งดังกล่าว นอกจากที่กำหนดไว้ในประกาศนี้ให้นำกฎหมายว่าด้วยวิธีปฏิบัติราชการทางปกครองมาใช้บังคับโดยอนุโลม เว้นแต่ที่ขัดหรือแย้งกับความในประกาศนี้

ข้อ ๖ การแจ้งข้อกล่าวหา การแจ้งกำหนดนัด การแจ้งคำสั่งลงโทษปรับทางปกครอง การแจ้งผลพิจารณาอุทธรณ์ หรือการอย่างอื่น ให้กระทำเป็นหนังสือ

ข้อ ๗ ในกรณีมีเหตุจำเป็นเร่งด่วนหรือผู้ให้บริการได้แสดงความจำนงให้แจ้งด้วยวิธีอื่น การแจ้งข้อกล่าวหา การแจ้งกำหนดนัด การแจ้งคำสั่งลงโทษปรับทางปกครอง การแจ้งผลพิจารณาอุทธรณ์ หรือการอย่างอื่น จะใช้วิธีส่งทางโทรสาร จดหมายอิเล็กทรอนิกส์ หรือวิธีอื่นตามที่ผู้ให้บริการได้แจ้งความจำนงไว้ก็ได้ แต่ต้องมีหลักฐานการส่ง และต้องจัดส่งหนังสือแจ้งให้แก่ผู้ให้บริการในทันทีที่อาจกระทำได้ ในกรณีนี้ให้ถือว่าผู้ให้บริการได้รับแจ้งตามวัน เวลาที่ปรากฏในหลักฐานการส่งโทรสาร จดหมายอิเล็กทรอนิกส์ หรือวิธีอื่นนั้น เว้นแต่จะมีการพิสูจน์ได้ว่าไม่มีการได้รับหรือได้รับก่อนหรือหลังจากนั้น

หมวด ๒
การพิจารณาและการมีคำสั่งลงโทษปรับทางปกครอง

ข้อ ๘ เมื่อพนักงานเจ้าหน้าที่รวบรวมข้อเท็จจริงและพิจารณาในเบื้องต้นแล้วเห็นว่าผู้ถูกกล่าวหาใดมีการกระทำที่มีมูลควรจะได้รับโทษปรับทางปกครอง ให้รายงานต่อคณะกรรมการเพื่อพิจารณาตามความในหมวดนี้ต่อไป

ส่วนที่ ๑
การพิจารณาทางปกครอง

ข้อ ๙ การพิจารณาทางปกครองให้รวมถึงการดำเนินการดังต่อไปนี้

(๑) การแสวงหาพยานหลักฐานที่เห็นว่าจำเป็นแก่การพิสูจน์ข้อเท็จจริง

(๒) การรับฟังพยานหลักฐาน คำชี้แจงของผู้ถูกกล่าวหา ความเห็นของพนักงานเจ้าหน้าที่คณะกรรมการ หรือพยานบุคคลหรือพยานผู้เชี่ยวชาญที่พนักงานเจ้าหน้าที่ คณะกรรมการหรือผู้ถูกกล่าวหากล่าวอ้าง

(๓) การขอข้อเท็จจริงหรือความเห็นจากพยานบุคคล หรือพยานผู้เชี่ยวชาญ

(๔) การขอให้ผู้ครอบครองเอกสารส่งเอกสารที่เกี่ยวข้อง

(๕) การออกไปตรวจสถานที่

ผู้ถูกกล่าวหาต้องให้ความร่วมมือกับพนักงานเจ้าหน้าที่และคณะกรรมการในการพิสูจน์ข้อเท็จจริงและมีหน้าที่แจ้งพยานหลักฐานที่ตนทราบแก่พนักงานเจ้าหน้าที่และคณะกรรมการ

ข้อ ๑๐ เมื่อคณะกรรมการได้รับรายงานจากพนักงานเจ้าหน้าที่แล้ว หากพิจารณาเห็นว่าผู้ถูกกล่าวหาไม่ได้กระทำผิดให้คณะกรรมการมีคำสั่งยกข้อกล่าวหา แต่ถ้าพิจารณาเห็นว่ามีมูลที่ผู้ถูกกล่าวหาควรจะได้รับโทษปรับทางปกครอง ให้คณะกรรมการแจ้งข้อกล่าวหาให้ผู้ถูกกล่าวหาทราบเพื่อโต้แย้งและแสดงพยานหลักฐานของตน

ในกรณีที่คณะกรรมการพิจารณาแล้วเห็นว่าพยานหลักฐานที่มีอยู่ไม่เพียงพอจะพิจารณาให้คณะกรรมการแจ้งให้พนักงานเจ้าหน้าที่แสวงหาพยานหลักฐานเพิ่มเติมและรายงานต่อคณะกรรมการเพื่อพิจารณาต่อไป

เมื่อได้รับแจ้งข้อกล่าวหา ผู้ถูกกล่าวหามีสิทธิยื่นคำชี้แจงแก้ข้อกล่าวหาต่อคณะกรรมการภายในระยะเวลาสิบห้าวันนับแต่วันที่ได้รับแจ้ง

สิทธิยื่นคำชี้แจงตามวรรคสามมิให้นำมาใช้บังคับในกรณีดังต่อไปนี้ เว้นแต่คณะกรรมการจะเห็นสมควรปฏิบัติเป็นอย่างอื่น

(๑) เมื่อมีความจำเป็นเร่งด่วนหากปล่อยให้เนิ่นช้าไปจะก่อให้เกิดความเสียหายอย่างร้ายแรงแก่ผู้หนึ่งผู้ใดหรือจะกระทบต่อประโยชน์สาธารณะ

(๒) เมื่อเป็นข้อเท็จจริงที่ผู้ถูกกล่าวหาเองได้ให้ไว้ในคำชี้แจงหรือในการให้ถ้อยคำต่อพนักงานเจ้าหน้าที่

(๓) เมื่อโดยสภาพเห็นได้ชัดในตัวว่าการให้โอกาสดังกล่าวไม่อาจกระทำได้

ข้อ ๑๑ ภายใต้บังคับข้อ ๗ ในการแจ้งข้อกล่าวหา ให้คณะกรรมการแจ้งคำสั่งโดยทำเป็นหนังสือโดยมีสาระสำคัญดังต่อไปนี้

(๑) ชื่อผู้ถูกกล่าวหา

(๒) การกระทำทั้งหลายที่เข้าข่ายเป็นความผิดที่มีโทษปรับทางปกครอง พร้อมทั้งข้อเท็จจริงหรือพฤติการณ์ตามสมควรเกี่ยวกับการกระทำดังกล่าว

(๓) บทบัญญัติ ระเบียบ ข้อบังคับ ประกาศ หรือข้อกำหนดตามกฎหมายว่าด้วยการควบคุมดูแลการประกอบธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ที่เห็นว่าผู้ถูกกล่าวหาฝ่าฝืนไม่ปฏิบัติหรือปฏิบัติไม่ถูกต้อง

ข้อ ๑๒ เมื่อคณะกรรมการได้แจ้งข้อกล่าวหาแล้วผู้ถูกกล่าวหาไม่ชี้แจงข้อกล่าวหาภายในกำหนดเวลาตามข้อ ๑๐ วรรคสาม หรือเป็นกรณีที่คณะกรรมการเห็นสมควรปฏิบัติตามวรรคสี่ ให้คณะกรรมการพิจารณาพยานหลักฐานประกอบกับคำชี้แจงแก้ข้อกล่าวหา (ถ้ามี) ถ้าเห็นว่าผู้ถูกกล่าวหาไม่ได้กระทำผิด ให้คณะกรรมการมีคำสั่งยกข้อกล่าวหา แต่ถ้าเห็นว่าผู้ถูกกล่าวหากระทำผิดให้พิจารณากำหนดโทษปรับทางปกครองแล้วมีคำสั่งลงโทษปรับทางปกครองต่อไป

ให้คณะกรรมการแจ้งผลการพิจารณาให้ผู้ถูกกล่าวหาทราบโดยเร็ว

ข้อ ๑๓ การประชุมของคณะกรรมการต้องมีกรรมการมาประชุมอย่างน้อยกึ่งหนึ่งจึงจะเป็นองค์ประชุม

การลงมติของที่ประชุมให้ถือเสียงข้างมาก กรรมการคนหนึ่งให้มีหนึ่งเสียงในการลงคะแนน ทั้งนี้ในกรณีที่ไม่ใช่การวินิจฉัยชี้ขาดเพื่อพิจารณากำหนดโทษปรับทางปกครอง ถ้าปรากฏว่าคะแนนเสียงเท่ากันประธานในที่ประชุมอาจออกเสียงเพิ่มขึ้นอีกเสียงหนึ่งเป็นเสียงชี้ขาด

ส่วนที่ ๒
การกำหนดลงโทษปรับทางปกครอง

ข้อ ๑๔ ในการพิจารณาโทษปรับทางปกครองที่จะใช้กับผู้ถูกกล่าวหา คณะกรรมการต้องคำนึงถึงปัจจัยดังต่อไปนี้

(๑) ความผิดเกิดขึ้นโดยความจงใจ หรือความประมาทเลินเล่ออย่างร้ายแรงหรือขาดความระมัดระวังตามสมควร

(๒) ประโยชน์ที่ผู้ถูกกล่าวหาหรือบุคคลที่เกี่ยวข้องกับการกระทำผิดหรือบุคคลอื่นได้รับหรือจะได้รับจากการกระทำนั้น

(๓) ความเสียหายที่เกิดจากการกระทำนั้น

(๔) ระดับโทษปรับทางปกครองที่เคยใช้กับผู้ถูกกล่าวหารายอื่นในความผิดทำนองเดียวกัน (ถ้ามี)

(๕) ประวัติการถูกลงโทษทางปกครองของผู้ถูกกล่าวหา หรือในกรณีที่ผู้ถูกกล่าวหาเป็นนิติบุคคล ให้หมายความรวมถึงประวัติการถูกลงโทษปรับทางปกครองของบุคลากรที่เกี่ยวข้องกับการกระทำของนิติบุคคลที่ถูกกล่าวหานั้น

(๖) ข้อเท็จจริงอื่น ๆ ที่เกี่ยวข้อง

ส่วนที่ ๓
คำสั่งลงโทษปรับทางปกครอง

ข้อ ๑๕ คำสั่งลงโทษปรับทางปกครองให้ทำเป็นหนังสือระบุ วัน เดือน ปี ที่ทำคำสั่งโทษปรับทางปกครองที่ลง รวมทั้งชื่อ ลายมือชื่อประธานกรรมการ

ข้อ ๑๖ คำสั่งลงโทษปรับทางปกครองต้องจัดให้มีเหตุผลไว้ด้วย และเหตุผลนั้นอย่างน้อยต้องประกอบด้วย

(๑) ข้อเท็จจริงอันเป็นสาระสำคัญ

(๒) ข้อกฎหมายที่อ้างอิง

(๓) ข้อพิจารณาและข้อสนับสนุนในการใช้ดุลพินิจ

ความในวรรคหนึ่งไม่ใช้บังคับกับกรณีดังต่อไปนี้

(๑) เหตุผลนั้นเป็นที่รู้กันอยู่แล้วโดยไม่จำเป็นต้องระบุอีก

(๒) เป็นกรณีที่ต้องรักษาไว้เป็นความลับ

(๓) เป็นกรณีเร่งด่วน แต่ต้องให้เหตุผลเป็นลายลักษณ์อักษรในเวลาอันควรหากผู้ถูกลงโทษร้องขอ

คำสั่งลงโทษปรับทางปกครองให้ใช้ตามแบบ ทปค. ๑ ท้ายประกาศนี้

ข้อ ๑๗ การออกคำสั่งลงโทษปรับทางปกครอง คณะกรรมการอาจมีคำสั่งให้ผู้ถูกลงโทษดำเนินการใด ๆ เพื่อแก้ไขให้ถูกต้องหรือเหมาะสมได้

ข้อ ๑๘ คำสั่งลงโทษปรับทางปกครองให้มีผลใช้ยันต่อผู้ถูกลงโทษตั้งแต่ขณะที่ผู้นั้นได้รับแจ้งเป็นต้นไป

ส่วนที่ ๔
การอุทธรณ์

ข้อ ๑๙ การอุทธรณ์คำสั่งลงโทษปรับทางปกครองของคณะกรรมการตามมาตรา ๓๓ มาตรา ๓๔ แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ ให้ผู้อุทธรณ์ยื่นต่อสำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ภายในสิบห้าวันนับแต่วันที่ได้รับแจ้งคำสั่งดังกล่าว

ในการยื่นอุทธรณ์ตามวรรคหนึ่ง ผู้อุทธรณ์อาจยื่นด้วยตนเอง หรืออาจส่งทางไปรษณีย์ลงทะเบียนก็ได้ และเพื่อประโยชน์ในการนับระยะเวลายื่นอุทธรณ์ในกรณีการยื่นโดยทางไปรษณีย์ให้ถือว่าวันที่เจ้าพนักงานไปรษณีย์ต้นทางประทับตราไปรษณียากรบนซองหนังสืออุทธรณ์เป็นวันยื่นอุทธรณ์

ข้อ ๒๐ คำอุทธรณ์ต้องทำเป็นหนังสือลงลายมือชื่อผู้อุทธรณ์ โดยระบุเรื่องอันเป็นเหตุให้ต้องอุทธรณ์เหตุผลที่เป็นข้อโต้แย้งว่าไม่เห็นด้วยกับคำสั่งลงโทษปรับทางปกครองอย่างชัดเจน และต้องมีข้อเท็จจริงหรือข้อกฎหมายที่อ้างอิงประกอบด้วย

บรรดาเอกสารต่าง ๆ ที่เกี่ยวข้องกับเรื่องที่อุทธรณ์ซึ่งผู้อุทธรณ์เห็นว่าอาจเป็นประโยชน์ต่อการพิจารณาอุทธรณ์ ให้ผู้อุทธรณ์แนบเอกสารดังกล่าวพร้อมกับคำอุทธรณ์มาด้วย

คำอุทธรณ์ที่ได้ยื่นไว้แล้ว อาจถอนเสียในเวลาใดก็ได้ก่อนที่คณะกรรมการจะมีหนังสือแจ้งผลอุทธรณ์ให้ผู้อุทธรณ์ทราบและเมื่อมีการถอนคำอุทธรณ์ ให้สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์รายงานให้คณะกรรมการทราบ

ข้อ ๒๑ การพิจารณาอุทธรณ์ คณะกรรมการจะพิจารณาอุทธรณ์ให้แล้วเสร็จภายในหกสิบวันนับแต่วันที่สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ได้รับคำอุทธรณ์

ในกรณีที่มีเหตุจำเป็นไม่อาจพิจารณาอุทธรณ์ให้แล้วเสร็จภายในกำหนดเวลาตามวรรคหนึ่ง คณะกรรมการอาจขยายระยะเวลาพิจารณาอุทธรณ์ออกไปได้ไม่เกินสามสิบวันนับแต่วันที่ครบกำหนดดังกล่าว โดยต้องมีหนังสือแจ้งให้ผู้อุทธรณ์ทราบก่อนครบกำหนดเวลาดังกล่าวด้วย

ข้อ ๒๒ ในการพิจารณาอุทธรณ์ คณะกรรมการสามารถพิจารณาทบทวนคำสั่งลงโทษปรับทางปกครองได้ทั้งปัญหาข้อเท็จจริงและข้อกฎหมาย โดยอาจขอให้ผู้อุทธรณ์หรือสำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ จัดส่งเอกสารหลักฐานเพิ่มเติมหรือชี้แจงข้อเท็จจริงอันเกี่ยวกับเรื่องที่อุทธรณ์เพิ่มเติมภายในระยะเวลาที่กำหนด หรือรับฟังความคิดเห็นจากผู้อุทธรณ์หรือบุคคลใดตามที่เห็นสมควรก็ได้

ในกรณีที่คณะกรรมการเห็นด้วยกับคำอุทธรณ์ไม่ว่าทั้งหมดหรือบางส่วน ให้ดำเนินการเปลี่ยนแปลงคำสั่งลงโทษปรับทางปกครองตามความเห็นภายในกำหนดเวลาตามข้อ ๒๑

ข้อ ๒๓ เพื่อประโยชน์ในการพิจารณาอุทธรณ์คำสั่งลงโทษปรับทางปกครอง คณะกรรมการอาจมอบหมายให้กรรมการคนหนึ่งหรือคณะบุคคลคณะหนึ่งให้มีหน้าที่สรุปข้อเท็จจริงและข้อกฎหมายพร้อมทั้งเสนอความเห็นในเรื่องอุทธรณ์ต่อคณะกรรมการ เพื่อประกอบการพิจารณาก็ได้

ข้อ ๒๔ เมื่อคณะกรรมการพิจารณาอุทธรณ์เสร็จสิ้นแล้ว ให้สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์มีหนังสือแจ้งผลคำสั่งอุทธรณ์ให้ผู้อุทธรณ์ทราบพร้อมด้วยเหตุผลรวมทั้งสิทธิในการยื่นฟ้องคดีต่อศาลปกครอง

ข้อ ๒๕ การยื่นอุทธรณ์ไม่เป็นเหตุให้ทุเลาการบังคับตามคำสั่งลงโทษปรับทางปกครอง แต่ผู้อุทธรณ์อาจยื่นคำขอทุเลาการบังคับดังกล่าวมาพร้อมกับการยื่นอุทธรณ์ก็ได้ โดยชี้แจงเหตุผลอันเป็นความจำเป็นเร่งด่วนในการขอทุเลาการบังคับดังกล่าว

ในกรณีที่คณะกรรมการพิจารณาแล้วเห็นว่าเป็นเรื่องที่มีความจำเป็นเร่งด่วน และคำขอนั้นมีเหตุสมควรอันแท้จริง จะมีคำสั่งตามที่เห็นสมควรโดยจะกำหนดเงื่อนไขใด ๆ ตามที่จำเป็นด้วยก็ได้ และให้สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์มีหนังสือแจ้งผลการพิจารณาให้ผู้อุทธรณ์ทราบ

ส่วนที่ ๕
การบังคับโทษปรับทางปกครอง

ข้อ ๒๖ เมื่อถึงกำหนดให้ชำระค่าปรับตามคำสั่งลงโทษปรับทางปกครองแล้วไม่มีการชำระโดยถูกต้องครบถ้วน ให้เจ้าหน้าที่บังคับโทษปรับทางปกครองมีหนังสือเตือนให้ผู้ถูกสั่งปรับชำระภายในเวลาที่กำหนดแต่ต้องไม่น้อยกว่าเจ็ดวัน หนังสือแจ้งเตือนให้ชำระค่าปรับทางปกครองให้ใช้ตามแบบ ทปค. ๒ ท้ายประกาศนี้

เมื่อครบกำหนดเวลาให้นำเงินมาชำระตามหนังสือแจ้งเตือนแล้ว ถ้าผู้ถูกสั่งปรับไม่ชำระหรือชำระค่าปรับไม่ครบถ้วน ให้เจ้าหน้าที่บังคับโทษปรับทางปกครองดำเนินการยึด หรืออายัดและขายทอดตลาดทรัพย์สินของผู้ถูกสั่งปรับ เพื่อนำมาชำระค่าปรับ ทั้งนี้ให้นำประมวลกฎหมายวิธีพิจารณาความแพ่งมาใช้บังคับโดยอนุโลม

หมวด ๓
การรับและจ่ายเงิน

ข้อ ๒๗ การรับเงิน การนำส่งเงิน การเก็บรักษาเงินและการเบิกจ่ายเงินจากการขายทอดตลาดทรัพย์สิน ให้ดำเนินการตามระเบียบที่กระทรวงการคลังกำหนด

ข้อ ๒๘ เงินที่ได้จากการขายทอดตลาดทรัพย์สินให้หักชำระค่าธรรมเนียม ค่าใช้จ่ายในการยึดอายัด และขายทอดตลาดทรัพย์สินก่อนนำมาชำระเป็นเงินค่าปรับที่ผู้ถูกสั่งปรับต้องชำระ กรณีที่มีเงินเหลือให้คืนเงินที่เหลือนั้นให้แก่ผู้มีสิทธิได้รับ

หมวด ๔
เบ็ดเตล็ด

ข้อ ๒๙ กรณีที่มีปัญหาเกี่ยวกับการปฏิบัติหรือไม่สามารถปฏิบัติตามประกาศนี้ หรือมีปัญหาอื่นใดที่มิได้กล่าวไว้ในประกาศนี้ ให้เสนอคณะกรรมการพิจารณาสั่งการเป็นกรณี ๆ ไป

ประกาศ ณ วันที่ ๒๘ มีนาคม พ.ศ. ๒๕๕๔
จุติ ไกรฤกษ์
รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
ประธานกรรมการธุรกรรมทางอิเล็กทรอนิกส์

แบบ ทปค. ๑

คำสั่งคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
ที่ .... / ....
เรื่อง คำสั่งลงโทษปรับทางปกครอง
.....

ด้วยปรากฏข้อเท็จจริงว่า.....มีการกระทำ..... อันเป็นความผิดตามมาตรา.....แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ ประกอบกับ มาตรา.....แห่งพระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๑ ข้อ.....แห่งประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ (เรื่อง.....) และ ประกาศธนาคารแห่งประเทศไทย (.....)

ฉะนั้น อาศัยอำนาจตามมาตรา ๓๓ มาตรา ๓๔ แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ และ ข้อ.....แห่งประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง หลักเกณฑ์การพิจารณาลงโทษปรับทางปกครองสำหรับผู้ประกอบธุรกิจให้บริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๔ คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์จึงมีคำสั่งปรับทางปกครอง .....เป็นจำนวนเงิน.....บาท (.....)
ทั้งนี้ ให้นำเงินค่าปรับไปชำระ ณ.....ภายในสามสิบวันนับแต่วันที่ได้รับแจ้งคำสั่งนี้

ในกรณีที่ผู้ถูกสั่งปรับไม่เห็นด้วยกับคำสั่งนี้ให้มีสิทธิอุทธรณ์ต่อคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ภายในสิบห้าวันนับแต่วันที่ได้รับแจ้งคำสั่ง โดยยื่นอุทธรณ์ได้ที่สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

สั่ง ณ วันที่ .. เดือน ..... พ.ศ. ....

(ลงชื่อ)
(.....)
ประธานกรรมการธุรกรรมทางอิเล็กทรอนิกส์

หมายเหตุ เพื่อความสะดวกในการชำระค่าปรับทางปกครอง ขอให้ผู้ถูกสั่งปรับนำคำสั่งฉบับนี้ไปแสดงด้วย

แบบ ทปค. ๒

ที่...../.....

สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
.....

วันที่ .....

เรื่อง แจ้งเตือนให้ชำระค่าปรับทางปกครอง

เรียน .....

อ้างถึง คำสั่งคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ที่...../..... ลงวันที่.....
เรื่อง คำสั่งลงโทษปรับทางปกครอง

ตามคำสั่งที่อ้างถึง คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ได้มีคำสั่งลงโทษปรับทางปกครองแก่ท่านซึ่งกระทำการฝ่าฝืน/ไม่ปฏิบัติตามมาตรา.....อันเป็นความผิดตามมาตรา..... แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ ประกอบกับ มาตรา.....แห่งพระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๑ ข้อ..... แห่งประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ (เรื่อง.....) และ ประกาศธนาคารแห่งประเทศไทย (.....) และสั่งให้ท่านไปชำระค่าปรับทางปกครอง เป็นเงินจำนวน .....บาท (.....) ณ .....ภายในสามสิบวันนับแต่วันที่ได้รับแจ้งคำสั่ง นั้น

บัดนี้ ได้ล่วงเลยกำหนดเวลาดังกล่าวแล้ว จึงแจ้งมาเพื่อให้ท่านนำเงินค่าปรับทางปกครองตามจำนวนดังกล่าวข้างต้นไปชำระภายในสิบห้าวันนับแต่วันที่ได้รับหนังสือนี้ หากพ้นกำหนดนี้แล้ว คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์จะดำเนินการยึด อายัดทรัพย์สินของท่าน เพื่อชำระค่าปรับทางปกครองต่อไป

จึงแจ้งมาเพื่อให้ดำเนินการให้เรียบร้อย

ขอแสดงความนับถือ

(.....)
เจ้าหน้าที่บังคับโทษปรับทางปกครอง

หน่วยงานเจ้าของเรื่อง
โทร. .....
หมายเหตุ เพื่อความสะดวกในการชำระค่าปรับทางปกครอง ขอให้ท่านนำหนังสือเตือนฉบับนี้ไปแสดงด้วย

ประกาศธนาคารแห่งประเทศไทย
ที่ สรข. ๑/๒๕๕๒
เรื่อง การให้บริการเงินอิเล็กทรอนิกส์ตามบัญชี ก ที่ไม่ต้องแจ้งให้ทราบก่อนให้บริการ

ประกาศธนาคารแห่งประเทศไทย

ที่ สรข. ๑/๒๕๕๒

เรื่อง การให้บริการเงินอิเล็กทรอนิกส์ตามบัญชี ก ที่ไม่ต้องแจ้งให้ทราบก่อนให้บริการ

---

๑. เหตุผลในการออกประกาศ

เพื่อกำหนดประเภทของการให้บริการเงินอิเล็กทรอนิกส์ ซึ่งใช้ซื้อสินค้าหรือรับบริการเฉพาะอย่างตามรายการที่กำหนดไว้ล่วงหน้า จากผู้ขายสินค้าหรือผู้ให้บริการเพียงรายเดียวที่ไม่ต้องแจ้งให้ทราบก่อนให้บริการ

๒. อำนาจตามกฎหมาย

อาศัยอำนาจตามความในบัญชีท้ายพระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๑ ธนาคารแห่งประเทศไทยโดยความเห็นชอบของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ จึงประกาศกำหนดประเภทของการให้บริการเงินอิเล็กทรอนิกส์ตามบัญชี ก ที่ไม่ต้องแจ้งให้ทราบก่อนให้บริการ

๓. ขอบเขตการบังคับใช้

ประกาศฉบับนี้ให้ใช้บังคับกับการให้บริการเงินอิเล็กทรอนิกส์ บัญชี ก ตามที่กำหนดไว้ในบัญชีท้ายพระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๑

๔. เนื้อหา

ธนาคารแห่งประเทศไทยโดยความเห็นชอบของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ประกาศกำหนดให้การให้บริการเงินอิเล็กทรอนิกส์ที่ใช้ซื้อสินค้าหรือรับบริการเฉพาะอย่างตามรายการที่กำหนดไว้ล่วงหน้า จากผู้ขายสินค้าหรือผู้ให้บริการเพียงรายเดียวที่ใช้จำกัดเพื่ออำนวยความสะดวกแก่ผู้บริโภคโดยไม่แสวงหากำไรจากการออกบัตรดังต่อไปนี้ เป็นธุรกิจบริการที่ไม่ต้องแจ้งให้ทราบก่อนให้บริการ

๔.๑ เงินอิเล็กทรอนิกส์ที่ใช้เพื่อชำระค่าสินค้าหรือบริการเฉพาะอย่างอันเป็นธุรกิจของตนเอง เช่น บัตรโดยสารรถสาธารณะ บัตรโทรศัพท์สาธารณะ บัตรชำระค่าผ่านทางสาธารณะ

๔.๒ เงินอิเล็กทรอนิกส์ที่ใช้เฉพาะชำระค่าอาหารและเครื่องดื่มภายในศูนย์อาหาร

๕. วันเริ่มต้นใช้บังคับ

ประกาศฉบับนี้ให้ใช้บังคับนับแต่วันที่ประกาศในราชกิจจานุเบกษาเป็นต้นไป

ประกาศ ณ วันที่ ๓๐ มกราคม พ.ศ. ๒๕๕๒

ธาริษา วัฒนเกส

ผู้ว่าการ

ธนาคารแห่งประเทศไทย

ประกาศธนาคารแห่งประเทศไทย
ที่ สรข. ๒/๒๕๕๒
เรื่อง หลักเกณฑ์ วิธีการ และเงื่อนไข
ว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงิน
ทางอิเล็กทรอนิกส์

