ประกาศธนาคารแห่งประเทศไทย

ที่ สนช. ๑๑/๒๕๖๑

เรื่อง นโยบายและมาตรการการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศ

---

๑. เหตุผลในการออกประกาศ

เพื่อให้มีมาตรฐานในการกำหนดนโยบายและมาตรการการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศ สำหรับการให้บริการระบบการชำระเงินที่มีความสำคัญ ระบบการชำระเงินภายใต้การกำกับ และบริการการชำระเงินภายใต้การกำกับ ตามกฎหมายว่าด้วยระบบการชำระเงิน และเพื่อใช้เป็นแนวทางกำหนดวิธีปฏิบัติในการตรวจสอบและรักษาความมั่นคงปลอดภัยของระบบสารสนเทศที่เกี่ยวข้องกับระบบการชำระเงินที่มีความสำคัญ ระบบการชำระเงินภายใต้การกำกับ และบริการการชำระเงินภายใต้การกำกับ ให้มีความน่าเชื่อถือ มีความมั่นคงปลอดภัย และสามารถให้บริการได้อย่างต่อเนื่อง

ธนาคารแห่งประเทศไทยได้กำหนดกรอบนโยบายและมาตรการการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศ ประกอบด้วย ๑) การควบคุมการเข้าถึง และการพิสูจน์ตัวตนผู้ใช้ ๒) การรักษาความลับของข้อมูล และความถูกต้องเชื่อถือได้ของระบบสารสนเทศ ๓) การรักษาสภาพความพร้อมใช้งานของการให้บริการ ๔) การตรวจสอบความมั่นคงปลอดภัยทางระบบสารสนเทศ เพื่อใช้เป็นแนวทางในการกำหนดมาตรการการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศที่เกี่ยวข้องกับระบบการชำระเงินที่มีความสำคัญ ระบบการชำระเงินภายใต้การกำกับ และบริการการชำระเงินภายใต้การกำกับ เพื่อให้ครอบคลุมและป้องกันความเสี่ยงทางระบบสารสนเทศได้อย่างมีประสิทธิภาพตามแนวทางที่เป็นมาตรฐานสากล นอกจากนี้ ผู้ให้บริการระบบการชำระเงินที่มีความสำคัญ และผู้ประกอบธุรกิจระบบการชำระเงินและบริการการชำระเงินภายใต้การกำกับ ต้องพิจารณาปรับใช้และกำหนดรายละเอียดของมาตรการการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศของผู้ให้บริการหรือผู้ประกอบธุรกิจให้เหมาะสมกับประเภทและความซับซ้อนของบริการตนเองด้วย

๒. อำนาจตามกฎหมาย

อาศัยอำนาจตามความในมาตรา ๗ และมาตรา ๒๔ แห่งพระราชบัญญัติว่าด้วยระบบการชำระเงิน พ.ศ. ๒๕๖๐ ธนาคารแห่งประเทศไทยกำหนดนโยบายและมาตรการการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศให้ผู้ให้บริการระบบการชำระเงินที่มีความสำคัญ ผู้ประกอบธุรกิจระบบการชำระเงินภายใต้การกำกับ และผู้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับตามความในประกาศฉบับนี้

๓. ขอบเขตการบังคับใช้

ประกาศฉบับนี้ให้ใช้บังคับกับผู้ให้บริการระบบการชำระเงินที่มีความสำคัญ ผู้ประกอบธุรกิจระบบการชำระเงินภายใต้การกำกับ และผู้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับตามกฎหมายว่าด้วยระบบการชำระเงิน

๔. เนื้อหา

๔.๑ นิยาม

ในประกาศฉบับนี้

“ผู้ให้บริการ” หมายความว่า ผู้ให้บริการระบบการชำระเงินที่มีความสำคัญตามกฎหมายว่าด้วยระบบการชำระเงิน

“ผู้ประกอบธุรกิจ” หมายความว่า ผู้ประกอบธุรกิจระบบการชำระเงินภายใต้การกำกับและผู้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับ ตามกฎหมายว่าด้วยระบบการชำระเงิน

“สมาชิก” หมายความว่า ผู้ใช้บริการที่ยินยอมผูกพันตามหลักเกณฑ์ในการใช้บริการระบบการชำระเงินที่มีความสำคัญ

“ผู้ใช้บริการ” หมายความว่า ผู้ใช้บริการจากผู้ประกอบธุรกิจที่ได้รับอนุญาตหรือขึ้นทะเบียนตามกฎหมายว่าด้วยระบบการชำระเงิน

๔.๒ นโยบายและมาตรการการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศ

ผู้ให้บริการระบบการชำระเงินที่มีความสำคัญ ผู้ประกอบธุรกิจระบบการชำระเงินภายใต้การกำกับ และผู้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับ ต้องถือปฏิบัติตามนโยบายและมาตรการการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศ ดังนี้

