ธนาคารแห่งประเทศไทย

1 กุมภาพันธ์ 2564

เรียน ผู้จัดการ
สถาบันผู้ใช้บริการบาทเนต

ที่ ฝชพ.(ว.) 3 /2564 เรื่อง นำส่งแนวปฏิบัติ เรื่อง การรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ลูกข่ายของผู้ใช้บริการบาทเนต

ธนาคารแห่งประเทศไทย (ธปท.) ขอนำส่งแนวปฏิบัติ เรื่อง การรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ลูกข่ายของผู้ใช้บริการบาทเนต (เอกสารแนบ) ซึ่งได้ปรับปรุงการรักษาความมั่นคงปลอดภัยของคอมพิวเตอร์ลูกข่ายให้ครอบคลุมถึงการบริหารจัดการความเสี่ยงจากภัยฉ้อโกง (Fraud Incident) ตามแนวทางของ Bank of International Settlement - Committee on Payments and Market Infrastructures (BIS-CPMI) ที่ได้เผยแพร่ลงในเอกสาร "Reducing the risk of wholesale payments fraud related to endpoint security: a toolkit" เมื่อเดือนตุลาคม 2562 เพื่อให้สถาบันผู้ใช้บริการบาทเนตนำไปปรับให้สอดคล้องกับสภาพแวดล้อม และสามารถบริหารจัดการความเสี่ยงจากการฉ้อโกงที่เกี่ยวข้องกับการโอนเงินผ่านระบบบาทเนตได้อย่างเหมาะสม ทันการณ์

สาระสำคัญของการปรับปรุงแนวปฏิบัติฉบับนี้ คือ สถาบันผู้ใช้บริการบาทเนตมีแนวทางในการปฏิบัติตามมาตรการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศ รวมถึงแนวทางในการบริหารจัดการความเสี่ยงจากภัยฉ้อโกงที่เกี่ยวข้องกับการโอนเงินผ่านระบบบาทเนต ซึ่งสอดคล้องกับแนวทางของ BIS–CPMI ในการจัดการความเสี่ยงจากการฉ้อโกงที่เกี่ยวข้องกับการโอนเงินผ่านระบบ RTGS ของธนาคารกลางในระดับสากล

จึงเรียนมาเพื่อโปรดทราบและถือปฏิบัติ

ขอแสดงความนับถือ

(นายบัญชา มนูญกุลชัย)
ผู้อำนวยการอาวุโส ฝ่ายการชำระเงินและพันธบัตร
ผู้ว่าการแทน

สิ่งที่ส่งมาด้วย แนวปฏิบัติ เรื่อง การรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ลูกข่ายของผู้ใช้บริการบาทเนต

ฝ่ายการชำระเงินและพันธบัตร
โทรศัพท์ 0 2356 7665, 0 2283 5900

หมายเหตุ [ ] ธนาคารแห่งประเทศไทยจะจัดให้มีการประชุมชี้แจงในวันที่ ..... ณ .....
[×] ไม่มีการจัดประชุมชี้แจง

แนวปฏิบัติ

เรื่อง การรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ลูกข่ายของผู้ใช้บริการบาทเนต

1 กุมภาพันธ์ 2564

ธนาคารแห่งประเทศไทย

จัดทำโดย

ฝ่ายการชำระเงินและพันธบัตร

สายระบบข้อสนเทศ

ธนาคารแห่งประเทศไทย

โทรศัพท์ 0 2283 5034

e-mail : PBD-CPMIEndpoint@bot.or.th

สารบัญ

หัวข้อ **หน้า**

แนวปฏิบัติธนาคารแห่งประเทศไทย

เรื่อง การรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ลูกข่ายของผู้ใช้บริการบาทเนต

