

-ร่าง- แนวปฏิบัติ

เรื่อง การรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ลูกข่าย BAHTNET Lite
ของผู้ใช้บริการบาทเน็ต

สิงหาคม 2566



ธนาคารแห่งประเทศไทย

จัดทำโดย

ฝ่ายการชำระเงินและพันธบัตร

สายระบบข้อเสนอเทศ

ธนาคารแห่งประเทศไทย

โทรศัพท์ 0 2283 6667 และ 0 2283 6539

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

สารบัญ

หัวข้อ	หน้า
1. เหตุผลในการออกแนวปฏิบัติ.....	1
2. ขอบเขตการบังคับใช้.....	2
3. เนื้อหา	2
3.1 ความหมาย	2
3.2 รายละเอียดของแนวปฏิบัติ	2
4. วันเริ่มต้นบังคับใช้.....	4
ภาคผนวก 1 : แนวทางการจัดเตรียมเครื่องคอมพิวเตอร์ลูกข่ายระบบ BAHTNET Lite พร้อมคำถาม - คำตอบ	5
ภาคผนวก 2 : ระเบียบ ประกาศ และข้อกำหนดที่เกี่ยวข้อง.....	7

แนวปฏิบัติธนาคารแห่งประเทศไทย

เรื่อง การรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ลูกค้าระบบ BAHTNET Lite ของผู้ใช้บริการบาทเน็ต

1. เหตุผลในการออกแนวปฏิบัติ

ด้วยธนาคารแห่งประเทศไทย (ธปท.) ได้ตระหนักถึงความเสี่ยงกรณีเกิดเหตุวินาศภัยหรือเหตุฉุกเฉินที่ทำให้ ธปท. ไม่สามารถให้บริการระบบบาทเน็ตได้โดยสิ้นเชิง เช่น การถูกคุกคามด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ (Cyber Attack) การก่อการร้าย ภัยพิบัติรุนแรง เป็นต้น จึงได้จัดทำแผนฉุกเฉินการดำเนินการกรณีระบบบาทเน็ตไม่สามารถให้บริการได้โดยสิ้นเชิง (BAHTNET Offline: BNO) พร้อมทั้งพัฒนาระบบ BAHTNET Lite ซึ่งเป็นเครื่องมือการปฏิบัติงานในช่วงที่ ธปท. ประกาศใช้ BNO ที่รองรับมาตรฐานข้อความทางการเงิน ISO 20022 เพื่อให้การชำระเงินระหว่างสถาบันสามารถดำเนินการได้อย่างต่อเนื่อง ไม่เกิดผลกระทบในวงกว้าง

ธปท. จึงกำหนดแนวปฏิบัติการรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ลูกค้าระบบ BAHTNET Lite ของผู้ใช้บริการบาทเน็ต เพื่อกำหนดแนวทางดำเนินการสำหรับผู้ใช้บริการบาทเน็ตในการรักษาความมั่นคงปลอดภัยของคอมพิวเตอร์ลูกค้าระบบ BAHTNET Lite ที่ใช้ปฏิบัติงานในช่วงที่ ธปท. ประกาศใช้ BNO โดยผู้ใช้บริการบาทเน็ตจะต้องจัดการให้มีการบริหารจัดการความเสี่ยงที่อาจเกิดขึ้นจากการใช้งานระบบ BAHTNET Lite ผ่านเครือข่าย Internet เช่น ความเสี่ยงจากข้อมูลสำคัญรั่วไหลไปยังผู้ไม่มีหน้าที่เกี่ยวข้องทั้งภายในและภายนอกองค์กร (Data Leak) ความเสี่ยงจากการถูกคุกคามด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ (Cyber Attack) เป็นต้น

