ภาคผนวก ก

ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
เรื่อง หลักเกณฑ์เกี่ยวกับคุณสมบัติของพนักงานเจ้าหน้าที่
ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
พ.ศ. ๒๕๕๐

เพื่อให้การแต่งตั้งพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ มีความชัดเจนและเป็นไปอย่างมีประสิทธิภาพอาศัยอำนาจตามความในมาตรา ๒๘ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารจึงได้กำหนดหลักเกณฑ์เกี่ยวกับคุณสมบัติของพนักงานเจ้าหน้าที่ ดังต่อไปนี้

ข้อ ๑ ในประกาศนี้

“พนักงานเจ้าหน้าที่” หมายความว่า ผู้ซึ่งรัฐมนตรีแต่งตั้งให้ปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

“รัฐมนตรี” หมายความว่า รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

ข้อ ๒ พนักงานเจ้าหน้าที่ ต้องมีคุณสมบัติ ดังต่อไปนี้

(๑) มีความรู้และความชำนาญเกี่ยวกับระบบคอมพิวเตอร์

(๒) สำเร็จการศึกษาไม่น้อยกว่าระดับปริญญาตรีทางวิศวกรรมศาสตร์ วิทยาศาสตร์วิทยาการคอมพิวเตอร์ 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 หรือสอบไล่ได้เป็นเนติบัณฑิต

ตามหลักสูตรของสำนักอบรมศึกษากฎหมายแห่งเนติบัณฑิตยสภา 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 โดยบุคคลดังกล่าวต้องผ่านการประเมินความรู้ความสามารถหรือทดสอบตามหลักสูตรและหลักเกณฑ์ที่รัฐมนตรีประกาศกำหนดการแต่งตั้งบุคคลใดเป็นพนักงานเจ้าหน้าที่ตามวรรคหนึ่ง 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

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	กฎหมายอาญาและวิธีพิจารณาความอาญาที่เกี่ยวข้องกับการกระทำความผิดเกี่ยวกับ
๓	คอมพิวเตอร์
๔	รูปแบบการกระทำความผิดและกรณีศึกษา (Case Studies)

ลำดับ	เนื้อหาหลักสูตร (ภาคบังคับ) Compulsory Course
๕	การสืบสวนทางเทคนิค เช่น การตรวจสอบหมายเลข IP Address หรือแหล่งที่มาของ การกระทำความผิด การขอข้อมูลจราจรทางคอมพิวเตอร์ (Traffic Data) จากผู้ให้บริการการวิเคราะห์และเชื่อมโยงข้อมูล/พยานหลักฐานข้างต้น แนวทางปฏิบัติในการดำเนินคดี/การทำสำนวนคดี เช่น การร้องทุกข์กล่าวโทษ
๖	(การแจ้งความ) การประสานความร่วมมือกับหน่วยงานที่เกี่ยวข้อง การรวบรวมพยาน หลักฐาน และแสวงหาข้อเท็จจริง การตรวจสถานที่เกิดเหตุ การยื่นคำร้องต่อศาล การยึดอายัดและคืนพยานหลักฐาน การเก็บรักษาพยานหลักฐาน การเก็บรักษา พยานหลักฐานให้คงความน่าเชื่อถือในกระบวนการ การเปรียบเทียบปรับและการ ดำเนินคดี เป็นต้น 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

ลำดับ	เนื้อหาหลักสูตร (ภาคบังคับ) Compulsory Course
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

ลำดับ	เนื้อหาหลักสูตร (ภาคบังคับ) Compulsory Course
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	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

ลำดับ	เนื้อหาหลักสูตร (ภาคบังคับ) Compulsory Course
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

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 หรือเชื่อว่าได้เกิดขึ้นภายในเขตอำนาจของตนหรือผู้ต้องหามีที่อยู่ หรือถูกจับภายในเขตอำนาจของตน และเป็นความผิดที่บัญญัติไว้ในหมวด ๑ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

ข้อ ๕ ในกรณีที่พนักงานสอบสวนได้รับคำร้องทุกข์ หรือคำกล่าวโทษตามข้อ ๔ แล้วให้พนักงานสอบสวนประสานงานกับพนักงานเจ้าหน้าที่เพื่อประโยชน์ในการแสวงหาพยานหลักฐานประกอบการกระทำความผิด

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

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

ผู้ว่าการธนาคารแห่งประเทศไทย

ภาคผนวก ข

แนบท้ายประกาศรัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๕๐

.....