ประกาศธนาคารแห่งประเทศไทย

ที่ สรข. ๒/๒๕๕๒

เรื่อง หลักเกณฑ์ วิธีการ และเงื่อนไข ว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์

---

๑. เหตุผลในการออกประกาศ

เพื่อประโยชน์ในการควบคุมดูแลการประกอบธุรกิจของผู้ให้บริการการชำระเงินทางอิเล็กทรอนิกส์ให้เกิดความมั่นคงทางการเงินและการพาณิชย์ เกิดความน่าเชื่อถือและยอมรับในระบบข้อมูลอิเล็กทรอนิกส์ และป้องกันไม่ให้เกิดความเสียหายต่อสาธารณชน

๒. อำนาจตามกฎหมาย

อาศัยอำนาจตามความในมาตรา ๔ และมาตรา ๑๗ แห่งพระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๑ ธนาคารแห่งประเทศไทย (ธปท.) จึงได้กำหนดหลักเกณฑ์ วิธีการ และเงื่อนไขในการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์

๓. ขอบเขตการบังคับใช้

ประกาศฉบับนี้ให้ใช้บังคับกับผู้ให้บริการตามพระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๑

๔. เนื้อหา

๔.๑ ในประกาศฉบับนี้

"ผู้ให้บริการ" หมายความว่า ผู้ประกอบธุรกิจให้บริการการชำระเงินทางอิเล็กทรอนิกส์ตามที่กำหนดไว้ในบัญชีท้ายพระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๑ ประกอบด้วยธุรกิจบริการที่ต้องแจ้งให้ทราบก่อนให้บริการ (บัญชี ก) ธุรกิจบริการที่ต้องขอขึ้นทะเบียนก่อนให้บริการ (บัญชี ข) และธุรกิจบริการที่ต้องได้รับอนุญาตก่อนให้บริการ (บัญชี ค)

"ธุรกิจบริการที่ต้องแจ้งให้ทราบก่อนให้บริการ" (บัญชี ก) ได้แก่ การให้บริการเงินอิเล็กทรอนิกส์ที่ใช้ซื้อสินค้าหรือรับบริการเฉพาะอย่างตามรายการที่กำหนดไว้ล่วงหน้า จากผู้ขายสินค้าหรือให้บริการเพียงรายเดียว ทั้งนี้ เว้นแต่การให้บริการเงินอิเล็กทรอนิกส์ที่ใช้จำกัดเพื่ออำนวยความสะดวกแก่ผู้บริโภคโดยมิได้แสวงหากำไรจากการออกบัตร ตามที่ธนาคารแห่งประเทศไทยประกาศกำหนดโดยความเห็นชอบของคณะกรรมการ (e-Money บัญชี ก)

"ธุรกิจบริการที่ต้องขอขึ้นทะเบียนก่อนให้บริการ" (บัญชี ข) ได้แก่

(๑) การให้บริการเครือข่ายบัตรเครดิต (Credit Card Network)

(๒) การให้บริการเครือข่ายอีดีซี (EDC Network)

(๓) การให้บริการสวิตช์ชิ่งในการชำระเงินระบบหนึ่งระบบใด (Transaction Switching บัญชี ข)

(๔) การให้บริการเงินอิเล็กทรอนิกส์ที่ใช้ซื้อสินค้า และหรือรับบริการเฉพาะอย่างตามรายการที่กำหนดไว้ล่วงหน้าจากผู้ขายสินค้าหรือให้บริการหลายราย ณ สถานที่ที่อยู่ภายใต้ระบบการจัดจำหน่ายและการให้บริการเดียวกัน (e-Money บัญชี ข)

"ธุรกิจบริการที่ต้องได้รับอนุญาตก่อนให้บริการ" (บัญชี ค) ได้แก่

(๑) การให้บริการหักบัญชี (Clearing)

(๒) การให้บริการชำระดุล (Settlement)

(๓) การให้บริการชำระเงินทางอิเล็กทรอนิกส์ผ่านอุปกรณ์อย่างหนึ่งอย่างใด หรือผ่านทางเครือข่าย

(๔) การให้บริการสวิตช์ชิ่งในการชำระเงินหลายระบบ (Transaction Switching บัญชี ค)

(๕) การให้บริการรับชำระเงินแทน

(๖) การให้บริการเงินอิเล็กทรอนิกส์ที่ใช้ซื้อสินค้า และหรือรับบริการเฉพาะอย่างตามรายการที่กำหนดไว้ล่วงหน้า จากผู้ขายสินค้าหรือให้บริการหลายราย โดยไม่จำกัดสถานที่และไม่อยู่ภายใต้ระบบการจัดจำหน่ายและการให้บริการเดียวกัน (e-Money บัญชี ค)

๔.๒ การให้บริการเงินอิเล็กทรอนิกส์ (e-Money)

๔.๒.๑ ผู้ให้บริการเงินอิเล็กทรอนิกส์บัญชี ก บัญชี ข และบัญชี ค ต้องดำรงฐานะทางการเงินและสภาพคล่อง เพื่อให้บริการได้อย่างต่อเนื่องและไม่ก่อให้เกิดความเสียหายต่อผู้ใช้บริการ

๔.๒.๒ ผู้ให้บริการเงินอิเล็กทรอนิกส์บัญชี ค ต้องกันเงินรับล่วงหน้าที่ได้รับจากผู้ใช้บริการแยกไว้ต่างหากจากเงินทุนหมุนเวียนของผู้ให้บริการ และให้ฝากไว้ที่สถาบันการเงินหรือสถาบันการเงินเฉพาะกิจ ณ เวลาใดเวลาหนึ่งไม่น้อยกว่ายอดคงค้างของเงินรับล่วงหน้า เว้นแต่ผู้ให้บริการที่เป็นสถาบันการเงินให้ถือปฏิบัติตามหลักเกณฑ์เกี่ยวกับการให้บริการเงินอิเล็กทรอนิกส์ที่ออกตามพระราชบัญญัติธุรกิจสถาบันการเงิน พ.ศ. ๒๕๕๑

๔.๓ การให้บริการชำระดุล (Settlement)

ผู้ให้บริการต้องกำหนดหลักเกณฑ์และเงื่อนไขเกี่ยวกับผลสิ้นสุดสมบูรณ์ของการโอนเงิน (Finality) ซึ่งผู้รับสามารถใช้เงินได้ทันทีโดยปราศจากเงื่อนไขและไม่สามารถเพิกถอนได้ (Irrevocable) พร้อมทั้งแจ้งให้ผู้ใช้บริการทราบ

๔.๔ การให้บริการชำระเงินทางอิเล็กทรอนิกส์ผ่านอุปกรณ์อย่างหนึ่งอย่างใดหรือผ่านทางเครือข่าย

ผู้ให้บริการต้องออกหลักฐานการชำระเงิน หลักฐานการโอนเงิน หรือหลักฐานอื่นใดที่มีข้อความทำนองเดียวกัน และจัดส่งให้ผู้ใช้บริการตามวิธีการที่ตกลงกับผู้ใช้บริการ

๔.๕ การให้บริการรับชำระเงินแทน

เมื่อได้รับชำระเงินแล้ว ผู้ให้บริการต้องออกหลักฐานเพื่อแสดงว่าได้รับชำระเงินจากผู้ใช้บริการ ในรูปของใบเสร็จรับเงิน ใบรับเงิน ใบรับฝากชำระ หรือหลักฐานอื่นใด ที่มีข้อความทำนองเดียวกันและจัดส่งให้ผู้ใช้บริการตามวิธีการที่ตกลงกับผู้ใช้บริการ โดยต้องมีรายละเอียดอย่างน้อย ดังนี้

๔.๕.๑ ชื่อผู้ให้บริการ และชื่อเจ้าหนี้

๔.๕.๒ จำนวนเงินและรายละเอียดของสินค้าหรือบริการที่ชำระ โดยอาจระบุเป็นชื่อย่อหรือรหัสก็ได้ รวมถึงรายละเอียดที่อ้างอิงถึงผู้ใช้บริการ

๔.๕.๓ วัน เดือน ปี และเวลาที่ออกหลักฐานการรับชำระเงิน

เมื่อผู้ให้บริการได้ออกหลักฐานการรับชำระเงินแล้ว ให้ถือว่าการชำระเงินของผู้ใช้บริการมีผลเสร็จสิ้นสมบูรณ์ เว้นแต่การรับชำระเงินด้วยเช็คให้ถือว่าการชำระเงินเสร็จสิ้นสมบูรณ์ เมื่อเช็คนั้นสามารถเรียกเก็บเงินได้ครบถ้วน

๔.๖ ในกรณีที่ ธปท. เห็นสมควร อาจกำหนดให้ผู้ให้บริการตามบัญชี ข และบัญชี ค ต้องจัดให้มีการตรวจสอบทางด้านความมั่นคงปลอดภัยโดยผู้ตรวจสอบอิสระตามรายชื่อที่คณะกรรมการธุรกรรมอิเล็กทรอนิกส์กำหนดด้วยก็ได้

๕. วันเริ่มต้นใช้บังคับ

ประกาศฉบับนี้ให้ใช้บังคับนับแต่วันที่ประกาศในราชกิจจานุเบกษาเป็นต้นไป

ประกาศ ณ วันที่ ๓๐ มกราคม พ.ศ. ๒๕๕๒

ธาริษา วัฒนเกส

ผู้ว่าการ

ธนาคารแห่งประเทศไทย

ประกาศธนาคารแห่งประเทศไทย
ที่ สรข. ๓/๒๕๕๒
เรื่อง นโยบายและมาตรการการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศในการประกอบธุรกิจของผู้ให้บริการการชำระเงินทางอิเล็กทรอนิกส์

ประกาศธนาคารแห่งประเทศไทย

ที่ สรข. ๓/๒๕๕๒

เรื่อง นโยบายและมาตรการการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศ ในการประกอบธุรกิจของผู้ให้บริการการชำระเงินทางอิเล็กทรอนิกส์

---

๑. เหตุผลในการออกประกาศ

เพื่อให้มีมาตรฐานในการกำหนดนโยบายและมาตรการการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศในการประกอบธุรกิจของผู้ให้บริการการชำระเงินทางอิเล็กทรอนิกส์ และใช้เป็นแนวทางกำหนดวิธีปฏิบัติในการตรวจสอบและรักษาความมั่นคงปลอดภัยของระบบสารสนเทศที่เกี่ยวข้องกับการให้บริการการชำระเงินทางอิเล็กทรอนิกส์ให้มีความน่าเชื่อถือ มีความมั่นคงปลอดภัย และสามารถให้บริการได้อย่างต่อเนื่อง

๒. อำนาจตามกฎหมาย

อาศัยอำนาจตามความในมาตรา ๔ และมาตรา ๑๐ แห่งพระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๑ ธนาคารแห่งประเทศไทย (ธปท.) จึงได้กำหนดหลักเกณฑ์ วิธีการ และเงื่อนไขในการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์

๓. ขอบเขตการบังคับใช้

ประกาศฉบับนี้ให้ใช้บังคับกับผู้ให้บริการตามพระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๑

๔. เนื้อหา

ผู้ให้บริการตามพระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๑ ต้องถือปฏิบัติตามมาตรฐานนโยบายและมาตรการการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศ ดังนี้

๔.๑ นโยบายการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศ

(๑) ผู้ให้บริการจะต้องจัดทำนโยบายการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศเป็นลายลักษณ์อักษร โดยได้รับการพิจารณาอนุมัติจากคณะกรรมการบริหารหรือผู้บริหารระดับสูงของผู้ให้บริการ ทั้งนี้ ผู้ให้บริการจะต้องเผยแพร่นโยบายดังกล่าว และอบรมให้แก่บุคลากรที่เกี่ยวข้องเพื่อถือปฏิบัติ รวมทั้งจัดให้มีการทบทวนหรือปรับปรุงนโยบายให้เหมาะสมกับสถานการณ์อย่างสม่ำเสมอ

(๒) นโยบายการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศที่เกี่ยวข้องกับการให้บริการ อย่างน้อยต้องครอบคลุมในเรื่องดังต่อไปนี้

(ก) การควบคุมการเข้าถึง และการพิสูจน์ตัวตนผู้ใช้

(ข) การรักษาความลับของข้อมูล และความถูกต้องเชื่อถือได้ของระบบสารสนเทศ

(ค) การรักษาสภาพความพร้อมใช้งานของการให้บริการ

(ง) การตรวจสอบความมั่นคงปลอดภัยทางระบบสารสนเทศ

๔.๒ มาตรการการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศ

ผู้ให้บริการจะต้องจัดให้มีมาตรการการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศที่เกี่ยวข้องกับการให้บริการการชำระเงินทางอิเล็กทรอนิกส์ให้สอดคล้องกับนโยบายที่ได้กำหนดขึ้น และมาตรการดังกล่าวจะต้องเหมาะสมกับลักษณะของธุรกิจ โดยครอบคลุมถึงการควบคุมการเข้าถึงและการพิสูจน์ตัวตนผู้ใช้ การรักษาความลับของข้อมูล การรักษาความถูกต้องเชื่อถือได้ของระบบสารสนเทศ การรักษาสภาพความพร้อมใช้งานของการให้บริการ การแก้ไขปัญหาและการรายงาน รวมถึงจัดให้มีการตรวจสอบความมั่นคงปลอดภัยทางระบบสารสนเทศอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง

ทั้งนี้ ผู้ให้บริการจะต้องดำเนินการทบทวนหรือปรับปรุงมาตรการตามระยะเวลาที่กำหนด หรือเมื่อมีการเปลี่ยนแปลงที่ส่งผลกระทบกับนโยบายและมาตรการที่ได้กำหนดไว้ ตลอดจนจัดอบรมและให้ความรู้แก่บุคลากรที่เกี่ยวข้อง

อนึ่ง ธปท. ได้จัดทำแนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศที่เกี่ยวข้องกับการให้บริการการชำระเงินทางอิเล็กทรอนิกส์ ลงวันที่ ๒๙ มกราคม ๒๕๕๒ (เอกสารแนบ) เพื่อเป็นแนวทางในการกำหนดมาตรการการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศให้น่าเชื่อถือและให้เป็นที่ยอมรับของผู้ใช้บริการ ทั้งนี้ การกำหนดมาตรการการรักษาความมั่นคงปลอดภัยของผู้ให้บริการแต่ละรายอาจแตกต่างจากแนวปฏิบัติดังกล่าวได้ หากผู้ให้บริการเห็นว่าสามารถป้องกันความเสี่ยงทางระบบสารสนเทศได้อย่างมีประสิทธิภาพเพียงพอ และอยู่ในมาตรฐานที่ยอมรับได้

๕. วันเริ่มต้นใช้บังคับ

ประกาศฉบับนี้ให้ใช้บังคับนับแต่วันที่ประกาศในราชกิจจานุเบกษาเป็นต้นไป

ประกาศ ณ วันที่ ๓๐ มกราคม พ.ศ. ๒๕๕๒

ธาริษา วัฒนเกส

ผู้ว่าการ

ธนาคารแห่งประเทศไทย

แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศ
ที่เกี่ยวข้องกับการให้บริการการชำระเงินทางอิเล็กทรอนิกส์

เพื่อสนับสนุนให้การประกอบธุรกิจของผู้ให้บริการการชำระเงินทางอิเล็กทรอนิกส์เป็นไปอย่างมีประสิทธิภาพ ปลอดภัย ถูกต้อง และน่าเชื่อถือ ธนาคารแห่งประเทศไทยได้จัดทำแนวปฏิบัติเพื่อเป็นแนวทางในการกำหนดมาตรการการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศที่เกี่ยวข้องกับการให้บริการการชำระเงินทางอิเล็กทรอนิกส์ แนวปฏิบัตินี้เป็นเพียงกรอบแนวทางทั่วไป ผู้ให้บริการอาจกำหนดมาตรการการรักษาความมั่นคงปลอดภัยที่แตกต่างจากแนวปฏิบัติฉบับนี้ได้ หากสามารถป้องกันความเสี่ยงทางระบบสารสนเทศได้อย่างมีประสิทธิภาพเพียงพอ และอยู่ในมาตรฐานที่ยอมรับได้ นอกจากนี้ ผู้ให้บริการต้องพิจารณาปรับใช้และกำหนดรายละเอียดของมาตรการการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศของผู้ให้บริการให้เหมาะสมกับประเภทและความซับซ้อนของธุรกิจตนเองด้วย

สาระสำคัญของแนวปฏิบัติฉบับนี้ประกอบด้วย

1. <u>การควบคุมการเข้าถึง และการพิสูจน์ตัวตนผู้ใช้</u>

ผู้ให้บริการต้องคำนึงถึงการกำหนดบุคลากรหรือหน่วยงานทางเทคโนโลยีสารสนเทศและการแบ่งแยกหน้าที่ให้เหมาะสม การควบคุมการเข้าถึงระบบสารสนเทศ การพิสูจน์ตัวตนผู้ใช้ และการป้องกันการปฏิเสธการรับผิด ดังนี้

1.1 การกำหนดบุคลากรหรือหน่วยงานทางระบบสารสนเทศ และการแบ่งแยกอำนาจหน้าที่ที่เหมาะสมในการบริหารจัดการทางระบบสารสนเทศของผู้ให้บริการ

ผู้ให้บริการต้องกำหนดหน้าที่และความรับผิดชอบของบุคลากรหรือหน่วยงานที่ดูแลเกี่ยวกับความมั่นคงปลอดภัยทางระบบสารสนเทศของผู้ให้บริการ โดยสร้างความตระหนัก ให้ความรู้ และให้มีการอบรม ตลอดจนจัดให้มีกระบวนการทางวินัยเพื่อลงโทษในกรณีฝ่าฝืนหรือละเมิดระเบียบปฏิบัติเกี่ยวกับความมั่นคงปลอดภัย

<u>แนวปฏิบัติ</u>

(1) กำหนดหน้าที่ความรับผิดชอบ และแบ่งแยกหน้าที่ในการปฏิบัติงานด้านต่าง ๆ ที่เกี่ยวกับความมั่นคงปลอดภัยทางระบบสารสนเทศของผู้ให้บริการออกจากกันให้ชัดเจน ให้มีการถ่วงดุลอำนาจ เพื่อป้องกันความเสี่ยงในการปฏิบัติการที่อาจเกิดขึ้น

(2) มีการอบรม เพิ่มเติมความรู้แก่บุคลากรเก่า และใหม่อย่างสม่ำเสมอ

(3) จัดให้มีกระบวนการทางวินัย เพื่อลงโทษบุคลากรที่ฝ่าฝืน ละเมิดนโยบายหรือระเบียบปฏิบัติเกี่ยวกับความมั่นคงปลอดภัยทางระบบสารสนเทศของผู้ให้บริการ

1.2 การควบคุมการเข้าถึงระบบสารสนเทศ

ผู้ให้บริการต้องจัดให้มีขั้นตอนปฏิบัติเป็นลายลักษณ์อักษรสำหรับการควบคุมและจำกัดสิทธิการใช้ระบบสารสนเทศที่เกี่ยวกับการให้บริการและข้อมูลตามความจำเป็นในการใช้งาน ป้องกันการลักลอบการเข้าถึงระบบโดยผู้ที่ไม่มีสิทธิ ทั้งจากภายในและภายนอกองค์กร

<u>แนวปฏิบัติ</u>

(1) จัดทำทะเบียนทรัพย์สิน หรืออุปกรณ์ระบบสารสนเทศให้ถูกต้องอยู่เสมอ รวมถึงจัดให้มีผู้รับผิดชอบดูแลทรัพย์สินเหล่านั้น

(2) มีกฎ ระเบียบ ในการใช้ระบบสารสนเทศ และทรัพย์สินที่เกี่ยวข้องกับระบบสารสนเทศที่เหมาะสม

(3) ต้องมีการควบคุม และป้องกันการเข้าถึงสถานที่ตั้ง การควบคุมการเข้าถึงอุปกรณ์ และระบบสารสนเทศที่เกี่ยวกับการให้บริการ โดยกระบวนการดังกล่าวครอบคลุมถึง

(3.1) การจัดวาง ติดตั้งอุปกรณ์ที่เกี่ยวกับการให้บริการที่เป็นสัดส่วน แบ่งเขตควบคุมอุปกรณ์สำคัญ จัดให้มีการควบคุมการเข้าออกบริเวณพื้นที่ควบคุม ป้องกันการลักลอบเข้าถึงโดยผู้ไม่มีสิทธิ ทั้งภายในและภายนอกองค์กร

(3.2) กำหนดวิธีการและสิทธิการเข้าถึงระบบสารสนเทศที่เกี่ยวกับการให้บริการ โดยแบ่งแยกตามระดับอำนาจหน้าที่ และจัดให้มีการตรวจสอบสิทธิในการเข้าถึงระบบสารสนเทศดังกล่าว ทั้งจากผู้ใช้บริการ และบุคลากรที่เกี่ยวข้องก่อนอนุญาตให้เข้าใช้ระบบ โดยต้องทบทวนและปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

(3.3) กำหนดให้มีการบันทึกการเข้าใช้ระบบสารสนเทศของผู้ใช้บริการและบุคลากรที่เกี่ยวข้อง เพื่อใช้ประโยชน์ในการตรวจสอบติดตามความผิดปกติต่าง ๆ ที่อาจเกิดขึ้น

1.3 การตรวจสอบตัวตน และการป้องกันการปฏิเสธการรับผิด

ผู้ให้บริการต้องจัดให้มีการระบุ ตรวจสอบ หรือพิสูจน์ตัวตนและตรวจสอบสิทธิของผู้ใช้ระบบโดยพิจารณาใช้เทคโนโลยีที่เหมาะสมกับระดับความเสี่ยงของประเภทธุรกิจที่ให้บริการ เช่น การใช้รหัสผ่าน (Password) เลขประจำตัว (Personal Identification Number) อุปกรณ์หรือบัตรที่เก็บข้อมูลส่วนบุคคล (Token or Smart Card) ลักษณะทางชีวมาตร (Biometric) เทคโนโลยีกุญแจสาธารณะ (Public Key Infrastructure) เพื่อป้องกันการปฏิเสธการรับผิดกรณีมีข้อพิพาทเกิดขึ้น

แนวปฏิบัติ

(1) จัดให้มีวิธีการระบุ หรือตรวจสอบ หรือพิสูจน์ตัวตนก่อนเข้าใช้ระบบสารสนเทศของผู้ใช้บริการและบุคลากรที่เกี่ยวข้องของผู้ให้บริการ เพื่อให้ทราบได้ว่าการเข้าใช้งานนั้นมาจากผู้มีสิทธิในการเข้าถึงระบบสารสนเทศ รวมทั้งป้องกันไม่ให้มีการปฏิเสธความรับผิดหรือข้อโต้แย้งในการทำรายการ

(2) มีการบันทึกรายละเอียดการเข้าถึงระบบสารสนเทศไว้เป็นหลักฐานสำหรับการตรวจสอบกรณีเกิดปัญหา เพื่อป้องกันการปฏิเสธการรับผิด

2. <u>การรักษาความลับของข้อมูล และความถูกต้องเชื่อถือได้ของระบบสารสนเทศ</u>

ผู้ให้บริการต้องกำหนดมาตรการในการรักษาความลับของข้อมูล และการรักษาความถูกต้องเชื่อถือได้ของระบบสารสนเทศที่ให้บริการ เช่น การควบคุมการเปลี่ยนแปลง การปรับปรุงแก้ไขระบบ หรืออุปกรณ์ประมวลผลสารสนเทศ และการจัดการระบบเครือข่ายที่เกี่ยวกับการให้บริการเพื่อให้ระบบสารสนเทศมีความถูกต้องอยู่เสมอ

2.1 การรักษาความลับของข้อมูล

ผู้ให้บริการต้องกำหนดขั้นตอน วิธีการในการรับส่ง ประมวลผล และการจัดเก็บข้อมูลอย่างเหมาะสม เพื่อรักษาความลับ ความถูกต้องสมบูรณ์ของข้อมูล

แนวปฏิบัติ

(1) กำหนดชั้นความลับของข้อมูลตามระดับความสำคัญ รวมถึงกำหนดสิทธิผู้ที่สามารถเข้าถึงข้อมูลความลับดังกล่าว

(2) การจัดให้มีวิธีการรับส่ง ประมวลผล และจัดเก็บข้อมูลลับในลักษณะที่มั่นคงปลอดภัยตามระดับความสำคัญ เพื่อป้องกันการเข้าแก้ไขเปลี่ยนแปลงโดยผู้ที่ไม่มีสิทธิ หรือไม่ได้รับอนุญาต

(3) กำหนดวิธีปฏิบัติในการจัดเก็บ ใช้งาน และทำลายข้อมูลแต่ละประเภทชั้นความลับ

2.2 การควบคุมการเปลี่ยนแปลง การปรับปรุงแก้ไขระบบสารสนเทศหรืออุปกรณ์ประมวลผลสารสนเทศ

ผู้ให้บริการต้องกำหนดขั้นตอนปฏิบัติอย่างเป็นระบบสำหรับควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบสารสนเทศ เพื่อลดความเสี่ยงที่จะทำให้ระบบที่ให้บริการเกิดความเสียหายหรือทำงานผิดปกติ

แนวปฏิบัติ

(1) จัดให้มีขั้นตอนปฏิบัติสำหรับการควบคุมการแก้ไขเปลี่ยนแปลงข้อมูลในกระบวนการประมวลผล การรับส่งข้อมูล การจัดเก็บ การจัดหา การปรับปรุงอุปกรณ์ และการพัฒนาระบบสารสนเทศ เช่น มีขั้นตอนการประเมินผลกระทบที่เกี่ยวข้อง การอนุมัติจากผู้มีอำนาจ ขั้นตอนการพัฒนา หรือปรับปรุงแก้ไข การทดสอบก่อนดำเนินการ รวมถึงการบันทึกการแก้ไขเปลี่ยนแปลง การแจ้งให้ผู้ที่ได้รับผลกระทบจากการเปลี่ยนแปลงนั้นได้รับทราบ และปรับปรุงเอกสารที่เกี่ยวข้อง

(2) ต้องแยกระบบสำหรับการพัฒนา และระบบที่ใช้งานจริงออกจากกัน ซึ่งอาจเป็นการแยกอุปกรณ์เป็นคนละเครื่อง และใช้ผู้ควบคุมระบบแยกกัน

(3) การใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น

(3.1) จัดให้มีสัญญาดำเนินการเป็นลายลักษณ์อักษร ระบุขอบเขตการดำเนินงาน หน้าที่ความรับผิดชอบของคู่สัญญาแต่ละฝ่ายให้ชัดเจน

(3.2) จัดให้มีการบริหารความเสี่ยงในการใช้บริการจากผู้ให้บริการรายอื่น รวมทั้งการคัดเลือก การติดตาม ประเมิน และตรวจสอบการให้บริการอย่างเหมาะสม

(3.3) จัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูล ซึ่งรวมถึงการรักษาความลับและความเป็นส่วนตัวของข้อมูลผู้ใช้บริการ

(3.4) ความรับผิดชอบต่อผู้ใช้บริการในการให้บริการที่ต่อเนื่อง มั่นคงปลอดภัย และน่าเชื่อถือเสมือนกับการให้บริการโดยผู้ให้บริการเอง

