บริษัท บริหารสินทรัพย์ ธนาคารอิสลามแห่งประเทศไทย จำกัด

นโยบายการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ
(Information Technology Risk Control Policy)
บริษัท บริหารสินทรัพย์ ธนาคารอิสลามแห่งประเทศไทย จำกัด

---

1. หลักการและเหตุผล

การนำเทคโนโลยีสารสนเทศมาใช้ในการดำเนินธุรกิจของบริษัท บริหารสินทรัพย์ ธนาคารอิสลามแห่งประเทศไทย จำกัด (บริษัท) เพื่อเพิ่มประสิทธิภาพและช่วยให้บริษัทสามารถตอบสนองต่อความต้องการของลูกค้าได้ดีขึ้น แต่หากขาดการบริหารความเสี่ยงที่ดีในการใช้เทคโนโลยีสารสนเทศดังกล่าวอาจก่อให้เกิดความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk) และภัยคุกคามทางไซเบอร์ (Cyber Threat) ที่ส่งผลกระทบต่อบริษัทในด้านความเสียหายที่เป็นจำนวนเงินและส่งผลต่อความเชื่อมั่นของลูกค้าที่มีต่อการใช้บริการทางการเงินได้ ดังนั้น เพื่อให้บริษัทมีธรรมาภิบาลด้านเทคโนโลยีสารสนเทศที่ดี มีการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และมีการบริหารความเสี่ยงดังกล่าว บริษัทจึงได้กำหนดนโยบายการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อใช้เป็นแนวปฏิบัติในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ทั้งนี้ หลักการและเหตุผลในการออกนโยบายการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศให้เป็นไปตามประกาศธนาคารแห่งประเทศไทย เรื่อง หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk)

2. วัตถุประสงค์

วัตถุประสงค์ของนโยบายและแนวทางการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk Control Policy) มีดังต่อไปนี้

2.1 เพื่อให้บริษัทมีธรรมาภิบาลด้านเทคโนโลยีที่ดี มีการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และตระหนักถึงการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศอยู่เสมอ

2.2 เพื่อให้การปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ การตรวจสอบด้านเทคโนโลยีสารสนเทศ และการบริหารจัดการโครงการด้านเทคโนโลยีสารสนเทศอย่างมีประสิทธิภาพและรัดกุม โดยอยู่ภายใต้กรอบหลักการที่สำคัญ คือ การรักษาความลับของระบบและข้อมูล (Confidentiality) ความถูกต้องเชื่อถือได้ของระบบและข้อมูล (Integrity) และความพร้อมใช้งานของเทคโนโลยีสารสนเทศ (Availability) และอยู่บนพื้นฐานของการคุ้มครองข้อมูลและรักษาผลประโยชน์ของลูกค้า

2.3 เพื่อให้มีการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศให้สอดคล้องกับลักษณะการดำเนินธุรกิจ ปริมาณธุรกรรม ความซับซ้อนของเทคโนโลยีสารสนเทศ และความเสี่ยงที่เกี่ยวข้อง

3. คำนิยาม

"บริษัท" หมายความว่า บริษัท บริหารสินทรัพย์ ธนาคารอิสลามแห่งประเทศไทย จำกัด

"คณะกรรมการบริษัท" หมายความว่า คณะกรรมการบริษัท บริหารสินทรัพย์ ธนาคารอิสลามแห่งประเทศไทย จำกัด

"ผู้จัดการบริษัท" หมายความว่า ผู้จัดการบริษัท บริหารสินทรัพย์ ธนาคารอิสลามแห่งประเทศไทย จำกัด และในกรณีที่ผู้จัดการบริษัทเป็นกรรมการบริษัทด้วย ให้เรียกว่า "กรรมการผู้จัดการบริษัท"

"พนักงานระดับบริหาร" หมายความว่า พนักงานที่ดำรงตำแหน่งรองผู้จัดการบริษัท ผู้ช่วยผู้จัดการบริษัท และผู้จัดการฝ่าย ตามลำดับชั้น

"พนักงาน" หมายความว่า ผู้ซึ่งบริษัทได้จ้างไว้ให้ปฏิบัติงานในลักษณะประจำ และรับเงินเดือนตามระดับตำแหน่งที่กำหนด ทั้งนี้ ไม่รวมถึงผู้จัดการบริษัท

"ความเสี่ยงด้านเทคโนโลยีสารสนเทศ" หมายความว่า ความเสี่ยงที่อาจเกิดขึ้นจากการใช้เทคโนโลยีสารสนเทศในการดำเนินธุรกิจซึ่งจะมีผลกระทบต่อระบบหรือการปฏิบัติงานของบริษัท รวมถึงความเสี่ยงที่เกิดจากภัยคุกคามทางไซเบอร์ (Cyber Threat)

"หน่วยงาน" หมายความว่า ฝ่ายงาน สำนัก ส่วนงาน หรือหน่วยงานเรียกชื่ออื่นใด ตามประกาศโครงสร้างองค์กรของบริษัท

"เทคโนโลยีสารสนเทศ" หมายความว่า เทคโนโลยีสารสนเทศที่นำมาใช้ในการดำเนินธุรกิจ ซึ่งครอบคลุมถึงข้อมูล ระบบปฏิบัติการ ระบบงาน ระบบฐานข้อมูล อุปกรณ์คอมพิวเตอร์ และระบบเครือข่ายสื่อสาร เป็นต้น

4. หลักการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

หลักการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ มีรายละเอียดโดยสรุปดังนี้

4.1 การใช้เทคโนโลยีสารสนเทศสอดคล้องกับกลยุทธ์ในการดำเนินธุรกิจและการเปลี่ยนแปลง

บริษัทมีการเตรียมความพร้อมของระบบเทคโนโลยีสารสนเทศเพื่อพร้อมรับการเปลี่ยนแปลงที่เป็นไปอย่างรวดเร็ว รวมถึงเพื่อรองรับการดำเนินธุรกิจในอนาคต

4.2 คณะกรรมการบริษัท คณะอนุกรรมการที่ได้รับมอบหมาย และพนักงานระดับบริหารของบริษัทมีบทบาทสำคัญในการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ

บริษัทกำหนดให้การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ เป็นการกำกับดูแลในระดับองค์กร โดยเป็นความรับผิดชอบของคณะกรรมการบริษัท คณะอนุกรรมการที่เกี่ยวข้อง ที่สนับสนุนและกำหนดกลยุทธ์ และนโยบายด้านเทคโนโลยีสารสนเทศ และผลักดันให้มีการสร้างความตระหนักในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างต่อเนื่องและมีประสิทธิภาพ

