แนวปฏิบัติ

เรื่อง การรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ลูกข่าย BAHTNET API

ธนาคารแห่งประเทศไทย

จัดทำโดย
ฝ่ายเทคโนโลยีสารสนเทศ
สายระบบข้อสนเทศ
ธนาคารแห่งประเทศไทย

สารบัญ

หัวข้อ **หน้า**

แนวปฏิบัติธนาคารแห่งประเทศไทย

เรื่อง การรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ลูกข่าย BAHTNET API

---

1. เหตุผลในการออกแนวปฏิบัติ

ธนาคารแห่งประเทศไทย (ธปท.) ได้ดำเนินการแผนงานระบบ BAHTNET Application Programming Interface (BAHTNET API) ภายใต้โครงการ BAHTNET NextGen เพื่อปรับระบบบาทเนตให้รองรับกับความก้าวหน้าทางเทคโนโลยีที่เปลี่ยนแปลงไป โดยพัฒนา Domestic Network ที่ใช้เทคโนโลยี Application Programming Interface ซึ่งสามารถสนับสนุนให้เกิดนวัตกรรมและการต่อยอดบริการด้านการชำระเงิน รองรับการจัดการความเสี่ยง Geopolitical Risk และเป็นรากฐานของการพัฒนา New Core Infrastructure ของระบบบาทเนต (BAHTNET Modernization) ในอนาคต

ในการนี้ ธปท. จึงได้ออกแนวปฏิบัติฉบับนี้ เพื่อกำหนดแนวทางการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ของผู้ใช้บริการบาทเนต เพื่อการใช้งาน BAHTNET API ให้มีแนวปฏิบัติที่ครอบคลุมและเป็นมาตรฐานเดียวกัน รวมถึงสอดคล้องกับการเปลี่ยนแปลงทางเทคโนโลยีในปัจจุบัน และเสริมสร้างมาตรฐานการรักษาความมั่นคงปลอดภัยในเรื่องการควบคุมระบบคอมพิวเตอร์ เพื่อใช้เป็นกรอบแนวทางให้ผู้ใช้บริการบาทเนตนำไปปรับใช้ให้เหมาะสม และบริหารความเสี่ยงที่เกี่ยวข้องกับการทำธุรกรรมได้อย่างมีประสิทธิภาพมากยิ่งขึ้น

ทั้งนี้ ผู้ใช้บริการบาทเนตสามารถกำหนดมาตรการรักษาความมั่นคงปลอดภัย ที่แตกต่างจากแนวปฏิบัติฉบับนี้ได้ หากมาตรการดังกล่าวมีความสอดคล้องและสามารถป้องกันความเสี่ยงของระบบคอมพิวเตอร์ได้อย่างมีประสิทธิภาพและเป็นไปตามมาตรฐานที่ยอมรับได้ นอกจากนี้ ผู้ใช้บริการบาทเนตต้องดำเนินการให้มีการรักษาความมั่นคงปลอดภัยในองค์กรตามข้อกำหนดในกฎหมาย ระเบียบ และประกาศที่เกี่ยวข้อง (ภาคผนวก 1) และให้มีการรายงานเหตุการณ์ความเสี่ยงตามที่กำหนด (ภาคผนวก 2) เพื่อให้มั่นใจว่ากระบวนการทำงานและ ธุรกรรมมีการรักษาความมั่นคงปลอดภัยที่ดี สอดคล้องกับข้อกำหนดตามกฎหมายในปัจจุบัน และเป็นไปตาม มาตรฐานสากล รวมทั้งที่มีการปรับปรุงเพิ่มเติมหรือที่มีข้อกำหนดเพิ่มขึ้นในอนาคต

2. ขอบเขตการบังคับใช้

แนวปฏิบัตินี้เป็นกรอบแนวทางให้ผู้ใช้บริการบาทเนตใช้กำหนดมาตรการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ของผู้ใช้บริการบาทเนต เครือข่าย อุปกรณ์เครือข่ายที่เชื่อมโยงกับ BAHTNET API ของ ธปท. และอุปกรณ์ Hardware Security Module (HSM) ของผู้ใช้บริการบาทเนต รวมถึงการควบคุมด้านการปฏิบัติงานและการจัดการด้านบุคลากรและการสื่อสารที่เกี่ยวข้อง