(3.5) การจัดทำแผนฉุกเฉินสำหรับการดำเนินการด้านงานเทคโนโลยีสารสนเทศของผู้ให้บริการรายอื่นหรือบุคคลอื่นให้สอดคล้องกับแผนฉุกเฉินของผู้ให้บริการ

(4) จัดทำคู่มือต่าง ๆ ที่เกี่ยวข้องกับระบบสารสนเทศที่ให้บริการ อบรมและเผยแพร่ให้พนักงานไว้ใช้งาน

2.3 การจัดการเครือข่ายที่เกี่ยวกับการให้บริการ

ผู้ให้บริการต้องกำหนดมาตรการป้องกันการเข้าถึงระบบที่ให้บริการทางเครือข่ายโดยไม่ได้รับอนุญาต

แนวปฏิบัติ

(1) บริหารจัดการเครือข่ายที่เกี่ยวกับการให้บริการ เพื่อป้องกันภัยคุกคามทางเครือข่าย หรือข้อมูลที่ส่งผ่านทางเครือข่าย เช่น

(1.1) ต้องกำหนดมาตรการควบคุมการเชื่อมต่อทางเครือข่าย การอนุญาตการเชื่อมต่อโดยอุปกรณ์จากภายนอก

(1.2) การตรวจสอบตัวตนในการใช้งานเครือข่าย

(1.3) การแบ่งแยกเครือข่ายตามกลุ่มบริการสารสนเทศ

(1.4) ติดตั้งโปรแกรมป้องกันภัยคุกคามจากภายนอก

(2) มีมาตรการควบคุมและป้องกันไวรัสที่มีประสิทธิภาพและปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

3. <u>การรักษาสภาพความพร้อมใช้งานของการให้บริการ</u>

ผู้ให้บริการต้องจัดให้มีการให้บริการที่มีประสิทธิภาพและมีสภาพความพร้อมใช้งานในการให้บริการตลอดเวลา สามารถรองรับการทำธุรกรรมตามความต้องการของผู้ใช้บริการได้อย่างพอเพียง ตอบสนองการทำธุรกรรมได้อย่างรวดเร็วทั้งในเวลาปกติและเวลาที่มีการใช้บริการอย่างหนาแน่น (Peak Time) รวมทั้งมีการสำรองข้อมูลอย่างเหมาะสม เพื่อให้สามารถกู้ระบบให้กลับมาทำงานได้ตามปกติในกรณีที่เกิดความเสียหาย

3.1 การประเมิน และจัดการความเสี่ยงของระบบที่ให้บริการ

ผู้ให้บริการต้องมีวิธีการประเมินความเสี่ยงของระบบที่ให้บริการที่เหมาะสม กำหนดเกณฑ์ในการยอมรับความเสี่ยงและระบุระดับความเสี่ยงที่ยอมรับได้ รวมถึงกำหนดวิธีการจัดการความเสี่ยงที่อาจเกิดขึ้น ทั้งนี้ ผู้ให้บริการต้องจัดให้มีการทบทวนความเสี่ยงอยู่เสมอให้สอดคล้องกับพัฒนาการทางเทคโนโลยีและสถานการณ์ปัจจุบัน

<u>แนวปฏิบัติ</u>

(1) กำหนดวิธีการประเมินความเสี่ยงที่เป็นรูปธรรม

(2) วิเคราะห์และประเมินผลกระทบที่มีต่อธุรกิจที่อาจเป็นผลจากความล้มเหลวของการรักษาความมั่นคงปลอดภัย

(3) กำหนดเกณฑ์ในการยอมรับความเสี่ยง และระดับความเสี่ยงที่ยอมรับได้

(4) ระบุและประเมินทางเลือกในการจัดการกับความเสี่ยงในการดำเนินการที่อาจเกิดขึ้นได้ เพื่อหลีกเลี่ยงความเสี่ยงและลดความเสียหายที่จะเกิดขึ้น

3.2 การติดตามตรวจสอบความผิดปกติและความล่อแหลมของระบบสารสนเทศ

ผู้ให้บริการต้องกำหนดให้มีการติดตาม ตรวจสอบความผิดปกติ ตลอดจนข้อมูลข่าวสารที่เกี่ยวกับช่องโหว่ในระบบต่าง ๆ ที่ให้บริการ เพื่อประเมินความเสี่ยงและกำหนดมาตรการรองรับเพื่อลดความเสี่ยงดังกล่าว

แนวปฏิบัติ

(1) ติดตามตรวจสอบรายการที่ไม่ปกติ และโอกาสที่จะเกิดภัยคุกคาม หรือการลักลอบเข้าถึงระบบสารสนเทศ

(2) ประเมินช่องโหว่ของระบบ (Vulnerability Assessment) จัดเตรียมแนวทางการแก้ไข หรือปิดช่องโหว่จากความล่อแหลมของระบบ โดยเฉพาะในส่วนของระบบเครือข่ายที่เกี่ยวกับการให้บริการ รวมถึงโปรแกรมระบบงานและฐานข้อมูล

(3) กรณีระบบมีความเสี่ยงสูง ควรจัดให้มีการทดสอบเจาะระบบ (Penetration Test) เพื่อทดสอบประสิทธิภาพของเทคโนโลยีการรักษาความมั่นคงปลอดภัย

3.3 การแก้ไขปัญหา บันทึกเหตุการณ์ และการรายงาน กรณีระบบสารสนเทศได้รับความเสียหาย

ผู้ให้บริการต้องมีการติดตาม บันทึก และรายงานเหตุการณ์ละเมิดความมั่นคงปลอดภัย ผ่านช่องทางการรายงานที่กำหนดไว้ โดยดำเนินการอย่างรวดเร็วที่สุดเท่าที่จะทำได้ รวมทั้งให้มีการเรียนรู้จากเหตุการณ์ที่เกิดขึ้นแล้ว เพื่อเตรียมการป้องกันที่จำเป็นไว้ล่วงหน้า

แนวปฏิบัติ

(1) กำหนดขั้นตอนการแก้ไขปัญหา ทีมงานหรือผู้รับผิดชอบ รวมถึงวิธีการรายงานปัญหาให้กับผู้บริหาร และแจ้งให้กับผู้เกี่ยวข้องทราบ

(2) เก็บรวบรวมหลักฐานต่าง ๆ ที่เป็นประโยชน์

(3) บันทึกเหตุการณ์ หรือจัดทำรายงานที่เป็นลายลักษณ์อักษรเพื่อเก็บไว้เป็นแนวทางในการแก้ปัญหา

3.4 การสำรองข้อมูล

ผู้ให้บริการต้องจัดให้มีการสำรองและทดสอบข้อมูลที่สำรองเก็บไว้อย่างสม่ำเสมอ เพื่อรักษาความถูกต้องสมบูรณ์ และสภาพความพร้อมใช้งานของการให้บริการ

แนวปฏิบัติ

(1) สำรองข้อมูลที่สำคัญ และข้อมูลอื่นที่จำเป็นต่อการปฏิบัติงาน สำรองให้พร้อมใช้งานได้

(2) กำหนดวิธีปฏิบัติ หรือขั้นตอนในการสำรองข้อมูลให้ชัดเจน เช่น ข้อมูลที่จะสำรอง ความถี่ในการสำรองข้อมูล สื่อที่ใช้ สถานที่เก็บ วิธีการเก็บรักษา และการนำมาใช้งาน

(3) ทดสอบข้อมูลที่เก็บสำรองไว้อย่างสม่ำเสมอ และให้เป็นไปตามนโยบายการสำรองข้อมูลของผู้ให้บริการ

3.5 การจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง หรือแผนฉุกเฉินทางระบบสารสนเทศ

ผู้ให้บริการต้องจัดทำแผนสร้างความต่อเนื่องให้กับการให้บริการการชำระเงินทางอิเล็กทรอนิกส์ และนำแผนมาดำเนินการเพื่อให้บริการสามารถดำเนินต่อไปได้ตามระยะเวลาที่กำหนดไว้หลังจากที่มีเหตุการณ์ที่ทำให้บริการหยุดชะงัก

แนวปฏิบัติ

(1) วิเคราะห์และระบุความเสี่ยง และการดำเนินงานที่สำคัญของการให้บริการ

(2) กำหนดระยะเวลาหยุดดำเนินงานที่ยอมรับได้ (Recovery Time Objectives)

(3) จัดทำแผนเป็นลายลักษณ์อักษร กำหนดขั้นตอนรายละเอียดการดำเนินการเมื่อมีการหยุดชะงักของการดำเนินงานที่สำคัญ เพื่อให้สามารถกลับมาดำเนินงานได้ตามระยะเวลาที่กำหนด รายละเอียดของแผนอย่างน้อยประกอบด้วย

ก. ชื่อแผน

ข. วัตถุประสงค์ และขอบเขตของแผน

ค. รายละเอียดของระบบเทคโนโลยีสารสนเทศ ทรัพยากรที่จำเป็นสำหรับปฏิบัติงานทดแทน

ง. ผู้รับผิดชอบ ผู้มีอำนาจตัดสินใจ การติดต่อสื่อสารกับผู้เกี่ยวข้องทั้งภายในและภายนอก

จ. วิธีการปฏิบัติกรณีเกิดปัญหา และสถานที่ปฏิบัติงานทดแทน

(4) จัดให้มีการฝึกอบรมแผนแก่พนักงานและผู้มีส่วนเกี่ยวข้องกับการดำเนินการตามแผนอย่างสม่ำเสมอ

(5) ทดสอบและทบทวนแผนสำหรับการดำเนินงานที่สำคัญอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงปัจจัยที่มีผลต่อความเสี่ยง

3.6 การบำรุงรักษาอุปกรณ์ระบบสารสนเทศ

ผู้ให้บริการต้องกำหนดให้มีการบำรุงรักษาอุปกรณ์ต่าง ๆ อย่างสม่ำเสมอ เพื่อให้อุปกรณ์ทำงานได้อย่างต่อเนื่อง และอยู่ในสภาพที่มีความสมบูรณ์ต่อการใช้งาน

แนวปฏิบัติ

กำหนดให้มีการบำรุงรักษาอุปกรณ์ต่าง ๆ อย่างสม่ำเสมอ เพื่อให้อุปกรณ์ทำงานได้อย่างต่อเนื่อง และให้อยู่ในสภาพพร้อมใช้งานตลอดเวลา

4. <u>การตรวจสอบความมั่นคงปลอดภัยทางระบบสารสนเทศ</u>

ผู้ให้บริการจะต้องจัดให้มีการตรวจสอบความมั่นคงปลอดภัยทางระบบสารสนเทศอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่านโยบายและมาตรการการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศที่เกี่ยวข้องกับการให้บริการเป็นไปอย่างมีประสิทธิภาพ มั่นคงปลอดภัยสามารถให้บริการได้อย่างต่อเนื่อง

<u>แนวปฏิบัติ</u>

(1) จัดให้มีผู้ตรวจสอบและดำเนินการตรวจสอบความมั่นคงปลอดภัยทางระบบสารสนเทศในเรื่องที่มีความเสี่ยงหรือมีความสำคัญต่อการให้บริการอย่างน้อยปีละ 1 ครั้ง และจัดทำรายงานผลการตรวจสอบเสนอผู้บริหารของผู้ให้บริการเพื่อพิจารณาระดับความเสี่ยงที่เป็นอยู่และกำหนดแนวทางการปรับปรุง และแจ้งให้หน่วยงานภายในที่เกี่ยวข้องทราบเพื่อนำไปปฏิบัติ

(2) ติดตาม ตรวจสอบการให้บริการการชำระเงินทางอิเล็กทรอนิกส์ให้เป็นไปตามกฎระเบียบ ข้อบังคับที่เกี่ยวข้องทั้งหมด เพื่อหลีกเลี่ยงการละเมิดข้อกำหนดทางกฎหมาย ระเบียบปฏิบัติ ข้อกำหนดในสัญญา และข้อกำหนดด้านความมั่นคงปลอดภัย

ฝ่ายระบบการชำระเงิน
ธนาคารแห่งประเทศไทย
29 มกราคม 2552

ประกาศธนาคารแห่งประเทศไทย
ที่ สรข. ๔/๒๕๕๒
เรื่อง การแต่งตั้งพนักงานเจ้าหน้าที่
ตามพระราชกฤษฎีกาว่าด้วยการควบคุมดูแล
ธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์
พ.ศ. ๒๕๕๑

ประกาศธนาคารแห่งประเทศไทย

ที่ สรข. ๔/๒๕๕๒

เรื่อง การแต่งตั้งพนักงานเจ้าหน้าที่ตามพระราชกฤษฎีกา
ว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๑

---

๑. เหตุผลในการออกประกาศ

เพื่อแต่งตั้งพนักงานธนาคารแห่งประเทศไทยเป็นพนักงานเจ้าหน้าที่เพื่อปฏิบัติการตามพระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๑

๒. อำนาจตามกฎหมาย

อาศัยอำนาจตามมาตรา ๓ และมาตรา ๒๐ แห่งพระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๑

๓. เนื้อหา

ธนาคารแห่งประเทศไทยแต่งตั้งพนักงานของธนาคารแห่งประเทศไทยต่อไปนี้ เป็นพนักงานเจ้าหน้าที่ ตามความในพระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๑

๑. นายฉิม ตันติยาสวัสดิกุล
๒. นางสาวจริญญา แก้วมณี
๓. นายรณศักดิ์ เรืองวีรยุทธ
๔. นางสาวกุฎา รณะนันทน์
๕. นางอัจฉรา ทรัพย์เมลือง
๖. นายรณรงค์ ขุนภายี
๗. นางสิริเนตร แสนสุดสวาสดิ์
๘. นางวลัย วัชโรบล
๙. นางเสาวลักษณ์ ตรีพจนีย์
๑๐. นางณัฐกา ดวงทิพย์
๑๑. นายอุดม โหสกุล

๑๒. นางสุทธินี ศิลา

๑๓. นางอรชุมา ประชาศรัยสรเดช

๑๔. นางสาวจิตรา นุชประเสริฐ

๑๕. นายสุทธิศักดิ์ ถาวรสุข

๑๖. นางสุชนนี จิตตานนท์

๔. วันเริ่มต้นบังคับใช้

ประกาศฉบับนี้ให้ใช้บังคับนับแต่วันที่ประกาศในราชกิจจานุเบกษาเป็นต้นไป

ประกาศ ณ วันที่ ๓๐ มกราคม พ.ศ. ๒๕๕๒

ธาริษา วัฒนเกส

ผู้ว่าการ

ธนาคารแห่งประเทศไทย

พระราชกฤษฎีกา
ว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรม
ทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓

พระราชกฤษฎีกา

ว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์

พ.ศ. ๒๕๕๓

ภูมิพลอดุลยเดช ป.ร.

ให้ไว้ ณ วันที่ ๒๓ สิงหาคม พ.ศ. ๒๕๕๓

เป็นปีที่ ๖๕ ในรัชกาลปัจจุบัน

พระบาทสมเด็จพระปรมินทรมหาภูมิพลอดุลยเดช มีพระบรมราชโองการโปรดเกล้า ฯ ให้ประกาศว่า

โดยที่เป็นการสมควรกำหนดวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์

อาศัยอำนาจตามความในมาตรา ๑๘๗ ของรัฐธรรมนูญแห่งราชอาณาจักรไทย และมาตรา ๒๕ แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ อันเป็นกฎหมายที่มีบทบัญญัติบางประการเกี่ยวกับการจำกัดสิทธิและเสรีภาพของบุคคล ซึ่งมาตรา ๒๘ ประกอบกับมาตรา ๔๓ ของรัฐธรรมนูญแห่งราชอาณาจักรไทย บัญญัติให้กระทำได้โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมาย จึงทรงพระกรุณาโปรดเกล้า ฯ ให้ตราพระราชกฤษฎีกาขึ้นไว้ ดังต่อไปนี้

มาตรา ๑ พระราชกฤษฎีกานี้เรียกว่า “พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓”

มาตรา ๒ พระราชกฤษฎีกานี้ให้ใช้บังคับเมื่อพ้นกำหนดหนึ่งร้อยแปดสิบวันนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

มาตรา ๓ ในพระราชกฤษฎีกานี้

“วิธีการแบบปลอดภัย” หมายความว่า วิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์

“ทรัพย์สินสารสนเทศ” หมายความว่า

(๑) ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

(๒) ตัวเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล และอุปกรณ์อื่นใด

(๓) ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์

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

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

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

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

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

"การรักษาสภาพพร้อมใช้งาน" (availability) หมายความว่า การจัดทำให้ทรัพย์สินสารสนเทศสามารถทำงาน เข้าถึง หรือใช้งานได้ในเวลาที่ต้องการ

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

มาตรา ๔ วิธีการแบบปลอดภัยมีสามระดับ ดังต่อไปนี้

(๑) ระดับเคร่งครัด

(๒) ระดับกลาง

(๓) ระดับพื้นฐาน

มาตรา ๕ วิธีการแบบปลอดภัยตามมาตรา ๔ ให้ใช้สำหรับการทำธุรกรรมทางอิเล็กทรอนิกส์ดังต่อไปนี้

(๑) ธุรกรรมทางอิเล็กทรอนิกส์ซึ่งมีผลกระทบต่อความมั่นคงหรือความสงบเรียบร้อยของประเทศ หรือต่อสาธารณชน

(๒) ธุรกรรมทางอิเล็กทรอนิกส์ของหน่วยงานหรือองค์กร หรือส่วนงานของหน่วยงานหรือองค์กรที่ถือเป็นโครงสร้างพื้นฐานสำคัญของประเทศ

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

ให้คณะกรรมการประกาศกำหนดรายชื่อหรือประเภทของหน่วยงานหรือองค์กร หรือส่วนงานของหน่วยงานหรือองค์กรที่ถือเป็นโครงสร้างพื้นฐานสำคัญของประเทศตามมาตรา ๕ (๒) ซึ่งต้องกระทำตามวิธีการแบบปลอดภัยในระดับเคร่งครัด ระดับกลาง หรือระดับพื้นฐาน แล้วแต่กรณี

มาตรา ๗ วิธีการแบบปลอดภัยตามมาตรา ๔ ในแต่ละระดับ ให้มีมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามหลักเกณฑ์ที่คณะกรรมการประกาศกำหนด

โดยมาตรฐานดังกล่าวสำหรับวิธีการแบบปลอดภัยในแต่ละระดับนั้น อาจมีการกำหนดหลักเกณฑ์ที่แตกต่างกันตามความจำเป็น แต่อย่างน้อยต้องมีการกำหนดเกี่ยวกับหลักเกณฑ์ ดังต่อไปนี้

(๑) การสร้างความมั่นคงปลอดภัยด้านบริหารจัดการ

(๒) การจัดโครงสร้างด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ในส่วนการบริหารจัดการด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ทั้งภายในและภายนอกหน่วยงานหรือองค์กร

(๓) การบริหารจัดการทรัพย์สินสารสนเทศ

(๔) การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร

(๕) การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม

(๖) การบริหารจัดการด้านการสื่อสารและการดำเนินงานของระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

(๗) การควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์

(๘) การจัดหาหรือจัดให้มี การพัฒนา และการบำรุงรักษาระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

(๙) การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด

(๑๐) การบริหารจัดการด้านการบริการหรือการดำเนินงานของหน่วยงานหรือองค์กรเพื่อให้มีความต่อเนื่อง

(๑๑) การตรวจสอบและการประเมินผลการปฏิบัติตามนโยบาย มาตรการ หลักเกณฑ์ หรือกระบวนการใด ๆ รวมทั้งข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

มาตรา ๘ เพื่อประโยชน์ในการเป็นแนวทางสำหรับการจัดทำนโยบายหรือแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของหน่วยงานหรือองค์กร คณะกรรมการอาจระบุหรือแสดงตัวอย่างมาตรฐานทางเทคโนโลยีซึ่งเป็นที่ยอมรับเป็นการทั่วไปว่าเป็นมาตรฐานทางเทคโนโลยีที่เชื่อถือได้ไว้ในประกาศตามมาตรา ๗ ด้วยก็ได้

มาตรา ๙ ธุรกรรมทางอิเล็กทรอนิกส์ใดได้กระทำโดยวิธีการที่มีการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศในระดับที่เทียบเท่าหรือไม่ต่ำกว่ามาตรฐานความมั่นคงปลอดภัยของระบบสารสนเทศตามประกาศตามมาตรา ๗ ซึ่งได้กำหนดไว้สำหรับระดับของวิธีการแบบปลอดภัยในการทำ

ธุรกรรมทางอิเล็กทรอนิกส์นั้น ให้ถือว่าธุรกรรมทางอิเล็กทรอนิกส์ดังกล่าวได้กระทำตามวิธีการที่เชื่อถือได้ตามมาตรา ๒๕ แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔

มาตรา ๑๐ ในการทำธุรกรรมทางอิเล็กทรอนิกส์ตามวิธีการแบบปลอดภัยตามพระราชกฤษฎีกานี้ ผู้กระทำต้องคำนึงถึงหลักการพื้นฐานของการรักษาความลับ การรักษาความครบถ้วน และการรักษาสภาพพร้อมใช้งาน รวมทั้งต้องปฏิบัติตามนโยบายและแนวปฏิบัติในการควบคุมการปฏิบัติงานและการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของหน่วยงานหรือองค์กรนั้นด้วย

มาตรา ๑๑ ในกรณีที่คณะกรรมการเห็นว่าหน่วยงานหรือองค์กรใด หรือส่วนงานหนึ่งส่วนงานใดของหน่วยงานหรือองค์กรใด มีการจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศโดยสอดคล้องกับวิธีการแบบปลอดภัยตามพระราชกฤษฎีกานี้ คณะกรรมการอาจประกาศเผยแพร่รายชื่อหน่วยงานหรือองค์กร หรือส่วนงานของหน่วยงานหรือองค์กรนั้นเพื่อให้สาธารณชนทราบเป็นการทั่วไปก็ได้

มาตรา ๑๒ ให้คณะกรรมการพิจารณาทบทวนหลักเกณฑ์เกี่ยวกับวิธีการแบบปลอดภัยตามพระราชกฤษฎีกานี้และประกาศที่ออกตามพระราชกฤษฎีกานี้ รวมทั้งกฎหมายอื่นที่เกี่ยวข้อง อย่างน้อยทุกรอบระยะเวลาสองปีนับแต่วันที่พระราชกฤษฎีกานี้ใช้บังคับ ทั้งนี้ โดยพิจารณาถึงความเหมาะสมและความสอดคล้องกับเทคโนโลยีที่ได้มีการพัฒนาหรือเปลี่ยนแปลงไป และจัดทำเป็นรายงานเสนอต่อคณะรัฐมนตรีเพื่อทราบต่อไป

มาตรา ๑๓ ให้นายกรัฐมนตรีรักษาการตามพระราชกฤษฎีกานี้

ผู้รับสนองพระบรมราชโองการ
อภิสิทธิ์ เวชชาชีวะ
นายกรัฐมนตรี

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

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง ประเภทของธุรกรรมทางอิเล็กทรอนิกส์ และหลักเกณฑ์การประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ ตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

เรื่อง ประเภทของธุรกรรมทางอิเล็กทรอนิกส์ และหลักเกณฑ์การประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ตามวิธีการแบบปลอดภัย

พ.ศ. ๒๕๕๕

โดยที่พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓ กำหนดให้คณะกรรมการประกาศกำหนดประเภทของธุรกรรมทางอิเล็กทรอนิกส์ หรือหลักเกณฑ์การประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ เพื่อให้การทำธุรกรรมทางอิเล็กทรอนิกส์ใดที่ได้กระทำตามวิธีการแบบปลอดภัยที่คณะกรรมการกำหนดเป็นวิธีการที่เชื่อถือได้

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

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง ประเภทของธุรกรรมทางอิเล็กทรอนิกส์ และหลักเกณฑ์การประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕”

ข้อ ๒ ให้ธุรกรรมทางอิเล็กทรอนิกส์ในประเภทดังต่อไปนี้ ใช้วิธีการแบบปลอดภัยในระดับเคร่งครัด

(๑) ธุรกรรมทางอิเล็กทรอนิกส์ด้านการชำระเงินทางอิเล็กทรอนิกส์ตามพระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๑

(๒) ธุรกรรมทางอิเล็กทรอนิกส์ด้านการเงินของธนาคารพาณิชย์ตามกฎหมายว่าด้วยธุรกิจสถาบันการเงิน

(๓) ธุรกรรมทางอิเล็กทรอนิกส์ด้านประกันภัยตามกฎหมายว่าด้วยประกันชีวิตและประกันวินาศภัย

(๔) ธุรกรรมทางอิเล็กทรอนิกส์ด้านหลักทรัพย์ของผู้ประกอบธุรกิจหลักทรัพย์ตามกฎหมายว่าด้วยหลักทรัพย์และตลาดหลักทรัพย์

(๕) ธุรกรรมทางอิเล็กทรอนิกส์ที่จัดเก็บ รวบรวม และให้บริการข้อมูลของบุคคลหรือทรัพย์สินหรือทะเบียนต่าง ๆ ที่เป็นเอกสารมหาชนหรือที่เป็นข้อมูลสาธารณะ

(๖) ธุรกรรมทางอิเล็กทรอนิกส์ในการให้บริการด้านสาธารณูปโภคและบริการสาธารณะที่ต้องดำเนินการอย่างต่อเนื่องตลอดเวลา

ข้อ ๓ ในการประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ ให้หน่วยงานหรือองค์กรยึดถือหลักการประเมินความเสี่ยงของระบบเทคโนโลยีสารสนเทศซึ่งเป็นที่ยอมรับเป็นการทั่วไปว่าเชื่อถือได้เป็นแนวทางในการประเมินระดับผลกระทบ

ข้อ ๔ การประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ จะต้องประเมินผลกระทบในด้านต่อไปนี้ด้วย

(๑) ผลกระทบด้านมูลค่าความเสียหายทางการเงิน

(๒) ผลกระทบต่อจำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับอันตรายต่อชีวิต ร่างกายหรืออนามัย

(๓) ผลกระทบต่อจำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับความเสียหายอื่นใดนอกจาก (๒)

(๔) ผลกระทบด้านความมั่นคงของรัฐ

ข้อ ๕ ในการประเมินผลกระทบด้านมูลค่าความเสียหายทางการเงิน ให้จัดเป็นสามระดับโดยมีเกณฑ์ในการประเมิน ดังนี้

(๑) ในกรณีมูลค่าความเสียหายทางการเงินไม่เกินหนึ่งล้านบาท ให้จัดเป็นผลกระทบระดับต่ำ

(๒) ในกรณีมูลค่าความเสียหายทางการเงินเกินกว่าหนึ่งล้านบาทแต่ไม่เกินหนึ่งร้อยล้านบาท ให้จัดเป็นผลกระทบระดับกลาง

(๓) ในกรณีมูลค่าความเสียหายทางการเงินเกินกว่าหนึ่งร้อยล้านบาทขึ้นไป ให้จัดเป็นผลกระทบระดับสูง

ในการประเมินมูลค่าความเสียหายทางการเงินตามวรรคหนึ่ง ให้คำนวณจากความเสียหายที่จะเกิดขึ้นในหนึ่งวันและคำนวณความเสียหายโดยตรงเท่านั้น

ข้อ ๖ ในการประเมินผลกระทบต่อจำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับอันตรายต่อชีวิต ร่างกายหรืออนามัย ให้จัดเป็นสามระดับ โดยมีเกณฑ์ในการประเมิน ดังนี้

(๑) ในกรณีที่ไม่มีผู้ใช้บริการหรือผู้มีส่วนได้เสียได้รับผลกระทบต่อชีวิต ร่างกายหรืออนามัย ให้จัดเป็นผลกระทบระดับต่ำ