4.3 ความเสี่ยงด้านเทคโนโลยีสารสนเทศเป็นความเสี่ยงในระดับองค์กร (Enterprise Wide Risk)

บริษัทกำหนดให้การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศเป็นเรื่องที่พนักงานทุกระดับและทุกฝ่ายในบริษัทต้องให้ความตระหนักและมีแนวทางบริหารความเสี่ยงที่เกิดขึ้นจากการใช้เทคโนโลยีสารสนเทศ ครอบคลุมทั้งในเชิงกลยุทธ์และเชิงปฏิบัติการ เพื่อให้มีการป้องกัน ติดตาม และรับมือความเสี่ยงที่อาจเกิดขึ้น

4.4 มีการกำกับดูแลเป็นไปตามหลัก 3 Lines of Defence

บริษัทมีการกำหนดโครงสร้างการกำกับดูแลการปฏิบัติงานและการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศที่สอดคล้องตามหลัก 3 Lines of Defence เพื่อให้สอดคล้องตามหลักการถ่วงดุล (Check And Balance)

4.5 การรักษาความมั่นคงปลอดภัยและการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศสอดคล้องกับความเสี่ยงที่เพิ่มขึ้น

บริษัทกำหนดให้มีการบริหารจัดการและควบคุมความเสี่ยงที่เกิดจากเทคโนโลยีสารสนเทศเพื่อป้องกันการเกิดช่องโหว่ด้านการรักษาความปลอดภัย ความถูกต้องเชื่อถือได้ และความพร้อมใช้ของระบบในการดำเนินงานของบริษัท เพื่อป้องกันความเสี่ยงด้านความน่าเชื่อถือ ชื่อเสียง ภาพลักษณ์ การปฏิบัติตามกฎหมาย และหลักเกณฑ์ที่เกี่ยวข้อง

4.6 การบริหารจัดการโครงการด้านเทคโนโลยีสารสนเทศอย่างรัดกุมและมีประสิทธิภาพ

บริษัทกำหนดให้มีการบริหารจัดการทรัพยากรที่มีอยู่อย่างจำกัดให้มีประสิทธิภาพสูงสุด

4.7 มีการพัฒนาความรู้ความสามารถของคณะกรรมการบริษัท คณะอนุกรรมการที่ได้รับมอบหมาย พนักงานระดับบริหาร และพนักงานทุกระดับ

บริษัทกำหนดให้คณะกรรมการบริษัท คณะอนุกรรมการที่เกี่ยวข้อง พนักงานระดับบริหาร และพนักงานทุกระดับ ได้รับการพัฒนาความรู้ด้านเทคโนโลยีสารสนเทศ และความเสี่ยงต่อธุรกิจ รวมถึงติดตามภัยคุกคามทางไซเบอร์ เพื่อให้มีความรู้เท่าทันภัยคุกคามใหม่ที่เกิดขึ้น

5. หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ

5.1 ธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ (IT Governance)

5.1.1 บทบาทและหน้าที่ความรับผิดชอบ

คณะกรรมการบริษัท มีบทบาทและหน้าที่ความรับผิดชอบ ดังต่อไปนี้

(1) คณะกรรมการบริษัท ประกอบด้วยกรรมการที่มีความรู้หรือประสบการณ์ด้านเทคโนโลยีสารสนเทศอย่างน้อย 1 ท่าน เพื่อให้คณะกรรมการบริษัทสามารถกำหนดทิศทางและกำกับดูแลให้บริษัทมีการใช้เทคโนโลยีสารสนเทศสอดรับกับกลยุทธ์ในการดำเนินธุรกิจ มีความรู้เกี่ยวกับความเสี่ยงและพัฒนาการด้านเทคโนโลยีสารสนเทศที่เปลี่ยนแปลงไป ซึ่งให้การกำกับดูแลการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศเป็นไปอย่างมีประสิทธิภาพ

(2) ดูแลให้มีการใช้เทคโนโลยีที่สอดรับกับกลยุทธ์ในการดำเนินธุรกิจ และดูแลให้การใช้เทคโนโลยีสารสนเทศให้มีความยืดหยุ่นเพียงพอที่จะรองรับการเปลี่ยนแปลงด้านเทคโนโลยีสารสนเทศและการเปลี่ยนแปลงการดำเนินธุรกิจในอนาคต

(3) ดูแลให้มีการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศซึ่งเป็นความเสี่ยงที่สำคัญโดยถือเป็นส่วนหนึ่งของการบริหารความเสี่ยงในภาพรวมของบริษัท (Enterprise Risk Management : ERM)

(4) ดูแลให้มีการกำหนดนโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security Policy) ซึ่งรวมถึงนโยบายในการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ และนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management Policy) ให้สอดคล้องกับลักษณะการดำเนินธุรกิจ ปริมาณธุรกรรม ความซับซ้อนของเทคโนโลยีสารสนเทศ และความเสี่ยงที่เกี่ยวข้อง รวมทั้งอนุมัติใช้นโยบายดังกล่าว

(5) ดูแลให้มีมาตรฐาน ระเบียบวิธีปฏิบัติ กระบวนการ เครื่องมือ และพนักงานในการรักษาความมั่นคงปลอดภัยและการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ เป็นไปตามนโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ ซึ่งรวมถึงนโยบายในการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ และนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ รวมถึงดูแลให้มีการนำไปปฏิบัติอย่างเหมาะสม และมีการทบทวนและประเมินประสิทธิภาพของนโยบายดังกล่าว อย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

(6) ดูแลให้มีการติดตาม ตรวจสอบ และรายงานต่อคณะกรรมการของบริษัท คณะอนุกรรมการที่ได้รับมอบหมาย หรือพนักงานระดับบริหารอย่างเหมาะสม ในเรื่องที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ผลการทดสอบและการปฏิบัติตามแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ และการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

(7) ดูแลและสนับสนุนให้มีการสื่อสารกับพนักงานของบริษัท เพื่อให้ตระหนักถึงความสำคัญของความเสี่ยงด้านเทคโนโลยีสารสนเทศ และให้เข้าใจถึงการใช้เทคโนโลยีสารสนเทศที่ถูกต้องเพื่อช่วยลดความเสี่ยงด้านเทคโนโลยีสารสนเทศ

5.1.2 โครงสร้างการกำกับดูแล

(1) คณะอนุกรรมการที่ทำหน้าที่กำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ

บริษัทกำหนดให้มีคณะอนุกรรมการที่ทำหน้าที่กำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ ดังต่อไปนี้

(1.1) คณะอนุกรรมการบริหารจัดการและกำกับดูแลการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ

ทำหน้าที่กำกับดูแลให้มีการกำหนดกลยุทธ์ นโยบาย และแผนงานด้านเทคโนโลยีสารสนเทศที่สอดคล้องกับกลยุทธ์ของบริษัท รวมทั้งกำกับดูแลและติดตามการดำเนินงาน และการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

(1.2) คณะอนุกรรมการกำกับความเสี่ยง

ทำหน้าที่กำกับดูแลให้มีการกำหนดนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ รวมทั้งกำกับดูแลและติดตามให้เป็นไปตามนโยบายที่กำหนดไว้ โดยมีการเชื่อมโยงกับความเสี่ยงในภาพรวมของบริษัท

(1.3) คณะกรรมการตรวจสอบ

ทำหน้าที่กำกับดูแลให้มีการตรวจสอบด้านเทคโนโลยีสารสนเทศ ซึ่งการตรวจสอบครอบคลุมถึงการปฏิบัติงานด้านเทคโนโลยีสารสนเทศและการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ รวมทั้งกำกับดูแลให้มีการสอบทานการปฏิบัติตามกฎหมาย ข้อบังคับ มาตรฐาน และหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ

(2) โครงสร้างองค์กร

บริษัทกำหนดโครงสร้างองค์กรที่เอื้อต่อการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เหมาะสม และสอดคล้องตามหลักการแบ่งแยกหน้าที่ความรับผิดชอบ 3 ระดับ โดยมีการแบ่งแยกหน้าที่ความรับผิดชอบอย่างชัดเจนระหว่างการทำหน้าที่ คือ

(2.1) ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ ได้แก่ หน่วยงานด้านเทคโนโลยีสารสนเทศ และหน่วยงานอื่นที่เป็นผู้ใช้งานระบบ

(2.2) การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ได้แก่ หน่วยงานด้านบริหารความเสี่ยงและกำกับดูแลการปฏิบัติงาน

(2.3) ตรวจสอบด้านเทคโนโลยี ได้แก่ หน่วยงานตรวจสอบภายใน

นอกจากนี้ จัดให้มีการถ่วงดุลอำนาจกันอย่างอิสระ โดยเฉพาะการทำหน้าที่ตรวจสอบด้านเทคโนโลยีสารสนเทศ และการทำหน้าที่บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

(3) การบริหารจัดการบุคลากร

บริษัทกำหนดให้มีการบริหารจัดการพนักงานที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ การกำกับการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ และตรวจสอบด้านเทคโนโลยีสารสนเทศ รวมถึงบุคลากรที่ใช้เทคโนโลยีสารสนเทศในการปฏิบัติงานประจำวันอย่างเหมาะสม โดยคำนึงถึงความรู้ความสามารถของพนักงาน ปริมาณงาน และการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ โดยบริษัทกำหนดบทบาทหน้าที่ความรับผิดชอบของหน่วยงานที่เกี่ยวข้องกับการบริหารจัดการพนักงาน ดังต่อไปนี้

(3.1) การบริหารจัดการพนักงานที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ กำกับการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ และตรวจสอบด้านเทคโนโลยีสารสนเทศ ที่ครอบคลุมในเรื่องดังต่อไปนี้

(3.1.1) กระบวนการคัดเลือกพนักงาน เพื่อให้ได้พนักงานที่มีคุณสมบัติเหมาะสม มีความรู้หรือประสบการณ์เพียงพอในการปฏิบัติหน้าที่ตามที่ได้รับมอบหมาย โดยอาจพิจารณาการได้รับการรับรองความรู้ความสามารถตามมาตรฐานที่รับรองทั่วไป (Certificate) เฉพาะด้านที่เกี่ยวข้องกับงานด้านเทคโนโลยีสารสนเทศที่ได้รับมอบหมายนั้น

(3.1.2) ความเพียงพอของพนักงาน เพื่อให้มีปริมาณพนักงานเพียงพอกับปริมาณการใช้เทคโนโลยีสารสนเทศ

(3.1.3) มาตรการในการสร้างและส่งเสริมความตระหนักถึงความสำคัญของความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อให้พนักงานมีการตระหนักถึงบทบาทหน้าที่และความรับผิดชอบของตน และมาตรการดูแลให้พนักงานปฏิบัติตามหน้าที่และรับผิดชอบตามที่กำหนดไว้

(3.2) การอบรมความรู้ให้แก่คณะกรรมการบริษัท คณะอนุกรรมการที่เกี่ยวข้อง พนักงานระดับบริหาร และพนักงาน ที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ บริหารความเสี่ยงด้าน

เทคโนโลยีสารสนเทศ กำกับการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ และตรวจสอบด้านเทคโนโลยีสารสนเทศอย่างเพียงพอตามระยะเวลาที่เหมาะสม โดยครอบคลุมเนื้อหาต่าง ๆ ที่เกี่ยวข้อง เพื่อให้คณะกรรมการบริษัท คณะอนุกรรมการที่เกี่ยวข้อง พนักงานระดับบริหาร และพนักงาน มีความรู้และทักษะที่เพียงพอต่อการกำกับดูแลหรือปฏิบัติงานในส่วนที่เกี่ยวข้อง

(3.3) มีการระบุเรื่องความรับผิดชอบเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัทอย่างชัดเจนลงในข้อกำหนดหรือเงื่อนไขในสัญญาจ้างงานของพนักงาน เพื่อป้องกันการรั่วไหลของข้อมูลหรือความเสียหายที่อาจเกิดขึ้นต่อทรัพย์สินด้านเทคโนโลยีสารสนเทศของบริษัท

(3.4) การบริหารจัดการสิทธิของพนักงานที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ โดยการแจ้งข้อมูลกรณีมีการเปลี่ยนแปลงตำแหน่งงาน หรือสิ้นสุดการจ้างงานให้แก่หน่วยงานที่เกี่ยวข้องทราบ เพื่อทำการทบทวนสิทธิให้เป็นปัจจุบัน เช่น ทบทวนสิทธิในการเข้าถึงข้อมูล รวมทั้งสื่อสารให้ผู้ที่เกี่ยวข้องรับทราบถึงการเปลี่ยนแปลงสิทธิ หน้าที่ และความรับผิดชอบดังกล่าว เป็นต้น