---

1. เหตุผลในการออกแนวปฏิบัติ

ปัจจุบันอาชญากรรมทางคอมพิวเตอร์ รวมถึงการฉ้อโกงรูปแบบใหม่ ๆ มีการพัฒนาและก้าวหน้ามากขึ้น และอาจก่อให้เกิดความเสียหายแก่ผู้ใช้บริการบาทเนต เพื่อลดผลกระทบและลดความเสี่ยงจากภัยคุกคามดังกล่าว ผู้ใช้บริการบาทเนตต้องมีนโยบายและกระบวนการรักษาความมั่นคงปลอดภัยของระบบคอมพิวเตอร์ที่ใช้เชื่อมโยงกับระบบบาทเนตของธนาคารแห่งประเทศไทย (ธปท.) ตามมาตรฐานที่ยอมรับได้ และสอดคล้องกับแนวทางในการจัดการความเสี่ยงจากการฉ้อโกง (Fraud Incident) ที่เกี่ยวข้องกับการโอนเงินผ่านระบบ RTGS ของ Bank of International Settlement - Committee on Payments and Market Infrastructures (BIS-CPMI) [1/]

ธปท. จึงได้ปรับปรุง "แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ลูกข่ายของผู้ใช้บริการบาทเนต" ลงวันที่ 15 สิงหาคม 2559 โดยเพิ่มเติมในส่วนของการบริหารจัดการความเสี่ยงจากการฉ้อโกง ให้สอดคล้องตามแนวทางของ BIS-CPMI เพื่อกำหนดแนวทางดำเนินการสำหรับผู้ใช้บริการบาทเนตในการรักษาความมั่นคงปลอดภัยของ "คอมพิวเตอร์ลูกข่าย" ซึ่งเป็นระบบคอมพิวเตอร์ที่เชื่อมโยงกับระบบบาทเนตของ ธปท. ทั้งในส่วนของระบบคอมพิวเตอร์สำหรับการส่งข้อความผ่านสวิฟท์ (SWIFT) บริการด้านการเงินด้วยวิธีอิเล็กทรอนิกส์ (Electronic Financial Services) และระบบงานคอมพิวเตอร์อื่นที่เชื่อมโยงเพื่อการรับส่งข้อมูลโดยตรงกับระบบคอมพิวเตอร์แม่ข่ายของ ธปท. (Host to Host) ให้มีความชัดเจน ปลอดภัย ถูกต้อง และน่าเชื่อถือ ป้องกันระบบคอมพิวเตอร์จากภัยคุกคาม การลักลอบเข้าถึงและการโจรกรรมข้อมูลสำคัญทั้งของผู้ใช้บริการบาทเนต และลูกค้า อันจะนำไปสู่ความเสียหายทางการเงิน ความเสียหายต่อชื่อเสียง และการขาดความเชื่อมั่นของผู้ใช้บริการต่อการให้บริการทางการเงินโดยรวม

ทั้งนี้ ผู้ใช้บริการบาทเนตสามารถกำหนดมาตรการรักษาความมั่นคงปลอดภัย ที่แตกต่างจากแนวปฏิบัติฉบับนี้ได้ หากมาตรการดังกล่าวมีความสอดคล้องและสามารถป้องกันความเสี่ยงของคอมพิวเตอร์ลูกข่ายได้อย่างมีประสิทธิภาพและเป็นไปตามมาตรฐานที่ยอมรับได้ นอกจากนี้ ผู้ใช้บริการบาทเนตต้องดำเนินการให้มีการรักษาความมั่นคงปลอดภัยในองค์กรตามข้อกำหนดในระเบียบ ธปท. ว่าด้วยการบริการบาทเนต และหลักเกณฑ์การกำกับดูแลตามกฎหมายที่ควบคุมการประกอบธุรกิจนั้นเป็นการเฉพาะ (ตามภาคผนวก) เพื่อให้มั่นใจว่ากระบวนการทำงานและธุรกรรมมีการรักษาความมั่นคงปลอดภัยที่ดี สอดคล้องกับข้อกำหนดตามกฎหมายในปัจจุบัน และเป็นไปตามมาตรฐานสากล รวมทั้งมีการปรับปรุงเพิ่มเติมหากมีข้อกำหนดเพิ่มขึ้นในอนาคต

