ธนาคารอิสลาม
แห่งประเทศไทย
ISLAMIC BANK OF THAILAND • البنك الإسلامي بتايلاند

บันทึก เรื่อง ประกาศ นโยบายธรรมาภิบาลข้อมูล (Data Governance Policy)

ที่ กกร.(บ.) 797 / 2567 วันที่ 30 ธันวาคม พ.ศ. 2567

ส่วนงาน ฝ่ายกำกับการปฏิบัติงานและระเบียบ

เรียน ผู้บริหารสายงาน/ผู้บริหารกลุ่มงาน
ผู้อำนวยการฝ่าย/สำนัก อาวุโส
ผู้อำนวยการฝ่าย/สำนัก
ผู้จัดการสำนักงานเขต/ผู้จัดการบริหารส่วน/สาขา และหน่วยงานที่เกี่ยวข้อง

ด้วยคณะกรรมการธนาคารอิสลามแห่งประเทศไทย ในการประชุมครั้งที่ 12/2567 เมื่อวันที่ 25 ธันวาคม พ.ศ. 2567 ซึ่งมีมติอนุมัตินโยบายธรรมาภิบาลข้อมูล (Data Governance Policy) เพื่อเป็นแนวทางในการปฏิบัติงานของพนักงาน

ธนาคารจึงขอประกาศใช้นโยบายฯ ฉบับดังกล่าว มายังหน่วยงานทุกหน่วยงานที่เกี่ยวข้องเพื่อทราบและถือปฏิบัติ โดยให้มีผลบังคับใช้ตั้งแต่วันที่ 30 ธันวาคม พ.ศ. 2567 เป็นต้นไป พร้อมนี้ให้ยกเลิกนโยบายธรรมาภิบาลข้อมูล (Data Governance Policy) ฉบับลงวันที่ 16 ธันวาคม พ.ศ. 2563 และให้ใช้นโยบายฉบับนี้แทน

จึงเรียนมาเพื่อทราบ และถือปฏิบัติ

(นายธีระพล ฤทธิ์ภิญโญ)
รองผู้อำนวยการฝ่าย (แทนผู้อำนวยการฝ่าย)
ฝ่ายกำกับการปฏิบัติงานและระเบียบ

ฝ่ายงานเจ้าของเรื่อง ฝ่ายบริหารและพัฒนาระบบงานสารสนเทศ
โทร. 02-6506999 ต่อ 5123, 1113

นโยบายธรรมาภิบาลข้อมูล
(Data Governance Policy)

อาศัยอำนาจตามความในมาตรา 25 แห่งพระราชบัญญัติธนาคารอิสลามแห่งประเทศไทย พ.ศ. 2545 คณะกรรมการธนาคารอิสลามแห่งประเทศไทย ได้กำหนดนโยบายธรรมาภิบาลข้อมูล (Data Governance Policy) ไว้ดังต่อไปนี้

1. หลักการ

ธนาคารอิสลามแห่งประเทศไทย เป็นธนาคารเฉพาะกิจของรัฐ สังกัดกระทรวงการคลัง และอยู่ภายใต้พระราชบัญญัติธนาคารอิสลามแห่งประเทศไทย พ.ศ.2545 และเป็นธนาคารที่ดำเนินธุรกิจทางการเงินตามหลักการของศาสนาอิสลาม โดยธนาคารมีข้อมูลซึ่งจัดเป็นหนึ่งในทรัพย์สินที่สำคัญ และเป็นกลไกในการขับเคลื่อนการดำเนินงานของธนาคาร ดังนั้นเพื่อให้การนำข้อมูลไปใช้งานเกิดประโยชน์อย่างเต็มที่และมีประสิทธิภาพ รวมทั้งมีการบริหารจัดการข้อมูลของธนาคารทุกขั้นตอนอย่างเป็นระบบมีความชัดเจน และเป็นไปตามกฎหมาย หรือประกาศที่เกี่ยวข้อง ธนาคารจึงกำหนดนโยบายธรรมาภิบาลข้อมูลฉบับนี้ไว้เพื่อเป็นกรอบให้ฝ่ายจัดการและพนักงานของธนาคารปฏิบัติตาม โดยนโยบายธรรมาภิบาลข้อมูลจัดเป็นหนึ่งในองค์ประกอบพื้นฐานของธรรมาภิบาลข้อมูล เพื่อให้ครอบคลุมกระบวนการบริหารและกระบวนการจัดการข้อมูล ตลอดทั้งวงจรชีวิตของข้อมูล ตั้งแต่การสร้างข้อมูล การจัดเก็บข้อมูลและทำลายข้อมูล การประมวลผลข้อมูลและการใช้ข้อมูล การแลกเปลี่ยนและการเชื่อมโยงข้อมูล การเปิดเผยข้อมูล และรวมไปจนถึงการวัดการดำเนินการและความสำเร็จของการดำเนินงานด้านธรรมาภิบาลข้อมูลของธนาคาร