๑. ผู้ให้บริการแก่บุคคลทั่วไปในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น ทั้งนี้ โดยผ่านทางระบบคอมพิวเตอร์ ไม่ว่าจะเป็นการให้บริการในนามของตนเองหรือเพื่อประโยชน์ของบุคคลอื่น ตามข้อ ๕ (๑) สามาถจำแนกได้ ๓ 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, ผู้ให้บริการ frame relay, ผู้ให้บริการ ATM, ผู้ให้บริการ MPLS เป็นต้น เว้นแต่ผู้ให้บริการนั้น ให้บริการแต่เพียง physical media หรือสายสัญญาณอย่างเดียว (cabling) เท่านั้น (เช่น ผู้ให้บริการ Dark Fiber , ผู้ให้บริการสายใยแก้ว นำแสง ซึ่งอาจไม่มีสัญญาน Internet หรือไม่มี IP traffic) ๔)ผู้ให้บริการดาวเทียม (Satellite service provider) ๕)ผู้ให้บริการสื่อสารไร้สาย (Wireless access service provider) หมายเหตุอาจต้องพิจารณาเพิ่มเติมเปลี่ยนเป็นผู้ให้บริการตามที่กทช. และกสช.

ข.ผู้ให้บริการการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ (Access Service Provider)	๑)ผู้ให้บริการเครือข่ายสาธารณะ (Public network service provider) ทั้งมีสายและไร้สาย ๒) ผู้ประกอบการซึ่งให้บริการในการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ในห้องพัก ห้องเช่า โรงแรม หรือร้านอาหารและเครื่องดื่ม ในแต่ละกลุ่มอย่างหนึ่งอย่างใด ๓)ผู้ให้บริการเข้าถึงระบบเครือข่ายคอมพิวเตอร์สำหรับองค์กร เช่น หน่วยงานราชการ บริษัทหรือ สถาบันการศึกษา
ค.ผู้ให้บริการเช่าระบบคอมพิวเตอร์เพื่อให้บริการโปรแกรมประยุกต์ต่างๆ (Hosting Service Provider)	๑)ผู้ให้บริการเช่าระบบคอมพิวเตอร์ (Web hosting) (ตัวอย่าง การให้บริการเช่า Web server ๒)ผู้ให้บริการแลกเปลี่ยนแฟ้มข้อมูล (File server หรือ File sharing) ๓)ผู้ให้บริการการเข้าถึงจดหมายอิเล็กทรอนิกส์ (Mail Server Service Provider) ๔)ผู้ให้บริการศูนย์รับฝากข้อมูลทางอินเทอร์เน็ต (Internet Data Center)
ง.ผู้ให้บริการร้านอินเทอร์เน็ต	๑. Internet Café ๒.ผู้ให้บริการเกมออนไลน์

๒. ผู้ให้บริการในการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลตาม ข้อ ๕ (๒) เช่น ผู้ให้บริการข้อมูลคอมพิวเตอร์ผ่านแอพพลิเคชั่นต่างๆ (Content Service Provider) ประกอบด้วยผู้ให้บริการดังภาคผนวก ก แนบท้ายประกาศนี้

ประเภท	ตัวอย่างของผู้ให้บริการ
ผู้ให้บริการข้อมูลคอมพิวเตอร์ผ่านแอพพลิเคชั่นต่างๆ (Content and Application Provider)	๑)ผู้ให้บริการเว็บบอร์ด (Web board) หรือผู้ให้บริการบล็อค (blog) ๒) ผู้ให้บริการการทำธุรกรรมทางการเงินทางอินเทอร์เน็ต (Internet Banking) และผู้ให้บริการชำระเงินทางอิเล็กทรอนิกส์ (Electronic payment service provider) ๓)ผู้ให้บริการเว็บเซอร์วิส (Web services) ๔)ผู้ให้บริการพาณิชย์อิเล็กทรอนิกส์ (e-Commerce) หรือธุรกรรมทางอิเล็กทรอนิกส์ (e-Transactions)

แนบท้ายประกาศรัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

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	วัน ที่ 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)ข้อมูลซึ่งระบุที่ตั้งทางกายภาพของโทรศัพท์มือถือ อันเชื่อมโยงกับข้อมูลที่ตั้งของ Cell ID ขณะที่มีการติดต่อสื่อสาร ๓)จัดให้มีระบบบริการตรวจสอบบุคคลผู้ใช้บริการ

๒.ข้อมูลจราจรทางคอมพิวเตอร์ซึ่งผู้ให้บริการตามประกาศข้อ ๕ (๑) ข. ถึง ค. มีหน้าที่ต้องเก็บรักษามีดังต่อไปนี้

