ธนาคารแห่งประเทศไทย

21 ตุลาคม 2564

เรียน ผู้จัดการ

สถาบันผู้ใช้บริการบาทเนต
ธนาคารสมาชิกในระบบการหักบัญชีเช็คด้วยภาพเช็คและระบบการจัดเก็บภาพเช็ค (ICAS)

ที่ ฝชพ.(ว.) 161 /2564 เรื่อง นำส่งแนวปฏิบัติ เรื่อง การใช้เครื่องคอมพิวเตอร์ลูกข่ายระบบ BAHTNET และระบบ ICAS ในการปฏิบัติงานนอกสถานที่ทำการ ภายใต้สถานการณ์ฉุกเฉินการระบาดของไวรัสโคโรนา 2019 (COVID-19)

ด้วยสถานการณ์การระบาดของไวรัสโคโรนา 2019 (COVID-19) ส่งผลกระทบต่อการปฏิบัติงานของผู้ใช้บริการบาทเนต (BAHTNET) และธนาคารสมาชิกระบบ ICAS เพื่อให้บริการด้านการชำระเงินแก่ภาคธุรกิจและประชาชนสามารถดำเนินการได้อย่างต่อเนื่อง รวมทั้งให้ความสำคัญในการดูแลความปลอดภัยของพนักงานของสถาบันผู้ใช้บริการและธนาคารสมาชิก

ธนาคารแห่งประเทศไทย (ธปท.) ได้หารือร่วมกับผู้แทนจากสมาคมธนาคารไทย สมาคมธนาคารนานาชาติ และสมาคมธนาคารเฉพาะกิจ และกำหนดแนวปฏิบัติ เรื่อง การใช้เครื่องคอมพิวเตอร์ลูกข่ายระบบ BAHTNET และระบบ ICAS ในการปฏิบัติงานนอกสถานที่ทำการ ภายใต้สถานการณ์ฉุกเฉินการระบาดของ COVID-19 เพื่อเป็นแนวทางเบื้องต้นในการกำหนดมาตรการรักษาความมั่นคงปลอดภัยและให้มีการบริหารจัดการความเสี่ยงที่อาจเกิดขึ้นจากการปฏิบัติงานนอกสถานที่ทำการ โดยผู้ใช้บริการ BAHTNET และธนาคารสมาชิกระบบ ICAS สามารถกำหนดมาตรการรักษาความมั่นคงปลอดภัยที่แตกต่างสูงขึ้นจากแนวปฏิบัติฉบับนี้ได้

จึงเรียนมาเพื่อโปรดทราบและถือปฏิบัติ จนกว่าสถานการณ์จะกลับเข้าสู่ภาวะปกติ และ ธปท. จะแจ้งยกเลิกต่อไป

ขอแสดงความนับถือ

(นายบัญชา มนูญกุลชัย)
ผู้อำนวยการอาวุโส ฝ่ายการชำระเงินและพันธบัตร
ผู้ว่าการแทน

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

ฝ่ายการชำระเงินและพันธบัตร
โทรศัพท์ 0 2283 5045, 0 2283 6150

แนวปฏิบัติ

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

ตุลาคม 2564

ธนาคารแห่งประเทศไทย

จัดทำโดย

ฝ่ายการชำระเงินและพันธบัตร

สายระบบข้อสนเทศ

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 ประกอบกับนโยบายภาครัฐที่สนับสนุนให้มีการทำงานจากที่บ้านในช่วงการระบาด สถานการณ์ดังกล่าวอาจส่งผลกระทบต่อการปฏิบัติงานของผู้ใช้บริการ BAHTNET และธนาคารสมาชิกในระบบการหักบัญชีเช็คด้วยภาพเช็คและระบบการจัดเก็บภาพเช็ค (ธนาคารสมาชิกระบบ ICAS) ซึ่งยังคงให้บริการด้านการชำระเงินแก่ภาคธุรกิจและประชาชนอย่างต่อเนื่อง รวมทั้งให้ความสำคัญในการดูแลความปลอดภัยในชีวิตและสุขภาพของพนักงานของสถาบันผู้ใช้บริการและธนาคารสมาชิก