(๒) ในกรณีจำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียได้รับผลกระทบต่อร่างกายหรืออนามัยตั้งแต่หนึ่งคน แต่ไม่เกินหนึ่งพันคน ให้จัดเป็นผลกระทบระดับกลาง

(๓) ในกรณีจำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียได้รับผลกระทบต่อร่างกายหรืออนามัยเกินกว่าหนึ่งพันคน หรือต่อชีวิตตั้งแต่หนึ่งคน ให้จัดเป็นผลกระทบระดับสูง

ในการประเมินผลกระทบต่อจำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับอันตรายต่อชีวิต ร่างกายหรืออนามัยตามวรรคหนึ่ง ให้คำนวณจากจำนวนของบุคคลดังกล่าวที่ได้รับผลกระทบในหนึ่งวัน

ข้อ ๗ ในการประเมินผลกระทบต่อจำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับความเสียหายอื่นนอกจากข้อ ๔ (๒) ให้จัดเป็นสามระดับ โดยมีเกณฑ์ในการประเมิน ดังนี้

(๑) ในกรณีจำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับผลกระทบไม่เกินหนึ่งหมื่นคน ให้จัดเป็นผลกระทบระดับต่ำ

(๒) ในกรณีจำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับผลกระทบเกินกว่าหนึ่งหมื่นคน แต่ไม่เกินหนึ่งแสนคน ให้จัดเป็นผลกระทบระดับกลาง

(๓) ในกรณีจำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับผลกระทบเกินกว่าหนึ่งแสนคน ให้จัดเป็นผลกระทบระดับสูง

ในการประเมินผลกระทบต่อจำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับความเสียหายตามวรรคหนึ่ง ให้คำนวณจากจำนวนของบุคคลดังกล่าวที่ได้รับผลกระทบ ในหนึ่งวันและคำนวณความเสียหายโดยตรงเท่านั้น

ข้อ ๘ ในการประเมินผลกระทบด้านความมั่นคงของรัฐ ให้จัดเป็นสองระดับ โดยมีเกณฑ์ในการประเมิน ดังนี้

(๑) ในกรณีไม่มีผลกระทบต่อความมั่นคงของรัฐ ให้จัดเป็นผลกระทบระดับต่ำ

(๒) ในกรณีมีผลกระทบต่อความมั่นคงของรัฐ ให้จัดเป็นผลกระทบระดับสูง

ข้อ ๙ หากปรากฏว่ามีผลประเมินที่เป็นผลกระทบในระดับสูงด้านหนึ่งด้านใดให้ธุรกรรมทางอิเล็กทรอนิกส์นั้นต้องใช้วิธีการแบบปลอดภัยในระดับเคร่งครัด และหากมีผลกระทบในระดับกลางอย่างน้อยสองด้านขึ้นไปให้ใช้วิธีการแบบปลอดภัยในระดับกลางขึ้นไป

ในกรณีที่ไม่เป็นไปตามวรรคหนึ่ง ให้ธุรกรรมทางอิเล็กทรอนิกส์ใช้วิธีการแบบปลอดภัยในระดับไม่ต่ำกว่าระดับพื้นฐาน

ข้อ ๑๐ ประกาศนี้ให้ใช้บังคับเมื่อพ้นกำหนดสามร้อยหกสิบวัน นับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

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

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัย
ของระบบสารสนเทศตามวิธีการแบบปลอดภัย
พ.ศ. ๒๕๕๕

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕

โดยที่พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓ กำหนดให้คณะกรรมการประกาศกำหนดมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในแต่ละระดับ เพื่อให้การทำธุรกรรมทางอิเล็กทรอนิกส์ใดที่ได้กระทำตามวิธีการแบบปลอดภัยที่คณะกรรมการกำหนดเป็นวิธีการที่เชื่อถือได้

อาศัยอำนาจตามความในมาตรา ๗ แห่งพระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓ คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์จึงออกประกาศไว้ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕”

ข้อ ๒ ในกรณีที่จะต้องปฏิบัติให้เป็นไปตามมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับเคร่งครัด ระดับกลาง หรือระดับพื้นฐาน ให้หน่วยงานหรือองค์กร หรือส่วนงานของหน่วยงานหรือองค์กรปฏิบัติตามมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามหลักเกณฑ์ที่กำหนดในแนบท้ายประกาศฉบับนี้

ข้อ ๓ ประกาศนี้ให้ใช้บังคับเมื่อพ้นกำหนดสามร้อยหกสิบวันนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

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

บัญชีแนบท้ายประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕

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

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

๑. มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับพื้นฐาน

การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับพื้นฐานต้องปฏิบัติดังนี้

ข้อ ๑. การสร้างความมั่นคงปลอดภัยด้านบริหารจัดการหน่วยงานต้องกำหนดนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยผ่านการอนุมัติและผลักดันโดยผู้บริหารระดับสูง และมีการประกาศนโยบายดังกล่าวให้พนักงานและบุคคลภายนอกที่เกี่ยวข้องรับทราบโดยทั่วกัน

ข้อ ๒. การจัดโครงสร้างด้านความมั่นคงปลอดภัยของระบบสารสนเทศในส่วนการบริหารจัดการด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ทั้งภายในและภายนอกหน่วยงานหรือองค์กร

๒.๑ ผู้บริหารระดับสูงของหน่วยงานมีหน้าที่ดูแลรับผิดชอบงานด้านสารสนเทศของหน่วยงานให้การสนับสนุน และกำหนดทิศทางการดำเนินงานเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศที่ชัดเจน รวมทั้งมีการมอบหมายงานที่เกี่ยวข้องให้กับผู้ปฏิบัติงานอย่างชัดเจน ตลอดจนรับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกับระบบสารสนเทศไม่ว่ากรณีใด ๆ

๒.๒ สำหรับระบบสารสนเทศใหม่ มีการกำหนดขั้นตอนการพิจารณาทบทวน เพื่ออนุมัติการสร้าง การติดตั้ง หรือการใช้งานในแง่มุมต่าง ๆ เช่น การบริหารจัดการผู้ใช้งานระบบ หรือความสามารถในการทำงานร่วมกันได้ระหว่างระบบเดิมและระบบใหม่

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

๒.๔ มีข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศสำหรับการอนุญาตให้ผู้ใช้บริการที่เป็นบุคคลภายนอกเข้าถึงระบบสารสนเทศ หรือใช้ข้อมูลสารสนเทศของหน่วยงาน

๒.๕ สำหรับข้อตกลงเพื่ออนุญาตให้บุคคลภายนอกเข้าถึงระบบสารสนเทศ หรือใช้ข้อมูลสารสนเทศของหน่วยงาน เพื่อการอ่าน การประมวลผล การบริหารจัดการระบบสารสนเทศ หรือการพัฒนาระบบสารสนเทศ ควรมีข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศระบุไว้ในข้อตกลง

ข้อ ๓. การบริหารจัดการทรัพย์สินสารสนเทศมีการเก็บบันทึกข้อมูลทรัพย์สินสารสนเทศ โดยข้อมูลที่จัดเก็บต้องประกอบด้วยข้อมูลที่จำเป็นในการค้นหาเพื่อการใช้งานในภายหลัง

ข้อ ๔. การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร

๔.๑ กำหนดหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยด้านสารสนเทศของพนักงาน หรือหน่วยงานหรือบุคคลภายนอกที่ว่าจ้าง โดยให้สอดคล้องกับความมั่นคงปลอดภัยด้านสารสนเทศและนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่หน่วยงานประกาศใช้

๔.๒ ผู้บริหารระดับสูงของหน่วยงานต้องกำหนดให้พนักงาน หน่วยงานหรือบุคคลภายนอกที่ว่าจ้างปฏิบัติงานตามนโยบายหรือระเบียบปฏิบัติด้านความมั่นคงปลอดภัยที่หน่วยงานประกาศใช้

๔.๓ กำหนดให้มีขั้นตอนการลงโทษพนักงานที่ฝ่าฝืนนโยบายหรือระเบียบปฏิบัติเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศในหน่วยงาน

๔.๔ กำหนดหน้าที่ความรับผิดชอบในการยุติการจ้าง หรือการเปลี่ยนแปลงสถานะการจ้างให้ชัดเจน และมอบหมายให้มีผู้รับผิดชอบอย่างชัดเจน

๔.๕ พนักงาน หน่วยงานหรือบุคคลภายนอกที่ว่าจ้างต้องส่งคืนทรัพย์สินสารสนเทศของหน่วยงานเมื่อสิ้นสุดสถานะการเป็นพนักงาน หรือสิ้นสุดสัญญาหรือข้อตกลงการปฏิบัติงานให้กับหน่วยงาน

๔.๖ ให้ยกเลิกสิทธิของพนักงาน หน่วยงานหรือบุคคลภายนอกในการเข้าใช้งานระบบสารสนเทศ เมื่อสิ้นสุดสถานะการเป็นพนักงาน หรือสิ้นสุดสัญญาหรือข้อตกลงการปฏิบัติงาน และให้ปรับเปลี่ยนระดับสิทธิในการเข้าใช้งานระบบสารสนเทศให้เหมาะสมเมื่อมีการเปลี่ยนแปลงหน้าที่ความรับผิดชอบใด ๆ เกิดขึ้น

ข้อ ๕. การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม

๕.๑ ให้มีการป้องกันขอบเขตพื้นที่ตั้งของหน่วยงาน (Security perimeter) ที่มีการติดตั้ง จัดเก็บ หรือใช้งาน ระบบสารสนเทศและข้อมูลสารสนเทศ

๕.๒ มีการออกแบบและติดตั้งการป้องกันความมั่นคงปลอดภัยด้านกายภาพ เพื่อป้องกันภัยจากภายนอก ภัยในระดับหายนะทั้งที่ก่อโดยมนุษย์หรือภัยธรรมชาติ เช่น อัคคีภัย อุทกภัย แผ่นดินไหว ระเบิด การก่อจลาจล เป็นต้น

๕.๓ จัดวางและป้องกันอุปกรณ์สารสนเทศ เพื่อลดความเสี่ยงจากภัยธรรมชาติหรืออันตรายต่าง ๆ และเพื่อป้องกันการเข้าถึงโดยมิได้รับอนุญาต

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

๕.๕ มีการดูแลอุปกรณ์สารสนเทศอย่างถูกวิธี เพื่อให้คงไว้ซึ่งความถูกต้องครบถ้วนและอยู่ในสภาพพร้อมใช้งานอยู่เสมอ

ข้อ ๖. การบริหารจัดการด้านการสื่อสารและการดำเนินงานของระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

๖.๑ มีการจัดทำ ปรับปรุง และดูแลเอกสารขั้นตอนการปฏิบัติงานที่อยู่ในสภาพพร้อมใช้งาน เพื่อให้พนักงานสามารถนำไปปฏิบัติได้

๖.๒ มีการดูแลให้บุคคลหรือหน่วยงานภายนอกที่ให้บริการแก่หน่วยงานตามที่ว่างจ้างปฏิบัติตามสัญญาหรือข้อตกลงให้บริการที่ระบุไว้ ซึ่งต้องครอบคลุมถึงงานด้านความมั่นคงปลอดภัย ลักษณะการให้บริการ และระดับการให้บริการ

๖.๓ มีการติดตามตรวจสอบรายงานหรือบันทึกการให้บริการของบุคคลหรือหน่วยงานภายนอกที่ให้บริการแก่หน่วยงานตามที่ว่าจ้างอย่างสม่ำเสมอ

๖.๔ จัดให้มีเกณฑ์การตรวจรับระบบสารสนเทศที่มีการปรับปรุง หรือที่มีเวอร์ชั่นใหม่ และควรมีการทดสอบระบบสารสนเทศทั้งในช่วงการพัฒนาระบบและก่อนการตรวจรับ

๖.๕ มีขั้นตอนควบคุมการตรวจสอบ ป้องกัน และกู้คืนในกรณีมีการใช้งานโปรแกรมไม่พึงประสงค์ และให้มีการสร้างความตระหนักรู้ให้กับผู้ใช้งานระบบสารสนเทศหรือข้อมูลสารสนเทศเกี่ยวกับโปรแกรมไม่พึงประสงค์

๖.๖ มีการสำรองข้อมูลสารสนเทศ และทดสอบการนำกลับมาใช้งาน โดยให้เป็นไปตามนโยบายการสำรองข้อมูลที่หน่วยงานประกาศใช้

๖.๗ มีการบริหารจัดการการควบคุมเครือข่ายคอมพิวเตอร์ เพื่อป้องกันภัยคุกคาม และมีการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและแอพพลิเคชั่นที่ทำงานบนเครือข่ายคอมพิวเตอร์ รวมทั้งข้อมูลสารสนเทศที่มีการแลกเปลี่ยนบนเครือข่ายดังกล่าว

๖.๘ มีการกำหนดรูปแบบการรักษาความมั่นคงปลอดภัย ระดับการให้บริการ ข้อกำหนดการบริหารจัดการในข้อตกลงการให้บริการด้านเครือข่ายคอมพิวเตอร์ ไม่ว่าเป็นการให้บริการโดยหน่วยงานเอง หรือจ้างช่วงไปยังผู้ให้บริการภายนอก

๖.๙ จัดให้มีนโยบายและขั้นตอนปฏิบัติงาน รวมทั้งควบคุมการแลกเปลี่ยนข้อมูลสารสนเทศผ่านช่องทางการสื่อสารในรูปแบบข้อมูลอิเล็กทรอนิกส์

๖.๑๐ จัดให้มีข้อตกลงในการแลกเปลี่ยนข้อมูลสารสนเทศหรือซอฟต์แวร์ระหว่างหน่วยงานกับบุคคลหรือหน่วยงานภายนอก

๖.๑๑ จัดให้มีนโยบายและขั้นตอนการปฏิบัติงาน เพื่อป้องกันข้อมูลสารสนเทศที่มีการสื่อสารหรือแลกเปลี่ยนผ่านระบบสารสนเทศที่มีการเชื่อมต่อกับระบบสารสนเทศต่าง ๆ

๖.๑๒ มีการป้องกันข้อมูลสารสนเทศที่มีการแลกเปลี่ยนในการทำพาณิชย์อิเล็กทรอนิกส์ (Electronic commerce) ผ่านเครือข่ายคอมพิวเตอร์สาธารณะ เพื่อมิให้มีการฉ้อโกง ละเมิดสัญญา หรือมีการรั่วไหลหรือข้อมูลสารสนเทศถูกแก้ไขโดยมิได้รับอนุญาต

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

๖.๑๔ สำหรับข้อมูลสารสนเทศที่มีการเผยแพร่ต่อสาธารณชน ให้มีการป้องกันมิให้มีการแก้ไขเปลี่ยนแปลงโดยมิได้รับอนุญาต และเพื่อรักษาความถูกต้องครบถ้วนของข้อมูลสารสนเทศ

๖.๑๕ มีการเก็บบันทึกข้อมูล Audit log ซึ่งบันทึกข้อมูลกิจกรรมการใช้งานของผู้ใช้งานระบบสารสนเทศและเหตุการณ์เกี่ยวกับความมั่นคงปลอดภัยต่าง ๆ เพื่อประโยชน์ในการสืบสวน สอบสวน ในอนาคต และเพื่อการติดตามการควบคุมการเข้าถึง

๖.๑๖ มีขั้นตอนการเฝ้าติดตามสังเกตการใช้งานระบบสารสนเทศ และมีการติดตามประเมินผลการติดตามสังเกตดังกล่าวอย่างสม่ำเสมอ

๖.๑๗ มีการป้องกันระบบสารสนเทศที่จัดเก็บ Log และข้อมูล Log เพื่อป้องกันการเข้าถึงหรือแก้ไขเปลี่ยนแปลงโดยมิได้รับอนุญาต

๖.๑๘ มีการจัดเก็บ Log ที่เกี่ยวข้องกับการดูแลระบบสารสนเทศโดยผู้ดูแลระบบ (System administrator หรือ System operator)

ข้อ ๗. การควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์

๗.๑ จัดให้มีนโยบายควบคุมการเข้าถึง โดยจัดทำเป็นเอกสาร และมีการติดตามทบทวนให้นโยบายดังกล่าวสอดคล้องกับข้อกำหนดหรือความต้องการด้านการดำเนินงานหรือการให้บริการ และด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

๗.๒ จัดให้มีการลงทะเบียนบัญชีผู้ใช้งานระบบสารสนเทศ และยกเลิกบัญชีผู้ใช้อย่างเป็นทางการเพื่อควบคุมการให้สิทธิและการยกเลิกสิทธิในการเข้าใช้งานระบบสารสนเทศใด ๆ ของหน่วยงาน

๗.๓ การกำหนดสิทธิในการเข้าถึงระดับสูง ให้ทำอย่างจำกัดและอยู่ภายใต้การควบคุม

๗.๔ ผู้ใช้งานต้องดูแลป้องกันอุปกรณ์สารสนเทศใดที่อยู่ภายใต้ความดูแลรับผิดชอบ ในระหว่างที่ไม่มีการใช้งาน

๗.๕ จำกัดการเข้าถึงเครือข่ายคอมพิวเตอร์ของหน่วยงานที่สามารถเข้าถึงได้จากภายนอก โดยให้สอดคล้องกับนโยบายควบคุมการเข้าถึง และข้อกำหนดการใช้งานแอพพลิเคชั่นเพื่อการดำเนินงาน

๗.๖ ให้ผู้ใช้งานทุกคนมีบัญชีผู้ใช้งานเป็นของตนเอง และให้ระบบสารสนเทศมีเทคนิคการตรวจสอบตัวตนที่เพียงพอ เพื่อให้สามารถระบุตัวตนของผู้เข้าใช้งานระบบสารสนเทศได้

๗.๗ ให้ยุติหรือปิดหน้าจอการใช้งานระบบสารสนเทศโดยอัตโนมัติ หากไม่มีการใช้งานเกินระยะเวลาสูงสุดที่กำหนดไว้

๗.๘ จำกัดการเข้าถึงข้อมูลสารสนเทศและฟังก์ชั่นต่าง ๆ ในแอพพลิเคชั่นของผู้ใช้งานและผู้ดูแลระบบสารสนเทศ โดยให้สอดคล้องกับนโยบายการเข้าถึงที่ได้กำหนดไว้

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

ข้อ ๘. การจัดหาหรือจัดให้มีการพัฒนา และการบำรุงรักษาระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

๘.๑ ในการจัดทำข้อกำหนดขั้นต่ำของระบบสารสนเทศใหม่ หรือการปรับปรุงระบบสารสนเทศเดิม ให้มีการระบุข้อกำหนดด้านการควบคุมความมั่นคงปลอดภัยด้านสารสนเทศไว้ด้วย

๘.๒ ให้ดูแล ควบคุม ติดตามตรวจสอบการทำงานในการจ้างช่วงพัฒนาซอฟต์แวร์

ข้อ ๙. การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิดให้มีการรายงานสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิดผ่าน ช่องทางการบริหารจัดการที่เหมาะสมโดยเร็วที่สุด

ข้อ ๑๐. การบริหารจัดการด้านการบริการหรือการดำเนินงานของหน่วยงานหรือองค์กรเพื่อให้มีความต่อเนื่อง ให้กำหนดแผนเพื่อรักษาไว้หรือกู้คืนการให้บริการสารสนเทศ หลังเกิดเหตุการณ์ที่ทำให้ การดำเนินงานหยุดชะงัก เพื่อให้ข้อมูลสารสนเทศอยู่ในสภาพพร้อมใช้งานตามระดับที่กำหนดไว้ ภายในระยะเวลาที่กำหนดไว้

ข้อ ๑๑. การตรวจสอบและการประเมินผลการปฏิบัติตามนโยบาย มาตรการ หลักเกณฑ์ หรือกระบวนการใด ๆ รวมทั้งข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

๑๑.๑ ให้มีการระบุไว้ให้ชัดเจนถึงแนวทางในการดำเนินงานของระบบสารสนเทศที่มีความสอดคล้องตามกฎหมายและข้อกำหนดตามสัญญาต่าง ๆ ของหน่วยงาน โดยต้องจัดทำเป็นเอกสาร และมีการปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๑๑.๒ ป้องกันมิให้มีการใช้งานระบบสารสนเทศผิดวัตถุประสงค์

๑๑.๓ พนักงานของหน่วยงานต้องดูแลให้งานที่เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศที่อยู่ในขอบเขตความรับผิดชอบได้ดำเนินการไปโดยสอดคล้องกับกฎหมายและข้อกำหนดตามสัญญาต่าง ๆ ของหน่วยงาน

๒. มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับกลาง

การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับกลาง ให้ปฏิบัติตามมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับพื้นฐาน และต้องปฏิบัติเพิ่มเติม ดังนี้

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

ข้อ ๒. การจัดโครงสร้างด้านความมั่นคงปลอดภัยของระบบสารสนเทศในส่วนการบริหารจัดการด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ทั้งภายในและภายนอกหน่วยงานหรือองค์กร

๒.๑ มีการกำหนดเนื้องานหรือหน้าที่ความรับผิดชอบต่าง ๆ เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศไว้อย่างชัดเจน

๒.๒ มีการกำหนดขั้นตอนและช่องทางในการติดต่อกับหน่วยงานภายนอกที่มีความเชี่ยวชาญเฉพาะด้านหรือหน่วยงานที่มีความเชี่ยวชาญด้านความมั่นคงปลอดภัยด้านสารสนเทศภายใต้สถานการณ์ต่าง ๆ ไว้อย่างชัดเจน

๒.๓ จัดให้มีการพิจารณาทบทวนแนวทางในการบริหารจัดการงานเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศอย่างสม่ำเสมอ หรือเมื่อมีการเปลี่ยนแปลงใด ๆ ในการดำเนินงาน ทั้งนี้ การพิจารณาทบทวนดังกล่าวควรดำเนินการโดยผู้ไม่มีส่วนได้เสียกับงานที่มีการพิจารณาทบทวน

ข้อ ๓. การบริหารจัดการทรัพย์สินสารสนเทศ

๓.๑ มีการกำหนดบุคคลผู้มีหน้าที่ดูแลควบคุมการใช้งานและรับผิดชอบทรัพย์สินสารสนเทศไว้ชัดเจน

๓.๒ มีการกำหนดกฎระเบียบในการใช้งานทรัพย์สินสารสนเทศไว้อย่างชัดเจน โดยจัดทำเป็นเอกสาร และมีการประกาศใช้ในหน่วยงาน

๓.๓ มีการจำแนกประเภทของข้อมูลสารสนเทศ โดยจำแนกตามมูลค่าของข้อมูล ข้อกำหนดทางกฎหมาย ระดับชั้นความลับและความสำคัญต่อหน่วยงาน

๓.๔ มีการกำหนดและประกาศใช้ขั้นตอนที่เหมาะสมในการจำแนกประเภทของข้อมูลสารสนเทศ และจัดการข้อมูลสารสนเทศ โดยให้สอดคล้องกับแนวทางการจำแนกประเภทของข้อมูลสารสนเทศที่หน่วยงานประกาศใช้

ข้อ ๔. การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร พนักงาน หน่วยงานหรือบุคคลภายนอกต้องได้รับการอบรมเพื่อสร้างความตระหนักรู้เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศในส่วนที่เกี่ยวข้องกับหน้าที่ความรับผิดชอบของตน และได้รับการสื่อสารให้ทราบถึงนโยบายหรือระเบียบปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศที่หน่วยงานประกาศใช้อย่างสม่ำเสมอ หรือเมื่อมีการเปลี่ยนแปลง

ข้อ ๕. การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม

๕.๑ มีการออกแบบและติดตั้งการป้องกันความมั่นคงปลอดภัยด้านกายภาพ เพื่อป้องกันพื้นที่หรือสถานที่ปฏิบัติงาน หรืออุปกรณ์สารสนเทศต่าง ๆ

๕.๒ ไม่ควรนำอุปกรณ์สารสนเทศ ข้อมูลสารสนเทศ หรือซอฟต์แวร์ออกจากสถานที่ปฏิบัติงานของหน่วยงานหากมิได้รับอนุญาต

ข้อ ๖. การบริหารจัดการด้านการสื่อสารและการดำเนินงานของระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

๖.๑ มีการจัดการควบคุมการเปลี่ยนแปลงของระบบสารสนเทศ

๖.๒ มีการติดตามผลการใช้งานทรัพยากรสารสนเทศ และวางแผนด้านทรัพยากรสารสนเทศให้รองรับการปฏิบัติงานในอนาคตอย่างเหมาะสม

๖.๓ มีขั้นตอนการปฏิบัติงานในการจัดการและจัดเก็บข้อมูลสารสนเทศเพื่อมิให้ข้อมูลรั่วไหลหรือถูกนำไปใช้ผิดประเภท

๖.๔ มีการจัดเก็บ Log ที่เกี่ยวข้องกับข้อผิดพลาดใด ๆ ของระบบสารสนเทศ มีการวิเคราะห์ Log ดังกล่าวอย่างสม่ำเสมอ และมีการจัดการแก้ไขข้อผิดพลาดที่ตรวจพบอย่างเหมาะสม

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

ข้อ ๗. การควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์

๗.๑ มีข้อบังคับให้ผู้ใช้งานปฏิบัติตามขั้นตอนเพื่อการเลือกใช้รหัสผ่านอย่างมั่นคงปลอดภัยตามที่หน่วยงานกำหนด

๗.๒ ผู้ใช้งานสามารถเข้าถึงเฉพาะบริการทางเครือข่ายคอมพิวเตอร์ที่ตนเองได้รับอนุญาตให้ใช้ได้เท่านั้น

๗.๓ ให้มีการกำหนดวิธีการตรวจสอบตัวตนที่เหมาะสมเพื่อควบคุมการเข้าถึงระบบสารสนเทศของหน่วยงานจากระยะไกล

๗.๔ มีการควบคุมการเข้าถึงช่องทางการดูแลระบบสารสนเทศทั้งทางกายภาพและการเชื่อมต่อผ่านคอมพิวเตอร์ สำหรับระบบสารสนเทศที่สามารถเข้าถึงจากระยะไกลได้ เช่น Remote diagnostic หรือ Configuration facility ของอุปกรณ์เครือข่ายคอมพิวเตอร์

๗.๕ มีการจัดกลุ่มตามประเภทของข้อมูลสารสนเทศที่ให้บริการ ระบบสารสนเทศ กลุ่มผู้ใช้งานโดยมีการแบ่งแยกบนเครือข่ายคอมพิวเตอร์อย่างเป็นสัดส่วน

๗.๖ กำหนดให้มีการควบคุมเส้นทางการไหลของข้อมูลสารสนเทศในระบบเครือข่ายคอมพิวเตอร์เพื่อไม่ให้ขัดแย้งกับนโยบายควบคุมการเข้าถึงของแอพพลิเคชั่น

๗.๗ กำหนดขั้นตอนการ Log-on เพื่อควบคุมการเข้าถึงระบบปฏิบัติการคอมพิวเตอร์

๗.๘ ให้จัดทำหรือจัดให้มีระบบการบริหารจัดการรหัสผ่านที่สามารถทำงานแบบเชิงโต้ตอบกับผู้ใช้งาน (Interactive) และสามารถรองรับการใช้งานรหัสผ่านที่มีความมั่นคงปลอดภัย

ข้อ ๘. การจัดหาหรือจัดให้มีการพัฒนา และการบำรุงรักษาระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

๘.๑ ให้มีการตรวจสอบ (Validate) ข้อมูลใด ๆ ที่จะรับเข้าสู่แอพพลิเคชั่นก่อนเสมอ เพื่อให้มั่นใจได้ว่าข้อมูลมีความถูกต้องและมีรูปแบบเหมาะสม

