ธนาคารแห่งประเทศไทย

26 พฤษภาคม 2560

เรียน ผู้จัดการ

สถาบันผู้ใช้บริการบาทเนต
ธนาคารสมาชิกศูนย์หักบัญชีอิเล็กทรอนิกส์

ที่ ธปท.ฝชพ.(31) ว. 794 /2560 เรื่อง นำส่งประกาศ ธปท. เรื่อง มาตรฐานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของคอมพิวเตอร์ลูกข่ายระบบ BAHTNET และระบบ ICAS

ด้วยปัจจุบันความเสี่ยงจากภัยคุกคามด้านไซเบอร์ได้ทวีความรุนแรงเพิ่มขึ้นเป็นลำดับ อาจก่อให้เกิดความเสียหายต่อสถาบันการเงินทั้งในด้านการเงินและชื่อเสียง ส่งผลกระทบต่อประชาชนและเศรษฐกิจในวงกว้าง รวมทั้งอาจมีผลต่อเนื่องไปถึงความเชื่อมั่นของระบบการชำระเงิน และระบบการเงินของประเทศได้ เพื่อลดผลกระทบและความเสี่ยงจากภัยคุกคามดังกล่าว ธนาคารแห่งประเทศไทย (ธปท.) จึงมีมาตรการยกระดับการจัดการความมั่นคงปลอดภัยสารสนเทศของระบบโครงสร้างพื้นฐานการชำระเงินของประเทศ อันได้แก่ ระบบ BAHTNET และระบบ ICAS ให้ได้มาตรฐานสากล ซึ่งที่ผ่านมาได้ดำเนินการให้คอมพิวเตอร์แม่ข่ายของระบบดังกล่าว ผ่านการรับรองตามมาตรฐาน ISO/IEC 27001 แล้วในปี 2558 และมีการรักษาสถานภาพการรับรองอย่างต่อเนื่อง รวมถึงมีแผนจะขยายผลไปยังคอมพิวเตอร์ลูกข่ายต่อไป นั้น

เพื่อให้การป้องกันความเสี่ยงจากภัยคุกคามด้านไซเบอร์สามารถครอบคลุมครบวงจรทั้งระบบ ธปท. จึงกำหนดให้คอมพิวเตอร์ลูกข่ายของระบบ BAHTNET และระบบ ICAS ต้องผ่านการรับรองการจัดการความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC 27001 ภายในปี 2561 และรักษาสถานภาพการรับรองอย่างต่อเนื่อง โดย ธปท. ได้หารือและทำ Workshop เพื่อรับฟังความคิดเห็นกับสมาชิกเป็นระยะ ๆ จนได้ข้อสรุปร่วมกัน และออกเป็นประกาศ ธปท. 2 ฉบับ เรื่อง มาตรฐานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของคอมพิวเตอร์ลูกข่ายระบบ BAHTNET และระบบ ICAS ที่แนบมาพร้อมนี้

จึงเรียนมาเพื่อโปรดทราบและถือปฏิบัติ

ขอแสดงความนับถือ

(นายเพิ่มสุข สุทธินุ่น)
ผู้ช่วยผู้ว่าการ สายระบบข้อสนเทศ
ผู้ว่าการแทน

สิ่งที่ส่งมาด้วย 1. ประกาศธนาคารแห่งประเทศไทย ที่ สรข. 4/2560 เรื่อง มาตรฐานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของคอมพิวเตอร์ลูกข่ายระบบบาทเนต วันที่ 23 พ.ค. 2560
2. ประกาศธนาคารแห่งประเทศไทย ที่ สรข. 5/2560 เรื่อง มาตรฐานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของคอมพิวเตอร์ลูกข่ายระบบการหักบัญชีเช็คด้วยภาพเช็คและระบบการจัดเก็บภาพเช็ค วันที่ 23 พ.ค. 2560

ฝ่ายการชำระเงินและพันธบัตร
โทรศัพท์ 0 2283 5056, 0 2283 5034

ประกาศธนาคารแห่งประเทศไทย
ที่ สรข. 4 /2560
เรื่อง มาตรฐานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
ของคอมพิวเตอร์ลูกข่ายระบบบาทเนต

---

1. เหตุผลในการออกประกาศ

ธนาคารแห่งประเทศไทย (ธปท.) ตระหนักถึงความเสี่ยงด้านความปลอดภัย (Security Risk) ของข้อมูล ระบบ และเครือข่ายที่ใช้ในการให้บริการโอนเงินผ่านระบบบาทเนต ซึ่งเป็นระบบการชำระเงินที่มีความสำคัญของประเทศ และเห็นว่ามาตรฐาน ISO/IEC 27001 เป็นมาตรฐานที่มุ่งเน้นด้านการรักษาและเสริมสร้างความมั่นคงปลอดภัยให้กับระบบสารสนเทศขององค์กรและใช้เป็นแนวทางกำหนดวิธีปฏิบัติในการตรวจสอบและรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