แนวปฏิบัตินี้เป็นแนวทางเบื้องต้นในการกำหนดมาตรการรักษาความมั่นคงปลอดภัยขั้นต่ำสำหรับการใช้เครื่องคอมพิวเตอร์ลูกค้าระบบ BAHTNET Lite โดยผู้ใช้บริการบาทเน็ตสามารถกำหนดมาตรการรักษาความมั่นคงปลอดภัยที่สูงขึ้นจากแนวปฏิบัติฉบับนี้ได้ หากมาตรการดังกล่าวมีความสอดคล้อง และสามารถป้องกันความเสี่ยงของคอมพิวเตอร์ลูกค้าระบบ BAHTNET Lite ได้อย่างมีประสิทธิภาพและเป็นไปตามมาตรฐานที่ยอมรับได้ นอกจากนี้ ผู้ใช้บริการบาทเน็ตต้องดำเนินการให้มีการรักษาความมั่นคงปลอดภัยในองค์กรตามข้อกำหนดในระเบียบ ธปท. ว่าด้วยการบริการบาทเน็ต ประกาศ ธปท. เรื่อง มาตรฐานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของคอมพิวเตอร์ลูกค้าระบบบาทเน็ต และแนวปฏิบัติการรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ลูกค้าของผู้ใช้บริการบาทเน็ต (รายละเอียดตามภาคผนวก 2 ท้ายแนวปฏิบัติ)

2. ขอบเขตการบังคับใช้

แนวปฏิบัตินี้เป็นกรอบแนวทางให้ผู้ใช้บริการบาทเน็ต ทั้งที่เป็นสถาบันการเงินและไม่ใช่สถาบันการเงิน ใช้กำหนดมาตรการรักษาความมั่นคงปลอดภัยของคอมพิวเตอร์ลูกค้าระบบ BAHTNET Lite

3. เนื้อหา

3.1 ความหมาย ในแนวปฏิบัติฉบับนี้

“แนวปฏิบัติ” หมายถึง แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ลูกข่ายระบบ BAHTNET Lite ของผู้ให้บริการบาทเน็ต

“คอมพิวเตอร์ลูกข่ายระบบ BAHTNET Lite” หมายถึง ระบบคอมพิวเตอร์ของผู้ให้บริการบาทเน็ตที่ใช้เชื่อมโยงกับระบบ BAHTNET Lite ของ ธปท.

“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)

“เหตุการณ์ละเมิดต่อความมั่นคงปลอดภัย” หมายถึง เหตุการณ์ หรือการกระทำที่มีเจตนาทำให้มีความเสี่ยง หรือก่อให้เกิดผลกระทบต่อความมั่นคงปลอดภัยของคอมพิวเตอร์ลูกข่าย รวมถึงการฉ้อโกง อันนำไปสู่ความเสียหายทางการเงิน ความเสียหายต่อชื่อเสียง และการขาดความเชื่อมั่นของผู้ใช้บริการต่อการให้บริการทางการเงินโดยรวม

“บริการ EFS” หมายถึง บริการด้านการเงินด้วยวิธีอิเล็กทรอนิกส์ตามระเบียบธนาคารแห่งประเทศไทยว่าด้วยการให้บริการด้านการเงินด้วยวิธีอิเล็กทรอนิกส์ (Electronic Financial Services)

3.2 รายละเอียดของแนวปฏิบัติ

ผู้ให้บริการบาทเน็ตต้องกำหนดมาตรการรักษาความมั่นคงปลอดภัย รวมถึงควบคุมการเปลี่ยนแปลงของเครือข่าย และระบบคอมพิวเตอร์ที่เชื่อมโยงกับคอมพิวเตอร์ลูกข่ายระบบ BAHTNET Lite ตามที่กำหนดใน “แนวปฏิบัติธนาคารแห่งประเทศไทย เรื่อง การรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ลูกข่ายของผู้ให้บริการบาทเน็ต” ยกเว้น “ข้อ 4.2.1 การควบคุมเครือข่ายและระบบคอมพิวเตอร์” ให้ใช้แนวปฏิบัติฉบับนี้แทน โดยมีรายละเอียดดังนี้

(1) ควบคุมการเข้าถึงศูนย์คอมพิวเตอร์ของผู้ใช้บริการบาทเน็ต รวมถึงอุปกรณ์ Network ที่เชื่อมต่อกับระบบ BAHTNET Lite

(2) จัดให้มีการรักษาความมั่นคงปลอดภัยของเครือข่ายที่เชื่อมต่อระหว่างคอมพิวเตอร์ลูกข่ายระบบ BAHTNET Lite กับระบบ BAHTNET Lite ของ ธปท. เช่น การติดตั้ง Firewall เป็นต้น

(3) คอมพิวเตอร์ลูกข่ายระบบ BAHTNET Lite ต้องมีประสิทธิภาพและการรักษาความมั่นคงปลอดภัยเทียบเท่ากับคอมพิวเตอร์ลูกข่ายที่ใช้เชื่อมโยงกับระบบบาทเน็ตของ ธปท.

