



ธนาคารแห่งประเทศไทย

9 กันยายน 2565

เรียน ผู้จัดการ

สถาบันผู้ให้บริการบาทเน็ต

ที่ ผพพ.(ว.) 53 /2565 เรื่อง ยกเลิกการผ่อนผันการปฏิบัติตามเกณฑ์เกี่ยวกับระบบบาทเน็ต และระบบ ICAS และแนวปฏิบัติเกี่ยวกับการใช้เครื่องคอมพิวเตอร์ลูกข่ายระบบ BAHTNET และระบบ ICAS ในการปฏิบัติงานนอกสถานที่ทำการ จากสถานการณ์การระบาดของ COVID-19

ตามที่ธนาคารแห่งประเทศไทย (ธปท.) ได้ออกหนังสือเวียน 2 ฉบับในปี 2564 แจ้งแนวทางดำเนินการและการผ่อนผันเกณฑ์เกี่ยวกับระบบบาทเน็ตและระบบ ICAS กรณีการระบาดของไวรัสโคโรนา 2019 (COVID-19) และแนวปฏิบัติเกี่ยวกับการใช้เครื่องคอมพิวเตอร์ลูกข่ายระบบ BAHTNET และระบบ ICAS ในการปฏิบัติงานนอกสถานที่ทำการ ภายใต้สถานการณ์ฉุกเฉินการระบาดของไวรัสโคโรนา 2019 (COVID-19) นั้น

ด้วยสถานการณ์การแพร่ระบาดของ COVID-19 มีความรุนแรงลดลง ประกอบกับแนวนโยบายภาครัฐมีการยกเลิกมาตรการการป้องกันและควบคุมการระบาดต่าง ๆ เช่น การลดและจำกัดการเดินทาง (lock down) และมีแนวโน้มในการเปลี่ยนผ่านเป็นโรคประจำถิ่น เพื่อให้การปฏิบัติงานเกี่ยวกับระบบบาทเน็ตดำเนินการได้อย่างเป็นปกติและสอดคล้องกับแนวนโยบายของ ธปท. ในด้านอื่น ๆ ธปท. จึงเห็นสมควรยกเลิกการผ่อนผันการปฏิบัติตามเกณฑ์ รวมทั้งยกเลิกแนวปฏิบัติเกี่ยวกับการใช้เครื่องคอมพิวเตอร์ลูกข่ายในการปฏิบัติงานนอกสถานที่ทำการ ภายใต้สถานการณ์ฉุกเฉินการระบาดของไวรัสโคโรนา 2019 (COVID-19) ทั้ง 2 ฉบับข้างต้น โดยให้มีผลตั้งแต่วันที่ 1 ตุลาคม 2565 เป็นต้นไป ทั้งนี้ สถาบันผู้ให้บริการบาทเน็ต ยังควรเตรียมความพร้อมเพื่อให้ระบบงานดังกล่าวสามารถดำเนินการทางธุรกิจและให้บริการแก่ลูกค้าได้อย่างต่อเนื่อง ภายใต้สถานการณ์ฉุกเฉิน

จึงเรียนมาเพื่อทราบ

ขอแสดงความนับถือ

(นายบัญชา มนูญกุลชัย)

ผู้อำนวยการอาวุโส ฝ่ายการชำระเงินและพันธบัตร

ผู้ว่าการแทน

- สิ่งที่ส่งมาด้วย 1. แนวทางดำเนินการและการผ่อนผันเกณฑ์เกี่ยวกับระบบบาทเน็ตและระบบ ICAS กรณีการระบาดของไวรัสโคโรนา 2019 (COVID-19)
2. แนวปฏิบัติ เรื่อง การใช้เครื่องคอมพิวเตอร์ลูกข่ายระบบ BAHTNET และระบบ ICAS ในการปฏิบัติงานนอกสถานที่ทำการ ภายใต้สถานการณ์ฉุกเฉินการระบาดของไวรัสโคโรนา 2019 (COVID-19)

ฝ่ายการชำระเงินและพันธบัตร

โทรศัพท์ 0 2283 5055

วิสัยทัศน์ เป็นองค์กรที่มองไกล มีหลักการ และร่วมมือ เพื่อความเป็นอยู่ที่ดีอย่างยั่งยืนของไทย

www.bot.or.th

แนวทางการดำเนินการและการผ่อนผันเกณฑ์ของระบบบาทเน็ต
เพื่อรองรับการระบาดของไวรัสโคโรนา 2019 (COVID-19)

ด้วยสถานการณ์การระบาดของไวรัสโคโรนา 2019 (COVID-19) ซึ่งลุกลามและส่งผลกระทบต่อเศรษฐกิจและประชาชนทั่วไปทั้งทางตรงและทางอ้อม เพื่อให้การดำเนินธุรกิจและการให้บริการด้านการชำระเงินมีความต่อเนื่องสามารถรองรับความจำเป็นของภาคธุรกิจและประชาชน รวมทั้งลดผลกระทบกับสถาบันการเงินและสร้างความเชื่อมั่นในระบบการชำระเงินของประเทศ

แนวทางการดำเนินการและการผ่อนผันเกณฑ์การขยายเวลา ค่าธรรมเนียม และค่าปรับนี้ ใช้ในการดำเนินงานระบบบาทเน็ตตั้งแต่วันที่ 2 สิงหาคม 2564 เป็นต้นไป จนกว่าจะกลับเข้าสู่ภาวะปกติ โดย ธปท.จะแจ้งให้ทราบต่อไป

