(ร่าง) แนวนโยบายธนาคารแห่งประเทศไทย
เรื่อง การบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศขั้นต้นที่จำเป็น
ของผู้ประกอบธุรกิจสินเชื่อที่มิใช่สถาบันการเงิน

31 มีนาคม 2569

ธนาคารแห่งประเทศไทย

จัดทำโดย
ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ
สายกำกับระบบการชำระเงินและคุ้มครองผู้ใช้บริการทางการเงิน
ธนาคารแห่งประเทศไทย
โทรศัพท์ 0-2283-XXXX
e-mail: tsd-techpolicy@bot.or.th

สารบัญ

แนวนโยบายธนาคารแห่งประเทศไทย
เรื่อง การบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศขั้นต้นที่จำเป็น
สำหรับผู้ประกอบธุรกิจสินเชื่อที่มิใช่สถาบันการเงิน

---

1. เหตุผลในการออกแนวนโยบาย

ปัจจุบันผู้ประกอบธุรกิจสินเชื่อที่มิใช่สถาบันการเงินนำระบบเทคโนโลยีสารสนเทศมาใช้เป็นโครงสร้างพื้นฐานสำคัญในการดำเนินธุรกิจและการให้บริการลูกค้ามามากขึ้น เพื่อเพิ่มประสิทธิภาพในการทำธุรกิจและความสะดวกในการเข้าถึงบริการทางการเงินของลูกค้า ในขณะเดียวกัน ความเสี่ยงจากการใช้เทคโนโลยีสารสนเทศและภัยคุกคามไซเบอร์มีความซับซ้อนและมีแนวโน้มเพิ่มขึ้นต่อเนื่อง โดยหากไม่มีการกำกับดูแลและควบคุมการใช้เทคโนโลยีสารสนเทศอย่างเหมาะสม อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของธุรกรรมและข้อมูลลูกค้า

ธนาคารแห่งประเทศไทย (ธปท.) จึงออกแนวนโยบายการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศขั้นต่ำสำหรับผู้ประกอบธุรกิจสินเชื่อที่มิใช่สถาบันการเงิน เพื่อใช้เป็นแนวทางในการดูแลระบบและข้อมูลสำคัญให้มีความมั่นคงปลอดภัย โดยผู้ประกอบธุรกิจสามารถนำไปปรับใช้ให้เหมาะสมสอดคล้องกับความซับซ้อนและบริบทของการดำเนินธุรกิจ

2. ขอบเขตการใช้แนวนโยบาย

แนวนโยบายฉบับนี้ใช้กับ

2.1 ผู้ประกอบธุรกิจสินเชื่อส่วนบุคคลภายใต้การกำกับตามประกาศกระทรวงการคลังว่าด้วยกิจการที่ต้องขออนุญาตตามข้อ 5 แห่งประกาศของคณะปฏิวัติ ฉบับที่ 58 (เรื่อง สินเชื่อส่วนบุคคลภายใต้การกำกับ) และมิได้เป็นบริษัทในกลุ่มธุรกิจทางการเงินตามประกาศธนาคารแห่งประเทศไทยว่าด้วยหลักเกณฑ์การกำกับดูแลกลุ่มธุรกิจทางการเงินและที่เกี่ยวข้องทุกแห่ง

2.2 ผู้ประกอบธุรกิจสินเชื่อรายย่อยเพื่อการประกอบอาชีพภายใต้การกำกับตามประกาศกระทรวงการคลังว่าด้วยกิจการที่ต้องขออนุญาตตามข้อ 5 แห่งประกาศของคณะปฏิวัติ ฉบับที่ 58 (เรื่อง สินเชื่อรายย่อยเพื่อการประกอบอาชีพภายใต้การกำกับ) และมิได้เป็นบริษัทในกลุ่มธุรกิจทางการเงินตามประกาศธนาคารแห่งประเทศไทยว่าด้วยหลักเกณฑ์การกำกับดูแลกลุ่มธุรกิจทางการเงินและที่เกี่ยวข้องทุกแห่ง

2.3 ผู้ประกอบธุรกิจระบบหรือเครือขายอิเล็กทรอนิกสสำหรับธุรกรรมสินเชื่อระหวางบุคคลกับบุคคลที่มิใชสถาบันการเงิน ตามประกาศกระทรวงการคลังวาดวยกิจการที่ตองขออนุญาตตามขอ 5 แหงประกาศของคณะปฏิวัติ ฉบับที่ 58 (เรื่อง ธุรกิจระบบหรือเครือขาย อิเล็กทรอนิกสสำหรับธุรกรรมสินเชื่อระหวางบุคคลกับบุคคล)