2. วัตถุประสงค์

2.1. เพื่อให้ธนาคารมีกรอบและแนวทางปฏิบัติในการบริหารจัดการและกำกับดูแลข้อมูลอย่างมีธรรมาภิบาล โปร่งใสและตรวจสอบได้ ส่งผลให้ข้อมูลมีคุณภาพ มีความมั่นคงปลอดภัย และธนาคารสามารถนำข้อมูลไปใช้เพื่อประโยชน์ในการดำเนินธุรกิจ การวางแผนกลยุทธ์ การบริหารความเสี่ยง และการควบคุมภายในได้อย่างมีประสิทธิภาพ

2.2. เพื่อให้การส่งมอบคุณค่าของข้อมูลเป็นไปโดยสอดคล้องกับยุทธศาสตร์ธนาคาร

2.3. เพื่อให้ธนาคารได้รับข้อมูลที่มีคุณภาพที่ดียิ่งขึ้น (Data Quality) สามารถใช้ข้อมูลเพื่อบรรลุเป้าประสงค์ทางยุทธศาสตร์ได้อย่างมีประสิทธิภาพ

3. ขอบเขตการบังคับใช้

นโยบายธรรมาภิบาลข้อมูลฉบับนี้มีผลบังคับใช้กับข้อมูลทั้งหมดที่อยู่ในความรับผิดชอบของธนาคาร โดยผู้ทำหน้าที่ดูแลข้อมูล ผู้ใช้ข้อมูล คณะทำงานธรรมาภิบาลข้อมูล (Data Governance Council) คณะทำงานบริกรข้อมูล (Data Stewards) และบุคลากรอื่นๆ ของหน่วยงาน มีหน้าที่โดยตรงที่จะต้องสนับสนุนดำเนินการและปฏิบัติตามนโยบายอย่างเคร่งครัด พนักงานและผู้ใช้อื่นที่เกี่ยวข้อง แต่ไม่มีหน้าที่ในการดูแลข้อมูลจะต้องให้ความร่วมมือในการดำเนินการตามนโยบายนี้ ผู้ฝ่าฝืนนโยบายนี้มีความผิดและจะต้องได้รับการดำเนินการตามระเบียบของธนาคาร

4. คำนิยาม

"ธนาคาร" หมายความว่า ธนาคารอิสลามแห่งประเทศไทย

"ผู้จัดการ" หมายความว่า ผู้จัดการธนาคารอิสลามแห่งประเทศไทย

"ฝ่ายจัดการ" หมายความว่า กรรมการผู้จัดการ รองกรรมการผู้จัดการ และผู้ช่วยกรรมการผู้จัดการ

"พนักงาน" หมายความว่า ผู้ที่ธนาคารจ้างไว้ปฏิบัติงานในลักษณะประจำและรับเงินเดือนตามตำแหน่งและขั้นที่บรรจุ และรวมถึงผู้ดำรงตำแหน่งผู้จัดการ

"หน่วยงาน" หมายความว่า สายงาน กลุ่มงาน ฝ่ายงาน สำนัก ของธนาคาร

"ข้อมูล" หมายความว่า สิ่งที่สื่อความหมายให้รู้เรื่องราวข้อเท็จจริง ข้อมูลหรือสิ่งใดๆ ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใดๆ และไม่ว่าจะจัดทำไว้ในรูปแบบของเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ฟิล์ม การบันทึกภาพหรือเสียงการบันทึกโดยเครื่องคอมพิวเตอร์หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏเป็นทรัพย์สินชนิดหนึ่งที่มีมูลค่าและความสำคัญแก่ธนาคาร

"ชุดข้อมูล (Data Set)" หมายความว่า ข้อมูลที่มีการรวบรวมจากแหล่งข้อมูลต่างๆ และนำมาจัดเป็นชุดให้ถูกต้องตามคุณสมบัติและลักษณะโครงสร้างของข้อมูลเพื่อให้สามารถใช้ในการประมวลผลได้

"เมทาดาตา (Meta Data)" หมายความว่า ข้อมูลที่ใช้อธิบายชุดข้อมูล (Data Set) โดยระบุรายละเอียดแหล่งข้อมูลและคำอธิบายรายละเอียดเกี่ยวกับข้อมูล ซึ่งจะทำให้ผู้ใช้ข้อมูลทราบว่าข้อมูลมาจากแหล่งใด มีรูปแบบอย่างไร ช่วยอำนวยความสะดวกในการสืบค้นข้อมูล และใช้ประโยชน์ในการจัดทำบัญชีข้อมูลของหน่วยงาน เพื่อสนับสนุนให้เกิดการเปิดเผย เชื่อมโยง และแลกเปลี่ยนข้อมูล แบ่งเป็น เมทาดาตาเชิงธุรกิจ (Business Metadata) และเมทาดาตาเชิงเทคนิค (Technical Metadata)

"เมทาดาตาเชิงธุรกิจ (Business Metadata)" หมายความว่า ข้อมูลที่ใช้อธิบายชุดข้อมูล (Data Set) ซึ่งให้รายละเอียดในด้านธุรกิจ เหมาะสำหรับผู้ใช้งานข้อมูล (Data User) นักวิเคราะห์ข้อมูล (Data Analyst) และวิทยาการข้อมูล (Data Scientist)

"เมทาดาตาเชิงเทคนิค (Technical Metadata)" หมายความว่า ข้อมูลที่ใช้อธิบายชุดข้อมูล (Data Set) ซึ่งให้รายละเอียดในด้านเทคนิคเหมาะสำหรับผู้บริหารจัดการฐานข้อมูล (Database Administrator)