ทั้งนี้ ผู้ใช้บริการบาทเนตต้องดำเนินการให้มีการตรวจรับรองระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC 27001 อย่างต่อเนื่อง โดยครอบคลุมระบบและอุปกรณ์ดังกล่าวข้างต้น

3. เนื้อหา

3.1 ความหมาย ในแนวปฏิบัติฉบับนี้

“แนวปฏิบัติ” หมายถึง แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ลูกข่าย BAHTNET API ของผู้ใช้บริการบาทเนต

“คอมพิวเตอร์ลูกข่าย BAHTNET API” หมายถึง ระบบคอมพิวเตอร์ของผู้ใช้บริการบาทเนต ที่ใช้เชื่อมโยงกับ BAHTNET API ของ ธปท. แบบ Host to Host ผ่านเครือข่ายเฉพาะที่ ธปท. กำหนด

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

“ศูนย์คอมพิวเตอร์ของผู้ใช้บริการบาทเนต” หมายถึง ศูนย์คอมพิวเตอร์ที่ใช้ในการจัดเก็บคอมพิวเตอร์ลูกข่าย BAHTNET API ของผู้ใช้บริการบาทเนต โดยมีสถานที่ตั้งภายในองค์กร (On-Premises) หรือสถานที่ของผู้ให้บริการภายนอก (Off-Premises)

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

“เหตุการณ์ละเมิดต่อความมั่นคงปลอดภัย” หมายถึง เหตุการณ์ หรือการกระทำที่มีเจตนาทำให้มีความเสี่ยง หรือก่อให้เกิดผลกระทบต่อความมั่นคงปลอดภัยของคอมพิวเตอร์ลูกข่าย BAHTNET API และอุปกรณ์ Hardware Security Module (HSM) รวมถึงการฉ้อโกง อันนำไปสู่ความเสียหายทางการเงิน ความเสียหายต่อชื่อเสียง และการขาดความเชื่อมั่นของผู้ใช้บริการบาทเนตต่อการให้บริการทางการเงินโดยรวม

3.2 รายละเอียดของแนวปฏิบัติ

3.2.1 การควบคุมคอมพิวเตอร์ลูกข่าย เครือข่าย และอุปกรณ์เครือข่ายที่เชื่อมโยงกับ BAHTNET API ของ ธปท.

ผู้ใช้บริการบาทเนตต้องกำหนดมาตรการรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ลูกข่าย BAHTNET API เครือข่าย และอุปกรณ์เครือข่ายที่เชื่อมโยงกับ BAHTNET API ของ ธปท. ทั้งนี้ มาตรการดังกล่าวควรครอบคลุมถึง

(1) ควบคุมการเข้าถึงศูนย์คอมพิวเตอร์ของผู้ใช้บริการบาทเนต รวมถึงอุปกรณ์เครือข่ายที่เชื่อมโยงกับ BAHTNET API ของ ธปท.

(2) กำหนดวิธีการและสิทธิการเข้าถึงคอมพิวเตอร์ลูกข่าย BAHTNET API โดยจัดให้มีการแบ่งอำนาจหน้าที่ของพนักงานอย่างเหมาะสมเพื่อป้องกันมิให้พนักงานผู้ใดได้รับสิทธิอย่างเบ็ดเสร็จ และมีกระบวนการจัดการ User ที่มีสิทธิสูง (Privilege Account Management) รวมถึงทบทวนสิทธิดังกล่าวโดยสม่ำเสมอ

(3) จัดให้มีการรักษาความมั่นคงปลอดภัยของเครือข่ายที่เชื่อมโยงระหว่างคอมพิวเตอร์ลูกข่าย BAHTNET API กับ BAHTNET API ของ ธปท. เช่น การติดตั้ง Firewall เป็นต้น

(4) ควบคุมการเข้าถึงคอมพิวเตอร์ลูกข่าย BAHTNET API จากระบบงานอื่นที่ไม่จำเป็นต้องเชื่อมโยง เช่น แยกเครือข่ายคอมพิวเตอร์ลูกข่าย BAHTNET API ออกจากเครือข่ายสำหรับระบบงานภายในองค์กร เป็นต้น

(5) ไม่ใช้งานคอมพิวเตอร์ลูกข่าย BAHTNET API ร่วมกับระบบงานอื่น ยกเว้นอาจใช้ร่วมกับบริการด้านการเงินด้วยวิธีอิเล็กทรอนิกส์ของ ธปท.

