ประกาศ

ธนาคารไทยเครดิต จำกัด (มหาชน)

ที่ 131/2566

เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

(IT Security Policy)

เพื่อให้ธนาคารสามารถบริหารจัดการทางด้านความปลอดภัยของระบบสารสนเทศ รวมถึงบริหารจัดการความมั่นคงปลอดภัยในด้านทรัพย์สินสารสนเทศ ด้านบุคลากร ด้านกายภาพและสภาพแวดล้อม ได้อย่างมีประสิทธิภาพเพียงพอ เหมาะสมต่อการดำเนินธุรกิจ

ที่ประชุมคณะกรรมการธนาคาร ครั้งที่ 10/2566 วันที่ 30 สิงหาคม 2566 มีมติอนุมัติทบทวนและปรับปรุงนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security Policy) ของธนาคารไทยเครดิต จำกัด (มหาชน) ประจำปี 2566 โดยมีรายละเอียดตามเอกสารแนบท้าย และให้มีผลบังคับใช้ตั้งแต่ 1 กันยายน 2566 เป็นต้นไป

ทั้งนี้ ให้ยกเลิกประกาศที่ 112/2565 นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security Policy) และให้ใช้ประกาศฉบับนี้แทน

ประกาศ ณ วันที่ 30 สิงหาคม 2566

(นายรอยย์ ออกุสตินัส กุนารา)

กรรมการผู้จัดการ

หน่วยงานรักษาความปลอดภัยเทคโนโลยีสารสนเทศ

นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

IT Security Policy

ธนาคารไทยเครดิต จำกัด (มหาชน)

ประจำปี 2566

อนุมัติโดย : คณะกรรมการธนาคาร

อ้างอิงรายงานการประชุมคณะกรรมการธนาคาร ครั้งที่ 10/2566 วันที่ 30 สิงหาคม 2566

บมจ.ธนาคารไทยเครดิต
123 อาคารไทยประกันชีวิต ถนนรัชดาภิเษก แขวงดินแดง เขตดินแดง กรุงเทพฯ 10400

Thai Credit Bank Public Company Limited
123 Thai Life Insurance Bldg., Ratchadaphisek Rd., Dindaeng, Bangkok 10400

Tel. (662) 697-5300 Fax. (662) 642-3096
www.thaicreditbank.com

ส่วนที่ 1 บททั่วไป (Preface)

1.1 วัตถุประสงค์

1. เพื่อให้ธนาคารสามารถบริหารจัดการทางด้านการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศได้อย่างมีประสิทธิภาพ สอดคล้องกับกลยุทธ์ทางธุรกิจและไม่ขัดต่อกฎหมายข้อกำหนดของธนาคารแห่งประเทศไทย และจรรยาบรรณของธนาคารไทยเครดิต จำกัด (มหาชน)
2. เพื่อใช้ในการรักษาความลับ ความถูกต้องเชื่อถือได้ของระบบและข้อมูล และให้อยู่ในสภาพพร้อมใช้งานของเทคโนโลยีสารสนเทศ รวมถึงบริหารจัดการความมั่นคงปลอดภัยในด้านทรัพย์สินสารสนเทศ ความปลอดภัยของข้อมูล การควบคุมการเข้าถึง ด้านกายภาพและสภาพแวดล้อม ระบบเครือข่ายสื่อสาร ด้านการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ การจัดหาและพัฒนาระบบ การบริหารจัดการเหตุการณ์ผิดปกติและปัญหา การจัดทำแผนฉุกเฉิน และการบริหารจัดการผู้ให้บริการภายนอก
3. เพื่อให้พนักงานของธนาคาร และบุคคลที่เกี่ยวข้องได้ตระหนักถึงความสำคัญของการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ รวมถึงเป็นการกำหนดทิศทางในการสนับสนุนการดำเนินการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของธนาคาร
4. เพื่อใช้เป็นแนวทางกำหนดวิธีปฏิบัติในการตรวจสอบ ทำให้เกิดความน่าเชื่อถือของระบบงานและข้อมูล มีความมั่นคงปลอดภัย ตลอดจนมีกระบวนการที่สามารถให้บริการได้อย่างต่อเนื่อง รวมถึงกำหนดระเบียบปฏิบัติที่เกี่ยวข้อง

1.2 ขอบเขต

นโยบายฉบับนี้ครอบคลุมการบริหารจัดการทางด้านการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของธนาคาร โดยมีสาระสำคัญของนโยบาย ประกอบด้วย

ส่วนที่ 1 บททั่วไป (Preface)
ส่วนที่ 2 บทบาท หน้าที่ ความรับผิดชอบ (Role and Responsibility)
ส่วนที่ 3 คำนิยาม (Definition)
ส่วนที่ 4 การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security)

1.3 ประกาศ หลักเกณฑ์ หรือกฎหมายที่เกี่ยวข้อง

- ประกาศธนาคารแห่งประเทศไทย ที่ สนส. 21/2562 เรื่อง หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ของสถาบันการเงิน และแนวปฏิบัติการบริหารจัดการความเสี่ยงจากบุคคลภายนอก ลงวันที่ 1 ตุลาคม 2562

บมจ.ธนาคารไทยเครดิต
123 อาคารไทยประกันชีวิต ถนนรัชดาภิเษก แขวงดินแดง เขตดินแดง กรุงเทพฯ 10400
Thai Credit Bank Public Company Limited
123 Thai Life Insurance Bldg. Ratchadaphisek Rd., Dindaeng Bangkok 10400
Tel. (662) 697-5300 Fax. (662) 642-3096
www.thaicreditbank.com

- ประกาศธนาคารแห่งประเทศไทย ที่ สนช. 11/2561 เรื่อง นโยบายและมาตรการการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศ ลงวันที่ 17 เมษายน 2561
- ประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ที่ สธ. 38/2565 เรื่อง ข้อกำหนดในรายละเอียดเกี่ยวกับการให้มีระบบเทคโนโลยีสารสนเทศและนป. 7/2565 เรื่อง แนวปฏิบัติในการจัดให้มีระบบเทคโนโลยีสารสนเทศ
- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
- พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 และ 2560
- มาตรฐาน ISO/IEC27001 : 2022 ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

1.4 การทบทวนนโยบาย

ธนาคารจะทบทวนนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญที่มีผลต่อนโยบายฉบับนี้

1.5 การขอยกเว้นไม่ปฏิบัติตามนโยบาย

กรณีที่มีระบบงานใด ไม่สามารถปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ให้หน่วยงานเจ้าของระบบงานและหน่วยงานที่รับผิดชอบในขอบเขตงานที่ขอยกเว้น ทำการประเมินความเสี่ยงพร้อมทั้งแนวทางควบคุมความเสี่ยง และขอความเห็นชอบจากฝ่ายจัดการความเสี่ยง และฝ่ายรักษาความปลอดภัยเทคโนโลยีสารสนเทศ เพื่อนำเสนอลงนามอนุมัติโดยผู้บริหารสูงสุดสายงานเทคโนโลยีสารสนเทศ

บมจ.ธนาคารไทยเครดิต
123 อาคารไทยประกันชีวิต ถนนรัชดาภิเษก แขวงดินแดง เขตดินแดง กรุงเทพฯ 10400
Thai Credit Bank Public Company Limited
123 Thai Life Insurance Bldg., Ratchadaphisek Rd., Dindaeng, Bangkok 10400
Tel. (662) 697-5300 Fax. (662) 642-3096
www.thaicreditbank.com

ส่วนที่ 2 บทบาท หน้าที่ ความรับผิดชอบ (Role and Responsibility)

2.1 คณะกรรมการธนาคาร

- พิจารณาอนุมัติการกำหนดนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security Policy) โดยมอบหมายให้คณะเจ้าหน้าที่บริหาร หรือคณะกรรมการที่รับผิดชอบในการบริหารจัดการการรักษาความมั่นคงความปลอดภัยด้านเทคโนโลยีสารสนเทศ พิจารณาเห็นชอบดำเนินการให้เป็นไปตามนโยบายที่กำหนด ภายใต้กรอบอำนาจของคณะกรรมการดังกล่าว

2.2 คณะเจ้าหน้าที่บริหารและคณะกรรมการกำกับความเสี่ยง

- พิจารณาให้ความเห็นชอบการกำหนดนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ เพื่อให้เป็นไปตามแนวปฏิบัติ หลักเกณฑ์ กฎหมายที่เกี่ยวข้อง

2.3 คณะกรรมการ IT Steering

- พิจารณาให้ความเห็นชอบการกำหนดนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ เพื่อให้แน่ใจว่าธนาคารมีการบริหารจัดการการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศได้อย่างมีประสิทธิภาพและเหมาะสม โดยนำเสนอขออนุมัตินโยบายต่อคณะกรรมการธนาคาร
- กำกับดูแลให้มีการกำหนดแนวทางและระเบียบปฏิบัติที่เกี่ยวข้องกับนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ รวมทั้งทบทวนนโยบาย เพื่อให้มีการปฏิบัติเป็นไปตามนโยบายที่กำหนด เหมาะสมกับการดำเนินธุรกิจของธนาคาร

บมจ.ธนาคารไทยเครดิต
123 อาคารไทยประกันชีวิต ถนนรัชดาภิเษก แขวงดินแดง เขตดินแดง กรุงเทพฯ 10400
Thai Credit Bank Public Company Limited
123 Thai Life Insurance Bldg., Ratchadaphisek Rd., Dindaeng Bangkok 10400
Tel. (662) 697-5300 Fax. (662) 642-3095
www.thaicreditbank.com

ส่วนที่ 3 คำนิยาม (Definition)

คำศัพท์	คำอธิบาย
เทคโนโลยีสารสนเทศ	หมายถึง เทคโนโลยีสารสนเทศที่นำมาใช้ในการดำเนินธุรกิจ ซึ่งครอบคลุมถึง ข้อมูล ระบบปฏิบัติการ (Operating System) ระบบงาน (Application System) ระบบฐานข้อมูล (Database System) อุปกรณ์คอมพิวเตอร์ (Hardware) และระบบเครือข่ายสื่อสาร (Communication) เป็นต้น
พนักงาน	หมายถึง พนักงานประจำของธนาคาร กรรมการและผู้บริหารระดับสูง รวมถึงพนักงานที่อยู่ในระหว่างทดลองงาน พนักงานสัญญาจ้าง รวมถึงผู้ให้บริการภายนอก (Outsource) ที่ธนาคารใช้บริการ ต้องมีหน้าที่ในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ให้เป็นไปตามนโยบาย และระเบียบปฏิบัติที่เกี่ยวข้องที่ธนาคารกำหนดขึ้น
ผู้ได้รับสิทธิ	หมายถึง พนักงานที่ได้รับอนุมัติจากผู้มีอำนาจของหน่วยงานให้ใช้งานเทคโนโลยีสารสนเทศ ที่ธนาคารจัดหาให้สำหรับใช้ในการปฏิบัติงานเพื่อรองรับธุรกิจของธนาคาร
ทรัพย์สินสารสนเทศ	- ทรัพย์สินอุปกรณ์ (Hardware Asset) หมายถึง เครื่องคอมพิวเตอร์ เครื่องคอมพิวเตอร์พกพา อุปกรณ์สื่อสาร สื่อจัดเก็บข้อมูล อุปกรณ์ที่สำคัญและจำเป็นสำหรับคอมพิวเตอร์ - ทรัพย์สินซอฟต์แวร์ (Software Asset) หมายถึง โปรแกรมประยุกต์ (Application Software) ซอฟต์แวร์ระบบ(System Software) โปรแกรมอรรถประโยชน์(Utilities) และเครื่องมือที่ใช้ในการพัฒนาและบริหารจัดการ (Development Tools) และอื่นๆ - ทรัพย์สินข้อมูล (Information and Document Asset) หมายถึง ฐานข้อมูล ไฟล์ข้อมูล เอกสารระบบ (System Document) ข้อมูลสารสนเทศ เป็นต้น
ข้อมูล	ข้อมูลธนาคาร ข้อมูลลูกค้า ข้อมูลบริษัทคู่ค้า ข้อมูลพนักงานและข้อมูลอื่นๆ ที่อยู่ในรูปเอกสาร ข้อมูลในระบบงานและระบบเครือข่ายของธนาคาร และข้อมูลที่จัดเก็บในสื่อประเภทต่างๆโดยมีลักษณะข้อมูลเป็นข้อความ (Text) ข้อมูลตัวเลข (Numbers) รูปภาพ (Images) ไฟล์เสียง (Sound) และภาพเคลื่อนไหว (Video)

บมจ.ธนาคารไทยเครดิต
123 อาคารไทยประกันชีวิต ถนนรัชดาภิเษก แขวงดินแดง เขตดินแดง กรุงเทพฯ 10400
Thai Credit Bank Public Company Limited
123 Thai Life Insurance Bldg., Ratchadaphisek Rd., Dindaeng Bangkok 10400
Tel. (662) 697-5300 Fax. (662) 642-3086
www.thaicreditbank.com

คำศัพท์	คำอธิบาย
อีเมล	จดหมายอิเล็กทรอนิกส์ที่ใช้ติดต่อสื่อสารกันในเครือข่ายอินเทอร์เน็ต
เครือข่ายคอมพิวเตอร์เสมือน (Virtual Private Network: VPN)	เครือข่ายคอมพิวเตอร์ที่เสมือนที่มีการใช้เทคโนโลยีการเข้ารหัสในการรับส่งข้อมูลทำให้ข้อมูลมีความมั่นคงปลอดภัยจากการดักจับข้อมูลที่ส่งผ่านเครือข่ายโดยผู้ไม่ประสงค์ดี
การเข้ารหัสข้อมูล (Cryptography)	การใช้อัลกอริทึ่มที่มีความมั่นคงปลอดภัยเข้ารหัสข้อมูล ให้ข้อมูลไม่สามารถเรียกดู หรือถูกดักจับและอ่านข้อมูลนั้นได้ง่าย
ไวรัสคอมพิวเตอร์	โปรแกรมที่สร้างโดยบุคคลผู้ไม่หวังดี เพื่อมุ่งหวังโจมตี บุกรุก ขัดขวาง ก่อกวน สร้างความรำคาญ แก่ผู้ใช้งานระบบสารสนเทศ

บมจ.ธนาคารไทยเครดิต
123 อาคารไทยประกันชีวิต ถนนรัชดาภิเษก แขวงดินแดง เขตดินแดง กรุงเทพฯ 10400
Thai Credit Bank Public Company Limited
123 Thai Life Insurance Bldg., Ratchadaphisek Rd., Dindaeng, Bangkok 10400
Tel. (662) 697-5300 Fax. (662) 642-3095
www.thaicreditbank.com

ส่วนที่ 4 การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security)

1. กำหนดให้พนักงานทุกคนมีหน้าที่ต้องปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ผู้บังคับบัญชาแต่ละหน่วยงานทำหน้าที่รับผิดชอบในการสื่อสารและควบคุมการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ เพื่อให้มั่นใจว่าพนักงานในสังกัดให้ความสำคัญและปฏิบัติตามนโยบายของธนาคาร

2. กำหนดให้ทุกๆ ระบบงานต้องมีการระบุหน่วยงานเจ้าของระบบ โดยหน่วยงานเจ้าของระบบเป็นผู้อนุญาตให้บุคคลที่จำเป็นต้องใช้งาน สามารถเข้าระบบได้ และกำหนดขอบเขตการใช้ ผ่านกระบวนการขอใช้ระบบงาน เพื่อให้มั่นใจว่ามีระบบมีการป้องกันที่เหมาะสม

3. การเข้าใช้งาน การเข้าถึงระบบ (Access) และการใช้ทรัพยากรบนระบบ ต้องอยู่บนพื้นฐานขอบเขตหน้าที่ที่รับผิดชอบ ความจำเป็นต้องใช้งานและต้องได้รับอนุญาตจากเจ้าของระบบ

4. กำหนดให้มีเพียงข้อมูลทางธุรกิจ กฎหมาย ข้อมูลที่จำเป็นต้องใช้ในการปฏิบัติงานให้กับธนาคารเท่านั้นที่สามารถจัดเก็บ ประมวลผลในเครื่องคอมพิวเตอร์ เครื่องแม่ข่าย ระบบคอมพิวเตอร์ และระบบเครือข่ายการสื่อสารของธนาคารได้ โดยมีไว้เพื่อการดำเนินงานของธนาคาร จะต้องเก็บข้อมูลเฉพาะที่เกี่ยวข้องกับการดำเนินธุรกิจของธนาคาร

5. การทำงานกับบุคคลภายนอก (Third Party) จะต้องมีการป้องกันที่เหมาะสม เพื่อให้มั่นใจว่าจะไม่มีผลกระทบต่อนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของธนาคาร และต้องมีการระบุให้ชัดเจนในสัญญาของผู้ให้บริการ ครอบคลุมการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของธนาคารอย่างเคร่งครัด

6. กำหนดให้มีการแบ่งแยกหน้าที่และลักษณะงานอย่างเหมาะสม ตามความจำเป็นในการปฏิบัติงานอยู่ภายใต้กรอบหลักการที่สำคัญ 3 ประการ คือ การรักษาความลับของระบบและข้อมูล ความถูกต้องเชื่อถือได้ของระบบและข้อมูล ความพร้อมใช้งานของเทคโนยีสารสนเทศ

7. เพื่อให้การปฏิบัติเป็นไปตามนโยบาย กำหนดให้มีการออกหลักเกณฑ์ คู่มือ ระเบียบ คำสั่ง ประกาศและบันทึก โดยให้เป็นไปตามระเบียบที่ธนาคารกำหนด

8. ให้พนักงานทุกคนมีหน้าที่ต้องรายงานเหตุการณ์ที่ผิดปกติด้านเทคโนโลยีสารสนเทศ ไปยังหน่วยงานที่เกี่ยวข้อง เช่น แผนกบริหารความเสี่ยงด้านปฏิบัติการ หรือสายงานเทคโนโลยีสารสนเทศ เป็นต้น

9. กำหนดให้คณะกรรมการ IT Steering หรือคณะกรรมการที่ได้รับมอบหมาย ทำหน้าที่พิจารณาให้ความเห็นชอบและอนุมัติการบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของธนาคาร

บมจ.ธนาคารไทยเครดิต
123 อาคารไทยประกันชีวิต ถนนรัชดาภิเษก แขวงดินแดง เขตดินแดง กรุงเทพฯ 10400
Thai Credit Bank Public Company Limited
123 Thai Life Insurance Bldg. Ratchadaphisek Rd., Dindaeng Bangkok 10400
Tel. (662) 697-5300 Fax. (662) 642-3096
www.thaicreditbank.com

การรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ รวมถึงการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยครอบคลุมหัวข้อดังต่อไปนี้

1. โครงสร้างการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Organization of Information Security)
2. ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human Resource Security)
3. การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT Asset Management)
4. การรักษาความมั่นคงปลอดภัยของข้อมูล (Information Security)
5. การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environmental Security)
6. การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร (Communications Security)
7. การควบคุมการเข้าถึง (Access Control)
8. การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT Operations Security)
    - การบริหารจัดการการเปลี่ยนแปลง (Change Management)
    - การบริหารจัดการการตั้งค่าระบบ (System Configuration Management)
    - การบริหารจัดการ patch (Patch Management)
    - การจัดเก็บข้อมูลบันทึกเหตุการณ์ (Logging)
    - การบริหารจัดการขีดความสามารถของระบบ (Capacity Management)
    - การติดตามดูแลระบบและเฝ้าระวังภัยคุกคาม (Security Monitoring)
    - การบริหารจัดการช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Management and Penetration Test)
    - การสำรองข้อมูล (Data Backup)
    - การรักษาความปลอดภัยในอุปกรณ์ที่ใช้ปฏิบัติงาน (Endpoint Security)
9. การจัดหาและการพัฒนาระบบ (System Acquisition and Development)
10. การบริหารจัดการเหตุการณ์ผิดปกติและปัญหาด้านเทคโนโลยีสารสนเทศ (IT Incident and Problem Management)
11. การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (Disaster Recovery Plan:DRP)
12. การบริหารจัดการผู้ให้บริการภายนอก (Third Party Management)
13. การปฏิบัติตามข้อกำหนด (Compliance)
14. การรักษาความปลอดภัยในการใช้ทรัพย์สินสารสนเทศและอุปกรณ์ที่ใช้ในการปฏิบัติงาน และหนังสือยอมรับเงื่อนไขนโยบายการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศสำหรับผู้ใช้งาน (IT Acceptable Use Policy : AUP)

