**แบบสำรวจข้อมูลด้านความปลอดภัยในระบบงานคอมพิวเตอร์ของผู้ใช้บริการบาทเนต**

**วัตถุประสงค์** :

ด้วยธนาคารแห่งประเทศไทย (ธปท.) ในฐานะผู้ให้บริการระบบบาทเนตได้ตระหนักถึงภัยคุกคามและอาชญากรรมทางด้านระบบงานและระบบเครือข่ายคอมพิวเตอร์ที่มีแนวโน้มเพิ่มขึ้น จึงมีนโยบายและแผนงานเพิ่มความมั่นคงปลอดภัยและลดความเสี่ยงจากภัยคุกคามในระบบบาทเนต โดย ธปท. อยู่ระหว่างศึกษาและรวบรวมข้อมูลจากผู้ใช้บริการบาทเนต  
 จึงขอความร่วมมือสถาบันท่านตอบแบบสำรวจข้อมูลด้านความปลอดภัยในระบบงานคอมพิวเตอร์ของผู้ใช้บริการบาทเนต โดยแบบสำรวจประกอบด้วย 3 ส่วน คือ  
 ส่วนที่ 1 ข้อมูลด้านความปลอดภัยในระบบงานคอมพิวเตอร์ที่เกี่ยวข้องกับระบบบาทเนต  
 ส่วนที่ 2 ข้อมูลด้านความปลอดภัยที่เกี่ยวข้องกับการใช้งาน SWIFT (เฉพาะสถาบันที่ใช้ SWIFT)  
 ส่วนที่ 3 ข้อเสนอแนะอื่น ๆ

**สถาบัน / ธนาคาร** ธนาคารแห่งประเทศจีน (ไทย) จำกัด (มหาชน)

**ชื่อผู้ตอบแบบสำรวจ** ธัญวรรณ บุญฑริกพรพันธุ์  
ตำแหน่ง Accounting Department (Back office) ฝ่าย Accounting and IT Department

โทรศัพท์ 02-2861010 ต่อ3106 โทรสาร 02-286-5688

E-mail address: tunyawan.b@mail.notes.bank-of-china.com

**ชื่อผู้ประสานงานด้าน IT Security** วัชนันท์ ชูแสงเลิศวิจิตร

ตำแหน่ง IT ฝ่าย Accounting and IT Department

โทรศัพท์ 02-286-1010 ต่อ 3201 โทรสาร 02-286-5688

E-mail address infotech.th@bankofchina.com

โปรดตอบกลับ : ทีมวิเคราะห์และพัฒนา 1 ฝ่ายการชำระเงินและพันธบัตร ธปท.

E-mail : To: [analysis1PBD@bot.or.th](mailto:analysis1PBD@bot.or.th)

ตอบกลับภายใน : วันจันทร์ที่ 23 พฤษภาคม 2559

หากมีข้อสงสัยกรุณาติดต่อ : คุณสมภพ สุรัตนกวีกุล / คุณศรัณย์ พุทธิขจร ฝ่ายเทคโนโลยีสารสนเทศ ธปท.

โทร. 0-2283-6067, 0-2283-5879

**ส่วนที่ 1 ข้อมูลด้านความปลอดภัยระบบคอมพิวเตอร์ที่เกี่ยวข้องกับระบบบาทเนต**

**ด้านเครื่องคอมพิวเตอร์ผู้ใช้งาน (End user Computer)**

1. ท่านใช้งานเครื่องคอมพิวเตอร์ที่ใช้บริการบาทเนตร่วมกับระบบงานอื่น (รวมถึงการใช้ E-mail) หรือไม่  
 หากมี โปรดระบุชื่อระบบงาน

ไม่

2. ท่านควบคุมการใช้งานเครื่องคอมพิวเตอร์ที่ใช้บริการบาทเนตในช่วงนอกเวลาทำการอย่างไร   
 (เช่น ห้ามใช้เครื่องนอกเวลาทำการ เป็นต้น) โปรดระบุรายละเอียดวิธีการควบคุม

อนุญาตให้สามารถใช้นอกเวลาทำการได้ แต่ต้องใช้ Smart Card หรือ Token ในการเข้าระบบซึ่งจะถูกเก็บที่ตัวบุคคลเท่านั้น