หากมีระบบงานอื่นในระดับ Logical เช่น Virtual Machine ที่ต้องการใช้งานบนเครื่อง Physical Server เดียวกัน ระบบงานดังกล่าวจะต้องมีการรักษาความปลอดภัยเทียบเท่ากับคอมพิวเตอร์ลูกข่าย BAHTNET API

กรณีคอมพิวเตอร์ลูกข่าย BAHTNET API ติดตั้งที่ศูนย์คอมพิวเตอร์ที่ใช้งานร่วมกับผู้ใช้บริการรายอื่น ต้องมีการแยกการใช้งานออกจากผู้ใช้บริการรายอื่นอย่างชัดเจน ทั้งในระดับเครือข่ายและระดับ Logical เป็นอย่างน้อย เช่น การแยก VLAN และการแยก Virtual Machine

(6) อนุญาตให้เชื่อมต่อบริการหรือระบบงานอื่นที่อยู่ภายในศูนย์คอมพิวเตอร์ของผู้ใช้บริการบาทเนตที่จำเป็นสำหรับการปฏิบัติงาน และการรักษาความมั่นคงปลอดภัยเท่านั้น เช่น ระบบ Infrastructure พื้นฐาน เป็นต้น

(7) อนุญาตให้เชื่อมต่อบริการหรือระบบงานที่อยู่ภายนอกศูนย์คอมพิวเตอร์ของผู้ใช้บริการบาทเนต เฉพาะ Certificate Authority และ Endpoint Protection

(8) มีกลไกป้องกันและตรวจจับการบุกรุกของโปรแกรมประสงค์ร้าย (Endpoint Protection) โดย Update Signature จากผู้ผลิตอย่างสม่ำเสมอ และมีการทำ Scheduled Scan ตามระยะเวลาที่เหมาะสม

สำหรับคอมพิวเตอร์ลูกข่าย BAHTNET API ที่ไม่สามารถติดตั้งโปรแกรมป้องกันและตรวจจับการบุกรุกของโปรแกรมประสงค์ร้าย (Endpoint Protection) ควรประเมินความเสี่ยงและมีมาตรการควบคุมทดแทน

(9) จัดให้มีการประเมินช่องโหว่ (Vulnerability Assessment) และติดตั้งโปรแกรมเพื่อปิดช่องโหว่ (Windows Security Patch) ตามกรอบเวลาการติดตั้ง Patch ขององค์กร อย่างน้อยปีละ 1 ครั้ง

(10) จัดให้มีการทดสอบเจาะระบบ (Penetration Test) โดยผู้เชี่ยวชาญภายในหรือภายนอกที่มีความเป็นอิสระ ครอบคลุมระบบงานและระบบเครือข่ายอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

(11) มีการบริหารจัดการการตั้งค่าระบบ (System Configuration Management) โดยจัดให้มีการตั้งค่าการรักษาความมั่นคงปลอดภัย (Security Hardening) เป็นไปตามมาตรฐานการรักษาความมั่นคงปลอดภัยขั้นต่ำ (Minimum Security Baseline) ขององค์กร รวมทั้งดำเนินการสอบทานการตั้งค่าอย่างสม่ำเสมอตามที่ได้กำหนดไว้

(12) มีการรักษาความมั่นคงปลอดภัยของระบบงาน (Application Security) เป็นไปตามมาตรฐานและแนวปฏิบัติขององค์กรหรือที่ได้รับการยอมรับในระดับสากล เช่น OWASP เป็นต้น

(13) กำหนดวิธีการควบคุมการแก้ไขเปลี่ยนแปลง (Change Management) ของคอมพิวเตอร์ลูกข่าย BAHTNET API เครือข่าย และอุปกรณ์เครือข่ายที่เชื่อมโยงกับ BAHTNET API ของ ธปท.