3. เนื้อหา

3.1 นิยาม

“เทคโนโลยีสารสนเทศ” (Information Technology : IT) หมายความว่า เทคโนโลยีสารสนเทศ ที่นำมาใช้ในการให้บริการหรือดำเนินธุรกิจ ซึ่งครอบคลุมถึง ข้อมูล ระบบปฏิบัติการ (operating system) ระบบงาน (application system) ระบบฐานข้อมูล (database system) อุปกรณ์คอมพิวเตอร์ (computer hardware) และระบบเครือข่ายสื่อสาร (communication) เป็นต้น

“ความเสี่ยงด้านเทคโนโลยีสารสนเทศ” (Information Technology Risk : IT risk) หมายความว่า ความเสี่ยงที่อาจเกิดขึ้นจากการใช้เทคโนโลยีสารสนเทศ รวมถึงความเสี่ยงที่เกิดจากภัยคุกคามทางไซเบอร์ (cyber threats)

“บุคคลภายนอก” หมายความว่า บุคคลหรือนิติบุคคลภายนอกซึ่งเป็นผู้ให้บริการด้านเทคโนโลยีสารสนเทศแทนผู้ประกอบธุรกิจ หรือเป็นผู้ที่มีการเชื่อมต่อกับระบบเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจ หรือเป็นผู้ที่สามารถเข้าถึงข้อมูลสำคัญของผู้ประกอบธุรกิจ หรือลูกค้าที่ควบคุมดูแลโดยผู้ประกอบธุรกิจได้ ทั้งนี้ บุคคลภายนอกไม่ครอบคลุมถึงสมาชิกหรือลูกค้าที่ใช้ผลิตภัณฑ์และบริการของผู้ประกอบธุรกิจ

“ผู้ประกอบธุรกิจสินเชื่อที่มิใช่สถาบันการเงิน” หมายความว่า ผู้ประกอบธุรกิจสินเชื่อส่วนบุคคลภายใต้การกำกับที่มิใช่สถาบันการเงิน ผู้ประกอบธุรกิจสินเชื่อรายย่อยเพื่อการประกอบอาชีพภายใต้การกำกับที่มิใช่สถาบันการเงิน และผู้ประกอบธุรกิจระบบหรือเครือขายอิเล็กทรอนิกสสำหรับธุรกรรมสินเชื่อระหวางบุคคลกับบุคคลที่มิใชสถาบันการเงิน และมิได้เป็นบริษัทในกลุ่มธุรกิจทางการเงินตามประกาศธนาคารแห่งประเทศไทยว่าด้วยหลักเกณฑ์การกำกับดูแลกลุ่มธุรกิจทางการเงินและประกาศที่เกี่ยวข้อง

“ผู้ประกอบธุรกิจ” หมายความว่า ผู้ประกอบธุรกิจสินเชื่อที่มิใช่สถาบันการเงิน

3.2 หลักเกณฑ์การบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศขั้นต้นที่จำเป็น

ผู้ประกอบธุรกิจควรมีการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เพียงพอเหมาะสมสอดคล้องตามความซับซ้อนและบริบทของการดำเนินธุรกิจ เพื่อดูแลระบบเทคโนโลยีสารสนเทศและข้อมูลสำคัญของผู้ประกอบธุรกิจให้มีความมั่นคงปลอดภัย โดยผู้ประกอบธุรกิจควรดำเนินการ ดังนี้

(1) ธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ

คณะกรรมการและผู้บริหารระดับสูงของผู้ประกอบธุรกิจมีบทบาทหน้าที่และความรับผิดชอบในการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยดูแลให้มีการกำหนดนโยบายด้านการรักษาความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษรและพิจารณาอนุมัติ รวมทั้ง ดูแลติดตามให้มีการทบทวนและปรับปรุงนโยบายให้เหมาะสมกับสถานการณ์อย่างสม่ำเสมอ นอกจากนี้ มีการกำกับดูแลให้มีการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศอย่างเหมาะสมสอดคล้องตามนโยบายที่กำหนด เพื่อให้มั่นใจว่าระบบเทคโนโลยีสารสนเทศและข้อมูลสำคัญมีความปลอดภัย ตลอดจนติดตามประเด็นปัญหาด้านเทคโนโลยีสารสนเทศที่มีนัยสำคัญ