๔.๒.๑ นโยบายการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศ

(๑) ผู้ให้บริการหรือผู้ประกอบธุรกิจจะต้องจัดทำนโยบายการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศเป็นลายลักษณ์อักษร โดยได้รับการพิจารณาอนุมัติจากคณะกรรมการบริษัท ทั้งนี้ ผู้ให้บริการหรือผู้ประกอบธุรกิจจะต้องเผยแพร่นโยบายดังกล่าว และอบรมให้แก่บุคลากรที่เกี่ยวข้องเพื่อถือปฏิบัติ รวมทั้งจัดให้มีการทบทวนหรือปรับปรุงนโยบายให้เหมาะสมกับสถานการณ์อย่างสม่ำเสมอ

(๒) นโยบายการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศที่เกี่ยวข้องกับระบบการชำระเงินที่มีความสำคัญ การให้บริการระบบการชำระเงินภายใต้การกำกับ และการให้บริการการชำระเงินภายใต้การกำกับ แล้วแต่กรณี อย่างน้อยต้องครอบคลุมในเรื่องดังต่อไปนี้

(๒.๑) การควบคุมการเข้าถึง และการพิสูจน์ตัวตนผู้ใช้

(๒.๒) การรักษาความลับของข้อมูล และความถูกต้องเชื่อถือได้ของระบบสารสนเทศ

(๒.๓) การรักษาสภาพความพร้อมใช้งานของการให้บริการ

(๒.๔) การตรวจสอบความมั่นคงปลอดภัยทางระบบสารสนเทศ

๔.๒.๒ มาตรการการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศ

ผู้ให้บริการหรือผู้ประกอบธุรกิจต้องจัดให้มีมาตรการการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศที่เกี่ยวข้องกับระบบการชำระเงินที่มีความสำคัญ ระบบการชำระเงินภายใต้การกำกับ และบริการการชำระเงินภายใต้การกำกับ แล้วแต่กรณี ให้สอดคล้องกับนโยบายที่ได้กำหนดขึ้น และมาตรการดังกล่าวจะต้องเหมาะสมกับลักษณะของการให้บริการ โดยครอบคลุมถึงการควบคุมการเข้าถึงและการพิสูจน์ตัวตนผู้ใช้ การรักษาความลับของข้อมูล การรักษาความถูกต้องเชื่อถือได้ของระบบสารสนเทศ การรักษาสภาพความพร้อมใช้งานของการให้บริการ มีการแก้ไขปัญหาและการรายงาน รวมถึงจัดให้มีการตรวจสอบความมั่นคงปลอดภัยทางระบบสารสนเทศอย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง ตลอดจนจัดให้มีกระบวนการดูแลโดยคณะกรรมการบริษัทหรือผู้บริหารระดับสูง เพื่อให้มีการปฏิบัติตามมาตรการที่กำหนด ทั้งนี้ การตรวจสอบความมั่นคงปลอดภัยทางระบบสารสนเทศของผู้ให้บริการระบบการชำระเงินที่มีความสำคัญ ผู้ประกอบธุรกิจระบบการชำระเงินภายใต้การกำกับ และผู้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับ ให้ปฏิบัติตามประกาศธนาคารแห่งประเทศไทยที่เกี่ยวข้องกับหลักเกณฑ์การกำกับดูแลด้วย

นอกจากนี้ ผู้ให้บริการหรือผู้ประกอบธุรกิจต้องดำเนินการทบทวนหรือปรับปรุงมาตรการตามระยะเวลาที่กำหนดหรือเมื่อมีการเปลี่ยนแปลงที่ส่งผลกระทบกับนโยบายและมาตรการที่ได้กำหนดไว้ ตลอดจนจัดอบรมและให้ความรู้แก่บุคลากรที่เกี่ยวข้อง

ทั้งนี้ ธปท. ได้จัดทำแนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศเพื่อเป็นแนวทางในการกำหนดมาตรการการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศให้น่าเชื่อถือและให้เป็นที่ยอมรับของผู้ใช้บริการ โดยการกำหนดมาตรการการรักษาความมั่นคงปลอดภัยของผู้ให้บริการหรือผู้ประกอบธุรกิจแต่ละรายอาจแตกต่างกันได้ เพื่อให้ครอบคลุมและป้องกันความเสี่ยงทางระบบสารสนเทศได้อย่างมีประสิทธิภาพตามแนวทางที่เป็นมาตรฐานสากล