(14) มีคอมพิวเตอร์ลูกข่าย เครือข่าย และอุปกรณ์เครือข่ายที่เชื่อมโยงกับ BAHTNET API ของ ธปท. ติดตั้งที่ศูนย์คอมพิวเตอร์สำรอง (Disaster Recovery Site) ที่มีความพร้อมใช้งานและสามารถปฏิบัติ

งานทดแทนได้เมื่อศูนย์คอมพิวเตอร์หลัก (primary site) หยุดชะงัก โดยต้องสอดคล้องกับระยะเวลาในการกู้คืนระบบ (Recover Time Objective : RTO) 2 ชั่วโมง และระยะเวลาการให้บริการ (Availability) ในรอบ 1 ปีปฏิทิน ควรไม่น้อยกว่า 99.90%

3.2.2 การควบคุมอุปกรณ์ Hardware Security Module (HSM)

ผู้ใช้บริการบาทเนตต้องกำหนดมาตรการด้านการรักษาความมั่นคงปลอดภัยอุปกรณ์ Hardware Security Module (HSM) ทั้งนี้ มาตรการดังกล่าวควรครอบคลุมถึง

(1) ควบคุมการเข้าถึงอุปกรณ์ Hardware Security Module (HSM) โดยกำหนดวิธีการและสิทธิการเข้าถึงอุปกรณ์ Hardware Security Module (HSM) จัดให้มีการแบ่งอำนาจหน้าที่ของพนักงานอย่างเหมาะสมเพื่อป้องกันมิให้พนักงานผู้ใดได้รับสิทธิอย่างเบ็ดเสร็จ และมีกระบวนการจัดการ User ที่มีสิทธิสูง (Privilege Account Management) รวมถึงทบทวนสิทธิดังกล่าวโดยสม่ำเสมอ

(2) อนุญาตให้เชื่อมต่อบริการหรือระบบงานอื่นที่อยู่ภายในศูนย์คอมพิวเตอร์ของผู้ใช้บริการบาทเนตที่จำเป็นสำหรับการปฏิบัติงาน และการรักษาความมั่นคงปลอดภัยเท่านั้น เช่น ระบบ Infrastructure พื้นฐาน เป็นต้น

(3) ไม่อนุญาตให้เชื่อมต่อบริการหรือระบบงานที่อยู่ภายนอกศูนย์คอมพิวเตอร์ของผู้ใช้บริการบาทเนต

(4) การสร้างและจัดเก็บ Key ที่ใช้สำหรับลายมือชื่อดิจิทัล รวมถึงการสร้างลายมือชื่อดิจิทัล ต้องดำเนินการในอุปกรณ์ Hardware Security Module (HSM) ที่มีมาตรฐานความปลอดภัย FIPS 140-2 Level 2 ขึ้นไป โดยมีการแบ่งแยกการจัดเก็บ Key ออกจากระบบงานอื่นภายในองค์กร เช่น แยกอุปกรณ์ HSM หรือ แยก Partition บนอุปกรณ์ HSM เป็นต้น

กรณี Key สำหรับสร้างลายมือชื่อดิจิทัล มิได้เก็บไว้ที่ผู้ใช้บริการบาทเนต แต่ถูกเก็บไว้บนอุปกรณ์ Hardware Security Module (HSM) ของผู้ให้บริการหรือหน่วยงานภายนอก อาจพิจารณาปฏิบัติตามข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยบริการลงลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล (Remote Signing) ตามประกาศสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ เพิ่มเติม

(5) กำหนดวิธีการควบคุมการแก้ไขเปลี่ยนแปลง (Change Management) อุปกรณ์ Hardware Security Module (HSM)

(6) มีอุปกรณ์ Hardware Security Module (HSM) ติดตั้งที่ศูนย์คอมพิวเตอร์สำรอง (Disaster Recovery Site) ที่มีความพร้อมใช้งานและสามารถปฏิบัติงานทดแทนได้เมื่อศูนย์คอมพิวเตอร์หลัก (Primary Site) หยุดชะงัก โดยต้องสอดคล้องกับระยะเวลาในการกู้คืนระบบ (Recover Time Objective : RTO) 2 ชั่วโมง และระยะเวลาการให้บริการ (Availability) ในรอบ 1 ปีปฏิทิน ควรไม่น้อยกว่า 99.90%