บมจ.ธนาคารไทยเครดิต
123 อาคารไทยประกันชีวิต ถนนรัชดาภิเษก แขวงดินแดง เขตดินแดง กรุงเทพฯ 10400
Thai Credit Bank Public Company Limited
123 Thai Life Insurance Bldg., Ratchadaphisek Rd., Dindaeng, Bangkok 10400
Tel. (662) 697-5300 Fax (662) 642-3096
www.thaicreditbank.com

1. โครงสร้างการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

(Organization of Information Security)

วัตถุประสงค์

เพื่อเป็นแนวทางในการกำหนดกรอบโครงสร้างและการบริหารความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ สอดคล้องกับการแบ่งแยกหน้าที่ความรับผิดชอบในธนาคาร

1. ธนาคารได้จัดทำแผนผังโครงสร้างการบริหารในธนาคาร และกำหนดหน้าที่ความรับผิดชอบของแต่ละตำแหน่ง (Job Description)
2. กำหนดให้คณะกรรมการ IT Steering หรือคณะกรรมการที่ได้รับมอบหมาย ทำหน้าที่บริหารจัดการและดูแลให้มีการใช้เทคโนโลยีที่สอดรับกับกลยุทธ์ในการดำเนินธุรกิจ ดูแลให้การใช้เทคโนโลยีของธนาคารมีความยืดหยุ่นเพียงพอที่จะรองรับการเปลี่ยนแปลงด้านเทคโนโลยีและการดำเนินธุรกิจในอนาคต พร้อมทั้งดูแลให้มีการบริหารความเสี่ยงด้านเทคโนโลยีอย่างเหมาะสม
3. กำหนดให้คณะกรรมการ IT Steering หรือคณะกรรมการที่ได้รับมอบหมาย มีอำนาจหน้าที่บริหารจัดการ พิจารณาแผนงานด้านเทคโนโลยี กำกับดูแลการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ และบริหารความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของธนาคาร
4. กำหนดให้มีการแบ่งแยกหน้าที่และลักษณะงานอย่างเหมาะสม ตามความจำเป็นในการปฏิบัติงานอยู่ภายใต้กรอบหลักการที่สำคัญ 3 ประการ คือ การรักษาความลับของระบบและข้อมูล ความถูกต้องเชื่อถือได้ของระบบและข้อมูล ความพร้อมใช้งานของเทคโนยีสารสนเทศ
5. ธนาคารต้องมีการบริหารจัดการบุคลากรที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ และการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม

บมจ.ธนาคารไทยเครดิต
123 อาคารไทยประกันชีวิต ถนนรัชดาภิเษก แขวงดินแดง เขตดินแดง กรุงเทพฯ 10400
Thai Credit Bank Public Company Limited
123 Thai Life Insurance Bldg., Ratchadaphisek Rd., Dindaeng, Bangkok 10400
Tel. (662) 697-5300 Fax. (662) 642-3096
www.thaicreditbank.com

2. ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human Resource Security)

วัตถุประสงค์

เพื่อกำหนดและคัดสรรบุคคลก่อนที่จะเข้ามาทำงาน เพื่อลดความเสี่ยงจากความผิดพลาด การขโมย การปลอมแปลง และการนำไปใช้ในทางที่ไม่เหมาะสมของพนักงานอันเกิดจากการปฏิบัติงานกับระบบสารสนเทศ และทรัพยากรสารสนเทศอื่นๆ ขององค์กร

1. การตรวจสอบคุณสมบัติของผู้สมัคร (Screening)

- การคัดเลือกพนักงานมาปฏิบัติงานในธนาคารต้องคัดเลือกตามคุณสมบัติของตำแหน่งงานที่กำหนดไว้ในแต่ละตำแหน่ง
- สายงานบริหารทรัพยากรบุคคล ต้องตรวจสอบประวัติความเป็นมาของผู้สมัครงานก่อนการว่าจ้าง โดยระมัดระวังที่จะไม่ละเมิดต่อกฎหมาย ระเบียบ หรือข้อบังคับที่เกี่ยวข้องกับความเป็นส่วนบุคคล การจ้างงาน หรือแรงงาน
- สายงานบริหารทรัพยากรบุคคลต้องตรวจสอบเอกสาร ข้อมูล หรือบุคคลอ้างอิงของผู้สมัครงาน ประวัติการทำงาน การศึกษา คุณสมบัติ ข้อมูลหลักฐานแสดงตนของผู้สมัครงาน บัตรประชาชน ประวัติหนี้สิน ประวัติอาชญากรของผู้สมัครงาน
- ในกรณีที่เป็นการจ้างงานผ่านทางบริษัทจัดหางาน สายงานบริหารทรัพยากรบุคคลและฝ่ายกฎหมายควรตรวจสอบความเหมาะสมของสัญญาการจ้างงาน

2. การกำหนดเงื่อนไขการจ้างงาน (Terms and Conditions of Employment)

- ต้องให้พนักงานใหม่ลงนามในสัญญาการว่าจ้างและสัญญารักษาความลับของธนาคาร
- เพื่อให้การบริหารจัดการบัญชีผู้ใช้ (User ID) เป็นไปอย่างถูกต้องและเป็นปัจจุบันที่สุด สายงานบริหารทรัพยากรบุคคล ต้องแจ้งให้สายงานเทคโนโลยีสารสนเทศทราบ เมื่อมีเหตุดังนี้
  - การว่าจ้างงาน
  - การเปลี่ยนแปลงสภาพการว่าจ้างงาน
  - การลาออกจากงาน หรือการสิ้นสุดการเป็นผู้บริหาร พนักงาน และลูกจ้าง หรือการถึงแก่กรรม
  - การโยกย้ายหน่วยงาน
  - การพักงาน การลงโทษทางวินัย หรือระงับการปฏิบัติหน้าที่

3. การสร้างความตระหนักเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศขณะเป็นพนักงาน (During Employment)

- เมื่อพนักงานมาปฏิบัติงาน ทางหัวหน้างานจะมอบหมายการปฏิบัติงานให้สอดคล้องกับหน้าที่ความรับผิดชอบของแต่ละตำแหน่ง

บมจ.ธนาคารไทยเครดิต
123 อาคารไทยประกันชีวิต ถนนรัชดาภิเษก แขวงดินแดง เขตดินแดง กรุงเทพฯ 10400
Thai Credit Bank Public Company Limited
123 Thai Life Insurance Bldg., Ratchadaphisek Rd., Dindaeng Bangkok 10400
Tel. (662) 697-5300 Fax. (662) 642-3095
www.thaicreditbank.com

- จัดให้มีการอบรมให้ความรู้ สร้างความตระหนักเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security Awareness) และการรักษาความปลอดภัยข้อมูลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล แก่พนักงานใหม่เมื่อเริ่มทำงาน และจัดฝึกอบรมให้แก่พนักงานทุกคน เพื่อให้ความรู้และทำให้เป็นที่แน่ใจว่าพนักงานของธนาคารจะปฏิบัติตามกฎหมาย รวมถึงนโยบายและกระบวนการปฏิบัติงานที่เกี่ยวข้อง อย่างน้อยปีละ 1 ครั้ง
- พนักงานทุกคนมีหน้าที่รับผิดชอบในการดูแลและปกป้องทรัพย์สินสารสนเทศ รวมทั้งข้อมูลของธนาคาร
- พนักงานทุกคนต้องไม่เข้าถึงระบบเทคโนโลยีสารสนเทศของธนาคารโดยไม่ได้รับอนุญาต ต้องไม่ดำเนินการใดๆ ที่ส่งผลกระทบต่อผู้อื่นและระบบงานของธนาคาร จนทำให้ไม่สามารถปฏิบัติงานต่อไปได้หรือทำให้เกิดความเสียหายต่อทรัพย์สินสารสนเทศของธนาคาร
- พนักงานทุกคนมีหน้าที่รับผิดชอบในการรายงานเหตุการณ์ความเสี่ยงหรือเหตุการณ์ความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศที่พบ ไปยังฝ่ายจัดการความเสี่ยง สายงานเทคโนโลยีสารสนเทศ และหน่วยงานที่เกี่ยวข้อง
- การควบคุมระเบียบวินัยนั้น ทางธนาคารมีการกำหนดบทลงโทษทางวินัยสำหรับผู้ที่ฝ่าฝืนนโยบาย กฎ และ/หรือระเบียบปฏิบัติของธนาคาร แต่หากเป็นการละเมิดข้อกฎหมาย บทลงโทษให้เป็นไปตามฐานความผิดที่ได้กระทำตามที่ระบุในแต่ละข้อกฎหมายนั้น

4. การลาออก ยกเลิกการจ้างงาน หรือเปลี่ยนแปลง (Termination / Change of Employment)

- หน่วยงานต้นสังกัดของพนักงาน ให้ดำเนินการยกเลิกหน้าที่ความรับผิดชอบของพนักงาน (Termination Responsibility)
- สายงานบริหารทรัพยากรบุคคลและหน่วยงานต้นสังกัดของพนักงาน ต้องแจ้งให้หน่วยงานที่เกี่ยวข้องทราบ เมื่อมีการลาออก แต่งตั้งโยกย้าย ปลดหรือเปลี่ยนแปลงหน้าที่ความรับผิดชอบของพนักงาน เพื่อทำการปรับปรุง ระงับยกเลิกบัญชีผู้ใช้ และยกเลิกสิทธิ์ในการเข้าถึงระบบและข้อมูล

5. การคืนทรัพย์สิน (Return on Assets)

- พนักงานธนาคารซึ่งพ้นสภาพจากการจ้างงาน ต้องคืนทรัพย์สินของธนาคารทั้งหมดซึ่งเกี่ยวข้องกับระบบงานคอมพิวเตอร์ รวมทั้งกุญแจ บัตรประจำตัวพนักงาน บัตรผ่านเข้า-ออก เครื่องคอมพิวเตอร์ และอุปกรณ์ต่อพ่วง คู่มือ และเอกสารต่างๆ ให้แก่ผู้บังคับบัญชาหรือสายงานเทคโนโลยีสารสนเทศ เมื่อสิ้นสุดหรือพ้นสภาพการเป็นพนักงาน

6. การยกเลิก / ปรับปรุงสิทธิ์การเข้าถึง (Removal or adjustment of access rights)

- เมื่อมีการยกเลิกหรือเปลี่ยนแปลงตำแหน่งการเป็นพนักงานของธนาคาร สายงานบริหารทรัพยากรบุคคลจะต้องแจ้งต่อหน่วยงานที่เกี่ยวข้องทราบ และหน่วยงานต้นสังกัดต้องแจ้งต่อ ลูกค้า บริษัทคู่ค้า ผู้ให้บริการภายนอก ให้รับทราบตามความเหมาะสม เพื่อระงับหรือยกเลิกการเข้าถึงข้อมูลต่างๆ ของพนักงาน

บมจ.ธนาคารไทยเครดิต
123 อาคารไทยประกันชีวิต ถนนรัชดาภิเษก แขวงดินแดง เขตดินแดง กรุงเทพฯ 10400
Thai Credit Bank Public Company Limited
123 Thai Life Insurance Bldg. Ratchadaphisek Rd., Dindaeng Bangkok 10400
Tel. (662) 697-5300 Fax. (662) 642-3096
www.thaicreditbank.com

3. การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT Asset Management)

วัตถุประสงค์

เพื่อให้ธนาคารมีการจัดทำทะเบียนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศอย่างครบถ้วนและควบคุมดูแลทรัพย์สินด้านเทคโนโลยีสารสนเทศให้มีความพร้อมใช้งาน และสามารถรองรับการดำเนินธุรกิจได้อย่างต่อเนื่อง

1. กำหนดมาตรฐานและระเบียบวิธีปฏิบัติการบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ ครอบคลุมการจัดทำทะเบียนรายการทรัพย์สิน การปรับปรุงทะเบียนรายการทรัพย์สิน การยกเลิกและเรียกคืนทรัพย์สิน
2. ความเป็นเจ้าของทรัพย์สิน (Owner of Assets)
   - จัดให้มีหน่วยงานผู้รับผิดชอบในการจัดทำปรับปรุงทะเบียนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศ และบำรุงรักษาทรัพย์สินด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม รวมทั้งวางแผนรองรับทรัพย์สินด้านเทคโนโลยีสารสนเทศที่ใกล้จะสิ้นสุดตามอายุการใช้งาน (end of life) หรือสิ้นสุดการให้บริการ (End of support)
3. ทะเบียนทรัพย์สินด้านเทคโนโลยีสารสนเทศ (Inventory of Assets)
   - มีการจัดทำทะเบียนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT inventory list) ของฮาร์ดแวร์ (Hardware) และซอฟต์แวร์ (Software) ที่รองรับระบบเทคโนโลยีสารสนเทศของธนาคาร เพื่อนำมาประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศและดำเนินการในการบริหารจัดการความเสี่ยง กำหนดแนวทางการรักษาความปลอดภัยด้านเทคโนโลยีได้อย่างเหมาะสม
   - มีการปรับปรุงทะเบียนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศให้เป็นปัจจุบันอย่างต่อเนื่องอย่างน้อยปีละ 1 ครั้ง
4. การยกเลิกและเรียกคืนทรัพย์สิน (Return Asset)
   - เมื่อสิ้นสุดการใช้งาน ครอบคลุมทั้งทรัพย์สินด้านเทคโนโลยีสารสนเทศที่ใช้งานภายในธนาคาร และกรณีที่ผู้ให้บริการภายนอกมีการใช้งานทรัพย์สินของธนาคารทันทีที่มีการยกเลิกสัญญาจ้างด้วย
   - กรณีที่พนักงานพ้นสภาพจากการจ้างงาน ต้องคืนทรัพย์สินทั้งหมดซึ่งเกี่ยวข้องกับระบบงานคอมพิวเตอร์ รวมทั้งกุญแจ บัตรประจำตัวพนักงาน บัตรผ่านเข้า-ออก เครื่องคอมพิวเตอร์ และอุปกรณ์ต่อพ่วง คู่มือ และเอกสารต่างๆ ให้แก่ผู้บังคับบัญชาเมื่อพ้นสภาพการเป็นพนักงาน
   - กรณีที่ธนาคารได้จัดเตรียมอุปกรณ์ให้ผู้ให้บริการภายนอก (Vendor/Outsource) ระหว่างการปฏิบัติงานแก่ธนาคาร ต้องมีการคืนทรัพย์สินทุกครั้งเมื่อสิ้นสุดการปฏิบัติงานหรือยกเลิกสัญญาจ้าง

บมจ.ธนาคารไทยเครดิต
123 อาคารไทยประกันชีวิต ถนนรัชดาภิเษก แขวงดินแดง เขตดินแดง กรุงเทพฯ 10400
Thai Credit Bank Public Company Limited
123 Thai Life Insurance Bldg. Ratchadaphisek Rd. Dindaeng Bangkok 10400
Tel. (662) 697-5300 Fax. (662) 642-3096
www.thaicreditbank.com

4. การรักษาความมั่นคงปลอดภัยของข้อมูล (Information Security)

วัตถุประสงค์

เพื่อให้ธนาคารมีการรักษาความมั่นคงปลอดภัยและความลับของข้อมูล ครอบคลุมการรับส่งข้อมูลผ่านเครือข่ายสื่อสาร การจัดเก็บหรือใช้งานบนระบบและสื่อบันทึกข้อมูลต่างๆ

การรักษาความมั่นคงปลอดภัยของข้อมูล (Information Security)

1. หลักเกณฑ์การจัดชั้นความลับของข้อมูล (Information Classification) ให้ดำเนินการตามนโยบายของธนาคาร เรื่องการจัดชั้นข้อมูล (Data Classification Policy)
2. กำหนดให้มีเจ้าของข้อมูล (Information Owner) รับผิดชอบในการกำหนดผู้ใช้งาน สิทธิ์การเข้าถึงและการใช้งานข้อมูลอย่างปลอดภัย
3. กำหนดแนวทางการรักษาความมั่นคงปลอดภัยของข้อมูล สอดคล้องตามหลักเกณฑ์การจัดชั้นความลับของข้อมูล
   - ข้อมูลที่อยู่บนอุปกรณ์ที่ใช้ปฏิบัติงาน (Data at endpoint) ให้มีการเข้ารหัสข้อมูลที่อยู่อุปกรณ์ พิจารณาจากเกณฑ์การประเมินความเสี่ยงและหลักเกณฑ์การจัดชั้นความลับของข้อมูล ด้วยเครื่องมือที่เหมาะสมในการดำเนินการ
   - ข้อมูลที่อยู่ระหว่างการรับส่งผ่านเครือข่าย (Data in transit) ต้องมีการออกแบบและดำเนินการให้มีการรับส่งข้อมูลผ่านเครือข่ายที่มีความปลอดภัย
   - ข้อมูลที่อยู่บนระบบงานและสื่อบันทึกข้อมูล (Data at rest) ให้มีการออกแบบและดำเนินการให้มั่นใจว่าข้อมูลถูกจัดเก็บอย่างปลอดภัย มีการกำหนดสิทธิ์ในการเข้าใช้งานอย่างเหมาะสม
4. การจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ (Management of removable media)
   - สื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ (Removable Media) ที่นำมาใช้งานภายในธนาคารต้องได้รับการอนุมัติตามนโยบายที่ธนาคารกำหนด
   - การนำข้อมูลออกจากธนาคาร ต้องดำเนินการตามหลักเกณฑ์การจัดชั้นความลับของข้อมูล (Information Classification) ทั้งการระบุชั้นข้อมูล (Labeling) และวิธีการจัดส่งข้อมูล
   - ห้ามนำสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ มาเชื่อมต่อโดยตรงกับเครื่องแม่ข่ายหรืออุปกรณ์ เว้นแต่ได้รับอนุญาตจากผู้มีอำนาจอนุมัติ และต้องดำเนินการตรวจเช็คไวรัสก่อนการเชื่อมต่อระบบ
5. การควบคุมดูแลรักษาความปลอดภัยสื่อบันทึกข้อมูลระหว่างขนส่ง (Physical Media Transfer)
   - ต้องดำเนินการตามหลักเกณฑ์การจัดชั้นความลับของข้อมูล เพื่อให้มีการควบคุมการเข้าถึงสื่อที่มีข้อมูลสำคัญในระหว่างการขนส่ง
   - จัดเก็บในบรรจุภัณฑ์ที่ปิดมิดชิด มีการล็อกป้องกันการเข้าถึงและป้องกันความเสียหายได้

บมจ.ธนาคารไทยเครดิต
123 อาคารไทยประกันชีวิต ถนนรัชดาภิเษก แขวงดินแดง เขตดินแดง กรุงเทพฯ 10400
Thai Credit Bank Public Company Limited
123 Thai Life Insurance Bldg., Ratchadaphisek Rd., Dindaeng Bangkok 10400
Tel. (662) 697-5300 Fax. (662) 642-3095
www.thaicreditbank.com

6. การทำลายข้อมูล (Information Disposal)
   - กำหนดมาตรฐานและระเบียบวิธีปฏิบัติการทำลายข้อมูล (Information Disposal)
   - พิจารณาวิธีการทำลายข้อมูลให้สอดคล้องตามหลักเกณฑ์การจัดชั้นความลับของข้อมูล โดยมีกระบวนการควบคุมการทำลายข้อมูล ที่ครอบคลุมการอนุมัติจากหน่วยงานเจ้าของข้อมูล หรือผู้มีอำนาจอนุมัติก่อนดำเนินการ
   - จัดให้มีการทำลายข้อมูลก่อนทุกครั้งเมื่อมีการยุติหรือยกเลิกการใช้งาน เช่น หมดอายุเสื่อมสภาพ หรือหมดสัญญาส่งคืน หรือถ่ายโอน หรือบริจาค หรือจัดจำหน่ายต่อ หรือไม่ใช้งานแล้ว
   - การทำลายข้อมูลในสื่อสำรองบันทึกข้อมูลด้านเทคโนโลยีสารสนเทศ ที่มีอายุใช้งานเกิน 10 ปี หรือตามที่กฎหมายกำหนด