ธปท. จึงออกประกาศฉบับนี้เพื่อให้คอมพิวเตอร์ลูกข่ายของระบบบาทเนตผ่านการรับรองตามมาตรฐาน ISO/IEC 27001 ซึ่งจะเป็นการยกระดับความมั่นคงปลอดภัยคอมพิวเตอร์ลูกข่ายของระบบบาทเนต ให้มีความน่าเชื่อถือและสามารถให้บริการได้อย่างต่อเนื่องเป็นไปตามมาตรฐานสากล

2. อำนาจตามกฎหมาย

เพื่ออนุวัติตามข้อ 15 แห่งระเบียบธนาคารแห่งประเทศไทย ว่าด้วยการบริการบาทเนต พ.ศ. 2549

3. ขอบเขตการบังคับใช้

ประกาศฉบับนี้ใช้บังคับกับผู้ใช้บริการบาทเนตตามระเบียบธนาคารแห่งประเทศไทย ว่าด้วยการบริการบาทเนต

4. เนื้อหา

ข้อ 1 ในประกาศฉบับนี้

"คอมพิวเตอร์ลูกข่าย" หมายถึง ระบบคอมพิวเตอร์ของผู้ใช้บริการบาทเนตสำหรับการปฏิบัติงานจริงและสำหรับเป็นชุดสำรองที่ใช้เชื่อมโยงกับระบบบาทเนตของ ธปท. ได้แก่ ระบบคอมพิวเตอร์สำหรับบริการด้านการเงินด้วยวิธีอิเล็กทรอนิกส์ (Electronic Financial Services) หรือระบบงานคอมพิวเตอร์อื่นที่เชื่อมโยงเพื่อการรับส่งข้อมูลโดยตรงกับระบบคอมพิวเตอร์แม่ข่ายของ ธปท. (Host to Host) ทั้งนี้ ไม่รวมถึงระบบคอมพิวเตอร์สำหรับการส่งข้อความผ่านสวิฟท์ (SWIFT)

"ผู้ตรวจสอบอิสระ" หมายถึง ผู้ตรวจสอบงานด้านเทคโนโลยีสารสนเทศ ซึ่งอาจเป็นผู้ตรวจสอบภายในที่มีความเป็นอิสระจากหน่วยงานที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศและหน่วยงานที่ทำหน้าที่ด้านบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ หรือผู้ตรวจสอบภายนอกซึ่งสามารถดำเนินการตรวจประเมินระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ตามมาตรฐาน ISO/IEC 27001 (Information Security Management) โดยผ่านการรับรองหรือได้รับใบประกาศนียบัตรด้านความมั่นคงปลอดภัยระดับสากล เช่น Certified Information System Auditor (CISA), Certified Information Security Manager (CISM), Certified Information Security Professional (CISSP)

"หน่วยงานรับรองระบบสารสนเทศ (Certification Body)" หมายถึง หน่วยงานที่ทำหน้าที่ตรวจรับรองระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC 27001

"การตรวจประเมิน (Assessment)" หมายถึง การตรวจประเมินระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC 27001 โดยผู้ตรวจสอบอิสระ

"การตรวจรับรอง (Certification)" หมายถึง การตรวจรับรองระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC 27001 โดยหน่วยงานรับรองระบบสารสนเทศ

ข้อ 2 ผู้ใช้บริการบาทเนตต้องดำเนินการให้คอมพิวเตอร์ลูกข่ายของตนผ่านการตรวจรับรองตามแนวทางใดแนวทางหนึ่ง ดังนี้

(1) ผ่านการตรวจรับรองภายในปี 2560 หรือ

(2) ผ่านการตรวจประเมินภายในปี 2560 และผ่านการตรวจรับรองภายในปี 2561

กรณีสถาบันที่เข้าเป็นผู้ใช้บริการบาทเนตภายหลังจากวันที่ประกาศนี้ใช้บังคับ ให้สถาบันนั้นดำเนินการให้คอมพิวเตอร์ลูกข่ายผ่านการตรวจประเมินภายใน 180 วันนับจากวันที่เป็นผู้ใช้บริการบาทเนต และต้องผ่านการตรวจรับรองภายใน 1 ปีนับจากวันที่ผ่านการตรวจประเมิน