1. การขอขยายเวลาปิดระบบบาทเน็ต

ผู้ให้บริการบาทเน็ตสามารถแจ้งความประสงค์ขอขยายเวลาปิดระบบได้ตามจำเป็น โดยดำเนินการตามแนวปฏิบัติที่ผ่านมา ทั้งนี้ ธปท. จะขยายเวลาให้ตามความจำเป็นแต่ไม่เกิน 19.00 น. และผ่อนผันไม่คิดค่าธรรมเนียมการขอขยายเวลา

2. การผ่อนผันค่าธรรมเนียมและค่าปรับ

2.1 ธปท. จะคิดค่าธรรมเนียมรายการโอนเงินทุกประเภทที่เกิดขึ้นในช่วงเวลา 16.00 น. ถึงปิดระบบบาทเน็ต ด้วยค่าธรรมเนียมอัตรา Zone ที่ 2 ยกเว้น ค่าส่งต่าง ๆ ที่ส่งผ่านระบบเชื่อมโยงเพื่อชำระราคาหลักทรัพย์หรือตามแต่ที่บริษัท ศูนย์รับฝากหลักทรัพย์ จำกัด (TSD) ประกาศกำหนด

2.2 ผู้ให้บริการบาทเน็ตที่ไม่สามารถปฏิบัติตามเกณฑ์สัดส่วนในการโอนเงินผ่านบาทเน็ต (30 : 70) ของประกาศ ธปท. ว่าด้วยเกณฑ์การดำรงเงินสภาพคล่องระหว่างวัน (ILF) และสัดส่วนในการโอนเงินผ่านบาทเน็ต จะยังคงได้รับส่วนลดค่าธรรมเนียมสำหรับเดือนนั้น

3. การส่งหนังสือยืนยันรายการโอนเงิน

ผู้ให้บริการบาทเน็ตได้รับการผ่อนผันให้ส่งหนังสือยืนยันรายการโอนเงินผ่านบาทเน็ตภายหลังได้จนกว่าจะเข้าสู่สถานการณ์ปกติและ ธปท. แจ้งยกเลิกการผ่อนผันนี้

4. การสอบถามข้อมูล และหรือรายงานในระบบบาทเน็ต

กรณีที่มีความประสงค์จะสอบถามข้อมูลยอดคงเหลือ บัญชีกระแสรายวัน รายการเคลื่อนไหว รายการโอนเงิน และหรือรายงานในระบบ ให้ผู้ให้บริการบาทเน็ตจัดทำแบบแจ้งรายชื่อผู้ประสานงานเพื่อกรณีนี้ตามแบบฟอร์มแนบ ทั้งนี้ ธปท. จะส่งข้อมูล/รายงานที่ขอ ให้ทาง e-mail เพื่อควบคุมการเปิดเผยข้อมูลให้ผู้ที่ไม่เกี่ยวข้อง และจะนำส่งข้อมูลของสถาบันท่านไปตามรายชื่อในแบบแจ้งรายชื่อผู้ประสานงานที่แจ้งไว้กับ ธปท. เท่านั้น

5. การเปลี่ยนสถานที่ปฏิบัติงาน หรือ การเปลี่ยนผู้ประสานงานกับ ธปท.

ให้สถาบันผู้ให้บริการบาทเน็ตแจ้งการเปลี่ยนแปลง และประสานงานกับ BAHTNET Help Desk รวมทั้งรายชื่อผู้ประสานงานเพื่อติดต่อผ่าน Microsoft Team : BAHTNET Group Chat เพื่อให้สามารถติดต่อได้ตลอดเวลา

6. การให้บริการทำรายการโอนเงินตามหนังสือสั่งโอน

กรณีที่ผู้ใช้บริการมีความจำเป็นต้องทำรายการโอนเงิน แต่ไม่สามารถดำเนินการได้ในสถานที่ของสมาชิกได้โดยสิ้นเชิง ธปท. ได้จัดเตรียมแนวทางกรณีฉุกเฉิน (Last Resort) ในการให้บริการทำรายการโอนเงินตามหนังสือสั่งโอน โดยสถาบันที่ประสงค์จะขอใช้บริการให้ประสานงานกับทีมบาทเน็ตเพื่อเตรียมการ สำหรับแนวปฏิบัติในการทำรายการโอนเงินตามหนังสือสั่งโอน สามารถ download ได้จาก BOT Website หัวข้อระบบการชำระเงิน / หนังสือเวียน

หากมีข้อสงสัยเกี่ยวกับแนวทางดำเนินการข้างต้น สามารถติดต่อสอบถามเพิ่มเติมได้ที่

ทีมบาทเน็ต โทรศัพท์ 0-2283-5045 หรือ Email : bnhelpdesk@bot.or.th

ฝ่ายการชำระเงินและพันธบัตร
ธนาคารแห่งประเทศไทย

**แบบแจ้งรายชื่อผู้ประสานงานระบบบาทเน็ต
รองรับการระบาดของไวรัสโคโรนา 2019 (COVID-19)**

สถาบันผู้ให้บริการบาทเน็ต :

เงื่อนไข รายชื่อตามแบบแจ้งนี้ใช้สำหรับการติดต่อประสานงานกับ ธปท. และขอข้อมูลของสถาบัน
ท่านในช่วงการระบาดของ COVID-19 ในเรื่องต่อไปนี้เท่านั้น