ประเภท	รายการ
ก. ข้อมูลอินเทอร์เน็ตที่เกิดจากการเข้าถึงระบบเครือข่าย	๑) ข้อมูล log ที่มีการบันทึกไว้เมื่อมีการเข้าถึงระบบเครือข่ายซึ่งระบุถึงตัวตนและสิทธิ ในการเข้าถึงเครือข่าย (Access logs specific to authentication and authorization servers, such as TACACS+ or RADIUS 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) ๒) ข้อมูลจดหมายอิเล็กทรอนิกส์ที่บันทึกการใช้บริการเรียกข้อมูลจดหมาย อิเล็กทรอนิกส์ผ่านโปรแกรมจัดการจากเครื่องของสมาชิก หรือการดึงข้อมูลจดหมายอิเล็กทรอนิกส์ไปยังเครื่องสมาชิกโดยยังคงจัดเก็บ ข้อมูลจดหมายอิเล็กทรอนิกส์ที่ดึงไปนั้นไว้ที่เครื่องให้บริการ (POP3 log or IMAP4 log) ๓) ข้อมูลวัน และเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ (Date and time of connection of client to server) ๔) ข้อมูลหมายเลขชุดอินเทอร์เน็ตของเครื่องบริการจดหมายอิเล็กทรอนิกส์ ที่ถูกเชื่อมต่ออยู่ในขณะนั้น (IP address of sending computer) ๕) ข้อมูลหมายเลขของข้อความที่ระบุในจดหมายอิเล็กทรอนิกส์ (Message ID)

	๖) ข้อมูลชื่อที่อยู่อิเล็กทรอนิกส์ของผู้ส่ง (Sender e-mail address) ๗) ข้อมูลชื่อที่อยู่อิเล็กทรอนิกส์ของผู้รับ (Receiver e-mail address) ๘) ข้อมูลที่บอกถึงสถานะในการตรวจสอบ (Status indicator) ๙) ข้อมูลที่บอกถึงวันเวลาในการเชื่อมต่อของเครื่องที่เข้าใช้บริการเชื่อมกับ เครื่องให้บริการ (Date and time of connection of client to server) ๑๐) ข้อมูลหมายเลขชุดอินเทอร์เน็ตของเครื่องคอมพิวเตอร์ผู้ใช้บริการที่เชื่อม ต่ออยู่ขณะเข้ามาใช้บริการ (IP address of client connected to server) ๑๑) ชื่อผู้ใช้งาน (User ID) ถ้ามี ๑๒) ข้อมูลจดหมายอิเล็กทรอนิกส์ที่ถูกส่งคืน
ค. ข้อมูลอินเทอร์เน็ตจากการโอนแฟ้มข้อมูลบนเครื่องให้บริการโอนแฟ้มข้อมูล	๑) ข้อมูล log ที่บันทึกเมื่อมีการเข้าถึงเครื่องให้บริการโอนแฟ้มข้อมูล ๒) ข้อมูลวัน และเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ (Date and time of connection of client to server) ๓) ข้อมูลหมายเลขชุดอินเทอร์เน็ตของเครื่อง

	คอมพิวเตอร์ผู้เข้าใช้ที่เชื่อมต่ออยู่ในขณะนั้น (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 ๕) ข้อมูลที่บ่งบอกถึงเส้นทางในการเรียกดูข้อมูล (URI : Uniform Resource Identifier) ดู ภาษาไทยใหม่
จ. ชนิดของข้อมูลบนเครือข่ายคอมพิวเตอร์ขนาดใหญ่ (Usenet)	๑) ข้อมูล log ที่บันทึกเมื่อมีการเข้าถึงเครือข่าย (NNTP 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 เช่นข้อมูลเกี่ยวกับวัน เวลาการติดต่อของผู้ใช้บริการ (Date and time of connection of client to server) และ/หรือข้อมูลชื่อเครื่องบนเครือข่าย และ/หรือหมายเลขเครื่องของผู้ให้บริการที่เครื่องคอมพิวเตอร์เชื่อมต่ออยู่ในขณะนั้น (Hostname and/or IP address) เป็นต้น

๓.ข้อมูลจราจรทางคอมพิวเตอร์ซึ่งผู้ให้บริการตามประกาศข้อ ๕ (๑) ง. มีหน้าที่ต้องเก็บรักษา มีดังต่อไปนี้

ประเภท	รายการ
ก. ผู้ให้บริการร้านอินเทอร์เน็ต	๑)ข้อมูลที่สามารถระบุตัวบุคคล ๒)เวลาของการเข้าใช้ และเลิกใช้บริการ ๓)หมายเลขเครื่องที่ใช้ IP Address

๔.ข้อมูลจราจรทางคอมพิวเตอร์ซึ่งผู้ให้บริการตามประกาศข้อ ๕ (๒) มีหน้าที่ต้องเก็บรักษา มีดังต่อไปนี้