(2) การบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

(2.1) การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT asset management)

จัดให้มีการบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศที่เหมาะสม โดยจัดทำทะเบียนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศอย่างครบถ้วน เพื่อให้สามารถระบุรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศและนำไปใช้กำหนดแนวทางการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศได้อย่างเหมาะสม นอกจากนี้ ต้องบำรุงรักษาทรัพย์สินด้านเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ รวมถึงบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศที่ใกล้หมดอายุ การใช้งานหรือสิ้นสุดการให้บริการอย่างเหมาะสมและเท่าทันกับความเสี่ยง เพื่อให้ระบบเทคโนโลยีสารสนเทศมีความมั่นคงปลอดภัย

(2.2) การรักษาความมั่นคงปลอดภัยของข้อมูล (information security)

จัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลสอดคล้องตามระดับชั้นความลับของข้อมูล (information classification) ครอบคลุมข้อมูลที่อยู่ระหว่างการรับส่งผ่านเครือข่ายสื่อสาร (data-in-transit) และข้อมูลที่จัดเก็บบนระบบงานหรือสื่อบันทึกข้อมูล (data-at-rest) รวมทั้ง กำหนดกระบวนการบริหารจัดการการเข้ารหัสข้อมูล (cryptography) ที่เชื่อถือได้และเป็นมาตรฐานสากลที่ยอมรับโดยทั่วไป โดยอย่างน้อย ควรมีการเข้ารหัสช่องทางสื่อสารที่ใช้รับส่งข้อมูลสำคัญ และเข้ารหัสข้อมูลสำคัญที่จัดเก็บบนระบบงาน สื่อบันทึกข้อมูลและอุปกรณ์ที่ใช้ปฏิบัติงาน เพื่อรักษาความมั่นคงปลอดภัยและความลับของข้อมูลสำคัญ

(2.3) การควบคุมการเข้าถึง (access control)

จัดให้มีการควบคุมการเข้าถึงระบบปฏิบัติการ ระบบงาน และระบบฐานข้อมูล โดยกำหนดสิทธิการเข้าถึงระบบปฏิบัติการ ระบบงานและระบบฐานข้อมูล สอดคล้องตามหลักการให้สิทธิ

ตามความจำเป็น (least privilege) รวมทั้ง ตรวจสอบการยืนยันตัวตนตามสิทธิที่กำหนดไว้ โดยให้สอดคล้องกับหลักการให้สิทธิตามความจำเป็น (least privilege) เพื่อป้องกันการเข้าถึง หรือเปลี่ยนแปลงระบบหรือข้อมูลโดยผู้ที่ไม่มีสิทธิ โดยต้องครอบคลุมอย่างน้อย ดังนี้

(2.3.1) การจัดการบัญชีผู้ใช้งานที่มีสิทธิสูง (privileged user) ต้องมีการกำหนดมาตรการควบคุมและจำกัดการใช้บัญชีผู้ใช้งานที่มีสิทธิสูงอย่างเข้มงวด เช่น การมอบหมายสิทธิ การเบิกใช้ กำหนดระยะเวลาการใช้งาน การสอบทานหลังการใช้ เพื่อป้องกันการเข้าถึงและเปลี่ยนแปลงระบบหรือข้อมูลโดยไม่ได้รับอนุญาต

(2.3.2) จัดให้มีการพิสูจน์ตัวตนแบบ multi-factor authentication ในกรณีดังต่อไปนี้

- บัญชีผู้ใช้งานที่มีสิทธิสูง (privileged user) ทุกบัญชีของระบบปฏิบัติการ ระบบฐานข้อมูล ระบบงาน อุปกรณ์เครือข่ายและอุปกรณ์รักษาความปลอดภัยเครือข่าย
- บัญชีผู้ใช้งาน (user) ทุกบัญชีที่เชื่อมต่อมาจากระบบเครือข่ายสื่อสารสาธารณะและสามารถเข้าถึงข้อมูลลูกค้าได้

ในกรณีที่ระบบปฏิบัติการ ระบบฐานข้อมูล ระบบงาน อุปกรณ์เครือข่ายและอุปกรณ์รักษาความปลอดภัยเครือข่าย ไม่รองรับการพิสูจน์ตัวตนแบบ multi-factor authentication ผู้ประกอบธุรกิจต้องจัดให้มีวิธีการอื่นใดที่มีประสิทธิภาพเทียบเท่าทดแทน เพื่อลดความเสี่ยงจากการถูกโจมตีการพิสูจน์ตัวตนได้โดยง่าย