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

แนวปฏิบัตินี้ เป็นแนวทางเบื้องต้นในการกำหนดมาตรการรักษาความมั่นคงปลอดภัยในการปฏิบัติงานนอกสถานที่ทำการขั้นต่ำ โดยผู้ใช้บริการ BAHTNET และธนาคารสมาชิกระบบ ICAS สามารถกำหนดมาตรการรักษาความมั่นคงปลอดภัยที่แตกต่างสูงขึ้นจากแนวปฏิบัติฉบับนี้ได้ ทั้งนี้ มาตรการดังกล่าวควรมีความสอดคล้องและสามารถป้องกันความเสี่ยงของคอมพิวเตอร์ลูกข่ายได้อย่างมีประสิทธิภาพและเป็นไปตามมาตรฐานที่ยอมรับได้ รวมทั้งสอดคล้องกับแนวปฏิบัติที่ดี (best practice) ในการเตรียมความพร้อมด้านเทคโนโลยีสารสนเทศภายใต้สถานการณ์การระบาดของ COVID-19 นอกจากนี้ ผู้ใช้บริการ BAHTNET ต้องดำเนินการให้มีการรักษาความมั่นคงปลอดภัยในองค์กรตามข้อกำหนดในระเบียบ ธปท. ว่าด้วยการบริการบาทเนต ตามประกาศ ธปท. เรื่อง มาตรฐานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของคอมพิวเตอร์ลูกข่ายระบบบาทเนต รวมทั้งแนวปฏิบัติการรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ลูกข่ายของผู้ใช้บริการบาทเนต ฉบับปรับปรุง และธนาคารสมาชิกระบบ ICAS ต้องดำเนินการให้มีการรักษาความมั่นคงปลอดภัยในองค์กรตามข้อกำหนดในระเบียบ ธปท. ว่าด้วยระบบการหักบัญชีเช็คด้วยภาพเช็คและระบบการจัดเก็บภาพเช็ค และประกาศ ธปท. เรื่อง มาตรฐานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของคอมพิวเตอร์ลูกข่ายการหักบัญชีเช็คด้วยภาพเช็คและระบบการจัดเก็บภาพเช็ค (รายละเอียดตามภาคผนวกท้ายแนวปฏิบัติ)

2. ขอบเขตการบังคับใช้

แนวปฏิบัตินี้เป็นกรอบแนวทางให้ผู้ใช้บริการ 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 ผู้ใช้บริการบาทเนตตามระเบียบธนาคารแห่งประเทศไทยว่าด้วยการบริการบาทเนต (BAHTNET) และธนาคารสมาชิกตามระเบียบธนาคารแห่งประเทศไทยว่าด้วยระบบการหักบัญชีเช็คด้วยภาพเช็คและระบบการจัดเก็บภาพเช็ค (ICAS)

“คอมพิวเตอร์ลูกข่าย” หมายถึง ระบบคอมพิวเตอร์ของผู้ใช้บริการบาทเนตและธนาคารสมาชิกที่ใช้เชื่อมโยงกับระบบงานของ 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 งานด้านเทคโนโลยีสารสนเทศที่ครอบคลุมถึงเครื่องคอมพิวเตอร์และอุปกรณ์รอบข้าง (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)

3.2 รายละเอียดของแนวปฏิบัติ

ก่อนที่สมาชิกจะปฏิบัติงานนอกสถานที่ทำการ สมาชิกต้องดำเนินการตามระเบียบ ประกาศ และแนวปฏิบัติที่เกี่ยวข้องตามที่กำหนดไว้ในภาคผนวก และต้องดำเนินการ ดังนี้

3.2.1 การกำหนดมาตรการในการกำกับดูแลกิจการ (Governance policy)

สมาชิกต้องจัดให้มีนโยบายและมาตรการในการกำกับดูแลกิจการและการบริหารความเสี่ยงที่อาจเกิดขึ้นจากการปฏิบัติงานนอกสถานที่ทำการ โดยได้รับอนุมัติจากคณะกรรมการบริหารความเสี่ยงขององค์กร (Risk committee) รวมทั้งมีการติดตามและตรวจสอบการปฏิบัติงานให้เป็นไปตามหลักเกณฑ์ที่กำหนดและตามที่ได้รับอนุมัติ ทั้งนี้ มาตรการดังกล่าวอย่างน้อยต้องครอบคลุมถึงกรณีดังต่อไปนี้