ประเภท	รายการ
ก. ข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์ (Content Service Provider)	๑) ข้อมูลรหัสประจำตัวผู้ใช้หรือข้อมูลที่สามารถระบุตัว ผู้ใช้บริการได้ และ/หรือเลขประจำตัว (User ID) ของผู้ขายสินค้าหรือบริการและ/หรือเลขประจำตัวผู้ใช้บริการ (User ID) และ/หรือที่อยู่จดหมายอิเล็กทรอนิกส์ของผู้ใช้บริการ ๒)บันทึกข้อมูลการเข้าใช้บริการ ๓) กรณีผู้ให้บริการเว็บบอร์ด (Web board) หรือผู้ให้บริการบล็อค (Blog) ให้เก็บข้อมูลของผู้ประกาศ (Post) ข้อมูล ๔) ข้อมูลที่จำเป็นต่อการทำธุรกรรมเฉพาะด้าน เช่น ชื่อ สกุล รหัสประจำตัวประชาชนของผู้ใช้บริการหรือเอกสารอื่นที่มีผลใช้บังคับได้ตามกฎหมาย หรือรหัสประจำตัวผู้ใช้ ที่สามารถระบุตัวผู้ใช้บริการได้ และ/หรือเลขบัญชีธนาคารของผู้ใช้บริการ และ/หรือข้อมูลที่เป็นประโยชน์ต่อการชำระเงิน เช่น เลขบัญชีธนาคาร หรือเลขบัตรเครดิต และ/หรือข้อมูลที่สามารถแสดงถึงการซื้อขายสินค้าหรือบริการ โดยข้อมูลที่กล่าวมาต้องได้รับการเข้ารหัสลับเพื่อป้องการสำเนาไปใช้ประโยชน์จากผู้ไม่มีสิทธิ

ประกาศธนาคารแห่งประเทศไทย
ที่ สรข. ๒/๒๕๕๒
เรื่อง หลักเกณฑ์ วิธีการ และเงื่อนไข ว่าด้วยการควบคุมดูแลธุรกิจบริการ
การชำระเงินทางอิเล็กทรอนิกส์

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) และธุรกิจบริการที่ต้องได้รับอนุญาต
ก่อนให้บริการ (บัญชี ค)

"ธุรกิจบริการที่ต้องแจ้งให้ทราบก่อนให้บริการ" (บัญชี ก) ได้แก่ การให้บริการเงินอิเล็กทรอนิกส์ที่ใช้ซื้อสินค้าหรือรับบริการเฉพาะอย่างตามรายการที่กำหนดไว้ล่วงหน้า จากผู้ขาย

สินค้าหรือให้บริการเพียงรายเดียว ทั้งนี้ เว้นแต่การให้บริการเงินอิเล็กทรอนิกส์ที่ใช้จำกัดเพื่ออำนวยความสะดวก
แก่ผู้บริโภคโดยมิได้แสวงหากำไรจากการออกบัตร ตามที่ธนาคารแห่งประเทศไทยประกาศกำหนดโดยความเห็นชอบของคณะกรรมการ (e-Money บัญชี ก)

"ธุรกิจบริการที่ต้องขอขึ้นทะเบียนก่อนให้บริการ" (บัญชี ข) ได้แก่

(๑) การให้บริการเครือข่ายบัตรเครดิต (Credit Card Network)

(๒) การให้บริการเครือข่ายอีดีซี (EDC Network)

(๓) การให้บริการสวิตช์ชิ่งในการชำระเงินระบบหนึ่งระบบใด (Transaction Switchingบัญชี 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 เว้นแต่ผู้

ให้บริการที่เป็นสถาบันการเงินให้ถือปฏิบัติตามหลักเกณฑ์เกี่ยวกับการให้บริการเงินอิเล็กทรอนิกส์ที่ออกตามพระราชบัญญัติธุรกิจสถาบันการเงิน 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

เมื่อผู้ให้บริการได้ออกหลักฐานการรับชำ ระเงินแล้ว ให้ถือว่าการชำ ระเงินของผู้ใช้บริการมีผลเสร็จสิ้นสมบูรณ์ 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

ผู้ว่าการธนาคารแห่งประเทศไทย

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

ผู้ว่าการธนาคารแห่งประเทศไทย

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 ตามความในพระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการการชำ ระเงินทางอิเล็กทรอนิกส์ 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. นางสุชนี จิตตานนท์