การบริหารจัดการแลกเปลี่ยนข้อมูลและการเข้ารหัสข้อมูล (information Transfer and Cryptography)

7. การเข้ารหัสข้อมูล ให้ปฏิบัติตามหลักเกณฑ์การจัดชั้นความลับของข้อมูล (Information Classification) ของนโยบายธนาคาร เรื่อง การจัดชั้นข้อมูล (Data Classification Policy)
8. กรณีที่มีการส่งข้อมูลที่เป็นความลับหรือความสำคัญผ่านช่องทางอิเล็กทรอนิกส์ หรือเคลื่อนย้ายสื่อบันทึกข้อมูลที่มีความสำคัญ ผู้รับผิดชอบต้องดำเนินการเข้ารหัสข้อมูล เพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงข้อมูลได้
9. การส่งข้อมูลสำคัญกับภายนอก ต้องกำหนดให้มีการเข้ารหัสข้อมูลสำคัญและช่องทางการสื่อสารที่ใช้รับส่งข้อมูลสำคัญกับภายนอกเป็นอย่างน้อย และได้รับการอนุมัติจากหน่วยงานเจ้าของข้อมูล
10. วิธีการเข้ารหัสข้อมูล ควรใช้มาตรฐานการเข้ารหัสข้อมูลที่เชื่อถือได้และเป็นมาตรฐานสากล เช่น การเข้ารหัสข้อมูลแบบสมมาตร (เช่น AES) การเข้ารหัสข้อมูลแบบอสมมาตร (เช่น Public Key Cryptography) เป็นต้น โดยมีการทบทวนประสิทธิภาพของวิธีการเข้ารหัสข้อมูลอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าวิธีการเข้ารหัสข้อมูลที่ใช้งานยังคงมีความแข็งแรงเพียงพอ
11. กำหนดให้มีกระบวนการบริหารจัดการกุญแจเข้ารหัสข้อมูล (Key Management) ที่มีความรัดกุมปลอดภัย
12. ในระบบงานที่ความเสี่ยงสูงและมีการเชื่อมต่อกับเครือข่ายสาธารณะ (Internet Facing) กำหนดให้ใช้อุปกรณ์รักษาความปลอดภัย HSM หรืออุปกรณ์ที่ทำหน้าที่ในลักษณะเดียวกันในการรักษาความปลอดภัยของกุญแจเข้ารหัสข้อมูลทั้งด้าน Physical และ Logical

บมจ.ธนาคารไทยเครดิต
123 อาคารไทยประกันชีวิต ถนนรัชดาภิเษก แขวงดินแดง เขตดินแดง กรุงเทพฯ 10400
Thai Credit Bank Public Company Limited
123 Thai Life Insurance Bldg. Ratchadaphisek Rd., Dindaeng, Bangkok 10400
Tel. (662) 697-5300 Fax. (662) 642-3095
www.thaicreditbank.com

5. การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม

(Physical and Environmental Security)

วัตถุประสงค์

เพื่อให้ธนาคารมีการรักษาความมั่นคงปลอดภัยและความพร้อมใช้งานของศูนย์คอมพิวเตอร์ และพื้นที่สำคัญที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศเพียงพอรองรับธุรกิจอย่างต่อเนื่อง

การเข้าถึงศูนย์คอมพิวเตอร์ และพื้นที่สำคัญ

1. ธนาคารมีการควบคุมทางกายภาพและมีระบบควบคุมการเข้าถึงตัวอาคารศูนย์คอมพิวเตอร์หลัก (ศูนย์ฯ) และพื้นที่สำคัญต่างๆ ให้เข้าถึงได้เฉพาะบุคคลที่ได้รับอนุญาตตามสิทธิ์ที่ได้รับมอบหมายเท่านั้น
2. ศูนย์คอมพิวเตอร์อยู่ในบริเวณที่ล้อมรอบด้วยกำแพงที่แข็งแรงสามารถทนความร้อน ประตูทางเข้าต้องล็อคเสมอ และอยู่ในอุณหภูมิที่กำหนด มีระบบกระแสไฟฟ้าสำรอง มีระบบป้องกันอัคคีภัย มีระบบตรวจจับควันไฟ และมีระบบตรวจจับน้ำรั่วซึม
3. กำหนดให้แยกพื้นที่ศูนย์คอมพิวเตอร์สำหรับระบบเทคโนโลยีสารสนเทศของธนาคาร ออกจากพื้นที่ของการปฏิบัติงานทั่วไป โดยกำหนดให้มีระบบ Access Control เพื่อใช้ในการพิสูจน์ตัวตนของผู้เข้าออกพื้นที่สำคัญภายในศูนย์ฯ
4. กำหนดให้มีการติดตั้งกล้องวงจรปิด และทำการบันทึกเหตุการณ์ต่างๆ ตลอด 24 ชั่วโมง โดยมีการจัดเก็บ Log ย้อนหลังเป็นระยะเวลาอย่างน้อย 90 วัน หรือตามกฎหมายที่เกี่ยวข้องกำหนด
5. กำหนดให้มีการป้องกันการบุกรุกของบุคคลภายนอกผ่านทางประตูหนีไฟ โดยให้ทำการล็อคประตูตลอดเวลา
6. กำหนดให้มีการตรวจสอบประตูหนีไฟอย่างสม่ำเสมอ เพื่อให้แน่ใจว่าสามารถใช้งานได้ตามปกติ
7. ศูนย์คอมพิวเตอร์ต้องกำหนดให้มีการควบคุมการเข้า-ออก และให้สิทธิเฉพาะหน่วยงานที่เกี่ยวข้องโดยผ่านขั้นตอนการอนุมัติจากผู้มีอำนาจอนุมัติ
8. กำหนดให้มีการทบทวน หรือยกเลิกสิทธิการเข้าถึงพื้นที่หรือบริเวณที่สำคัญอย่างน้อยปีละ 2 ครั้ง และกรณีที่พนักงานลาออกหรือมีการโยกย้ายให้ดำเนินการยกเลิกทันที
9. กำหนดให้เครื่องแม่ข่ายและอุปกรณ์เครือข่ายต่างๆ ให้จัดวางในตู้ Rack และล็อคกุญแจเสมอ
10. การนำอุปกรณ์เข้ามาติดตั้ง หรือนำอุปกรณ์ออกจากพื้นที่ปฏิบัติงาน ต้องได้รับการอนุญาตจากผู้มีอำนาจอนุมัติ และห้ามเชื่อมต่ออุปกรณ์อื่นใด โดยไม่ได้รับอนุญาต

บมจ.ธนาคารไทยเครดิต
123 อาคารไทยประกันชีวิต ถนนรัชดาภิเษก แขวงดินแดง เขตดินแดง กรุงเทพฯ 10400
Thai Credit Bank Public Company Limited
123 Thai Life Insurance Bldg. Ratchadaphisek Rd. Dindaeng Bangkok 10400
Tel. (662) 697-5300 Fax. (662) 642-3096 www.thaicreditbank.com

11. กำหนดให้มีการบำรุงรักษาอุปกรณ์ภายในศูนย์ฯ ตามรอบระยะเวลา และจัดเก็บบันทึกปัญหาข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว
12. ห้ามไม่ให้นำอุปกรณ์คอมพิวเตอร์ หรืออุปกรณ์ที่สามารถบันทึกภาพ/เสียงได้ เข้ามาภายในศูนย์ฯ และพื้นที่สำคัญ เว้นแต่จะได้รับอนุญาตโดยผู้ที่มีอำนาจอนุมัติ
13. กำหนดให้มีมาตรการควบคุมการส่งอุปกรณ์ไปซ่อมแซมนอกสถานที่ เพื่อป้องกันการสูญหายหรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
14. การเข้าถึงโดยพนักงานที่ไม่ได้มีหน้าที่ปฏิบัติงานประจำภายในศูนย์ฯ หรือบุคคลภายนอกมีกระบวนการในการควบคุมการเข้าถึงแบบชั่วคราว ดังนี้
    - มีการอนุมัติโดยผู้มีอำนาจอนุมัติก่อนทุกครั้ง
    - มีการมอบหมายให้มีเจ้าหน้าที่ศูนย์ฯ ติดตาม (Escort) ผู้เข้าถึงแบบชั่วคราวตลอดระยะเวลาที่เข้ามาปฏิบัติงานภายในศูนย์ฯ
    - จัดทำทะเบียนคุมสำหรับลงบันทึก วันและเวลาการเข้า-ออกพื้นที่สำคัญ และวัตถุประสงค์ของผู้ที่มาเยือน (Visitor)

การเข้าถึงสำนักงาน (Office Access)

15. กำหนดให้มีเจ้าหน้าที่รักษาความปลอดภัย และไม่อนุญาตให้บุคคลภายนอกเข้ามายังส่วนสำนักงานเพื่อความปลอดภัยของทรัพย์สินของธนาคาร
16. กำหนดให้บุคคลภายนอกที่มาติดต่อพนักงานในส่วนของสำนักงาน ต้องนำบัตรประชาชนแลกบัตร "Visitor" และติดบัตรให้เห็นพร้อมลงบันทึกเวลาเข้าออกและรายละเอียด ผู้ที่มาติดต่อ แผนก/ชั้น เรื่องที่มาติดต่อ
17. กำหนดให้ที่หน้าประตูแต่ละชั้นต้องติดตั้งระบบ Access Control ประตูควรปิดเสมอ มีการแจ้งเตือนหรือส่งเสียง Alarm เมื่อประตูถูกเปิดออกเป็นเวลานาน
18. สำนักงาน (Office) ควรติดกล้องวงจรปิด และทำการบันทึกเหตุการณ์ต่างๆ ตลอด 24 ชั่วโมง ที่ประตูเข้า-ออก

บมจ.ธนาคารไทยเครดิต
123 อาคารไทยประกันชีวิต ถนนรัชดาภิเษก แขวงดินแดง เขตดินแดง กรุงเทพฯ 10400
Thai Credit Bank Public Company Limited
123 Thai Life Insurance Bldg. Ratchadaphisek Rd., Dindaeng Bangkok 10400
Tel. (662) 697-5300 Fax. (662) 642-3095
www.thaicreditbank.com

6. การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร (Communications Security)

วัตถุประสงค์

เพื่อให้ธนาคารมีโครงสร้างของระบบเครือข่ายสื่อสารที่มั่นคงปลอดภัย มีการออกแบบระบบเครือข่ายสื่อสารที่เหมาะสม และมีการป้องกันหรือเฝ้าระวังการบุกรุกหรือภัยคุกคามในรูปแบบต่างๆ

การรักษาความปลอดภัยระบบเครือข่าย (Network Security Management)

1. มีการจัดแบ่งเครือข่ายอย่างเหมาะสม โดยคำนึงถึงระดับความสำคัญของระบบงาน ระดับความสำคัญของข้อมูลที่ถูกประมวลผล รวมถึงความจำเป็นในการเชื่อมต่อจากระบบงานอื่นๆ หรือจากภายนอกองค์กร และจัดให้มีการควบคุมการเชื่อมต่อจากระบบงานต่างๆ มายังระบบงานที่มีความสำคัญอย่างเข้มงวด
2. มีการแบ่งแยกเครือข่ายส่วนที่เป็น Private Network และ Public Network ออกจากกัน
3. มีการจัดตั้งโซนเครือข่าย Demilitarized Zone (DMZ) เพื่อรองรับระบบงานที่ต้องมีการให้บริการติดต่อสื่อสาร หรือแลกเปลี่ยนข้อมูลกับภายนอก เช่น ระบบงาน Internet Banking ระบบงาน E-mail เป็นต้น โดยไม่จัดวาง Server ที่เป็นระบบฐานข้อมูลสำคัญไว้ในโซนดังกล่าว
4. ในจุดที่มีการแบ่งแยกเครือข่ายที่พิจารณาว่ามีความสำคัญและมีความเสี่ยง ควรติดตั้งอุปกรณ์รักษาความปลอดภัยเครือข่ายที่มีความสามารถในการควบคุม คัดกรอง Traffic และการเข้าถึงเว็บไซต์ที่ส่งผ่านระบบเครือข่าย การเฝ้าระวังการบุกรุก การป้องกันการบุกรุก และการตรวจจับไวรัสหรือมัลแวร์ต่างๆ ที่อาจบุกรุกเข้าสู่เครือข่าย
5. มีการจำกัดให้เฉพาะบุคคลที่ได้รับมอบอำนาจเท่านั้นที่สามารถเข้าถึงระบบเครือข่าย โดยจำกัดสิทธิ์ในการเข้าถึงระบบเครือข่ายให้อยู่ในส่วนที่มีความจำเป็น และเหมาะสมตามหน้าที่การทำงานเท่านั้น
6. การเปลี่ยนแปลงติดตั้งค่าต่างๆ ที่เกี่ยวกับอุปกรณ์เครือข่าย และอุปกรณ์รักษาความปลอดภัยเครือข่าย การเปลี่ยนแปลงต้องผ่านกระบวนการบริหารจัดการการเปลี่ยนแปลงการตั้งค่าอุปกรณ์เครือข่าย และอุปกรณ์รักษาความปลอดภัยเครือข่ายอย่างเป็นขั้นตอน พร้อมทั้งได้รับการอนุมัติดำเนินการจากผู้มีอำนาจอนุมัติ
7. มีการเปลี่ยน Default Password ของอุปกรณ์เครือข่าย และอุปกรณ์รักษาความปลอดภัยเครือข่ายให้เป็นไปตามนโยบายรหัสผ่าน
8. มีการพิจารณาติดตั้ง Software Updates/ Patch อย่างเหมาะสมแก่อุปกรณ์เครือข่ายและอุปกรณ์รักษาความปลอดภัยเครือข่าย ตามคำแนะนำของผู้ผลิต โดยการติดตั้งต้องผ่านกระบวนการบริหารจัดการการเปลี่ยนแปลง (Change Management) อย่างเป็นขั้นตอน

บมจ.ธนาคารไทยเครดิต
123 อาคารไทยประกันชีวิต ถนนรัชดาภิเษก แขวงดินแดง เขตดินแดง กรุงเทพฯ 10400
Thai Credit Bank Public Company Limited
123 Thai Life Insurance Bldg., Ratchadaphisek Rd., Dindaeng, Bangkok 10400
Tel. (662) 697-5300 Fax. (662) 642-3096
www.thaicreditbank.com

9. มีการใช้ระบบในการควบคุมค่าเวลาของเครื่องประมวลผล ให้ตรงกับเครื่องเซิร์ฟเวอร์ NTP (Clock Synchronization) เพื่อให้ค่าเวลาในการบันทึกเหตุการณ์ (Log) มีความถูกต้องในลักษณะ Real-Time ซึ่งเซิร์ฟเวอร์ NTP ต้องรับสัญญาณนาฬิกาจากสถาบันที่มีความน่าเชื่อถือ ยกตัวอย่างเช่น กรมอุทกศาสตร์ (กองทัพเรือ) หรือ สถาบันมาตรวิทยา (กระทรวงวิทยาศาสตร์และเทคโนโลยี)
10. สำหรับระบบงานที่ต้องมีการติดต่อสื่อสาร หรือแลกเปลี่ยนข้อมูลผ่านระบบ Internet ควรมีกระบวนการประเมินช่องโหว่ (Vulnerability Assessment) และทดสอบเจาะระบบเครือข่าย (Network Penetration Test) โดยผู้เชี่ยวชาญอย่างน้อยปีละครั้ง และ/หรือทุกครั้งที่มีการเปลี่ยนแปลงค่าความปลอดภัย หรือมีการเปลี่ยนแปลงความเสี่ยงทางเทคโนโลยีที่มีนัยสำคัญ รวมทั้งควรจะมีการพิจารณาตามความเหมาะสม

การควบคุมการเชื่อมต่อกับระบบเครือข่ายสื่อสารของธนาคาร

11. ไม่นำเครื่องคอมพิวเตอร์ หรืออุปกรณ์อื่นใด ที่ธนาคารมิได้จัดหาให้มาเชื่อมต่อและใช้งานในระบบเครือข่ายสื่อสารของธนาคาร เว้นแต่ได้รับการพิจารณาอนุมัติจากหน่วยงานต้นสังกัด และผู้มีอำนาจอนุมัติของสายงานเทคโนโลยีสารสนเทศ เป็นกรณีๆ ไป
12. การใช้งานการเชื่อมต่อเครือข่ายของธนาคาร ต้องใช้หมายเลข IP Address ที่ผู้ดูแลระบบกำหนดให้เท่านั้น
13. เครื่องคอมพิวเตอร์ หรืออุปกรณ์อื่นใด ที่มีการเชื่อมต่อกับระบบเครือข่ายของธนาคาร ต้องดำเนินการผ่านการควบคุมโดยระบบรักษาความปลอดภัยเครือข่ายของธนาคาร
14. กำหนดให้มีวิธีการพิสูจน์ตัวตนสำหรับเครื่องคอมพิวเตอร์ ก่อนที่จะอนุญาตให้เข้ามาใช้งานเครือข่ายของธนาคาร

การควบคุมการการเชื่อมต่อมาจากเครือข่ายจากระยะไกล (Remote Access)

15. กรณีที่ต้องมีการเชื่อมต่อมาจากเครือข่ายจากระยะไกล (Remote Access) เพื่อทำการแก้ไขและ/หรือตั้งค่าพารามิเตอร์ของเครื่องแม่ข่าย อุปกรณ์เครือข่าย หรือโปรแกรมระบบงาน ควรมีการระบุตัวตนและพิสูจน์ตัวตนของบุคคลในลักษณะ Two-Factors Authentication และกระทำผ่านช่องทางที่มีความปลอดภัย เช่น SSH, VPN หรือ SSL/TLS เป็นต้น
16. ห้ามทำการเชื่อมต่อเพื่อเข้าถึงระบบเครือข่ายภายในองค์กรจากระยะไกลด้วยเครื่องคอมพิวเตอร์สาธารณะ เช่น เครื่องคอมพิวเตอร์ในร้านอินเตอร์เน็ตคาเฟ่ เป็นต้น
17. ในการเข้าถึงระบบจากระยะไกล ห้ามใช้บริการเครือข่ายหรือโปรโตคอลที่ไม่มั่นคงปลอดภัย เช่น Telnet, FTP, NFS, Terminal services เป็นต้น ในกรณีที่จำเป็น ต้องมีการควบคุมโดยจำกัดโซนในการเข้าถึง และการกำหนดสิทธิในการใช้งาน

บมจ.ธนาคารไทยเครดิต
123 อาคารไทยประกันชีวิต ถนนรัชดาภิเษก แขวงดินแดง เขตดินแดง กรุงเทพฯ 10400
Thai Credit Bank Public Company Limited
123 Thai Life Insurance Bldg., Ratchadaphisek Rd., Dindaeng Bangkok 10400
Tel. (662) 697-5300 Fax. (662) 642-3096
www.thaicreditbank.com

การควบคุมการเชื่อมต่อกับระบบไร้สาย (Wireless LAN)