(4) การส่งเสริมให้พนักงานตระหนักถึงความเสี่ยงด้านเทคโนโลยีสารสนเทศ

บริษัทกำหนดให้หน่วยงานที่เกี่ยวข้องกับการบริหารจัดการพนักงานร่วมกับหน่วยงานที่เกี่ยวข้อง ได้แก่ หน่วยงานด้านเทคโนโลยีสารสนเทศ หน่วยงานด้านบริหารความเสี่ยงและกำกับดูแลการปฏิบัติงาน และหน่วยงานที่เกี่ยวข้องกับการบริหารจัดการพนักงาน กำหนดโปรแกรมการอบรมและพัฒนาความรู้ความเชี่ยวชาญด้านเทคโนโลยีสารสนเทศที่ครอบคลุมการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ การกำกับการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ หรือหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศให้แก่พนักงานทุกระดับ พร้อมการวัดประสิทธิผล นอกจากนี้ มีการกำหนดโปรแกรมในการเสริมสร้างความตระหนักเรื่องการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ความเสี่ยงด้านเทคโนโลยีสารสนเทศ การใช้งานระบบอย่างปลอดภัยให้แก่คณะกรรมการบริษัท คณะอนุกรรมการที่เกี่ยวข้อง พนักงานระดับบริหาร และพนักงานทุกระดับ รวมถึงบุคคลภายนอกที่เกี่ยวข้อง รวมทั้งมีการจัดกิจกรรมเสริมสร้างความตระหนักอย่างต่อเนื่อง

(5) นโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้านเทคโนโลยี

บริษัทกำหนดให้มีนโยบายเป็นลายลักษณ์อักษรและอยู่ภายใต้กรอบหลักการที่สำคัญ 3 ประการ คือ การรักษาความลับของระบบและข้อมูล ความถูกต้องเชื่อถือได้ของระบบและข้อมูล และความพร้อมใช้งานของเทคโนโลยีสารสนเทศ โดยครอบคลุมนโยบายดังต่อไปนี้

(5.1) นโยบายการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ

(5.2) นโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศ

(5.3) นโยบายการใช้บริการจากผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศ

โดยนโยบายดังกล่าวมีความสอดคล้องกับกลยุทธ์ของบริษัท ในการนำเทคโนโลยีสารสนเทศมาใช้ในการดำเนินธุรกิจ และสอดคล้องกับแนวทางการบริหารความเสี่ยงและการรักษาความมั่นคงปลอดภัยตามมาตรฐานสากลและมาตรฐานที่ได้รับการยอมรับโดยทั่วไป

ทั้งนี้ บริษัทกำหนดให้มีการทบทวนนโยบายการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ และนโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศ อย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

5.2 การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

บริษัทมีการบริหารจัดการการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ โดยกำหนดบทบาทหน้าที่ความรับผิดชอบของหน่วยงานด้านปฏิบัติการเทคโนโลยีสารสนเทศ ดังต่อไปนี้

5.2.1 การนำนโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศมาจัดทำระเบียบ วิธีปฏิบัติ และกระบวนการในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ โดยครอบคลุมในเรื่องดังต่อไปนี้

(1) การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ

จัดให้มีการบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศที่เหมาะสม โดยมีการจัดทำทะเบียนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศเพื่อให้สามารถระบุรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศได้อย่างครบถ้วน และสามารถนำไปใช้ในการกำหนดแนวทางการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศได้อย่างเหมาะสม รวมถึงมีการบำรุงรักษาทรัพย์สินด้านเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ เพื่อให้มีความพร้อมใช้งานและสามารถรองรับการดำเนินธุรกิจได้อย่างต่อเนื่อง

(2) การรักษาความมั่นคงปลอดภัยของข้อมูล

จัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูล ทั้งในการรับส่งข้อมูลผ่านเครือข่ายสื่อสาร และการจัดเก็บข้อมูลบนระบบงานและสื่อบันทึกข้อมูลต่าง ๆ มีการจัดชั้นความลับของข้อมูล (Information Classification) มีการเก็บรักษาและทำลายข้อมูลให้เหมาะสมกับชั้นความลับ และมีการบริหารจัดการการเข้ารหัสข้อมูล (Cryptography) ที่เชื่อถือได้และเป็นมาตรฐานสากล เพื่อรักษาความมั่นคงปลอดภัยและความลับของข้อมูล

(3) การควบคุมการเข้าถึง

จัดให้มีการควบคุมการเข้าถึงระบบปฏิบัติการ ระบบงาน และระบบฐานข้อมูล โดยกำหนดให้มีการบริหารจัดการสิทธิและตรวจสอบยืนยันตัวตนตามสิทธิที่กำหนดไว้ตามความจำเป็นในการใช้งานและระดับความเสี่ยง เพื่อป้องกันการเข้าถึงและเปลี่ยนแปลงระบบหรือข้อมูลโดยผู้ที่ไม่มีสิทธิหรือผู้ที่ไม่ได้รับอนุญาต

(4) การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม

จัดให้มีการรักษาความมั่นคงปลอดภัยของศูนย์คอมพิวเตอร์ สถานที่ปฏิบัติงานที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ และพื้นที่ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศที่สำคัญ รวมทั้งมีระบบการป้องกันและกระบวนการในการบำรุงรักษาอุปกรณ์คอมพิวเตอร์ และระบบสาธารณูปโภค (Facility) ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศเพื่อป้องกันความเสียหายที่อาจเกิดขึ้นจากการบุกรุกหรือจากภัยธรรมชาติ และให้มีความพร้อมใช้งานสามารถรองรับการดำเนินธุรกิจอย่างต่อเนื่อง

(5) การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร

จัดให้มีการรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสารของบริษัท เพื่อให้ระบบเครือข่ายสื่อสารและข้อมูลที่มีการรับส่งผ่านเครือข่ายสื่อสารมีความมั่นคงปลอดภัย และสามารถป้องกันการบุกรุกหรือภัยคุกคามที่อาจเกิดขึ้น

(6) การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ

จัดให้มีการรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศเพื่อให้การปฏิบัติงานด้านเทคโนโลยีสารสนเทศมีความมั่นคงปลอดภัย โดยต้องครอบคลุมในเรื่องดังต่อไปนี้

(6.1) การบริหารจัดการขีดความสามารถของระบบและระบบสาธารณูปโภค (Capacity Management)