"วงจรชีวิตข้อมูล (Data Life Cycle)" หมายความว่า ลำดับขั้นตอนของข้อมูลโดยเริ่มตั้งแต่การเกิดของข้อมูล (Create) วิธีการเก็บ (Store) การนำไปใช้ (Use) การเผยแพร่ (Publish) หรือการแชร์ข้อมูล (Share) การจัดเก็บถาวร (Archive) การทำลายข้อมูล (Destroy) และการเชื่อมโยงและแลกเปลี่ยนข้อมูล (Linkage and Exchange)

"ข้อมูลส่วนบุคคล (Personal Data)" หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

"เจ้าของข้อมูล (Data Owner)" พนักงานหรือฝ่ายงานที่รับผิดชอบเกี่ยวกับข้อมูล มีอำนาจในการบริหารจัดการและควบคุมชุดข้อมูล สร้าง แก้ไข ลบ กำหนดสิทธิการเข้าถึง อนุญาตหรือปฏิเสธการเข้าถึงข้อมูล และเป็นผู้รับผิดชอบต่อความถูกต้อง ทันสมัย ความสมบูรณ์ และการทำลาย รวมถึงกำหนดระดับชั้นความลับ สิทธิการใช้งาน และความปลอดภัยของข้อมูล

"เจ้าของข้อมูลส่วนบุคคล (Data Subject)" หมายความว่า ตัวบุคคลที่ข้อมูลส่วนบุคคลระบุไปถึง เช่น กรรมการ ฝ่ายจัดการ พนักงาน ผู้ถือหุ้น ลูกค้า และผู้ที่เกี่ยวข้อง ที่เป็นบุคคลธรรมดา

"เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer : DPO)" หมายความว่า บุคคลหรือคณะทำงานที่ได้รับมอบหมายให้มีหน้าที่ให้คำแนะนำและตรวจสอบการดำเนินงานของผู้ประมวลผลข้อมูลส่วนบุคคล พนักงาน และผู้ที่เกี่ยวข้องกับการเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคลตลอดจนการลบหรือทำลายข้อมูลส่วนบุคคล รักษาความลับของข้อมูลส่วนบุคคลที่ตนได้มาหรือรับรู้ และประสานงานกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล รวมถึงดำเนินการอื่นตามที่กฎหมายกำหนด

"คณะทำงานธรรมาภิบาลข้อมูล (Data Governance Council)" หมายความว่า คณะทำงานที่มีหน้าที่กำหนดนโยบาย แนวปฏิบัติด้านธรรมาภิบาลข้อมูล รวมถึงมาตรฐาน เกณฑ์วัดคุณภาพข้อมูล การจัดชั้นข้อมูล และความมั่นคงปลอดภัยของข้อมูล

"คณะทำงานบริกรข้อมูล (Data Steward Team)" หมายความว่า คณะทำงานที่มีหน้าที่จัดทำร่างนโยบาย แนวปฏิบัติด้านธรรมาภิบาลข้อมูล มาตรฐาน เกณฑ์วัดคุณภาพข้อมูล การจัดชั้นข้อมูล และความมั่นคงปลอดภัยของข้อมูล รวมถึงจัดทำชุดข้อมูล บัญชีข้อมูลของธนาคารและนิยามคำอธิบายข้อมูล

"ระดับชั้นความลับ" หมายความว่า การกำหนดการเปิดเผยข้อมูลต่อผู้อื่นให้เหมาะสมกับสถานะการใช้งาน ได้แก่ ข้อมูลลับที่สุด ข้อมูลลับมาก ข้อมูลลับ ข้อมูลที่ใช้ในกิจกรรมของธนาคารเท่านั้น และข้อมูลที่เปิดเผยต่อบุคคลภายนอกได้

"ความมั่นคงปลอดภัยของข้อมูล" หมายความว่า การธำรงไว้ซึ่งความลับ ความถูกต้องครบถ้วน และการรักษาสภาพพร้อมใช้ของข้อมูล ตามหลักเกณฑ์ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสารสนเทศ

"ธรรมภิบาลข้อมูล" หมายความว่า การกำหนดสิทธิ หน้าที่และความรับผิดชอบของผู้มีส่วนได้เสียในการบริหารจัดการข้อมูลทุกขั้นตอน เพื่อให้การได้มาและการนำไปใช้ข้อมูลของหน่วยงานถูกต้อง ครบถ้วน เป็นปัจจุบันรักษาความเป็นส่วนบุคคล และสามารถเชื่อมโยงกันได้อย่างมีประสิทธิภาพ และมั่นคงปลอดภัย

"ระบบเทคโนโลยีสารสนเทศ" หมายความว่า ข้อมูลของธนาคารที่พร้อมสำหรับการใช้งาน หรือได้รับการรวบรวมไว้สำหรับใช้งาน ได้แก่ แบบฟอร์มและเอกสารสายงานสารสนเทศ ฐานข้อมูล โปรแกรมประยุกต์ต่างๆ เป็นต้น