(4) แยกคอมพิวเตอร์ลูกข่ายระบบ BAHTNET Lite ออกจากคอมพิวเตอร์ลูกข่ายที่ใช้เชื่อมโยงกับระบบบาทเน็ตของ ธปท.

(5) ไม่ใช้งานระบบงานอื่นบนคอมพิวเตอร์ลูกข่ายระบบ BAHTNET Lite รวมถึงระบบรับ-ส่งอีเมล

(6) แบ่งแยกเครือข่ายคอมพิวเตอร์ลูกข่ายระบบ BAHTNET Lite ออกจากเครือข่ายของคอมพิวเตอร์ลูกข่ายที่เชื่อมต่อกับระบบบาทเน็ตของ ธปท. และเครือข่ายอื่นที่ไม่จำเป็นต้องเชื่อมโยง เช่น แยกเครือข่ายของกลุ่มคอมพิวเตอร์ลูกข่ายระบบ BAHTNET Lite จากเครือข่ายสำหรับระบบงานอื่นภายในองค์กร เป็นต้น

(7) กรณีไม่สามารถแบ่งแยกเครือข่ายคอมพิวเตอร์ลูกข่ายระบบ BAHTNET Lite ออกจากเครือข่ายอื่นภายในองค์กร ต้องดำเนินการประเมินความเสี่ยงและกำหนดมาตรการควบคุมความเสี่ยงในทุกมิติ อาทิ ความเสี่ยงจากภัยคุกคามทางไซเบอร์ ความเสี่ยงจากข้อมูลสำคัญรั่วไหลไปยังผู้ไม่มีหน้าที่ที่เกี่ยวข้องทั้งภายในและภายนอกองค์กร (Data Leak) ไม่ว่าจะโดยเจตนาของผู้ปฏิบัติงานหรือโดยประมาท เป็นต้น

(8) อนุญาตการเชื่อมต่อเครือข่าย Internet กับคอมพิวเตอร์ลูกข่ายระบบ BAHTNET Lite เฉพาะในช่วงที่มีการประกาศใช้ BAHTNET Offline และยกเลิกการเชื่อมต่อเครือข่าย Internet เมื่อมีการประกาศยุติการประกาศใช้ BAHTNET Offline โดยจัดให้มีกระบวนการและคู่มือการอนุญาตและยกเลิกการเชื่อมต่อเครือข่าย Internet

(9) กำหนดให้การเชื่อมต่อเครือข่าย Internet กับคอมพิวเตอร์ลูกข่ายระบบ BAHTNET Lite สามารถทำได้ผ่านเครือข่ายภายในองค์กร หรือเชื่อมต่อผ่านอุปกรณ์ที่มีการรักษาความมั่นคงปลอดภัยเทียบเท่ากับอุปกรณ์เครือข่ายภายในองค์กร โดยอนุญาตให้เข้าใช้บริการได้เฉพาะระบบ BAHTNET Lite ของ ธปท. (IP Address Whitelisting) เท่านั้น

(10) ป้องกันและตรวจจับการบุกรุกของโปรแกรมประสงค์ร้าย (Malware) รวมถึงภัยคุกคามขั้นสูง (Advance Persistent Threat หรือ APT) เพื่อป้องกันความเสียหายที่จะเกิดขึ้นแก่คอมพิวเตอร์ลูกข่ายระบบ BAHTNET Lite หรือการรั่วไหลของข้อมูลที่เป็นความลับออกไปนอกองค์กร เช่น การติดตั้งโปรแกรม Anti-Virus Anti-Malware และ Update Signature จากผู้ผลิตอย่างสม่ำเสมอ มีการทำ Scheduled Scan ตามระยะเวลาที่เหมาะสม และพิจารณาติดตั้งระบบป้องกันภัยคุกคามขั้นสูง (APT Protection) ไม่นำโปรแกรมที่ไม่ได้รับการตรวจสอบหรือไม่มีลิขสิทธิ์ที่ถูกต้องมาใช้งาน เป็นต้น

