บริษัท บริหารสินทรัพย์ ธนาคารอิสลามแห่งประเทศไทย จำกัด

นโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศ
(Information Technology Security Policy)
บริษัท บริหารสินทรัพย์ ธนาคารอิสลามแห่งประเทศไทย จำกัด

---

1. หลักการและเหตุผล

บริษัท บริหารสินทรัพย์ ธนาคารอิสลามแห่งประเทศไทย จำกัด (บริษัท) เป็นรัฐวิสาหกิจ สังกัดกระทรวงการคลัง ได้นำระบบเทคโนโลยีสารสนเทศมาเป็นหลักในการให้บริการทางด้านการเงิน และข้อมูลสารสนเทศที่อยู่ในระบบเทคโนโลยีสารสนเทศ มีความสำคัญเทียบเท่ากับสินทรัพย์ประเภทอื่น ๆ ของบริษัท ซึ่งหากไม่มีการป้องกันและรักษาข้อมูลสารสนเทศอย่างเพียงพอ อาจเป็นสาเหตุให้เกิดความเสียหาย ซึ่งจะส่งผลกระทบต่อการปฏิบัติงานและการดำเนินธุรกิจ ดังนั้น บริษัทจึงจัดทำนโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศขึ้น เพื่อเป็นแนวทางการดำเนินงานรักษาความปลอดภัยแก่ข้อมูลและระบบสารสนเทศของบริษัทให้เป็นไปอย่างเหมาะสม

2. วัตถุประสงค์

2.1 เพื่อกำหนดแนวทางในการรักษาความปลอดภัยแก่ระบบสารสนเทศอย่างมีประสิทธิภาพ ตามมาตรฐานการรักษาความปลอดภัยด้านเทคโนโลยีสารเทศ ISO/IEC 27001 ตามเกณฑ์ของธนาคารแห่งประเทศไทย และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

2.2 เพื่อเสริมสร้างความมั่นใจให้กับลูกค้าของบริษัทในด้านความสามารถในการให้บริการและรักษาความลับของข้อมูลและระบบเทคโนโลยีสารสนเทศ

2.3 เพื่อเป็นแนวทางกำหนดในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศของบริษัทให้สอดคล้องกับการควบคุมภายในที่ดีด้านสารสนเทศ และให้เป็นไปตามกฎหมาย ระเบียบ และข้อกำหนดที่เกี่ยวข้องกับทางการ รวมทั้งเพื่อป้องกันมิให้เกิดการกระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และฉบับแก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ. 2560 ต่อการใช้ระบบสารสนเทศของบริษัท

3. คำนิยาม

“บริษัท” หมายความว่า บริษัท บริหารสินทรัพย์ ธนาคารอิสลามแห่งประเทศไทย จำกัด

“คณะกรรมการบริษัท” หมายความว่า คณะกรรมการบริษัท บริหารสินทรัพย์ ธนาคารอิสลามแห่งประเทศไทย จำกัด

“ผู้จัดการบริษัท” หมายความว่า ผู้จัดการบริษัท บริหารสินทรัพย์ ธนาคารอิสลามแห่งประเทศไทย จำกัด และในกรณีที่ผู้จัดการบริษัทเป็นกรรมการบริษัทด้วย ให้เรียกว่า “กรรมการผู้จัดการบริษัท” และให้หมายความรวมถึงผู้ปฏิบัติหน้าที่หรือผู้รักษาการในตำแหน่งผู้จัดการบริษัทด้วย

“พนักงานระดับบริหาร” หมายความว่า พนักงานที่ดำรงตำแหน่งรองผู้จัดการบริษัท ผู้ช่วยผู้จัดการบริษัท และผู้จัดการฝ่าย ตามลำดับชั้น

“พนักงาน” หมายความว่า ผู้ซึ่งบริษัทได้จ้างไว้ให้ปฏิบัติงานในลักษณะประจำ และรับเงินเดือนตามระดับตำแหน่งที่กำหนด ทั้งนี้ ไม่รวมถึงผู้จัดการบริษัท

“ผู้ใช้งาน” หมายความว่า พนักงานหรือเจ้าหน้าที่ ลูกจ้างประจำหรือลูกจ้างชั่วคราวของบริษัท และผู้ใช้งานทั่วไป โดยเป็นผู้ที่ได้รับอนุญาตจากบริษัทให้ใช้ข้อมูลระบบเทคโนโลยีสารสนเทศ โดยให้เป็นไปตามข้อกำหนดของบริษัท

“สินทรัพย์” หมายความว่า สิ่งที่มีคุณค่าหรือมูลค่าต่อบริษัท และเป็นสิ่งที่เกี่ยวข้องกับการประมวลผลสารสนเทศที่บริษัทเป็นเจ้าของ หรือผู้ถือลิขสิทธิ์การใช้งานอย่างถูกต้องตามกฎหมาย ซึ่งรวมถึงทรัพย์สินทางปัญญา ไม่ว่าจะได้มาจากการเช่า การว่าจ้าง การพัฒนา หรือการจัดซื้อ ได้แก่ ข้อมูลสารสนเทศ (Information Asset) ด้านกายภาพ (Physical Asset) ด้านซอฟท์แวร์ (Software Asset) การบริหารและกระบวนการ (Services and Processes Asset) และบุคลากร (People Asset)