ทั้งนี้ เมื่อผู้ใช้บริการบาทเนตได้ดำเนินการตามวรรคหนึ่ง หรือวรรคสองแล้วแต่กรณีแล้ว ให้จัดส่งเอกสารการตรวจประเมิน หรือการตรวจรับรองที่ได้รับจากการดำเนินการข้างต้น มาที่ ธปท. โดยเร็ว

ข้อ 3 ผู้ใช้บริการบาทเนตต้องรักษาสถานภาพการตรวจรับรองระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC 27001 ของคอมพิวเตอร์ลูกข่ายของตน โดยหน่วยงานรับรองระบบสารสนเทศตามข้อ 2 อย่างต่อเนื่อง

ทั้งนี้ ให้จัดส่งเอกสารการตรวจรับรองตามวรรคหนึ่ง มาที่ ธปท. โดยเร็ว

ข้อ 4 กรณีผู้ใช้บริการบาทเนตไม่สามารถดำเนินการตามที่กำหนดในข้อ 2 หรือข้อ 3 ข้างต้นได้ ให้ส่งหนังสือขอผ่อนผันพร้อมชี้แจงเหตุผลและความจำเป็น แนวทางแก้ไข และกำหนดเวลาที่จะดำเนินการให้แล้วเสร็จให้ ธปท. ทราบโดยเร็ว โดย ธปท. อาจพิจารณาขยายระยะเวลาให้หรือไม่ก็ได้ตามที่เห็นสมควร

5. วันเริ่มต้นบังคับใช้

ประกาศนี้ให้ใช้บังคับตั้งแต่วันที่ประกาศเป็นต้นไป

ประกาศ ณ วันที่ 23 พฤษภาคม 2560

(นายวิรไท สันติประภพ)
ผู้ว่าการ
ธนาคารแห่งประเทศไทย

ทีมพัฒนาธุรกิจ 1
ฝ่ายการชำระเงินและพันธบัตร
โทรศัพท์ 0 2283 5056

ประกาศธนาคารแห่งประเทศไทย
ที่ สรข. 5 /2560
เรื่อง มาตรฐานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
ของคอมพิวเตอร์ลูกข่ายระบบการหักบัญชีเช็คด้วยภาพเช็คและระบบการจัดเก็บภาพเช็ค

---

1. เหตุผลในการออกประกาศ

ธนาคารแห่งประเทศไทย (ธปท.) ตระหนักถึงความเสี่ยงด้านความปลอดภัย (Security Risk) ของข้อมูล ระบบ และเครือข่ายที่ใช้ในระบบการหักบัญชีเช็คด้วยภาพเช็คและระบบการจัดเก็บภาพเช็ค (Imaged Cheque Clearing and Archive System: ICAS) ซึ่งเป็นระบบการชำระเงินที่มีความสำคัญของประเทศ และเห็นว่ามาตรฐาน ISO/IEC 27001 เป็นมาตรฐานที่มุ่งเน้นด้านการรักษาและเสริมสร้างความมั่นคงปลอดภัยให้กับระบบสารสนเทศขององค์กรและใช้เป็นแนวทางกำหนดวิธีปฏิบัติในการตรวจสอบและรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

ธปท. จึงออกประกาศฉบับนี้เพื่อให้คอมพิวเตอร์ลูกข่ายของระบบ ICAS ผ่านการรับรองตามมาตรฐาน ISO/IEC 27001 ซึ่งจะเป็นการยกระดับความมั่นคงปลอดภัยคอมพิวเตอร์ลูกข่ายของระบบ ICAS ให้มีความน่าเชื่อถือและสามารถให้บริการได้อย่างต่อเนื่องเป็นไปตามมาตรฐานสากล

2. อำนาจตามกฎหมาย

เพื่ออนุวัติตามข้อ 5 แห่งระเบียบธนาคารแห่งประเทศไทย ที่ สรข. 1/2554 ว่าด้วยระบบการหักบัญชีเช็คด้วยภาพเช็คและระบบการจัดการภาพเช็ค

3. ขอบเขตการบังคับใช้

ประกาศฉบับนี้ใช้บังคับกับธนาคารสมาชิกตามระเบียบธนาคารแห่งประเทศไทยว่าด้วยระบบการหักบัญชีเช็คด้วยภาพเช็คและระบบการจัดเก็บภาพเช็ค