๕. บทเฉพาะกาล

ผู้ซึ่งให้บริการระบบการชำระเงินที่มีความสำคัญ หรือผู้ซึ่งประกอบกิจการระบบการชำระเงินภายใต้การกำกับ หรือผู้ซึ่งประกอบกิจการบริการการชำระเงินภายใต้การกำกับ อยู่ก่อนวันที่ประกาศนี้มีผลใช้บังคับ หากไม่สามารถเสนอนโยบายการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศให้คณะกรรมการบริษัทพิจารณาอนุมัติ ตามข้อ ๔.๒.๑ (๑) ให้ได้รับการยกเว้นการปฏิบัติตามหลักเกณฑ์ดังกล่าว แต่ทั้งนี้ ต้องดำเนินการให้เป็นไปตามหลักเกณฑ์ดังกล่าวภายใน ๙๐ วันนับแต่วันที่ได้รับอนุญาตหรือขึ้นทะเบียน แล้วแต่กรณี

๖. วันเริ่มต้นบังคับใช้

ประกาศนี้ให้ใช้บังคับตั้งแต่วันที่ ๑๖ เมษายน ๒๕๖๑ เป็นต้นไป

ประกาศ ณ วันที่ ๑๖ เมษายน พ.ศ. ๒๕๖๑
ฤชุกร สิริโยธิน
รองผู้ว่าการ ด้านเสถียรภาพสถาบันการเงิน
ผู้ว่าการแทน
ธนาคารแห่งประเทศไทย

<u>แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศที่เกี่ยวข้องกับระบบการชำระเงิน</u>

เพื่อสนับสนุนให้การให้บริการระบบการชำระเงินที่มีความสำคัญ การประกอบธุรกิจระบบการชำระเงินภายใต้การกำกับ และบริการการชำระเงินภายใต้การกำกับ เป็นไปอย่างมีประสิทธิภาพ ปลอดภัย ถูกต้อง และน่าเชื่อถือ ธนาคารแห่งประเทศไทยได้จัดทำแนวปฏิบัติเพื่อเป็นแนวทางในการกำหนดมาตรการการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศ ซึ่งเป็นเพียงกรอบแนวทางทั่วไป ผู้ให้บริการหรือผู้ประกอบธุรกิจอาจกำหนดมาตรการการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศของผู้ให้บริการหรือผู้ประกอบธุรกิจให้เหมาะสมกับประเภทและความซับซ้อนของบริการตนเองด้วย

สาระสำคัญของแนวปฏิบัติฉบับนี้ประกอบด้วย

1. การควบคุมการเข้าถึง และการพิสูจน์ตัวตนผู้ใช้

ผู้ให้บริการหรือผู้ประกอบธุรกิจต้องคำนึงถึงการกำหนดบุคลากรหรือหน่วยงานทางเทคโนโลยีสารสนเทศและการแบ่งแยกหน้าที่ให้เหมาะสม การควบคุมการเข้าถึงระบบสารสนเทศ การพิสูจน์ตัวตนผู้ใช้ และการป้องกันการปฏิเสธความรับผิด ดังนี้

1.1 การกำหนดบุคลากรหรือหน่วยงานทางระบบสารสนเทศ และการแบ่งแยกอำนาจหน้าที่ที่เหมาะสมในการบริหารจัดการทางระบบสารสนเทศ

ผู้ให้บริการหรือผู้ประกอบธุรกิจต้องกำหนดหน้าที่และความรับผิดชอบของบุคลากรหรือหน่วยงานที่ดูแลเกี่ยวกับความมั่นคงปลอดภัยทางระบบสารสนเทศ รวมถึงสร้างความตระหนัก ให้ความรู้ และมีการอบรมให้กับบุคลากรภายในองค์กร ตลอดจนจัดให้มีกระบวนการทางวินัยเพื่อลงโทษในกรณีฝ่าฝืนหรือละเมิดระเบียบปฏิบัติเกี่ยวกับความมั่นคงปลอดภัย

<u>แนวปฏิบัติ</u>

(1) มีการกำหนดหน้าที่ความรับผิดชอบ และแบ่งแยกหน้าที่ในการปฏิบัติงานด้านต่าง ๆ ที่เกี่ยวกับความมั่นคงปลอดภัยทางระบบสารสนเทศออกจากกันให้ชัดเจน ให้มีการถ่วงดุลอำนาจ เพื่อป้องกันความเสี่ยงในการปฏิบัติการที่อาจเกิดขึ้น

(2) มีการอบรม เพิ่มเติมความรู้ สร้างความตระหนัก ตลอดจนการสื่อสารให้ความรู้แก่บุคลากรภายในองค์กรอย่างสม่ำเสมอ เพื่อให้เท่าทันเทคโนโลยีและภัยคุกคามใหม่ ๆ

(3) มีกระบวนการทางวินัย เพื่อลงโทษบุคลากรที่ฝ่าฝืน ละเมิดนโยบายหรือระเบียบปฏิบัติเกี่ยวกับความมั่นคงปลอดภัยทางระบบสารสนเทศ