18. กำหนดให้มีวิธีการในการพิสูจน์ตัวตนและการเข้ารหัสข้อมูลที่ปลอดภัยตามมาตรฐานสากล สำหรับระบบเครือข่ายไร้สายของธนาคาร
19. มีอุปกรณ์ป้องกันเครือข่ายติดตั้งไว้ในระบบเครือข่ายไร้สาย เพื่อป้องกันการเข้าถึงเครือข่ายภายในของธนาคารและจำกัดการติดต่อสื่อสารที่ไม่ได้รับอนุญาต (Unauthorized Traffic)
20. กำหนดให้มีแยกเครือข่ายไร้สายสำหรับบุคคลภายนอกออกจากระบบเครือข่ายภายในของธนาคารออกจากกันอย่างชัดเจน
21. กำหนดให้ทำการปิดฟังก์ชั่น Wireless LAN ของเครื่องคอมพิวเตอร์ทุกเครื่อง หากคอมพิวเตอร์เครื่องใดที่มีความจำเป็นต้องเปิดใช้บริการฟังก์ชั่น Wireless LAN ให้ดำเนินการดังนี้
    - ต้องได้รับการพิจารณาอนุมัติจากหน่วยงานต้นสังกัด และผู้มีอำนาจอนุมัติของสายงานเทคโนโลยีสารสนเทศ เป็นกรณีๆ ไป
    - ต้องใช้มาตรฐานความปลอดภัยที่น่าเชื่อถือได้และเป็นปัจจุบันตามมาตรฐานสากล
    - ห้ามทำการเชื่อมต่อเพื่อเข้าถึงระบบเครือข่ายสาธารณะที่ไม่มีการรักษาความปลอดภัย

บมจ.ธนาคารไทยเครดิต
123 อาคารไทยประกันชีวิต ถนนเรืองดำเนินกลาง แขวงดินแดง เขตดินแดง กรุงเทพฯ 10400
Thai Credit Bank Public Company Limited
123 Thai Life Insurance Bldg., Ratchadaphisek Rd., Dindaeng Bangkok 10400
Tel. (662) 697-5300 Fax. (662) 642-3096
www.thaicreditbank.com

7. การควบคุมการเข้าถึง (Access Control)

วัตถุประสงค์

เพื่อให้ธนาคารมีการบริหารจัดการบัญชีสิทธิ์สูงและสิทธิ์ของผู้ใช้งานมีประสิทธิภาพเป็นไปตามหลักความจำเป็นของการใช้งานและสอดคล้องกับหลักการแบ่งแยกงานด้านเทคโนโลยีสารสนเทศที่ดี โดยสามารถป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

1. การบริหารจัดการบัญชีผู้ใช้ระบบ (User Access Management)

- กำหนดให้มีกระบวนการมาตรฐานในการเพิ่ม เปลี่ยนแปลง และลบ บัญชีผู้ใช้รวมถึงสิทธิ์ของผู้ใช้
- มีหน่วยงานที่รับผิดชอบในการจัดการเพิ่ม เปลี่ยนแปลง และลบ บัญชีผู้ใช้รวมถึงสิทธิ์ของผู้ใช้
- ในการเข้าใช้ระบบงานทุกครั้ง จะต้องมีการระบุตัวตนและพิสูจน์ตัวตนด้วยวิธีการที่เหมาะสม เช่น การใช้บัญชีผู้ใช้ (User ID) และรหัสผ่าน (Password) โดยจำกัดให้เฉพาะบุคคลที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงได้
- ในระบบงานที่มีความสำคัญอย่างยิ่ง ควรมีการจัดทำตารางควบคุมการให้สิทธิ์ (Authorization Matrix) ที่สอดคล้องกับตำแหน่งหน้าที่งาน ตามหลักการตามความจำเป็นของหน้าที่รับผิดชอบ
- กำหนดให้มีขั้นตอนการร้องสิทธิการเข้าใช้ระบบและมีการอนุมัติโดยผู้ที่มีอำนาจอนุมัติทุกครั้งที่มีการเพิ่ม ยกเลิก และ/หรือ เปลี่ยนแปลง ทั้งบัญชีผู้ใช้และสิทธิ์ของผู้ใช้
- เมื่อมีพนักงานลาออกจากงานหรือเปลี่ยนหน้าที่ความรับผิดชอบ กำหนดให้หน่วยงานต้นสังกัดและสายงานบริหารทรัพยากรบุคคล ต้องแจ้งสายงานเทคโนโลยีสารสนเทศทราบ เพื่อทำการปรับปรุง/ยกเลิกบัญชีผู้ใช้
- สำหรับระบบงานที่มีความสำคัญอย่างยิ่ง จัดให้มีการสอบทานบัญชีผู้ใช้และทบทวนสิทธิในการเข้าถึงระบบของพนักงาน (Review of user access rights) อย่างน้อยปีละ 2 ครั้ง สำหรับระบบงานอื่นๆ ให้พิจารณาดำเนินการตามรอบระยะเวลาที่เหมาะสม

2. การบริหารจัดการรหัสผ่าน (Password Management)

- รหัสผ่านควรมีความยาวไม่น้อยกว่า 8 ตัวอักษร
- รหัสผ่านควรประกอบด้วยตัวเลข ตัวอักษรใหญ่ อักษรเล็ก และ/หรือตัวอักขระพิเศษ
- กำหนดให้พนักงานทำการเปลี่ยนรหัสผ่านทุกๆ เดือน หรือทุก 30 วัน ไม่ควรใช้ชื่อที่เดาได้ง่าย เช่น ชื่อเล่น วันเดือนปีเกิด นามสกุล ทะเบียนรถยนต์ เป็นต้น
- รหัสผ่านถูกระงับการใช้ (Account Lock) เมื่อมีการใส่ผิด 3 ครั้งติดกัน
- รหัสผ่านไม่ควรซ้ำกับรหัสผ่านเดิมที่ใช้ 12 ครั้งที่ผ่านมา

บมจ.ธนาคารไทยเครดิต
123 อาคารไทยประกันชีวิต ถนนรัชดาภิเษก แขวงดินแดง เขตดินแดง กรุงเทพฯ 10400
Thai Credit Bank Public Company Limited
123 Thai Life Insurance Bldg., Ratchadaphisek Rd., Dindaeng Bangkok 10400
Tel. (662) 697-5300 Fax. (662) 642-3096
www.thaicreditbank.com

- เมื่อทำการเปลี่ยนรหัสผ่าน ต้องใช้รหัสผ่านดังกล่าวอย่างน้อย 14 วัน จึงจะเปลี่ยนรหัสผ่านได้อีกครั้ง
- ต้องป้องกันรหัสผ่านไม่ให้ผู้อื่นทราบ และห้ามใช้รหัสผ่านร่วมกันกับผู้อื่น
- รหัสผ่านทุกตัวถือเป็นข้อมูลประเภท "Secret"

3. การบริหารจัดการเข้าถึงระบบงาน (System and application access control)

- การบริหารสิทธิการเข้าถึงระบบของผู้มีหน้าที่ดูแลระบบงานประมวลผลหลัก ต้องมีการกำหนดสิทธิและแบ่งแยกหน้าที่ในการทำงานตามความจำเป็นและความเหมาะสม เพื่อไม่ให้บุคคลใดบุคคลหนึ่งปฏิบัติงานได้ตั้งแต่ต้นจนจบกระบวนการ
- มีการระงับหรือยกเลิก Default Account ที่ไม่มีความจำเป็นในการใช้งานหรือไม่มีความจำเป็นต่อการทำงานของระบบ เช่น Guest Accounts เป็นต้น
- มีการเปลี่ยน Default Password ของบัญชีผู้ใช้ที่มากับระบบงานให้เป็นไปตามมาตรฐานหรือนโยบายการบริหารจัดการรหัสผ่าน หากกรณีจำเป็นต้องใช้จะต้องกำหนดให้มีการทบทวน Log การเข้าถึงและการเข้าใช้งานของบัญชีผู้ใช้ที่มากับระบบงานด้วย
- ระบบที่มีความสำคัญอย่างยิ่งควรพิจารณาจัดเก็บประวัติการเข้าถึงได้ เพื่อใช้ในการสอบทานกิจกรรมย้อนหลัง
- การบริหารจัดการบัญชีผู้ใช้สิทธิสูง (High privilege user ID) ให้ดำเนินการดังนี้
    - มีกระบวนการควบคุมดูแลการเบิกใช้บัญชีผู้ใช้งานที่มีสิทธิ์สูงสุด (Highest Privilege User) อย่างเหมาะสม
    - มีการจัดเก็บรหัสผ่านของบัญชีผู้ใช้ที่มีสิทธิ์สูงสุดโดยหน่วยงานที่มีความเป็นอิสระจากหน่วยงานของผู้ขอเบิกใช้
    - ทำการเปลี่ยนรหัสผ่านหลังการใช้งานและตามรอบระยะเวลา
    - มีขั้นตอนในการอนุมัติการเบิกใช้งานบัญชีผู้ใช้งานที่มีสิทธิ์สูงสุดโดยหัวหน้างานของผู้ขอเบิกใช้และหน่วยงานผู้จัดเก็บบัญชีผู้ใช้ที่มีสิทธิ์สูงสุด มีการควบคุมไม่ให้มีการเบิกใช้งานบัญชีผู้ใช้ที่มีสิทธิ์สูงสุดในเวลาเดียวกัน

บมจ.ธนาคารไทยเครดิต
123 อาคารไทยประกันชีวิต ถนนรัชดาภิเษก แขวงดินแดง เขตดินแดง กรุงเทพฯ 10400
Thai Credit Bank Public Company Limited
123 Thai Life Insurance Bldg. Ratchadaphisek Rd., Dindaeng Bangkok 10400
Tel. (662) 697-5300 Fax. (662) 642-3096
www.thaicreditbank.com

8. การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ

(IT Operations Security)

วัตถุประสงค์

เพื่อให้มีแนวทางในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศให้มีความมั่นคงปลอดภัย เพื่อให้มีกระบวนการควบคุมการเปลี่ยนแปลงที่มีความรัดกุมปลอดภัยและเป็นไปตามมาตรฐานที่กำหนด

การบริหารจัดการการเปลี่ยนแปลง (Change Management)

1. กำหนดมาตรฐานและระเบียบวิธีปฏิบัติการบริหารจัดการการเปลี่ยนแปลง เพื่อควบคุมการเปลี่ยนแปลงโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศให้มีความรัดกุมเพียงพอ
2. กำหนดบทบาทหน้าที่และความรับผิดชอบของผู้บริหารที่ได้รับมอบหมายหรือคณะทำงานจัดการการเปลี่ยนแปลง เพื่อทำหน้าที่ประเมินผลกระทบและพิจารณาเหตุผลความจำเป็นก่อนอนุมัติให้ดำเนินการเปลี่ยนแปลงระบบ ป้องกันการแก้ไขเปลี่ยนแปลงโดยไม่ได้รับอนุญาตและไม่ให้เกิดผลกระทบที่อาจเกิดกับระบบที่เกี่ยวข้อง
3. ผู้ที่เกี่ยวข้องในกระบวนการบริหารจัดการการเปลี่ยนแปลง ควรมีการแบ่งแยกหน้าที่อย่างเหมาะสม (segregation of duties) เพื่อไม่ให้บุคคลใดบุคคลหนึ่งสามารถปฏิบัติงานได้ตั้งแต่ต้นจนจบกระบวนการ เช่น ผู้มีสิทธิ์ร้องขอ ผู้ที่มีอำนาจในการอนุมัติการเปลี่ยนแปลง ผู้ที่สามารถดำเนินการเปลี่ยนแปลงระบบ เป็นต้น
4. คำขอการเปลี่ยนแปลง (change request) ควรได้รับการอนุมัติจากหน่วยงานเจ้าของระบบ (system owner) เพื่อให้มั่นใจได้ว่าการขอเปลี่ยนแปลงได้รับการพิจารณาความจำเป็นอย่างเหมาะสมจากหน่วยงานเจ้าของระบบ
5. มีการประเมินผลกระทบหรือทำการทดสอบก่อนนำไปตั้งค่าบนระบบที่ให้บริการจริง เพื่อลดความเสี่ยงและผลกระทบที่อาจเกิดขึ้น
6. ควรมีการติดตามผลหลังการเปลี่ยนแปลงระบบ (post implementation review) เพื่อให้มั่นใจได้ว่าการเปลี่ยนแปลงนั้นเป็นไปตามวัตถุประสงค์ที่กำหนด

การบริหารจัดการการตั้งค่าระบบ (System Configuration Management)

7. กำหนดมาตรฐานและระเบียบวิธีปฏิบัติการควบคุมการเปลี่ยนแปลงการตั้งค่าระบบ มีการจัดทำเอกสารการตั้งค่าของระบบงาน อุปกรณ์เครือข่ายสื่อสาร และมีการทบทวนปรับปรุงเอกสารให้เป็นปัจจุบันอย่างสม่ำเสมอ

บมจ.ธนาคารไทยเครดิต
123 อาคารไทยประกันชีวิต ถนนรัชดาภิเษก แขวงดินแดง
เขตดินแดง กรุงเทพฯ 10400
Thai Credit Bank Public Company Limited
123 Thai Life Insurance Bldg., Ratchadaphisek Rd., Dindaeng
Bangkok 10400
Tel. (662) 697-5300 Fax. (662) 642-3095
www.thaicreditbank.com

8. มีการตั้งค่าระบบที่มีความปลอดภัยของระบบงาน และอุปกรณ์เครือข่ายสื่อสารต่างๆ มีการสอบทานการตั้งค่าตามรอบระยะเวลา เพื่อให้สอดคล้องตามมาตรฐานของธนาคาร

9. การเปลี่ยนแปลงการตั้งค่าบนระบบที่ให้บริการจริง ต้องผ่านกระบวนการบริหารจัดการการเปลี่ยนแปลงที่ธนาคารกำหนด มีการสำรองการตั้งค่าของระบบทุกครั้ง ก่อนการดำเนินการเปลี่ยนแปลง เพื่อป้องกันความเสี่ยงหรือข้อผิดพลาดในการปฏิบัติงาน

10. ติดตั้งโปรแกรมรักษาความปลอดภัย anti-Virus / anti-malware โดยมีการปรับปรุงประสิทธิภาพของการป้องกันโปรแกรมไม่ประสงค์ดี (Malware) สำหรับเครื่องคอมพิวเตอร์แม่ข่ายให้เพียงพอและเป็นปัจจุบัน เพื่อให้เท่าทันในการป้องกันภัยคุกคามใหม่ๆ

การบริหารจัดการ patch (Patch Management)

11. กำหนดมาตรฐานและระเบียบวิธีปฏิบัติในการบริหารจัดการ patch เพื่อให้มีการควบคุมที่รัดกุมปลอดภัย และติดตั้งได้อย่างเหมาะสมทันการณ์

12. กำหนดให้ผู้ดูแลระบบทำการติดตั้ง patch โดยประเมินจากการประเมินความเสี่ยงและการจัดความสำคัญของระบบ โดยจัดให้มีกระบวนการทดสอบ patch ก่อนนำไปติดตั้งบนระบบที่ให้บริการจริง

13. การติดตั้ง patch บนระบบที่ให้บริการจริง ต้องผ่านกระบวนการบริหารจัดการการเปลี่ยนแปลงที่ธนาคารกำหนด เพื่อป้องกันความเสี่ยงหรือข้อผิดพลาดในการปฏิบัติงาน

14. มีการทบทวนและปรับปรุงกระบวนการบริหารจัดการ patch เพื่อให้มั่นใจได้ว่าธนาคารสามารถทดสอบและติดตั้ง patch ด้านการรักษาความปลอดภัย ได้ทันต่อสถานการณ์ที่เปลี่ยนไปและสามารถรองรับความเสี่ยงที่เพิ่มขึ้นได้อย่างรวดเร็ว

การจัดเก็บข้อมูลบันทึกเหตุการณ์ (Logging)

15. มีการจัดเก็บข้อมูลบันทึกเหตุการณ์ของเครื่องแม่ข่าย ระบบงาน อุปกรณ์เครือข่ายสื่อสารที่สำคัญด้วยวิธีการที่ปลอดภัย กำหนดให้บันทึกกิจกรรมการใช้งานของผู้ใช้ การให้บริการของระบบ และเหตุการณ์ต่างๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัย และจัดเก็บย้อนหลังเป็นระยะเวลาอย่างน้อย 90 วัน หรือตามกฎหมายที่เกี่ยวข้องกำหนด

16. มีการใช้ระบบในการควบคุมค่าเวลาของเครื่องแม่ข่าย ระบบงาน อุปกรณ์เครือข่ายสื่อสารให้ตรงกับเครื่องแม่ข่าย Network Time Protocol : NTP (clock synchronization) เพื่อให้ค่าเวลาในการบันทึกเหตุการณ์มีความถูกต้องในลักษณะ real-time ซึ่งเครื่องแม่ข่าย NTP ต้องรับสัญญาณนาฬิกาจากแหล่งที่มีความน่าเชื่อถือ

บมจ.ธนาคารไทยเครดิต
123 อาคารไทยประกันชีวิต ถนนรัชดาภิเษก แขวงดินแดง เขตดินแดง กรุงเทพฯ 10400
Thai Credit Bank Public Company Limited
123 Thai Life Insurance Bldg., Ratchadaphisek Rd., Dindaeng, Bangkok 10400
Tel. (662) 697-5300 Fax. (662) 642-3096
www.thaicreditbank.com

17. ข้อมูลการบันทึกเหตุการณ์ของอุปกรณ์สำคัญควรจัดเก็บไว้ที่เครื่องแม่ข่ายที่แยกเฉพาะ อย่างน้อยครอบคลุม access log และ activity log โดยมีการรักษาความปลอดภัยที่รัดกุมเพียงพอในการป้องกันการเปลี่ยนแปลงแก้ไข หรือทำลาย

18. ระบบต้องมีการบันทึกการเข้าถึง (access Log) และบันทึกการดำเนินงาน (activity log) ของผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศที่มีสิทธิ์สูง เช่น system administrator หรือ system operator เป็นต้น เพื่อใช้ในการสอบทานการเข้าถึงของผู้ปฏิบัติงานและการปฏิบัติงานตามขอบเขตหน้าที่ที่ได้รับมอบหมาย

การบริหารจัดการขีดความสามารถของระบบ (Capacity Management)

19. กำหนดให้มีการประเมินและติดตามดูแลความเพียงพอของโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศที่ครอบคลุมถึง ระบบคอมพิวเตอร์ ระบบฐานข้อมูล ระบบเครือข่ายสื่อสาร และระบบสาธารณูปโภคที่เกี่ยวข้องกับงานเทคโนโลยีสารสนเทศ

20. มีการประเมินแนวโน้มการใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศเพื่อวางแผนรองรับการใช้งานในอนาคต (capacity planning) โดยครอบคลุมทั้งระบบหลักและระบบสำรอง

21. จัดทำรายงานความเพียงพอของทรัพยากรด้านเทคโนโลยีสารสนเทศนาเสนอต่อคณะกรรมการที่ได้รับมอบหมายหรือผู้บริหารระดับสูงที่เกี่ยวข้องรับทราบตามแผนงานของหน่วยงาน เพื่อให้มีการกำกับดูแลความพร้อมและความเพียงพอของระบบในการรองรับการให้บริการทางธุรกิจได้อย่างต่อเนื่อง รวมทั้งเพื่อพิจารณาแนวทางลดความเสี่ยงได้ทันการณ์

การติดตามดูแลระบบและเฝ้าระวังภัยคุกคาม (Security Monitoring)

22. กำหนด มาตรฐานและระเบียบในการติดตามดูแลระบบและเฝ้าระวังภัยคุกคาม เพื่อให้มีการติดตามดูแลความปลอดภัยของระบบอย่างต่อเนื่อง

23. กำหนดกระบวนการหรือเครื่องมือในการตรวจจับเหตุการณ์ผิดปกติที่กระทบต่อความปลอดภัยของระบบที่สำคัญและระบบเครือข่ายสื่อสาร เพื่อให้รับทราบความผิดปกติหรือภัยคุกคาม และสามารถดำเนินการป้องกันหรือรับมือได้อย่างเหมาะสม

24. มีกระบวนการหรือเครื่องมือในการรับข้อมูลจากแหล่งข้อมูลที่เชื่อถือได้ มีการวิเคราะห์และจัดการข้อมูลภัยคุกคามที่อาจเกิดขึ้นอย่างต่อเนื่อง ครอบคลุม ลักษณะการโจมตี ความเป็นไปได้ที่จะเกิดเหตุการณ์ภัยคุกคาม รวมถึงวิธีการรับมือกับภัยคุกคามนั้น เพื่อนำมาใช้สนับสนุนการรับมือต่อภัยคุกคามทางไซเบอร์