อย่างไรก็ตาม กรณีที่ไม่สามารถปฏิบัติตามได้ในบางระบบหรืออุปกรณ์ ต้องจัดให้มีกระบวนการขออนุมัติยกเว้นและดำเนินการประเมินความเสี่ยง รวมทั้งพิจารณาแนวทางควบคุมความเสี่ยงที่เพียงพอเหมาะสม

(2.4) การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร (communications security)

จัดให้มีการรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร เพื่อให้ระบบเครือข่ายสื่อสารและข้อมูลที่รับส่งผ่านระบบเครือข่ายสื่อสารมีความมั่นคงปลอดภัย สามารถป้องกันการบุกรุกหรือภัยคุกคามที่อาจเกิดขึ้น

(2.5) การรักษาความมั่นคงปลอดภัยของเครื่องแม่ข่าย (server) และอุปกรณ์ที่ใช้ปฏิบัติงานของผู้ใช้เทคโนโลยีสารสนเทศ (endpoint)

จัดให้มีการรักษาความมั่นคงปลอดภัยของเครื่องแม่ข่าย (server) และอุปกรณ์ที่ใช้ปฏิบัติงานของผู้ใช้เทคโนโลยีสารสนเทศ (endpoint) ให้สามารถป้องกันการโจมตีด้วยรูปแบบต่าง ๆ หรือภัยจากโปรแกรมไม่ประสงค์ดี (malware) รวมทั้งติดตามให้มีการปรับปรุงให้เป็นปัจจุบันและเท่าทันภัย

คุกคามใหม่อย่างสม่ำเสมอ เพื่อเป็นการลดความเสี่ยงจากการถูกโจมตี และป้องกันการรั่วไหลของข้อมูล หรือการเข้าใช้งานโดยไม่ได้รับอนุญาต

(2.6) การสำรองข้อมูล (data backup)

สำรองข้อมูลด้วยวิธีการและระยะเวลาที่เหมาะสมกับความสำคัญของข้อมูลและความเสี่ยงข้อมูล เช่น การสำรองข้อมูลประจำวัน นอกจากนี้ กำหนดให้มีการทดสอบความพร้อมใช้ของข้อมูลสำรองเป็นประจำสม่ำเสมอ เพื่อให้มั่นใจว่าข้อมูลสำรองที่มีความพร้อมใช้งานในกรณีที่ระบบและข้อมูลหลักเกิดเหตุขัดข้องหรือได้รับความเสียหาย

(2.7) การจัดเก็บข้อมูลบันทึกเหตุการณ์ (logging)

จัดเก็บข้อมูลบันทึกเหตุการณ์ของเครื่องแม่ข่าย ระบบงาน และอุปกรณ์เครือข่ายที่สำคัญอย่างครบถ้วน เช่น ข้อมูลบันทึกการเข้าถึงระบบ (access log) ข้อมูลบันทึกการดำเนินงาน (activity log) รวมทั้ง ดูแลให้ระบบงานหรือข้อมูลที่ใช้จัดเก็บข้อมูลบันทึกเหตุการณ์มีการรักษาความมั่นคงปลอดภัย เพื่อให้สามารถใช้ในการติดตาม ตรวจสอบการเข้าถึงหรือการใช้งานระบบหรือข้อมูล และใช้เป็นหลักฐานการทำธุรกรรมทางอิเล็กทรอนิกส์ตามที่กฎหมายกำหนด

(2.8) การเฝ้าระวังภัยคุกคาม (security monitoring)

จัดให้มีการติดตามดูแลระบบและเฝ้าระวังภัยคุกคาม โดยมีกระบวนการหรือเครื่องมือสำหรับตรวจจับเหตุการณ์ผิดปกติหรือภัยคุกคามทางไซเบอร์ที่มีผลกระทบต่อความมั่นคงปลอดภัยของระบบที่สำคัญ รวมทั้ง มีการติดตามภัยคุกคามใหม่ ๆ เพื่อให้สามารถตรวจจับ ป้องกัน และรับมือเหตุการณ์ผิดปกติและภัยคุกคามได้อย่างทันท่วงที

(2.9) การบริหารจัดการช่องโหว่ (vulnerability management)