1.2 การควบคุมการเข้าถึงระบบสารสนเทศ

ผู้ให้บริการหรือผู้ประกอบธุรกิจต้องจัดให้มีขั้นตอนปฏิบัติที่เป็นลายลักษณ์อักษรสำหรับการควบคุม และจำกัดสิทธิการใช้ระบบสารสนเทศที่เกี่ยวกับการให้บริการและข้อมูลตามความจำเป็นในการใช้งาน เพื่อป้องกันการลักลอบการเข้าถึงระบบโดยผู้ที่ไม่มีสิทธิ ทั้งจากภายในและภายนอกองค์กร

<u>แนวปฏิบัติ</u>

(1) ทำทะเบียนทรัพย์สิน หรืออุปกรณ์ระบบสารสนเทศให้ถูกต้องอยู่เสมอ รวมถึงจัดให้มีผู้รับผิดชอบดูแลทรัพย์สินเหล่านั้น

(2) มีกฎ ระเบียบ ในการใช้ระบบสารสนเทศ และทรัพย์สินที่เกี่ยวข้องกับระบบสารสนเทศที่เหมาะสม

(3) มีการควบคุม และป้องกันการเข้าถึงสถานที่ตั้ง การควบคุมการเข้าถึงอุปกรณ์และระบบสารสนเทศที่เกี่ยวกับการให้บริการ โดยกระบวนการดังกล่าวครอบคลุมถึง

(3.1) การจัดวาง ติดตั้งอุปกรณ์ที่เกี่ยวกับการให้บริการที่เป็นสัดส่วน แบ่งเขตควบคุมอุปกรณ์สำคัญ จัดให้มีการควบคุมการเข้าออกบริเวณพื้นที่ควบคุม เพื่อป้องกันการลักลอบเข้าถึงโดยผู้ไม่มีสิทธิ ทั้งภายในและภายนอกองค์กร

(3.2) กำหนดวิธีการในการบริหารจัดการและสิทธิการเข้าถึงระบบสารสนเทศที่เกี่ยวกับการให้บริการ โดยแบ่งแยกตามระดับอำนาจหน้าที่ และจัดให้มีการตรวจสอบสิทธิในการเข้าถึงระบบสารสนเทศดังกล่าว ทั้งจากสมาชิก ผู้ใช้บริการ และบุคลากรที่เกี่ยวข้องก่อนอนุญาตให้เข้าใช้ระบบ โดยต้องทบทวนและปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

(3.3) กำหนดให้มีการบันทึกการเข้าใช้ระบบสารสนเทศของสมาชิก ผู้ใช้บริการและบุคลากรที่เกี่ยวข้อง เพื่อใช้ประโยชน์ในการตรวจสอบติดตามความผิดปกติต่าง ๆ ที่อาจเกิดขึ้น และจัดให้มีการสอบทานโดยหน่วยงานด้านความมั่นคงปลอดภัยทางระบบสารสนเทศ หรือหน่วยงานที่มีความเป็นอิสระอย่างสม่ำเสมอ

1.3 การตรวจสอบตัวตน และการป้องกันการปฏิเสธความรับผิด

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

<u>แนวปฏิบัติ</u>

(1) มีวิธีการระบุ หรือตรวจสอบ หรือพิสูจน์ตัวตนก่อนเข้าใช้ระบบสารสนเทศของสมาชิก ผู้ใช้บริการ และบุคลากรที่เกี่ยวข้อง เพื่อให้ทราบได้ว่าการเข้าใช้งานนั้นมาจากผู้มีสิทธิในการเข้าถึงระบบสารสนเทศ รวมทั้งป้องกันไม่ให้มีการปฏิเสธความรับผิด หรือข้อโต้แย้งในการทำรายการ

(2) มีการบันทึกรายละเอียดการเข้าถึงระบบสารสนเทศไว้เป็นหลักฐานสำหรับการตรวจสอบกรณีเกิดปัญหา เพื่อป้องกันการปฏิเสธความรับผิด

2. การรักษาความลับของข้อมูล และความถูกต้องเชื่อถือได้ของระบบสารสนเทศ

ผู้ให้บริการหรือผู้ประกอบธุรกิจต้องกำหนดมาตรการในการรักษาความลับของข้อมูล และการรักษาความถูกต้องเชื่อถือได้ของระบบสารสนเทศที่ให้บริการ เช่น การพัฒนา การควบคุม การเปลี่ยนแปลง การปรับปรุงแก้ไขระบบหรืออุปกรณ์ประมวลผลสารสนเทศ และการจัดการระบบเครือข่ายที่เกี่ยวกับการให้บริการเพื่อให้ระบบสารสนเทศมีความถูกต้องอยู่เสมอ