“ข้อมูล” หมายความว่า สิ่งที่สื่อความหมายให้รู้เรื่องราว ข้อเท็จจริง ข้อมูล หรือสิ่งใด ๆ ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเอง หรือโดยผ่านวิธีการใด ๆ และไม่ว่าจะจัดทำไว้ในรูปแบบของเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏเป็นสินทรัพย์ชนิดหนึ่งที่มีมูลค่าและความสำคัญแก่บริษัท

“ความมั่นคงปลอดภัยด้านสารสนเทศ” หมายความว่า การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพความพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิดชอบ (Accountability) การห้ามปฏิเสธความรับผิดชอบ (Non-Repudiation) และความน่าเชื่อถือ (Reliability)

“เหตุการณ์ด้านความมั่นคงปลอดภัย” หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์สถานะของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศหรือมาตรการป้องกันที่ล้มเหลวหรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

“สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด” หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบของบริษัทถูกบุกรุกหรือถูกโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

“สิทธิของผู้ใช้งาน” หมายความว่า สิทธิในการกระทำการใด ๆ ต่อระบบสารสนเทศและข้อมูลสารสนเทศของบริษัท

"การเข้าถึงหรือการควบคุมการใช้งานสารสนเทศ" หมายความว่า การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์หรือทางกายภาพ

"ผู้ให้บริการภายนอก" หมายความว่า บุคคลภายนอก ทั้งในและต่างประเทศ รวมถึงบริษัทในกลุ่มธุรกิจเดียวกัน ซึ่งเข้าทำสัญญาหรือทำข้อตกลงในการให้บริการงานให้กับบริษัท อันมีลักษณะที่โดยปกติแล้วบริษัทต้องดำเนินการเอง

"ผู้พัฒนาระบบ" หมายความว่า ผู้ที่ได้รับมอบหมายจากบริษัทให้เขียนโปรแกรมคอมพิวเตอร์ และพัฒนาระบบงานทางคอมพิวเตอร์

"คณะอนุกรรมการบริหารจัดการและกำกับดูแลการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ" หมายความว่า คณะอนุกรรมการที่ทำหน้าที่กำหนดแผนและควบคุมดูแลการพัฒนาระบบสารสนเทศ พิจารณาการลงทุนและความเหมาะสมเกี่ยวกับระบบงานสารสนเทศที่จะดำเนินการ เสนอแนะ และให้คำปรึกษาในการแก้ไขปัญหา และอุปสรรคเกี่ยวกับระบบสารสนเทศของบริษัท มีอำนาจในการเรียกข้อมูลเอกสาร บุคคล หรือหน่วยงานที่เกี่ยวข้องมาตรวจสอบหรือให้คำชี้แจงได้ และส่งรายงานการประชุมให้คณะกรรมการบริษัทรับทราบ และปฏิบัติหน้าที่อื่น ๆ ตามที่ได้รับมอบหมายจากคณะกรรมการบริษัท

"ระบบเทคโนโลยีสารสนเทศ" หมายความว่า ข้อมูลของบริษัทที่พร้อมสำหรับการใช้งาน หรือได้รับการรวบรวมไว้สำหรับใช้งาน ได้แก่ แบบฟอร์มและเอกสารสายงานสารสนเทศ ฐานข้อมูล และโปรแกรมประยุกต์ต่าง ๆ

"เครือข่ายคอมพิวเตอร์" หมายความว่า เครือข่ายคอมพิวเตอร์ของบริษัท

"งานเทคโนโลยีสารสนเทศ" หมายความว่า งานด้านเทคโนโลยีสารสนเทศ (Information Technology – IT) ที่ครอบคลุมถึงระบบงาน (Application) ข้อมูล (Information) โครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ (Infrastructure) และบุคลากรและกระบวนการที่จัดการด้านเทคโนโลยีสารสนเทศ (People and Process)

"อุปกรณ์พกพา" หมายความว่า อุปกรณ์ที่ใช้ในการติดต่อสื่อสาร ประมวลผลข้อมูล และ/หรือจัดเก็บข้อมูล โดยผู้ใช้งานสามารถนำพาและเคลื่อนย้ายได้โดยสะดวก ซึ่งรวมถึงอุปกรณ์พกพาที่เป็นสินทรัพย์ของบริษัทและอุปกรณ์พกพาส่วนตัวที่ผู้ใช้งานนำมาใช้เองโดยนำมาใช้ภายในเครือข่ายของบริษัทที่ได้ลงทะเบียนและได้รับอนุญาตจากทางบริษัทให้ใช้ในการเข้าถึงข้อมูลและระบบเทคโนโลยีสารสนเทศของบริษัท เช่น เครื่องคอมพิวเตอร์แบบพกพา (Notebook/Laptop Computer) สมาร์ทโฟน (Smartphone) และแท็บเล็ต (Tablet) เป็นต้น