จัดให้มีการประเมินช่องโหว่สำหรับทุกระบบงานตามระดับความเสี่ยง โดยระบบงานสำคัญต้องดำเนินการอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ รวมทั้งกำหนดแนวทางการดำเนินการและระยะเวลาในการแก้ไขช่องโหว่ให้สอดคล้องตามระดับความเสี่ยงและความสำคัญของระบบงาน

(2.10) การทดสอบเจาะระบบ (penetration testing)

จัดให้มีการทดสอบเจาะระบบ โดยผู้เชี่ยวชาญภายในหรือภายนอกที่มีความเป็นอิสระอย่างน้อยครอบคลุมระบบงานและระบบเครือข่ายที่มีการเชื่อมต่อกับเครือข่ายสื่อสารสาธารณะ

(Internet facing) สม่ำเสมออย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เพื่อให้ทราบถึงช่องโหว่และสามารถดำเนินการแก้ไขและป้องกันภัยคุกคามที่อาจเกิดขึ้นได้อย่างทันการณ์

(2.11) การบริหารจัดการการเปลี่ยนแปลง (change management)

จัดให้มีกระบวนการบริหารจัดการการเปลี่ยนแปลงและควบคุมการเปลี่ยนแปลงอย่างรัดกุมและเพียงพอ เช่น การนำระบบขึ้นใช้งานจริง (system deployment) การตั้งค่าระบบ (system configuration) การติดตั้ง patch เพื่อให้การเปลี่ยนแปลงเป็นไปตามวัตถุประสงค์ที่กำหนดไว้อย่างถูกต้องครบถ้วน และป้องกันการเปลี่ยนแปลงโดยที่ไม่ได้รับอนุญาต

(2.12) การกำหนดด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ (security baseline and hardening)

จัดให้มีการกำหนดมาตรฐานการรักษาความมั่นคงปลอดภัยขั้นต่ำ (minimum security baseline) และกระบวนการตั้งค่าการรักษาความมั่นคงปลอดภัยสอดคล้องกับมาตรฐานดังกล่าว (security hardening) ครอบคลุมระบบปฏิบัติการ ระบบฐานข้อมูล ระบบงาน อุปกรณ์เครือข่ายและอุปกรณ์รักษาความปลอดภัยเครือข่ายที่รองรับระบบงานสำคัญให้ชัดเจนเป็นลายลักษณ์อักษร รวมทั้งดำเนินการตั้งค่าและสอบทานการตั้งค่าอย่างสม่ำเสมอตามที่ได้กำหนดไว้ เพื่อให้มั่นใจว่าระบบงานที่รองรับการให้บริการมีการรักษาความมั่นคงปลอดภัยขั้นต่ำตามมาตรฐานที่กำหนดไว้

ในกรณีที่ผู้ประกอบธุรกิจไม่สามารถปฏิบัติตามมาตรฐานที่ได้กำหนดไว้ข้างต้น ต้องจัดให้มีกระบวนการขออนุมัติยกเว้น (exception) เพื่อประเมินความเสี่ยงและพิจารณาแนวทางควบคุมความเสี่ยงที่เพียงพอเหมาะสมก่อนดำเนินการ

(2.13) การบริหารจัดการ security patch (security patch management)

จัดให้มีกระบวนการบริหารจัดการ security patch สำหรับทุกระบบงานและอุปกรณ์ เพื่อเป็นการลดความเสี่ยงที่ระบบเทคโนโลยีสารสนเทศถูกโจมตีจากช่องโหว่ใหม่ ๆ โดยต้องดำเนินการให้แล้วเสร็จในระยะเวลาที่เหมาะสมตามระดับความเสี่ยงของช่องโหว่และระดับความสำคัญของระบบงาน ในกรณีที่ผู้ผลิตระบบงานหรืออุปกรณ์ยังไม่แจ้งการปรับปรุง security patch อย่างเป็นทางการเพื่อปิดช่องโหว่ใหม่ ๆ ที่เพิ่งค้นพบ ผู้ประกอบธุรกิจต้องจัดให้มีการควบคุมอื่นทดแทน เพื่อลดความเสี่ยงจากการถูกโจมตีจากช่องโหว่นั้น ๆ

ทั้งนี้ กรณีที่ไม่สามารถติดตั้ง security patch ได้ ต้องจัดให้มีกระบวนการขออนุมัติยกเว้นและดำเนินการประเมินความเสี่ยง รวมทั้งพิจารณาแนวทางควบคุมความเสี่ยงที่เพียงพอเหมาะสม เพื่อลดความเสี่ยงที่ระบบเทคโนโลยีสารสนเทศจะถูกโจมตี