2.1 การรักษาความลับของข้อมูล

ผู้ให้บริการหรือผู้ประกอบธุรกิจต้องกำหนดขั้นตอน วิธีการในการรับส่ง ประมวลผล และการจัดเก็บข้อมูลอย่างเหมาะสม เพื่อรักษาความลับ ความถูกต้องสมบูรณ์ของข้อมูล

<u>แนวปฏิบัติ</u>

(1) กำหนดชั้นความลับของข้อมูลตามระดับความสำคัญ รวมถึงกำหนดสิทธิผู้ที่สามารถเข้าถึงข้อมูลความลับดังกล่าว โดยให้ครอบคลุมถึงการจัดการและเก็บรักษาข้อมูลส่วนบุคคลของสมาชิกหรือผู้ใช้บริการ เพื่อให้เป็นไปตามหลักเกณฑ์หรือกฎหมายที่เกี่ยวข้องด้วย

(2) มีวิธีการรับส่ง การประมวลผล และการจัดเก็บข้อมูลลับในลักษณะที่มั่นคงปลอดภัยตามระดับความสำคัญ เพื่อป้องกันการเข้าแก้ไขเปลี่ยนแปลงโดยผู้ที่ไม่มีสิทธิหรือไม่ได้รับอนุญาต

(3) กำหนดวิธีปฏิบัติในการจัดเก็บ ใช้งาน และทำลายข้อมูลแต่ละประเภทชั้นความลับ

2.2 การพัฒนาระบบ การควบคุมการเปลี่ยนแปลง การปรับปรุงแก้ไขระบบสารสนเทศหรืออุปกรณ์ประมวลผลสารสนเทศ

ผู้ให้บริการหรือผู้ประกอบธุรกิจต้องกำหนดขั้นตอนปฏิบัติและการควบคุมภายในอย่างเป็นระบบสำหรับการพัฒนาและการควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบสารสนเทศ เพื่อลดความเสี่ยงที่จะทำให้ระบบที่ให้บริการเกิดความเสียหายหรือทำงานผิดปกติ

<u>แนวปฏิบัติ</u>

(1) มีกระบวนการในการพัฒนาระบบงานให้มีความถูกต้องเชื่อถือได้ โดยครอบคลุมตั้งแต่กระบวนการออกแบบระบบ พัฒนา ทดสอบ และนำออกใช้งาน โดยต้องจัดให้มีการประเมินช่องโหว่ของระบบ (Vulnerability Assessment) และการทดสอบเจาะระบบ (Penetration Test) โดยผู้เชี่ยวชาญภายนอกสำหรับระบบงานสำคัญที่มีการเชื่อมต่อกับเครือข่ายสาธารณะก่อนนำออกใช้งาน และจัดให้มีการแยกระบบสำหรับการพัฒนา และระบบที่ใช้งานจริงออกจากกัน ซึ่งอาจเป็นการแยกอุปกรณ์เป็นคนละเครื่อง และใช้ผู้ควบคุมระบบแยกกัน

(2) มีขั้นตอนปฏิบัติสำหรับการควบคุมการแก้ไขเปลี่ยนแปลงข้อมูลในกระบวนการประมวลผล การรับส่งข้อมูล การจัดเก็บ การจัดหา การปรับปรุงอุปกรณ์ และการพัฒนาระบบสารสนเทศ เช่น มีขั้นตอนการประเมินผลกระทบที่เกี่ยวข้อง การอนุมัติจากผู้มีอำนาจ ขั้นตอนการพัฒนา หรือ

ปรับปรุงแก้ไข การทดสอบก่อนดำเนินการ รวมถึงการบันทึกการแก้ไขเปลี่ยนแปลง การแจ้งให้ผู้ที่ได้รับผลกระทบจากการเปลี่ยนแปลงนั้นได้รับทราบ และปรับปรุงเอกสารที่เกี่ยวข้อง

(3) การใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการภายนอก

(3.1) มีสัญญาดำเนินการเป็นลายลักษณ์อักษร ระบุขอบเขตการดำเนินงาน หน้าที่ความรับผิดชอบของคู่สัญญาแต่ละฝ่ายให้ชัดเจน

(3.2) มีการบริหารความเสี่ยงในการใช้บริการจากผู้ให้บริการภายนอก รวมทั้งการคัดเลือก การติดตาม การประเมิน และการตรวจสอบการให้บริการอย่างเหมาะสม

(3.3) มีการรักษาความมั่นคงปลอดภัยของข้อมูล ซึ่งรวมถึงการรักษาความลับและความเป็นส่วนตัวของข้อมูลสมาชิกหรือผู้ใช้บริการ

(3.4) มีความรับผิดชอบต่อสมาชิกหรือผู้ใช้บริการในการให้บริการที่ต่อเนื่องมั่นคงปลอดภัย และน่าเชื่อถือเสมือนกับการให้บริการโดยผู้ให้บริการหรือผู้ประกอบธุรกิจเอง