1. ข้อมูลการเคลื่อนไหวของบัญชีเงินฝาก/บัญชีชำระหนี้ของสถาบัน
2. รายงานสถานะการเงินบัญชี (Statement)
3. เกณฑ์สำหรับการโอนเงินผ่านระบบบาทเน็ต
4. เกณฑ์การดำรงตราสารหนี้ตามระเบียบ ธปท. ว่าด้วยมาตรการจัดการความเสี่ยงจาก
การชำระหนี้สุทธิต่อกันหลายฝ่าย (SRS)
5. เกณฑ์การดำรงตราสารหนี้ตามระเบียบ ธปท. ว่าด้วยการรับซื้อตราสารหนี้โดยมีสัญญา
ว่าผู้ขายจะซื้อคืนเพื่อเป็นเงินสภาพคล่องระหว่างวัน (ILF)
6. ข้อมูลบัญชีเงินฝากเพื่อแจ้งผู้สอบบัญชี
7. การประสานงานผ่าน Microsoft Team : BAHTNET Group Chat

<u>ชื่อ-นามสกุล</u>	<u>ตัวอย่างลายมือชื่อ</u>	<u>เงื่อนไข</u>	<u>โทรศัพท์</u>	<u>e-mail</u> <u>ขององค์กรท่านนั้น</u>
.....				
.....				
.....				
.....				
.....				
.....				

ทั้งนี้ การมอบอำนาจดังกล่าวให้มีผลตั้งแต่วันที่.....เป็นต้นไป

ลงลายมือชื่อ(ผู้อำนาจลงนาม).....

ลงลายมือชื่อ(ผู้อำนาจลงนาม).....

(.....)

(.....)

เพื่อ(ชื่อสถาบัน).....

หมายเหตุ ลงนามโดยผู้มีอำนาจลงนามตามหนังสือมอบอำนาจ ตามระเบียบธนาคารแห่งประเทศไทยว่าด้วย
การบริการบาทเน็ต (แบบฟอร์ม B-2.1)

แนวทางการดำเนินการและการผ่อนผันเกณฑ์ของระบบ ICAS
เพื่อรองรับการระบาดของไวรัสโคโรนา 2019 (COVID-19)

ด้วยสถานการณ์การระบาดของไวรัสโคโรนา 2019 (COVID-19) ซึ่งลุกลามและส่งผลกระทบต่อ
รุนแรงในวงกว้างต่อธุรกิจและประชาชนทั่วไปทั้งทางตรงและทางอ้อม เพื่อให้การดำเนินธุรกิจและการ
ให้บริการด้านการชำระเงินมีความต่อเนื่องสามารถรองรับความจำเป็นของภาคธุรกิจและประชาชน รวมทั้ง
ลดผลกระทบกับสถาบันการเงินและสร้างความเชื่อมั่นในระบบการชำระเงินของประเทศ

แนวทางการดำเนินการและการผ่อนผันเกณฑ์การขยายเวลา ค่าธรรมเนียม และค่าปรับนี้ใช้ในการ
ดำเนินงานระบบการหักบัญชีเช็คด้วยภาพเช็คและระบบการจัดเก็บภาพเช็ค (ICAS) ตั้งแต่วันที่ 2 สิงหาคม
2564 เป็นต้นไป จนกว่าจะกลับเข้าสู่ภาวะปกติ โดย ธปท.จะแจ้งให้ทราบต่อไป

1. การขอขยายเวลารอบการชำระดุลหักบัญชีการรับส่งข้อมูลเช็คเรียกเก็บ

1.1 รอบ Same-day

ให้ธนาคารสมาชิกดำเนินการตามพิธีปฏิบัติที่ผ่านมา คือ แจ้ง ธปท. ขอขยายเวลาก่อนถึง cut-off
15 นาฬิกา (ภายใน 15.45 น.) ธปท. จะขยายเวลาปิดรอบการชำระดุลหักบัญชีให้ไม่เกิน 16.30 น. และชำระ
ดุลการหักบัญชีเวลา 17.00 น. โดย ธปท. ผ่อนผันไม่คิดค่าธรรมเนียมการขอขยายเวลา

1.2 รอบ Next day

ให้ธนาคารสมาชิกดำเนินการตามพิธีปฏิบัติที่ผ่านมา คือ แจ้ง ธปท. ขอขยายเวลาก่อนถึง cut-off
15 นาฬิกา (ภายใน 10.00 น.) ธปท. จะขยายเวลาปิดรอบการชำระดุลหักบัญชีให้ไม่เกิน 10.30 น. และชำระ
การหักบัญชีเวลา 11.30 น. โดย ธปท. ผ่อนผันไม่คิดค่าธรรมเนียมการขอขยายเวลา

2. การสอบถามข้อมูล และหรือรายงานในระบบ ICAS

กรณีที่มีความประสงค์จะสอบถามข้อมูลและหรือขอรับรายงานดุลการหักบัญชีรายธนาคาร (Net
Clearing Position) และข้อมูลเช็คเรียกเก็บในระบบ ICAS จาก ธปท. ให้ธนาคารสมาชิกจัดทำแบบ
แจ้งรายชื่อผู้ประสานงานเพื่อกรณีนี้ตามแบบฟอร์มแนบ ทั้งนี้ ธปท. จะส่งข้อมูล/รายงานที่ขอ ให้ทาง
e-mail เพื่อควบคุมการเปิดเผยข้อมูลให้ผู้ที่ไม่เกี่ยวข้อง และจะนำส่งข้อมูลของสถาบันท่านไปตามรายชื่อ
ในแบบแจ้งรายชื่อผู้ประสานงานที่แจ้งไว้กับ ธปท. เท่านั้น

3. การเปลี่ยนสถานที่ปฏิบัติงาน หรือ การเปลี่ยนผู้ประสานงานกับ ธปท.