การบริหารจัดการช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Management and Penetration Test)

25. กำหนดมาตรฐานและระเบียบวิธีปฏิบัติการบริหารจัดการช่องโหว่และการทดสอบเจาะระบบ

บมจ.ธนาคารไทยเครดิต
123 อาคารไทยประกันชีวิต ถนนรัชดาภิเษก แขวงดินแดง เขตดินแดง กรุงเทพฯ 10400
Thai Credit Bank Public Company Limited
123 Thai Life Insurance Bldg., Ratchadapisek Rd., Dindaeng Bangkok 10400
Tel. (662) 697-5300 Fax. (662) 642-3096
www.thaicreditbank.com

26. การบริหารจัดการช่องโหว่ (Vulnerability Management) จัดให้มีกระบวนการและเครื่องมือในการประเมินช่องโหว่ (vulnerability assessment) กำหนดขอบเขตและความถี่ของการประเมินช่องโหว่ของระบบที่เหมาะสมตามระดับความเสี่ยง โดยต้องประเมินช่องโหว่ของระบบงานที่มีนัยสำคัญทุกระบบงานควรจัดทำอย่างน้อยปีละ 1 ครั้งและเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

27. มีการทดสอบเจาะระบบ (Penetration Test) โดยจัดให้มีผู้เชี่ยวชาญที่มีความเป็นอิสระทำหน้าที่ทดสอบเจาะระบบ ครอบคลุมระบบงาน (Application) และระบบเครือข่าย (Network) ที่มีการเชื่อมต่อกับเครือข่ายสาธารณะ (Internet Facing) อย่างน้อยปีละ 1 ครั้งและเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เพื่อให้ทราบถึงช่องโหว่และสามารถดำเนินการแก้ไขและป้องกันภัยคุกคามที่อาจเกิดขึ้นได้อย่างทันการณ์

28. จัดให้มีการรายงานผลการประเมินช่องโหว่และการทดสอบเจาะระบบ พร้อมทั้งแนวทางและแผนการดำเนินการปรับปรุงแก้ไข เสนอต่อผู้บริหารที่ได้รับมอบหมายและคณะกรรมการที่เกี่ยวข้องรับทราบ

การสำรองข้อมูล (Data Backup)

29. กำหนดให้มีข้อมูลสำรองพร้อมใช้และมีความปลอดภัย มีกระบวนการสำรองทั้งระบบ (Full Backup) ทุกครั้งภายหลังจากที่มีการเปลี่ยนแปลงระบบปฏิบัติการและระบบงาน เพื่อให้ระบบสำรองมีความเป็นปัจจุบัน

30. มีระบบหรือทะเบียนควบคุมการจัดเก็บและเรียกใช้งานสื่อบันทึกข้อมูลตามประเภทของสื่อที่จัดเก็บ โดยมีการระบุข้อมูล ชื่อ วันที่ และช่วงเวลาที่จัดเก็บ ที่สามารถติดตามตรวจสอบได้

31. มีการจัดเก็บสื่อบันทึกข้อมูลสำรองไว้นอกศูนย์คอมพิวเตอร์หลักหรือนอกสถานที่ปฏิบัติงานหลัก โดยมีการรักษาสภาพแวดล้อมและการควบคุมความปลอดภัยในการเข้าถึงข้อมูลที่จัดเก็บไว้

32. จัดให้มีการสอบทานการสำรองข้อมูล เพื่อให้มั่นใจว่ามีการสำรองข้อมูลครบถ้วนถูกต้อง พร้อมใช้งานและปลอดภัย

การรักษาความปลอดภัยในอุปกรณ์ที่ใช้ปฏิบัติงาน (Endpoint Security)

33. ติดตั้งระบบปฏิบัติการและโปรแกรมพื้นฐานที่ใช้ในการปฏิบัติงานบนเครื่องคอมพิวเตอร์ (Personal Computer / Notebook) ตามที่ธนาคารกำหนดเท่านั้น โดยมีกระบวนการหรือเครื่องมือในการควบคุมและติดตามไม่ให้พนักงานสามารถติดตั้งโปรแกรมอื่นๆ นอกเหนือจากที่กำหนด

34. ติดตั้งโปรแกรมรักษาความปลอดภัย Anti-virus / Anti-malware โดยมีการปรับปรุงประสิทธิภาพของการป้องกันโปรแกรมไม่ประสงค์ดี (Malware) ให้เพียงพอและเป็นปัจจุบัน เพื่อให้เท่าทันในการป้องกันภัยคุกคามใหม่ๆ

บมจ.ธนาคารไทยเครดิต
123 อาคารไทยประกันชีวิต ถนนรัชดาภิเษก แขวงดินแดง เขตดินแดง กรุงเทพฯ 10400
Thai Credit Bank Public Company Limited
123 Thai Life Insurance Bldg. Ratchadaphisek Rd. Dindaeng Bangkok 10400
Tel. (662) 697-5300 Fax. (662) 642-3095
www.thaicreditbank.com

35. ไม่ให้มีการจัดเก็บข้อมูลที่มีระดับชั้นความลับสูงสุดในเครื่องคอมพิวเตอร์ของพนักงาน แต่หากมีความจำเป็นต้องจัดเก็บ พนักงานต้องจัดให้มีการรักษาความปลอดภัยที่รัดกุมเพียงพอ เช่น กำหนดสิทธิการเข้าถึง มีการเข้ารหัส เป็นต้น

36. จำกัดการเข้าถึง Shared Drive หรือ Shared Folder ตามความจำเป็นในการใช้งานเท่านั้น โดยต้องได้รับการอนุญาตจากหน่วยงานเจ้าของข้อมูลก่อนการเข้าใช้งาน

37. การควบคุมการใช้งานอินเตอร์เน็ต ได้จัดให้มีเครื่องมือในการควบคุมให้อุปกรณ์ที่สามารถเชื่อมต่ออินเตอร์เน็ตเข้าถึงเฉพาะเว็บไซต์ที่ได้รับอนุญาตเท่านั้น รวมถึงมีการจำกัดการดาวน์โหลดหรืออัพโหลดข้อมูลจากอินเตอร์เน็ต

38. การขอเปิดใช้ฟังก์ชั่น Universal Serial Bus (USB) สำหรับการใช้สื่อบันทึกข้อมูลพกพา (Removable Media) เช่น Universal Serial Bus (USB) หรือ External Harddisk เป็นต้น ต้องได้รับการพิจารณาอนุมัติจากผู้มีอำนาจอนุมัติ

39. กำหนดให้มีเครื่องมือป้องกันและเครื่องมือตรวจจับการรับส่งข้อมูลสำคัญผ่านช่องทางต่างๆ โดยไม่ได้รับอนุญาต

40. การบริหารจัดการอุปกรณ์ส่วนตัว (Bring Your Own Device : BYOD)

    - ดำเนินการควบคุมการการใช้ BYOD ในการเข้าถึงระบบเครือข่ายสื่อสาร ระบบงานและข้อมูลของธนาคาร โดยต้องได้รับการพิจารณาอนุมัติจากหน่วยงานต้นสังกัดและผู้มีอำนาจอนุมัติของธนาคารเป็นกรณีๆ ไป
    - ทำการตรวจสอบ วิเคราะห์ และความเสี่ยงของอุปกรณ์ที่นำมาใช้งานในธนาคาร โดยเครื่องคอมพิวเตอร์ต้องติดตั้ง Anti-virus/ Anti-malware หรือโปรแกรมตามที่ธนาคารกำหนด
    - กำหนดรหัสผ่านเพื่อใช้ในการล็อกหรือปลดล็อกในการเข้าถึงอุปกรณ์ส่วนตัว
    - ไม่อนุญาตให้อุปกรณ์โทรศัพท์เคลื่อนที่ (Tablet, Smartphone) ที่ถูกปรับแต่ง (Rooted หรือ Jail broken) ลงทะเบียนใช้งาน BYOD

บมจ.ธนาคารไทยเครดิต
123 อาคารไทยประกันชีวิต ถนนรัชดาภิเษก แขวงดินแดง
เขตดินแดง กรุงเทพฯ 10400
Thai Credit Bank Public Company Limited
123 Thai Life Insurance Bldg., Ratchadaphisek Rd., Dindaeng
Bangkok 10400
Tel. (662) 697-5300 Fax. (662) 642-3096
www.thaicreditbank.com

9. การจัดหาและการพัฒนาระบบ (System Acquisition and Development)

วัตถุประสงค์

เพื่อให้มั่นใจได้ว่ากระบวนการจัดหาและการพัฒนาระบบ มีการควบคุมการรักษาความปลอดภัยอย่างรัดกุม และสอดคล้องตามหลักการควบคุมที่เป็นมาตรฐานสากล

การจัดหาระบบ (System Acquisition)

1. ให้จัดทำหลักเกณฑ์การพิจารณาคัดเลือกระบบและผู้ให้บริการ และทำการประเมินผู้ให้บริการในการจัดหาระบบงาน
2. สายงานเทคโนโลยีสารสนเทศ ทำหน้าที่ควบคุมดูแลผู้ให้บริการปฏิบัติตามมาตรฐานและระเบียบวิธีปฏิบัติการออกแบบและพัฒนาระบบ
3. สายงานเทคโนโลยีสารสนเทศ ทำหน้าที่กำหนดเกณฑ์ในการตรวจสอบและส่งมอบระบบเทคโนโลยีสารสนเทศ

การพัฒนาระบบเทคโนโลยีสารสนเทศ (System Development)

4. กำหนดมาตรฐานและระเบียบวิธีปฏิบัติในการออกแบบและพัฒนาระบบ โดยคำนึงถึงการรักษาความมั่นคงปลอดภัย ครอบคลุมกระบวนการตั้งแต่จัดทำความต้องการ (Requirement) การออกแบบ การพัฒนา และการทดสอบระบบก่อนใช้งานจริง
5. กำหนดให้หน่วยงานธุรกิจที่เกี่ยวข้องสอบทานความถูกต้องครบถ้วนตามความต้องการของหน่วยงานธุรกิจ (Business Requirement) โดยครอบคลุมการรักษาความปลอดภัยตามนโยบายหรือมาตรฐานที่ธนาคารกำหนด (Security Requirement) รวมทั้งพิจารณาจัดทำเอกสารรายละเอียดคุณสมบัติทางเทคนิค (Technical Specification) ก่อนเริ่มพัฒนาระบบ

การพัฒนาระบบ

6. บทบาทหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องในกระบวนการพัฒนาระบบควรเป็นไปตามหลักการแบ่งแยกหน้าที่อย่างเหมาะสม (Segregation of duties) เพื่อไม่ให้บุคคลใดบุคคลหนึ่งสามารถปฏิบัติงานได้ตั้งแต่ต้นจนจบกระบวนการ เช่น ควรแยกผู้พัฒนาระบบ ออกจากผู้นำระบบขึ้นใช้งานจริง เป็นต้น
7. ระบบงานที่มีความสำคัญ ควรมีการแบ่งแยกสภาพแวดล้อมของระบบงานที่ใช้สำหรับการพัฒนา (Development) การทดสอบ (Testing) และระบบที่ให้บริการจริง (Production) ออกจากกัน เพื่อควบคุมการทดสอบและลดผลกระทบที่อาจเกิดขึ้นจากการนำระบบขึ้นใช้งานจริง
8. มีการควบคุมเวอร์ชันของคำสั่งในการเขียนโปรแกรม (Source Code Version Control) เพื่อป้องกันความเสี่ยงที่อาจมีการคำสั่งในการเขียนโปรแกรมผิดเวอร์ชัน

บมจ.ธนาคารไทยเครดิต
123 อาคารไทยประกันชีวิต ถนนรัชดาภิเษก แขวงดินแดง เขตดินแดง กรุงเทพฯ 10400
Thai Credit Bank Public Company Limited
123 Thai Life Insurance Bldg. Ratchadaphisek Rd. Din Daeng Bangkok 10400
Tel. (662) 697-5300 Fax. (662) 642-3096
www.thaicreditbank.com

9. มีการควบคุมไม่ให้มีการติดตั้งเครื่องมือการพัฒนาระบบ (Development Tools) และเครื่องมือแปลโปรแกรม (Compilers) ไว้บนระบบที่ให้บริการจริง เพื่อป้องกันความเสี่ยงที่อาจถูกปรับเปลี่ยนหรือติดตั้งโปรแกรมโดยไม่ได้รับอนุญาต

การทดสอบระบบ

10. จัดทำขอบเขตการทดสอบให้ครอบคลุมฟังก์ชันและเงื่อนไขต่างๆ ด้านประสิทธิภาพ ตามความต้องการของหน่วยงานธุรกิจ (Business Requirement) รวมถึงการควบคุมความมั่นคงปลอดภัยตามนโยบายหรือมาตรฐานที่ธนาคารกำหนด
11. มีการทดสอบระบบก่อนการใช้งานจริง เช่น ทดสอบการทำงานของแต่ละระบบ (Unit test) ทดสอบการทำงานร่วมกันของระบบต่างๆ (System integration test) ทดสอบความพร้อมใช้งานตามกระบวนการและความต้องการของผู้ใช้งาน (User acceptance test) และทดสอบความปลอดภัยของระบบ (Security test) ตามกระบวนการรักษาความมั่นคงปลอดภัย ที่กำหนดในเอกสารรายละเอียดคุณสมบัติทางเทคนิค (Technical specification)
12. มีการทดสอบบนสภาพแวดล้อมใกล้เคียงระบบที่ให้บริการจริง เพื่อลดความเสี่ยงของการเปลี่ยนแปลงบนระบบที่ให้บริการจริง
13. สำหรับการเปลี่ยนแปลงระบบมีการใช้งานหรือเชื่อมโยงกับระบบอื่นจำนวนมาก ควรจัดให้มีการทดสอบประสิทธิภาพ (Performance test) เพื่อให้มั่นใจได้ว่าระบบมีเสถียรภาพเพียงพอในการรองรับการทำงาน
14. สำหรับการเปลี่ยนแปลงระบบในส่วนที่เป็นการทำธุรกรรมสำคัญของระบบที่มีความสำคัญอย่างยิ่งและมีการเชื่อมต่อกับเครือข่ายสาธารณะ ควรจัดให้มีการสอบทานคำสั่งในการเขียนโปรแกรม (Source code review)
15. ควรจัดให้มีกระบวนการและเอกสารการ Sign off ผลการทดสอบระบบจากหน่วยงานที่เกี่ยวข้อง ก่อนนำระบบขึ้นใช้งานจริง
16. มีแนวทางการควบคุมการรักษาความปลอดภัยและความลับของข้อมูลสำคัญที่นำไปใช้ในการทดสอบ เช่น Data masking เป็นต้น เพื่อป้องกันความเสี่ยงในการรั่วไหลของข้อมูลสำคัญดังกล่าว
17. มีการจัดทำคู่มือและอบรมผู้ใช้งานระบบ เพื่อให้มีความเข้าใจฟังก์ชันการทำงานและมีการใช้งานระบบอย่างปลอดภัย รวมถึงจัดให้มีคู่มือการดูแลระบบและอบรมผู้ดูแลระบบ เพื่อสามารถตรวจสอบและจัดการแก้ไขปัญหาได้

การนำระบบขึ้นใช้งานจริง (system deployment)

18. การนำระบบขึ้นใช้งานจริง ต้องผ่านกระบวนการบริหารจัดการการเปลี่ยนแปลงที่ธนาคารกำหนด เพื่อป้องกันความเสี่ยงหรือข้อผิดพลาดในการปฏิบัติงาน

บมจ. ธนาคารไทยเครดิต
123 อาคารไทยประกันชีวิต ถนนรัชดาภิเษก แขวงดินแดง
เขตดินแดง กรุงเทพฯ 10400
Thai Credit Bank Public Company Limited
123 Thai Life Insurance Bldg., Ratchadaphisek Rd., Dindaeng
Bangkok 10400
Tel. (662) 697-5300 Fax. (662) 642-3095
www.thaicreditbank.com

10. การบริหารจัดการเหตุการณ์ผิดปกติและปัญหาด้านเทคโนโลยีสารสนเทศ

(IT Incident and Problem Management)

วัตถุประสงค์

เพื่อให้ธนาคารมีแนวทางในการบริหารจัดการเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ ซึ่งรวมถึงเหตุการณ์ผิดปกติจากภัยคุกคามทางไซเบอร์อย่างเหมาะสมทันการณ์ ให้สามารถจัดการแก้ไขปัญหาให้กลับสู่สภาพปกติได้อย่างรวดเร็วและจำกัดความเสียหายที่ส่งผลกระทบต่อธุรกิจของธนาคาร และเพื่อให้มีกระบวนการติดตามหาสาเหตุที่แท้จริง ให้มีแนวทางป้องกันไม่ให้เกิดเหตุการณ์ผิดปกติซ้ำในอนาคต

การบริหารจัดการเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ (IT Incident Management)

1. กำหนดมาตรฐานและระเบียบวิธีปฏิบัติการบริหารจัดการเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ ควรครอบคลุมตั้งแต่กระบวนการหรือเครื่องมือในการบันทึกเหตุการณ์ผิดปกติ การกำหนดประเภท การจัดระดับความรุนแรง การวิเคราะห์หาสาเหตุ การดำเนินการแก้ไข การติดตามแก้ไข การรายงานเหตุการณ์ผิดปกติ

2. กำหนดหลักเกณฑ์การส่งต่อเหตุการณ์ผิดปกติ (escalation) และรายงานความคืบหน้าเหตุการณ์ผิดปกติให้ผู้เกี่ยวข้อง ผู้บริหารระดับสูง คณะกรรมการที่เกี่ยวข้องได้รับทราบ ให้สอดคล้องกับระดับความรุนแรงของเหตุการณ์ผิดปกติ

3. การจัดระดับความรุนแรงของปัญหา ควรพิจารณาอย่างน้อยให้ครอบคลุม ผลกระทบต่อการให้บริการ ผลกระทบต่อผู้ใช้งาน โดยกรอบระยะเวลาในการแก้ไขเหตุการณ์ผิดปกติควรคำนึงถึงเป้าหมายระยะเวลาในการกู้คืนระบบ (Recovery Time Objective : RTO) และเป้าหมายระยะเวลาสูงสุดที่ยอมให้ธุรกิจหยุดชะงัก (Maximum Tolerance Period of Disruption : MTPD) เพื่อที่จะสามารถตัดสินใจใช้แผนสำรองอย่างเหมาะสมทันการณ์

4. จัดให้มีศูนย์รับแจ้งเหตุการณ์ผิดปกติ โดยทำหน้าที่ในการบันทึกและแก้ไขในเบื้องต้น หรือส่งต่อเหตุการณ์ผิดปกติ ไปยังสายงานเทคโนโลยีสารสนเทศที่เกี่ยวข้อง

5. จัดทำแผนการรับมือกับเหตุการณ์ผิดปกติ (incident response plan) ตามความสำคัญของเหตุการณ์ เพื่อให้สามารถรับมือและตอบสนองต่อเหตุการณ์ได้อย่างรวดเร็วและทันการณ์ โดยอย่างน้อยแผนควรระบุกระบวนการรับมือและช่องทางประสานงานจากผู้เชี่ยวชาญทั้งภายในและภายนอก และมีแนวทางการตรวจสอบ วิเคราะห์หาสาเหตุ และประเมินผลกระทบ

บมจ.ธนาคารไทยเครดิต
123 อาคารไทยประกันชีวิต ถนนรัชดาภิเษก แขวงดินแดง เขตดินแดง กรุงเทพฯ 10400
Thai Credit Bank Public Company Limited
123 Thai Life Insurance Bldg., Ratchadaphisek Rd., Dindaeng, Bangkok 10400
Tel. (662) 697-5300 Fax. (662) 642-3096
www.thaicreditbank.com