"ผู้ดูแลระบบ" หมายความว่า ผู้ที่ได้รับมอบหมายให้ดูแลงานเทคโนโลยีสารสนเทศ อันประกอบไปด้วย

(1) ผู้ดูแลระบบเครือข่าย (Network)

(2) ผู้ดูแลระบบปฏิบัติการ (Operation system)

(3) ผู้ดูแลระบบอิเล็กทรอนิกส์เมล์ (E-mail)

(4) ผู้ดูแลระบบ Gateway web / Proxy / Cache / Internet

(5) ผู้ดูแลระบบ Firewall / Remote access

(6) ผู้ดูแลระบบการจัดการฐานข้อมูล

(7) ผู้ดูแลระบบโปรแกรมประยุกต์

(8) ผู้ดูแลอุปกรณ์คอมพิวเตอร์และอุปกรณ์ต่อพ่วง

(9) ผู้ดูแลระบบเทคโนโลยีสารสนเทศอื่น ๆ ที่เกี่ยวข้อง

"ศูนย์ข้อมูล" หมายความว่า ศูนย์ข้อมูลหลัก และศูนย์ข้อมูลสำรอง

4. มาตรการการจัดการความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ

4.1 การกำหนดทิศทางป้องกันและรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ

บริษัทได้กำหนดทิศทางและให้การสนับสนุนการดำเนินการด้านความมั่นคงและปลอดภัยสำหรับสารสนเทศ ให้เป็นไปตามหรือสอดคล้องกับข้อกำหนดทางธุรกิจ กฎหมาย และระเบียบปฏิบัติที่เกี่ยวข้อง ดังนี้

4.1.1 บริษัทจะจัดทำนโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศสำหรับระบบสารสนเทศขององค์กรให้เป็นลายลักษณ์อักษร และเอกสารนโยบายดังกล่าว ต้องได้รับการอนุมัติจากคณะอนุกรรมการบริหารจัดการและกำกับดูแลการปฏิบัติงานด้านเทคโนโลยีสารสนเทศก่อนนำไปใช้งาน และต้องเผยแพร่ให้พนักงานและหน่วยงานภายนอกทั้งหมดที่เกี่ยวข้องได้รับทราบ

4.1.2 บริษัทต้องดำเนินการทบทวนนโยบายที่เกี่ยวข้องกับความปลอดภัยด้านเทคโนโลยีสารสนเทศ โดยจะต้องทบทวนตามรอบที่กำหนด หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ หรือทบทวนอย่างน้อยปีละ 1 ครั้ง

4.2 การกำหนดโครงสร้างหน้าที่การป้องกันและรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศภายในองค์กร (Organizational of Information Security)

4.2.1 คณะกรรมการบริษัทจะดำเนินการแต่งตั้ง "คณะอนุกรรมการบริหารจัดการและกำกับดูแลการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ" ขึ้น เพื่อทำหน้าที่บริหารและจัดการด้านความปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัท และทำหน้าที่เป็นที่ปรึกษาด้านระบบความปลอดภัยสารสนเทศ รวมทั้งพิจารณาถึงความเสี่ยงด้านเทคโนโลยีสารสนเทศที่มีผลกระทบต่อองค์กร เพื่อเสนอแนวทางป้องกันและแก้ไขต่อคณะกรรมการบริษัท

4.2.2 ฝ่ายงานที่มีหน้าที่ดูแลระบบจะต้องดำเนินการพิจารณาจัดวางกลยุทธ และมาตรการป้องกันและการรักษาความปลอดภัยเทคโนโลยีสารสนเทศ ทั้งด้านระบบสารสนเทศ และด้านการปฏิบัติงานของบุคลากร ให้เป็นไปตามนโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศฉบับนี้ และเพื่อประสานงานและให้ความร่วมมือกับหน่วยงานด้านความมั่นคงปลอดภัยภายนอก รวมถึงพิจารณาความเสี่ยงและการใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศในระดับที่เหมาะสมเพื่อให้เกิดคุณค่าเพิ่มและให้ทันต่อเหตุการณ์และสภาพแวดล้อมที่เกี่ยวข้อง ตลอดจนการปรับปรุงหรือทบทวนนโยบายดังกล่าวให้สอดคล้องกับมาตรฐานสากล

4.2.3 ผู้ดูแลระบบมีหน้าที่ดูแลบำรุงรักษาระบบเทคโนโลยีสารสนเทศของบริษัท และจัดทำรายงานการใช้งานระบบเครือข่าย รายงานการปรับปรุง การป้องกันต่าง ๆ ให้กับผู้บังคับบัญชาตามลำดับชั้นของฝ่ายงานที่มีหน้าที่รับผิดชอบดูแลเป็นรายเดือนหรือเมื่อเกิดเหตุเร่งด่วน เช่น ถูกบุกรุก หรือถูกโจมตีอย่างหนักจากผู้บุกรุก หรือระบบเครือข่ายเกิดปัญหา หรือมีเหตุอันควรต้องสงสัยได้ว่าจะเกิดปัญหาขึ้นในระบบเป็นต้น เพื่อเสนอแนวทางป้องกัน และแก้ไข ซึ่งในกรณีเกิดเหตุเร่งด่วนนี้ จะต้องรายงานผ่านระบบงานที่กำหนดให้กับหน่วยงานด้านบริหารความเสี่ยงรับทราบโดยทันทีอีกทางหนึ่งด้วย