(3.5) จัดทำแผนฉุกเฉินสำหรับการดำเนินการด้านงานเทคโนโลยีสารสนเทศของผู้ให้บริการภายนอกให้สอดคล้องกับแผนฉุกเฉินของผู้ให้บริการหรือผู้ประกอบธุรกิจ

(4) จัดทำคู่มือต่าง ๆ ที่เกี่ยวข้องกับระบบสารสนเทศที่ให้บริการ อบรม และเผยแพร่ให้พนักงานไว้ใช้งาน

2.3 การจัดการเครือข่ายที่เกี่ยวกับการให้บริการ

ผู้ให้บริการหรือผู้ประกอบธุรกิจต้องกำหนดมาตรการป้องกันการเข้าถึงระบบที่ให้บริการทางเครือข่ายโดยไม่ได้รับอนุญาต

<u>แนวปฏิบัติ</u>

(1) บริหารจัดการเครือข่ายที่เกี่ยวกับการให้บริการ เพื่อป้องกันภัยคุกคามทางเครือข่าย หรือข้อมูลที่ส่งผ่านทางเครือข่าย เช่น

(1.1) กำหนดมาตรการควบคุมการเชื่อมต่อทางเครือข่าย การอนุญาตการเชื่อมต่อโดยอุปกรณ์จากภายนอก

(1.2) การตรวจสอบตัวตนในการใช้งานเครือข่าย

(1.3) การแบ่งแยกเครือข่ายตามกลุ่มบริการสารสนเทศ

(1.4) ติดตั้งโปรแกรมป้องกันภัยคุกคามจากภายนอก

(2) มีมาตรการควบคุมและป้องกันภัยคุกคามต่าง ๆ ที่มีประสิทธิภาพและปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

3. การรักษาสภาพความพร้อมใช้งานของการให้บริการ

ผู้ให้บริการหรือผู้ประกอบธุรกิจต้องจัดให้มีการให้บริการที่มีประสิทธิภาพและมีสภาพความพร้อมใช้งานในการให้บริการตลอดเวลา สามารถรองรับการทำธุรกรรมตามความต้องการของ

สมาชิกหรือผู้ใช้บริการได้อย่างพอเพียง ตอบสนองการทำธุรกรรมได้อย่างรวดเร็วทั้งในเวลาปกติและเวลาที่มีการใช้บริการอย่างหนาแน่น (Peak Time) รวมทั้งมีการสำรองข้อมูลอย่างเหมาะสม เพื่อให้สามารถกู้ระบบให้กลับมาทำงานได้ตามปกติ ในกรณีที่ระบบเกิดความเสียหาย

3.1 การประเมิน และจัดการความเสี่ยงของระบบที่ให้บริการ

ผู้ให้บริการหรือผู้ประกอบธุรกิจต้องมีวิธีการประเมินความเสี่ยงของระบบที่ให้บริการที่เหมาะสม กำหนดเกณฑ์ในการยอมรับความเสี่ยงและระบุระดับความเสี่ยงที่ยอมรับได้ รวมถึงกำหนดวิธีการจัดการความเสี่ยงที่อาจเกิดขึ้น ทั้งนี้ ผู้ให้บริการและผู้ประกอบธุรกิจต้องจัดให้มีการทบทวนความเสี่ยงอยู่เสมอ ให้สอดคล้องกับพัฒนาการทางเทคโนโลยีและสถานการณ์ปัจจุบัน

<u>แนวปฏิบัติ</u>

(1) กำหนดวิธีการประเมินความเสี่ยงที่เป็นรูปธรรม

(2) วิเคราะห์และประเมินผลกระทบที่มีต่อธุรกิจที่อาจเป็นผลจากความล้มเหลวของการรักษาความมั่นคงปลอดภัย

(3) กำหนดเกณฑ์ในการยอมรับความเสี่ยง และระดับความเสี่ยงที่ยอมรับได้

(4) ระบุและประเมินทางเลือกในการจัดการกับความเสี่ยงในการดำเนินการที่อาจเกิดขึ้นได้ เพื่อหลีกเลี่ยงความเสี่ยงและลดความเสียหายที่จะเกิดขึ้น

3.2 การติดตามตรวจสอบความผิดปกติและช่องโหว่ของระบบสารสนเทศ

ผู้ให้บริการหรือผู้ประกอบธุรกิจต้องกำหนดให้มีการติดตาม ตรวจสอบความผิดปกติตลอดจนข้อมูลข่าวสารที่เกี่ยวกับช่องโหว่ในระบบต่าง ๆ ที่ให้บริการ เพื่อประเมินความเสี่ยงและกำหนดมาตรการรองรับเพื่อลดความเสี่ยงดังกล่าว