(11) กำหนดความถี่ในการติดตั้งโปรแกรมเพื่อปิดช่องโหว่ (Windows Security Patch) สำหรับ Window Operating System ของเครื่องคอมพิวเตอร์ลูกข่ายระบบ BAHTNET Lite อย่างเหมาะสม อย่างน้อยตามมาตรฐานที่ยอมรับโดยทั่วไป

(12) กำหนดวิธีการควบคุมการแก้ไขเปลี่ยนแปลง (Change Management) การตั้งค่าเครือข่าย และโปรแกรมระบบคอมพิวเตอร์ ที่เกี่ยวข้องกับคอมพิวเตอร์ลูกข่ายระบบ BAHTNET Lite เช่น มีการทำทะเบียนอุปกรณ์ บันทึก และขออนุมัติเมื่อเข้าใช้งานหรือปรับเปลี่ยนการตั้งค่าโปรแกรมระบบคอมพิวเตอร์ และอุปกรณ์ Network เป็นต้น

(13) ปิดคอมพิวเตอร์ลูกข่ายระบบ BAHTNET Lite เมื่อไม่มีการใช้งาน โดยอาจใช้เป็นเครื่องสำรองเพื่อการใช้บริการ EFS ได้โดยอัตโนมัติ

(14) กรณีคอมพิวเตอร์ลูกข่ายระบบ BAHTNET Lite ถูกนำไปใช้กับบริการ EFS ต้องผ่านกระบวนการตรวจสอบความมั่นคงปลอดภัยของเครื่องคอมพิวเตอร์ลูกข่ายตามมาตรฐานขององค์กร เช่น ดำเนินการ Full Scan บนคอมพิวเตอร์ลูกข่าย, ตรวจสอบ Alerts/Logs บน Antimalware และ Endpoint Detection and Response (EDR), ตรวจสอบ Malicious event บนคอมพิวเตอร์ลูกข่ายและ Network Traffic ที่ต้องสงสัย เป็นต้น หรือผ่านกระบวนการทำลายข้อมูล (Format) และติดตั้งโปรแกรมตาม “คู่มือการตั้งค่าพื้นฐานสำหรับคอมพิวเตอร์ลูกข่ายระบบ BAHTNET Lite (BAHTNET Lite Client)” ก่อนนำกลับมาใช้งานเป็นเครื่องคอมพิวเตอร์ลูกข่ายระบบ BAHTNET Lite

(15) กรณีที่มีความจำเป็นต้องนำคอมพิวเตอร์ลูกข่ายที่ใช้เชื่อมโยงกับระบบบาทเน็ต หรือนำคอมพิวเตอร์อื่น ๆ ภายในองค์กร มาใช้งานเป็นคอมพิวเตอร์ลูกข่ายระบบ BAHTNET Lite ผู้ให้บริการบาทเน็ตต้องนำคอมพิวเตอร์ดังกล่าวผ่านกระบวนการทำลายข้อมูล (Format) และติดตั้งโปรแกรมตาม “คู่มือการตั้งค่าพื้นฐานสำหรับคอมพิวเตอร์ลูกข่ายระบบ BAHTNET Lite (BAHTNET Lite Client)” ก่อนนำมาใช้เป็นเครื่องคอมพิวเตอร์ลูกข่ายระบบ BAHTNET Lite

ทั้งนี้ เพื่อลดเวลาของกระบวนการตามวรรคหนึ่ง ผู้ให้บริการบาทเน็ตควรกำหนดกระบวนการและเครื่องมือ รวมทั้งจัดทำคู่มือปฏิบัติงาน เช่น จัดทำเอกสารขั้นตอนในการทำลายข้อมูล (Format) และติดตั้งโปรแกรม หรือจัดทำ Image สำหรับคอมพิวเตอร์ลูกข่ายระบบ BAHTNET Lite เป็นต้น

(16) ผู้ให้บริการบาทเน็ตต้องดำเนินการให้มีคอมพิวเตอร์ลูกข่ายระบบ BAHTNET Lite ที่พร้อมใช้งานอย่างน้อย 1 เครื่อง ภายใน 1 ชั่วโมง นับจากที่ได้รับแจ้งจาก ธปท. (รายละเอียดตามภาคผนวก 1 ท้ายแนວปฏิบัติฉบับนี้)