4. เนื้อหา

ข้อ 1 ในประกาศฉบับนี้

“คอมพิวเตอร์ลูกข่าย” หมายถึง ระบบคอมพิวเตอร์พร้อมติดตั้งอุปกรณ์และโปรแกรมเพื่อใช้งานระบบ ICAS และบริการด้านการเงินด้วยวิธีอิเล็กทรอนิกส์ของธนาคารสมาชิกสำหรับการปฏิบัติงานจริงและสำหรับเป็นชุดสำรองที่ใช้เชื่อมโยงกับระบบ ICAS ของ ธปท. ซึ่งประกอบด้วยเครื่องรับส่งข้อมูลและภาพเช็ค (Imaged Cheque Member Gateway: ICMG) และเครื่องเพื่อการใช้งานระบบ ICAS ผ่านบริการด้านการเงินด้วยวิธีอิเล็กทรอนิกส์ (Electronic Financial Services)

"ผู้ตรวจสอบอิสระ" หมายถึง ผู้ตรวจสอบงานด้านเทคโนโลยีสารสนเทศ ซึ่งอาจเป็นผู้ตรวจสอบภายในที่มีความเป็นอิสระจากหน่วยงานที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศและหน่วยงานที่ทำหน้าที่ด้านบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ หรือผู้ตรวจสอบภายนอกซึ่งสามารถดำเนินการตรวจประเมินระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ตามมาตรฐาน ISO/IEC 27001 (Information Security Management) โดยผ่านการรับรองหรือได้รับใบประกาศนียบัตรด้านความมั่นคงปลอดภัยระดับสากล เช่น Certified Information System Auditor (CISA), Certified Information Security Manager (CISM), Certified Information Security Professional (CISSP)

"หน่วยงานรับรองระบบสารสนเทศ (Certification Body)" หมายถึง หน่วยงานที่ทำหน้าที่ตรวจรับรองระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC 27001

"การตรวจประเมิน (Assessment)" หมายถึง การตรวจประเมินระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC 27001 โดยผู้ตรวจสอบอิสระ

"การตรวจรับรอง (Certification)" หมายถึง การตรวจรับรองระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC 27001 โดยหน่วยงานรับรองระบบสารสนเทศ

ข้อ 2 ธนาคารสมาชิกต้องดำเนินการให้คอมพิวเตอร์ลูกข่ายของตนผ่านการตรวจรับรองตามแนวทางใดแนวทางหนึ่ง ดังนี้

(1) ผ่านการตรวจรับรองภายในปี 2560 หรือ

(2) ผ่านการตรวจประเมินภายในปี 2560 และผ่านการตรวจรับรองภายในปี 2561

กรณีธนาคารที่เข้าเป็นสมาชิกของระบบ ICAS ภายหลังจากวันที่ประกาศนี้ใช้บังคับ ให้ธนาคารนั้นดำเนินการให้คอมพิวเตอร์ลูกข่ายผ่านการตรวจประเมินภายใน 180 วันนับจากวันที่เป็นธนาคารสมาชิก และต้องผ่านการตรวจรับรองภายใน 1 ปีนับจากวันที่ผ่านการตรวจประเมิน

ทั้งนี้ เมื่อธนาคารสมาชิกได้ดำเนินการตามวรรคหนึ่ง หรือวรรคสองแล้วแต่กรณีแล้ว ให้จัดส่งเอกสารการตรวจประเมิน หรือการตรวจรับรองที่ได้รับจากการดำเนินการข้างต้น มาที่ ธปท. โดยเร็ว

ข้อ 3 ธนาคารสมาชิกต้องรักษาสถานภาพการตรวจรับรองระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC 27001 ของคอมพิวเตอร์ลูกข่ายของตน โดยหน่วยงานรับรองระบบสารสนเทศ ตามข้อ 2 ข้างต้นอย่างต่อเนื่อง

ทั้งนี้ ให้จัดส่งเอกสารการตรวจรับรองตามวรรคหนึ่ง มาที่ ธปท. โดยเร็ว

ข้อ 4 กรณีธนาคารสมาชิกไม่สามารถดำเนินการตามที่กำหนดในข้อ 2 หรือข้อ 3 ข้างต้นได้ ให้ส่งหนังสือขอผ่อนผันพร้อมชี้แจงเหตุผลและความจำเป็น แนวทางแก้ไข และกำหนดเวลาที่จะดำเนินการให้แล้วเสร็จให้ ธปท. ทราบโดยเร็ว โดย ธปท. อาจพิจารณาขยายเวลาให้หรือไม่ก็ได้ตามที่เห็นสมควร

5. วันเริ่มต้นบังคับใช้

ประกาศนี้ให้ใช้บังคับตั้งแต่วันที่ประกาศเป็นต้นไป

ประกาศ ณ วันที่ 23 พฤษภาคม 2560

(นายวิรไท สันติประภพ)
ผู้ว่าการ
ธนาคารแห่งประเทศไทย

ทีมพัฒนาธุรกิจ 2
ฝ่ายการชำระเงินและพันธบัตร
โทรศัพท์ 0 2283 5034