2. ขอบเขตการบังคับใช้

แนวปฏิบัตินี้เป็นกรอบแนวทางให้สถาบันผู้ใช้บริการบาทเนต ทั้งที่เป็นสถาบันการเงินและไม่ใช่สถาบันการเงิน ใช้กำหนดมาตรการรักษาความมั่นคงปลอดภัยของคอมพิวเตอร์ลูกข่าย

[1/] อ้างอิงตามเอกสาร Reducing the risk of wholesale payments fraud related to endpoint security: a toolkit (https://www.bis.org/cpmi/publ/d188.pdf)

3. แนวปฏิบัติที่ยกเลิก

ให้ยกเลิกแนวปฏิบัติธนาคารแห่งประเทศไทย การรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ลูกข่ายของผู้ใช้บริการบาทเนต ลงวันที่ 15 สิงหาคม 2559 โดยให้ใช้แนวปฏิบัติฉบับนี้แทน

4. เนื้อหา

4.1 ความหมาย ในแนวปฏิบัติฉบับนี้

"แนวปฏิบัติ" หมายถึง แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ลูกข่ายของผู้ใช้บริการบาทเนต

"คอมพิวเตอร์ลูกข่าย" หมายถึง ระบบคอมพิวเตอร์ของผู้ใช้บริการบาทเนตที่ใช้เชื่อมโยงกับระบบบาทเนตของ ธปท. ได้แก่ ระบบคอมพิวเตอร์สำหรับการส่งข้อความผ่าน SWIFT บริการด้านการเงินด้วยวิธีอิเล็กทรอนิกส์ (Electronic Financial Services) และระบบงานคอมพิวเตอร์อื่นที่เชื่อมโยงเพื่อการรับส่งข้อมูลโดยตรงกับระบบคอมพิวเตอร์แม่ข่ายของ ธปท. (Host to Host)

"ระบบคอมพิวเตอร์" หมายถึง งานด้านเทคโนโลยีสารสนเทศที่ครอบคลุมถึง เครื่องคอมพิวเตอร์และอุปกรณ์รอบข้าง (Hardware) ระบบงาน (Application) ข้อมูล (Information) โครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ (Infrastructure) เครือข่าย (Network) บุคลากร (People) และกระบวนการจัดการด้านเทคโนโลยีสารสนเทศ (Process)

"ความมั่นคงปลอดภัย" หมายถึง การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-repudiation) และความน่าเชื่อถือ (Reliability)

"เหตุการณ์ละเมิดต่อความมั่นคงปลอดภัย" หมายถึง เหตุการณ์ หรือการกระทำที่มีเจตนาทำให้มีความเสี่ยง หรือก่อให้เกิดผลกระทบต่อความมั่นคงปลอดภัยของคอมพิวเตอร์ลูกข่าย รวมถึงการฉ้อโกงอันนำไปสู่ความเสียหายทางการเงิน ความเสียหายต่อชื่อเสียง และการขาดความเชื่อมั่นของผู้ใช้บริการต่อการให้บริการทางการเงินโดยรวม

4.2 รายละเอียดของแนวปฏิบัติ

4.2.1 <u>การควบคุมเครือข่ายและระบบคอมพิวเตอร์</u>

ผู้ใช้บริการบาทเนตต้องกำหนดมาตรการรักษาความมั่นคงปลอดภัย รวมถึงควบคุมการเปลี่ยนแปลงของเครือข่าย และระบบคอมพิวเตอร์ที่เชื่อมโยงกับคอมพิวเตอร์ลูกข่าย เพื่อป้องกันผู้ประสงค์ร้ายที่จะลักลอบเข้าทางเครือข่ายหรือระบบงานอื่น ทั้งนี้ มาตรการดังกล่าวควรครอบคลุมถึง

(1) ควบคุมการเข้าถึงศูนย์คอมพิวเตอร์ของผู้ใช้บริการบาทเนต รวมถึงอุปกรณ์ Network ที่เชื่อมต่อกับบาทเนต