4. วันเริ่มต้นบังคับใช้

แนวปฏิบัติฉบับนี้ให้ใช้บังคับตั้งแต่วันที่ สิงหาคม 2566 เป็นต้นไป

แนวทางการจัดเตรียมเครื่องคอมพิวเตอร์ลูกข่ายระบบ BAHTNET Lite

ให้ผู้ใช้บริการบาทเน็ตจัดเตรียมเครื่อง BAHTNET Lite Client โดยสามารถเลือกดำเนินการได้ 4 วิธี ดังรายละเอียดและภาพประกอบด้านล่าง

วิธีที่ 1 ใช้เครื่อง BAHTNET Client: ให้นำเครื่องดังกล่าวผ่านกระบวนการ Format และติดตั้งโปรแกรมที่จำเป็นสำหรับการใช้งาน BAHTNET Lite

วิธีที่ 2 ใช้เครื่อง EFS Client: สามารถดำเนินการได้ 2 แนวทาง ดังนี้

2.1 นำเครื่องดังกล่าวผ่านกระบวนการตรวจสอบความมั่นคงปลอดภัยขององค์กร (เช่น Full Scan บนคอมพิวเตอร์ลูกข่าย, ตรวจสอบ Alerts/Logs บน Antimalware และ Endpoint Detection and Response (EDR), ตรวจสอบ Malicious event บนคอมพิวเตอร์ลูกข่าย และ Network Traffic ที่ต้องสงสัย เป็นต้น) ทั้งนี้ หากตรวจสอบแล้วพบว่าเครื่องดังกล่าวไม่ปลอดภัยตามมาตรฐานขององค์กร ให้ดำเนินการตามแนวทางข้อ 2.2

2.2 นำเครื่องดังกล่าวผ่านกระบวนการ Format และติดตั้งโปรแกรมที่จำเป็นสำหรับการใช้งาน BAHTNET Lite

วิธีที่ 3 ใช้เครื่อง PC/Notebook ใด ๆ: ให้นำเครื่องดังกล่าวผ่านกระบวนการ Format และติดตั้งโปรแกรมที่จำเป็นสำหรับการใช้งาน BAHTNET Lite

วิธีที่ 4 ใช้เครื่อง BAHTNET Lite Client ที่จัดเตรียมไว้เป็นการเฉพาะ: สามารถนำเครื่องดังกล่าวไม่ว่าจะเป็นเครื่อง Production หรือเครื่อง Backup มาใช้งานได้ทันทีเมื่อ กระทบ. ประกาศใช้ BNO

อย่างไรก็ตาม หากมีความจำเป็นต้องนำ BAHTNET Lite Client ไปใช้เพื่อวัตถุประสงค์อื่น ต้องดำเนินการดังนี้

- กรณีนำไปใช้กับบริการ EFS: ก่อนนำกลับมาใช้เป็น BAHTNET Lite Client ให้ดำเนินการเช่นเดียวกับการนำเครื่อง EFS Client มาใช้เป็นเครื่อง BAHTNET Lite Client ตามที่กล่าวในวิธีที่ 2

- กรณีนำไปใช้เพื่อการทดสอบ BAHTNET Lite (IWT): ก่อนนำกลับมาใช้เป็น BAHTNET Lite Client ให้นำเครื่องดังกล่าวผ่านกระบวนการ Format และติดตั้งโปรแกรมที่จำเป็นสำหรับการใช้งาน BAHTNET Lite

แนวทางการจัดเตรียมเครื่องคอมพิวเตอร์ลูกข่ายระบบ BAHTNET Lite

การเชื่อมต่อกับ BN Lite Production	วิธีที่ 1 BAHTNET Client	วิธีที่ 2 EFS Client	วิธีที่ 3 Any PC / Notebook	วิธีที่ 4 BAHTNET Lite Client
1. เชื่อมต่อได้ทันที	✗	✗	✗	✓
2. ต้องผ่านกระบวนการตรวจสอบความมั่นคงปลอดภัยขององค์กร*	✗	✓ หรือ	✗	✓ กรณีนำไปใช้เป็น EFS Client
3. ต้อง Format & Setup for BN Lite	✓	✓	✓	✓ กรณีนำไปใช้ทดสอบ BN Lite (IWT)