"ฐานข้อมูล" หมายความว่า กลุ่มข้อมูลที่มีความสัมพันธ์กันได้ถูกรวบรวมเข้าไว้ด้วยกัน ซึ่งสนับสนุนกิจกรรมของธนาคาร

"คลังข้อมูล" หมายความว่า เป็นข้อมูลที่ได้จากการเชื่อมโยงข้อมูล (Data Integration) ซึ่งเกิดจากการรวบรวมข้อมูลจากแหล่งข้อมูลต่าง ๆ ที่มีหลากหลายรูปแบบมาเก็บในคลังข้อมูลต่างๆ ของธนาคาร

5. บทบาท หน้าที่ และความรับผิดชอบ

5.1 คณะกรรมการธนาคาร

พิจารณาอนุมัตินโยบายธรรมาภิบาลข้อมูล(Data Governance Policy) ของธนาคารให้สอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง หรือข้อกำหนดอื่นๆ ที่เกี่ยวข้อง

5.2 คณะทำงานธรรมาภิบาลข้อมูล (Data Governance Council)

(1) พิจารณานโยบาย คำสั่งแนวปฏิบัติด้านธรรมาภิบาล ให้สอดคล้องกับภารกิจของธนาคาร รวมทั้งควบคุมการดำเนินการทบทวนและปรับปรุงธรรมาภิบาลข้อมูลของธนาคาร ให้มีความเหมาะสมอย่างต่อเนื่อง

(2) อนุมัติมาตรฐานข้อมูล เกณฑ์วัดคุณภาพข้อมูล การจัดชั้นข้อมูล ความมั่นคงปลอดภัยของข้อมูล และข้อบังคับอื่นๆ ที่เกี่ยวข้องกับข้อมูล เพื่อให้สามารถใช้ เชื่อมโยง แลกเปลี่ยนบูรณาการข้อมูลระหว่างกันทั้งภายในและภายนอกหน่วยงานได้อย่างมีประสิทธิภาพ และคุ้มครองข้อมูลให้มีความมั่นคงปลอดภัย เป็นไปตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้อง

(3) กำกับดูแลการบริหารจัดการข้อมูล การบริหารความเสี่ยงที่เกี่ยวข้องกับข้อมูล และการปฏิบัติตามนโยบาย คำสั่ง แนวปฏิบัติ ด้านธรรมาภิบาลข้อมูล และเกณฑ์ข้อบังคับที่กำหนด

(4) เห็นชอบแผนงานหลักของการดำเนินงานด้านธรรมาภิบาลข้อมูล และให้คำแนะนำ ข้อเสนอแนะ และแก้ไขปัญหาที่เกี่ยวข้องกับข้อมูล เพื่อให้การใช้ข้อมูลของธนาคารเกิดประโยชน์สูงสุด

(5) ผลักดัน ส่งเสริม สนับสนุนให้มีการสื่อสารกับบุคลากรในธนาคารให้ตระหนักถึงความสำคัญของข้อมูล การใช้ข้อมูลอย่างปลอดภัย เพื่อให้เกิดการกำกับดูแลข้อมูลที่ดีภายในธนาคาร และสนับสนุนเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO) ในการปฏิบัติงาน

5.3 คณะทำงานบริกรข้อมูล (Data Steward Team)

(1) จัดทำร่างนโยบาย คำสั่งแนวปฏิบัติด้านธรรมาภิบาลข้อมูลให้สอดคล้องกับภารกิจของธนาคาร รวมทั้งดำเนินการทบทวนและปรับปรุงให้มีความเหมาะสมอย่างต่อเนื่อง

(2) กำหนดมาตรฐานข้อมูล ความต้องการด้านคุณภาพข้อมูล (Data Quality) เกณฑ์การจัดชั้นข้อมูล ความมั่นคงปลอดภัยของข้อมูล และข้อบังคับอื่นๆ ที่เกี่ยวข้องกับข้อมูล รวมทั้งมาตรการควบคุม และการประเมินพัฒนาคุณภาพของข้อมูล เพื่อให้ข้อมูลมีความถูกต้องครบถ้วนเป็นปัจจุบัน มั่นคงปลอดภัย และไม่ถูกละเมิดความเป็นส่วนบุคคล ให้สอดคล้องตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้อง

(3) จำแนกหมวดหมู่ของข้อมูล เพื่อจัดทำชุดข้อมูล บัญชีข้อมูลของธนาคาร และนิยามคำอธิบายข้อมูล ให้มีความถูกต้องครบถ้วนและเป็นปัจจุบัน

(4) สนับสนุนและให้ข้อเสนอแนะ ในการบริหารจัดการความเสี่ยงที่เกิดขึ้นและแนวทางการจัดการความเสี่ยงจากการกำกับดูแลข้อมูล และการบริหารจัดการข้อมูล

(5) ดูแลและสนับสนุน ให้มีการให้ความรู้ความเข้าใจทางด้านการกำกับดูแลข้อมูลภายในธนาคาร ร่วมกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO) ในการจัดให้มีการประชุมหน่วยงานที่เกี่ยวข้อง วิเคราะห์ พิจารณา และให้ความเห็นเกี่ยวกับปัญหา การเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคลของธนาคาร การใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล การดำเนินการเมื่อข้อมูลส่วนบุคคลถูกละเมิด เพื่อนำเสนอต่อผู้จัดการเพื่ออนุมัติดำเนินการต่อไป