(2) จัดให้มีการรักษาความมั่นคงปลอดภัยของเครือข่ายที่เชื่อมต่อระหว่างคอมพิวเตอร์ลูกข่ายกับบาทเนตของ ธปท. เช่น การติดตั้ง Firewall เป็นต้น

(3) แบ่งแยกเครือข่ายคอมพิวเตอร์ลูกข่ายออกจากเครือข่ายอื่นที่ไม่จำเป็นต้องเชื่อมโยงกับคอมพิวเตอร์ลูกข่าย เช่น แยกเครือข่ายของกลุ่มเครื่องคอมพิวเตอร์ลูกข่ายจากเครือข่ายสำหรับระบบงานอื่นภายในองค์กร เป็นต้น

(4) ไม่ใช้งานระบบงานอื่นบนคอมพิวเตอร์ลูกข่ายรวมถึงระบบรับ-ส่งอีเมล์ ยกเว้นอาจใช้ร่วมกับบริการด้านการเงินด้วยวิธีอิเล็กทรอนิกส์ของ ธปท. ได้โดยอนุโลม

(5) ไม่เชื่อมต่อเครือข่าย Internet กับคอมพิวเตอร์ลูกข่าย

(6) ป้องกันและตรวจจับการบุกรุกของโปรแกรมประสงค์ร้าย (Malware) รวมถึงภัยคุกคามขั้นสูง (Advanced Persistent Threat หรือ APT) เพื่อป้องกันความเสียหายที่จะเกิดขึ้นแก่คอมพิวเตอร์ลูกข่าย หรือการรั่วไหลของข้อมูลที่เป็นความลับออกไปนอกองค์กร เช่น การติดตั้งโปรแกรม Anti-Virus Anti-Malware และ Update Signature จากผู้ผลิตอย่างสม่ำเสมอ มีการทำ Scheduled Scan ตามระยะเวลาที่เหมาะสม และพิจารณาติดตั้งระบบป้องกันภัยคุกคามขั้นสูง (APT Protection) ไม่นำโปรแกรมที่ไม่ได้รับการตรวจสอบหรือไม่มีลิขสิทธิ์ที่ถูกต้องมาใช้งาน เป็นต้น

(7) กำหนดความถี่ในการติดตั้งโปรแกรมเพื่อปิดช่องโหว่ (Windows Security Patch) สำหรับ Windows Operating System ของเครื่องคอมพิวเตอร์ลูกข่ายอย่างเหมาะสม อย่างน้อยตามมาตรฐานที่ยอมรับโดยทั่วไป

(8) กำหนดวิธีการควบคุมการแก้ไขเปลี่ยนแปลง (Change Management) การตั้งค่าเครือข่าย และโปรแกรมระบบคอมพิวเตอร์ ที่เกี่ยวข้องกับคอมพิวเตอร์ลูกข่าย เช่น มีการทำทะเบียนอุปกรณ์ บันทึก และขออนุมัติเมื่อเข้าใช้งานหรือปรับเปลี่ยนการตั้งค่าโปรแกรมระบบคอมพิวเตอร์ และอุปกรณ์ Network เป็นต้น

4.2.2 การควบคุมการเข้าใช้คอมพิวเตอร์ลูกข่าย

ผู้ใช้บริการบาทเนตต้องจัดให้มีมาตรการที่ใช้ควบคุมการเข้าใช้งานคอมพิวเตอร์ลูกข่ายเพื่อป้องกันการลักลอบนำบัญชีผู้ใช้ไปทำธุรกรรม โดยผู้ที่ไม่มีสิทธิทั้งจากภายในและภายนอกองค์กร ทั้งนี้ มาตรการดังกล่าวควรครอบคลุมถึง

(1) จัดวางและติดตั้งอุปกรณ์ที่เกี่ยวข้องกับคอมพิวเตอร์ลูกข่ายให้เป็นสัดส่วน ยากแก่การเข้าถึงของผู้ที่ไม่มีหน้าที่เกี่ยวข้อง รวมทั้งจัดให้มีการควบคุมการเข้าออกบริเวณพื้นที่ใช้งาน ลดโอกาสการลักลอบเข้าถึงโดยผู้ไม่มีสิทธิ