๘.๒ ให้มีการตรวจสอบ (Validate) ข้อมูลใด ๆ อันเป็นผลจากการประมวลผลของแอพพลิเคชั่น เพื่อให้มั่นใจได้ว่า ข้อมูลที่ได้จากการประมวลผลถูกต้องและเหมาะสม

๘.๓ จัดให้มีแนวทางการบริหารจัดการกุญแจ (Key) เพื่อรองรับการใช้งานเทคนิคที่เกี่ยวข้องกับการเข้ารหัสลับของหน่วยงาน

๘.๔ ให้เลือกชุดข้อมูลสารสนเทศที่จะนำไปใช้เพื่อการทดสอบในระบบสารสนเทศอย่างระมัดระวัง รวมทั้งมีแนวทางควบคุมและป้องกันข้อมูลรั่วไหล

๘.๕ ให้มีการจำกัดการเข้าถึงซอร์สโค้ด (Source code) ของโปรแกรม

๘.๖ หากมีการเปลี่ยนแปลงใด ๆ ในระบบปฏิบัติการคอมพิวเตอร์ ให้มีการตรวจสอบทบทวนการทำงานของโปรแกรมที่มีความสำคัญ และทดสอบการใช้งานเพื่อให้มั่นใจว่าผลของการเปลี่ยนแปลงดังกล่าว จะไม่ส่งผลกระทบใด ๆ ต่อความมั่นคงปลอดภัยของระบบสารสนเทศและการให้บริการของหน่วยงาน

ข้อ ๙. การบริหารจัดการด้านการบริการหรือการดำเนินงานของหน่วยงานหรือองค์กรเพื่อให้มีความต่อเนื่อง

๙.๑ จัดให้มีข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศที่จำเป็น โดยกำหนดให้เป็นส่วนหนึ่งของขั้นตอนการบริหารจัดการเพื่อการดำเนินงานอย่างต่อเนื่องในภาวะฉุกเฉิน

๙.๒ กำหนดให้มีกรอบงานหลักสำหรับการพัฒนาแผนการบริหารจัดการเพื่อการดำเนินงานอย่างต่อเนื่องในภาวะฉุกเฉิน เพื่อให้การพัฒนาแผนต่าง ๆ เป็นไปในทิศทางเดียวกัน รวมทั้งสอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัย ตลอดจนมีการจัดลำดับความสำคัญก่อนหลังในการทดสอบและการดูแล

๙.๓ ให้มีการทดสอบและปรับปรุงแผนการบริหารจัดการเพื่อการดำเนินงานอย่างต่อเนื่องในภาวะฉุกเฉินอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าแผนดังกล่าวเป็นปัจจุบันและมีประสิทธิผลอยู่เสมอ

ข้อ ๑๐. การตรวจสอบและการประเมินผลการปฏิบัติตามนโยบาย มาตรการ หลักเกณฑ์ หรือกระบวนการใด ๆ รวมทั้งข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

๑๐.๑ จัดให้มีการคุ้มครองข้อมูลส่วนบุคคลโดยให้สอดคล้องกับกฎหมายและข้อกำหนดตามสัญญาต่าง ๆ ของหน่วยงาน

๑๐.๒ ใช้เทคนิคการเข้ารหัสลับ ที่สอดคล้องกับกฎหมายและข้อกำหนดตามสัญญาต่าง ๆ ของหน่วยงาน

๑๐.๓ ให้มีการทบทวนตรวจสอบระบบสารสนเทศในด้านเทคนิคอย่างสม่ำเสมอเพื่อให้สอดคล้องกับมาตรฐานการพัฒนางานด้านความมั่นคงปลอดภัยด้านสารสนเทศ

๑๐.๔ วางแผนและจัดให้มีข้อกำหนดการตรวจสอบและกิจกรรมที่เกี่ยวข้องกับการตรวจสอบระบบสารสนเทศ เพื่อลดความเสี่ยงในการเกิดการหยุดชะงักของการให้บริการ

๑๐.๕ ป้องกันการเข้าใช้งานเครื่องมือที่ใช้เพื่อการตรวจสอบ เพื่อมิให้เกิดการใช้งานผิดประเภทหรือถูกละเมิดการใช้งาน (Compromise)

๓. มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับเคร่งครัด

การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับเคร่งครัด ให้ปฏิบัติตามมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับพื้นฐานและระดับกลาง และต้องปฏิบัติเพิ่มเติม ดังนี้

ข้อ ๑. การจัดโครงสร้างด้านความมั่นคงปลอดภัยของระบบสารสนเทศในส่วนการบริหารจัดการด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ทั้งภายในและภายนอกหน่วยงานหรือองค์กร

๑.๑ มีการสร้างความร่วมมือระหว่างผู้ที่มีบทบาทเกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน ในงานหรือกิจกรรมใด ๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศ

๑.๒ มีการกำหนดขั้นตอนและช่องทางในการติดต่อกับหน่วยงานภายนอกที่มีหน้าที่ในการกำกับดูแล หรือหน่วยงานที่เกี่ยวข้องกับการบังคับใช้กฎหมาย รวมทั้งหน่วยงานที่ควบคุมดูแลสถานการณ์ฉุกเฉินภายใต้สถานการณ์ต่าง ๆ ไว้อย่างชัดเจน

๑.๓ ก่อนที่จะอนุญาตให้หน่วยงานหรือบุคคลภายนอกเข้าถึงระบบสารสนเทศหรือใช้ข้อมูลสารสนเทศของหน่วยงาน ให้มีการระบุความเสี่ยงที่อาจเกิดขึ้นและกำหนดแนวทางป้องกันเพื่อลดความเสี่ยงนั้นก่อนการอนุญาต

ข้อ ๒. การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร

๒.๑ ในการพิจารณารับพนักงานเข้าทำงาน หรือการว่าจ้างหน่วยงานหรือบุคคลภายนอก ให้มีการตรวจสอบประวัติหรือคุณสมบัติเพื่อให้เป็นไปตามกฎหมาย กฎระเบียบและจริยธรรมที่เกี่ยวข้อง โดยให้คำนึงถึงระดับชั้นความลับของข้อมูลสารสนเทศที่จะให้เข้าถึง และระดับความเสี่ยงที่ได้ประเมิน

๒.๒ ในสัญญาจ้างหรือข้อตกลงการปฏิบัติงานของพนักงาน หรือสัญญาว่าจ้างหน่วยงานหรือบุคคลภายนอก ให้ระบุหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยด้านสารสนเทศไว้ในสัญญา

ข้อ ๓. การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม

๓.๑ ในพื้นที่ที่ต้องมีการรักษาความมั่นคงปลอดภัยด้านกายภาพ (Secure area) ต้องมีการควบคุมการเข้าออก โดยให้เฉพาะผู้มีสิทธิที่สามารถเข้าออกได้

๓.๒ มีการออกแบบแนวทางการป้องกันทางกายภาพสำหรับการทำงานในพื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัยด้านกายภาพ (Secure area) และกำหนดให้มีการนำไปใช้งาน

๓.๓ มีการควบคุมบริเวณที่ผู้ไม่มีสิทธิเข้าถึงอาจสามารถเข้าถึงได้ เช่น จุดรับส่งของ เป็นต้น หรือหากเป็นไปได้ให้แยกบริเวณดังกล่าวออกจากพื้นที่ที่มีการติดตั้ง จัดเก็บ หรือใช้งาน ระบบสารสนเทศและข้อมูลสารสนเทศเพื่อหลีกเลี่ยงการเข้าถึงโดยมิได้รับอนุญาต

๓.๔ มีการป้องกันสายเคเบิลที่ใช้เพื่อการสื่อสาร หรือสายไฟ เพื่อมิให้มีการดักรับสัญญาณ (Interception) หรือมีความเสียหายเกิดขึ้น

๓.๕ มีการรักษาความมั่นคงปลอดภัยให้กับอุปกรณ์สารสนเทศที่มีการนำไปใช้งานนอกสถานที่ปฏิบัติงานของหน่วยงาน โดยให้คำนึงถึงระดับความเสี่ยงที่แตกต่างกันจากการนำไปใช้งานในสถานที่ต่าง ๆ

๓.๖ ก่อนการยกเลิกการใช้งานหรือจำหน่ายอุปกรณ์สารสนเทศที่ใช้ในการจัดเก็บข้อมูลสารสนเทศต้องมีการตรวจสอบอุปกรณ์สารสนเทศนั้นว่า ได้มีการลบ ย้าย หรือทำลาย ข้อมูลที่สำคัญหรือซอฟต์แวร์ที่จัดซื้อและติดตั้งไว้ด้วยวิธีการที่ทำให้ไม่สามารถกู้คืนได้อีก

ข้อ ๔. การบริหารจัดการด้านการสื่อสารและการดำเนินงานของระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

๔.๑ มีการแบ่งแยกหน้าที่และขอบเขตความรับผิดชอบอย่างชัดเจน เพื่อลดโอกาสความผิดพลาดในการเปลี่ยนแปลงหรือใช้งานระบบสารสนเทศหรือข้อมูลสารสนเทศที่ผิดประเภท

๔.๒ มีการแยกระบบสารสนเทศสำหรับการพัฒนา ทดสอบ และใช้งานจริงออกจากกัน เพื่อลดความเสี่ยงในการเข้าใช้งานหรือการเปลี่ยนแปลงระบบสารสนเทศโดยมิได้รับอนุญาต

๔.๓ มีการบริหารจัดการการเปลี่ยนแปลงใด ๆ เกี่ยวกับการจัดเตรียมการให้บริการ และการดูแลปรับปรุงนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ขั้นตอนปฏิบัติงาน หรือการควบคุมเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ โดยคำนึงถึงระดับความสำคัญของการดำเนินธุรกิจที่เกี่ยวข้องและการประเมินความเสี่ยงอย่างต่อเนื่อง

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

๔.๕ มีขั้นตอนการปฏิบัติงานสำหรับการบริหารจัดการอุปกรณ์ที่ใช้ในการบันทึกข้อมูลอิเล็กทรอนิกส์ที่สามารถถอดหรือต่อพ่วงกับเครื่องคอมพิวเตอร์ได้ (Removable media)

๔.๖ มีขั้นตอนการปฏิบัติงานในการทำลายอุปกรณ์ที่ใช้ในการบันทึกข้อมูลอิเล็กทรอนิกส์ที่สามารถถอดหรือต่อพ่วงกับเครื่องคอมพิวเตอร์ได้ (Removable media) อย่างมั่นคงปลอดภัย

๔.๗ มีการป้องกันมิให้ข้อมูลหรือเอกสารเกี่ยวกับระบบสารสนเทศ (System documentation) ถูกเข้าถึงโดยมิได้รับอนุญาต

๔.๘ ในกรณีที่มีการเคลื่อนย้ายอุปกรณ์ที่จัดเก็บข้อมูลสารสนเทศ ให้มีการป้องกันอุปกรณ์ที่ใช้จัดเก็บข้อมูลดังกล่าว เพื่อมิให้มีการเข้าถึงโดยมิได้รับอนุญาต หรือถูกนำไปใช้งานผิดประเภท หรืออุปกรณ์หรือข้อมูลสารสนเทศได้รับความเสียหาย

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

ข้อ ๕. การควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์

๕.๑ จัดให้มีขั้นตอนการบริหารจัดการเรื่องการกำหนดรหัสผ่านอย่างเป็นทางการ

๕.๒ กำหนดให้ผู้บริหารติดตามทบทวนระดับสิทธิในการเข้าถึงของผู้ใช้งานอย่างเป็นทางการเป็นประจำ

๕.๓ มีการกำหนดนโยบาย Clear desk สำหรับข้อมูลสารสนเทศในรูปแบบกระดาษและที่จัดเก็บในอุปกรณ์บันทึกข้อมูลอิเล็กทรอนิกส์ที่สามารถถอดหรือต่อพ่วงกับเครื่องคอมพิวเตอร์ได้ และนโยบาย Clear screen สำหรับระบบสารสนเทศ

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

๕.๕ ให้จำกัดการเข้าถึงการใช้งานโปรแกรมอรรถประโยชน์ต่าง ๆ อย่างเข้มงวด เนื่องจากโปรแกรมดังกล่าวอาจมีความสามารถควบคุมดูแลและเปลี่ยนแปลงการทำงานของระบบสารสนเทศได้

๕.๖ จำกัดระยะเวลาการเชื่อมต่อกับระบบสารสนเทศที่มีระดับความเสี่ยงสูง เพื่อเพิ่มระดับการรักษาความมั่นคงปลอดภัย

๕.๗ สำหรับระบบสารสนเทศที่มีความสำคัญสูง ต้องจัดให้ระบบสารสนเทศทำงานในสภาพแวดล้อมที่แยกออกมาต่างหาก โดยไม่ใช้ปะปนกับระบบสารสนเทศอื่น

๕.๘ กำหนดให้มีนโยบาย แผนงานและขั้นตอนการปฏิบัติงานที่เกี่ยวข้องกับกิจกรรมใด ๆ ที่มีการปฏิบัติงานจากภายนอกหน่วยงาน (Teleworking)

ข้อ ๖. การจัดหาหรือจัดให้มีการพัฒนา และการบำรุงรักษาระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

๖.๑ ให้มีการตรวจสอบ (Validate) การทำงานของแอพพลิเคชั่นเพื่อตรวจหาข้อผิดพลาดของข้อมูลที่อาจเกิดจากการทำงานหรือการประมวลผลที่ผิดพลาด

๖.๒ ให้มีข้อกำหนดขั้นต่ำสำหรับการรักษาความถูกต้องแท้จริง (Authenticity) และความถูกต้องครบถ้วน (Integrity) ของข้อมูลในแอพพลิเคชั่น รวมทั้งมีการระบุและปฏิบัติตามวิธีการป้องกันที่เหมาะสม

๖.๓ จัดให้มีนโยบายในการใช้งานเทคนิคที่เกี่ยวข้องกับการเข้ารหัสลับ

๖.๔ กำหนดให้มีขั้นตอนการปฏิบัติงานเพื่อควบคุมการติดตั้งซอฟต์แวร์บนระบบสารสนเทศที่ให้บริการ

๖.๕ ให้มีการควบคุมการเปลี่ยนแปลงต่าง ๆ ในการพัฒนาระบบสารสนเทศ โดยมีขั้นตอนการควบคุมที่เป็นทางการ

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

๖.๘ มีมาตรการป้องกันเพื่อลดโอกาสที่เกิดการรั่วไหลของข้อมูลสารสนเทศ

ข้อ ๗. การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด

๗.๑ กำหนดให้พนักงานหรือผู้ใช้งานที่เป็นบุคคลภายนอก มีการบันทึกและรายงานจุดอ่อนใด ๆ ที่อาจสังเกตพบระหว่างการใช้งานระบบสารสนเทศ

๗.๒ กำหนดขอบเขตความรับผิดชอบของผู้บริหารและขั้นตอนการปฏิบัติงาน เพื่อตอบสนองต่อสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด อย่างรวดเร็ว มีระเบียบ และมีประสิทธิผล

๗.๓ หากในขั้นตอนการติดตามผลกับบุคคลหรือหน่วยงานภายหลังจากเกิดสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด ซึ่งเกี่ยวข้องกับการดำเนินการทางกฎหมาย (ไม่ว่าทางแพ่งหรือทางอาญา) ให้มีการรวบรวม จัดเก็บ และนำเสนอหลักฐาน ให้สอดคล้องกับหลักเกณฑ์ของกฎหมายที่ใช้บังคับ

ข้อ ๘. การบริหารจัดการด้านการบริการหรือการดำเนินงานของหน่วยงานหรือองค์กรเพื่อให้มีความต่อเนื่อง ให้มีการระบุเหตุการณ์ใด ๆ ที่อาจส่งผลให้การดำเนินงานหยุดชะงัก และความเป็นไปได้ในการเกิดผลกระทบ ตลอดจนผลต่อเนื่องจากการหยุดชะงักนั้นในแง่ของความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ ๙. การตรวจสอบและการประเมินผลการปฏิบัติตามนโยบาย มาตรการ หลักเกณฑ์ หรือกระบวนการใด ๆ รวมทั้งข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

๙.๑ กำหนดขั้นตอนปฏิบัติงานเพื่อให้มั่นใจว่าในการใช้งานข้อมูลที่อาจถือเป็นทรัพย์สินทางปัญญาหรือการใช้งานซอฟต์แวร์มีความสอดคล้องกับกฎหมายและข้อกำหนดตามสัญญาต่าง ๆ

๙.๒ ป้องกันมิให้ข้อมูลสารสนเทศที่สำคัญเกิดความเสียหาย สูญหายหรือถูกปลอมแปลง โดยให้สอดคล้องกับกฎหมาย ข้อกำหนดตามสัญญาต่าง ๆ ของหน่วยงาน และข้อกำหนดการให้บริการ

พระราชบัญญัติ
ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
พ.ศ. ๒๕๕๐

พระราชบัญญัติ

ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

พ.ศ. ๒๕๕๐

ภูมิพลอดุลยเดช ป.ร.

ให้ไว้ ณ วันที่ ๑๐ มิถุนายน พ.ศ. ๒๕๕๐

เป็นปีที่ ๖๒ ในรัชกาลปัจจุบัน

พระบาทสมเด็จพระปรมินทรมหาภูมิพลอดุลยเดช มีพระบรมราชโองการโปรดเกล้า ฯ ให้ประกาศว่า

โดยที่เป็นการสมควรมีกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

จึงทรงพระกรุณาโปรดเกล้า ฯ ให้ตราพระราชบัญญัติขึ้นไว้โดยคำแนะนำและยินยอมของสภานิติบัญญัติแห่งชาติ ดังต่อไปนี้

มาตรา ๑ พระราชบัญญัตินี้เรียกว่า “พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐”

มาตรา ๒ พระราชบัญญัตินี้ให้ใช้บังคับเมื่อพ้นกำหนดสามสิบวันนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

มาตรา ๓ ในพระราชบัญญัตินี้

“ระบบคอมพิวเตอร์” หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

"ข้อมูลคอมพิวเตอร์" หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

"ข้อมูลจราจรทางคอมพิวเตอร์" หมายความว่า ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

"ผู้ให้บริการ" หมายความว่า

(๑) ผู้ให้บริการแก่บุคคลอื่นในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น โดยผ่านทางระบบคอมพิวเตอร์ ทั้งนี้ ไม่ว่าจะเป็นการให้บริการในนามของตนเอง หรือในนามหรือเพื่อประโยชน์ของบุคคลอื่น

(๒) ผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลอื่น

"ผู้ใช้บริการ" หมายความว่า ผู้ใช้บริการของผู้ให้บริการไม่ว่าต้องเสียค่าใช้บริการหรือไม่ก็ตาม

"พนักงานเจ้าหน้าที่" หมายความว่า ผู้ซึ่งรัฐมนตรีแต่งตั้งให้ปฏิบัติการตามพระราชบัญญัตินี้

"รัฐมนตรี" หมายความว่า รัฐมนตรีผู้รักษาการตามพระราชบัญญัตินี้

มาตรา ๔ ให้รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารรักษาการตามพระราชบัญญัตินี้ และให้มีอำนาจออกกฎกระทรวงเพื่อปฏิบัติการตามพระราชบัญญัตินี้

กฎกระทรวงนั้น เมื่อได้ประกาศในราชกิจจานุเบกษาแล้วให้ใช้บังคับได้

หมวด ๑
ความผิดเกี่ยวกับคอมพิวเตอร์

มาตรา ๕ ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๖ ผู้ใดล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะถ้านำมาตรการดังกล่าวไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๗ ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินสองปีหรือปรับไม่เกินสี่หมื่นบาทหรือทั้งจำทั้งปรับ

มาตรา ๘ ผู้ใดกระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๙ ผู้ใดทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

มาตรา ๑๐ ผู้ใดกระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

มาตรา ๑๑ ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นโดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท

มาตรา ๑๒ ถ้าการกระทำความผิดตามมาตรา ๙ หรือมาตรา ๑๐

(๑) ก่อให้เกิดความเสียหายแก่ประชาชน ไม่ว่าความเสียหายนั้นจะเกิดขึ้นในทันทีหรือในภายหลังและไม่ว่าจะเกิดขึ้นพร้อมกันหรือไม่ ต้องระวางโทษจำคุกไม่เกินสิบปี และปรับไม่เกินสองแสนบาท

(๒) เป็นการกระทำโดยประการที่น่าจะเกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือการบริการสาธารณะ หรือเป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีไว้เพื่อประโยชน์สาธารณะ ต้องระวางโทษจำคุกตั้งแต่สามปีถึงสิบห้าปี และปรับตั้งแต่หกหมื่นบาทถึงสามแสนบาท

ถ้าการกระทำความผิดตาม (๒) เป็นเหตุให้ผู้อื่นถึงแก่ความตาย ต้องระวางโทษจำคุกตั้งแต่สิบปีถึงยี่สิบปี

มาตรา ๑๓ ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามมาตรา ๕ มาตรา ๖ มาตรา ๗ มาตรา ๘ มาตรา ๙ มาตรา ๑๐ หรือมาตรา ๑๑ ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๑๔ ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

(๑) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน

(๒) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศหรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

(๓) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

(๔) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันลามกและข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

(๕) เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ตาม (๑) (๒) (๓) หรือ (๔)

มาตรา ๑๕ ผู้ให้บริการผู้ใดจงใจสนับสนุนหรือยินยอมให้มีการกระทำความผิดตามมาตรา ๑๔ ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตามมาตรา ๑๔

มาตรา ๑๖ ผู้ใดนำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้ โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

ถ้าการกระทำตามวรรคหนึ่ง เป็นการนำเข้าข้อมูลคอมพิวเตอร์โดยสุจริต ผู้กระทำไม่มีความผิด

ความผิดตามวรรคหนึ่งเป็นความผิดอันยอมความได้

ถ้าผู้เสียหายในความผิดตามวรรคหนึ่งตายเสียก่อนร้องทุกข์ ให้บิดา มารดา คู่สมรส หรือบุตรของผู้เสียหายร้องทุกข์ได้ และให้ถือว่าเป็นผู้เสียหาย

มาตรา ๑๗ ผู้ใดกระทำความผิดตามพระราชบัญญัตินี้นอกราชอาณาจักรและ

(๑) ผู้กระทำความผิดนั้นเป็นคนไทย และรัฐบาลแห่งประเทศที่ความผิดได้เกิดขึ้นหรือผู้เสียหายได้ร้องขอให้ลงโทษ หรือ

(๒) ผู้กระทำความผิดนั้นเป็นคนต่างด้าว และรัฐบาลไทยหรือคนไทยเป็นผู้เสียหายและผู้เสียหายได้ร้องขอให้ลงโทษ

จะต้องรับโทษภายในราชอาณาจักร

หมวด ๒
พนักงานเจ้าหน้าที่

มาตรา ๑๘ ภายใต้บังคับมาตรา ๑๙ เพื่อประโยชน์ในการสืบสวนและสอบสวนในกรณีที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่มีอำนาจอย่างหนึ่งอย่างใด ดังต่อไปนี้ เฉพาะที่จำเป็นเพื่อประโยชน์ในการใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิดและหาตัวผู้กระทำความผิด

(๑) มีหนังสือสอบถามหรือเรียกบุคคลที่เกี่ยวข้องกับการกระทำความผิดตามพระราชบัญญัตินี้มาเพื่อให้ถ้อยคำ ส่งคำชี้แจงเป็นหนังสือ หรือส่งเอกสาร ข้อมูล หรือหลักฐานอื่นใดที่อยู่ในรูปแบบที่สามารถเข้าใจได้

(๒) เรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการเกี่ยวกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์หรือจากบุคคลอื่นที่เกี่ยวข้อง

(๓) สั่งให้ผู้ให้บริการส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการที่ต้องเก็บตามมาตรา ๒๖ หรือที่อยู่ในความครอบครองหรือควบคุมของผู้ให้บริการให้แก่พนักงานเจ้าหน้าที่

(๔) ทำสำเนาข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ จากระบบคอมพิวเตอร์ที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ ในกรณีที่ระบบคอมพิวเตอร์นั้นยังมิได้อยู่ในความครอบครองของพนักงานเจ้าหน้าที่

(๕) สั่งให้บุคคลซึ่งครอบครองหรือควบคุมข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ ส่งมอบข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ดังกล่าวให้แก่พนักงานเจ้าหน้าที่

(๖) ตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ของบุคคลใด อันเป็นหลักฐานหรืออาจใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิด หรือเพื่อสืบสวนหาตัวผู้กระทำความผิดและสั่งให้บุคคลนั้นส่งข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ ที่เกี่ยวข้องเท่าที่จำเป็นให้ด้วยก็ได้

(๗) ถอดรหัสลับของข้อมูลคอมพิวเตอร์ของบุคคลใด หรือสั่งให้บุคคลที่เกี่ยวข้องกับการเข้ารหัสลับของข้อมูลคอมพิวเตอร์ ทำการถอดรหัสลับ หรือให้ความร่วมมือกับพนักงานเจ้าหน้าที่ในการถอดรหัสลับดังกล่าว

(๘) ยึดหรืออายัดระบบคอมพิวเตอร์เท่าที่จำเป็นเฉพาะเพื่อประโยชน์ในการทราบรายละเอียดแห่งความผิดและผู้กระทำความผิดตามพระราชบัญญัตินี้

มาตรา ๑๙ การใช้อำนาจของพนักงานเจ้าหน้าที่ตามมาตรา ๑๘ (๔) (๕) (๖) (๗) และ (๘) ให้พนักงานเจ้าหน้าที่ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งอนุญาตให้พนักงานเจ้าหน้าที่ดำเนินการตามคำร้อง ทั้งนี้ คำร้องต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดกระทำหรือกำลังจะกระทำการอย่างหนึ่งอย่างใดอันเป็นความผิดตามพระราชบัญญัตินี้ เหตุที่ต้องใช้อำนาจ ลักษณะของการกระทำความผิด รายละเอียดเกี่ยวกับอุปกรณ์ที่ใช้ในการกระทำความผิดและผู้กระทำความผิด เท่าที่สามารถจะระบุได้ ประกอบคำร้องด้วยในการพิจารณาคำร้องให้ศาลพิจารณาคำร้องดังกล่าวโดยเร็ว

เมื่อศาลมีคำสั่งอนุญาตแล้ว ก่อนดำเนินการตามคำสั่งของศาล ให้พนักงานเจ้าหน้าที่ส่งสำเนาบันทึกเหตุอันควรเชื่อที่ทำให้ต้องใช้อำนาจตามมาตรา ๑๘ (๔) (๕) (๖) (๗) และ (๘) มอบให้เจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์นั้นไว้เป็นหลักฐาน แต่ถ้าไม่มีเจ้าของหรือผู้ครอบครองเครื่องคอมพิวเตอร์อยู่ ณ ที่นั้น ให้พนักงานเจ้าหน้าที่ส่งมอบสำเนาบันทึกนั้นให้แก่เจ้าของหรือผู้ครอบครองดังกล่าวในทันทีที่กระทำได้

ให้พนักงานเจ้าหน้าที่ผู้เป็นหัวหน้าในการดำเนินการตามมาตรา ๑๘ (๔) (๕) (๖) (๗) และ (๘) ส่งสำเนาบันทึกรายละเอียดการดำเนินการและเหตุผลแห่งการดำเนินการให้ศาลที่มีเขตอำนาจภายในสี่สิบแปดชั่วโมงนับแต่เวลาลงมือดำเนินการ เพื่อเป็นหลักฐาน

การทำสำเนาข้อมูลคอมพิวเตอร์ตามมาตรา ๑๘ (๔) ให้กระทำได้เฉพาะเมื่อมีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ และต้องไม่เป็นอุปสรรคในการดำเนินกิจการของเจ้าของหรือผู้ครอบครองข้อมูลคอมพิวเตอร์นั้นเกินความจำเป็น