5.4 ฝ่ายกำกับการปฏิบัติงาน

ติดตาม ให้คำปรึกษา และกำกับดูแลการปฏิบัติงานที่เกี่ยวข้องกับข้อมูล เพื่อป้องกันการละเมิดหรือการไม่ปฏิบัติตามกฎเกณฑ์และกฎหมายที่เกี่ยวข้องกับข้อมูล

5.5 ฝ่ายบริหารความเสี่ยง

(1) จัดทำกรอบและกระบวนการบริหารความเสี่ยงให้ครอบคลุมความเสี่ยงด้านข้อมูล รวมทั้งสนับสนุนให้หน่วยงานต่างๆ มีการประเมินความเสี่ยงด้านข้อมูล

(2) ให้คำปรึกษา ติดตาม และทบทวนความเสี่ยงด้านข้อมูลให้อยู่ในระดับที่ยอมรับได้ รวมทั้งรวบรวมและเชื่อมโยงความเสี่ยงด้านข้อมูลกับความเสี่ยงด้านอื่น และนำเสนอผลการบริหารจัดการความเสี่ยงต่อคณะกรรมการที่เกี่ยวข้อง

5.6 กลุ่มตรวจสอบ

มีอำนาจหน้าที่เป็นไปตามกฎบัตรการตรวจสอบภายใน

5.7 พนักงาน

ปฏิบัติตามระเบียบว่าด้วยนโยบายการบริหารจัดการข้อมูล รวมทั้ง คำสั่ง ประกาศ วิธีปฏิบัติงานที่ประกาศใช้ภายใต้นโยบายนี้

6. เนื้อหานโยบาย

ธนาคารกำหนดให้มีกรอบและแนวทางในการบริหารจัดการข้อมูลตลอดวงจรชีวิตของข้อมูล ตั้งแต่การสร้างหรือการได้มาซึ่งข้อมูล การจัดเก็บ การใช้งานและการประมวลผล การเผยแพร่ การจัดเก็บถาวร การทำลาย การแลกเปลี่ยนและการเชื่อมโยงข้อมูล โดยคำนึงถึงความเสี่ยงที่อาจเกิดขึ้นในแต่ละขั้นตอนของวงจรชีวิต พร้อมทั้งกำหนดให้มีการควบคุมดูแลที่เหมาะสมเพื่อให้มั่นใจว่าข้อมูลในทุกขั้นตอนของวงจรชีวิตมีคุณภาพ มีความมั่นคงปลอดภัย และมีความเป็นส่วนบุคคล โดยมีรายละเอียด ดังนี้

6.1 ข้อกำหนดทั่วไป

(1) กำหนดบทบาทและความรับผิดชอบที่ประกอบกันเป็นโครงสร้างธรรมาภิบาลข้อมูล โดยต้องได้รับการมอบอำนาจและการอนุมัติจากผู้จัดการ

(2) กำหนดกลุ่มบุคคลหรือบุคคลภายในธนาคาร เพื่อเป็นเจ้าของข้อมูลในการบริหารจัดการข้อมูลของหน่วยงาน เพราะหน่วยงานถือเป็นเจ้าของข้อมูลทุกประเภทที่เกิดจากการดำเนินงานภายในหน่วยงานนั้น ๆ

(3) กำหนดขอบเขตข้อมูลที่นโยบายธรรมาภิบาลข้อมูลครอบคลุม เช่น

1) ข้อมูลที่มีโครงสร้าง (ฐานข้อมูล และ Comma Separated Value (CSV))
2) ข้อมูลกึ่งโครงสร้าง (Extensible Markup Language (XML) และ JavaScript Object Notation (JSON))
3) ข้อมูลที่ไม่มีโครงสร้าง (เอกสาร เสียง ภาพ และภาพเคลื่อนไหว)

(4) กำหนดมาตรการรักษาความปลอดภัยของข้อมูล เพื่อป้องกันการเข้าถึง การใช้ การสูญหาย การทำลาย หรือการเปลี่ยนแปลงข้อมูลโดยปราศจากอำนาจหรือโดยมิชอบ

(5) นำระบบเทคโนโลยีสารสนเทศหรือระบบอัตโนมัติมาใช้ในการจัดทำเมทาดาตา หรือเข้ามาช่วยในการบริหารจัดการข้อมูล

(6) ตรวจสอบความสอดคล้องกันระหว่างนโยบายธรรมภิบาลข้อมูลกับการดำเนินการใดๆ ของผู้มีส่วนได้เสีย อย่างน้อยปีละ 1 ครั้ง

(7) ทบทวนและดำเนินการปรับปรุงนโยบายธรรมภิบาลข้อมูลอย่างต่อเนื่อง หากพบว่านโยบายธรรมาภิบาลข้อมูลยังไม่มีประสิทธิภาพเพียงพอ

(8) สื่อสารและเผยแพร่นโยบายธรรมาภิบาลข้อมูลให้กับผู้ที่เกี่ยวข้องภายในธนาคาร และหน่วยงานภายนอกที่ธนาคารมีการเปิดเผยหรือเผยแพร่ แลกเปลี่ยน หรือเชื่อมโยงข้อมูลระหว่างกัน