๔. วันเริ่มต้นบังคับใช้

ประกาศฉบับนี้ให้ใช้บังคับนับแต่วันที่ประกาศในราชกิจจานุเบกษาเป็นต้นไป

ประกาศ ณ วันที่ ๓๐ มกราคม พ.ศ. ๒๕๕๒

ธาริษา วัฒนเกส

ผู้ว่าการธนาคารแห่งประเทศไทย

แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศ

ที่เกี่ยวข้องกับการให้บริการการชำระเงินทางอิเล็กทรอนิกส์

เพื่อสนับสนุนให้การประกอบธุรกิจของผู้ให้บริการการชำระเงินทางอิเล็กทรอนิกส์เป็นไปอย่างมีประสิทธิภาพ ปลอดภัย ถูกต้อง และน่าเชื่อถือ ธนาคารแห่งประเทศไทยได้จัดทำแนวปฏิบัติเพื่อเป็นแนวทางในการกำหนดมาตรการการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศที่เกี่ยวข้องกับการให้บริการการชำระเงินทางอิเล็กทรอนิกส์ แนวปฏิบัตินี้เป็นเพียงกรอบแนวทางทั่วไป ผู้ให้บริการอาจกำหนดมาตรการการรักษาความมั่นคงปลอดภัยที่แตกต่างจากแนวปฏิบัติฉบับนี้ได้ หากสามารถป้องกันความเสี่ยงทางระบบสารสนเทศได้อย่างมีประสิทธิภาพเพียงพอ และอยู่ในมาตรฐานที่ยอมรับได้ นอกจากนี้ ผู้ให้บริการต้องพิจารณาปรับใช้และกำหนดรายละเอียดของมาตรการการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศของผู้ให้บริการให้เหมาะสมกับประเภทและความซับซ้อนของธุรกิจตนเองด้วย

สาระสำคัญของแนวปฏิบัติฉบับนี้ประกอบด้วย

1. การควบคุมการเข้าถึง และการพิสูจน์ตัวตนผู้ใช้

ผู้ให้บริการต้องคำนึงถึงการกำหนดบุคลากรหรือหน่วยงานทางเทคโนโลยีสารสนเทศและการแบ่งแยกหน้าที่ให้เหมาะสม การควบคุมการเข้าถึงระบบสารสนเทศ การพิสูจน์ตัวตนผู้ใช้ และการป้องกันการปฏิเสธการรับผิด ดังนี้

1.1 การกำหนดบุคลากรหรือหน่วยงานทางระบบสารสนเทศ และการแบ่งแยกอำนาจหน้าที่ที่เหมาะสมในการบริหารจัดการทางระบบสารสนเทศของผู้ให้บริการผู้ให้บริการต้องกำหนดหน้าที่และความรับผิดชอบของบุคลากรหรือหน่วยงานที่ดูแลเกี่ยวกับความมั่นคงปลอดภัยทางระบบสารสนเทศของผู้ให้บริการ โดยสร้างความตระหนัก ให้ความรู้ และให้มีการอบรม ตลอดจนจัดให้มีกระบวนการทางวินัยเพื่อลงโทษในกรณีฝ่าฝืนหรือละเมิดระเบียบปฏิบัติเกี่ยวกับความมั่นคงปลอดภัย

แนวปฏิบัติ

(1) กำหนดหน้าที่ความรับผิดชอบ และแบ่งแยกหน้าที่ในการปฏิบัติงานด้านต่าง ๆ ที่เกี่ยวกับความมั่นคงปลอดภัยทางระบบสารสนเทศของผู้ให้บริการออกจากกันให้ชัดเจน ให้มีการถ่วงดุลอำนาจ เพื่อป้องกันความเสี่ยงในการปฏิบัติการที่อาจเกิดขึ้น

(2) มีการอบรม เพิ่มเติมความรู้แก่บุคลากรเก่า และใหม่อย่างสม่ำเสมอ

(3) จัดให้มีกระบวนการทางวินัย เพื่อลงโทษบุคลากรที่ฝ่าฝืน ละเมิดนโยบายหรือระเบียบปฏิบัติเกี่ยวกับความมั่นคงปลอดภัยทางระบบสารสนเทศของผู้ให้บริการ

1.2 การควบคุมการเข้าถึงระบบสารสนเทศ

ผู้ให้บริการต้องจัดให้มีขั้นตอนปฏิบัติเป็นลายลักษณ์อักษรสำหรับการควบคุมและจำกัดสิทธิการใช้ระบบสารสนเทศที่เกี่ยวกับการให้บริการและข้อมูลตามความจำเป็นในการใช้งานป้องกันการลักลอบการเข้าถึงระบบโดยผู้ที่ไม่มีสิทธิ ทั้งจากภายในและภายนอกองค์กร

แนวปฏิบัติ

(1) จัดทำทะเบียนทรัพย์สิน หรืออุปกรณ์ระบบสารสนเทศให้ถูกต้องอยู่เสมอรวมถึงจัดให้มีผู้รับผิดชอบดูแลทรัพย์สินเหล่านั้น

(2) มีกฎ ระเบียบ ในการใช้ระบบสารสนเทศ และทรัพย์สินที่เกี่ยวข้องกับระบบสารสนเทศที่เหมาะสม

(3) ต้องมีการควบคุม และป้องกันการเข้าถึงสถานที่ตั้ง การควบคุมการเข้าถึงอุปกรณ์ และระบบสารสนเทศที่เกี่ยวกับการให้บริการ โดยกระบวนการดังกล่าวครอบคลุมถึง