(6.2) การรักษาความมั่นคงปลอดภัยของเครื่องแม่ข่าย (Server) และ อุปกรณ์ที่ใช้ปฏิบัติงานของผู้ใช้เทคโนโลยีสารสนเทศ (Endpoint)

(6.3) การสำรองข้อมูล (Data Backup) ด้วยวิธีการและระยะเวลาที่เหมาะสม

(6.4) การจัดเก็บข้อมูลบันทึกเหตุการณ์ (Logging) ของเครื่องแม่ข่าย ระบบงาน และอุปกรณ์เครือข่ายที่สำคัญ

(6.5) การติดตามดูแลระบบและเฝ้าระวังภัยคุกคาม (Security Monitoring) โดยมีกระบวนการหรือเครื่องมือในการตรวจจับเหตุการณ์ผิดปกติหรือภัยคุกคามที่มีผลกระทบต่อความมั่นคงปลอดภัยของระบบที่สำคัญ

(6.6) การบริหารจัดการช่องโหว่ (Vulnerability Management) ของระบบที่เหมาะสมตามระดับความเสี่ยง เพื่อให้ทราบถึงช่องโหว่และสามารถดำเนินการแก้ไขและป้องกันภัยคุกคามที่อาจเกิดขึ้นได้อย่างทันการณ์ โดยต้องมีการประเมินช่องโหว่ของระบบงานสำคัญทุกระบบอย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

(6.7) การทดสอบเจาะระบบ (Penetration Test) โดยมีผู้เชี่ยวชาญภายในหรือภายนอกที่มีความเป็นอิสระทำหน้าที่ทดสอบเจาะระบบ โดยเฉพาะระบบงาน (Application) และระบบเครือข่าย (Network) ที่มีการเชื่อมต่อกับระบบเครือข่ายสื่อสารสาธารณะ (Internet Facing) สม่ำเสมออย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เพื่อให้ทราบถึงช่องโหว่และสามารถดำเนินการแก้ไขและป้องกันภัยคุกคามที่อาจเกิดขึ้นได้อย่างทันการณ์

(6.8) การบริหารจัดการการเปลี่ยนแปลง (Change Management) โดยมีกระบวนการในการบริหารจัดการการเปลี่ยนแปลงและควบคุมการเปลี่ยนแปลงอย่างรัดกุมและเพียงพอ เช่น การนำระบบขึ้นใช้งานจริง (System Deployment) การตั้งค่าระบบ (System Configuration) การติดตั้ง (Patch) เป็นต้น เพื่อให้การเปลี่ยนแปลงเป็นไปตามวัตถุประสงค์ที่กำหนดไว้อย่างถูกต้อง ครบถ้วน และป้องกันการเปลี่ยนแปลงโดยที่ไม่ได้รับอนุญาต

(6.9) การบริหารจัดการการตั้งค่าระบบ (System Configuration Management) โดยมีกระบวนการในการควบคุมการตั้งค่าของระบบที่ใช้งานจริงและมีการสอบทานการตั้งค่าอย่างสม่ำเสมอ เพื่อป้องกันข้อผิดพลาดในการปฏิบัติงาน

(6.10) การบริหารจัดการการติดตั้ง (Patch Management) โดยมีกระบวนการในการควบคุมการติดตั้ง (Patch) ของระบบที่ใช้งานจริง เพื่อให้สามารถติดตั้ง (Patch) ที่สำคัญในการรักษาความมั่นคงปลอดภัยได้อย่างทันการณ์

(7) การจัดหาและการพัฒนาระบบ

(7.1) การจัดหาระบบ

กำหนดหลักเกณฑ์ที่ชัดเจนและเหมาะสมในการคัดเลือกระบบและผู้ให้บริการ เช่น ความน่าเชื่อถือของระบบและผู้ให้บริการ การได้รับการรับรองตามมาตรฐานสากลหรือมาตรฐานด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้องที่ได้รับการยอมรับโดยทั่วไป (Certificate) ความมั่นคงปลอดภัยของระบบและการสนับสนุนและการบำรุงรักษาระบบ เป็นต้น เพื่อให้มั่นใจว่าระบบและผู้ให้บริการสามารถตอบสนองต่อความต้องการในการดำเนินธุรกิจของบริษัทได้ รวมถึงต้องคำนึงถึงความยืดหยุ่นในการเปลี่ยนแปลงผู้ให้บริการ การเปลี่ยนแปลงเทคโนโลยีสารสนเทศ หรือการเปลี่ยนแปลงกลยุทธ์ในการดำเนินธุรกิจในอนาคต

(7.2) การพัฒนาระบบ

กำหนดให้มีการออกแบบ พัฒนา และทดสอบระบบ เพื่อให้มั่นใจว่าระบบมีความถูกต้อง มั่นคงปลอดภัย เชื่อถือได้ พร้อมใช้งาน และมีความยืนหยุ่น เพียงพอที่จะรองรับการปรับปรุงเปลี่ยนแปลงระบบในอนาคต โดยจัดให้มีในเรื่องดังต่อไปนี้

- เอกสารรายละเอียดคุณสมบัติทางเทคนิค (Technical Specification) โดยครอบคลุมถึงเรื่องการรักษาความมั่นคงปลอดภัย ซึ่งรวมถึงกระบวนการในการทดสอบ การดูแล และการติดตามความมั่นคงปลอดภัยในการใช้งาน

- กระบวนการหรือเครื่องมือในการควบคุมเวอร์ชั่นของคำสั่งในการเขียนโปรแกรม

- การแบ่งแยกบทบาท หน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องในกระบวนการพัฒนาระบบ เช่น การแบ่งแยกระหว่างผู้พัฒนาระบบ และผู้นำระบบขึ้นใช้งานจริง เป็นต้น

- การแบ่งแยกสภาพแวดล้อมของระบบงานที่ใช้สำหรับการพัฒนาและการทดสอบ ออกจากระบบงานที่ให้บริการจริง

- การทดสอบระบบก่อนการใช้งานจริง เช่น ทดสอบการทำงานของแต่ละระบบ ทดสอบการทำงานร่วมกันของระบบต่าง ๆ ทดสอบความพร้อมใช้งานตามกระบวนการและความต้องการของผู้ใช้งาน และทดสอบความปลอดภัยของระบบตามกระบวนการในการรักษาความมั่นคงปลอดภัยที่กำหนดในเอกสารรายละเอียดคุณสมบัติทางเทคนิค เป็นต้น

- การพัฒนาหรือการเปลี่ยนแปลงระบบที่เกี่ยวข้องกับการให้บริการหรือการทำธุรกรรมทางอิเล็กทรอนิกส์ ต้องจัดให้มีการทดสอบประสิทธิภาพ