ให้ธนาคารสมาชิกแจ้งการเปลี่ยนแปลงและประสานงานกับ ICAS Help Desk รวมทั้งรายชื่อ
ผู้ประสานงานเพื่อติดต่อผ่าน MS Team เพื่อให้สามารถติดต่อสื่อสารได้ตลอดเวลา

4. กรณีรองรับแผนฉุกเฉินระบบ ICS ด้านธนาคารสมาชิกขัดข้อง

4.1 ธนาคารสมาชิกสร้าง ICS Package ได้

4.1.1 การเรียกเก็บเช็ค (วัน T)

กรณี ICMG ของธนาคารสมาชิกขัดข้องไม่สามารถรับส่งข้อมูลและภาพเช็คได้ ให้ธนาคาร
สมาชิกแจ้งให้ ICAS Help Desk ทราบ ซึ่งธนาคารสมาชิกอาจรับหรือส่งข้อมูลและภาพเช็คผ่าน ICMG สำรอง
ของธนาคารสมาชิก หากไม่สามารถรับหรือส่งข้อมูลและภาพเช็คได้ ให้ธนาคารสมาชิกจัดทำข้อมูล NIC และ
ดุลเจ้าหนี้ด้วยโปรแกรม ICS BCP จากข้อมูล NOC Package เฉพาะที่ยังไม่ได้ส่งเข้าระบบ ICS ต่อจากนั้นให้
ธนาคารสมาชิกที่ขัดข้องดำเนินการ ดังนี้

- (1) ส่งข้อมูลดุลเจ้าหนี้ และรายงาน Out-clearing Summary Report ให้ ธปท. ผ่านช่องทาง e-Exchange Service
 - (2) ส่งข้อมูล NIC และ Summary Report of In-clearing Cheque By Bank ให้ธนาคารผู้จ่ายผ่านช่องทาง e-Exchange Service
- ธปท. จะนำดุลการหักบัญชีรอบ Same-day ของธนาคารสมาชิกที่ขัดข้องจากข้อมูลดุลเจ้าหนี้ ตาม (1) ไปคำนวณรวมกับดุลในระบบ และแจ้งยอดชำระดุลระหว่างธนาคารให้ธนาคารสมาชิกที่เกี่ยวข้องแยกตามรายธนาคารผ่านช่องทาง e-Exchange Service และแจ้งให้ธนาคารผู้จ่ายนำข้อมูล NIC ตาม (2) ไปประมวลผลเพื่ออนุมัติตัดจ่ายต่อไป

4.1.2 การคืนเช็ค (วัน T+1)

กรณี ICMG ของธนาคารสมาชิกขัดข้องไม่สามารถรับส่งข้อมูลและภาพเช็คได้ ให้ธนาคารสมาชิกที่ขัดข้องในฐานะธนาคารผู้จ่ายจัดทำข้อมูลเช็คคืนในรูปแบบ CSV file ตามรูปแบบที่ ธปท. กำหนดในคู่มือแผนฉุกเฉินระบบ ICAS แยกตามรายธนาคาร ส่งให้ธนาคารผู้ส่งเรียกเก็บผ่านช่องทาง e-Exchange Service ตามแนวทางดำเนินการแผนฉุกเฉิน MB-03: กรณีระบบงาน ICS ของธนาคารสมาชิกขัดข้องรอบ Next-day

ธนาคารสมาชิกที่ขัดข้องดำเนินการขอปรับดุลการหักบัญชีกับธนาคารสมาชิกที่เกี่ยวข้องในรอบแก้ไขตลาดเคลื่อนพิเศษ (เฉพาะกรณีฉุกเฉิน) เวลา 11.00 น. (ธปท. อาจเพิ่มรอบ 14.00 น. หากจำเป็น)

4.2 ธนาคารสมาชิกไม่สามารถสร้าง ICS Package

ให้ธนาคารสมาชิกดำเนินการตามแผนฉุกเฉิน MB-02: กรณีระบบงาน ICS ของธนาคารสมาชิกขัดข้องรอบ Same-day และแก้ปัญหาด้วยการส่งตัวเช็คให้ธนาคารผู้จ่ายเพื่อเรียกเก็บแบบ In-house Cheque และแผนฉุกเฉิน MB-03: กรณีระบบงาน ICS ของธนาคารสมาชิกขัดข้องรอบ Next-day

4.2.1 การเรียกเก็บเช็ค (วัน T)

ให้ธนาคารสมาชิกทำข้อมูลเช็คส่งเรียกเก็บในรูปแบบ CSV File ตามรูปแบบที่ ธปท. กำหนดในคู่มือแผนฉุกเฉินระบบ ICAS พร้อมใบนำส่งเช็คที่แสดงยอดรวมจำนวนฉบับและจำนวนเงินของเช็คที่นำส่งแยกตามรายธนาคาร และส่งให้ธนาคารผู้จ่ายผ่านช่องทาง e-Exchange Service สำหรับตัวเช็คให้นำส่งธนาคารผู้จ่ายคู่มือเพื่อเรียกเก็บแบบ In-house

4.2.2 การคืนเช็ค (วัน T+1)

ให้ธนาคารผู้จ่ายจัดทำข้อมูลเช็คคืนในรูปแบบ CSV file ตามรูปแบบที่ ธปท. กำหนดในคู่มือแผนฉุกเฉินระบบ ICAS โดยแยกตามรายธนาคารผู้ส่งเรียกเก็บ และส่งให้ธนาคารผู้ส่งเรียกเก็บผ่านช่องทาง e-Exchange Service