(3.1) การจัดวาง ติดตั้งอุปกรณ์ที่เกี่ยวกับการให้บริการที่เป็นสัดส่วนแบ่งเขตควบคุมอุปกรณ์สำคัญ จัดให้มีการควบคุมการเข้าออกบริเวณพื้นที่ควบคุม ป้องกันการลักลอบเข้าถึงโดยผู้ไม่มีสิทธิ ทั้งภายในและภายนอกองค์กร

(3.2) กำหนดวิธีการและสิทธิการเข้าถึงระบบสารสนเทศที่เกี่ยวกับการให้บริการโดยแบ่งแยกตามระดับอำนาจหน้าที่ และจัดให้มีการตรวจสอบสิทธิในการเข้าถึงระบบสารสนเทศดังกล่าว ทั้งจากผู้ใช้บริการ และบุคลากรที่เกี่ยวข้องก่อนอนุญาตให้เข้าใช้ระบบโดยต้องทบทวนและปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

(3.3) กำหนดให้มีการบันทึกการเข้าใช้ระบบสารสนเทศของผู้ใช้บริการและบุคลากรที่เกี่ยวข้อง เพื่อใช้ประโยชน์ในการตรวจสอบติดตามความผิดปกติต่าง ๆ ที่อาเกิดขึ้น

1.3 การตรวจสอบตัวตน และการป้องกันการปฏิเสธการรับผิด

ผู้ให้บริการต้องจัดให้มีการระบุ ตรวจสอบ หรือพิสูจน์ตัวตนและตรวจสอบสิทธิของผู้ใช้ระบบโดยพิจารณาใช้เทคโนโลยีที่เหมาะสมกับระดับความเสี่ยงของประเภทธุรกิจที่ให้บริการเช่น 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. การรักษาความลับของข้อมูล และความถูกต้องเชื่อถือได้ของระบบสารสนเทศ

ผู้ให้บริการต้องกำหนดมาตรการในการรักษาความลับของข้อมูล และการรักษาความถูกต้องเชื่อถือได้ของระบบสารสนเทศที่ให้บริการ เช่น การควบคุมการเปลี่ยนแปลงการปรับปรุงแก้ไขระบบหรืออุปกรณ์ประมวลผลสารสนเทศ 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 รวมถึงการบันทึกการแก้ไขเปลี่ยนแปลงการแจ้งให้ผู้ที่ได้รับผลกระทบจากการเปลี่ยนแปลงนั้นได้รับทราบ และปรับปรุงเอกสารที่เกี่ยวข้อง

(2) ต้องแยกระบบสำหรับการพัฒนา และระบบที่ใช้งานจริงออกจากกันซึ่งอาจเป็นการแยกอุปกรณ์เป็นคนละเครื่อง 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. การรักษาสภาพความพร้อมใช้งานของการให้บริการ

ผู้ให้บริการต้องจัดให้มีการให้บริการที่มีประสิทธิภาพและมีสภาพความพร้อมใช้งานในการให้บริการตลอดเวลา สามารถรองรับการทำธุรกรรมตามความต้องการของผู้ใช้บริการได้อย่างพอเพียง ตอบสนองการทำธุรกรรมได้อย่างรวดเร็วทั้งในเวลาปกติและเวลาที่มีการใช้บริการอย่างหนาแน่น (Peak Time) รวมทั้งมีการสำรองข้อมูลอย่างเหมาะสม เพื่อให้สามารถกู้ระบบให้กลับมาทำงานได้ตามปกติในกรณีที่เกิดความเสียหาย

3.1 การประเมิน และจัดการความเสี่ยงของระบบที่ให้บริการ

ผู้ให้บริการต้องมีวิธีการประเมินความเสี่ยงของระบบที่ให้บริการที่เหมาะสม กำหนดเกณฑ์ในการยอมรับความเสี่ยงและระบุระดับความเสี่ยงที่ยอมรับได้ รวมถึงกำหนดวิธีการจัดการความเสี่ยง

ที่อาจเกิดขึ้น ทั้งนี้ ผู้ให้บริการต้องจัดให้มีการทบทวนความเสี่ยงอยู่เสมอให้สอดคล้องกับพัฒนาการทางเทคโนโลยีและสถานการณ์ปัจจุบัน

แนวปฏิบัติ

(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 โดยดำเนินการอย่างรวดเร็วที่สุดเท่าที่จะทำได้รวมทั้งให้มีการเรียนรู้จากเหตุการณ์ที่เกิดขึ้นแล้ว 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 อย่างสม่ำเสมอเพื่อให้อุปกรณ์ทำงานได้อย่างต่อเนื่อง และอยู่ในสภาพที่มีความสมบูรณ์ต่อการใช้งาน

แนวปฏิบัติ

กำหนดให้มีการบำรุงรักษาอุปกรณ์ต่าง ๆ อย่างสม่ำเสมอ เพื่อให้อุปกรณ์ทำงานได้อย่างต่อเนื่อง และให้อยู่ในสภาพพร้อมใช้งานตลอดเวลา