4.2.4 ฝ่ายงานที่เกี่ยวข้องและฝ่ายงานที่เป็นผู้ใช้งานมีหน้าที่สนับสนุนข้อมูลต่าง ๆ ที่เกี่ยวข้องให้กับหน่วยงานที่ดูแลงานเทคโนโลยีสารสนเทศ เพื่อทำการวิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศ และสำหรับใช้ในการจัดทำและทบทวนนโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศ

4.2.5 ผู้ใช้งานมีหน้าที่ใช้ระบบสารสนเทศตามข้อกำหนดของบริษัทเท่านั้น หากพบข้อผิดปกติของงานเทคโนโลยีสารสนเทศ ผู้ใช้งานมีหน้าที่ในการแจ้งความผิดปกติที่พบให้หน่วยงานที่ดูแลงานเทคโนโลยีสารสนเทศทราบถึงความผิดปกติที่พบ

4.2.6 ผู้ใช้งานต้องให้ความร่วมมือในการเข้ารับการฝึกอบรมในด้านการรักษาความปลอดภัยข้อมูลและระบบสารสนเทศ เพื่อให้ผู้ใช้งานทุกคนรับทราบหน้าที่และความรับผิดชอบต่อระบบสารสนเทศของบริษัท รวมถึงต้องให้มีความตระหนักในการใช้งานเทคโนโลยีสารสนเทศ ให้เป็นไปตามระเบียบปฏิบัติของบริษัท

4.2.7 การใช้งานอุปกรณ์พกพาอย่างปลอดภัย (Mobile Device Security) เพื่อลดความเสี่ยงหรือความเสียหายที่อาจเกิดจากอุปกรณ์สื่อสารประเภทพกพา ต้องให้มีการควบคุมและปฏิบัติตามระเบียบปฏิบัติงานของบริษัท

4.2.8 เพื่อรักษาความมั่นคงปลอดภัยด้านสารสนเทศจากการปฏิบัติงานภายนอกบริษัท เพื่อลดความเสี่ยงหรือความเสียหายที่อาจเกิดขึ้น ต้องให้มีการควบคุมและปฏิบัติตามระเบียบปฏิบัติงานของบริษัท

4.3 การจัดการด้านการป้องกันและรักษาความปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human Resource Security)

4.3.1 การบริหารจัดการก่อนการจ้างงาน เพื่อให้มั่นใจว่าผู้ใช้งานเข้าใจถึงบทบาท หน้าที่ และความรับผิดชอบที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศก่อนการปฏิบัติงานอย่างเหมาะสม ต้องให้มีการควบคุมและปฏิบัติตามระเบียบปฏิบัติงานของบริษัท

4.3.2 การบริหารจัดการระหว่างการปฏิบัติงานเพื่อให้มั่นใจว่าผู้ใช้งานมีความตระหนักและมีความรู้ความเข้าใจในบทบาทหน้าที่ความรับผิดชอบเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ ต้องให้มีการควบคุมและปฏิบัติตามระเบียบปฏิบัติงานของบริษัท

4.3.3 การบริหารจัดการเมื่อสิ้นสุดการจ้างงาน เพื่อให้มั่นใจว่ามีมาตรการในการปกป้องผลประโยชน์ของบริษัทโดยมีกระบวนการที่เหมาะสมเมื่อผู้ใช้งานพ้นจากสภาพการจ้างงานหรือมีการเปลี่ยนแปลงโยกย้ายตำแหน่งหน้าที่งาน ต้องให้มีการควบคุมและปฏิบัติตามระเบียบปฏิบัติงานของบริษัท

4.4 การจัดการหมวดหมู่ และการควบคุมสินทรัพย์ของบริษัท (Assets Classification and Controlling)

บริษัทดำเนินการจัดทำทะเบียนบัญชีสินทรัพย์ ซึ่งรวมถึงทรัพย์สินทางปัญญาของบริษัทที่ได้จัดหามาให้เป็นหมวดหมู่ พร้อมกับวางมาตรการควบคุมที่รัดกุม เพื่อลดความเสี่ยงต่อการเสียหายหรือสูญหายของสินทรัพย์ และข้อมูลของบริษัทโดยให้เป็นไปตามกฎหมายด้านลิขสิทธิ์

4.4.1 การจัดหมวดหมู่สารสนเทศ (Information Classification)

จัดทำทะเบียนข้อมูลแบ่งตามหมวดหมู่ของสารสนเทศ ได้แก่ Hardware ประเภทต่าง ๆ และ Software ต่าง ๆ ที่ใช้อยู่ในปัจจุบัน ทั้งแบบมีลิขสิทธิ์ แบบใช้ฟรี และแบบเปิดเผย Source Code รวมไปถึงการกำหนดเกณฑ์ในการจำแนกระดับชั้นความลับของข้อมูล โดยคำนึงถึง มูลค่า กฎหมาย ความละเอียดอ่อน จะต้องมีการจำแนกระดับชั้นความลับของข้อมูล พร้อมทั้งกำหนดรูปแบบในการจัดการให้มีความเหมาะสมกับระดับชั้นความลับ