ธนาคารสมาชิกที่ขัดข้องขอปรับดุลการหักบัญชีรอบ Next-day สำหรับเช็คส่วนที่ยังไม่ได้ขอปรับดุลการหักบัญชีในวัน T และเช็คคืน กับธนาคารสมาชิกที่เกี่ยวข้องในรอบแก้ไขตลาดเคลื่อนพิเศษ (เฉพาะกรณีฉุกเฉิน) เวลา 11.00 น. (ธปท. อาจเพิ่มรอบ 14.00 น. หากจำเป็น)

หากมีข้อสงสัยเกี่ยวกับแนวทางดำเนินการข้างต้น สามารถติดต่อสอบถามเพิ่มเติมได้ที่

ทีมหักบัญชีเช็ค โทรศัพท์ 0-2283-6150 หรือ Email : ICAS-HelpDesk@bot.or.th

ฝ่ายการชำระเงินและพันธบัตร
ธนาคารแห่งประเทศไทย

แบบแจ้งรายชื่อผู้ประสานงานระบบ ICAS
รองรับการระบาดของไวรัสโคโรนา 2019 (COVID-19)

ชื่อธนาคารสมาชิก :

เงื่อนไข รายชื่อตามแบบแจ้งนี้ใช้สำหรับการติดต่อประสานงานกับ ธปท. เพื่อขอข้อมูลของสถาบัน
ท่านในช่วงการระบาดของ COVID-19 ในเรื่องต่อไปนี้เท่านั้น

1. รายงานดุลการหักบัญชีรายธนาคาร (Net Clearing Position)
2. ข้อมูลเช็คเรียกเก็บในระบบ ICAS
3. การประสานงานผ่าน Microsoft Team : ICAS Group Chat

<u>ชื่อ-นามสกุล</u>	<u>ตัวอย่างลายมือชื่อ</u>	<u>เงื่อนไข</u>	<u>โทรศัพท์</u>	<u>e-mail</u> <u>ขององค์กรท่านนั้น</u>
.....				
.....				
.....				
.....				
.....				
.....				

ทั้งนี้ การมอบอำนาจดังกล่าวให้มีผลตั้งแต่วันที่.....เป็นต้นไป

ลงลายมือชื่อ(ผู้อำนาจลงนาม)..... ลงลายมือชื่อ(ผู้อำนาจลงนาม).....
(.....) (.....)

เพื่อ(ชื่อสถาบัน).....

หมายเหตุ ลงนามโดยผู้มีอำนาจลงนามตามหนังสือมอบอำนาจ ตามระเบียบธนาคารแห่งประเทศไทยว่าด้วย
ระบบการหักบัญชีเช็คด้วยภาพเช็คและระบบการจัดเก็บภาพเช็ค (แบบฟอร์ม I-2)

แนวปฏิบัติ
เรื่อง การใช้เครื่องคอมพิวเตอร์ลูกข่ายระบบ BAHTNET และระบบ ICAS
ในการปฏิบัติงานนอกสถานที่ทำการ ภายใต้สถานการณ์ฉุกเฉินการระบาดของ
ไวรัสโคโรนา 2019 (COVID-19)

ตุลาคม 2564



ธนาคารแห่งประเทศไทย

จัดทำโดย

ฝ่ายการชำระเงินและพันธบัตร

สายระบบข้อมูลสารสนเทศ

ธนาคารแห่งประเทศไทย

โทรศัพท์ 0 2283 5045, 0 2283 6150

แนวปฏิบัติธนาคารแห่งประเทศไทย

เรื่อง การใช้เครื่องคอมพิวเตอร์ลูกข่ายระบบ BAHTNET และระบบ ICAS ในการปฏิบัติงานนอกสถานที่ทำการ ภายใต้สถานการณ์ฉุกเฉินการระบาดของไวรัสโคโรนา 2019 (COVID-19)

1. เหตุผลในการออกแนวปฏิบัติ

ด้วยสถานการณ์การระบาดของไวรัสโคโรนา 2019 (COVID-19) มีความรุนแรง และมีแนวโน้มยืดเยื้อต่อเนื่อง ประกอบกับนโยบายภาครัฐที่สนับสนุนให้การทำงานจากที่บ้านในช่วงการระบาด สถานการณ์ดังกล่าวอาจส่งผลกระทบต่อการทำงานของผู้ใช้บริการ BAHTNET และธนาคารสมาชิกในระบบการหักบัญชีเช็คด้วยภาพเช็คและระบบการจัดเก็บภาพเช็ค (ธนาคารสมาชิกในระบบ ICAS) ซึ่งยังคงให้บริการด้านการชำระเงินแก่ภาคธุรกิจและประชาชนอย่างต่อเนื่อง รวมทั้งให้ความสำคัญในการดูแลความปลอดภัยในชีวิตและสุขภาพของพนักงานของสถาบันผู้ใช้บริการและธนาคารสมาชิก

ธนาคารแห่งประเทศไทย (ธปท.) จึงกำหนดแนวปฏิบัติการใช้เครื่องคอมพิวเตอร์ลูกข่ายระบบ BAHTNET และระบบ ICAS ในการปฏิบัติงานนอกสถานที่ทำการภายใต้สถานการณ์ฉุกเฉินการระบาดของไวรัสโคโรนา 2019 (COVID-19) (แนวปฏิบัติ) เพื่อเป็นแนวทางการดำเนินการของสถาบันผู้ใช้บริการ BAHTNET และธนาคารสมาชิกในระบบ ICAS ที่ประสงค์จะไปปฏิบัติงานนอกสถานที่ทำการ ภายใต้สถานการณ์ฉุกเฉินการระบาดของ COVID-19 โดยให้มีการบริหารจัดการความเสี่ยงที่อาจเกิดขึ้นจากการปฏิบัติงานนอกสถานที่ทำการ เช่น ความเสี่ยงจากข้อมูลสำคัญรั่วไหลไปยังผู้ไม่มีหน้าที่เกี่ยวข้องทั้งภายในและภายนอกองค์กร (Data Leak) ความเสี่ยงจากภัยฉ้อโกง (Fraud Incident) ความเสี่ยงจากการถูกคุกคามด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ (Cyber Attack) ฯลฯ