6. จัดทำรายงานเหตุการณ์ผิดปกติ เสนอต่อคณะกรรมการที่ได้รับมอบหมายหรือผู้บริหารระดับสูงที่ได้รับมอบหมาย โดยครอบคลุม วัน เวลา เหตุการณ์ ความเสียหาย การวิเคราะห์สาเหตุที่แท้จริง การวิเคราะห์ผลกระทบ การแก้ไขปัญหาและแนวทางหรือแผนดำเนินการเพื่อป้องกันเหตุการณ์ผิดปกติในอนาคต

7. ในกรณีเกิดปัญหาหรือเหตุการณ์ผิดปกติที่เกิดจากการใช้งานเทคโนโลยีสารสนเทศ จนเป็นเหตุให้ธนาคารไม่สามารถให้บริการทางการเงินพื้นฐาน เช่น การฝากเงิน การถอนเงิน การโอนเงิน และการชำระเงิน แก่ลูกค้าในวงกว้าง หรือเกิดเหตุการณ์ที่มีนัยสำคัญซึ่งอาจส่งผลกระทบต่อชื่อเสียงของธนาคาร รวมถึงกรณีเทคโนโลยีสารสนเทศที่สำคัญของธนาคาร ถูกโจมตีหรือถูกขู่โจมตีจากภัยคุกคามทางไซเบอร์ และเป็นปัญหาหรือเหตุการณ์ที่ต้องรายงานต่อผู้บริหารในตำแหน่งสูงสุดของธนาคารทราบ ให้สายงานเทคโนโลยีสารสนเทศจัดทำรายงานปัญหาหรือเหตุการณ์ผิดปกติที่เกิดขึ้น ส่งไปยังสายงานกำกับการปฏิบัติตามกฎเกณฑ์ทันที เพื่อรายงานต่อฝ่ายตรวจสอบเทคโนโลยีสารสนเทศ สายงานนโยบายระบบการชำระเงินและเทคโนโลยีทางการเงิน ธนาคารแห่งประเทศไทย ภายในไม่เกิน 24 ชั่วโมง นับแต่เกิดหรือรับรู้ปัญหาหรือเหตุการณ์ผิดปกติ และให้ธนาคารแจ้งสาเหตุและการแก้ไขปัญหาเพิ่มเติมภายหลัง

การบริหารจัดการปัญหาด้านเทคโนโลยีสารสนเทศ (IT Problem Management)

1. มีมาตรฐานและระเบียบวิธีปฏิบัติการบริหารจัดการปัญหาด้านเทคโนโลยีสารสนเทศ เพื่อให้มีการนำเหตุการณ์ผิดปกติที่ยังไม่ทราบสาเหตุที่แท้จริง (unknown root cause) เหตุการณ์ผิดปกติที่เกิดขึ้นซ้ำ (repeated incident) มาวิเคราะห์และพิจารณาแนวทางแก้ไขปัญหาจากสาเหตุที่แท้จริง (root cause)

2. มีกระบวนการหรือเครื่องมือในการบันทึกปัญหา หลักเกณฑ์ในการจัดประเภทปัญหา การจัดลำดับความสำคัญ วิเคราะห์ และจัดให้มีการติดตามการแก้ไขปัญหาเพื่อให้ปัญหาได้รับการแก้ไข

3. มีกระบวนการหรือเครื่องมือบันทึกปัญหาที่เคยเกิดขึ้น เพื่อให้เป็นแหล่งข้อมูลความรู้ให้สามารถสืบค้นเหตุการณ์ปัญหาและแนวทางการแก้ไขปัญหาได้ในภายหลังอย่างรวดเร็วและมีประสิทธิภาพ

บมจ.ธนาคารไทยเครดิต
123 อาคารไทยประกันชีวิต ถนนรัชดาภิเษก แขวงดินแดง เขตดินแดง กรุงเทพฯ 10400
Thai Credit Bank Public Company Limited
123 Thai Life Insurance Bldg., Ratchadaphisek Rd., Dindaeng, Bangkok 10400
Tel. (662) 697-5300 Fax. (662) 642-3096
www.thaicreditbank.com

11. การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (Disaster Recovery Plan : DRP)

วัตถุประสงค์

เพื่อให้ธนาคารมีแนวทางรองรับเหตุการณ์ผิดปกติที่ระบบเกิดหยุดชะงักหรือเกิดความเสียหาย โดยที่ธุรกิจดำเนินการต่อไปได้อย่างต่อเนื่องและสามารถกู้คืนระบบให้กลับคืนสู่สภาพปกติภายในระยะเวลาที่ยอมรับได้

1. กำหนดนโยบายการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ โดยคำนึงความสอดคล้องกับนโยบายการบริหารความต่อเนื่องของธุรกิจและนโยบายการบริหารความเสี่ยงของธนาคาร

2. นโยบายดังกล่าวต้องได้รับอนุมัติจากคณะกรรมการที่ได้รับมอบหมายและได้รับการทบทวนอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงที่ส่งผลกระทบกับแผนฯ เช่น มีการเปลี่ยนแปลงกลยุทธ์ทางธุรกิจ นโยบายการบริหารความเสี่ยงโดยรวม สภาพแวดล้อมของการดำเนินธุรกิจหรือทรัพยากรหรือโครงสร้างระบบ IT เป็นต้น

3. มีการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ ที่สอดคล้องกับแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan : BCP) โดยการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศควรครอบคลุมถึงการกำหนดระยะเวลาในการกู้คืนระบบ (Recovery Time Objective : RTO) และระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย (Recovery Point Objective : RPO) ที่สอดคล้องกับความสำคัญของระบบ รวมทั้งการกำหนดระยะเวลาสูงสุดที่ยอมให้ธุรกิจหยุดชะงัก (Maximum Tolerance Period of Disruption : MTPD) เพื่อรองรับการดำเนินธุรกิจอย่างต่อเนื่องของธนาคาร โดยต้องได้รับการอนุมัติจากคณะกรรมการที่ได้รับมอบหมาย โดยจัดให้มีการทบทวนอย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

4. การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศและจัดเตรียมทรัพยากรที่จำเป็น (redundancies) ควรคำนึงถึงลักษณะการดำเนินธุรกิจ ปริมาณธุรกรรม ความซับซ้อนของเทคโนโลยีสารสนเทศ ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ เหตุการณ์ความเสียหายต่างๆ และความเสี่ยงที่เกี่ยวข้องในการดำเนินธุรกิจของธนาคาร ให้มีความต่อเนื่องในการให้บริการ เช่น ความเสี่ยงด้านปฏิบัติการ (operation risk) ความเสี่ยงด้านชื่อเสียง (reputational risk) ความเสี่ยงจากการพึ่งพาองค์กรอื่นในการดำเนินธุรกิจ (interdependency risk) ความเสี่ยงจากการกระจุกตัวของระบบงานหรือทรัพยากรที่สำคัญ (concentration risk) และความเสี่ยงที่มีผลกระทบต่อธนาคาร ผู้ใช้บริการ ผู้มีส่วนได้เสียและระบบสถาบันการเงิน (systemic risk)

บมจ.ธนาคารไทยเครดิต
123 อาคารไทยประกันชีวิต ถนนรัชดาภิเษก แขวงดินแดง เขตดินแดง กรุงเทพฯ 10400
Thai Credit Bank Public Company Limited
123 Thai Life Insurance Bldg., Ratchadaphisek Rd., Dindaeng Bangkok 10400
Tel. (662) 697-5300 Fax. (662) 642-3096
www.thaicreditbank.com

5. จัดให้มีคณะทำงานหรือหน่วยงานที่รับผิดชอบในการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ โดยมีผู้บริหารและบุคลากรของหน่วยงานด้านต่างๆ ที่เกี่ยวข้องเข้าร่วมด้วย เช่น ด้านเทคโนโลยีสารสนเทศ ด้านธุรกิจ และด้านสื่อสารองค์กร เป็นต้น

6. จัดให้มีคู่มือหรือเอกสารประกอบการดำเนินการตามแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ รวมทั้งประชาสัมพันธ์และฝึกอบรมเพื่อให้พนักงานทุกคนที่มีส่วนเกี่ยวข้องกับการดำเนินการตามแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศมีความเข้าใจและสามารถปฏิบัติตามแผนดังกล่าวได้

7. จัดให้มีการทบทวนและทดสอบการปฏิบัติตามแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศประจำปีอย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

8. จัดให้มีศูนย์คอมพิวเตอร์สำรอง (disaster recovery site) ที่มีความพร้อมใช้งานและสามารถปฏิบัติงานทดแทนได้เมื่อศูนย์คอมพิวเตอร์หลัก (primary site) หยุดชะงัก โดยศูนย์คอมพิวเตอร์สำรองควรอยู่ห่างจากศูนย์คอมพิวเตอร์หลักอย่างเพียงพอที่จะมิให้เกิดปัญหา หรือได้รับผลกระทบในลักษณะเดียวกันในช่วงเวลาเดียวกัน เช่น ระบบไฟฟ้าขัดข้อง และภัยธรรมชาติ

บมจ.ธนาคารไทยเครดิต
123 อาคารไทยประกันชีวิต ถนนรัชดาภิเษก แขวงดินแดง เขตดินแดง กรุงเทพฯ 10400
Thai Credit Bank Public Company Limited
123 Thai Life Insurance Bldg. Ratchadaphisek Rd. Dindaeng Bangkok 10400
Tel. (662) 697-5300 Fax. (662) 642-3095
www.thaicreditbank.com

12. การบริหารจัดการความเสี่ยงจากบุคคลภายนอก (Third Party Risk Management)

วัตถุประสงค์

เพื่อให้ธนาคารมีแนวทางการบริหารจัดการความเสี่ยงจากบุคคลภายนอก ในกรณีที่ใช้บริการงานด้านเทคโนโลยีสารสนเทศจากบุคคลภายนอก (IT Outsourcing) หรือเชื่อมต่อระบบเทคโนโลยีสารสนเทศกับบุคคลภายนอก หรือกรณีที่บุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญของธนาคารหรือข้อมูลของลูกค้าที่ควบคุมดูแลโดยธนาคาร

1. ในกรณีที่มีการใช้บริการงานด้านเทคโนโลยีสารสนเทศจากบุคคลภายนอก (IT Outsourcing) หรือการเชื่อมต่อระบบเทคโนโลยีสารสนเทศกับบุคคลภายนอก หรือกรณีที่บุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญของธนาคารหรือข้อมูลของลูกค้าที่ควบคุมดูแลโดยธนาคาร ให้ปฏิบัติตามประกาศของธนาคารแห่งประเทศไทยว่าด้วยเรื่องการบริหารความเสี่ยงจากบุคคลภายนอก (Third Party Risk Management Implementation Guideline) และนโยบายธนาคาร เรื่องการบริหารความเสี่ยงจากบุคคลภายนอก (Third Party Risk Management Policy) รวมทั้งประกาศธนาคารเรื่องแนวปฏิบัติการนำเทคโนโลยีมาใช้ หรือการเปลี่ยนแปลงระบบงานหรือเทคโนโลยี ที่มีนัยสำคัญ
2. กำหนดมาตรฐานและระเบียบวิธีปฏิบัติในการบริหารจัดการความเสี่ยงจากบุคคลภายนอก เพื่อให้มีการกำกับความเสี่ยง กระบวนการบริหารความเสี่ยงและการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการรักษาความปลอดภัยจากภัยไซเบอร์ สอดคล้องตามระดับความเสี่ยงและระดับความมีนัยสำคัญ ตามหลักการดังนี้
   - กำหนดบทบาท หน้าที่ และความรับผิดชอบระหว่างธนาคารและบุคคลภายนอกอย่างชัดเจนและเป็นลายลักษณ์อักษร รวมทั้งควรระบุเงื่อนไข ให้ธนาคารแห่งประเทศไทยมีสิทธิเข้าตรวจสอบการดำเนินงานของบุคคลภายนอกด้วย
   - กำกับดูแล ติดตาม และบริหารจัดการความเสี่ยงจากการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก สอดคล้องตามระดับความเสี่ยงและระดับความมีนัยสำคัญ และความเสี่ยงจากการใช้บริการด้านเทคโนโลยีสารสนเทศจากผู้ให้บริการรายเดียวกัน
   - รักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่สอดคล้องกับมาตรฐานการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของธนาคารและอ้างอิงมาตรฐานสากลที่ยอมรับโดยทั่วไป และตามมาตรฐานหรือแนวทางที่ธนาคารกำหนดโดยด้านการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ครอบคลุม การรักษาความลับของระบบและข้อมูล(Confidentiality) ความถูกต้องเชื่อถือได้ของระบบและข้อมูล(Integrity) และความพร้อมใช้งานด้านเทคโนโลยีสารสนเทศ(Availability)
   - เตรียมความพร้อมรับมือต่อเหตุการณ์ที่อาจเกิดขึ้นและมีผลกระทบต่อธนาคารอย่างมีนัยสำคัญ เพื่อให้สามารถดำเนินธุรกิจได้อย่างต่อเนื่อง รวมถึงการมีข้อมูลพร้อมใช้สำหรับการดำเนินธุรกิจและการให้บริการแก่ลูกค้า

บมจ.ธนาคารไทยเครดิต
123 อาคารไทยประกันชีวิต ถนนรัชดาภิเษก แขวงดินแดง เขตดินแดง กรุงเทพฯ 10400
Thai Credit Bank Public Company Limited
123 Thai Life Insurance Bldg., Ratchadaphisek Rd., Dindaeng Bangkok 10400
Tel. (662) 697-5300 Fax. (662) 642-3056
www.thaicreditbank.com

13. การปฏิบัติตามข้อกำหนด (Compliance)

วัตถุประสงค์

เพื่อไม่ให้เกิดการละเมิดข้อกำหนดทางกฎหมาย ระเบียบปฏิบัติข้อกำหนดในสัญญา และข้อกำหนดทางด้านความมั่นคงปลอดภัยอื่นๆ

1. พนักงานทุกคนต้องลงนามรับทราบ ทำความเข้าใจ และปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และระเบียบปฏิบัติต่างๆ อย่างเคร่งครัด โดยไม่ขัดต่อกฎหมาย ข้อกำหนดของธนาคารแห่งประเทศไทย และจรรยาบรรณของธนาคารไทยเครดิต จำกัด (มหาชน) หากนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศไม่มีการเปลี่ยนแปลงใดๆ สามารถอ้างอิงการรับทราบที่ได้ดำเนินการไว้แล้ว
2. กรณีพนักงานใหม่ สายงานบริหารทรัพยากรบุคคลเป็นผู้ดำเนินการให้รับทราบนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ
3. ข้อมูลที่ถูกสร้าง เก็บรักษา หรือส่งผ่านบนระบบเทคโนโลยีสารสนเทศของธนาคาร ถือเป็นทรัพย์สินของธนาคาร (ยกเว้น ข้อมูลที่เป็นทรัพย์สินของลูกค้า หรือบุคคลภายนอก รวมถึงซอฟต์แวร์ หรือวัสดุอื่นๆ ที่ได้รับการคุ้มครองโดยสิทธิบัตร หรือลิขสิทธิ์ของบุคคลภายนอก) ทั้งนี้ธนาคารสามารถเปิดเผยหรือใช้งานข้อมูลเหล่านี้ เป็นหลักฐานในการสืบสวนความผิดต่างๆ โดยไม่จำเป็นต้องแจ้งให้ผู้ใช้งานทราบล่วงหน้า
4. เพื่อวัตถุประสงค์ในการบริหารจัดการและรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของธนาคาร ขอสงวนสิทธิ์ในการตรวจสอบการใช้งานเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ และระบบเครือข่ายของผู้ใช้งาน เพื่อให้มั่นใจว่ามีการใช้งานตรงตามที่นโยบายต่างๆ ที่ธนาคารกำหนดไว้
5. ธนาคารขอสงวนสิทธิ์ในการเข้าถึง ทบทวน และตรวจสอบอีเมล์ของผู้ใช้งาน โดยไม่จำเป็นต้องแจ้งให้ทราบล่วงหน้า อย่างไรก็ตาม ธนาคารจะดำเนินการตรวจสอบดังกล่าวต่อเมื่อมีความจำเป็นเท่านั้น และจะไม่เปิดเผยข้อมูลใดๆ ของผู้ใช้งาน เว้นแต่เป็นการเปิดเผยตามคำสั่งจากผู้มีอำนาจของธนาคาร ศาล ตามบทบังคับของกฎหมาย หรือด้วยความยินยอมจากผู้ใช้งานเท่านั้น
6. ห้ามมิให้พนักงานใช้งานทรัพย์สินและระบบเทคโนโลยีสารสนเทศของธนาคารกระทำการใดๆ ที่ขัดแย้งต่อกฎหมายแห่งราชอาณาจักรไทย และกฎหมายระหว่างประเทศ ไม่ว่าโดยกรณีใดก็ตาม
7. ห้ามมิให้ผู้ใช้งานทำการใช้งาน ทำซ้ำ หรือเผยแพร่ รูปภาพ บทเพลง บทความ หนังสือ หรือเอกสารใดๆ ที่เป็นการละเมิดลิขสิทธิ์ หรือติดตั้งซอฟต์แวร์ละเมิดลิขสิทธิ์บนระบบเทคโนโลยีสารสนเทศของธนาคารโดยเด็ดขาด

บมจ.ธนาคารไทยเครดิต
123 อาคารไทยประกันชีวิต ถนนรัชดาภิเษก แขวงดินแดง เขตดินแดง กรุงเทพฯ 10400
Thai Credit Bank Public Company Limited
123 Thai Life Insurance Bldg., Ratchadaphisek Rd., Dindaeng Bangkok 10400
Tel. (662) 697-5300 Fax. (662) 642-3098
www.thaicreditbank.com

8. การส่งซอฟต์แวร์ ข้อมูลลับ ซอฟต์แวร์การเข้ารหัส หรือเทคโนโลยีใดๆ ออกนอกประเทศ ต้องไม่ขัดต่อข้อกฎหมายใดๆ ทั้งของราชอาณาจักรไทย ระหว่างประเทศ และของประเทศปลายทาง ทั้งนี้ ผู้ใช้งานต้องได้รับการอนุมัติจากผู้บังคับบัญชา และผู้เชี่ยวชาญด้านกฎหมายก่อนดำเนินการส่งออก
9. การเจตนาเข้าถึงระบบหรือการเข้าถึงข้อมูลส่วนบุคคล (data privacy) โดยไม่ได้รับอนุญาต การจงใจใส่ข้อมูลที่ผิดพลาด และการเจตนาเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต ถือเป็นสิ่งต้องห้ามทั้งสิ้น การไม่ปฏิบัติตามนโยบายการรักษาความมั่นคงด้านเทคโนโลยีสารสนเทศนี้ ถือว่ามีความผิดทางวินัย
10. เพื่อให้มั่นใจได้ว่ามีการปฏิบัติตามนโยบายนี้อย่างเคร่งครัด ธนาคารจึงจำเป็นต้องจัดให้มีการสอบทานติดตามการปฏิบัติงานของพนักงาน ตลอดจนบุคคลอื่นที่เกี่ยวข้องเป็นระยะๆ ผ่านการตรวจสอบติดตามการปฏิบัติงานภายใน (Internal audit) และการตรวจสอบ Security logs/ Audit trails ที่เกี่ยวข้อง ทั้งนี้ธนาคารขอสงวนสิทธิในการกระทำการใดๆ ที่เห็นว่าจำเป็น เพื่อจัดการและป้องกันความมั่นคงปลอดภัยให้แก่ข้อมูลและระบบเทคโนโลยีสารสนเทศของธนาคาร
11. ธนาคารจัดให้มีหน่วยงานที่เป็นอิสระ เข้ามาดำเนินการตรวจสอบเกี่ยวกับความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ รวมถึงกฎหมายและนโยบายที่กำหนดขึ้นตามความเหมาะสม

บมจ.ธนาคารไทยเครดิต
123 อาคารไทยประกันชีวิต ถนนรัชดาภิเษก แขวงดินแดง เขตดินแดง กรุงเทพฯ 10400
Thai Credit Bank Public Company Limited
123 Thai Life Insurance Bldg., Ratchadaphisek Rd., Dindaeng Bangkok 10400
Tel. (662) 697-5300 Fax. (662) 642-3095
www.thaicreditbank.com