4. การตรวจสอบความมั่นคงปลอดภัยทางระบบสารสนเทศ

ผู้ให้บริการจะต้องจัดให้มีการตรวจสอบความมั่นคงปลอดภัยทางระบบสารสนเทศอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่านโยบายและมาตรการการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศที่เกี่ยวข้องกับการให้บริการเป็นไปอย่างมีประสิทธิภาพมั่นคงปลอดภัย สามารถให้บริการได้อย่างต่อเนื่อง

แนวปฏิบัติ

(1) จัดให้มีผู้ตรวจสอบและดำเนินการตรวจสอบความมั่นคงปลอดภัยทางระบบสารสนเทศในเรื่องที่มีความเสี่ยงหรือมีความสำคัญต่อการให้บริการอย่างน้อยปีละ 1 ครั้ง และจัดทำรายงานผลการตรวจสอบเสนอผู้บริหารของผู้ให้บริการเพื่อพิจารณาระดับความเสี่ยงที่เป็นอยู่และกำหนดแนวทางการปรับปรุง และแจ้งให้หน่วยงานภายในที่เกี่ยวข้องทราบเพื่อนำไปปฏิบัติ

(2) ติดตาม ตรวจสอบการให้บริการการชำระเงินทางอิเล็กทรอนิกส์ให้เป็นไปตามกฎระเบียบข้อบังคับที่เกี่ยวข้องทั้งหมด เพื่อหลีกเลี่ยงการละเมิดข้อกำหนดทางกฎหมาย ระเบียบปฏิบัติ ข้อกำหนดในสัญญา และข้อกำหนดด้านความมั่นคงปลอดภัย

ฝ่ายระบบการชำระเงิน

ธนาคารแห่งประเทศไทย

29 มกราคม 2552

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 ๒๙ ประกอบกับมาตรา ๔๓ของรัฐธรรมนูญแห่งราชอาณาจักรไทย บัญญัติให้กระทำได้โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมาย จึงทรงพระกรุณาโปรดเกล้า ฯ ให้ตราพระราชกฤษฎีกาขึ้นไว้ ดังต่อไปนี้

มาตรา ๑ พระราชกฤษฎีกานี้เรียกว่า “พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓”

มาตรา ๒ พระราชกฤษฎีกานี้ให้ใช้บังคับเมื่อพ้นกำหนดหนึ่งร้อยแปดสิบวันนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

มาตรา ๓ ในพระราชกฤษฎีกานี้

“วิธีการแบบปลอดภัย” หมายความว่า วิธีการแบบปลอดภัยในการทำ ธุรกรรมทางอิเล็กทรอนิกส์

"ทรัพย์สินสารสนเทศ" หมายความว่า

(๑) ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

(๒) ตัวเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล และอุปกรณ์อื่นใด

(๓) ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์

"ความมั่นคงปลอดภัยของระบบสารสนเทศ" (information security) หมายความว่าการป้องกันทรัพย์สินสารสนเทศจากการเข้าถึง ใช้ เปิดเผย ขัดขวาง เปลี่ยนแปลงแก้ไข ทำให้สูญหายทำให้เสียหาย ถูกทำลาย หรือล่วงรู้โดยมิชอบ

"ความมั่นคงปลอดภัยด้านบริหารจัดการ" (administrative security) หมายความว่าการกระทำในระดับบริหารโดยการจัดให้มีนโยบาย มาตรการ หลักเกณฑ์ หรือกระบวนการใด ๆเพื่อนำมาใช้ในกระบวนการคัดเลือก การพัฒนา การนำไปใช้ หรือการบำรุงรักษาทรัพย์สินสารสนเทศให้มีความมั่นคงปลอดภัย

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

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

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

"การรักษาสภาพพร้อมใช้งาน" (availability) หมายความว่า การจัดทำให้ทรัพย์สินสารสนเทศสามารถทำงาน เข้าถึง หรือใช้งานได้ในเวลาที่ต้องการ

"โครงสร้างพื้นฐานสำคัญของประเทศ" (critical infrastructure) หมายความว่า บรรดาหน่วยงานหรือองค์กร หรือส่วนงานหนึ่งส่วนงานใดของหน่วยงานหรือองค์กร ซึ่งธุรกรรมทาง

อิเล็กทรอนิกส์ของหน่วยงานหรือองค์กร 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 แล้วแต่กรณีทั้งนี้ โดยให้คำนึงถึงระดับความเสี่ยงต่อความมั่นคงปลอดภัยของระบบสารสนเทศ ผลกระทบต่อมูลค่าและความเสียหายที่ผู้ใช้บริการอาจได้รับ รวมทั้งผลกระทบต่อเศรษฐกิจและสังคมของประเทศ