แนวปฏิบัตินี้เป็นแนวทางเบื้องต้นในการกำหนดมาตรการรักษาความมั่นคงปลอดภัยในการปฏิบัติงานนอกสถานที่ทำการขั้นต่ำ โดยผู้ใช้บริการ BAHTNET และธนาคารสมาชิกในระบบ ICAS สามารถกำหนดมาตรการรักษาความมั่นคงปลอดภัยที่แตกต่างสูงขึ้นจากแนวปฏิบัติฉบับนี้ได้ ทั้งนี้ มาตรการดังกล่าวควรมีความสอดคล้อง และสามารถป้องกันความเสี่ยงของคอมพิวเตอร์ลูกข่ายได้อย่างมีประสิทธิภาพและเป็นไปตามมาตรฐานที่ยอมรับได้ รวมทั้งสอดคล้องกับแนวปฏิบัติที่ดี (best practice) ในการเตรียมความพร้อมด้านเทคโนโลยีสารสนเทศ ภายใต้สถานการณ์การระบาดของ COVID-19 นอกจากนี้ ผู้ใช้บริการ BAHTNET ต้องดำเนินการให้มีการรักษาความมั่นคงปลอดภัยในองค์กรตามข้อกำหนดในระเบียบ ธปท. ว่าด้วยการบริการบาทเน็ต ตามประกาศ ธปท. เรื่อง มาตรฐานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของคอมพิวเตอร์ลูกข่ายระบบบาทเน็ต รวมทั้งแนวปฏิบัติการรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ลูกข่ายของผู้ใช้บริการบาทเน็ต ฉบับปรับปรุง และธนาคารสมาชิกในระบบ ICAS ต้องดำเนินการให้มีการรักษาความมั่นคงปลอดภัยในองค์กรตามข้อกำหนดในระเบียบ ธปท. ว่าด้วยระบบการหักบัญชีเช็คด้วยภาพเช็คและระบบการจัดเก็บภาพเช็ค และ ประกาศ ธปท. เรื่อง มาตรฐานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของคอมพิวเตอร์ลูกข่ายการหักบัญชีเช็คด้วยภาพเช็คและระบบการจัดเก็บภาพเช็ค (รายละเอียดตามภาคผนวกท้ายแนวปฏิบัติ)

2. ขอบเขตการบังคับใช้

แนวปฏิบัตินี้เป็นกรอบแนวทางให้ผู้ให้บริการ BAHTNET และธนาคารสมาชิกระบบ ICAS ถือปฏิบัติภายใต้สถานการณ์การระบาดของ COVID-19 จนกว่าสถานการณ์จะกลับเข้าสู่ภาวะปกติ โดย ธปท. จะแจ้งการเริ่มใช้แนวปฏิบัติและการยกเลิกต่อไป

3. เนื้อหา

3.1 ความหมาย ในแนวปฏิบัติฉบับนี้

“แนวปฏิบัติ” หมายถึง แนวปฏิบัติธนาคารแห่งประเทศไทย เรื่อง การใช้เครื่องคอมพิวเตอร์ลูกข่ายระบบ BAHTNET และระบบ ICAS ในการปฏิบัติงานนอกสถานที่ทำการ ภายใต้สถานการณ์การระบาดของไวรัสโคโรนา 2019 (COVID-19)

“สมาชิก” หมายถึง ผู้ใช้บริการบาทเน็ตตามระเบียบธนาคารแห่งประเทศไทยว่าด้วยการบริการบาทเน็ต (BAHTNET) และธนาคารสมาชิกตามระเบียบธนาคารแห่งประเทศไทยว่าด้วยระบบการหักบัญชีเช็คด้วยภาพเช็คและระบบการจัดเก็บภาพเช็ค (ICAS)

“คอมพิวเตอร์ลูกข่าย” หมายถึง ระบบคอมพิวเตอร์ของผู้ใช้บริการบาทเน็ตและธนาคารสมาชิกที่ใช้เชื่อมโยงกับระบบงานของ ธปท. ประกอบด้วย

(1) ระบบ BAHTNET เฉพาะในส่วนของระบบคอมพิวเตอร์สำหรับการส่งข้อความผ่าน SWIFT และบริการด้านการเงินด้วยวิธีอิเล็กทรอนิกส์ (Electronic Financial Services) ไม่รวมระบบงานคอมพิวเตอร์อื่นที่เชื่อมโยงเพื่อการรับส่งข้อมูลโดยตรงกับระบบคอมพิวเตอร์แม่ข่ายของ ธปท. (Host to Host)

(2) ระบบ ICAS เฉพาะเครื่องคอมพิวเตอร์เพื่อการใช้งานระบบ ICAS ผ่าน บริการด้านการเงินด้วยวิธีอิเล็กทรอนิกส์ (Electronic Financial Services) ไม่รวม เครื่องรับส่งข้อมูลและภาพเช็ค (Imaged Cheque Member Gateway: ICMG)

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

“ความมั่นคงปลอดภัย” หมายถึง การดำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิดชอบ (Accountability) การห้ามปฏิเสธความรับผิดชอบ (Non-repudiation) และความน่าเชื่อถือ (Reliability)