(2) กำหนดวิธีการและสิทธิการเข้าถึงคอมพิวเตอร์ลูกข่าย โดยจัดให้มีการแบ่งอำนาจหน้าที่ของพนักงานอย่างเหมาะสมเพื่อป้องกันมิให้พนักงานผู้ใดได้รับสิทธิอย่างเบ็ดเสร็จ และหลีกเลี่ยงการให้สิทธิ admin ในการเข้าถึงคอมพิวเตอร์ลูกข่าย รวมถึงทบทวนสิทธิดังกล่าวโดยสม่ำเสมออย่างน้อยทุก 180 วัน

(3) มีการบันทึกประวัติการเข้าใช้เครื่องคอมพิวเตอร์ลูกข่ายเพื่อติดตามและตรวจสอบ การเข้าใช้ที่ผิดปกติ โดยอาจจัดให้มีอุปกรณ์ฮาร์ดแวร์และซอฟท์แวร์เพื่อช่วยในการบันทึก เช่น อุปกรณ์ Security Information Event Management (SIEM) สำหรับการบันทึก Log ของ Active Directory เป็นต้น

(4) ปิดคอมพิวเตอร์ลูกข่ายเมื่อไม่มีการใช้งานหรือนอกเวลาทำการ

(5) ควบคุมหรือหลีกเลี่ยงการนำอุปกรณ์เชื่อมต่อ (Peripheral device) เช่น USB Storage Device, DVD, และ CD เป็นต้น มาเชื่อมต่อกับคอมพิวเตอร์ลูกข่าย โดยต้องกำหนดข้อปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องคอมพิวเตอร์ลูกข่ายจากความเสี่ยงของการใช้อุปกรณ์ดังกล่าว

(6) กำหนดกระบวนการควบคุมการใช้อุปกรณ์ USB Token รหัสผ่าน ใบรับรอง และบัญชีผู้ใช้งาน เช่น ให้เฉพาะผู้ที่ได้รับมอบหมายเข้าใช้บริการบาทเนตเท่านั้น ไม่นำบัญชีผู้ใช้งานของบุคคลอื่นให้ผู้ปฏิบัติงานอื่นเข้าระบบบาทเนตแทน เป็นต้น

(7) กำหนดความถี่ในการเปลี่ยนรหัสผ่าน (PIN/Password) ของอุปกรณ์ USB Token สำหรับการใช้บริการบาทเนต โดยอย่างน้อยควรเปลี่ยนทุก 90 วัน

(8) กำหนดความถี่ในการเปลี่ยนรหัสผ่านสำหรับ Windows บนคอมพิวเตอร์ลูกข่าย โดยอย่างน้อยควรเปลี่ยนทุก 90 วัน

(9) จัดให้มีการควบคุมการกำหนดรหัสผ่าน (Password) ตามข้อ (7) และ (8) อย่างรัดกุม และคาดเดาได้ยาก (Strong Password) เช่น รหัสผ่านควรมีความยาวอย่างน้อยแปดตัว ประกอบด้วยอักขระที่เป็นตัวพิมพ์ใหญ่ ตัวพิมพ์เล็ก ตัวเลข และสัญลักษณ์พิเศษที่พบบนแป้นพิมพ์ (อักขระบนแป้นพิมพ์ทั้งหมดที่ไม่ได้ถูกกำหนดเป็นตัวอักษรหรือตัวเลข) เป็นต้น

4.2.3 การควบคุมด้านการปฏิบัติงาน

ผู้ใช้บริการบาทเนตต้องกำหนดมาตรการด้านการรักษาความมั่นคงปลอดภัย เพื่อกำหนดแนวทางติดตาม และเตรียมความพร้อมสำหรับเหตุละเมิดความมั่นคงปลอดภัยคอมพิวเตอร์ลูกข่าย ทั้งนี้ มาตรการดังกล่าวควรครอบคลุมถึง