ประเด็นคำถาม – คำตอบ
แนวทางการจัดเตรียมเครื่องคอมพิวเตอร์ลูกข่ายระบบ BAHTNET Lite

ข้อ	ประเด็นคำถาม	คำตอบ
1	ผู้ใช้บริการบาทเน็ตสามารถนำเครื่อง BAHTNET Client หรือเครื่อง PC/Notebook ใด ๆ ที่ผ่านกระบวนการตรวจสอบความมั่นคงปลอดภัยขององค์กร มาใช้เป็นเครื่อง BAHTNET Lite Client ได้หรือไม่	ไม่ได้ เนื่องจากเครื่องดังกล่าวมีความเสี่ยงค่อนข้างสูง จึงกำหนดให้ต้องผ่านกระบวนการ Format และติดตั้งโปรแกรมที่จำเป็นสำหรับการใช้งาน BAHTNET Lite เท่านั้น
2	เครื่อง BAHTNET Lite Client ชุด Production และชุดทดสอบ IWT สามารถนำมาใช้ร่วมกันได้หรือไม่ อย่างไร	สามารถทำได้ โดยก่อนนำไปใช้เป็นชุด Production จะต้องผ่านกระบวนการ Format และติดตั้งโปรแกรมที่จำเป็นสำหรับการใช้งาน BAHTNET Lite <i>หมายเหตุ: สำหรับการทดสอบแผนฉุกเฉิน BAHTNET Lite ประจำปีของ ธปท. ในอนาคต จะกำหนดให้ผู้ใช้บริการบาทเน็ตใช้ BAHTNET Lite Client ชุด Production ทดสอบร่วมกับระบบงาน BAHTNET Lite ชุด Production ของ ธปท.</i>
3	ผู้ใช้บริการบาทเน็ตสามารถเลือกแนวทางในการจัดเตรียมเครื่อง BAHTNET Lite Client มากกว่า 1 แนวทางได้หรือไม่	สามารถเลือกได้มากกว่า 1 แนวทาง ตามความเหมาะสมของแต่ละสถาบัน
4	ผู้ใช้บริการบาทเน็ตจำเป็นต้องเตรียมเครื่อง BAHTNET Lite Client ชุด Backup ด้วยหรือไม่	ควรจัดเตรียมชุด Backup เพื่อสำรองไว้ใช้ในกรณีฉุกเฉินที่เครื่อง Production ชัดข้อง
5	ธปท. จะพิจารณาเพิ่มเวลาให้กับผู้ใช้บริการบาทเน็ตในการจัดเตรียมเครื่อง BAHTNET Lite Client นับจากที่ได้รับแจ้งจาก ธปท. ให้มากกว่า 1 ชั่วโมง ได้หรือไม่	ธปท. มีความจำเป็นต้องคงกำหนดเวลาดังกล่าว เพื่อให้ผู้ใช้บริการบาทเน็ตมีเวลาในการปฏิบัติงานตามกระบวนการ BNO ได้อย่างเพียงพอ ทั้งนี้ ผู้ใช้บริการบาทเน็ตอาจใช้วิธีจัดเตรียม BAHTNET Lite Client ไว้เพียง 1 เครื่อง เพื่อใช้ในกระบวนการ Reconcile ได้โดยเร็ว หลังจากนั้นจึงทยอยจัดเตรียมเครื่องด้วยวิธีการอื่นจนครบจำนวนตามความจำเป็นในการใช้งานต่อไป

ฝ่ายการชำระเงินและพันธบัตร

โทรศัพท์: 0-2283-6667 และ 0-2283-6539

ระเบียบ ประกาศ และข้อกำหนดที่เกี่ยวข้อง

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

1. ระเบียบธนาคารแห่งประเทศไทยว่าด้วยการบริการบาทเนต
2. ประกาศ ธปท.ที่ สรข. 4/2560 เรื่อง มาตรฐานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของคอมพิวเตอร์ลูกข่ายระบบบาทเนต
3. แนวปฏิบัติเรื่อง การรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ลูกข่ายของผู้ใช้บริการบาทเนตตามหนังสือเวียน ผชพ. (ว.) 3/2564 ลงวันที่ 1 กุมภาพันธ์ 2564