(9) สนับสนุนให้มีการฝึกอบรมเพื่อสร้างความตระหนักถึงธรรมาภิบาลข้อมูล และการบริหารจัดการข้อมูล โดยครอบคลุมกระบวนการของธรรมาภิบาลข้อมูล และวงจรชีวิตข้อมูล

(10) กำหนดมาตรฐานและระเบียบวิธีปฏิบัติการบริหารจัดการคำอธิบายชุดข้อมูล ให้ครอบคลุมบทบาทหน้าที่ของผู้ที่รับผิดชอบ กระบวนการจัดทำคำอธิบายชุดข้อมูลการควบคุมดูแล และสอบทานคำอธิบายชุดข้อมูล

(11) กำหนดให้มีหน่วยงานหรือผู้รับผิดชอบในการจัดทำ ปรับปรุงแก้ไข และสอบทานคำอธิบายชุดข้อมูลทั้งในเชิงธุรกิจและเชิงเทคนิคกับทุกชุดข้อมูลสำคัญอย่างครบถ้วน รวมถึงปรับปรุงทะเบียนรายการคำอธิบายชุดข้อมูลให้เป็นปัจจุบัน และมีการเผยแพร่รายละเอียดชุดข้อมูล (Data Set) ผ่านช่องทางที่เหมาะสม

(12) กำหนดให้มีข้อมูลหลักที่จำเป็นต้องมีคุณภาพ (Critical data element) ในแต่ละชุดข้อมูล และต้องมีการกำหนดระดับคุณภาพข้อมูลในแต่ละชุดข้อมูล เพื่อใช้ในการประเมินคุณภาพของชุดข้อมูล

(13) กำหนดให้มีการประเมินคุณภาพข้อมูลตามหลักเกณฑ์คุณภาพข้อมูล เช่น การตรวจสอบและวิเคราะห์คุณภาพข้อมูลในเชิงเทคนิค (Data profiling) กับข้อมูลหลักที่จำเป็นต้องมีคุณภาพในแต่ละชุดข้อมูล รวมถึงการเปรียบเทียบกับระดับคุณภาพข้อมูลที่ธนาคารกำหนด

(14) กำหนดให้มีการวัดผลการดำเนินการและความสำเร็จของธรรมาภิบาลข้อมูล มีการติดตามและรายงานผลการดำเนินงาน อย่างน้อยปีละ 1 ครั้ง เพื่อนำไปปรับปรุงกระบวนการธรรมาภิบาลข้อมูลให้มีประสิทธิภาพมากขึ้น

6.2 การสร้างหรือการได้มาซึ่งข้อมูล

เพื่อให้การสร้างและได้มาซึ่งข้อมูล เป็นไปโดยถูกต้อง สามารถนำข้อมูลไปใช้งานได้อย่างมีประสิทธิภาพ ธนาคารกำหนดนโยบายการสร้างหรือการได้มาซึ่งข้อมูลดังนี้

(1) กำหนดความสัมพันธ์ระหว่างข้อมูลกับส่วนงาน ข้อมูลกับกระบวนการปฏิบัติงาน และข้อมูลกับระบบงาน

(2) กำหนดความต้องการของข้อมูล และข้อกำหนดทางธุรกิจโดยเป็นไปตามกฎหมายที่เกี่ยวข้อง

(3) การสร้างและการรวบรวมข้อมูล ต้องมีการรักษาความมั่นคงปลอดภัยและความเป็นส่วนบุคคลของข้อมูล และปฏิบัติตามนโยบายคุ้มครองข้อมูลส่วนบุคคล นโยบายด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ (IT Security Policy) แนวปฏิบัติการรักษาความมั่นคงปลอดภัยสารสนเทศ (IT Security Guideline) รวมถึงกฎหมายที่เกี่ยวข้อง

(4) เจ้าของข้อมูลต้องมีการจัดระดับชั้นความลับของข้อมูล และกำหนดสิทธิในการเข้าถึงให้สอดคล้องกับแนวทางการจัดระดับชั้นความลับของข้อมูล และสอดคล้องกับระดับความเสี่ยงของข้อมูล

(5) เจ้าของข้อมูลต้องจัดทำเมทาดาตา (Metadata) หรือคำอธิบายข้อมูล สำหรับข้อมูลที่จัดเก็บอยู่ในฐานข้อมูล (Database) ไฟล์ข้อมูล หรือข้อมูลที่จัดเก็บในรูปแบบอื่น ในทุกชุดข้อมูล

(6) ต้องมีมาตรการกลไกการควบคุมและการประเมินคุณภาพของข้อมูล ในการตรวจสอบการนำเข้าของข้อมูลให้เป็นไปตามมาตรฐานข้อมูล เพื่อให้ข้อมูลมีคุณภาพ มีความครบถ้วน ถูกต้องเป็นปัจจุบัน สอดคล้องกัน ไม่ซ้ำซ้อน และพร้อมใช้

6.3 การจัดเก็บข้อมูล

เพื่อให้ข้อมูลถูกต้องสมบูรณ์ มีคุณภาพ และมีความมั่นคงปลอดภัย ธนาคารจึงกำหนดสภาพแวดล้อมของการจัดเก็บข้อมูลให้เป็นไปตามข้อกำหนดการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของธนาคาร ภายใต้หลักการดังต่อไปนี้