4.4.2 หน้าที่ความรับผิดชอบต่อสินทรัพย์ขององค์กร (Responsibility for Assets)

ควบคุมทะเบียนข้อมูลของสินทรัพย์ทางด้านระบบสารสนเทศของบริษัท ทั้งด้าน Hardware และ Software พร้อมทั้งรายงานการเคลื่อนย้าย และการเปลี่ยนแปลงของสินทรัพย์ จนถึงก่อนการตัดจำหน่าย

4.4.3 การจัดการสื่อบันทึกข้อมูล (Media Handling)

กำหนดให้มีกระบวนการจัดการสื่อบันทึกข้อมูล โดยมีการควบคุม การจัดเก็บการเคลื่อนย้าย และการทำลายสื่อบันทึกข้อมูล

4.5 การจัดการและการควบคุมการเข้าถึงระบบสารสนเทศ (Access Control)

บริษัทกำหนดมาตรการ หน้าที่ความรับผิดชอบ และสิทธิการใช้ระบบสารสนเทศ รวมทั้งการเข้าถึงข้อมูลสารสนเทศให้แก่ผู้ใช้งานตามความเหมาะสมและตามความจำเป็น ทั้งในส่วนควบคุมการเข้าถึง (Access Control) และการควบคุมการพิสูจน์ตัวตนจาก User Profile Access Level Matrix เพื่อให้ระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศของลูกค้าและของบริษัท ได้รับการปกป้องและมีการป้องกัน เพื่อให้เกิดความปลอดภัยและมีความถูกต้องแม่นยำเป็นที่เชื่อถือได้ และเพื่อให้การใช้ระบบเครือข่ายสื่อสารของบริษัทเป็นไปอย่างมีประสิทธิภาพ รวมทั้งจะต้องเก็บประวัติการเขาถึงข้อมูลสารสนเทศ (Access Log) ทั้งหมดที่เกิดขึ้น เพื่อป้องกันการปฏิเสธการรับผิดชอบต่อความเสียหายที่อาจเกิดขึ้นจากการเข้าถึงระบบสารสนเทศ

การมีข้อกำหนดการใช้งานตามข้อกำหนดทางธุรกิจ เพื่อควบคุมการเข้าถึงสารสนเทศ (Business requirements for access control) การเข้าถึงหรือการควบคุมการใช้งานสารสนเทศ จะพิจารณาจากความต้องการทางธุรกิจ และทางด้านความมั่นคงปลอดภัยในการเข้าถึงสินทรัพย์สารสนเทศของบริษัทเป็นสำคัญ และให้ปฏิบัติตามระเบียบปฏิบัติงาน เรื่อง การรักษาความปลอดภัยระบบสารสนเทศ

4.6 การเข้ารหัสข้อมูล (Cryptography)

4.6.1 บริษัทกำหนดให้มีการเข้ารหัสข้อมูลที่มีความสำคัญกับบริษัทและลูกค้า เพื่อรักษาความมั่นคงปลอดภัยของข้อมูลที่มีความสำคัญ ทั้งในด้านการรักษาความลับของข้อมูล (Data Confidentiality) ความถูกต้องของข้อมูล (Data Integrity) และการป้องกันการปฏิเสธความรับผิดชอบ (Non-Repudiation) รวมไปถึงการป้องกันการรั่วไหลของข้อมูลออกสู่ภายนอกบริษัท (Information Leakage) โดยมาตรการในการเข้ารหัสข้อมูลนั้นจะต้อง

(1) กำหนดอัลกอริทึม และความยาวของกุญแจที่เข้ารหัส ให้มีความเหมาะสมกับระดับชั้นความลับข้อมูลของบริษัท

(2) เป็นอัลกอริทึมที่ใช้ในการเข้ารหัส จะต้องเป็นอัลกอริทึมที่เป็นมาตรฐานสากล หลีกเลี่ยงการสร้างอัลกอริทึมในการเข้ารหัสโดยผู้พัฒนาระบบ

(3) ทบทวนอัลกอริทึมที่ใช้ในการเข้ารหัส และความยาวของกุญแจที่เข้ารหัส เพื่อให้ยังคงรักษาความมั่นคงปลอดภัยให้กับข้อมูลของบริษัท

4.6.2 จะต้องมีกระบวนการในการบริหารจัดการกุญแจที่ใช้ในการเข้ารหัส โดยครอบคลุมการสร้างการจัดเก็บ การจัดส่ง และการเปลี่ยนแปลง

4.7 การจัดการด้านการป้องกันและรักษาความปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environmental Security)

บริษัทจัดสถานที่ทำงานหรือสถานที่เก็บทรัพยากรสารสนเทศที่สำคัญให้มีความมั่นคงปลอดภัยตามระดับที่เหมาะสม พร้อมกับจัดวางมาตรฐานการรักษาความปลอดภัยตามระดับความสำคัญ เพื่อปกป้อง