(2.14) การบริหารจัดการความเสี่ยงจากบุคคลภายนอก (third party risk management)

ในกรณีที่ผู้ประกอบธุรกิจดำเนินการดังต่อไปนี้ (1) ใช้บริการงานด้านเทคโนโลยีสารสนเทศจากบุคคลภายนอก (IT outsourcing) (2) เชื่อมต่อระบบเทคโนโลยีสารสนเทศกับบุคคลภายนอก หรือ (3) ให้บุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญของผู้ประกอบธุรกิจ หรือเข้าถึงข้อมูลลูกค้าในรูปแบบอิเล็กทรอนิกส์ ผู้ประกอบธุรกิจต้องกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศและความเสี่ยงจากภัยไซเบอร์ให้สอดคล้องตามระดับความเสี่ยงและระดับความมีนัยสำคัญบนพื้นฐานที่ต้องรับผิดชอบต่อการให้บริการหรือดำเนินธุรกิจแก่ลูกค้าและคงไว้ซึ่งความน่าเชื่อถือชื่อเสียง และประสิทธิภาพในการให้บริการตามหลักการดังนี้

(2.14.1) กำหนดบทบาท หน้าที่ และความรับผิดชอบระหว่างผู้ประกอบธุรกิจกับบุคคลภายนอกอย่างชัดเจนและเป็นลายลักษณ์อักษร โดยกรณีการใช้บริการงานด้านเทคโนโลยีสารสนเทศจากบุคคลภายนอก (IT outsourcing) ที่มีนัยสำคัญ ควรระบุให้ผู้ตรวจสอบภายในและผู้ตรวจสอบภายนอกมีสิทธิเข้าตรวจสอบการดำเนินการด้านเทคโนโลยีสารสนเทศของบุคคลภายนอกเป็นเงื่อนไขในสัญญาหรือข้อตกลงบุคคลภายนอก

ทั้งนี้ สำหรับกรณีที่ไม่สามารถระบุสิทธิให้ผู้ตรวจสอบภายในหรือผู้ตรวจสอบภายนอกมีสิทธิเข้าตรวจสอบการดำเนินการด้านเทคโนโลยีสารสนเทศของบุคคลภายนอกที่ให้บริการงานด้านเทคโนโลยีสารสนเทศ (IT outsourcing) ในเงื่อนไขสัญญาหรือข้อตกลงกับบุคคลภายนอก ผู้ประกอบธุรกิจต้องมั่นใจว่าบุคคลภายนอกรายดังกล่าวมีผลการตรวจสอบจากผู้ตรวจสอบภายนอกที่เป็นอิสระทดแทน

(2.14.2) กำกับดูแล ติดตาม และบริหารจัดการความเสี่ยงจากบุคคลภายนอกสอดคล้องตามระดับความเสี่ยงและระดับความมีนัยสำคัญ

(2.14.3) รักษาความมั่นคงปลอดภัยของระบบงานและข้อมูลที่มีการใช้บริการการเชื่อมต่อ หรือเข้าถึงข้อมูลจากบุคคลภายนอกที่สอดคล้องกับมาตรฐานการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจและอ้างอิงมาตรฐานสากลที่ยอมรับโดยทั่วไป

(2.14.4) เตรียมความพร้อมรับมือต่อเหตุการณ์ที่อาจเกิดขึ้นและมีผลกระทบอย่างมีนัยสำคัญ เพื่อให้สามารถให้บริการหรือดำเนินธุรกิจได้อย่างต่อเนื่อง รวมถึงการมีข้อมูลพร้อมใช้สำหรับการให้บริการหรือดำเนินธุรกิจแก่ลูกค้า

3.3 การรายงานปัญหาด้านเทคโนโลยีสารสนเทศ

ผู้ประกอบธุรกิจรายงานเหตุการณ์ด้านไซเบอร์ที่ถูกโจมตีสำเร็จต่อ ธปท. ทันทีเมื่อเกิดเหตุหรือรับรู้ปัญหาหรือเหตุการณ์นั้นตามรูปแบบและช่องทางที่ ธปท. กำหนด และแจ้งสาเหตุและการแก้ไขปัญหาเพิ่มเติมในภายหลัง เพื่อให้ ธปท. สามารถกำกับดูแลและติดตามความเสี่ยงด้านเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจได้เท่าทันต่อสถานการณ์