14. การรักษาความปลอดภัยในการใช้ทรัพย์สินสารสนเทศและอุปกรณ์ที่ใช้ในการปฏิบัติงาน และหนังสือยอมรับเงื่อนไขนโยบายการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศสำหรับผู้ใช้งาน

(IT Acceptable Use Policy : AUP)

วัตถุประสงค์

เพื่อกำหนดแนวทางในการรักษาความปลอดภัยในการใช้ทรัพย์สินสารสนเทศและอุปกรณ์ที่ใช้ในการปฏิบัติงานของธนาคาร และจัดทำหนังสือยอมรับเงื่อนไขนโยบายการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศสำหรับผู้ใช้งาน (IT Acceptable Use Policy: AUP)

การเข้าถึงระบบงานและการพิสูจน์ตัวตน

1. พนักงานต้องมีบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนเอง
2. พนักงานมีหน้าที่ในการดูแลรักษา บัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) โดยห้ามใช้งานร่วมกัน ห้ามมิให้ทำการเผยแพร่ แจกจ่าย หรือทำให้ผู้อื่นล่วงรู้บัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password)
3. พนักงานต้องรับผิดชอบต่อการกระทำใดๆ ที่เกิดขึ้นจาก บัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ไม่ว่าการกระทำนั้นๆ จะเกิดจากพนักงานหรือไม่ก็ตาม
4. พนักงานมีหน้าที่ในการตั้งรหัสผ่าน (Password) ให้มีความปลอดภัย ตามนโยบายรหัสผ่าน (Password Policy) โดยรหัสผ่านต้องมีความยาวไม่น้อยกว่า 8 ตัวอักษร ประกอบด้วยตัวอักษรตัวใหญ่ ตัวเล็ก ตัวเลข และ/หรือตัวอักขระพิเศษ
5. ห้ามไม่ให้พนักงานใช้งานรหัสผ่าน (Password) ที่เคยถูกใช้งานมาแล้ว 12 ครั้งที่ผ่านมา
6. พนักงานใส่รหัสผ่านผิดติดต่อกัน 3 ครั้ง ระบบจะถูกระงับการใช้งาน
7. เมื่อทำการเปลี่ยนรหัสผ่าน ต้องใช้รหัสผ่านดังกล่าวอย่างน้อย 14 วัน จึงจะเปลี่ยนรหัสผ่านได้อีกครั้ง
8. พนักงานต้องทำการพิสูจน์ตัวตนก่อนเข้าระบบเทคโนโลยีสารสนเทศของธนาคาร หากพบว่ามีปัญหาในการพิสูจน์ตัวตน ไม่ว่าจะเกิดจากรหัสผ่าน (Password) โดนล็อก หรือเกิดจากความผิดพลาดใดๆ พนักงานต้องแจ้งให้ผู้มีหน้าที่รับผิดชอบสายงานเทคโนโลยีสารสนเทศทราบโดยทันที

การบริหารจัดการทรัพย์สินสารสนเทศ

9. ผู้ได้รับสิทธิใช้งานทรัพย์สินสารสนเทศตามสิทธิ์และหน้าที่ความรับผิดชอบที่ได้รับมอบหมายเพื่อรองรับการปฏิบัติงานในธุรกิจของธนาคารเท่านั้น
10. ผู้ได้รับสิทธิต้องไม่นำทรัพย์สินสารสนเทศ ระบบสารสนเทศของธนาคาร รวมทั้งข้อมูลของธนาคารหรือที่ธนาคารครอบครอง ไปใช้นอกกิจการธนาคาร หรือทำให้เกิดความเสียหายต่อธนาคาร

บมจ.ธนาคารไทยเครดิต
123 อาคารไทยประกันชีวิต ถนนรัชดาภิเษก แขวงดินแดง เขตดินแดง กรุงเทพฯ 10400
Thai Credit Bank Public Company Limited
123 Thai Life Insurance Bldg., Ratchadaphisek Rd., Dindaeng, Bangkok 10400
Tel. (662) 697-5300 Fax. (662) 642-3096
www.thaicreditbank.com

11. พนักงานต้องไม่ให้บุคคลอื่นยืมทรัพย์สินสารสนเทศ ไม่ว่าในกรณีใดๆ เว้นแต่ได้รับการพิจารณาอนุมัติจากหน่วยงานต้นสังกัดหรือผู้มีอำนาจอนุมัติของธนาคาร
12. มีการควบคุม ห้ามวางทิ้งทรัพย์สินสารสนเทศหรือข้อมูลสำคัญไว้ในที่ที่ไม่ปลอดภัยโดยไม่มีผู้ดูแล
13. พนักงานต้องรับผิดชอบชดใช้ค่าเสียหาย ไม่ว่าจะเป็นการชำรุด สูญหาย ตามมูลค่าทรัพย์สิน หากความเสียหายนั้นเกิดจากความประมาทเลินเล่อของพนักงาน

การใช้งานอุปกรณ์คอมพิวเตอร์

14. ผู้ได้รับสิทธิมีหน้าที่รับผิดชอบต่อการรักษาความปลอดภัยข้อมูลที่ถูกจัดเก็บอยู่ในเครื่องคอมพิวเตอร์ของผู้ได้รับสิทธิ รับผิดชอบต่อการใช้งานเครื่องคอมพิวเตอร์ และซอฟต์แวร์ที่ตนได้รับสิทธิใช้งาน รวมถึงการป้องกันมิให้บุคคลภายนอกหรือผู้ที่ไม่ได้รับสิทธิใช้เครื่องคอมพิวเตอร์ของตนเองโดยไม่ได้รับอนุญาต
15. พนักงานต้องทำการล็อกอิน (Log In) ทุกครั้งที่มีการใช้งาน เมื่อเข้าใช้เครื่องคอมพิวเตอร์ ระบบงาน และระบบเครือข่าย โดยใช้บัญชีผู้ใช้ (User ID) และรหัสผ่าน (Password) ตามที่ตนได้รับสิทธิให้ใช้เท่านั้น ทั้งนี้รหัสผ่าน (Password) ต้องเป็นไปตามนโยบายรหัสผ่าน (Password Policy)
16. พนักงานต้องทำการล็อกหน้าจอ (Screen Lock) ทุกครั้งเมื่อไม่ได้ใช้งานเครื่องคอมพิวเตอร์ มากกว่า 15 นาที เพื่อป้องกันผู้ประสงค์ร้ายมาสวมสิทธิ์การใช้งานเครื่อง
17. พนักงานต้องทำการปิดเครื่อง (Shut down) เครื่องคอมพิวเตอร์และจอภาพทุกครั้งหลังใช้งานเสร็จแล้ว
18. การใช้สื่อบันทึกข้อมูลพกพา (Removable media) เช่น Universal Serial Bus (USB) หรือ External Harddisk เป็นต้น ต้องได้รับการพิจารณาอนุมัติจากหน่วยงานต้นสังกัดและสายงานเทคโนโลยีสารสนเทศ พร้อมทั้งต้องมีการตรวจสอบไวรัสคอมพิวเตอร์ สปายแวร์ สแปมเมล์ ก่อนนำมาใช้งาน เพื่อป้องกันการแพร่กระจายไวรัสคอมพิวเตอร์ในองค์กร
19. ผู้ได้รับสิทธิในการใช้งานเครื่องคอมพิวเตอร์ประเภท Notebook / Tablet ต้องดำเนินการดังนี้
    (1) ไม่วาง หรือฝากเครื่องคอมพิวเตอร์ Notebook / Tablet โดยไม่มีผู้ดูแลหรือไม่มีอุปกรณ์ในการป้องกันการสูญหาย
    (2) ติดตั้งอุปกรณ์รักษาความปลอดภัย เช่น สายล็อกที่โต๊ะทำงาน รวมทั้งเมื่อนำเครื่องคอมพิวเตอร์ Notebook/Tablet ไปใช้ในที่สาธารณะ เช่น ห้องประชุม/สัมมนา ห้องพักในโรงแรม
    (3) ไม่เชื่อมต่อเครื่องคอมพิวเตอร์ Notebook/Tablet กับเครือข่ายสาธารณะที่ไม่มีระบบการรักษาความปลอดภัยที่เพียงพอ (Unsecured)
    (4) กำหนดให้พนักงานที่มีความจำเป็นต้องเชื่อมต่อเข้ามายังระบบสารสนเทศของธนาคารจากภายนอก ต้องผ่าน เครือข่าย VPN ที่ธนาคารกำหนด

บมจ.ธนาคารไทยเครดิต
123 อาคารไทยประกันชีวิต ถนนรัชดาภิเษก เขตดินแดง
เขตดินแดง กรุงเทพฯ 10400
Thai Credit Bank Public Company Limited
123 Thai Life Insurance Bldg., Ratchadaphisek Rd., Dindaeng,
Bangkok 10400
Tel. (662) 697-5300 Fax. (662) 642-3096
www.thaicreditbank.com

20. ห้ามผู้ได้รับสิทธิ ดำเนินการโยกย้ายเครื่องคอมพิวเตอร์จากสถานที่ตั้งที่กำหนด ไม่ว่าจะเป็นภายในชั้นเดียวกัน อาคารเดียวกัน หรือต่างอาคารต่างชั้น ตลอดจนกระทำการใดๆ อันเป็นเหตุให้เครื่องคอมพิวเตอร์และซอฟต์แวร์ไม่สามารถใช้งานได้
21. ห้ามดำเนินการถอดถอน หรือปรับแต่ง ต่อเติมเครื่องคอมพิวเตอร์และซอฟต์แวร์ โดยไม่ได้รับอนุญาตจากสายงานเทคโนโลยีสารสนเทศ
22. ไม่นำเครื่องคอมพิวเตอร์ หรืออุปกรณ์อื่นใด ที่ธนาคารมิได้จัดหาให้มาใช้งานในระบบเครือข่ายสื่อสารของธนาคาร เว้นแต่ได้รับการพิจารณาอนุมัติจากหน่วยงานต้นสังกัด และผู้มีอำนาจสูงสุดของสายงานเทคโนโลยีสารสนเทศ เป็นกรณีๆ ไป
23. ห้ามผู้ได้รับสิทธิใช้งานเครื่องคอมพิวเตอร์โดยมีวัตถุประสงค์เพื่อการกุศล เพื่อความบันเทิง หรือเพื่อกิจกรรมอื่นใดที่ไม่เกี่ยวข้องกับธุรกิจของธนาคาร
24. ไม่ให้มีการจัดเก็บข้อมูลที่มีระดับชั้นความลับในเครื่องคอมพิวเตอร์ของพนักงาน แต่หากมีความจำเป็นต้องจัดเก็บ พนักงานต้องจัดให้มีการรักษาความปลอดภัยที่รัดกุมเพียงพอ โดยการกำหนดสิทธิการเข้าถึงหรือการเข้ารหัส เป็นต้น
25. ไม่ดำเนินการคัดลอกส่วนหนึ่งส่วนใดของข้อมูลความลับของธนาคารหรือลูกค้าออกนอกธนาคารโดยเด็ดขาด การละเมิดจะถูกดำเนินการทางวินัยและทางกฎหมายขั้นสูงสุด
26. พนักงานต้องดำเนินการจำกัดการเข้าถึง shared drive หรือ shared folder ตามความจำเป็นในการใช้งานและต้องบริหารจัดการเนื้อที่ในการจัดเก็บข้อมูลตามสิทธิ์ที่ได้รับและเพื่อการปฏิบัติงานเท่านั้น

การใช้งานทรัพย์สินด้านซอฟต์แวร์

27. ธนาคารให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญา ดังนั้นซอฟต์แวร์ที่ธนาคารอนุญาตให้ใช้งานหรือที่ธนาคารมีลิขสิทธิ์ พนักงานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น
28. ซอฟต์แวร์ที่ทางธนาคารได้จัดเตรียมไว้ให้พนักงาน ถือเป็นสิ่งจำเป็นต่อการทำงาน ห้ามมิให้พนักงานทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่นโดยพละการ
29. ไม่ติดตั้งซอฟต์แวร์ที่เครื่องคอมพิวเตอร์อื่นใดที่ธนาคารมิได้จัดหาให้ใช้งาน โดยการกระทำดังกล่าวถือเป็นการละเมิดนโยบายของธนาคาร ถึงแม้ซอฟต์แวร์ดังกล่าวจะเป็นซอฟต์แวร์ถูกกฎหมายก็ตาม และหากซอฟต์แวร์ที่ติดตั้งเป็นซอฟต์แวร์ละเมิดลิขสิทธิ์ ผู้ได้รับสิทธิต้องรับผิดชอบตาม พรบ. ลิขสิทธิ์ และกฎหมายอื่นๆ ที่เกี่ยวข้องทั้งหมด
30. ซอฟต์แวร์ที่นำมาใช้ในการประมวลผลและจัดเก็บข้อมูลลับหรือข้อมูลสำคัญขององค์กร ทั้งที่ได้มาจากการพัฒนาขึ้นโดยพนักงาน หรือที่ได้รับการจัดซื้อมา ต้องได้รับการตรวจสอบ ควบคุม และอนุมัติอย่างเหมาะสมโดยหน่วยงานเจ้าของระบบและสายงานเทคโนโลยีสารสนเทศ ก่อนนำมาติดตั้งใช้งานบนระบบเทคโนโลยีสารสนเทศของธนาคาร

บมจ.ธนาคารไทยเครดิต
123 อาคารไทยประกันชีวิต ถนนรัชดาภิเษก แขวงดินแดง เขตดินแดง กรุงเทพฯ 10400
Thai Credit Bank Public Company Limited
123 Thai Life Insurance Bldg., Ratchadaphisek Rd., Dindaeng Bangkok 10400
Tel. (662) 697-5300 Fax. (662) 642-3096
www.thaicreditbank.com

31. ระบบสารสนเทศทั้งหมดที่ถูกใช้งานโดยผู้ใช้งานทั่วไป ต้องมีเอกสารสนับสนุนการใช้งานอย่างเพียงพอ เพื่อให้ผู้ใช้งานทั่วไปขององค์กร มีความเข้าใจและสามารถใช้งานระบบสารสนเทศได้อย่างเหมาะสม

32. พนักงานต้องให้ความร่วมมือและอำนวยความสะดวกแก่ผู้บังคับบัญชา ผู้ดูแลเครือข่ายคอมพิวเตอร์ ในการตรวจสอบระบบความปลอดภัยของเครื่องคอมพิวเตอร์ส่วนบุคคลของพนักงาน และเครือข่ายคอมพิวเตอร์ รวมทั้งปฏิบัติตามคำแนะนำของผู้บังคับบัญชา ผู้ดูแลเครือข่ายคอมพิวเตอร์

การบริหารจัดการข้อมูล

33. พนักงานต้องปฏิบัติตามนโยบายที่เกี่ยวข้องกับการรักษาความปลอดภัยข้อมูลตามที่ธนาคารกำหนด

34. พนักงานต้องให้ความสำคัญและระมัดระวังต่อการใช้ข้อมูล ไม่ว่าข้อมูลนั้นจะเป็นของธนาคาร หรือเป็นข้อมูลของลูกค้า

35. ข้อมูลที่อยู่ภายในทรัพย์สินสารสนเทศของธนาคาร ถือเป็นทรัพย์สินของธนาคาร ห้ามไม่ให้พนักงานทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย โดยไม่ได้รับอนุญาต

36. พนักงานต้องบริหารจัดการข้อมูลหรือข้อมูลส่วนบุคคลให้เหมาะสมตามระดับชั้นข้อมูล (Data classification) เพื่อให้มีการรักษาความปลอดภัยข้อมูลอย่างเพียงพอ มีการรักษาความลับของข้อมูล (Confidentiality) ข้อมูลมีความถูกต้องเชื่อถือได้ (Integrity) และข้อมูลมีความพร้อมใช้งาน (Availability)

    (1) การจัดทำข้อมูล พนักงานจะต้องมีการกำหนดระดับชั้นความสำคัญของข้อมูลโดยอาจพิจารณาใช้สัญลักษณ์ หรือข้อความในการสื่อสาร เพื่อให้ผู้เกี่ยวข้องทราบและสามารถใช้ข้อมูลอย่างถูกต้อง

    (2) พนักงานต้องกำหนด การจัดเก็บ การสำรองข้อมูล ให้เหมาะสมกับประเภทของข้อมูล เพื่อป้องกันการสูญหาย และให้ข้อมูลมีความพร้อมใช้งาน

    (3) การใช้งานข้อมูล และการรับ-ส่ง เพื่อป้องกันการถูกเปิดเผย การนำไปใช้ และการเปลี่ยนแปลงแก้ไขข้อมูลโดยไม่ได้รับอนุญาต พนักงานต้องพิจารณากำหนดวิธีการให้เหมาะสมกับข้อมูลในแต่ละระดับชั้น การกำหนดสิทธิ์การเข้าถึงข้อมูล การป้องกันการเข้าถึงข้อมูล (Data Protection) เช่น การกำหนดรหัสการเปิดใช้ข้อมูล เป็นต้น

    (4) การเปิดเผยข้อมูลให้หน่วยงาน/บุคคลภายนอก (Disclose)

    - การเปิดเผยข้อมูลสามารถทำได้เพื่อบรรลุวัตถุประสงค์ในการประมวลผลข้อมูล หรือเกี่ยวข้องกับวัตถุประสงค์ในการเก็บรวบรวมข้อมูล โดยกำหนดผู้อนุมัติตามระดับชั้นความลับของข้อมูล

บมจ.ธนาคารไทยเครดิต
123 อาคารไทยประกันชีวิต ถนนรัชดาภิเษก แขวงดินแดง เขตดินแดง กรุงเทพฯ 10400
Thai Credit Bank Public Company Limited
123 Thai Life Insurance Bldg., Ratchadaphisek Rd., Dindaeng, Bangkok 10400
Tel. (662) 697-5300 Fax. (662) 642-3096
www.thaicreditbank.com

- การเปิดเผยข้อมูลส่วนบุคคล ต้องดำเนินการตามนโยบายคุ้มครองข้อมูลส่วนบุคคลที่ธนาคารประกาศใช้อย่างเคร่งครัด

(5) ข้อมูลที่ไม่ถูกใช้งานแล้ว พนักงานต้องมีการกำหนดวิธีการทำลายข้อมูลต้องมีการกำหนดวิธีการทำลายข้อมูล และระยะเวลาการทำลายข้อมูลที่เหมาะสมตามประเภทข้อมูล เพื่อป้องกันการเปิดเผยข้อมูล และให้เป็นไปตามระเบียบปฏิบัติธนาคารหรือหน่วยงานทางการที่เกี่ยวข้องได้กำหนดไว้

37. ห้ามพนักงานจัดเก็บข้อมูลและแชร์ไฟล์บนเว็บไซต์ที่ให้บริการฝากข้อมูลสาธารณะ (Public File Sharing)

38. ไม่ให้มีการจัดเก็บข้อมูลสำคัญหรือข้อมูลส่วนบุคคลในเครื่องคอมพิวเตอร์ของพนักงาน แต่หากมีความจำเป็นต้องจัดเก็บ พนักงานต้องจัดให้มีการรักษาความปลอดภัยที่รัดกุมเพียงพอ เช่น กำหนดสิทธิการเข้าถึง มีการเข้ารหัสข้อมูล เป็นต้น

39. ข้อมูลหรือข้อมูลส่วนบุคคลที่ใช้งานและจัดเก็บ ต้องไม่เป็นข้อมูลที่ได้มาจากการละเมิดลิขสิทธิ์ ข้อมูลที่ขัดต่อกฎหมาย ความสงบเรียบร้อย หรือศีลธรรมอันดีของประชาชน และการจัดเก็บข้อมูลส่วนบุคคลในทรัพย์สินของธนาคาร จะต้องไม่ก่อให้เกิดการรบกวนต่อการปฏิบัติงานหรือการใช้ระบบเทคโนโลยีสารสนเทศของธนาคาร ธนาคารมีสิทธิในการตรวจสอบการจัดเก็บข้อมูลหรือข้อมูลส่วนบุคคลได้ตลอดเวลา โดยไม่ต้องแจ้งให้พนักงานทราบ