ให้คณะกรรมการประกาศกำหนดรายชื่อหรือประเภทของหน่วยงานหรือองค์กร หรือส่วนงานของหน่วยงานหรือองค์กรที่ถือเป็นโครงสร้างพื้นฐานสำคัญของประเทศตามมาตรา ๕ (๒) ซึ่งต้องกระทำตามวิธีการแบบปลอดภัยในระดับเคร่งครัด ระดับกลาง หรือระดับพื้นฐาน แล้วแต่กรณี

มาตรา ๗ วิธีการแบบปลอดภัยตามมาตรา ๔ ในแต่ละระดับ ให้มีมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามหลักเกณฑ์ที่คณะกรรมการประกาศกำ หนดโดยมาตรฐานดังกล่าวสำหรับวิธีการแบบปลอดภัยในแต่ละระดับนั้น อาจมีการกำหนดหลักเกณฑ์ที่แตกต่างกันตามความจำเป็น แต่อย่างน้อยต้องมีการกำหนดเกี่ยวกับหลักเกณฑ์ ดังต่อไปนี้

(๑) การสร้างความมั่นคงปลอดภัยด้านบริหารจัดการ

(๒) การจัดโครงสร้างด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ในส่วนการบริหารจัดการด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ทั้งภายในและภายนอกหน่วยงานหรือองค์กร

(๓) การบริหารจัดการทรัพย์สินสารสนเทศ

(๔) การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร

(๕) การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม

(๖) การบริหารจัดการด้านการสื่อสารและการดำเนินงานของระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

(๗) การควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ระบบสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์

(๘) การจัดหาหรือจัดให้มี การพัฒนา และการบำรุงรักษาระบบเครือข่ายคอมพิวเตอร์ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

(๙) การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด

(๑๐) การบริหารจัดการด้านการบริการหรือการดำเนินงานของหน่วยงานหรือองค์กรเพื่อให้มีความต่อเนื่อง

(๑๑) การตรวจสอบและการประเมินผลการปฏิบัติตามนโยบาย มาตรการ หลักเกณฑ์หรือกระบวนการใด ๆ รวมทั้งข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

มาตรา ๘ เพื่อประโยชน์ในการเป็นแนวทางสำหรับการจัดทำนโยบายหรือแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของหน่วยงานหรือองค์กร คณะกรรมการอาจระบุหรือแสดงตัวอย่างมาตรฐานทางเทคโนโลยีซึ่งเป็นที่ยอมรับเป็นการทั่วไปว่าเป็นมาตรฐานทางเทคโนโลยีที่เชื่อถือได้ไว้ในประกาศตามมาตรา ๗ ด้วยก็ได้

มาตรา ๙ ธุรกรรมทางอิเล็กทรอนิกส์ใดได้กระทำโดยวิธีการที่มีการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศในระดับที่เทียบเท่าหรือไม่ต่ำกว่ามาตรฐานความมั่นคงปลอดภัยของระบบสารสนเทศตามประกาศตามมาตรา ๗ ซึ่งได้กำหนดไว้สำหรับระดับของวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์นั้น ให้ถือว่าธุรกรรมทางอิเล็กทรอนิกส์ดังกล่าวได้กระทำตามวิธีการที่เชื่อถือได้ตามมาตรา ๒๕ แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔

มาตรา ๑๐ ในการทำธุรกรรมทางอิเล็กทรอนิกส์ตามวิธีการแบบปลอดภัยตามพระราชกฤษฎีกานี้ผู้กระทำต้องคำนึงถึงหลักการพื้นฐานของการรักษาความลับ 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 แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์พ.ศ. ๒๕๔๔ บัญญัติให้ธุรกรรมทางอิเล็กทรอนิกส์ใดที่ได้กระทำตามวิธีการแบบปลอดภัยที่กำหนดในพระราชกฤษฎีกาแล้ว ให้สันนิษฐานว่าเป็นวิธีการที่เชื่อถือได้ จึงจำเป็นต้องตราพระราชกฤษฎีกานี้

ประวัติผู้เขียน

ชื่อ-นามสกุล	นายคมสัน สีหมนตรี	
วัน เดือน ปี เกิด	28 พฤษภาคม 2525	
ประวัติการศึกษา	ปีการศึกษา 2547	นิติศาสตรบัณฑิต มหาวิทยาลัยพายัพ
	ปีการศึกษา 2550	รัฐศาสตรบัณฑิต มหาวิทยาลัยสุโขทัยธรรมาธิราช ใบอนุญาตว่าความ รุ่นที่ 23
ประวัติการทำงาน	พ.ศ.2547-ปัจจุบัน	ทนายความประจำ บริษัท สัญลักษ์ทนายความ และที่ปรึกษากฎหมาย จำกัด