<u>แนวปฏิบัติ</u>

(1) ติดตามตรวจสอบรายการที่ไม่ปกติ และโอกาสที่จะเกิดภัยคุกคาม หรือการลักลอบเข้าถึงระบบสารสนเทศ

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

(3) กรณีระบบมีความเสี่ยงสูง เช่น ระบบที่ให้บริการผ่านเครือข่ายสาธารณะ ควรจัดให้มีการทดสอบเจาะระบบ (Penetration Test) เพื่อทดสอบประสิทธิภาพของเทคโนโลยีการรักษาความมั่นคงปลอดภัย

3.3 การแก้ไขปัญหา บันทึกเหตุการณ์ และการรายงาน กรณีระบบสารสนเทศได้รับความเสียหาย

ผู้ให้บริการหรือผู้ประกอบธุรกิจต้องมีการติดตาม บันทึก และรายงานเหตุการณ์ละเมิดความมั่นคงปลอดภัย ผ่านช่องทางการรายงานที่กำหนดไว้ โดยดำเนินการอย่างรวดเร็วที่สุด

เท่าที่จะทำได้ รวมทั้งให้มีการเรียนรู้จากเหตุการณ์ที่เกิดขึ้นแล้ว เพื่อเตรียมการป้องกันที่จำเป็นไว้ล่วงหน้า

แนวปฏิบัติ

(1) กำหนดขั้นตอนการแก้ไขปัญหา ทีมงานหรือผู้รับผิดชอบ รวมถึงวิธีการรายงานปัญหาให้กับผู้บริหาร และแจ้งให้กับผู้เกี่ยวข้องทราบ

(2) เก็บรวบรวมหลักฐานต่าง ๆ ที่เป็นประโยชน์

(3) บันทึกเหตุการณ์ หรือจัดทำรายงานที่เป็นลายลักษณ์อักษรเพื่อเก็บไว้เป็นแนวทางในการแก้ปัญหา

3.4 การสำรองข้อมูล

ผู้ให้บริการหรือผู้ประกอบธุรกิจต้องจัดให้มีการสำรองและทดสอบข้อมูลที่สำรองเก็บไว้อย่างสม่ำเสมอ เพื่อรักษาความถูกต้องสมบูรณ์ และสภาพความพร้อมใช้งานของการให้บริการ

แนวปฏิบัติ

(1) สำรองข้อมูลที่สำคัญ และข้อมูลอื่นที่จำเป็นต่อการปฏิบัติงาน เพื่อให้มีข้อมูลพร้อมใช้ภายในประเทศ สำหรับการดำเนินธุรกิจและการให้บริการแก่ลูกค้าอย่างต่อเนื่อง

(2) กำหนดวิธีปฏิบัติ หรือขั้นตอนในการสำรองข้อมูลให้เหมาะสม และสอดคล้องกับความเสี่ยงของรูปแบบหรือลักษณะการให้บริการระบบการชำระเงินที่มีความสำคัญ การประกอบธุรกิจระบบการชำระเงินภายใต้การกำกับและบริการการชำระเงินภายใต้การกำกับ แล้วแต่กรณี เช่น ข้อมูลที่จะสำรอง ความถี่ในการสำรองข้อมูล สื่อที่ใช้ สถานที่เก็บ วิธีการเก็บรักษา และการนำมาใช้งาน

(3) ทดสอบข้อมูลที่เก็บสำรองไว้อย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง และให้เป็นไปตามนโยบายการสำรองข้อมูลของผู้ให้บริการหรือผู้ประกอบธุรกิจ

3.5 การจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง หรือแผนฉุกเฉินทางระบบสารสนเทศ

ผู้ให้บริการหรือผู้ประกอบธุรกิจต้องจัดทำแผนสร้างความต่อเนื่องให้กับการให้บริการระบบการชำระเงินที่มีความสำคัญ ระบบการชำระเงินภายใต้การกำกับ หรือบริการการชำระเงินภายใต้การกำกับ แล้วแต่กรณี และนำแผนมาดำเนินการเพื่อให้บริการสามารถดำเนินต่อไปได้ตามระยะเวลาที่กำหนดไว้หลังจากที่มีเหตุการณ์ที่ทำให้บริการหยุดชะงัก

แนวปฏิบัติ

(1) วิเคราะห์และระบุความเสี่ยง และการดำเนินงานที่สำคัญของการให้บริการ

(2) กำหนดระยะเวลาหยุดดำเนินงานที่ยอมรับได้ (Recovery Time Objectives)

(3) จัดทำแผนเป็นลายลักษณ์อักษร กำหนดขั้นตอนรายละเอียดการดำเนินการเมื่อมีการหยุดชะงักของการดำเนินงานที่สำคัญ เพื่อให้สามารถกลับมาดำเนินงานได้ตามระยะเวลาที่กำหนด รายละเอียดของแผนอย่างน้อยประกอบด้วย