40. พนักงานมีหน้าที่ในการดูแลรักษาและรับผิดชอบต่อข้อมูล หากพนักงานนำไปใช้ในทางที่ผิด หรือนำไปเผยแพร่โดยไม่ได้รับอนุญาต หรือทำให้สูญหาย เสียหายโดยเจตนาไม่สุจริต เป็นเหตุให้เกิดความเสียหายต่อธนาคารหรือบุคคลภายนอก พนักงานจะต้องรับผิดชอบต่อความเสียหายนั้นเป็นการเฉพาะบุคคล

41. การเจตนาเข้าถึงระบบหรือการเข้าถึงข้อมูลส่วนบุคคล (Data Privacy) โดยไม่ได้รับอนุญาต การจงใจใส่ข้อมูลที่ผิดพลาด และการเจตนาเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต ถือเป็นสิ่งต้องห้ามทั้งสิ้น การไม่ปฏิบัติตามนโยบายการรักษาความมั่นคงด้านเทคโนโลยีสารสนเทศนี้ ถือว่ามีความผิดทางวินัย

การป้องกันโปรแกรมไม่ประสงค์ดี

42. เครื่องที่ใช้งานต้องมีการติดตั้งโปรแกรมรักษาความปลอดภัย Anti-virus / Anti-malware โดยมีการปรับปรุงประสิทธิภาพของการป้องกันโปรแกรมไม่ประสงค์ดี (Malware) ให้เพียงพอและเป็นปัจจุบัน เพื่อให้สามารถป้องกันภัยคุกคามใหม่ๆ ได้

43. พนักงานต้องทำการตรวจสอบเครื่องคอมพิวเตอร์ เครื่องคอมพิวเตอร์พกพา หรืออุปกรณ์อื่นๆ ที่ผู้ใช้งานรับผิดชอบให้มีการติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Anti-virus) และโปรแกรมป้องกันโปรแกรมไม่ประสงค์ดี (Anti-malware) และติดตามดูแลการอัปเดตซอฟต์แวร์ให้เป็นปัจจุบันอยู่เสมอ

บมจ.ธนาคารไทยเครดิต
123 อาคารไทยประกันชีวิต ถนนรัชดาภิเษก แขวงดินแดง เขตดินแดง กรุงเทพฯ 10400
Thai Credit Bank Public Company Limited
123 Thai Life Insurance Bldg., Ratchadaphisek Rd., Dindaeng, Bangkok 10400
Tel. (662) 697-5300 Fax. (662) 642-3096
www.thaicreditbank.com

44. ห้ามพนักงานดำเนินการถอดถอน ระงับการทำงาน หรือปรับแต่งโปรแกรมรักษาความปลอดภัย Anti-virus / Anti-malware จากเครื่องคอมพิวเตอร์ที่ใช้งาน

45. กำหนดให้พนักงานมีการตรวจสอบไวรัสคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดี (Scan) เป็นประจำสม่ำเสมอ ตามรอบระยะเวลาที่กำหนด ต้องทำการตรวจสอบข้อมูลที่ได้รับจากภายนอกองค์กรทุกครั้งด้วยโปรแกรมรักษาความปลอดภัย Anti-Virus / Anti-malware

46. หากพบว่ามีการติดไวรัสคอมพิวเตอร์ พนักงานต้องไม่เชื่อมต่อเข้าสู่ระบบเทคโนโลยีสารสนเทศของธนาคาร และต้องแจ้งสายงานเทคโนโลยีสารสนเทศทันที

การใช้งานอินเทอร์เน็ต

47. ธนาคารจัดหาบริการอินเทอร์เน็ตไว้เพื่อสนับสนุนการดำเนินธุรกิจของธนาคาร และอำนวยความสะดวกแก่พนักงานในการปฏิบัติงาน การวิจัยการค้นหาข้อมูลความรู้ และการติดต่อสื่อสารกับบุคคลภายนอก

48. พนักงานต้องใช้งานอินเทอร์เน็ตด้วยความระมัดระวัง และการใช้งานนั้นต้องไม่เป็นสาเหตุให้ธนาคารและบุคคลผู้ที่เกี่ยวข้องกับองค์กรเสื่อมเสียชื่อเสียง หรือเกี่ยวพันกับการกระทำที่ผิดกฎหมาย ทั้งนี้การใช้งานอินเทอร์เน็ตในทางที่ผิด ถือเป็นความผิดทางวินัยและอาจถูกดำเนินคดีตามกฎหมาย

49. การเข้าใช้งานอินเทอร์เน็ตต้องเข้าใช้งานผ่านช่องทาง (Gateway) ที่ได้รับอนุญาต หรือผ่านเครื่องคอมพิวเตอร์ลูกข่ายที่ได้รับการจัดเตรียมเพื่อใช้งานเท่านั้น ทั้งนี้ธนาคารขอสงวนสิทธิ์ในการตรวจสอบการใช้งานอินเทอร์เน็ตของพนักงาน เพื่อตรวจสอบการใช้งานในลักษณะที่ไม่เหมาะสม

50. ห้ามไม่ให้พนักงานดำเนินการ ดังต่อไปนี้

    (1) ใช้อินเทอร์เน็ตหรือระบบเครือข่ายคอมพิวเตอร์เพื่อการกระทำผิดกฎหมายหรือก่อความเสียหายให้แก่ธนาคาร หรือบุคคลอื่น

    (2) ใช้อินเทอร์เน็ตหรือระบบเครือข่ายคอมพิวเตอร์เพื่อขัดขวางการใช้งานของเครือข่ายคอมพิวเตอร์ของธนาคาร หรือเพื่อให้เครือข่ายคอมพิวเตอร์ของธนาคารไม่สามารถใช้งานได้ตามปกติ

    (3) คลิกหน้าต่างโฆษณา หรือเข้าสู่เว็บไซต์ใดๆ ที่โฆษณาโดยสแปม เนื่องจากเว็บไซต์เหล่านี้อาจมีโปรแกรมมุ่งร้ายแฝงอยู่ หรืออาจโจรกรรมข้อมูลในเครื่องคอมพิวเตอร์ของพนักงาน โดยที่พนักงานไม่ได้รับทราบหรือไม่ได้อนุญาต

    (4) เข้าชม ดาวน์โหลด หรือทำซ้ำสื่อลามกอนาจาร และสื่ออื่นใดที่ไม่เหมาะสมหรือผิดกฎหมาย

บมจ.ธนาคารไทยเครดิต
123 อาคารไทยประกันชีวิต ถนนรัชดาภิเษก แขวงดินแดง เขตดินแดง กรุงเทพฯ 10400
Thai Credit Bank Public Company Limited
123 Thai Life Insurance Bldg., Ratchadaphisek Rd., Dindaeng Bangkok 10400
Tel. (662) 697-5300 Fax. (662) 642-3026
www.thaicreditbank.com

(5) แสดงความคิดเห็นส่วนตัวในรูปแบบอิเล็กทรอนิกส์ (เช่น ผ่านทางเว็บบอร์ด บล็อก หรือโซเชียลมีเดีย) ของพนักงาน ทั้งนี้ความเสียหายใดๆ ที่อาจเกิดขึ้นจากการแสดงความคิดเห็นดังกล่าวถือเป็นความรับผิดชอบของพนักงาน

(6) คัดลอกข้อมูล หรือเผยแพร่ ข้อมูล ที่ไม่เหมาะสม หรืออาจก่อให้เกิดความรุนแรง ทำลายชื่อเสียงของธนาคารหรือของบุคคลภายนอก หยาบคาย ลามกอนาจารขัดต่อกฎหมาย ความสงบเรียบร้อย หรือศีลธรรมอันดีของประชาชน และความมั่นคงของประเทศ หรือกระทบต่อกิจการของธนาคาร

(7) ใช้อินเทอร์เน็ตหรือระบบเครือข่ายคอมพิวเตอร์เพื่อความบันเทิง เล่นการพนัน ขายสินค้า หาประโยชน์ส่วนตัว ละเมิดลิขสิทธิ์ หรือกระทำอื่นใดที่อยู่นอกเหนือขอบเขตจริยธรรม หรือพฤติกรรมอันเหมาะสม

(8) ใช้อินเทอร์เน็ตหรือระบบเครือข่ายคอมพิวเตอร์เพื่อการเปิดเผยที่เป็นความลับ ซึ่งได้มาจากการปฏิบัติงาน ทั้งข้อมูลของทางธนาคารและข้อมูลของลูกค้า

(9) ใช้อินเทอร์เน็ตหรือระบบเครือข่ายคอมพิวเตอร์ในทางละเมิดทรัพย์สินทางปัญญาของธนาคารหรือบุคคลอื่น

(10) เปิดหรือใช้งานโปรแกรมสื่อสารข้อความทางอินเทอร์เน็ต (Messaging/Chat) ทุกประเภท เว้นแต่จะได้รับการอนุญาตจากผู้มีอำนาจอนุมัติเท่านั้น

การใช้งานอีเมลหรือระบบจดหมายอิเล็กทรอนิกส์ (Electronic mail)

51. ผู้ได้รับสิทธิต้องใช้งานอีเมลตามสิทธิ์และหน้าที่ความรับผิดชอบที่ได้รับมอบหมาย เพื่อรองรับการปฏิบัติงานในธุรกิจของธนาคารเท่านั้น ห้ามมิให้ใช้งานเพื่อวัตถุประสงค์อื่น
52. ผู้ได้รับสิทธิมีหน้าที่ในการดูแล รักษา บัญชีอีเมลและรหัสผ่าน ห้ามผู้ใช้งานนำบัญชีอีเมลของตนเองไปให้ผู้อื่นใช้งาน
53. ผู้ได้รับสิทธิใช้งานอีเมลต้องคำนึงถึงการรักษาความมั่นคงปลอดภัยข้อมูล จัดให้มีการเข้ารหัสข้อมูลต้องปฏิบัติตามนโยบายการจัดชั้นข้อมูลของธนาคาร
54. การส่งอีเมล ผู้ได้รับสิทธิต้องระบุชื่อผู้รับ หัวเรื่อง ให้ชัดเจน พร้อมทั้งตรวจสอบความถูกต้องของชื่อผู้รับ เนื้อหาและข้อมูลที่แนบไปกับอีเมล เพื่อเป็นการป้องกันการรั่วไหลของข้อมูล
55. ผู้ได้รับสิทธิใช้งานอีเมลกลาง ต้องดำเนินการตรวจสอบอีเมลกลางเป็นประจำ หากไม่มีความจำเป็นต้องใช้งานให้ทำการขอยกเลิกการใช้อีเมลกลางนั้น
56. ผู้ได้รับสิทธิต้องดำเนินการลบอีเมลที่ไม่จำเป็นออกจาก Mailbox ของตนอยู่เสมอ เพื่อเป็นการรักษาพื้นที่เก็บอีเมลให้เป็นไปตามขนาดที่ธนาคารกำหนด

บมจ.ธนาคารไทยเครดิต
123 อาคารไทยประกันชีวิต ถนนรัชดาภิเษก แขวงดินแดง เขตดินแดง กรุงเทพฯ 10400
Thai Credit Bank Public Company Limited
123 Thai Life Insurance Bldg., Ratchadapisek Rd., Dindaeng, Bangkok 10400
Tel. (662) 697-5300 Fax. (662) 642-3096
www.thaicreditbank.com

57. ห้ามไม่ให้พนักงานดำเนินการ ดังต่อไปนี้

(1) ใช้ระบบอีเมลสาธารณะ (Public Email) หรือระบบอีเมลส่วนตัว เช่น Hotmail, Gmail, Yahoo mail เป็นต้น เว้นแต่ในกรณีที่ระบบอีเมลของธนาคารขัดข้องและต้องได้รับการพิจารณาอนุมัติจากผู้มีอำนาจอนุมัติเท่านั้น

(2) ส่งอีเมลหรือเอกสารสำคัญของธนาคารต่อบุคคลภายนอก โดยไม่ได้รับอนุญาต

(3) ให้ข้อมูลข่าวสารแก่บุคคลอื่น โดยไม่ได้รับอนุญาตจากธนาคารหรือผู้ที่มีสิทธิในข้อมูลดังกล่าว

(4) ส่งอีเมลที่มีลักษณะเป็นการผิดกฎหมาย ละเมิดสิทธิส่วนบุคคล หรือสื่อลามก ใช้ข้อความวาจาที่ไม่สุภาพ ขัดต่อศีลธรรม ความสงบเรียบร้อย

(5) ระมัดระวังการเปิดเอกสารหรือไฟล์แนบที่ส่งมาทางอีเมล หรือคลิกลิงก์ที่แนบมาในอีเมลที่ส่งมาจากบุคคลที่ไม่รู้จัก

(6) ใช้ระบบอีเมลของธนาคารเพื่อเผยแพร่ข้อมูลและโปรแกรมที่ไม่ประสงค์ดี มีลักษณะเป็นอันตรายต่อผู้อื่น

(7) ส่งข้อความที่เป็นความเห็นส่วนบุคคล โดยอ้างว่าเป็นความเห็นของธนาคาร หรือก่อให้เกิดความเสียหายต่อธนาคาร

(8) ส่งอีเมลครั้งละจำนวนมาก เช่น ส่งหาผู้รับทุกคนในธนาคาร (All Users) ผู้รับที่มีลักษณะเป็นกลุ่ม รวมทั้งส่งไฟล์ที่มีขนาดใหญ่ เว้นแต่ได้รับการพิจารณาอนุมัติจากผู้มีอำนาจอนุมัติเท่านั้น

(9) นำบัญชีอีเมล ซึ่งเป็นของธนาคารไปเผยแพร่สู่บุคคลอื่น ไม่ว่าจะเป็นทางใดก็ตาม เช่น การโพสต์ในช่องทางสื่ออิเล็กทรอนิกส์ เป็นต้น เว้นแต่การเผยแพร่นั้นจัดทำขึ้นเพื่อการดำเนินธุรกิจของธนาคาร และต้องได้รับการพิจารณาอนุมัติจากผู้มีอำนาจอนุมัติของธนาคารเท่านั้น

การใช้อุปกรณ์ส่วนตัว (Bring Your Own Device : BYOD)

58. ห้ามพนักงานใช้อุปกรณ์ส่วนตัว ในการเข้าถึงระบบเครือข่ายสื่อสาร ระบบงานและข้อมูลของธนาคาร หากมีความจำเป็นต้องได้รับการพิจารณาอนุมัติจากหน่วยงานต้นสังกัดและผู้มีอำนาจอนุมัติของธนาคาร เป็นกรณีๆ ไป

59. พนักงานต้องทำการตรวจสอบ วิเคราะห์ และความเสี่ยงของอุปกรณ์ที่นำมาใช้งานในธนาคาร โดยเครื่องคอมพิวเตอร์ ต้องติดตั้ง Anti-virus/ Anti-malware หรือโปรแกรมตามที่ธนาคารกำหนด

60. พนักงานต้องกำหนดรหัสผ่านเพื่อใช้ในการล็อกหรือปลดล็อกในการเข้าถึงอุปกรณ์ส่วนตัว

61. ห้ามพนักงานใช้อุปกรณ์โทรศัพท์เคลื่อนที่ (Tablet / Smartphone) ที่ถูกปรับแต่ง (Rooted หรือ Jail broken) ลงทะเบียนใช้งาน BYOD

บมจ.ธนาคารไทยเครดิต
123 อาคารไทยประกันชีวิต ถนนรัชดาภิเษก แขวงดินแดง เขตดินแดง กรุงเทพฯ 10400
Thai Credit Bank Public Company Limited
123 Thai Life Insurance Bldg., Ratchadaphisek Rd., Dindaeng, Bangkok 10400
Tel. (662) 697-5300 Fax. (662) 642-3096
www.thaicreditbank.com

การเข้าถึงพื้นที่สำนักงาน

62. พนักงานและบุคคลภายนอกต้องติดบัตรพนักงานตลอดเวลาที่อยู่ในพื้นที่สำนักงาน ทั้งนี้บัตรพนักงานและบัตรผู้มาติดต่อไม่อนุญาตให้โอนกรรมสิทธิ หรือหยิบยืมกันใช้งาน
63. พนักงานต้องแจ้งพนักงานรักษาความปลอดภัยทันที เมื่อพบเห็นบุคคลแปลกหน้าในพื้นที่สำนักงานโดยไม่มีผู้ติดตามดูแล (Escort)
64. พนักงานต้องติดตาม ควบคุมดูแล และให้คำแนะนำผู้ที่มาติดต่อกับตนตลอดเวลาที่ผู้มาติดต่อนั้นอยู่ในพื้นที่สำนักงาน

การปฏิบัติตามกฎหมาย นโยบาย และข้อบังคับ

65. กฎหมาย ระเบียบ ข้อบังคับ ที่เกี่ยวข้องกับการใช้เทคโนโลยีสารสนเทศ ซึ่งได้ประกาศใช้แล้วหรือที่จะประกาศใช้ในภายหน้า ถือเป็นสิ่งสำคัญที่พนักงานจะต้องให้ความสำคัญและปฏิบัติอย่างเคร่งครัด หากพนักงานกระทำความผิดหรือฝ่าฝืนต่อกฎหมาย นโยบาย และข้อบังคับ ให้ถือเป็นความผิดที่พนักงานจะต้องรับผิดเป็นการเฉพาะบุคคล
66. ธนาคารขอสงวนสิทธิ์ในการเข้าถึง ทบทวน และตรวจสอบอีเมลของผู้ใช้งาน โดยไม่จำเป็นต้องแจ้งให้ทราบล่วงหน้า อย่างไรก็ตาม ธนาคารจะดำเนินการตรวจสอบดังกล่าวต่อเมื่อมีความจำเป็นเท่านั้น และจะไม่เปิดเผยข้อมูลใดๆ ของผู้ใช้งาน เว้นแต่เป็นการเปิดเผยตามคำสั่งจากผู้มีอำนาจของธนาคาร ศาล ตามบทบังคับของกฎหมาย หรือด้วยความยินยอมจากผู้ใช้งานเท่านั้น

การบังคับใช้และบทลงโทษ

67. พนักงานต้องปฏิบัติตามนโยบายและข้อบังคับฉบับนี้โดยเคร่งครัด การกระทำที่มีเจตนาฝ่าฝืนที่อาจจะเกิดความเสียหายต่อธนาคารหรือต่อบุคคลอื่นหรือไม่ก็ตามให้ถือเป็นการปฏิบัติที่ขัดต่อนโยบายหรือข้อบังคับฉบับนี้
68. พนักงานมีหน้าที่ในการควบคุมการปฏิบัติงานของผู้ใต้บังคับบัญชา จะต้องควบคุมดูแลให้ผู้ใต้บังคับบัญชาปฏิบัติตามนโยบายและข้อบังคับฉบับนี้อย่างเคร่งครัด หากพบว่าผู้ใต้บังคับบัญชากระทำความผิด ผู้บังคับบัญชามีหน้าที่ต้อดำเนินการตามกฎระเบียบข้อบังคับของธนาคาร อย่างเคร่งครัด การละเว้นการปฏิบัติหน้าที่ถือเป็นความผิดเช่นเดียวกับพนักงานผู้กระทำความผิด
69. การพิจารณาลงโทษ ปฏิบัติตามประกาศข้อบังคับเกี่ยวกับการทำงาน ธนาคารไทยเครดิต จำกัด (มหาชน)
70. การกระทำที่ถือเป็นความผิดทางแพ่ง และอาญา พนักงานผู้นั้นต้องรับผิดเป็นการเฉพาะบุคคล

บมจ.ธนาคารไทยเครดิต
123 อาคารไทยประกันชีวิต ถนนรัชดาภิเษก แขวงดินแดง เขตดินแดง กรุงเทพฯ 10400
Thai Credit Bank Public Company Limited
123 Thai Life Insurance Bldg., Ratchadaphisek Rd., Dindaeng Bangkok 10400
Tel. (662) 697-5300 Fax. (662) 642-3096
www.thaicreditbank.com