(1) จัดให้มีผู้รับผิดชอบด้านความมั่นคงปลอดภัย ทั้งในระดับปฏิบัติงานและระดับบริหาร เพื่อติดตาม บันทึก แก้ไข และรายงานเมื่อมีการละเมิดความมั่นคงปลอดภัย

(2) จัดทำแผนฉุกเฉินกรณีที่เกิดความเสียหายจากภัยคุกคามต่อคอมพิวเตอร์ลูกข่าย ให้ครอบคลุมกรณีการบุกรุกของ Malware รวมถึงภัยคุกคามขั้นสูง โดยกำหนดขั้นตอนการแก้ไขปัญหา ทีมงานหรือผู้รับผิดชอบ รวมถึงวิธีการรายงานปัญหาให้กับผู้บริหาร และแจ้งผู้เกี่ยวข้องทราบอย่างรวดเร็วที่สุดเท่าที่จะทำได้ เพื่อแก้ไขปัญหาให้กลับคืนสู่สภาวะปกติโดยเร็ว

(3) จัดให้มีการติดตาม บันทึก และรายงานเหตุการณ์ละเมิดความมั่นคงปลอดภัยคอมพิวเตอร์ลูกข่ายให้เป็นไปตามมาตรฐานที่ดี รวมทั้งให้มีการเรียนรู้จากเหตุการณ์ที่เกิดขึ้นเพื่อเตรียมการป้องกันที่จำเป็นไว้ล่วงหน้า โดยครอบคลุมถึง

(3.1) แนวทางในการรับรู้ปัญหาที่เกิดขึ้นอย่างทันท่วงที โดยใช้ข้อมูลและเครื่องมือที่พัฒนาขึ้นตามกรอบแนวความเสี่ยง (a risk-based approach) และวิธีการอื่นใด เพื่อยับยั้ง ตรวจจับ ระบุ และสกัดกั้นเหตุการณ์ที่ละเมิดต่อความมั่นคงปลอดภัย

(3.2) กำหนดขั้นตอนการแก้ไขปัญหา วิธีการรายงานปัญหาให้กับผู้บริหาร วิธีการแจ้งให้ ธปท. และผู้เกี่ยวข้องทราบ รวมถึงวิธีการติดตามการแก้ไขปัญหา รวมทั้งกำหนดทีมงานหรือผู้รับผิดชอบที่สามารถติดต่อได้ในกรณีเร่งด่วน ทั้งในและนอกเวลาทำการ เพื่อให้สามารถปฏิบัติงานได้อย่างทันท่วงทีเมื่อมีการร้องขอ

(3.3) เก็บรวบรวมหลักฐานต่าง ๆ ที่เป็นประโยชน์

(3.4) บันทึกเหตุการณ์หรือจัดทำรายงานที่เป็นลายลักษณ์อักษร ซึ่งรวมถึงติดตามและตรวจสอบความผิดปกติของบันทึกเหตุการณ์ที่ละเมิดต่อความมั่นคงปลอดภัย เพื่อใช้เป็นแนวทาง

ในการแก้ปัญหา รวมทั้งทบทวนความเหมาะสมของแนวทางปัจจุบัน และพิจารณาปรับปรุงมาตรการที่จำเป็นเพิ่มเติม

4.2.4 การจัดการด้านบุคลากรและการสื่อสาร

ผู้ใช้บริการบาทเนตต้องจัดให้มีการติดตามพัฒนาการทางเทคโนโลยีและภัยคุกคามใหม่ ๆ ที่เกิดขึ้นอย่างใกล้ชิด รวมทั้งสื่อสาร แลกเปลี่ยนข้อมูล และประชาสัมพันธ์วิธีการป้องกันภัยคุกคามต่อระบบคอมพิวเตอร์ ทั้งภายในและภายนอกองค์กร ได้แก่