และป้องกันการเข้าถึงโดยไม่เหมาะสม และเป็นการลดความเสี่ยงต่อการสูญหายหรือสูญเสียทรัพยากรสารสนเทศของบริษัท รวมถึงข้อมูลสารสนเทศของบริษัทและลูกค้า

4.7.1 บริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย (Secure Areas)

กำหนดพื้นที่ (Zoning) และระดับของความปลอดภัย สำหรับศูนย์ข้อมูลและพื้นที่การทำงานที่เกี่ยวข้องกับระบบข้อมูลสารสนเทศให้เป็นพื้นที่ควบคุม พร้อมทั้งใช้ระบบ Access Control เพื่อกำหนดสิทธิในการเข้าศูนย์ข้อมูล รวมทั้งเก็บรหัสผ่านการบริหารระบบระดับสูงสุดไว้ในตู้นิรภัยของบริษัท

4.7.2 ความมั่นคงปลอดภัยของอุปกรณ์ (Equipment Security)

ทำประกันภัยอุปกรณ์คอมพิวเตอร์ (Insurance Service) และการดูแลรักษาอุปกรณ์คอมพิวเตอร์ให้มีความพร้อมในการใช้งานอยู่เสมอ โดยหน่วยงานที่มีหน้าที่ในการดูแลระบบจะต้องส่งเจ้าหน้าที่เข้าไปตรวจสอบศูนย์ข้อมูลและระบบเซิร์ฟเวอร์หลักอย่างสม่ำเสมอ และรายงานผลต่อพนักงานระดับบริหารอย่างต่อเนื่องเป็นระยะ

4.8 การปฏิบัติงานระบบสารสนเทศ (Operations Management)

ข้อมูลสารสนเทศของบริษัทต้องได้รับการปกป้องอย่างเหมาะสมและมีประสิทธิภาพในการใช้งาน พร้อมทั้งมีการสำรองข้อมูลสารสนเทศ ซึ่งนำไปจัดเก็บในที่มั่นคงปลอดภัย และพร้อมต่อการใช้งานอย่างสม่ำเสมอตามระดับความเสี่ยงและความสำคัญ

4.8.1 กำหนดหน้าที่ ความรับผิดชอบ และวิธีการปฏิบัติงานเกี่ยวกับการป้องกันและการใช้งานระบบสารสนเทศ ซึ่งรวมถึงทรัพยากรสารสนเทศ ข้อมูลสารสนเทศที่เหมาะสม เพื่อให้ระบบสารสนเทศของบริษัทมีความมั่นคงปลอดภัย

4.8.2 การกำหนดมาตรการในการสำรองข้อมูล และการทดสอบข้อมูลระบบงานต่าง ๆ ของบริษัท และจะต้องมีการจัดเก็บในที่ที่มีความมั่นคงปลอดภัยมีความสัมพันธ์กับกลยุทธ์ในการบริหารความต่อเนื่องทางธุรกิจของบริษัท

4.8.3 การตรวจสอบและเฝ้าสังเกตการณ์ระบบคอมพิวเตอร์ (Monitoring System Access) บริษัทมีจุดประสงค์เพื่อตรวจสอบและเฝ้าสังเกตการณ์ระบบคอมพิวเตอร์ กิจกรรมในระบบคอมพิวเตอร์ที่ไม่ได้รับอนุญาต รวมถึงป้องกันโปรแกรมไม่ประสงค์ดี

4.9 การจัดการและบริหารด้านเครือข่ายสื่อสาร (Communications Management)

4.9.1 กำหนดหน้าที่ ความรับผิดชอบ และวิธีการปฏิบัติงานเกี่ยวกับระบบเครือข่ายสื่อสารที่เหมาะสม เพื่อให้ระบบเครือข่ายสื่อสารของบริษัทมีความมั่นคงปลอดภัย

4.9.2 กำหนดจำกัดสิทธิของผู้ใช้งานและช่องทางการเข้าถึงระบบเครือข่ายของผู้ใช้งานโดยกำหนดสิทธิให้เท่าที่จำเป็น

4.9.3 กำหนดมาตรการในการสำรองข้อมูลและการทดสอบข้อมูลที่เกี่ยวข้องกับการตั้งค่าระบบเครือข่ายสื่อสาร และจะต้องมีการจัดเก็บในที่ที่มีความมั่นคงปลอดภัย มีความพร้อมในการนำมาใช้งานเมื่อต้องการ

4.9.4 กำหนดมาตรการในการแลกเปลี่ยนข้อมูลระหว่างบริษัทกับหน่วยงานภายนอก เช่น กระทรวงการคลัง ธนาคารแห่งประเทศไทย สถาบันการเงิน และผู้ให้บริการภายนอก เป็นต้น

4.10 การจัดการด้านการพัฒนาระบบสารสนเทศและการบำรุงรักษา (System Development and Maintenance)