3. ท่านกำหนดสิทธิใช้งานบน Windows ของเครื่องคอมพิวเตอร์ที่ใช้บริการบาทเนตอย่างไร   
 (เช่น ผู้ใช้งานไม่มีสิทธิเป็น Admin เครื่อง หรือให้สิทธิเฉพาะผู้ใช้งานบางท่าน เป็นต้น)

ผู้ใช้งานสามารถใช้งานบน Windows ได้โดยโปรแกรมพื้นฐาน ไม่เชื่อมต่อกับระบบอื่นใดยกเว้นระบบบาทเนตซึ่งต้องใช้ Smart Card หรือ Token ในการเข้าระบบซึ่งจะถูกเก็บที่ตัวบุคคลเท่านั้น

4. ท่านมีหลักเกณฑ์ในการกำหนด PIN / Password สำหรับอุปกรณ์ USB Token ที่ใช้บริการบาทเนต อย่างไร (เช่น กำหนดความถี่ในการเปลี่ยน PIN / Password เป็นต้น)

สิทธิ์ในการกำหนด PIN / Password ของอุปกรณ์ USB Token ขึ้นกับเจ้าของ USB Token

5. ท่านมีหลักเกณฑ์ในการกำหนด Windows Password ของผู้ใช้งานเครื่องคอมพิวเตอร์ที่ใช้บริการ  
 บาทเนตอย่างไร (เช่น มีการเปลี่ยน Password ทุก 3 เดือน เป็นต้น)   
ไม่มี

6. ท่านมีหลักเกณฑ์การใช้ USB Storage Device / DVD / CD ของเครื่องคอมพิวเตอร์ที่ใช้บริการ  
 บาทเนตอย่างไร (เช่น ไม่อนุญาตให้ใช้ USB Thumb Drive เป็นต้น) โปรดระบุรายละเอียดวิธีการควบคุม

อนุญาตให้ใช้ USB Thumbdrive เนื่องจากเครื่องคอมพิวเตอร์จะไม่เชื่อมต่อกับระบบภายในธนาคาร ต้องใช้เพื่อจัดเก็บข้อมูลออกมา

**ด้านระบบเครือข่าย (Network)**

7. ท่านมีหลักเกณฑ์การใช้ Internet ของเครื่องคอมพิวเตอร์ที่ใช้บริการบาทเนตอย่างไร   
 (เช่น ปิดการเชื่อมต่อ Internet เป็นต้น)   
ปิดการเชื่อมต่อ Internet

8. ท่านมีหลักเกณฑ์การใช้ Network ของเครื่องคอมพิวเตอร์ที่ใช้บริการบาทเนตในระดับผู้ใช้งานอย่างไร   
 (เช่น แยก Network ของกลุ่มเครื่องคอมพิวเตอร์ดังกล่าวจาก Network สำหรับระบบงานอื่นภายใน องค์กร เป็นต้น)  
แยก Network ของกลุ่มเครื่องคอมพิวเตอร์ดังกล่าวจาก Network สำหรับระบบงานอื่นภายในองค์กร

9. ท่านดูแลและรักษาความปลอดภัยของ Network ที่เชื่อมต่อระบบบาทเนตระหว่างสถาบันท่านกับ ธปท.  
 อย่างไร (เช่น มีการติดตั้ง Firewall เป็นต้น)

เชื่อมต่อโดย Private Line กับ ธปท ไม่มี Network อื่น ๆ เข้ามาเกี่ยวข้อง

**ด้านกระบวนการดูแลความปลอดภัย (Security Processes and Procedures)**

10. ท่านมีกระบวนการดูแลการเปลี่ยนแปลง (Change Management) และเข้าถึงเครื่องแม่ข่าย / อุปกรณ์  
 Network ที่เกี่ยวข้องกับระบบบาทเนตอย่างไร (เช่น มีการบันทึก / ขออนุมัติเมื่อเข้าใช้งานหรือ ปรับเปลี่ยนการตั้งค่าของเครื่องแม่ข่าย / อุปกรณ์ Network เป็นต้น)