(1) จัดให้มีการพัฒนา ฝึกอบรม และให้ความรู้อย่างต่อเนื่องแก่ผู้บริหารและพนักงานทุกระดับ เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบคอมพิวเตอร์โดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ (Security Awareness) เช่น จัดการอบรมเพิ่มเติมความรู้แต่บุคลากรเก่าและใหม่อย่างสม่ำเสมอ และจัดให้มีการประชาสัมพันธ์เพื่อรณรงค์ให้ไม่เปิดอีเมล์ที่ต้องสงสัยหรือไม่เข้า Web Site ที่ไม่เหมาะสม เป็นต้น

(2) จัดให้มีการประชาสัมพันธ์ให้ข้อมูลและคำแนะนำที่เป็นประโยชน์แก่ลูกค้าผู้ใช้บริการ เช่น วิธีการใช้บริการอย่างปลอดภัย เป็นต้น

(3) จัดให้มีการติดตามพัฒนาการทางเทคโนโลยีและภัยคุกคามใหม่ ๆ ที่อาจก่อให้เกิดเหตุการณ์ละเมิดต่อความมั่นคงปลอดภัยอย่างใกล้ชิด มีการหารือร่วมกับผู้เชี่ยวชาญทางด้านความมั่นคงปลอดภัยของระบบคอมพิวเตอร์ รวมทั้งสื่อสาร แลกเปลี่ยนข้อมูล เพื่อกำหนดวิธีการป้องกันภัยคุกคามต่อระบบคอมพิวเตอร์ทั้งภายในและภายนอกองค์กร และประชาสัมพันธ์ให้ผู้เกี่ยวข้องทราบ

4.2.5 การรักษาความปลอดภัยระบบคอมพิวเตอร์สำหรับผู้ใช้บริการบาทเนตผ่าน SWIFT

ผู้ใช้บริการบาทเนตซึ่งส่งข้อความผ่าน SWIFT ต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยตามที่ SWIFT กำหนด ทั้งนี้ มาตรการดังกล่าวควรครอบคลุมถึง

(1) ติดตามข้อมูลข่าวสาร ตลอดจนปฏิบัติตาม “Security Guidance for Alliance Access, Customer managed interface to SWIFT Network” หรือเอกสารด้านความปลอดภัยอื่นใดที่ SWIFT ประกาศอย่างครบถ้วน

(2) จัดให้มีการควบคุมและกำหนดความถี่ในการปรับปรุงโปรแกรมที่เกี่ยวข้องกับระบบ SWIFT เช่น Alliance Access หรือ Alliance Entry รวมถึงโปรแกรม SWIFT Interface อื่น ๆ ให้เป็นปัจจุบันอยู่เสมอโดยเฉพาะอย่างยิ่งกรณี Mandatory Update

(3) จัดให้มีการควบคุมขั้นตอนการรับส่งข้อความผ่านโปรแกรมที่เกี่ยวข้องกับระบบ SWIFT เช่น Alliance Access หรือ Alliance Entry รวมถึงโปรแกรม SWIFT Interface อื่น ๆ อย่างรัดกุม โดยแบ่งแยกอำนาจหน้าที่ ตามลำดับ เช่น Message entry Verification และ Validation เป็นต้น

(4) จัดให้มีการทบทวนสิทธิการเข้าถึงโปรแกรมที่เกี่ยวข้องกับระบบ SWIFT เช่น Alliance Access หรือ Alliance Entry รวมถึงโปรแกรม SWIFT Interface อื่น ๆ อย่างสม่ำเสมอ โดยอย่างน้อยควรทบทวนทุก 180 วัน

5. วันเริ่มต้นบังคับใช้

แนวปฏิบัติฉบับนี้ให้ใช้บังคับตั้งแต่วันที่ **2 สิงหาคม 2564** เป็นต้นไป

ภาคผนวก 1

กฎหมายที่เกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์และกฎหมายที่เกี่ยวข้อง[1/]