การยึดหรืออายัดตามมาตรา ๑๘ (๘) นอกจากจะต้องส่งมอบสำเนาหนังสือแสดงการยึดหรืออายัดมอบให้เจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์นั้นไว้เป็นหลักฐานแล้วพนักงานเจ้าหน้าที่จะสั่งยึดหรืออายัดไว้เกินสามสิบวันมิได้ ในกรณีจำเป็นที่ต้องยึดหรืออายัดไว้นานกว่านั้น ให้ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อขอขยายเวลายึดหรืออายัดได้ แต่ศาลจะอนุญาตให้ขยายเวลาครั้งเดียวหรือหลายครั้งรวมกันได้อีกไม่เกินหกสิบวัน เมื่อหมดความจำเป็นที่จะยึดหรืออายัดหรือครบกำหนดเวลาดังกล่าวแล้ว พนักงานเจ้าหน้าที่ต้องส่งคืนระบบคอมพิวเตอร์ที่ยึดหรือถอนการอายัดโดยพลัน

หนังสือแสดงการยึดหรืออายัดตามวรรคห้าให้เป็นไปตามที่กำหนดในกฎกระทรวง

มาตรา ๒๐ ในกรณีที่การกระทำความผิดตามพระราชบัญญัตินี้เป็นการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ที่อาจกระทบกระเทือนต่อความมั่นคงแห่งราชอาณาจักรตามที่กำหนดไว้ในภาคสองลักษณะ ๑ หรือลักษณะ ๑/๑ แห่งประมวลกฎหมายอาญา หรือที่มีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน พนักงานเจ้าหน้าที่โดยได้รับความเห็นชอบจากรัฐมนตรีอาจยื่นคำร้องพร้อมแสดงพยานหลักฐานต่อศาลที่มีเขตอำนาจขอให้มีคำสั่งระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์นั้นได้

ในกรณีที่ศาลมีคำสั่งให้ระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ตามวรรคหนึ่ง ให้พนักงานเจ้าหน้าที่ทำการระงับการทำให้แพร่หลายนั้นเอง หรือสั่งให้ผู้ให้บริการระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์นั้นก็ได้

มาตรา ๒๑ ในกรณีที่พนักงานเจ้าหน้าที่พบว่า ข้อมูลคอมพิวเตอร์ใดมีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย พนักงานเจ้าหน้าที่อาจยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อขอให้มีคำสั่งห้ามจำหน่ายหรือเผยแพร่ หรือสั่งให้เจ้าของหรือผู้ครอบครองข้อมูลคอมพิวเตอร์นั้นระงับการใช้ ทำลายหรือแก้ไขข้อมูลคอมพิวเตอร์นั้นได้ หรือจะกำหนดเงื่อนไขในการใช้ มีไว้ในครอบครอง หรือเผยแพร่ชุดคำสั่งไม่พึงประสงค์ดังกล่าวก็ได้

ชุดคำสั่งไม่พึงประสงค์ตามวรรคหนึ่งหมายถึงชุดคำสั่งที่มีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้ หรือโดยประการอื่นตามที่กำหนดในกฎกระทรวง ทั้งนี้ เว้นแต่เป็นชุดคำสั่งที่มุ่งหมายในการป้องกันหรือแก้ไขชุดคำสั่งดังกล่าวข้างต้น ตามที่รัฐมนตรีประกาศในราชกิจจานุเบกษา

มาตรา ๒๒ ห้ามมิให้พนักงานเจ้าหน้าที่เปิดเผยหรือส่งมอบข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการ ที่ได้มาตามมาตรา ๑๘ ให้แก่บุคคลใด

ความในวรรคหนึ่งมิให้ใช้บังคับกับการกระทำเพื่อประโยชน์ในการดำเนินคดีกับผู้กระทำความผิดตามพระราชบัญญัตินี้ หรือเพื่อประโยชน์ในการดำเนินคดีกับพนักงานเจ้าหน้าที่เกี่ยวกับการใช้อำนาจหน้าที่โดยมิชอบ หรือเป็นการกระทำตามคำสั่งหรือที่ได้รับอนุญาตจากศาล

พนักงานเจ้าหน้าที่ผู้ใดฝ่าฝืนวรรคหนึ่งต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๒๓ พนักงานเจ้าหน้าที่ผู้ใดกระทำโดยประมาทเป็นเหตุให้ผู้อื่นล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการ ที่ได้มาตามมาตรา ๑๘ ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๒๔ ผู้ใดล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์หรือข้อมูลของผู้ใช้บริการ ที่พนักงานเจ้าหน้าที่ได้มาตามมาตรา ๑๘ และเปิดเผยข้อมูลนั้นต่อผู้หนึ่งผู้ใด ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๒๕ ข้อมูล ข้อมูลคอมพิวเตอร์ หรือข้อมูลจราจรทางคอมพิวเตอร์ที่พนักงานเจ้าหน้าที่ได้มาตามพระราชบัญญัตินี้ ให้อ้างและรับฟังเป็นพยานหลักฐานตามบทบัญญัติแห่งประมวลกฎหมายวิธีพิจารณาความอาญาหรือกฎหมายอื่นอันว่าด้วยการสืบพยานได้ แต่ต้องเป็นชนิดที่มิได้เกิดขึ้นจากการจูงใจ มีคำมั่นสัญญา ขู่เข็ญ หลอกลวง หรือโดยมิชอบประการอื่น

มาตรา ๒๖ ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็นพนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการผู้ใดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบวันแต่ไม่เกินหนึ่งปีเป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวก็ได้

ผู้ให้บริการจะต้องเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการนับตั้งแต่เริ่มใช้บริการและต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่าเก้าสิบวันนับตั้งแต่การใช้บริการสิ้นสุดลง

ความในวรรคหนึ่งจะใช้กับผู้ให้บริการประเภทใด อย่างไร และเมื่อใด ให้เป็นไปตามที่รัฐมนตรีประกาศในราชกิจจานุเบกษา

ผู้ให้บริการผู้ใดไม่ปฏิบัติตามมาตรานี้ ต้องระวางโทษปรับไม่เกินห้าแสนบาท

มาตรา ๒๗ ผู้ใดไม่ปฏิบัติตามคำสั่งของศาลหรือพนักงานเจ้าหน้าที่ที่สั่งตามมาตรา ๑๘ หรือมาตรา ๒๐ หรือไม่ปฏิบัติตามคำสั่งของศาลตามมาตรา ๒๑ ต้องระวางโทษปรับไม่เกินสองแสนบาท และปรับเป็นรายวันอีกไม่เกินวันละห้าพันบาทจนกว่าจะปฏิบัติให้ถูกต้อง

มาตรา ๒๘ การแต่งตั้งพนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้ ให้รัฐมนตรีแต่งตั้งจากผู้มีความรู้และความชำนาญเกี่ยวกับระบบคอมพิวเตอร์และมีคุณสมบัติตามที่รัฐมนตรีกำหนด

มาตรา ๒๙ ในการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่เป็นพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ตามประมวลกฎหมายวิธีพิจารณาความอาญามีอำนาจรับคำร้องทุกข์หรือรับคำกล่าวโทษ และมีอำนาจในการสืบสวนสอบสวนเฉพาะความผิดตามพระราชบัญญัตินี้

ในการจับ ควบคุม ค้น การทำสำนวนสอบสวนและดำเนินคดีผู้กระทำความผิดตามพระราชบัญญัตินี้ บรรดาที่เป็นอำนาจของพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ หรือพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา ให้พนักงานเจ้าหน้าที่ประสานงานกับพนักงานสอบสวนผู้รับผิดชอบเพื่อดำเนินการตามอำนาจหน้าที่ต่อไป

ให้นายกรัฐมนตรีในฐานะผู้กำกับดูแลสำนักงานตำรวจแห่งชาติและรัฐมนตรีมีอำนาจร่วมกันกำหนดระเบียบเกี่ยวกับแนวทางและวิธีปฏิบัติในการดำเนินการตามวรรคสอง

มาตรา ๓๐ ในการปฏิบัติหน้าที่ พนักงานเจ้าหน้าที่ต้องแสดงบัตรประจำตัวต่อบุคคลซึ่งเกี่ยวข้อง

บัตรประจำตัวของพนักงานเจ้าหน้าที่ให้เป็นไปตามแบบที่รัฐมนตรีประกาศในราชกิจจานุเบกษา

ผู้รับสนองพระบรมราชโองการ
พลเอก สุรยุทธ์ จุลานนท์
นายกรัฐมนตรี

หมายเหตุ :- เหตุผลในการประกาศใช้พระราชบัญญัติฉบับนี้ คือ เนื่องจากในปัจจุบันระบบคอมพิวเตอร์ได้เป็นส่วนสำคัญของการประกอบกิจการและการดำรงชีวิตของมนุษย์ หากมีผู้กระทำด้วยประการใด ๆ ให้ระบบคอมพิวเตอร์ไม่สามารถทำงานตามคำสั่งที่กำหนดไว้หรือทำให้การทำงานผิดพลาดไปจากคำสั่งที่กำหนดไว้ หรือใช้วิธีการใด ๆ เข้าล่วงรู้ข้อมูล แก้ไข หรือทำลายข้อมูลของบุคคลอื่นในระบบคอมพิวเตอร์โดยมิชอบ หรือใช้ระบบคอมพิวเตอร์เพื่อเผยแพร่ข้อมูลคอมพิวเตอร์อันเป็นเท็จหรือมีลักษณะอันลามกอนาจาร ย่อมก่อให้เกิดความเสียหาย กระทบกระเทือนต่อเศรษฐกิจ สังคม และความมั่นคงของรัฐ รวมทั้งความสงบสุขและศีลธรรมอันดีของประชาชน สมควรกำหนดมาตรการเพื่อป้องกันและปราบปรามการกระทำดังกล่าว จึงจำเป็นต้องตราพระราชบัญญัตินี้

กฎกระทรวงกำหนดแบบหนังสือ แสดงการยึดหรืออายัดระบบคอมพิวเตอร์ พ.ศ. ๒๕๕๑

กฎกระทรวง

กำหนดแบบหนังสือแสดงการยึดหรืออายัดระบบคอมพิวเตอร์

พ.ศ. ๒๕๕๑

อาศัยอำนาจตามความในมาตรา ๔ และมาตรา ๑๙ วรรคหก แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ อันเป็นกฎหมายที่มีบทบัญญัติบางประการเกี่ยวกับการจำกัดสิทธิและเสรีภาพของบุคคล ซึ่งมาตรา ๒๙ ประกอบกับมาตรา ๓๖ และมาตรา ๔๑ ของรัฐธรรมนูญแห่งราชอาณาจักรไทย บัญญัติให้กระทำได้โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมาย รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารออกกฎกระทรวงไว้ ดังต่อไปนี้

หนังสือแสดงการยึดหรืออายัดระบบคอมพิวเตอร์ให้เป็นไปตามแบบ ทก.ยค. ท้ายกฎกระทรวงนี้

ให้ไว้ ณ วันที่ ๒๗ มิถุนายน พ.ศ. ๒๕๕๑
มั่น พัธโนทัย
รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

ทก.ยค.

หนังสือแสดงการยึดหรืออายัดระบบคอมพิวเตอร์

เขียนที่ .....
วันที่ .....

ข้าพเจ้า ..... ตำแหน่ง .....
เลขที่บัตรประจำตัว ..... พนักงานเจ้าหน้าที่ผู้ซึ่งรัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร แต่งตั้งตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ พร้อมด้วยพนักงานฝ่ายปกครองหรือตำรวจ ดังต่อไปนี้
(๑) ..... ตำแหน่ง .....
(๒) ..... ตำแหน่ง .....
ได้ทำการยึดหรืออายัดระบบคอมพิวเตอร์ตามคำสั่งอนุญาตให้ทำการยึดหรืออายัดของศาล .....
เลขที่ ..... ลงวันที่ ..... เพื่อประโยชน์ในการทราบรายละเอียดแห่งความผิดและผู้กระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐
สถานที่ยึดหรืออายัดระบบคอมพิวเตอร์ บ้านเลขที่ ..... หมู่ที่ .....
ตรอก/ซอย ..... ถนน ..... ตำบล/แขวง .....
อำเภอ/เขต ..... จังหวัด .....

ในการดำเนินการยึดหรืออายัด เนื่องจากปรากฏว่ามีระบบคอมพิวเตอร์ที่เชื่อว่า .....
.....
.....
จึงได้ยึดหรืออายัดไปเพื่อดำเนินการตรวจสอบ ดังมีรายการแสดงชื่อและจำนวนของสิ่งที่ยึดหรืออายัดไว้ทั้งหมด ..... รายการ ตามบัญชีท้ายหนังสือนี้

บรรดาระบบคอมพิวเตอร์หรือหลักฐานที่ยึดหรืออายัดไปนี้ หากท่านประสงค์จะตรวจสอบเพื่อดำเนินกิจการของท่าน ขอให้ท่านติดต่อได้ที่ .....
.....

พนักงานเจ้าหน้าที่ได้สอบถามเจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์อย่างสุภาพ ไม่มีการข่มขู่ และมิได้ทำให้เกิดความเสียหายหรือบุบสลายซึ่งทรัพย์สินของบุคคลที่เกี่ยวข้องแต่ประการใด เจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์ได้อ่านข้อความในหนังสือฉบับนี้และเข้าใจข้อความดังกล่าวดีแล้ว จึงลงลายมือชื่อไว้เป็นหลักฐานรับรองว่าถูกต้องและเป็นความจริงต่อหน้าพนักงานเจ้าหน้าที่และพยานผู้เข้าร่วมยึดหรืออายัด ทั้งนี้ พนักงานเจ้าหน้าที่ได้มอบสำเนาหนังสือแสดงการยึดหรืออายัดนี้ให้เจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์แล้ว

ลงชื่อ ..... พนักงานเจ้าหน้าที่ผู้ยึดหรืออายัด
(.....)
ลงชื่อ ..... เจ้าของหรือผู้ครอบครอง
(.....)
ลงชื่อ ..... ผู้นำยึดหรืออายัด
(.....)
ลงชื่อ ..... พยานผู้เข้าร่วมยึดหรืออายัด
(.....)
ลงชื่อ ..... พยานผู้เข้าร่วมยึดหรืออายัด
(.....)
ลงชื่อ ..... พนักงานเจ้าหน้าที่ผู้บันทึก
(.....)

ทก.ยค.

บัญชีแสดงรายละเอียดการยึดหรืออายัดระบบคอมพิวเตอร์

บัญชีลำดับที่ ..... ยึดหรืออายัดเมื่อวันที่ ..... เวลา ..... ถึงเวลา .....
บ้านเลขที่ ..... หมู่ที่ ..... ตรอก/ซอย ..... ถนน .....
ตำบล/แขวง ..... อำเภอ/เขต ..... จังหวัด .....

พนักงานเจ้าหน้าที่ผู้ยึดหรืออายัด ..... เลขที่บัตรประจำตัว .....
โดยมี ..... เป็นผู้นำยึดหรืออายัด

ลำดับที่	รายการ	จำนวน	เจ้าของ / ผู้ครอบครอง	หมายเหตุ

และตามบัญชีรายละเอียดระบบคอมพิวเตอร์ที่ยึดหรืออายัด ต่อท้ายบัญชีนี้อีก ..... รายการ

ทก.ยค.

บัญชีรายละเอียดระบบคอมพิวเตอร์ที่ยึดหรืออายัด

(ต่อท้ายบัญชีแสดงรายละเอียดการยึดหรืออายัดระบบคอมพิวเตอร์)

1. ประเภทอุปกรณ์คอมพิวเตอร์ที่ยึดหรืออายัด มีจำนวนทั้งหมด ..... เครื่อง ได้แก่

1.1 ชนิด ..... ยี่ห้อ .....

รุ่น (model) ..... หมายเลขเครื่อง(S/N) .....

Case Type: □ Mini Tower □ Mid Tower □ Full Tower □ อื่นๆ .....

หรือมีเอกลักษณะเป็น □ PC Stand-alone □ Server ..... □ Client

□ Workstation □ Mainframe □ อื่นๆ .....

ติดตั้งอยู่บริเวณ.....

มี Drives ดังนี้

Floppy drive(s) ขนาด $5\frac{1}{4}$ นิ้ว ..... Floppy drive(s) ขนาด $3\frac{1}{2}$นิ้ว ..... Zip drive(s) .....

Jazz drive(s) ..... Tape drive(s) ..... Speakers .....

CD-ROM drive(s) ..... CD-ROM types ..... Parallel port(s) .....

Serial port(s) ..... USB port(s) ..... Sound card/port .....

Modem card/port .....Video card/port ..... External SCSI card/port..... .

NIC card/port .....

Monitor .....

Printer .....

อุปกรณ์เพิ่มเติมอื่นๆ .....

1.2 ชนิด ..... ยี่ห้อ .....

รุ่น (model) ..... หมายเลขเครื่อง(S/N) .....

Case Type: □ Mini Tower □ Mid Tower □ Full Tower □ อื่นๆ .....

หรือมีเอกลักษณะเป็น □ PC Stand-alone □ Server ..... □ Client

□ Workstation □ Mainframe □ อื่นๆ .....

ติดตั้งอยู่บริเวณ.....

มี Drives ดังนี้

Floppy drive(s) ขนาด $5\frac{1}{4}$ นิ้ว ..... Floppy drive(s) ขนาด $3\frac{1}{2}$นิ้ว ..... Zip drive(s) .....

Jazz drive(s) ..... Tape drive(s) ..... Speakers .....

CD-ROM drive(s) ..... CD-ROM types ..... Parallel port(s) .....

Serial port(s) ..... USB port(s) ..... Sound card/port .....

Modem card/port .....Video card/port ..... External SCSI card/port..... .

NIC card/port .....

Monitor .....

Printer .....

อุปกรณ์เพิ่มเติมอื่นๆ .....

ทก.ยค.

1.3 ชนิด ..... ยี่ห้อ .....
รุ่น (model) ..... หมายเลขเครื่อง(S/N) .....
Case Type: □ Mini Tower □ Mid Tower □ Full Tower □ อื่นๆ .....
หรือมีเอกลักษณะเป็น □ PC Stand-alone □ Server ..... □ Client
□ Workstation □ Mainframe □ อื่นๆ .....
ติดตั้งอยู่บริเวณ.....
มี Drives ดังนี้
Floppy drive(s) ขนาด $5\frac{1}{4}$ นิ้ว ..... Floppy drive(s) ขนาด $3\frac{1}{2}$นิ้ว ..... Zip drive(s) .....
Jazz drive(s) ..... Tape drive(s) ..... Speakers .....
CD-ROM drive(s) ..... CD-ROM types ..... Parallel port(s) .....
Serial port(s) ..... USB port(s) ..... Sound card/port .....
Modem card/port .....Video card/port ..... External SCSI card/port..... .
NIC card/port .....
Monitor .....
Printer .....
อุปกรณ์เพิ่มเติมอื่นๆ .....

1.4 ชนิด ..... ยี่ห้อ .....
รุ่น (model) ..... หมายเลขเครื่อง(S/N) .....
Case Type: □ Mini Tower □ Mid Tower □ Full Tower □ อื่นๆ .....
หรือมีเอกลักษณะเป็น □ PC Stand-alone □ Server ..... □ Client
□ Workstation □ Mainframe □ อื่นๆ .....
ติดตั้งอยู่บริเวณ.....
มี Drives ดังนี้
Floppy drive(s) ขนาด $5\frac{1}{4}$ นิ้ว ..... Floppy drive(s) ขนาด $3\frac{1}{2}$นิ้ว ..... Zip drive(s) .....
Jazz drive(s) ..... Tape drive(s) ..... Speakers .....
CD-ROM drive(s) ..... CD-ROM types ..... Parallel port(s) .....
Serial port(s) ..... USB port(s) ..... Sound card/port .....
Modem card/port .....Video card/port ..... External SCSI card/port..... .
NIC card/port .....
Monitor .....
Printer .....
อุปกรณ์เพิ่มเติมอื่นๆ .....

2. .....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

หมายเหตุ :- เหตุผลในการประกาศใช้กฎกระทรวงฉบับนี้ คือ โดยที่มาตรา ๑๙ วรรคหก แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ บัญญัติให้หนังสือแสดงการยึดหรืออายัดระบบคอมพิวเตอร์เป็นไปตามที่กำหนดในกฎกระทรวง จึงจำเป็นต้องออกกฎกระทรวงนี้

ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจร
ทางคอมพิวเตอร์ของผู้ให้บริการ
พ.ศ. ๒๕๕๐

ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ

พ.ศ. ๒๕๕๐

ด้วยในปัจจุบันการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์หรือระบบอิเล็กทรอนิกส์เริ่มเข้าไปมีบทบาทและทวีความสำคัญเพิ่มขึ้นตามลำดับต่อระบบเศรษฐกิจและคุณภาพชีวิตของประชาชน แต่ในขณะเดียวกันการกระทำความผิดเกี่ยวกับคอมพิวเตอร์มีแนวโน้มขยายวงกว้าง และทวีความรุนแรงเพิ่มมากขึ้น ข้อมูลจราจรทางคอมพิวเตอร์นับเป็นพยานหลักฐานสำคัญในการดำเนินคดีอันเป็นประโยชน์อย่างยิ่งต่อการสืบสวน สอบสวน เพื่อนำตัวผู้กระทำความผิดมาลงโทษ จึงสมควรกำหนดให้ผู้ให้บริการมีหน้าที่ในการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ดังกล่าว

อาศัยอำนาจตามความในมาตรา ๒๖ วรรค ๓ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ดังนั้น รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร จึงได้กำหนดหลักเกณฑ์ไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๕๐”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ให้รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารรักษาการตามประกาศนี้

ข้อ ๔ ในประกาศนี้

“ผู้ให้บริการ” หมายความว่า

(๑) ผู้ให้บริการแก่บุคคลอื่นในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น โดยผ่านทางระบบคอมพิวเตอร์ ทั้งนี้ ไม่ว่าจะเป็นการให้บริการในนามของตนเองหรือเพื่อประโยชน์ของบุคคลอื่น

(๒) ผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลอื่น

“ข้อมูลจราจรทางคอมพิวเตอร์” หมายความว่า ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

"ระบบคอมพิวเตอร์" หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนด คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

"ผู้ใช้บริการ" หมายความว่า ผู้ใช้บริการของผู้ให้บริการไม่ว่าต้องเสียค่าใช้บริการหรือไม่ก็ตาม

ข้อ ๕ ภายใต้บังคับของมาตรา ๒๖ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ประเภทของผู้ให้บริการซึ่งมีหน้าที่ต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์แบ่งได้ ดังนี้

(๑) ผู้ให้บริการแก่บุคคลทั่วไปในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น ทั้งนี้ โดยผ่านทางระบบคอมพิวเตอร์ ไม่ว่าจะเป็นการให้บริการในนามของตนเองหรือเพื่อประโยชน์ของบุคคลอื่น สามารถจำแนกได้ ๔ ประเภท ดังนี้

ก. ผู้ประกอบกิจการโทรคมนาคมและการกระจายภาพและเสียง (Telecommunication and Broadcast Carrier) ประกอบด้วยผู้ให้บริการดังปรากฏตามภาคผนวก ก. แนบท้ายประกาศนี้

ข. ผู้ให้บริการการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ (Access Service Provider) ประกอบด้วยผู้ให้บริการดังปรากฏตามภาคผนวก ก. แนบท้ายประกาศนี้

ค. ผู้ให้บริการเช่าระบบคอมพิวเตอร์ หรือให้เช่าบริการโปรแกรมประยุกต์ต่าง ๆ (Host Service Provider) ประกอบด้วยผู้ให้บริการดังปรากฏตามภาคผนวก ก. แนบท้ายประกาศนี้

ง. ผู้ให้บริการร้านอินเทอร์เน็ต ดังปรากฏตามภาคผนวก ก. แนบท้ายประกาศนี้

(๒) ผู้ให้บริการในการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลตาม (๑) (Content Service Provider) เช่น ผู้ให้บริการข้อมูลคอมพิวเตอร์ผ่านแอพพลิเคชั่นต่าง ๆ (Application Service Provider) ประกอบด้วยผู้ให้บริการดังภาคผนวก ก. แนบท้ายประกาศนี้

ข้อ ๖ ข้อมูลจราจรทางคอมพิวเตอร์ที่ผู้ให้บริการต้องเก็บรักษา ปรากฏดังภาคผนวก ข. แนบท้ายประกาศนี้

ข้อ ๗ ผู้ให้บริการมีหน้าที่เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ดังนี้

(๑) ผู้ให้บริการตามข้อ ๕ (๑) ก. มีหน้าที่เก็บข้อมูลจราจรทางคอมพิวเตอร์ตามภาคผนวก ข. ๑

(๒) ผู้ให้บริการตามข้อ ๕ (๑) ข. มีหน้าที่เก็บข้อมูลจราจรทางคอมพิวเตอร์ตามภาคผนวก ข. ๒

ตามประเภท ชนิดและหน้าที่การให้บริการ

(๓) ผู้ให้บริการตามข้อ ๕ (๑) ค. มีหน้าที่เก็บข้อมูลจราจรทางคอมพิวเตอร์ตามภาคผนวก ข. ๒ ตามประเภท ชนิดและหน้าที่การให้บริการ

(๔) ผู้ให้บริการตามข้อ ๕ (๑) ง. มีหน้าที่เก็บข้อมูลจราจรทางคอมพิวเตอร์ตามภาคผนวก ข. ๓

(๕) ผู้ให้บริการตามข้อ ๕ (๒) มีหน้าที่เก็บข้อมูลจราจรทางคอมพิวเตอร์ตามภาคผนวก ข. ๔

ทั้งนี้ ในการเก็บรักษาข้อมูลจราจรตามภาคผนวกต่าง ๆ ที่กล่าวไปข้างต้นนั้น ให้ผู้ให้บริการเก็บเพียงเฉพาะในส่วนที่เป็นข้อมูลจราจรที่เกิดจากส่วนที่เกี่ยวข้องกับบริการของตนเท่านั้น

ข้อ ๘ การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ผู้ให้บริการต้องใช้วิธีการที่มั่นคงปลอดภัย ดังต่อไปนี้

(๑) เก็บในสื่อ (Media) ที่สามารถรักษาความครบถ้วนถูกต้องแท้จริง (Integrity) และระบุตัวบุคคล (Identification) ที่เข้าถึงสื่อดังกล่าวได้

(๒) มีระบบการเก็บรักษาความลับของข้อมูลที่จัดเก็บ และกำหนดชั้นความลับในการเข้าถึงข้อมูลดังกล่าว เพื่อรักษาความน่าเชื่อถือของข้อมูล และไม่ให้ผู้ดูแลระบบสามารถแก้ไขข้อมูลที่เก็บรักษาไว้ เช่น การเก็บไว้ใน Centralized Log Server หรือการทำ Data Archiving หรือทำ Data Hashing เป็นต้น เว้นแต่ ผู้มีหน้าที่เกี่ยวข้องที่เจ้าของหรือผู้บริหารองค์กร กำหนดให้สามารถเข้าถึงข้อมูลดังกล่าวได้ เช่น ผู้ตรวจสอบระบบสารสนเทศขององค์กร (IT Auditor) หรือบุคคลที่องค์กรมอบหมาย เป็นต้น รวมทั้งพนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้

(๓) จัดให้มีผู้มีหน้าที่ประสานงานและให้ข้อมูลกับพนักงานเจ้าหน้าที่ซึ่งได้รับการแต่งตั้งตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ เพื่อให้การส่งมอบข้อมูลนั้น เป็นไปด้วยความรวดเร็ว

(๔) ในการเก็บข้อมูลจราจรนั้น ต้องสามารถระบุรายละเอียดผู้ใช้บริการเป็นรายบุคคลได้ (Identification and Authentication) เช่น ลักษณะการใช้บริการ Proxy Server, Network Address Translation (NAT) หรือ Proxy Cache หรือ Cache Engine หรือบริการ Free Internet หรือ บริการ 1222 หรือ Wi-Fi Hotspot ต้องสามารถระบุตัวตนของผู้ใช้บริการเป็นรายบุคคลได้จริง

(๕) ในกรณีที่ผู้ให้บริการประเภทหนึ่งประเภทใด ในข้อ ๑ ถึงข้อ ๔ ข้างต้น ได้ให้บริการในนามตนเอง แต่บริการดังกล่าวเป็นบริการที่ใช้ระบบของผู้ให้บริการซึ่งเป็นบุคคลที่สาม เป็นเหตุให้ผู้ให้บริการในข้อ ๑ ถึงข้อ ๔ ไม่สามารถรู้ได้ว่า ผู้ใช้บริการที่เข้ามาในระบบนั้นเป็นใคร ผู้ให้บริการ

เช่นว่านั้นต้องดำเนินการให้มีวิธีการระบุและยืนยันตัวบุคคล (Identification and Authentication) ของผู้ใช้บริการผ่านบริการของตนเองด้วย

ข้อ ๙ เพื่อให้ข้อมูลจราจรมีความถูกต้องและนำมาใช้ประโยชน์ได้จริงผู้ให้บริการต้องตั้งนาฬิกาของอุปกรณ์บริการทุกชนิดให้ตรงกับเวลาอ้างอิงสากล (Stratum 0) โดยผิดพลาดไม่เกิน ๑๐ มิลลิวินาที

ข้อ ๑๐ ผู้ให้บริการซึ่งมีหน้าที่เก็บข้อมูลจราจรทางคอมพิวเตอร์ตามข้อ ๗ เริ่มเก็บข้อมูลดังกล่าวตามลำดับ ดังนี้

(๑) ผู้ให้บริการตามข้อ ๕ (๑) ก. เริ่มเก็บข้อมูลจราจรทางคอมพิวเตอร์เมื่อพ้นสามสิบวันนับจากวันประกาศในราชกิจจานุเบกษา

(๒) ให้ผู้ให้บริการตามข้อ ๕ (๑) ข. เฉพาะผู้ให้บริการเครือข่ายสาธารณะหรือผู้ให้บริการอินเทอร์เน็ต (ISP) เริ่มเก็บข้อมูลจราจรทางคอมพิวเตอร์เมื่อพ้นหนึ่งร้อยแปดสิบวันนับจากวันประกาศในราชกิจจานุเบกษา

ผู้ให้บริการอื่นนอกจากที่กล่าวมาในข้อ ๑๐ (๑) และข้อ ๑๐ (๒) ข้างต้น ให้เริ่มเก็บข้อมูลจราจรทางคอมพิวเตอร์เมื่อพ้นหนึ่งปีนับจากวันประกาศในราชกิจจานุเบกษา

ประกาศ ณ วันที่ ๒๑ สิงหาคม พ.ศ. ๒๕๕๐
สิทธิชัย โภไคยอุดม
รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

ภาคผนวก ก

แนบท้ายประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ

พ.ศ. ๒๕๕๐

.....