(3.1) ชื่อแผน

(3.2) วัตถุประสงค์ และขอบเขตของแผน

(3.3) รายละเอียดของระบบเทคโนโลยีสารสนเทศ ทรัพยากรที่จำเป็น สำหรับปฏิบัติงานทดแทน

(3.4) ผู้รับผิดชอบ ผู้มีอำนาจตัดสินใจ การติดต่อสื่อสารกับผู้เกี่ยวข้องทั้งภายในและภายนอก

(3.5) วิธีการปฏิบัติกรณีเกิดปัญหา และสถานที่ปฏิบัติงานทดแทน

(4) จัดให้มีการฝึกอบรมแผนแก่พนักงานและผู้มีส่วนเกี่ยวข้องกับการดำเนินการตามแผนอย่างสม่ำเสมอ

(5) ทดสอบและทบทวนแผนสำหรับการดำเนินงานที่สำคัญอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงปัจจัยที่มีผลต่อความเสี่ยง

3.6 การบำรุงรักษาอุปกรณ์ระบบสารสนเทศ

ผู้ให้บริการหรือผู้ประกอบธุรกิจต้องกำหนดให้มีการบำรุงรักษาอุปกรณ์ต่าง ๆ อย่างสม่ำเสมอ เพื่อให้อุปกรณ์ทำงานได้อย่างต่อเนื่อง และอยู่ในสภาพที่มีความสมบูรณ์ต่อการใช้งาน

4. การตรวจสอบความมั่นคงปลอดภัยทางระบบสารสนเทศ

ผู้ให้บริการหรือผู้ประกอบธุรกิจจะต้องจัดให้มีการตรวจสอบความมั่นคงปลอดภัยทางระบบสารสนเทศอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่านโยบายและมาตรการการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศที่เกี่ยวข้องกับการให้บริการเป็นไปอย่างมีประสิทธิภาพ มั่นคงปลอดภัยสามารถให้บริการได้อย่างต่อเนื่อง พร้อมจัดส่งสำเนาผลการตรวจสอบให้ ธปท. ภายใน 45 วันนับแต่วันที่ทำการตรวจสอบแล้วเสร็จ

<u>แนวปฏิบัติ</u>

(1) จัดให้มีผู้ตรวจสอบและดำเนินการตรวจสอบความมั่นคงปลอดภัยทางระบบสารสนเทศในเรื่องที่มีความเสี่ยงหรือมีความสำคัญต่อการให้บริการ อย่างน้อยปีละ 1 ครั้ง และจัดทำรายงานผลการตรวจสอบเสนอคณะกรรมการบริษัทหรือคณะกรรมการที่ได้รับมอบหมาย เพื่อพิจารณาระดับความเสี่ยงที่เป็นอยู่และกำหนดแนวทางการปรับปรุง และแจ้งให้หน่วยงานภายในที่เกี่ยวข้องทราบเพื่อนำไปปฏิบัติ

(2) ติดตาม ตรวจสอบการให้บริการระบบการชำระเงินที่มีความสำคัญ ระบบการชำระเงินภายใต้การกำกับ และบริการการชำระเงินภายใต้การกำกับ แล้วแต่กรณี ให้เป็นไปตามกฎระเบียบข้อบังคับที่เกี่ยวข้องทั้งหมด เพื่อหลีกเลี่ยงการละเมิดข้อกำหนดทางกฎหมาย ระเบียบปฏิบัติ ข้อกำหนดในสัญญา และข้อกำหนดด้านความมั่นคงปลอดภัย

5. การทบทวนหรือปรับปรุงมาตรการการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศ

ผู้ให้บริการหรือผู้ประกอบธุรกิจต้องดำเนินการทบทวนหรือปรับปรุงมาตรการการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศอย่างน้อยปีละครั้งหรือเมื่อมีการเปลี่ยนแปลงที่ส่งผลกระทบกับนโยบายและมาตรการที่ได้กำหนดไว้ ตลอดจนจัดอบรมและให้ความรู้แก่บุคลากรที่เกี่ยวข้อง

นอกจากนี้ ผู้ให้บริการหรือผู้ประกอบธุรกิจ ควรจัดให้มีความพร้อมในการรักษาความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศเพื่อรับมือกับภัยคุกคามทางไซเบอร์ โดยให้ครอบคลุมถึงการกำกับดูแลความเสี่ยงจากภัยไซเบอร์ การป้องกัน (Protection) การเฝ้าระวังและตรวจจับ (Detection) และการตอบสนองต่อเหตุการณ์และการกู้คืน (Response and Recovery) ตามความจำเป็นและเหมาะสมกับความเสี่ยง และความซับซ้อนของรูปแบบบริการ

ฝ่ายนโยบายระบบการชำระเงิน
ธนาคารแห่งประเทศไทย