- แนวทางในการควบคุมการรักษาความมั่นคงปลอดภัยและความลับของข้อมูลสำคัญที่นำไปใช้ในการทดสอบ

- การจัดทำคู่มือและอบรมผู้ใช้งานระบบและผู้ดูแลระบบ

(8) การบริหารจัดการเหตุการณ์ผิดปกติและปัญหา

กำหนดให้มีการบริหารจัดการเหตุการณ์ผิดปกติและปัญหาที่เกิดจากการใช้เทคโนโลยีสารสนเทศอย่างเหมาะสมและทันท่วงที โดยมีการบันทึก วิเคราะห์ และรายงานเหตุการณ์ผิดปกติ ปัญหา และการแก้ไข ให้คณะกรรมการบริษัท คณะอนุกรรมการที่ได้รับมอบหมาย หรือพนักงานระดับบริหารที่ได้รับมอบหมายทราบ ในระยะเวลาที่เหมาะสม นอกจากนี้ ยังมีการวิเคราะห์สาเหตุที่แท้จริง (Root Cause) ของปัญหา เพื่อหาแนวทางแก้ไขจากสาเหตุที่แท้จริง และป้องกันไม่ให้เกิดเหตุการณ์ผิดปกติในอนาคต

(9) การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ

(9.1) มีคณะทำงานหรือหน่วยงานที่รับผิดชอบในการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษร ให้เป็นไปตามนโยบายที่กำหนดไว้และแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศดังกล่าวที่ได้รับอนุมัติโดยคณะกรรมการบริษัทหรือคณะอนุกรรมการที่ได้รับมอบหมาย

(9.2) จัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ โดยคำนึงถึงลักษณะการดำเนินธุรกิจ ปริมาณธุรกรรม ความซับซ้อนของเทคโนโลยีสารสนเทศ และความเสี่ยงที่เกี่ยวข้องในการดำเนินธุรกิจของบริษัท รวมทั้งการบริหารความเสี่ยงที่อาจเกิดจากเหตุการณ์ความเสียหายต่าง ๆ และความเสี่ยงทั่วไป ได้แก่ ความเสี่ยงด้านปฏิบัติการ ความเสี่ยงด้านชื่อเสียง และความเสี่ยงอื่นที่เกี่ยวข้อง โดยความเสี่ยงอื่นที่เกี่ยวข้อง ได้แก่ ความเสี่ยงจากการพึ่งพาองค์กรอื่นในการดำเนินธุรกิจ ความเสี่ยงจากการกระจุกตัวของ

ระบบงาน หรือทรัพยากรที่สำคัญ และความเสี่ยงที่มีผลกระทบต่อบริษัท ผู้ใช้บริการ ผู้มีส่วนได้เสีย และระบบบริษัท

(9.3) แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ สามารถนำไปใช้ในทางปฏิบัติได้ และสามารถนำมาใช้รองรับความเสียหายที่เกิดขึ้นได้จริงและสอดคล้องกับแนวปฏิบัติของธนาคารแห่งประเทศไทย เรื่อง การบริหารความต่อเนื่องทางธุรกิจ (BCM) และการจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (BCP) โดยแผนฉุกเฉินดังกล่าวควรครอบคลุมถึงการกำหนดระยะเวลาในการกู้คืนระบบ (RTO) และระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย (RPO) ที่สอดคล้องกับความสำคัญของระบบ รวมทั้งการกำหนดระยะเวลาสูงสุดที่ยอมให้ธุรกิจหยุดชะงัก (MTPD) เพื่อรองรับการดำเนินธุรกิจอย่างต่อเนื่องของบริษัท และรองรับการเกิดเหตุการณ์ผิดปกติต่าง ๆ ที่อาจส่งผลให้เกิดการหยุดชะงักหรือเกิดความเสียหายต่อระบบ เช่น ภัยคุกคามทางไซเบอร์ และภัยธรรมชาติ เป็นต้น เพื่อให้บริษัทดำเนินการกู้ระบบและกลับสู่การทำงานได้ตามปกติให้เร็วที่สุด

(9.4) จัดทำคู่มือหรือเอกสารประกอบการดำเนินการตามแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ รวมทั้งประชาสัมพันธ์แผนและฝึกอบรม เพื่อให้พนักงานทุกคนที่มีส่วนเกี่ยวข้องกับการดำเนินการตามแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศมีความเข้าใจและสามารถปฏิบัติตามแผนได้

(9.5) จัดให้มีการทบทวนและทดสอบการปฏิบัติตามแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศอย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

(9.6) มีศูนย์คอมพิวเตอร์สำรองที่มีความพร้อมใช้งานและสามารถปฏิบัติงานทดแทนได้เมื่อศูนย์คอมพิวเตอร์หลักหยุดชะงัก โดยบริษัทควรพิจารณาให้ศูนย์คอมพิวเตอร์สำรองอยู่ห่างจากศูนย์คอมพิวเตอร์หลักเพียงพอที่จะไม่ให้เกิดปัญหาหรือได้รับผลกระทบในลักษณะเดียวกันในช่วงเวลาเดียวกัน เช่น ระบบไฟฟ้าขัดข้อง และภัยธรรมชาติ เป็นต้น

(10) การบริหารจัดการผู้ให้บริการภายนอก (Third Party Management)

ในกรณีที่มีการจัดจ้างผู้ให้บริการภายนอกหรือมีพันธมิตรทางธุรกิจที่มีการเชื่อมต่อกับระบบเทคโนโลยีสารสนเทศของบริษัทหรือสามารถเข้าถึงข้อมูลสำคัญของบริษัทหรือของลูกค้าของบริษัทได้ โดยมีการจัดทำสัญญาหรือข้อตกลงการให้บริการโดยระบุหน้าที่ ความรับผิดชอบ และเงื่อนไขในการให้บริการอย่างชัดเจน เช่น การทำลายข้อมูลของบริษัทหรือของลูกค้าทั้งหมดเมื่อสิ้นสุดสัญญาหรือเลิกใช้บริการ ความรับผิดชอบต่อการรั่วไหลของข้อมูลอันเนื่องมาจากการนำข้อมูลไปใช้ นอกเหนือจากที่ระบุไว้ในสัญญาหรือข้อตกลงการให้บริการ เป็นต้น นอกจากนี้ ในการจัดจ้างผู้ให้บริการภายนอกหรือมีพันธมิตรทางธุรกิจในการร่วมพัฒนาหรือให้บริการทางการเงิน ให้คำนึงถึงความต่อเนื่องในการดำเนินธุรกิจของบริษัท ข้อจำกัด หรือข้อตกลงในการเปลี่ยนแปลงผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจ และการยกเลิกหรือสิ้นสุดสัญญา เพื่อให้สามารถดำเนินธุรกิจได้อย่างต่อเนื่อง และพร้อมรับการเปลี่ยนแปลงด้านเทคโนโลยีสารสนเทศที่อาจเกิดขึ้นในอนาคต