3.2.3 การควบคุมด้านการปฏิบัติงาน

ผู้ใช้บริการบาทเนตต้องกำหนดมาตรการด้านการรักษาความมั่นคงปลอดภัยด้านการปฏิบัติงาน เพื่อกำหนดแนวทางติดตาม และเตรียมความพร้อมสำหรับเหตุละเมิดความมั่นคงปลอดภัยคอมพิวเตอร์ลูกข่าย BAHTNET API และอุปกรณ์ Hardware Security Module (HSM) ทั้งนี้ มาตรการดังกล่าวควรครอบคลุมถึง

(1) จัดให้มีผู้รับผิดชอบด้านความมั่นคงปลอดภัย ทั้งในระดับปฏิบัติงานและระดับบริหารเพื่อติดตาม บันทึก แก้ไข และรายงานเมื่อมีการละเมิดความมั่นคงปลอดภัย

(2) จัดทำแผนฉุกเฉินกรณีที่เกิดความเสียหายจากภัยคุกคามให้ครอบคลุมกรณีการบุกรุกของ Malware รวมถึงภัยคุกคามขั้นสูง โดยกำหนดขั้นตอนการแก้ไขปัญหา ทีมงานหรือผู้รับผิดชอบ รวมถึงวิธีการรายงานปัญหาให้กับผู้บริหาร และแจ้งผู้เกี่ยวข้องทราบอย่างรวดเร็วที่สุดเท่าที่จะทำได้ เพื่อแก้ไขปัญหาให้กลับคืนสู่สภาวะปกติโดยเร็ว

(3) มีการจัดเก็บข้อมูลบันทึกเหตุการณ์ของคอมพิวเตอร์ลูกข่าย BAHTNET API อุปกรณ์ Hardware Security Module (HSM) และระบบคอมพิวเตอร์ที่เกี่ยวข้อง ด้วยวิธีการที่ปลอดภัย โดยข้อมูลบันทึกเหตุการณ์ครอบคลุมอย่างน้อย Access log และ Activity log ที่สำคัญ รวมถึงเหตุการณ์ละเมิดความมั่นคงปลอดภัย (Security Events) เช่น การเข้าถึงระบบ การแก้ไขปรับแต่งระบบ การทำรายการธุรกรรมที่สำคัญ เป็นต้น และมีการจัดเก็บข้อมูลอย่างน้อย 90 วัน หรือตามระยะเวลาที่กฎหมายกำหนด โดยอาจจัดให้มี Security Information Event Management (SIEM) สำหรับการบันทึก Security Events

(4) จัดให้มีการติดตาม บันทึก และรายงานเหตุการณ์ละเมิดความมั่นคงปลอดภัยคอมพิวเตอร์ลูกข่าย BAHTNET API และอุปกรณ์ Hardware Security Module (HSM) ให้เป็นไปตามมาตรฐานที่ดี รวมทั้งให้มีการเรียนรู้จากเหตุการณ์ที่เกิดขึ้นเพื่อเตรียมการป้องกันที่จำเป็นไว้ล่วงหน้า โดยครอบคลุมถึง

(4.1) แนวทางในการรับรู้ปัญหาที่เกิดขึ้นอย่างทันท่วงที โดยใช้ข้อมูลและเครื่องมือที่พัฒนาขึ้นตามกรอบแนวความเสี่ยง (Risk-Based Approach) และวิธีการอื่นใด เพื่อยับยั้ง ตรวจจับ ระบุ และสกัดกั้นเหตุการณ์ที่ละเมิดต่อความมั่นคงปลอดภัย

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

(4.3) เก็บรวบรวมหลักฐานต่าง ๆ ที่เป็นประโยชน์

(4.4) บันทึกเหตุการณ์หรือจัดทำรายงานที่เป็นลายลักษณ์อักษร ซึ่งรวมถึงติดตามและตรวจสอบความผิดปกติของบันทึกเหตุการณ์ที่ละเมิดต่อความมั่นคงปลอดภัย เพื่อใช้เป็นแนวทางในการแก้ปัญหา รวมทั้งทบทวนความเหมาะสมของแนวทางปัจจุบัน และพิจารณาปรับปรุงมาตรการที่จำเป็นเพิ่มเติม