มีการบันทึกการเข้าใช้งานห้องควบคุมที่มีการติดตั้งอุปกรณ์ Network

11. ท่านมีกระบวนการและหลักเกณฑ์ในการติดตั้ง Security Patch สำหรับ Windows OS อย่างไร   
 (เช่น กำหนดความถี่ในการติดตั้งทุก 3 เดือน เป็นต้น)

มีการติดตั้งการอัพเดทของ Security Patch สำหรับ Windows OS ให้กับเครือข่ายภายในของธนาคารเท่านั้น ไม่เชื่อมต่อไปยังเครือข่ายของ ธปท

12. ท่านควบคุมการเข้าถึงพื้นที่เกี่ยวข้องกับเครื่องคอมพิวเตอร์ที่ใช้บริการบาทเนตอย่างไร   
 (เช่น มีการกั้นพื้นที่ / ห้องเพื่อป้องกันผู้ที่ไม่มีหน้าที่เกี่ยวข้อง เป็นต้น)

มีการกั้นพื้นที่เป็นห้องแยกออกจากส่วนงานอื่น ๆ

13. ท่านควบคุมการเข้าถึงพื้นที่เกี่ยวข้องกับเครื่องคอมพิวเตอร์แม่ข่าย / อุปกรณ์ Network ที่ใช้บริการ บาทเนตอย่างไร (เช่น มีการกั้นพื้นที่ / ห้องเพื่อป้องกันผู้ที่ไม่มีหน้าที่เกี่ยวข้อง เป็นต้น)

มีการกั้นพื้นที่เป็นห้องแยกออกจากส่วนงานอื่น ๆ

14. ท่านมีการเก็บประวัติการเข้าใช้เครื่องคอมพิวเตอร์ที่ใช้บริการบาทเนตของผู้ใช้งานอย่างไร  
 (เช่น มี Log ของ Active Directory / Log จากอุปกรณ์ SIEM เป็นต้น) โปรดระบุรายละเอียดวิธีการ ควบคุม

ไม่มี

**ส่วนที่ 2 ข้อมูลด้านความปลอดภัยที่เกี่ยวข้องกับการใช้งาน SWIFT (เฉพาะสถาบันที่ใช้ SWIFT)**

15. ท่านปฏิบัติตาม Guideline ของ SWIFT KB5020787 (Security Guidance for Customer Managed  
 Interface) หรือไม่ อย่างไร

------------------------------------------------------------------------------------------------------------------------------------  
------------------------------------------------------------------------------------------------------------------------------------

16. ท่านปฏิบัติตาม Guideline ของ SWIFT KB5020788 (Security Guidance for Alliance) หรือไม่ อย่างไร

------------------------------------------------------------------------------------------------------------------------------------

------------------------------------------------------------------------------------------------------------------------------------

17. ท่านใช้งาน SWIFT Alliance Access และ / หรือ Alliance Entry Version มากกว่าหรือเท่ากับ Version 7.1.14 หรือไม่

------------------------------------------------------------------------------------------------------------------------------------

------------------------------------------------------------------------------------------------------------------------------------

18. ท่านตรวจสอบตาม SWIFT KB5020870 หรือไม่

------------------------------------------------------------------------------------------------------------------------------------

------------------------------------------------------------------------------------------------------------------------------------

19. ท่านควบคุมการสร้างรายการเข้าระบบบาทเนตผ่าน SWIFT อย่างไร   
 (เช่น มีการแบ่งหน้าที่กันเป็น Dual Controls เป็นต้น)  
------------------------------------------------------------------------------------------------------------------------------------

------------------------------------------------------------------------------------------------------------------------------------  
------------------------------------------------------------------------------------------------------------------------------------

------------------------------------------------------------------------------------------------------------------------------------

**ส่วนที่ 3 ข้อเสนอแนะอื่น ๆ**

------------------------------------------------------------------------------------------------------------------------------------

------------------------------------------------------------------------------------------------------------------------------------

------------------------------------------------------------------------------------------------------------------------------------

------------------------------------------------------------------------------------------------------------------------------------

–––– ขอขอบคุณในความร่วมมือ ––––