(1) การจัดให้มีการประเมินความเสี่ยงและกำหนดมาตรการควบคุมความเสี่ยงจากการปฏิบัติงานนอกสถานที่ทำการในทุกมิติ อาทิ ความเสี่ยงจากภัยคุกคามทางไซเบอร์ ความเสี่ยงจากการมีผู้ปฏิบัติงานติดเชื้อ COVID-19 ในจำนวนที่มีนัยสำคัญต่อการปฏิบัติงาน ความเสี่ยงจากข้อมูลสำคัญรั่วไหลไปยังผู้ไม่มีหน้าที่ที่เกี่ยวข้องทั้งภายในและภายนอกองค์กร (Data Leak) ไม่ว่าโดยเจตนาของผู้ปฏิบัติงานหรือจากเหตุอื่น เช่น ผู้ปฏิบัติงานกระทำการโดยประมาททำให้อุปกรณ์สูญหาย เป็นต้น

(2) ขอบเขตการได้รับอนุมัติจากคณะกรรมการบริหารความเสี่ยงขององค์กร (Risk committee) ต้องมีการกำหนดรายละเอียดขอบเขตงานที่สามารถปฏิบัติงานนอกสถานที่ทำการ การประเมินความเสี่ยง และมาตรการควบคุมความเสี่ยง รวมทั้งจัดให้มีการติดตามและตรวจสอบการปฏิบัติตามหลักเกณฑ์ (Compliance) อย่างเหมาะสม โดยกำหนดให้มีการตรวจสอบการปฏิบัติงานและการรายงานผลการตรวจสอบเสนอผู้บริหารขององค์กรเพื่อให้มั่นใจว่าผู้ปฏิบัติงานสามารถปฏิบัติได้ตามแนวทางที่ได้รับอนุมัติจาก Risk committee แล้ว

(3) จัดให้มี Code of conducts สำหรับผู้ปฏิบัติงานนอกสถานที่ทำการ โดยให้ผู้ปฏิบัติงานลงนามยินยอมและถือปฏิบัติอย่างเคร่งครัด

3.2.2 การควบคุมการเข้าใช้คอมพิวเตอร์ลูกข่าย

สมาชิกต้องจัดให้มีมาตรการควบคุมการเข้าใช้งานคอมพิวเตอร์ลูกข่ายที่ตั้งอยู่นอกสถานที่ทำการ เพื่อป้องกันการลักลอบนำบัญชีของผู้ปฏิบัติงานไปทำธุรกรรม โดยผู้ที่ไม่มีสิทธิทั้งภายในและภายนอกองค์กร ทั้งนี้ มาตรการดังกล่าวอย่างน้อยต้องครอบคลุมถึงกรณีดังต่อไปนี้

(1) การจัดให้มีอุปกรณ์และเครือข่ายที่มั่นคงปลอดภัย โดยเฉพาะอุปกรณ์และเครือข่ายที่เชื่อมต่อไปยังคอมพิวเตอร์ลูกข่าย เพื่อควบคุมความเสี่ยงการเข้าถึงคอมพิวเตอร์ลูกข่ายและจากภัยคุกคามทางไซเบอร์ใหม่ ๆ ที่เกิดขึ้น เช่น ใช้อุปกรณ์และเครือข่ายที่ได้รับอนุญาตจากองค์กร เพิ่มการเฝ้าระวังภัยคุกคามทางไซเบอร์ บันทึกและติดตาม Log การเข้าใช้งานระบบงานสำคัญอย่างใกล้ชิด เป็นต้น

(2) กำหนดพื้นที่ในการปฏิบัติงานนอกสถานที่ทำการให้เป็นสัดส่วนและปลอดภัย เพื่อป้องกันไม่ให้ข้อมูลสำคัญรั่วไหลไปยังผู้ไม่มีหน้าที่เกี่ยวข้องทั้งภายในและภายนอกองค์กร รวมทั้งกำหนดสิทธิและหน้าที่การใช้งานระบบงานและการเข้าถึงข้อมูลในระบบ BAHTNET และระบบ ICAS ตามอำนาจหน้าที่ของผู้ปฏิบัติงาน และทำการทบทวนการกำหนดสิทธิและหน้าที่ดังกล่าวอย่างสม่ำเสมอโดยอย่างน้อยควรทบทวนทุก 30 วัน