3.2.4 การจัดการด้านบุคลากรและการสื่อสาร

ผู้ใช้บริการบาทเนตต้องจัดให้มีการติดตามพัฒนาการทางเทคโนโลยีและภัยคุกคามใหม่ ๆ ที่เกิดขึ้นอย่างใกล้ชิด รวมทั้งสื่อสาร แลกเปลี่ยนข้อมูล และประชาสัมพันธ์วิธีการป้องกันภัยคุกคามต่อระบบคอมพิวเตอร์ ทั้งภายในและภายนอกองค์กร ได้แก่

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

(2) จัดให้มีการประชาสัมพันธ์ให้ข้อมูลและคำแนะนำที่เป็นประโยชน์แก่ลูกค้าผู้ใช้บริการบาทเนต เช่น วิธีการใช้บริการอย่างปลอดภัย เป็นต้น

(3) จัดให้มีการติดตามพัฒนาการทางเทคโนโลยีและภัยคุกคามใหม่ ๆ ที่อาจก่อให้เกิดเหตุการณ์ละเมิดต่อความมั่นคงปลอดภัยอย่างใกล้ชิด มีการหารือร่วมกับผู้เชี่ยวชาญทางด้านความมั่นคงปลอดภัยของระบบคอมพิวเตอร์ รวมทั้งสื่อสาร แลกเปลี่ยนข้อมูล เพื่อกำหนดวิธีการป้องกันภัยคุกคามต่อระบบคอมพิวเตอร์ทั้งภายในและภายนอกองค์กร และประชาสัมพันธ์ให้ผู้เกี่ยวข้องทราบ

4. วันเริ่มต้นบังคับใช้

แนวปฏิบัติฉบับนี้ให้ใช้ตั้งแต่วันที่ 2 กันยายน 2569 เป็นต้นไป

ภาคผนวก 1

กฎหมายที่เกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์และข้อกำหนดที่เกี่ยวข้อง[1/]

ผู้ใช้บริการบาทเนตต้องดำเนินการให้มีการรักษาความมั่นคงปลอดภัยในองค์กร ดำเนินการตามกฎหมายควบคุมการประกอบธุรกิจอื่น ๆ เพื่อให้มั่นใจว่ากระบวนการทำงานและธุรกรรม มีการรักษาความมั่นคงปลอดภัยที่ดี สอดคล้องกับข้อกำหนดตามกฎหมายที่เกี่ยวข้อง และเป็นไปตามมาตรฐานสากล 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. **ระเบียบ ประกาศ แนวปฏิบัติของธนาคารแห่งประเทศไทย**
   - ระเบียบธนาคารแห่งประเทศไทย ว่าด้วยการบริการบาทเนต
   - ประกาศธนาคารแห่งประเทศไทย ที่ สรข. 4/2560 เรื่อง มาตรฐานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของคอมพิวเตอร์ลูกข่ายระบบบาทเนต
   - ประกาศธนาคารแห่งประเทศไทย ที่ สกช. 5/2566 เรื่องหลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ
   - ประกาศธนาคารแห่งประเทศไทย ที่ สนส. 27/2551 เรื่อง การอนุญาตให้บริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ให้บริการการเงินทางอิเล็กทรอนิกส์

---

[1] ธปท. ได้ทำการรวบรวมมาจากกฎหมาย ประกาศ รวมถึงหนังสือเวียน แนวปฏิบัติ และแนวนโยบายของธนาคารแห่งประเทศไทยที่มีผลใช้บังคับ ณ สิ้นเดือนธันวาคม พ.ศ. 2567 แต่อาจไม่ครอบคลุมทั้งหมด ทั้งนี้ หากกฎหมาย ประกาศ หนังสือเวียน แนวปฏิบัติ และแนวนโยบายที่เกี่ยวข้องตามที่ปรากฏในภาคผนวกนี้ได้มีการปรับปรุงแก้ไขเพิ่มเติม ให้ถือปฏิบัติตามกฎหมาย ประกาศ หนังสือเวียน แนวปฏิบัติ และแนวนโยบายที่ได้มีการแก้ไขเพิ่มเติมนั้น

- แนวปฏิบัติในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ที่ ฝตท.(01) ว. 20/2566 และที่แก้ไขเพิ่มเติม
- แนวปฏิบัติการบริหารจัดการความเสี่ยงจากบุคคลภายนอก ที่ ฝตท.(01) ว. 20/2566 และที่แก้ไขเพิ่มเติม

6. **ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์**

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

---