บริษัทกำหนดมาตรการ วิธีการจัดหาหรือพัฒนาระบบสารสนเทศอย่างเป็นขั้นตอน ถูกต้องตามกฎหมายลิขสิทธิ์ กำหนดมาตรการการใช้งาน การบำรุงรักษา เพื่อให้ระบบสารสนเทศซึ่งรวมถึงข้อมูลสารสนเทศมีความมั่นคงปลอดภัย

สามารถนำไปใช้บรรลุวัตถุประสงค์ตามที่ต้องการและอย่างต่อเนื่อง รวมไปถึงจัดให้มีกระบวนการในการรักษาความถูกต้องเชื่อถือได้ของระบบให้บริการ การประมวลผล และการจัดเก็บ รวมทั้งการดำเนินการใด ๆ ที่จะทำให้ระบบให้บริการทำงานได้อย่างถูกต้องมีประสิทธิภาพ โดยจัดทำข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ ดังนี้

4.10.1 การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (Security requirements of information systems) เพื่อกำหนดให้กระบวนการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเป็นส่วนหนึ่งของระบบสารสนเทศของทั้งภายในองค์กร และที่เกี่ยวข้องกับการให้บริการภายนอกผ่านเครือข่ายสาธารณะตลอดช่วงอายุการใช้งานระบบสารสนเทศ (Entire Life Cycle) ได้แก่ กระบวนการจัดหา กระบวนการพัฒนาระบบ (System Development Life Cycle) การใช้งานและการดูแลรักษา

4.10.2 การรักษาความมั่นคงปลอดภัยในกระบวนการพัฒนาระบบสารสนเทศ (Security in development and support process) เพื่อจัดให้มีการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตลอดช่วงการพัฒนาระบบสารสนเทศ (System Development Life Cycle)

4.10.3 การควบคุมข้อมูลที่ใช้ในการทดสอบ (Test Data) เพื่อจัดให้มีการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ในการปกป้องข้อมูลสำคัญที่นำมาใช้ในทดสอบ

4.11 การบริหารจัดการผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ (Supplier Relationship)

บริษัทกำหนดกลยุทธ์และมาตรการ เมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัย เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยของระบบสารสนเทศได้รับการแก้ไขอย่างถูกต้องมีประสิทธิภาพ ในระยะเวลาที่เหมาะสม ให้พิจารณาดังนี้

4.11.1 บริษัทต้องจัดให้มีขั้นตอนและกระบวนการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ รวมทั้งกำหนดหน่วยงานที่รับผิดชอบโดยตรง

4.11.2 บริษัทต้องจัดให้มีการรายงานสถานการณ์ที่เกิดขึ้นอย่างรวดเร็วและทันต่อเหตุการณ์ผ่านบุคคลหรือหน่วยงานที่ทำหน้าที่รับแจ้งเหตุการณ์ (Point of Contact)

4.11.3 ให้มีการรายงานเหตุการณ์และจุดอ่อนด้านความมั่นคงปลอดภัย (Reporting Information Security Events and Weaknesses) รวมทั้งแจ้งข้อมูลในส่วนที่เป็นจุดอ่อนในระบบสารสนเทศ พร้อมเสนอแนวทางแก้ไข และแนวทางการป้องกันให้คณะกรรมการระบบบริหารความมั่นคงปลอดภัยสารสนเทศ หรือคณะบุคคลที่ได้รับมอบหมายเพื่อพิจารณา

4.11.4 ศึกษาเหตุการณ์ด้านความมั่นคงปลอดภัยที่เกิดขึ้นเพื่อหาแนวทางการแก้ไขและป้องกัน โดยต้องวิเคราะห์หาสาเหตุของเหตุการณ์ด้านความมั่นคงปลอดภัย เพื่อหาวิธีการป้องกันไม่ให้เกิดขึ้นอีก

4.12 การบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศเพื่อสร้างความต่อเนื่องทางธุรกิจ (Information Security Aspects of Business Continuity Management)

บริษัทกำหนดกลยุทธ์และมาตรการการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อสร้างความต่อเนื่องทางธุรกิจ และเพื่อให้การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศเป็นส่วนหนึ่งของการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management) ของบริษัท ทั้งนี้ เพื่อให้ระบบสารสนเทศอยู่ในสภาพที่พร้อมใช้งานอยู่เสมอ โดยให้ดำเนินการดังนี้

4.12.1 ฝ่ายงานของบริษัทต้องมีการประเมินผลกระทบทางธุรกิจที่อาจส่งผลกระทบต่อการดำเนินงาน ผลิตภัณฑ์ หรือธุรกรรมของบริษัท พร้อมทั้งกำหนดวิธีการปฏิบัติงานการดำเนินงาน ในกรณีเกิดภัยพิบัติในระดับต่าง ๆ รวมถึงเหตุการณ์ผิดปกติทางไซเบอร์ (Cybersecurity Incident) เพื่อให้ผู้เกี่ยวข้อง เช่น ลูกหนี้ หรือคู่ค้า เป็นต้น เชื่อมั่นว่าการดำเนินงานทางธุรกิจและระบบสารสนเทศจะยังสามารถใช้บริการได้อย่างต่อเนื่อง