ผู้ใช้บริการบาทเนตต้องดำเนินการให้มีการรักษาความมั่นคงปลอดภัยในองค์กร นอกเหนือจากข้อกำหนดในระเบียบธนาคารแห่งประเทศไทย ว่าด้วยการบริการบาทเนตแล้ว ผู้ใช้บริการบาทเนตต้องดำเนินการตามกฎหมายควบคุมการประกอบธุรกิจอื่น ๆ เพื่อให้มั่นใจว่ากระบวนการทำงานและธุรกรรม มีการรักษาความมั่นคงปลอดภัยที่ดี สอดคล้องกับข้อกำหนดตามกฎหมายในปัจจุบัน และเป็นไปตามมาตรฐานสากล

โดยกฎหมายที่เกี่ยวข้อง มีตัวอย่างดังนี้

1. **พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม**
2. **พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549**
   - ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553
   - ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ (ฉบับที่ 2) พ.ศ. 2556
3. **พระราชบัญญัติระบบการชำระเงิน พ.ศ. 2560**
   - ประกาศธนาคารแห่งประเทศไทย ที่ สนช. 1/2561 เรื่อง หลักเกณฑ์การกำกับดูแลผู้ให้บริการระบบการชำระเงินที่มีความสำคัญ
   - ประกาศธนาคารแห่งประเทศไทย ที่ สนช. 2/2561 เรื่อง หลักเกณฑ์การกำกับดูแลสมาชิกของระบบการชำระเงินที่มีความสำคัญ
4. **พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553**
   - ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง ประเภทของธุรกรรมทางอิเล็กทรอนิกส์และหลักเกณฑ์การประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ตามวิธีการแบบปลอดภัย พ.ศ. 2555
   - ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555
5. **ประกาศธนาคารแห่งประเทศไทย**
   - ประกาศธนาคารแห่งประเทศไทย ที่ สนส. 27/2551 เรื่อง การอนุญาตให้บริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ให้บริการการเงินทางอิเล็กทรอนิกส์

[1/] ธปท. ได้ทำการรวบรวมมาจากกฎหมาย ประกาศ รวมถึงหนังสือเวียน แนวปฏิบัติ และแนวนโยบายของธนาคารแห่งประเทศไทยที่มีผลใช้บังคับ ณ สิ้นเดือนธันวาคม พ.ศ. 2563 แต่อาจไม่ครอบคลุมทั้งหมด ทั้งนี้ หากกฎหมาย ประกาศ หนังสือเวียน แนวปฏิบัติ และแนวนโยบายที่เกี่ยวข้องตามที่ปรากฏในภาคผนวกนี้ได้มีการปรับปรุงแก้ไขเพิ่มเติม ให้ถือปฏิบัติตามกฎหมาย ประกาศ หนังสือเวียน แนวปฏิบัติ และแนวนโยบายที่ได้มีการแก้ไขเพิ่มเติมนั้น โดยปรับปรุงล่าสุดเมื่อวันที่ 31 ธ.ค. 2563

ภาคผนวก 2

เกณฑ์การรายงานเหตุการณ์ความเสี่ยง

หากผู้ใช้บริการบาทเนตพบว่ามีคำสั่งโอนเงินที่ส่งเข้าระบบบาทเนตจากสถาบันของตน ซึ่งเข้าข่ายธุรกรรมทุจริต ผู้ใช้บริการบาทเนตมีหน้าที่ต้องรายงานเหตุการณ์ดังกล่าว ให้ ธปท. ทราบ ทั้งนี้ มีเกณฑ์เหตุการณ์ทุจริตที่ต้องรายงาน ดังนี้

1. มีโอกาสสร้างความเสียหายด้านข้อมูล ตัวเงินอย่างมีนัยสำคัญ รวมถึงผลกระทบด้านการรับรู้ และความเชื่อมั่นต่อสาธารณชน
2. อาจกระทบต่อเสถียรภาพระบบสถาบันการเงิน
3. อาจส่งผลกระทบต่อการให้บริการ ระบบ หรือ ชื่อเสียงของสถาบันการเงิน
4. มีการรายงานต่อผู้บริหารในระดับ Manager or Compliance Department