3.2 รายละเอียดของแนวปฏิบัติ

ก่อนที่สมาชิกจะปฏิบัติงานนอกสถานที่ทำการ สมาชิกต้องดำเนินการตามระเบียบ ประกาศ และแนวปฏิบัติที่เกี่ยวข้องตามที่กำหนดไว้ในภาคผนวก และต้องดำเนินการ ดังนี้

3.2.1 การกำหนดมาตรการในการกำกับดูแลกิจการ (Governance policy)

สมาชิกต้องจัดให้มีนโยบายและมาตรการในการกำกับดูแลกิจการและการบริหาร ความเสี่ยงที่อาจเกิดขึ้นจากการปฏิบัติงานนอกสถานที่ทำการ โดยได้รับอนุมัติจากคณะกรรมการบริหารความเสี่ยง ขององค์กร (Risk committee) รวมทั้งมีการติดตามและตรวจสอบการปฏิบัติงานให้เป็นไปตามหลักเกณฑ์ ที่กำหนดและตามที่ได้รับอนุมัติ ทั้งนี้ มาตรการดังกล่าวอย่างน้อยต้องครอบคลุมถึงกรณีดังต่อไปนี้

(1) การจัดให้มีการประเมินความเสี่ยงและกำหนดมาตรการควบคุมความเสี่ยงจาก การปฏิบัติงานนอกสถานที่ทำการในทุกมิติ อาทิ ความเสี่ยงจากภัยคุกคามทางไซเบอร์ ความเสี่ยงจากการ มีผู้ปฏิบัติงานติดเชื้อ COVID-19 ในจำนวนที่มีนัยสำคัญต่อการปฏิบัติงาน ความเสี่ยงจากข้อมูลสำคัญรั่วไหล ไปยังผู้ไม่มีหน้าที่ที่เกี่ยวข้องทั้งภายในและภายนอกองค์กร (Data Leak) ไม่ว่าโดยเจตนาของผู้ปฏิบัติงานหรือ จากเหตุอื่น เช่น ผู้ปฏิบัติงานกระทำการโดยประมาททำให้อุปกรณ์สูญหาย เป็นต้น

(2) ขอบเขตการได้รับอนุมัติจากคณะกรรมการบริหารความเสี่ยงขององค์กร (Risk committee) ต้องมีการกำหนดรายละเอียดขอบเขตงานที่สามารถปฏิบัติงานนอกสถานที่ทำการ การประเมินความเสี่ยง และมาตรการควบคุมความเสี่ยง รวมทั้งจัดให้มีการติดตามและตรวจสอบการปฏิบัติ ตามหลักเกณฑ์ (Compliance) อย่างเหมาะสม โดยกำหนดให้มีการตรวจสอบการปฏิบัติงานและการรายงานผล การตรวจสอบเสนอผู้บริหารขององค์กรเพื่อให้มั่นใจว่าผู้ปฏิบัติงานสามารถปฏิบัติตามแนวทางที่ได้รับอนุมัติ จาก Risk committee แล้ว

(3) จัดให้มี Code of conducts สำหรับผู้ปฏิบัติงานนอกสถานที่ทำการ โดยให้ ผู้ปฏิบัติงานลงนามยินยอมและถือปฏิบัติอย่างเคร่งครัด

3.2.2 การควบคุมการเข้าใช้คอมพิวเตอร์ลูกข่าย

สมาชิกต้องจัดให้มีมาตรการควบคุมการเข้าใช้งานคอมพิวเตอร์ลูกข่ายที่ตั้งอยู่ นอกสถานที่ทำการ เพื่อป้องกันการลักลอบนำบัญชีของผู้ปฏิบัติงานไปทำธุรกรรม โดยผู้ที่มีสิทธิทั้งภายใน และภายนอกองค์กร ทั้งนี้ มาตรการดังกล่าวอย่างน้อยต้องครอบคลุมถึงกรณีดังต่อไปนี้

(1) การจัดให้มีอุปกรณ์และเครือข่ายที่มั่นคงปลอดภัย โดยเฉพาะอุปกรณ์และ เครือข่ายที่เชื่อมต่อไปยังคอมพิวเตอร์ลูกข่าย เพื่อควบคุมความเสี่ยงการเข้าถึงคอมพิวเตอร์ลูกข่ายและจากภัย คุกคามทางไซเบอร์ใหม่ ๆ ที่เกิดขึ้น เช่น ใช้อุปกรณ์และเครือข่ายที่ได้รับอนุญาตจากองค์กร เพิ่มการเฝ้าระวัง ภัยคุกคามทางไซเบอร์ บันทึกและติดตาม Log การเข้าใช้งานระบบงานสำคัญอย่างใกล้ชิด เป็นต้น

(2) กำหนดพื้นที่ในการปฏิบัติงานนอกสถานที่ทำการให้เป็นสัดส่วนและปลอดภัย เพื่อป้องกันไม่ให้ข้อมูลสำคัญรั่วไหลไปยังผู้ไม่มีหน้าที่เกี่ยวข้องทั้งภายในและภายนอกองค์กร รวมทั้งกำหนด สิทธิและหน้าที่การใช้งานระบบงานและการเข้าถึงข้อมูลในระบบ BAHTNET และระบบ ICAS ตามอำนาจ หน้าที่ของผู้ปฏิบัติงาน และทำการทบทวนการกำหนดสิทธิและหน้าที่ดังกล่าวอย่างสม่ำเสมออย่างน้อย หนึ่งครั้งต่อปี