ทั้งนี้ ในกรณีที่บริษัทใช้บริการเทคโนโลยีสารสนเทศจากผู้ให้บริการภายนอกจะถือปฏิบัติตามนโยบายการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศของบริษัท

5.3 การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

บริษัทมีการบริหารจัดการเกี่ยวกับการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยกำหนดบทบาทหน้าที่ความรับผิดชอบของหน่วยงานด้านบริหารความเสี่ยง ดังต่อไปนี้ กำหนดนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศให้ครอบคลุมเรื่องโครงสร้างองค์กร และบทบาทหน้าที่ของผู้ที่เกี่ยวข้องในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ และนำนโยบายดังกล่าวมาจัดทำระเบียบ วิธีปฏิบัติ และกระบวนการในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัท โดยครอบคลุมในเรื่องดังนี้

5.3.1 การประเมินความเสี่ยง (Risk Assessment)

(1) การระบุความเสี่ยง (Risk Identification) มีการระบุถึงความเสี่ยงด้านเทคโนโลยีสารสนเทศ ซึ่งรวมถึงภัยคุกคามทางไซเบอร์ และช่องโหว่ต่าง ๆ โดยความเสี่ยงดังกล่าวอาจมีสาเหตุมาจากกระบวนการปฏิบัติงาน ระบบงาน พนักงาน หรือปัจจัยภายนอก

(2) การวิเคราะห์ความเสี่ยง (Risk Analysis) มีความเข้าใจและวิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อหาแนวทางในการจัดการความเสี่ยงที่เหมาะสม

(3) การประเมินค่าความเสี่ยง (Risk Evaluation) มีการประเมินถึงโอกาสที่ความเสี่ยงด้านเทคโนโลยีสารสนเทศจะเกิดขึ้นและผลกระทบต่อการปฏิบัติงานและการดำเนินธุรกิจ รวมถึงกำหนดระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ยอมรับได้ (IT Risk Appetite)

5.3.2 การจัดการความเสี่ยง (Risk Treatment)

มีแนวทางในการจัดการควบคุม และป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อให้ความเสี่ยงที่เหลืออยู่ (Residual Risk) อยู่ในระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ยอมรับได้ โดยต้องคำนึงถึงความสมดุลระหว่างต้นทุนในการป้องกันความเสี่ยงและผลประโยชน์ที่คาดว่าจะได้รับ นอกจากนี้ จัดให้มีการกำหนดดัชนีชี้วัดความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Key Risk Indicators) ที่เกี่ยวข้องกับการดำเนินธุรกิจ ให้สอดคล้องกับความสำคัญของเทคโนโลยีสารสนเทศแต่ละงาน เพื่อใช้ในการติดตามและทบทวนความเสี่ยง

5.3.3 การติดตามและทบทวนความเสี่ยง (Risk Monitoring And Review)

มีกระบวนการที่มีประสิทธิภาพในการติดตามและทบทวนความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อให้อยู่ภายใต้ระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ยอมรับได้ที่กำหนดไว้

5.3.4 การรายงานความเสี่ยง (Risk Reporting)

มีการรายงานผลการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ และแนวโน้มของความเสี่ยงด้านเทคโนโลยีสารสนเทศที่อาจเกิดขึ้นต่อคณะกรรมการบริษัท หรือคณะอนุกรรมการกำกับความเสี่ยงในระยะเวลาที่เหมาะสม

ทั้งนี้ กำหนดให้มีการทบทวนนโยบาย ระเบียบวิธีปฏิบัติ และกระบวนการในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ อย่างน้อยปีละ 1 ครั้งและทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

5.4 การปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ

บริษัทมีการบริหารจัดการเกี่ยวกับการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ ซึ่งกำหนดบทบาทหน้าที่ความรับผิดชอบของหน่วยงานด้านกำกับการปฏิบัติตามกฎหมายและหลักเกณฑ์ โดยจัดให้มีการกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (IT Compliance) เช่น กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และกฎหมายว่าด้วยระบบการชำระเงิน เป็นต้น เพื่อป้องกันการละเมิดหรือการไม่ปฏิบัติตามกฎหมายและหลักเกณฑ์ของหน่วยงานกำกับดูแลที่เกี่ยวข้อง

5.5 การตรวจสอบด้านเทคโนโลยีสารสนเทศ

บริษัทมีการบริหารจัดการเกี่ยวกับการตรวจสอบด้านเทคโนโลยีสารสนเทศ โดยกำหนดบทบาทหน้าที่ความรับผิดชอบของหน่วยงานตรวจสอบภายใน ดังต่อไปนี้

5.5.1 จัดให้มีผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศที่มีความรู้ประสบการณ์ และความเชี่ยวชาญเกี่ยวกับการตรวจสอบด้านเทคโนโลยีสารสนเทศ ซึ่งอาจเป็นผู้ตรวจสอบภายใน ผู้ตรวจสอบภายนอก

หรือผู้เชี่ยวชาญภายนอกที่มีความเป็นอิสระจากหน่วยงานที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ และหน่วยงานที่ทำหน้าที่บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

5.5.2 จัดทำแผนงานและขอบเขตการตรวจสอบด้านเทคโนโลยีสารสนเทศที่สอดคล้องกับความสำคัญและความเสี่ยงของการใช้เทคโนโลยีสารสนเทศของบริษัท และนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยแผนงานและขอบเขตการตรวจสอบดังกล่าว ต้องได้รับความเห็นชอบจากคณะอนุกรรมการตรวจสอบและครอบคลุมถึงเทคโนโลยีสารสนเทศที่สำคัญของบริษัท

ทั้งนี้ จะต้องทบทวนแผนงานและขอบเขตการตรวจสอบดังกล่าวอย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

5.5.3 จัดให้มีการตรวจสอบด้านเทคโนโลยีสารสนเทศอย่างน้อยปีละ 1 ครั้ง ตามแผนงานและขอบเขตที่กำหนดตามข้อ 5.5.2 และเมื่อมีเหตุการณ์ผิดปกติในเทคโนโลยีสารสนเทศที่มีนัยสำคัญ