(1) กำหนดสภาพแวดล้อมของการจัดเก็บข้อมูลที่เอื้อต่อการรักษาความมั่นคงปลอดภัยและคุณภาพของข้อมูล

(2) กำหนดชั้นความลับของข้อมูล และจัดเก็บให้สอดคล้องกับแนวทางหรือมาตรฐานการจัดชั้นความลับของข้อมูล (Data Classification Guideline/Standard) ที่กำหนดไว้ เพื่อให้ข้อมูลมีความมั่นคงปลอดภัย และรักษาคุณภาพของข้อมูล

(3) กำหนดสิทธิ์การเข้าถึงข้อมูล และเครื่องมือที่ใช้ในการเข้าถึงข้อมูล เฉพาะพนักงานที่เกี่ยวข้องและได้รับอนุญาตเท่านั้นที่จะมีสิทธิเข้าถึงข้อมูลได้ภายในระยะเวลาและขอบเขตการปฏิบัติงานที่กำหนด

(4) จัดเก็บข้อมูลให้สอดคล้องกับความต้องการ และวัตถุประสงค์ในการดำเนินงาน โดยข้อมูลนั้นจะต้องมีความถูกต้อง สมบูรณ์ และเป็นปัจจุบันอยู่เสมอ ทั้งนี้ควรจัดทำเมทาดาตาสำหรับชุดข้อมูลที่มีการจัดเก็บ

(5) จัดเก็บข้อมูลส่วนบุคคลหรือข้อมูลข่าวสารลับไว้ในสถานที่ปกปิด ซึ่งบุคคลที่ไม่เกี่ยวข้องกับข้อมูลดังกล่าวต้องไม่สามารถเข้าถึงได้

(6) ต้องมีการสำรองข้อมูล (Data Backup) ให้มีความพร้อมใช้งานอยู่ตลอดเวลา

6.4 การใช้งานและประมวลผลข้อมูล

เพื่อให้การใช้งานและการประมวลผลข้อมูล เป็นไปโดยถูกต้อง มีประสิทธิภาพ และเกิดประโยชน์ตรงตามวัตถุประสงค์ของการใช้ข้อมูล ธนาคารกำหนดนโยบายการใช้งานและประมวลผลข้อมูล ดังนี้

(1) ให้คณะทำงานธรรมาภิบาลข้อมูล (Data Governance Council) กำหนดแนวปฏิบัติและมาตรฐานของการประมวลผลข้อมูลและการใช้ข้อมูลเพื่อการวิเคราะห์ และสื่อสารให้หน่วยงานหรือพนักงานที่เกี่ยวข้องทราบและถือปฏิบัติ

(2) ให้หน่วยงานหรือพนักงานซึ่งประสงค์จะประมวลผลหรือใช้ข้อมูลส่วนบุคคล ต้องดำเนินการภายใต้ขอบเขตวัตถุประสงค์และเงื่อนไขที่ได้แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบ ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไว้เท่านั้น หากนอกเหนือจากขอบเขตวัตถุประสงค์และเงื่อนไขดังกล่าวข้างต้น จะต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อน

(3) ให้หน่วยงานหรือพนักงานที่ประมวลผลข้อมูลหรือใช้ข้อมูลเพื่อการวิเคราะห์ ทำการบันทึกประวัติการดำเนินการ (Log File) ไว้ด้วย เพื่อให้สามารถตรวจสอบย้อนกลับได้

(4) จัดทำเมทาดาตาสำหรับข้อมูลที่จัดเก็บอยู่ในคลังข้อมูล (Data Warehouse)

6.5 การเผยแพร่หรือเปิดเผยข้อมูล

ในการเปิดเผยหรือเผยแพร่ข้อมูลให้กับหน่วยงานกำกับดูแล (Regulator) บุคคล หรือหน่วยงานภายนอกที่เกี่ยวข้อง ให้หน่วยงานและพนักงานที่เกี่ยวข้องถือปฏิบัติให้เป็นไปโดยถูกต้องตรงตามวัตถุประสงค์ของการนำข้อมูลไปใช้ประโยชน์ของเจ้าของข้อมูล ภายใต้หลักการดังต่อไปนี้

(1) ห้ามเปิดเผยข้อมูลที่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง นโยบาย แนวปฏิบัติ ไม่ว่าข้อมูลจะอยู่ในรูปแบบใดหรือสถานที่ใดก็ตาม

(2) การเปิดเผยหรือเผยแพร่ข้อมูลส่วนบุคคลต้องได้รับการยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่ เป็นกรณีที่สามารถดำเนินการได้ตามกฎหมาย หรือมีการจัดทำข้อมูลให้เป็นข้อมูลนิรนามหรือข้อมูลที่ไม่สามารถระบุตัวบุคคลได้

(3) กำหนดกระบวนการเปิดเผยหรือเผยแพร่ข้อมูลให้ชัดเจนตั้งแต่ขั้นตอนการเตรียมการ ขั้นตอนเริ่มดำเนินการ ขั้นตอนระหว่างดำเนินการ และขั้นตอนสิ้นสุดการดำเนินการ ที่สอดคล้องกับเกณฑ์กำหนดระดับชั้นความลับของข้อมูล