3.2.3 การควบคุมด้านการปฏิบัติงาน

สมาชิกต้องกำหนดมาตรการด้านการรักษาความมั่นคงปลอดภัย เพื่อกำหนด แนวทางการติดตาม และการเตรียมความพร้อมสำหรับเหตุที่กระทบต่อความมั่นคงปลอดภัยคอมพิวเตอร์ ลูกข่ายหรืออาจเกิดความเสียหายต่อระบบ BAHTNET หรือระบบ ICAS ทั้งนี้ มาตรการดังกล่าวอย่างน้อย ต้องครอบคลุมถึงกรณีดังต่อไปนี้

(1) การจัดให้มีเครื่องมือหรือกระบวนการในการติดตาม ตรวจสอบ และตรวจจับ ธุรกรรมผิดปกติ ธุรกรรมต้องสงสัย รวมทั้งเฝ้าระวังภัยคุกคามทางไซเบอร์อย่างใกล้ชิด เช่น เพิ่มการตรวจสอบ ในกิจกรรมสำคัญ เพิ่มความถี่ในการติดตามและรายงานต่อผู้บริหาร เป็นต้น

(2) การจัดทำแผนฉุกเฉินสำหรับการรับมือและตอบสนองต่อเหตุการณ์ผิดปกติ ให้ครอบคลุมการปฏิบัติงานนอกสถานที่ทำการเพื่อตอบสนองต่อเหตุการณ์ความเสี่ยงสำคัญ เช่น ความเสี่ยง จากการทุจริตและประพฤติมิชอบ ข้อมูลสำคัญรั่วไหลไปยังผู้ไม่มีหน้าที่เกี่ยวข้องทั้งภายในและภายนอกองค์กร และการคุกคามทางไซเบอร์ รวมทั้งกรณีระบบงานขัดข้อง หรือไม่สามารถเชื่อมต่อคอมพิวเตอร์ลูกข่าย จากนอกที่สถานที่ทำการได้ โดยจัดให้มีระบบช่วยควบคุมการปฏิบัติงานโดยสามารถตรวจสอบข้อมูลย้อนหลังได้¹ และกำหนดขั้นตอนการแก้ไขปัญหา ทีมงานหรือผู้รับผิดชอบ รวมถึงวิธีการรายงานปัญหาให้กับผู้บริหาร และ ผู้เกี่ยวข้องทราบอย่างรวดเร็วที่สุดเท่าที่จะทำได้ เพื่อแก้ไขปัญหาให้กลับคืนสู่สภาวะปกติโดยเร็ว

3.2.4 การรักษาความปลอดภัยระบบคอมพิวเตอร์สำหรับผู้ให้บริการบาทเนตผ่าน SWIFT

กรณีผู้ให้บริการบาทเนต ซึ่งส่งข้อความผ่าน SWIFT ต้องจัดให้มีมาตรการรักษา ความมั่นคงปลอดภัยตามที่ SWIFT กำหนด โดยเฉพาะ SWIFT Customer Security Program (SWIFT CSP)

4. วันเริ่มต้นบังคับใช้

แนวปฏิบัติฉบับนี้ให้ใช้บังคับตั้งแต่วันที่ 21 ตุลาคม 2564 เป็นต้นไป จนกว่า ราช. แจ้งยกเลิก

¹ ตัวอย่างระบบช่วยควบคุมการปฏิบัติงาน เช่น VDI recording เพื่อบันทึกการทำงานตลอดเวลาปฏิบัติงานในเครื่อง VDI ของระบบงานสำคัญโดยต้องสามารถตรวจสอบย้อนหลังได้ หรือ Security Logging เพื่อบันทึก session การเข้าใช้ และเลิกใช้งานฟังก์ชันในระบบงานสำคัญ ซึ่งสามารถตรวจจับการใช้งานในเวลาที่เกิดผิดปกติได้ เป็นต้น

ระเบียบประกาศ และข้อกำหนดที่เกี่ยวข้อง

สมาชิกต้องดำเนินการให้มีการรักษาความมั่นคงปลอดภัยในองค์กร เพื่อให้มั่นใจว่ากระบวนการทำงานและธุรกรรม มีการรักษาความมั่นคงปลอดภัยที่ดี เป็นไปตามมาตรฐานสากล และดำเนินการให้สอดคล้องกับข้อกำหนดตามกฎหมายในปัจจุบัน โดยมีระเบียบ ประกาศ และแนวปฏิบัติที่เกี่ยวข้อง (และที่แก้ไขเพิ่มเติม) ดังนี้

1. แนวปฏิบัติที่ดี (best practice) ในการเตรียมความพร้อมด้านเทคโนโลยีสารสนเทศ ภายใต้สถานการณ์การระบาดของ COVID 19 ออกโดยฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ

2. ระบบ BAHTNET

- ระเบียบธนาคารแห่งประเทศไทยว่าด้วยการบริการบาทเน็ต
- ประกาศ ธปท.ที่ สรข. 4/2560 เรื่อง มาตรฐานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของคอมพิวเตอร์ลูกข่ายระบบบาทเน็ต
- แนวปฏิบัติเรื่อง การรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ลูกข่ายของผู้ใช้บริการบาทเน็ต ตามหนังสือเวียน ฝชพ. (ว.) 3/2564 ลงวันที่ 1 กุมภาพันธ์ 2564

3. ระบบ ICAS

- ระเบียบธนาคารแห่งประเทศไทยว่าด้วยระบบการหักบัญชีเช็คด้วยภาพเช็คและระบบการจัดเก็บภาพเช็ค
- ประกาศ ธปท. ที่สรข. 5/2560 เรื่อง มาตรฐานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของคอมพิวเตอร์ลูกข่ายระบบการหักบัญชีเช็คด้วยภาพเช็คและระบบจัดการภาพเช็ค