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 อบรม และเผยแพร่ให้พนักงานไว้ใช้งาน

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

<u>แนวปฏิบัติ</u>

(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

<u>แนวปฏิบัติ</u>

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