๑. ผู้ให้บริการแก่บุคคลทั่วไปในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น โดยผ่านทางระบบคอมพิวเตอร์ ไม่ว่าจะเป็นการให้บริการในนามของตนเองหรือเพื่อประโยชน์ของบุคคลอื่น ตามข้อ ๕ (๑) จำแนกได้ ๔ ประเภท ดังนี้

ประเภท	ตัวอย่างของผู้ให้บริการ
ก.ผู้ประกอบกิจการโทรคมนาคมและกิจการกระจายภาพและเสียง (Telecommunication and Broadcast Carrier)	๑) ผู้ให้บริการโทรศัพท์พื้นฐาน (Fixed Line Service Provider) ๒) ผู้ให้บริการโทรศัพท์เคลื่อนที่ (Mobile Service Provider) ๓) ผู้ให้บริการวงจรเช่า (Leased Circuit Service Provider) เช่น ผู้ให้บริการ Leased Line, ผู้ให้บริการสายเช่า Fiber Optic, ผู้ให้บริการ ADSL (Asymmetric Digital Subscriber Line), ผู้ให้บริการ Frame Relay, ผู้ให้บริการ ATM (Asynchronous Transfer Mode), ผู้ให้บริการ MPLS (Multi Protocol Label Switching) เป็นต้น เว้นแต่ผู้ให้บริการนั้นให้บริการแต่เพียง Physical Media หรือสายสัญญาณอย่างเดียว (Cabling) เท่านั้น (เช่น ผู้ให้บริการ Dark Fiber, ผู้ให้บริการสายใยแก้วนำแสง ซึ่งอาจไม่มีสัญญาน Internet หรือไม่มี IP Traffic) ๔) ผู้ให้บริการดาวเทียม (Satellite Service Provider)

ประเภท	ตัวอย่างของผู้ให้บริการ
ข.ผู้ให้บริการการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ (Access Service Provider)	๑) ผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider) ทั้งมีสายและไร้สาย ๒) ผู้ประกอบการซึ่งให้บริการในการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ในห้องพัก ห้องเช่า โรงแรม หรือร้านอาหารและเครื่องดื่ม ในแต่ละกลุ่มอย่างหนึ่งอย่างใด ๓) ผู้ให้บริการเข้าถึงระบบเครือข่ายคอมพิวเตอร์สำหรับองค์กร เช่น หน่วยงานราชการ บริษัทหรือ สถาบันการศึกษา
ค.ผู้ให้บริการเช่าระบบคอมพิวเตอร์เพื่อให้บริการโปรแกรมประยุกต์ต่างๆ (Hosting Service Provider)	๑) ผู้ให้บริการเช่าระบบคอมพิวเตอร์ (Web Hosting),การให้บริการเช่า Web Server ๒) ผู้ให้บริการแลกเปลี่ยนแฟ้มข้อมูล (File Server หรือ File Sharing) ๓) ผู้ให้บริการการเข้าถึงจดหมายอิเล็กทรอนิกส์ (Mail Server Service Provider) ๔) ผู้ให้บริการศูนย์รับฝากข้อมูลทางอินเทอร์เน็ต (Internet Data Center)
ง.ผู้ให้บริการร้านอินเทอร์เน็ต	๑.ผู้ให้บริการร้านอินเทอร์เน็ต (Internet Café) ๒.ผู้ให้บริการร้านเกมออนไลน์ (Game Online)

๒. ผู้ให้บริการในการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลตาม ข้อ ๕ (๒) ประกอบด้วยผู้ให้บริการดังภาคผนวก ก แนบท้ายประกาศนี้

ประเภท	ตัวอย่างของผู้ให้บริการ
ผู้ให้บริการข้อมูลคอมพิวเตอร์ผ่านแอพพลิเคชั่นต่างๆ (Content and Application Service Provider)	๑) ผู้ให้บริการเว็บบอร์ด (Web board) หรือ ผู้ให้บริการบล็อค (Blog) ๒) ผู้ให้บริการการทำธุรกรรมทางการเงินทางอินเทอร์เน็ต (Internet Banking) และผู้ให้บริการชำระเงินทางอิเล็กทรอนิกส์ (Electronic Payment Service Provider) ๓) ผู้ให้บริการเว็บเซอร์วิส (Web Services) ๔) ผู้ให้บริการพาณิชย์อิเล็กทรอนิกส์ (e-Commerce) หรือ ธุรกรรมทางอิเล็กทรอนิกส์ (e-Transactions)

ภาคผนวก ข
แนบท้ายประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ
พ.ศ. ๒๕๕๐

.....

๑.ข้อมูลจราจรทางคอมพิวเตอร์ซึ่งผู้ให้บริการตามประกาศข้อ ๕ (๑) ก. มีหน้าที่ต้องเก็บรักษา มีดังต่อไปนี้

ประเภท	รายการ
ก.ข้อมูลที่สามารถระบุและติดตามถึงแหล่งกำเนิด ต้นทาง ปลายทาง และทางสายที่ผ่านของการติดต่อสื่อสารของระบบคอมพิวเตอร์	-ข้อมูลระบบชุมสายโทรศัพท์พื้นฐาน โทรศัพท์วิทยุมือถือ และระบบตู้โทรศัพท์สาขา (Fixed Network Telephony and Mobile Telephony)
	-หมายเลขโทรศัพท์ หรือ เลขหมายวงจร รวมทั้งบริการเสริมอื่นๆ เช่น บริการโอนสาย และหมายเลขโทรศัพท์ที่ได้โอนสาย รวมทั้งหมายเลขโทรศัพท์ซึ่งถูกเรียกจากโทรศัพท์ที่มีการโอน
	-ชื่อ ที่อยู่ของผู้ใช้บริการหรือผู้ใช้งานที่ลงทะเบียน (Name and Address of Subscriber or Registered User)
	- ข้อมูลเกี่ยวกับวันที่, เวลา และที่ตั้งของ Cell ID ซึ่งมีการใช้บริการ (Date and Time of the Initial Activation of the Service and the Location Label (Cell ID))
ข.ข้อมูลที่สามารถระบุวันที่ เวลา และระยะเวลาของการติดต่อสื่อสารของระบบคอมพิวเตอร์	วันที่ รวมทั้งเวลาเริ่มต้นและสิ้นสุดของการใช้งาน (Fixed Network Telephony and Mobile Telephony, the Date and Time of the Start and End of the Communication)
ค.ข้อมูลซึ่งสามารถระบุที่ตั้งในการใช้โทรศัพท์มือถือ หรืออุปกรณ์ติดต่อสื่อสารแบบไร้สาย (Mobile Communication Equipment)	๑) ที่ตั้ง label ในการเชื่อมต่อ (Cell ID) ณ สถานที่เริ่มติดต่อสื่อสาร
	๒) ข้อมูลซึ่งระบุที่ตั้งทางกายภาพของโทรศัพท์มือถืออันเชื่อมโยงกับข้อมูลที่ตั้งของ Cell ID ขณะที่มีการติดต่อสื่อสาร
	๓) จัดให้มีระบบบริการตรวจสอบบุคคลผู้ใช้บริการ

๒.ข้อมูลจราจรทางคอมพิวเตอร์ซึ่งผู้ให้บริการตามประกาศข้อ ๕ (๑) ข. ถึง ค. มีหน้าที่ต้องเก็บรักษา มีดังต่อไปนี้

ประเภท	รายการ
ก. ข้อมูลอินเทอร์เน็ตที่เกิดจากการเข้าถึงระบบเครือข่าย	๑) ข้อมูล Log ที่มีการบันทึกไว้เมื่อมีการเข้าถึงระบบเครือข่าย ซึ่งระบุถึงตัวตนและสิทธิในการเข้าถึงเครือข่าย (Access Logs Specific to Authentication and Authorization Servers เช่น TACACS (Terminal Access Controller Access-Control System) or RADIUS (Remote Authentication Dial-In User Service) or DIAMETER (Used to Control Access to IP Routers or Network Access Servers)
	๒) ข้อมูลเกี่ยวกับวัน และเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ (Date and Time of Connection of Client to Server)
	๓) ข้อมูลเกี่ยวกับชื่อที่ระบุตัวตนผู้ใช้ (User ID)
	๔) ข้อมูลหมายเลขชุดอินเทอร์เน็ตที่ถูกกำหนดให้โดยระบบผู้ให้บริการ (Assigned IP Address)
	๕) ข้อมูลที่บอกถึงหมายเลขสายที่เรียกเข้ามา (Calling Line Identification)
ข. ข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการจดหมายอิเล็กทรอนิกส์ (e-mail servers)	๑) ข้อมูล Log ที่บันทึกไว้เมื่อเข้าถึงเครื่องให้บริการไปรษณีย์อิเล็กทรอนิกส์ (Simple Mail Transfer Protocol : SMTP Log) ซึ่งได้แก่ - ข้อมูลหมายเลขของข้อความที่ระบุในจดหมายอิเล็กทรอนิกส์ (Message ID) -ข้อมูลชื่อที่อยู่อิเล็กทรอนิกส์ของผู้ส่ง (Sender E-mail Address) - ข้อมูลชื่อที่อยู่อิเล็กทรอนิกส์ของผู้รับ (Receiver E-mail Address - ข้อมูลที่บอกถึงสถานะในการตรวจสอบ (Status Indicator) ซึ่งได้แก่ จดหมายอิเล็กทรอนิกส์ที่ส่งสำเร็จ จดหมายอิเล็กทรอนิกส์ที่ส่งคืน จดหมายอิเล็กทรอนิกส์ที่มีการส่งล่าช้า เป็นต้น
	๒) ข้อมูลหมายเลขชุดอินเทอร์เน็ตของเครื่องคอมพิวเตอร์ผู้ใช้บริการที่เชื่อมต่ออยู่ขณะเข้ามาใช้บริการ (IP Address of

ประเภท	รายการ
	Client Connected to Server)
	๓) ข้อมูลวัน และเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ (Date and time of connection of Client Connected to server)
	๔) ข้อมูลหมายเลขชุดอินเทอร์เน็ตของเครื่องบริการจดหมายอิเล็กทรอนิกส์ ที่ถูกเชื่อมต่ออยู่ในขณะนั้น (IP Address of Sending Computer)
	๕) ชื่อผู้ใช้งาน (User ID) (ถ้ามี)
	๖) ข้อมูลที่บันทึกการเข้าถึงข้อมูลจดหมายอิเล็กทรอนิกส์ ผ่านโปรแกรมจัดการจากเครื่องของสมาชิก หรือการเข้าถึงเพื่อเรียกข้อมูลจดหมายอิเล็กทรอนิกส์ไปยังเครื่องสมาชิก โดยยังคงจัดเก็บข้อมูลที่บันทึกการเข้าถึงข้อมูลจดหมายอิเล็กทรอนิกส์ที่ดึงไปนั้น ไว้ที่เครื่องให้บริการ (POP3 (Post Office Protocol version 3) Log or IMAP4 (Internet Message Access Protocol Version 4) Log)
ค. ข้อมูลอินเทอร์เน็ตจากการโอนแฟ้มข้อมูลบนเครื่องให้บริการโอนแฟ้มข้อมูล	๑) ข้อมูล Log ที่บันทึกเมื่อมีการเข้าถึงเครื่องให้บริการโอนแฟ้มข้อมูล
	๒) ข้อมูลวัน และเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ (Date and Time of Connection of Client to Server)
	๓) ข้อมูลหมายเลขชุดอินเทอร์เน็ตของเครื่องคอมพิวเตอร์ผู้เข้าใช้ที่เชื่อมต่ออยู่ในขณะนั้น (IP Source Address)
	๔) ข้อมูลชื่อผู้ใช้งาน (User ID) (ถ้ามี)
	๕) ข้อมูลตำแหน่ง (Path) และ ชื่อไฟล์ที่อยู่บนเครื่องให้บริการโอนถ่ายข้อมูลที่มีการ ส่งขึ้นมาบันทึก หรือให้ดึงข้อมูลออกไป (Path and Filename of Data Object Uploaded or Downloaded)
ง. ข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการเว็บ	๑) ข้อมูล Log ที่บันทึกเมื่อมีการเข้าถึงเครื่องผู้ให้บริการเว็บ
	๒) ข้อมูลวัน และเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ
	๓) ข้อมูลหมายเลขชุดอินเทอร์เน็ตของเครื่องคอมพิวเตอร์ผู้เข้าใช้ที่เชื่อมต่ออยู่ในขณะนั้น
	๔) ข้อมูลคำสั่งการใช้งานระบบ

ประเภท	รายการ
	๕) ข้อมูลที่บ่งบอกถึงเส้นทางในการเรียกดูข้อมูล (URI: Uniform Resource Identifier) เช่น ตำแหน่งของเว็บเพ็จ
จ. ชนิดของข้อมูลบนเครือข่ายคอมพิวเตอร์ขนาดใหญ่ (Usenet)	๑) ข้อมูล Log ที่บันทึกเมื่อมีการเข้าถึงเครือข่าย (NNTP (Network News Transfer Protocol) Log)
	๒) ข้อมูลวัน และเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ (Date and Time of Connection of Client to Server)
	๓) ข้อมูลหมายเลข Port ในการใช้งาน (Protocol Process ID)
	๔) ข้อมูลชื่อเครื่องให้บริการ (Host Name)
	๕) ข้อมูลหมายเลขลำดับข้อความที่ได้ถูกส่งไปแล้ว (Posted Message ID)
ฉ. ข้อมูลที่เกิดจากการโต้ตอบกันบนเครือข่ายอินเทอร์เน็ต เช่น Internet Relay Chat (IRC) หรือ Instance Messaging (IM) เป็นต้น	ข้อมูล Log เช่น ข้อมูลเกี่ยวกับวัน เวลาการติดต่อของผู้ใช้บริการ (Date and Time of Connection of Client to Server) และ ข้อมูลชื่อเครื่องบนเครือข่าย และ หมายเลขเครื่องของผู้ให้บริการที่เครื่องคอมพิวเตอร์เชื่อมต่ออยู่ในขณะนั้น (Hostname and IP Address) เป็นต้น

๓.ข้อมูลจราจรทางคอมพิวเตอร์ซึ่งผู้ให้บริการตามประกาศข้อ ๕ (๑) ง. มีหน้าที่ต้องเก็บรักษา มีดังต่อไปนี้

ประเภท	รายการ
ก. ผู้ให้บริการร้านอินเทอร์เน็ต	๑) ข้อมูลที่สามารถระบุตัวบุคคล ๒) เวลาของการเข้าใช้ และเลิกใช้บริการ ๓) หมายเลขเครื่องที่ใช้ IP Address (Internet Protocol address)

๔.ข้อมูลจราจรทางคอมพิวเตอร์ซึ่งผู้ให้บริการตามประกาศข้อ ๕ (๒) มีหน้าที่ต้องเก็บรักษา มีดังต่อไปนี้

ประเภท	รายการ
ก. ข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์ (Content Service Provider)	๑) ข้อมูลรหัสประจำตัวผู้ใช้หรือข้อมูลที่สามารถระบุตัวผู้ใช้บริการได้ หรือ เลขประจำตัว (User ID) ของผู้ขายสินค้าหรือบริการ หรือ เลขประจำตัวผู้ใช้บริการ (User ID) และ ที่อยู่จดหมายอิเล็กทรอนิกส์ของผู้ใช้บริการ
	๒) บันทึกข้อมูลการเข้าใช้บริการ
	๓) กรณีผู้ให้บริการเว็บบอร์ด (Web board) หรือผู้ให้บริการบล็อค (Blog) ให้เก็บข้อมูลของผู้ประกาศ (Post) ข้อมูล

ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
เรื่อง หลักเกณฑ์เกี่ยวกับคุณสมบัติ
ของพนักงานเจ้าหน้าที่ตามพระราชบัญญัติ
ว่าด้วยการกระทำความผิดเกี่ยวกับ
คอมพิวเตอร์ พ.ศ. ๒๕๕๐

ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

เรื่อง หลักเกณฑ์เกี่ยวกับคุณสมบัติของพนักงานเจ้าหน้าที่
ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
พ.ศ. ๒๕๕๐

เพื่อให้การแต่งตั้งพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ มีความชัดเจนและเป็นไปอย่างมีประสิทธิภาพ

อาศัยอำนาจตามความในมาตรา ๒๘ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร จึงได้กำหนดหลักเกณฑ์เกี่ยวกับคุณสมบัติของพนักงานเจ้าหน้าที่ ดังต่อไปนี้

ข้อ ๑ ในประกาศนี้

“พนักงานเจ้าหน้าที่” หมายความว่า ผู้ซึ่งรัฐมนตรีแต่งตั้งให้ปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

“รัฐมนตรี” หมายความว่า รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

ข้อ ๒ พนักงานเจ้าหน้าที่ ต้องมีคุณสมบัติ ดังต่อไปนี้

(๑) มีความรู้และความชำนาญเกี่ยวกับระบบคอมพิวเตอร์

(๒) สำเร็จการศึกษาไม่น้อยกว่าระดับปริญญาตรีทางวิศวกรรมศาสตร์ วิทยาศาสตร์ วิทยาการคอมพิวเตอร์ เทคโนโลยีสารสนเทศ สถิติศาสตร์ นิติศาสตร์ รัฐศาสตร์ หรือรัฐประศาสนศาสตร์

(๓) ผ่านการอบรมทางด้านความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security) สืบสวน สอบสวน และการพิสูจน์หลักฐานทางคอมพิวเตอร์ (Computer Forensics) ตามภาคผนวกท้ายประกาศนี้ และ

(๔) มีคุณสมบัติอื่นอย่างหนึ่งอย่างใด ดังต่อไปนี้

ก. รับราชการหรือเคยรับราชการไม่น้อยกว่าสองปีในตำแหน่งเจ้าหน้าที่ตรวจพิสูจน์พยานหลักฐานที่เป็นข้อมูลคอมพิวเตอร์หรือพยานหลักฐานอิเล็กทรอนิกส์

ข. สำเร็จการศึกษาตามข้อ ๒ (๒) ในระดับปริญญาตรี และมีประสบการณ์ที่เป็นประโยชน์ต่อการปฏิบัติงานตามพระราชบัญญัตินี้นับแต่สำเร็จการศึกษาดังกล่าวไม่น้อยกว่าสี่ปี

ค. สำเร็จการศึกษาตามข้อ ๒ (๒) ในระดับปริญญาโท หรือสอบไล่ได้เป็นเนติบัณฑิตตามหลักสูตรของสำนักอบรมศึกษากฎหมายแห่งเนติบัณฑิตยสภา และมีประสบการณ์ที่เป็นประโยชน์ต่อการปฏิบัติงานตามพระราชบัญญัตินี้นับแต่สำเร็จการศึกษาดังกล่าวไม่น้อยกว่าสามปี

ง. สำเร็จการศึกษาตามข้อ ๒ (๒) ในระดับปริญญาเอก หรือมีประสบการณ์ที่เป็นประโยชน์ต่อการปฏิบัติงาน ตามพระราชบัญญัตินี้นับแต่สำเร็จการศึกษาดังกล่าวไม่น้อยกว่าสองปี

จ. เป็นบุคคลที่ทำงานเกี่ยวกับความมั่นคงปลอดภัยของระบบสารสนเทศ การตรวจพิสูจน์หลักฐานทางคอมพิวเตอร์ หรือมีประสบการณ์ในการดำเนินคดีเกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์ไม่น้อยกว่าสองปี

ข้อ ๓ ในกรณีที่มีความจำเป็นเพื่อประโยชน์ของทางราชการในการสืบสวนและสอบสวนการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ จำเป็นต้องมีบุคลากรซึ่งมีความรู้ ความชำนาญ หรือประสบการณ์สูง เพื่อดำเนินการสืบสวนและสอบสวนการกระทำผิดหรือคดีเช่นว่านั้น หรือเป็นบุคลากรในสาขาที่ขาดแคลน รัฐมนตรีอาจยกเว้นคุณสมบัติตามข้อ ๒ ไม่ว่าทั้งหมดหรือบางส่วนสำหรับการบรรจุและแต่งตั้งบุคคลใดเป็นการเฉพาะก็ได้

ข้อ ๔ การแต่งตั้งบุคคลหนึ่งบุคคลใดเป็นพนักงานเจ้าหน้าที่ให้แต่งตั้งจากบุคคลซึ่งมีคุณสมบัติตามข้อ ๒ หรือข้อ ๓ โดยบุคคลดังกล่าวต้องผ่านการประเมินความรู้ความสามารถหรือทดสอบตามหลักสูตรและหลักเกณฑ์ที่รัฐมนตรีประกาศกำหนด

การแต่งตั้งบุคคลใดเป็นพนักงานเจ้าหน้าที่ตามวรรคหนึ่ง ให้พนักงานเจ้าหน้าที่ ดำรงตำแหน่งในวาระคราวละ ๔ ปี และการแต่งตั้งให้ประกาศในราชกิจจานุเบกษา

ข้อ ๕ พนักงานเจ้าหน้าที่ต้องไม่มีลักษณะต้องห้าม ดังต่อไปนี้

(๑) เป็นบุคคลล้มละลาย บุคคลไร้ความสามารถ หรือบุคคลเสมือนไร้ความสามารถ

(๒) เป็นสมาชิกสภาผู้แทนราษฎร สมาชิกวุฒิสภา ข้าราชการการเมือง สมาชิกสภาท้องถิ่น ผู้บริหารท้องถิ่น กรรมการหรือผู้ดำรงตำแหน่งที่รับผิดชอบในการบริหารพรรคการเมือง ที่ปรึกษาพรรคการเมือง หรือเจ้าหน้าที่ในพรรคการเมือง

(๓) เป็นผู้อยู่ระหว่างถูกสั่งให้พักราชการหรือถูกสั่งให้ออกจากราชการไว้ก่อน

(๔) ถูกไล่ออก ปลดออก หรือให้ออกจากราชการ หน่วยงานของรัฐหรือรัฐวิสาหกิจเพราะทำผิดวินัย หรือรัฐมนตรีให้ออกจากการเป็นพนักงานเจ้าหน้าที่ เพราะมีความประพฤติเสื่อมเสียบกพร่องหรือไม่สุจริตต่อหน้าที่หรือหย่อนความสามารถ

(๕) ได้รับโทษจำคุกโดยคำพิพากษาถึงที่สุดให้จำคุก เว้นแต่เป็นโทษ สำหรับความผิดที่กระทำโดยประมาทหรือความผิดลหุโทษ

(๖) ต้องคำพิพากษาหรือคำสั่งของศาลให้ทรัพย์สินตกเป็นของแผ่นดิน เพราะร่ำรวยผิดปกติหรือมีทรัพย์สินเพิ่มขึ้นผิดปกติ

ข้อ ๖ พนักงานเจ้าหน้าที่พ้นจากตำแหน่งเมื่อ

(๑) ตาย

(๒) ลาออก

(๓) ถูกจำคุกโดยคำพิพากษาถึงที่สุดให้จำคุก

(๔) ขาดคุณสมบัติหรือมีลักษณะต้องห้ามตามข้อ ๕

(๕) รัฐมนตรีให้ออก เพราะมีความประพฤติเสื่อมเสีย บกพร่องหรือไม่สุจริตต่อหน้าที่หรือหย่อนความสามารถ

(๖) ครบวาระการดำรงตำแหน่ง

ข้อ ๗ ประกาศนี้มีผลใช้บังคับตั้งแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ประกาศ ณ วันที่ ๒๑ สิงหาคม พ.ศ. ๒๕๕๐
สิทธิชัย โภไคยอุดม
รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

ภาคผนวก

ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

เรื่อง หลักเกณฑ์เกี่ยวกับคุณสมบัติของพนักงานเจ้าหน้าที่

ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

.....