3.2.3 การควบคุมด้านการปฏิบัติงาน

สมาชิกต้องกำหนดมาตรการด้านการรักษาความมั่นคงปลอดภัย เพื่อกำหนดแนวทางการติดตาม และการเตรียมความพร้อมสำหรับเหตุที่กระทบต่อความมั่นคงปลอดภัยคอมพิวเตอร์ลูกข่ายหรืออาจเกิดความเสียหายต่อระบบ BAHTNET หรือระบบ ICAS ทั้งนี้ มาตรการดังกล่าวอย่างน้อยต้องครอบคลุมถึงกรณีดังต่อไปนี้

(1) การจัดให้มีเครื่องมือหรือกระบวนการในการติดตาม ตรวจสอบ และตรวจจับธุรกรรมผิดปกติ ธุรกรรมต้องสงสัย รวมทั้งเฝ้าระวังภัยคุกคามทางไซเบอร์อย่างใกล้ชิด เช่น เพิ่มการตรวจสอบในกิจกรรมสำคัญ เพิ่มความถี่ในการติดตามและรายงานต่อผู้บริหาร เป็นต้น

(2) การจัดทำแผนฉุกเฉินสำหรับการรับมือและตอบสนองต่อเหตุการณ์ผิดปกติให้ครอบคลุมการปฏิบัติงานนอกสถานที่ทำการเพื่อตอบสนองต่อเหตุการณ์ความเสี่ยงสำคัญ เช่น ความเสี่ยงจากการทุจริตและประพฤติมิชอบ ข้อมูลสำคัญรั่วไหลไปยังผู้ไม่มีหน้าที่เกี่ยวข้องทั้งภายในและภายนอกองค์กร และการคุกคามทางไซเบอร์ รวมทั้งกรณีระบบงานขัดข้อง หรือไม่สามารถเชื่อมต่อคอมพิวเตอร์ลูกข่ายจากนอกที่สถานที่ทำการได้ โดยจัดให้มีระบบช่วยควบคุมการปฏิบัติงานโดยสามารถตรวจสอบข้อมูลย้อนหลังได้ [1] และกำหนดขั้นตอนการแก้ไขปัญหา ทีมงานหรือผู้รับผิดชอบ รวมถึงวิธีการรายงานปัญหาให้กับผู้บริหารและผู้เกี่ยวข้องทราบอย่างรวดเร็วที่สุดเท่าที่จะทำได้ เพื่อแก้ไขปัญหาให้กลับคืนสู่สภาวะปกติโดยเร็ว

3.2.4 การรักษาความปลอดภัยระบบคอมพิวเตอร์สำหรับผู้ใช้บริการบาทเนตผ่าน SWIFT

กรณีผู้ใช้บริการบาทเนต ซึ่งส่งข้อความผ่าน SWIFT ต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยตามที่ SWIFT กำหนด โดยเฉพาะ SWIFT Customer Security Program (SWIFT CSP)

4. วันเริ่มต้นบังคับใช้

แนวปฏิบัติฉบับนี้ให้ใช้บังคับตั้งแต่วันที่ **21 ตุลาคม 2564 เป็นต้นไป จนกว่า ธปท. แจ้งยกเลิก**

---

1 ตัวอย่างระบบช่วยควบคุมการปฏิบัติงาน เช่น VDI recording เพื่อบันทึกการทำงานตลอดเวลาปฏิบัติงานในเครื่อง VDI ของระบบงานสำคัญโดยต้องสามารถตรวจสอบย้อนหลังได้ หรือ Security Logging เพื่อบันทึก session การเข้าใช้และเลิกใช้งานฟังก์ชันในระบบงานสำคัญ ซึ่งสามารถตรวจจับการใช้งานในเวลาที่ผิดปกติได้ เป็นต้น

ระเบียบประกาศ และข้อกำหนดที่เกี่ยวข้อง

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

1. แนวปฏิบัติที่ดี (best practice) ในการเตรียมความพร้อมด้านเทคโนโลยีสารสนเทศภายใต้สถานการณ์การระบาดของ COVID 19 ออกโดยฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ

2. ระบบ BAHTNET

- ระเบียบธนาคารแห่งประเทศไทยว่าด้วยการบริการบาทเนต
- ประกาศ ธปท.ที่ สรข. 4/2560 เรื่อง มาตรฐานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของคอมพิวเตอร์ลูกข่ายระบบบาทเนต
- แนวปฏิบัติเรื่อง การรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ลูกข่ายของผู้ใช้บริการบาทเนต ตามหนังสือเวียน ฝชพ. (ว.) 3/2564 ลงวันที่ 1 กุมภาพันธ์ 2564

3. ระบบ ICAS

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