5.5.4 จัดให้มีผู้เชี่ยวชาญภายนอกที่เป็นอิสระ ทำหน้าที่ประเมินระบบหรือเทคโนโลยีที่มีความสำคัญ หากเห็นว่ามีความจำเป็นต้องประเมินแต่มีข้อจำกัดหรือผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศของบริษัทไม่สามารถประเมินได้ เช่น การประเมินระบบที่มีความซับซ้อน หรือมีการใช้เทคโนโลยีสารสนเทศใหม่ หรือการประเมินความสามารถของระบบในการปรับเปลี่ยน เป็นต้น เพื่อรองรับการทำธุรกิจของบริษัทในอนาคตภายใต้สภาวะการเปลี่ยนแปลงทางเทคโนโลยีสารสนเทศที่รวดเร็ว

5.5.5 จัดทำรายงานผลการตรวจสอบด้านเทคโนโลยีสารสนเทศ และเสนอต่อคณะกรรมการตรวจสอบ ตลอดจนจัดเก็บรายงานผลการตรวจสอบดังกล่าวไว้ที่บริษัท พร้อมไว้สำหรับการตรวจสอบหรือเมื่อร้องขอโดยธนาคารแห่งประเทศไทย

5.5.6 จัดให้มีการติดตามประเด็นจากการตรวจสอบด้านเทคโนโลยีสารสนเทศ และรายงานประเด็นสำคัญให้กับคณะกรรมการตรวจสอบและฝ่ายงานที่เกี่ยวข้องทราบ

5.6 การบริหารจัดการโครงการด้านเทคโนโลยีสารสนเทศ

บริษัทมีการบริหารจัดการโครงการด้านเทคโนโลยีสารสนเทศ โดยกำหนดบทบาทหน้าที่ความรับผิดชอบของหน่วยงานด้านเทคโนโลยีสารสนเทศ ดังต่อไปนี้

5.6.1 มีการศึกษาความจำเป็นและประโยชน์ที่คาดว่าจะได้รับของโครงการที่มีการนำเทคโนโลยีสารสนเทศมาใช้ในการดำเนินธุรกิจก่อนเริ่มโครงการ โดยพิจารณาเลือกใช้เทคโนโลยีสารสนเทศอย่างเหมาะสม และมีการประเมินความเสี่ยงและผลกระทบที่อาจเกิดขึ้นกับฝ่ายงานอื่น และระบบที่เกี่ยวข้อง รวมทั้งมีการจัดลำดับความสำคัญของโครงการและนำเสนอขออนุมัติโครงการต่อคณะกรรมการบริษัท คณะอนุกรรมการที่ได้รับมอบหมาย หรือพนักงานระดับบริหาร ตามขอบเขตอำนาจในการอนุมัติที่กำหนดไว้

5.6.2 กำหนดกรอบการบริหารจัดการโครงการที่ชัดเจนเป็นลายลักษณ์อักษร เพื่อใช้เป็นแนวทางในการบริหารจัดการโครงการ (Project Management) โดยครอบคลุมขั้นตอนตั้งแต่การเริ่มโครงการ การดำเนินการและการควบคุมโครงการ การปิดโครงการ และการสอบทานโครงการ รวมทั้งมีการกำหนดโครงสร้างการควบคุมและกำกับดูแลโครงการที่ชัดเจน (Project Governance) ในเรื่องต่อไปนี้

(1) คณะอนุกรรมการที่ได้รับมอบหมายในการกำกับดูแลโครงการ ทำหน้าที่กำกับดูแลความคืบหน้า ให้คำแนะนำ และพิจารณาตัดสินใจการดำเนินงานในโครงการที่สำคัญ เพื่อให้การดำเนินงานของโครงการเป็นไปตามแผนงานที่กำหนด ทั้งนี้ คณะอนุกรรมการที่ได้รับมอบหมาย ประกอบด้วยผู้บริหารหรือผู้แทนจากฝ่ายงานต่าง ๆ ที่เกี่ยวข้อง

(2) หน่วยงานหรือคณะทำงานดูแลภาพรวมของโครงการ (Project Management Office : PMO) ทำหน้าที่ในการกำหนดรูปแบบ กระบวนการ และเครื่องมือ ที่เป็นมาตรฐานในการบริหารจัดการ และติดตามความคืบหน้าของโครงการ รวมทั้งรายงานความคืบหน้าและภาพรวมของโครงการที่สำคัญของบริษัทต่อคณะกรรมการบริษัท คณะอนุกรรมการที่ได้รับมอบหมายในการกำกับดูแลโครงการ หรือพนักงานระดับบริหารที่เกี่ยวข้องทราบ เพื่อให้โครงการบรรลุวัตถุประสงค์ตามเป้าหมายที่วางไว้

(3) ผู้จัดการโครงการ (Project Manager) ทำหน้าที่ในการบริหารจัดการโครงการแต่ละโครงการตามขั้นตอนการบริหารจัดการโครงการ และส่งมอบงานในแต่ละขั้นตอนตามรูปแบบกระบวนการและเครื่องมือ ตามที่หน่วยงานหรือคณะทำงานดูแลภาพรวมของโครงการกำหนด เพื่อให้สามารถส่งมอบโครงการได้อย่างถูกต้องครบถ้วนตามแผนงานที่กำหนด

5.7 การรายงานต่อธนาคารแห่งประเทศไทย

บริษัทมีการรายงานต่อธนาคารแห่งประเทศไทยผ่านช่องทางการรายงานที่ธนาคารแห่งประเทศไทยกำหนด ในกรณีที่เกิดปัญหาหรือเหตุการณ์ที่มีนัยสำคัญในการใช้เทคโนโลยีสารสนเทศ ซึ่งส่งผลกระทบต่อการให้บริการระบบงาน หรือชื่อเสียงของบริษัท รวมถึงกรณีที่เทคโนโลยีสารสนเทศที่สำคัญของบริษัทถูกโจมตีหรือถูกขู่โจมตีจากภัยคุกคามทางไซเบอร์ และเป็นปัญหาหรือเหตุการณ์ที่บริษัทต้องรายงาน

ประกาศ ณ วันที่ 12 มิถุนายน พ.ศ. 2566

(นางญาใจ พัฒนสุขวสันต์)
ประธานกรรมการ
บริษัท บริหารสินทรัพย์ ธนาคารอิสลามแห่งประเทศไทย จำกัด