ผู้ที่จะได้รับการแต่งตั้งให้เป็นพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ จะต้องผ่านการอบรมด้านจริยธรรม สืบสวน สอบสวน ความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security) และการพิสูจน์หลักฐานทางคอมพิวเตอร์ (Computer Forensics) แล้วแต่กรณี ดังต่อไปนี้

๑. หลักสูตรมาตรฐานสากล (International Standard Courses)

วัตถุประสงค์ : เพื่อใช้เป็นแนวทางในการจัดอบรมให้กับบุคคลซึ่งจะได้รับการแต่งตั้งเป็นพนักงานเจ้าหน้าที่ในกรณีทั่วไป (หลักสูตรเต็มเวลาประมาณ ๑ เดือน ทั้งภาคทฤษฎีและปฏิบัติ ทั้งนี้ไม่รวมด้านที่สาม ข. และด้านที่สี่ ข. ซึ่งเป็นหลักสูตรความเชี่ยวชาญเฉพาะทาง)

เนื้อหาหลักสูตรที่อบรม :

ด้านแรก การอบรมด้านจริยธรรม/จรรยาบรรณที่พึงมีในบทบาทและอำนาจหน้าที่ของพนักงานเจ้าหน้าที่

ด้านที่สอง ความรู้พื้นฐานด้านการสืบสวนและสอบสวนเพื่อการบังคับใช้กฎหมาย (Law Enforcement)

ลำดับ	เนื้อหาหลักสูตร (ภาคบังคับ) Compulsory Course
๑.	กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
๒.	กฎหมายอาญาและวิธีพิจารณาความอาญาที่เกี่ยวข้องกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
๓.	รูปแบบการกระทำความผิดและกรณีศึกษา (Case Studies)
๔.	การสืบสวนทางเทคนิค เช่น การตรวจสอบหมายเลข IP Address หรือแหล่งที่มาของการกระทำความผิด การขอข้อมูลจราจรทางคอมพิวเตอร์ (Traffic Data) จากผู้ให้บริการ การวิเคราะห์และเชื่อมโยงข้อมูล/พยานหลักฐานข้างต้น

๕.	แนวทางปฏิบัติในการดำเนินคดี/การทำสำนวนคดี เช่น การร้องทุกข์กล่าวโทษ (การแจ้งความ) การประสานความร่วมมือกับหน่วยงานที่เกี่ยวข้อง การรวบรวมพยานหลักฐาน และแสวงหาข้อเท็จจริง การตรวจสถานที่เกิดเหตุ การยื่นคำร้องต่อศาล การยึดอายัดและคืนพยานหลักฐาน การเก็บรักษาพยานหลักฐาน การเก็บรักษาพยานหลักฐานให้คงความน่าเชื่อถือในกระบวนการ การเปรียบเทียบปรับและการดำเนินคดี เป็นต้น
๖.	การบริหารจัดการคดีให้เป็นไปอย่างมีประสิทธิภาพ

ด้านที่สาม ความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security)

ก. เนื้อหาหลักสูตรภาคบังคับสำหรับพนักงานเจ้าหน้าที่

ลำดับ	เนื้อหาหลักสูตร (ภาคบังคับ) **Compulsory Course**
๑.	General security concepts
๒.	Security Architecture
๓.	Access Controls
๔.	Applications Security
๕.	Operation Security
๖.	Security Management
๗.	Cryptography
๘.	Physical Security
๙.	Telecommunications and Network Security
๑๐.	Business Continuity Planning
๑๑.	Law, Investigations, and Ethics

ข. หลักสูตรความมั่นคงปลอดภัยของระบบสารสนเทศขั้นสูง (Advanced Information Security Course) สำหรับพนักงานเจ้าหน้าที่สายผู้เชี่ยวชาญด้านเทคนิค

ลำดับ	เนื้อหาหลักสูตร (ความชำนาญเฉพาะทาง)
๑.	Audit and Monitoring
๒.	Risk, Response and Recovery
๓.	Malicious Code Analysis
๔.	Vulnerabilities Assessment & Penetration Testing

ด้านที่สี่ การพิสูจน์หลักฐานทางคอมพิวเตอร์ (Computer Forensics)

ก.ความรู้ด้านการพิสูจน์หลักฐานทางคอมพิวเตอร์ (Computer Forensics)

ลำดับ	เนื้อหาหลักสูตร (ภาคบังคับ) Compulsory Course
๑.	The needs for Computer Forensics
๒.	Principles of Computer Forensics and Digital/Electronic Evidence
๓.	Crime scene, Digital/Electronic Evidence and Chain of Custody
๔.	Capturing the Data Image and Volatile Data
๕.	Extracting Information from Captured Data
๖.	Breaking Password and Encryption
๗.	Using Computer Forensics Tools
๘.	Investigation and Interrogation
๙.	Digital/Electronic Evidence Analysis and Synthesis
๑๐.	Testify in Court, Admissibility requirements
๑๑.	Different between Computer Forensics and Network/Internet Forensics
๑๒.	Network/Internet Forensics
๑๓.	Using Network/Internet Forensics Tools

ข.ความเชี่ยวชาญเฉพาะทางด้านการพิสูจน์หลักฐานทางคอมพิวเตอร์

(Professional Computer Forensics และ Certified Forensic Computer Examiner (CFCE))

ลำดับ	เนื้อหาหลักสูตร (ความชำนาญเฉพาะทาง)
๑.	Using Computer Forensic Tools เช่น Encase, Forensics Toolkits, ILook
๒.	Using Network / Internet Forensic Tools เช่น Encase Field Intelligence Model (FIM)
๓.	Wireless Forensic Tools เช่น Netstumbler, Kismet, Aircrack
๔.	Using Handheld Forensics Tools (Cell & PDA) Paraben, MobilEdit, Vogon
๕.	Cryptology ได้แก่ Cryptography และ Cryptanalysis

๒. หลักสูตรเร่งรัด (Intensive Courses) (๕ วัน)

วัตถุประสงค์ : เพื่อใช้เป็นแนวทางในการจัดการอบรมระยะสั้นแบบเร่งรัดให้กับบุคคลซึ่งจะได้รับการแต่งตั้งเป็นพนักงานเจ้าหน้าที่ในกรณีพิเศษ ซึ่งได้รับการยกเว้นตามหลักเกณฑ์ในการกำหนดคุณสมบัติของพนักงานเจ้าหน้าที่ตามปกติทั่วไป

เนื้อหาหลักสูตรที่อบรม :

ด้านแรก การอบรมด้านจริยธรรม/จรรยาบรรณที่พึงมีในบทบาทและอำนาจหน้าที่ของพนักงานเจ้าหน้าที่

ด้านที่สอง ความรู้พื้นฐานด้านการสืบสวนและสอบสวนเพื่อการบังคับใช้กฎหมาย (Law Enforcement)

ลำดับ	เนื้อหาหลักสูตร (ภาคบังคับ) Compulsory Course
๑.	กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
๒.	กฎหมายอาญาและวิธีพิจารณาความอาญาที่เกี่ยวข้องกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
๓.	รูปแบบการกระทำความผิดและกรณีศึกษา (Case Studies)
๔.	การสืบสวนทางเทคนิค เช่น การตรวจสอบหมายเลข IP Address หรือแหล่งที่มาของการกระทำความผิด การขอข้อมูลจราจรทางคอมพิวเตอร์ (Traffic Data) จากผู้ให้บริการ การวิเคราะห์และเชื่อมโยงข้อมูล/ พยานหลักฐานข้างต้น
๕.	แนวทางปฏิบัติในการดำเนินคดี/การทำสำนวนคดี เช่น การร้องทุกข์กล่าวโทษ (การแจ้งความ) การประสานความร่วมมือกับหน่วยงานที่เกี่ยวข้อง การรวบรวมพยาน หลักฐาน และแสวงหาข้อเท็จจริง การตรวจสถานที่เกิดเหตุ การยื่นคำร้องต่อศาล การยึดอายัดและคืนพยานหลักฐาน การเก็บรักษาพยานหลักฐาน การเก็บรักษาพยานหลักฐานให้คงความน่าเชื่อถือในกระบวนการ การเปรียบเทียบปรับและการดำเนินคดี เป็นต้น
๖.	การบริหารจัดการคดีให้เป็นไปอย่างมีประสิทธิภาพ

ด้านที่สาม การพิสูจน์หลักฐานทางคอมพิวเตอร์ (Computer Forensics)

ลำดับ	เนื้อหาหลักสูตรภาคบังคับ Compulsory Course
๑.	The needs for Computer Forensics
๒.	Principles of Computer Forensics and Digital/Electronic Evidence
๓.	Crime scene, Digital/Electronic Evidence and Chain of Custody
๔.	Capturing the Data Image and Volatile Data
๕.	Extracting Information from Captured Data
๖.	Breaking Password and Encryption
๗.	Using Computer Forensics Tools
๘.	Investigation and Interrogation
๙.	Digital/Electronic Evidence Analysis and Synthesis
๑๐.	Testify in Court, Admissibility requirements
๑๑.	Different between Computer Forensics and Network/Internet Forensics
๑๒.	Network/Internet Forensics
๑๓.	Using Network/Internet Forensics Tools

ระเบียบว่าด้วยการจับ ควบคุม ค้น การทำสำนวนสอบสวนและดำเนินคดี กับผู้กระทำความผิดตามพระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

ระเบียบ

ว่าด้วยการจับ ควบคุม ค้น การทำสำนวนสอบสวนและดำเนินคดีกับผู้กระทำความผิด
ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
พ.ศ. ๒๕๕๐

อาศัยอำนาจตามมาตรา ๒๙ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ นายกรัฐมนตรีและรัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ออกระเบียบไว้ ดังต่อไปนี้

ข้อ ๑ ระเบียบนี้เรียกว่า “ระเบียบ ว่าด้วยการจับ ควบคุม ค้น การทำสำนวนสอบสวนและดำเนินคดีกับผู้กระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐”

ข้อ ๒ ระเบียบนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ในระเบียบนี้

“พนักงานเจ้าหน้าที่” หมายความถึง ผู้ซึ่งรัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารแต่งตั้งให้ปฏิบัติการตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

“พนักงานสอบสวน” หมายความถึง เจ้าพนักงานซึ่งกฎหมายให้มีอำนาจและหน้าที่ทำการสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา

“การปฏิบัติหน้าที่ร่วมกัน” หมายความว่า การที่พนักงานเจ้าหน้าที่และหรือพนักงานสอบสวนได้ให้ความเห็นหรือคำแนะนำ และหรือตรวจสอบพยานหลักฐานตั้งแต่ชั้นเริ่มการสอบสวนในคดีโดยให้เริ่มดำเนินการนับแต่โอกาสแรกเท่าที่จะพึงกระทำได้

“การสอบสวนร่วมกัน” หมายความว่า การสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญาและพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

ข้อ ๔ ให้พนักงานเจ้าหน้าที่หรือพนักงานสอบสวนเป็นผู้รับคำร้องทุกข์ หรือคำกล่าวโทษในกรณีที่มีการกระทำความผิดเกิดขึ้น หรืออ้าง หรือเชื่อว่าได้เกิดขึ้นภายในเขตอำนาจของตน

หรือผู้ต้องหามีที่อยู่ หรือถูกจับภายในเขตอำนาจของตน และเป็นความผิดที่บัญญัติไว้ในหมวด ๑ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

ข้อ ๕ ในกรณีที่พนักงานสอบสวนได้รับคำร้องทุกข์ หรือคำกล่าวโทษตามข้อ ๔ แล้ว ให้พนักงานสอบสวนประสานงานกับพนักงานเจ้าหน้าที่เพื่อประโยชน์ในการแสวงหาพยานหลักฐานประกอบการกระทำความผิด

ข้อ ๖ ในการจับ ควบคุม และค้น เมื่อพนักงานเจ้าหน้าที่ประสานมายังพนักงานสอบสวนผู้รับผิดชอบแล้ว ให้พนักงานสอบสวนผู้รับผิดชอบดำเนินการตามอำนาจหน้าที่ต่อไป

ข้อ ๗ ให้พนักงานเจ้าหน้าที่ผู้รับผิดชอบดำเนินการแสวงหาพยานหลักฐานที่เกี่ยวข้องกับการกระทำความผิดตามที่บัญญัติไว้ในหมวด ๑ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ โดยให้มีการปฏิบัติหน้าที่ร่วมกัน และการสอบสวนร่วมกัน และมีหน้าที่ส่งมอบพยานหลักฐานที่รวบรวมได้ทั้งหมดให้กับพนักงานสอบสวนผู้รับผิดชอบ จนกว่าการสอบสวนในคดีนั้นจะเสร็จสิ้น

ข้อ ๘ เมื่อพนักงานสอบสวนผู้รับผิดชอบในการสอบสวน เห็นว่าการสอบสวนเสร็จสิ้นแล้ว ให้พนักงานสอบสวนเป็นผู้ทำความเห็นในรายงานความเห็นทางคดี และลงลายมือชื่อ และส่งสำนวนการสอบสวนไปยังพนักงานอัยการในท้องที่ที่มีเขตอำนาจ เพื่อพิจารณาสั่งการต่อไป

ข้อ ๙ บรรดาการใดที่พนักงานเจ้าหน้าที่และหรือพนักงานสอบสวน ได้ดำเนินการไปแล้วตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ก่อนระเบียบนี้มีผลใช้บังคับให้ใช้ระเบียบนี้บังคับ

ประกาศ ณ วันที่ ๓๐ พฤศจิกายน พ.ศ. ๒๕๕๐

พลเอก สุรยุทธ์ จุลานนท์
นายกรัฐมนตรี

โฆสิต ปั้นเปี่ยมรัษฎ์
รองนายกรัฐมนตรี รักษาราชการแทน
รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

ระเบียบสำนักนายกรัฐมนตรี
ว่าด้วยการเชื่อมโยงข้อมูลอิเล็กทรอนิกส์
สำหรับการนำเข้า การส่งออก
การนำผ่าน และโลจิสติกส์
พ.ศ. ๒๕๕๗

ระเบียบสำนักนายกรัฐมนตรี

ว่าด้วยการเชื่อมโยงข้อมูลอิเล็กทรอนิกส์ สำหรับการนำเข้า การส่งออก การนำผ่าน และโลจิสติกส์ พ.ศ. ๒๕๕๗

เพื่อเพิ่มขีดความสามารถในการแข่งขันของประเทศ การอำนวยความสะดวกทางการค้าระหว่างประเทศ และการให้บริการของรัฐที่ทันสมัย สะดวก รวดเร็ว และเป็นมาตรฐาน อีกทั้งเพื่อให้สอดคล้องกับความตกลงว่าด้วยการอำนวยความสะดวกด้านศุลกากรด้วยระบบอิเล็กทรอนิกส์ของอาเซียน (Agreement to Establish and Implement the ASEAN Single Window) จึงจำเป็นต้องจัดให้มีระบบการเชื่อมโยงข้อมูลอิเล็กทรอนิกส์ ณ จุดเดียว (National Single Window) และกำหนดให้การขอและการออกใบอนุญาต ใบรับรอง หรือเอกสารอื่นใด เกี่ยวกับการนำเข้า การส่งออก การนำผ่าน และโลจิสติกส์ สามารถดำเนินการได้ในรูปแบบของข้อมูลอิเล็กทรอนิกส์

อาศัยอำนาจตามความในมาตรา ๑๑ (๘) แห่งพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน พ.ศ. ๒๕๓๔ หัวหน้าคณะรักษาความสงบแห่งชาติในฐานะผู้ใช้อำนาจนายกรัฐมนตรีและคณะรัฐมนตรีตามมาตรา ๔๓ วรรคสอง ของรัฐธรรมนูญแห่งราชอาณาจักรไทย (ฉบับชั่วคราว) พุทธศักราช ๒๕๕๗ จึงวางระเบียบไว้ ดังต่อไปนี้

ข้อ ๑ ระเบียบนี้เรียกว่า “ระเบียบสำนักนายกรัฐมนตรี ว่าด้วยการเชื่อมโยงข้อมูลอิเล็กทรอนิกส์สำหรับการนำเข้า การส่งออก การนำผ่าน และโลจิสติกส์ พ.ศ. ๒๕๕๗”

ข้อ ๒ ระเบียบนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ นอกจากที่บัญญัติไว้ในระเบียบนี้ ในการเชื่อมโยงข้อมูลอิเล็กทรอนิกส์ ให้หน่วยงานของรัฐดำเนินการและปฏิบัติตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

ข้อ ๔ ในระเบียบนี้

“การเชื่อมโยงข้อมูลอิเล็กทรอนิกส์” หมายความว่า การเชื่อมโยงข้อมูลทางอิเล็กทรอนิกส์แบบไร้เอกสาร ระหว่างระบบข้อมูลอิเล็กทรอนิกส์ของหน่วยงานของรัฐ หรือระหว่างระบบข้อมูลอิเล็กทรอนิกส์ของหน่วยงานของรัฐกับเอกชน ที่เกี่ยวข้องในกระบวนการการนำเข้า การส่งออก การนำผ่าน และโลจิสติกส์ โดยผ่านระบบการเชื่อมโยงข้อมูลอิเล็กทรอนิกส์ ณ จุดเดียว (National Single Window)

“ระบบข้อมูลอิเล็กทรอนิกส์” หมายความว่า ระบบข้อมูลที่เกี่ยวกับกระบวนการการนำเข้า การส่งออก การนำผ่าน และโลจิสติกส์ที่จัดทำขึ้นในรูปของอิเล็กทรอนิกส์เพื่อประโยชน์ในการเชื่อมโยงข้อมูลอิเล็กทรอนิกส์ และให้หมายความรวมถึงระบบการเชื่อมโยงข้อมูลอิเล็กทรอนิกส์ไปยังระบบการเชื่อมโยงข้อมูลอิเล็กทรอนิกส์ ณ จุดเดียว (National Single Window) ด้วย

“ใบอนุญาต” หมายความว่า ใบอนุญาตนำเข้า ส่งออก นำผ่าน และโลจิสติกส์ และให้หมายความรวมถึงใบรับรองหรือเอกสารอื่นใดที่หน่วยงานของรัฐเป็นผู้ออกให้ เพื่อการนำเข้า การส่งออก การนำผ่าน และโลจิสติกส์

“โลจิสติกส์” หมายความว่า กระบวนการดำเนินการบริหารจัดการอย่างมีประสิทธิภาพเกี่ยวกับการจัดการคลังสินค้า การขนส่ง การเคลื่อนย้าย การจัดเก็บ การรวบรวม หรือการกระจายสินค้าหรือบริการ รวมทั้งกิจการที่เกี่ยวเนื่อง ทั้งนี้ ไม่รวมถึงการบริการขนส่งผู้โดยสาร

“ผู้ขอ” หมายความว่า บุคคลธรรมดาหรือนิติบุคคลที่มีความประสงค์จะขอใบอนุญาตจากหน่วยงานของรัฐ

“หน่วยงานของรัฐ” หมายความว่า กระทรวง ทบวง กรม ส่วนราชการที่เรียกชื่ออย่างอื่นและมีฐานะเป็นกรม ราชการส่วนภูมิภาค ราชการส่วนท้องถิ่น รัฐวิสาหกิจที่ตั้งขึ้นโดยพระราชบัญญัติหรือพระราชกฤษฎีกา และให้หมายความรวมถึงนิติบุคคล คณะบุคคล หรือบุคคลซึ่งมีอำนาจหน้าที่ดำเนินงานของรัฐไม่ว่าในการใด ๆ ที่เกี่ยวข้องกับการนำเข้า การส่งออก การนำผ่าน และโลจิสติกส์

ข้อ ๕ ให้หน่วยงานของรัฐที่ต้องปฏิบัติตามระเบียบนี้มีอำนาจออกระเบียบ ประกาศ คำสั่ง หรือข้อกำหนดเพื่อปฏิบัติตามระเบียบนี้

บรรดาระเบียบ ประกาศ คำสั่ง หรือข้อกำหนดนั้น เมื่อได้ประกาศในราชกิจจานุเบกษาแล้วให้ใช้บังคับได้

ข้อ ๖ ให้หน่วยงานของรัฐผู้มีหน้าที่พิจารณาออกใบอนุญาตให้กับผู้นำเข้า ส่งออก นำผ่าน และโลจิสติกส์ จัดให้มีระบบข้อมูลอิเล็กทรอนิกส์เพื่อประโยชน์ในการเชื่อมโยงข้อมูลอิเล็กทรอนิกส์ที่เกี่ยวข้องในกระบวนการการนำเข้า การส่งออก การนำผ่าน และโลจิสติกส์

ข้อ ๗ เมื่อผู้ขอส่งข้อมูลคำขออนุญาตซึ่งสินค้าที่ต้องมีใบอนุญาตในการนำเข้า การส่งออก การนำผ่าน และโลจิสติกส์ ต่อหน่วยงานของรัฐผู้มีหน้าที่พิจารณาออกใบอนุญาต ให้หน่วยงานของรัฐพิจารณาคำขออนุญาตและแจ้งผลการอนุญาตให้กรมศุลกากรทราบโดยผ่านระบบการเชื่อมโยงข้อมูลอิเล็กทรอนิกส์ ณ จุดเดียว

ในกรณีที่หน่วยงานของรัฐใดมีอำนาจตามกฎหมายและได้รับมอบอำนาจจากหน่วยงานของรัฐอื่นให้ดำเนินการออกใบอนุญาตสำหรับสินค้าชนิดเดียวกัน ให้หน่วยงานของรัฐนั้นแจ้งผลการอนุญาตรวมเป็นข้อมูลเดียวให้กรมศุลกากรทราบโดยผ่านระบบการเชื่อมโยงข้อมูลอิเล็กทรอนิกส์ ณ จุดเดียว

ในการดำเนินการตามวรรคหนึ่งหรือวรรคสอง หากหน่วยงานของรัฐผู้มีหน้าที่พิจารณาออกใบอนุญาตจำเป็นต้องตรวจสอบสินค้าก่อนการส่งมอบของจากอารักขาของศุลกากร ให้กรมศุลกากรส่งข้อมูลใบขนสินค้าตามที่ได้ตกลงร่วมกันผ่านระบบการเชื่อมโยงข้อมูลอิเล็กทรอนิกส์ ณ จุดเดียว เพื่อให้หน่วยงานของรัฐดำเนินการตรวจสอบสินค้า และเมื่อได้ตรวจสอบสินค้าแล้ว ให้บันทึกผลการตรวจสอบและแจ้งให้กรมศุลกากรทราบโดยผ่านระบบการเชื่อมโยงข้อมูลอิเล็กทรอนิกส์ ณ จุดเดียว

เมื่อกรมศุลกากรดำเนินพิธีการศุลกากรเรียบร้อยแล้ว ให้แจ้งผลการพิจารณาตรวจปล่อยสินค้าให้ผู้ขอและหน่วยงานของรัฐที่เกี่ยวข้องทราบโดยผ่านระบบการเชื่อมโยงข้อมูลอิเล็กทรอนิกส์ ณ จุดเดียว

ข้อ ๘ ให้หน่วยงานของรัฐผู้มีหน้าที่พิจารณาออกใบอนุญาตรวบรวมข้อมูลสินค้าที่ต้องขอใบอนุญาตแจ้งให้กรมศุลกากรทราบ และให้หน่วยงานของรัฐร่วมกับกรมศุลกากรจัดประเภทพิกัดอัตราศุลกากรฮาร์โมไนซ์อาเซียน และรหัสสถิติสินค้าที่ต้องขอใบอนุญาต เพื่อใช้และจัดทำฐานข้อมูลสินค้าดังกล่าวเพื่อประโยชน์ในการเชื่อมโยงข้อมูลอิเล็กทรอนิกส์

ในกรณีที่มีการเปลี่ยนแปลงหรือเพิ่มเติมข้อมูลรายการสินค้าแตกต่างจากที่แจ้งไว้ตามวรรคหนึ่ง ให้หน่วยงานของรัฐแจ้งให้กรมศุลกากรทราบเพื่อให้ฐานข้อมูลสินค้าที่ได้ร่วมกันจัดทำตามวรรคหนึ่งมีความถูกต้องและทันสมัย

ข้อ ๙ เพื่อประโยชน์ในการเชื่อมโยงข้อมูลอิเล็กทรอนิกส์ให้เป็นระบบเดียวกัน ให้หน่วยงานของรัฐผู้มีหน้าที่พิจารณาออกใบอนุญาตให้กับผู้นำเข้า ส่งออก นำผ่าน และโลจิสติกส์พัฒนาระบบข้อมูลอิเล็กทรอนิกส์เพื่อให้สามารถรับส่งข้อมูลผ่านระบบการเชื่อมโยงข้อมูลอิเล็กทรอนิกส์ ณ จุดเดียว ได้ และพัฒนาระบบข้อมูลอิเล็กทรอนิกส์ดังกล่าวให้ทันสมัยและเป็นมาตรฐานสากลอย่างต่อเนื่อง

ข้อ ๑๐ รูปแบบและมาตรฐานของข้อมูลที่นำมาแลกเปลี่ยนข้อมูลระหว่างหน่วยงานของรัฐและวิธีการในการแลกเปลี่ยนข้อมูลระหว่างหน่วยงานของรัฐ ให้เป็นไปตามความตกลงระหว่างหน่วยงานของรัฐและต้องสอดคล้องกับมาตรฐานสากล

ข้อ ๑๑ ให้หน่วยงานของรัฐผู้รับและผู้ส่งพิจารณาและให้ความเห็นชอบเกี่ยวกับข้อมูลอิเล็กทรอนิกส์ที่จะนำมาใช้ในการเชื่อมโยงข้อมูลอิเล็กทรอนิกส์ และเมื่อหน่วยงานของรัฐผู้รับและผู้ส่งเห็นชอบร่วมกันว่าข้อมูลอิเล็กทรอนิกส์เพียงพอที่จะใช้ในการเชื่อมโยงข้อมูลอิเล็กทรอนิกส์ได้แล้ว ให้ใช้ข้อมูลอิเล็กทรอนิกส์ดังกล่าวในการปฏิบัติตามภารกิจของแต่ละหน่วยงานของรัฐได้

ข้อ ๑๒ ให้หน่วยงานของรัฐจัดตั้งงบประมาณรายจ่ายประจำปีหรืองบรายจ่ายอื่นเป็นค่าใช้จ่ายในการจัดทำและพัฒนาระบบข้อมูลอิเล็กทรอนิกส์เพื่อประโยชน์ในการเชื่อมโยงข้อมูลอิเล็กทรอนิกส์ตามระเบียบนี้

ข้อ ๑๓ ให้กรมศุลกากรมีหน้าที่ดูแลและพัฒนาระบบการเชื่อมโยงข้อมูลอิเล็กทรอนิกส์ ณ จุดเดียว ตามระเบียบนี้

ข้อ ๑๔ เพื่อประโยชน์ในการเชื่อมโยงข้อมูลอิเล็กทรอนิกส์ระหว่างหน่วยงานของรัฐ และระหว่างหน่วยงานของรัฐกับเอกชน ให้มีประสิทธิภาพมากยิ่งขึ้น ให้กรมศุลกากรประสานงานกับหน่วยงานของรัฐเพื่อประเมินผลการดำเนินการเชื่อมโยงข้อมูลอิเล็กทรอนิกส์ และรายงานผลให้นายกรัฐมนตรีทราบทุก ๖ เดือน

ข้อ ๑๕ ในกรณีที่หน่วยงานของรัฐใดยังไม่มีความพร้อมในการเชื่อมโยงข้อมูลอิเล็กทรอนิกส์ให้หน่วยงานของรัฐนั้นพัฒนาและประสานงานกับกรมศุลกากรเพื่อให้สามารถเชื่อมโยงข้อมูลอิเล็กทรอนิกส์ตามระเบียบนี้ ภายในวันที่ ๓๐ กันยายน ๒๕๕๗

ข้อ ๑๖ ให้นายกรัฐมนตรีรักษาการตามระเบียบนี้

ประกาศ ณ วันที่ ๔ กันยายน พ.ศ. ๒๕๕๗
พลเอก ประยุทธ์ จันทร์โอชา
หัวหน้าคณะรักษาความสงบแห่งชาติ

Electronic Transactions Commission

สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
๑๒๐ หมู่ ๓ ศูนย์ราชการเฉลิมพระเกียรติฯ อาคารรัฐประศาสนภักดี ชั้น ๖
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ ๑๐๒๑๐
โทรศัพท์ ๐ ๒๑๔๑ ๖๙๘๕-๙๙ โทรสาร ๐ ๒๑๔๓ ๘๐๓๖-๓๗
เว็บไซต์กระทรวง : http://www.mict.go.th
เว็บไซต์คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ : http://www.etcommission.go.th