4.12.2 ฝ่ายงานของบริษัทจะต้องจัดทำแผนบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) ที่สามารถตอบสนองต่อเหตุการณ์ที่อาจส่งผลกระทบต่อการดำเนินทางธุรกิจหรือธุรกรรมของทางบริษัท และสามารถตอบสนองได้ตามเป้าหมายในการกู้คืน โดยจะต้องทบทวนและปรับปรุง อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

4.12.3 หน่วยงานด้านเทคโนโลยีสารสนเทศและหน่วยงานที่เกี่ยวข้องจะต้องจัดทำแผนกู้คืนระบบสารสนเทศ (Disaster Recovery Plan : DRP) เพื่อตอบสนองต่อภัยพิบัติและคุกคามที่มีผลกระทบต่อการหยุดชะงัก และให้มีการทบทวนและปรับปรุงแก้ไขอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

4.12.4 ให้มีการทดสอบแผนบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) และแผนกู้คืนระบบสารสนเทศ (Disaster Recovery Plan : DRP) อย่างน้อยปีละ 1 ครั้ง ของการให้บริการในระบบสารสนเทศ เพื่อรักษาความพร้อมใช้ของระบบ (System Availability) ซึ่งระบบสารสนเทศจะสามารถทำงานได้อย่างต่อเนื่อง และทดสอบการรับมือต่อเหตุการณ์ผิดปกติทางไซเบอร์ (Cybersecurity Incident) พร้อมทั้งรายงานผลการทดสอบต่อพนักงานระดับบริหารเพื่อนำเสนอต่อคณะอนุกรรมการบริหารจัดการและกำกับดูแลการปฏิบัติงานด้านเทคโนโลยีสารสนเทศต่อไป

4.13 การจัดการด้านการปฏิบัติตามกฎหมาย กฎระเบียบ และข้อกำหนด (Compliance)

บริษัทกำหนดให้มีระเบียบ คำสั่ง ข้อกำหนด ประกาศ หรือจัดทำเป็นสัญญา ที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศหรือการปฏิบัติตามกฎหมาย เพื่อให้เป็นไปตามกฎหมายลิขสิทธิ์หรือทรัพย์สินทางปัญญา รวมทั้งมาตรการหรือคำสั่งเพื่อป้องกันการละเมิดลิขสิทธิ์และป้องกันข้อมูลสารสนเทศของบริษัทและข้อมูลลูกค้า พร้อมทั้งกำหนดมาตรการและวิธีการทบทวน การตรวจสอบ การสอบทาน การประเมินผลและการรายงานให้เป็นไปอย่างโปร่งใสตามหลักธรรมาภิบาล รวมถึงการทบทวนนโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศเป็นระยะ เพื่อให้ปัจจุบันและสอดคล้องกับมาตาฐานสากล

4.13.1 บรรดากฎหมาย และ/หรือข้อบังคับใด ๆ ที่เกี่ยวกับระบบสารสนเทศ ที่ได้ประกาศใช้ในประเทศ ถือเป็นสิ่งสำคัญที่ผู้ใช้งานจะต้องตระหนัก และปฏิบัติตามอย่างเคร่งครัดและการไม่กระทำความผิดฝ่าฝืนบทบัญญัตินั้น ทั้งนี้ หากใช้งานกระทำความผิดนั้นเป็นการกระทำความผิดส่วนบุคคล ซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดนั้น

4.13.2 บริษัทต้องระบุบกฎหมาย หลักเกณฑ์ของทางการ และข้อกำหนดตามสัญญาต่าง ๆ ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ โดยจัดทำเป็นเอกสารและปรับปรุงให้เป็นปัจจุบันอย่างสม่ำเสมอ

4.13.3 หน่วยงานที่มีหน้าที่ดูแลงานด้านตรวจสอบภายใน มีหน้าที่ความรับผิดชอบ ดังนี้

(1) ตรวจสอบว่าบริษัทมีการปฏิบัติงานที่สอดคล้องตามกฎหมาย และกฎระเบียบที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศ และตรวจสอบความมั่นคงปลอดภัยด้านสารสนเทศตามรอบที่กำหนด

(2) ตรวจประเมินระบบมาตรฐานความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อตรวจสอบว่าปฏิบัติได้สอดคล้องกับมาตรฐานความมั่นคงปลอดภัย และผลการประเมินอยู่ในระดับที่สามารถยอมรับได้หรือไม่

4.13.4 ให้ผู้บริหารมีหน้าที่กำกับดูแลตรวจสอบการปฏิบัติงานตามนโยบาย ระเบียบ และคู่มือปฏิบัติงาน อย่างสม่ำเสมอ

4.13.5 ให้บริษัทมีการตรวจสอบประเมินความมั่นคงปลอดภัยทางด้านเทคนิคของระบบสารสนเทศอย่างสม่ำเสมอ

ประกาศ ณ วันที่ 12 มิถุนายน พ.ศ. 2566

(นางญาใจ พัฒนสุขวสันต์)
ประธานกรรมการ
บริษัท บริหารสินทรัพย์ ธนาคารอิสลามแห่งประเทศไทย จำกัด