(4) กำหนดบทบาทหน้าที่ที่เกี่ยวข้องกับการเปิดเผยหรือเผยแพร่ข้อมูล ได้แก่ กำหนดบุคคลหรือกลุ่มบุคคลที่มีสิทธิตัดสินใจในการเปิดเผยข้อมูล กำหนดบุคคลหรือกลุ่มบุคคลในการดำเนินการและปรับปรุงการเปิดเผยข้อมูล และกำหนดบุคคลหรือกลุ่มบุคคลในการรับเรื่องและแก้ไขปัญหาเบื้องต้นในการเข้าถึงข้อมูลและการนำข้อมูลไปใช้

(5) ควรมีการเปิดเผยเมทาดาตาควบคู่ไปกับข้อมูลที่เปิดเผย

(6) สามารถตรวจสอบได้ว่าการเปิดเผยข้อมูลได้ถูกดำเนินการอย่างเหมาะสมหรือเป็นไปตามแนวทางที่ได้กำหนดไว้ เพื่อให้ได้ข้อมูลที่มีคุณภาพ และเป็นการรักษาคุณภาพของข้อมูล

(7) ให้มีการกำหนดผู้รับผิดชอบหลัก ระบุขั้นตอน และวิธีการนำชุดข้อมูลขึ้นเผยแพร่สู่สาธารณะ

(8) ให้มีการคัดเลือกชุดข้อมูลที่ต้องการเผยแพร่ โดยหน่วยงานเจ้าของข้อมูลหรือผู้ที่ได้รับมอบหมาย

(9) ควรมีการระบุช่องทางการเปิดเผยข้อมูลที่เข้าถึงและนำไปใช้ได้ง่าย

(10) บันทึกประวัติรายละเอียดการเปิดเผยข้อมูลแต่ละครั้งเพื่อประโยชน์ในการตรวจสอบ

6.6 การทำลายข้อมูล

การทำลายข้อมูลจะต้องดำเนินการตามหลักเกณฑ์และวิธีการที่กำหนด รวมถึงต้องปฏิบัติตามระเบียบและคำสั่ง ว่าด้วยเรื่องนโยบายด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ (IT Security Policy) และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของธนาคาร โดยให้ถือปฏิบัติตามหลักการดังต่อไปนี้

(1) ต้องมีการทบทวนอายุการใช้งานของข้อมูล และแนวทางในการทำลายข้อมูลให้สอดคล้องกับระดับชั้นความลับของข้อมูล โดยเฉพาะข้อมูลที่อ่อนไหวจะต้องมีการทำลายที่เหมาะสม โดยต้องไม่ขัดกับกฎเกณฑ์และกฎหมายที่เกี่ยวข้อง

(2) ให้หน่วยงานที่เกี่ยวข้องทำลายข้อมูลในกรณีดังต่อไปนี้

ก. ในกรณีที่มีการร้องขอให้ทำลายข้อมูลส่วนบุคคลจากเจ้าของข้อมูล ผู้ควบคุมหรือหน่วยงานที่จัดเก็บต้องดำเนินการทำลายให้เร็วที่สุด ทั้งนี้ต้องไม่ขัดต่อข้อตกลงระหว่างเจ้าของข้อมูลกับผู้ควบคุม หรือไม่ขัดต่อข้อกฎหมายใด ๆ

ข. เมื่อเจ้าของข้อมูลส่วนบุคคลถอนความยินยอม หรือคัดค้านการเก็บ รวบรวมใช้ หรือเปิดเผยข้อมูลตามที่กฎหมายกำหนด

ค. เมื่อเจ้าของข้อมูลส่วนบุคคลร้องขอให้ทำลายข้อมูลส่วนบุคคลของตน

ง. เมื่อพ้นกำหนดการเก็บรักษาไว้ตามคำสั่ง เรื่องแนวปฏิบัติการจัดเก็บและทำลายเอกสาร หรือตามระยะเวลาที่กำหนดในกฎหมายอื่นที่เกี่ยวข้อง

จ. เมื่อฝ่ายงานที่เป็นเจ้าของข้อมูลร้องขอให้ทำลายข้อมูลที่จัดเก็บไว้โดยไม่มีการใช้ประโยชน์อีกต่อไป

ฉ. กำหนดแนวทางในการทำลายข้อมูลเมื่อข้อมูลนั้นไม่มีการใช้งานหรือมีการเก็บข้อมูลไว้นานเกินกว่าระยะเวลาที่กำหนด แต่ควรมีการเก็บรักษาเมทาดาตาของข้อมูลที่ทำลายไว้เพื่อใช้สำหรับการตรวจสอบภายหลัง

ช. เมื่อคณะทำงานบริกรข้อมูล (Data Steward Team) แจ้งให้ฝ่ายงานที่เป็นเจ้าของข้อมูลทำลายข้อมูลที่จัดเก็บไว้เกินกว่าระยะเวลาที่กำหนด เว้นแต่ฝ่ายงานที่เป็นเจ้าของข้อมูลจะมีเหตุผลความจำเป็นในการจัดเก็บข้อมูลเกินกว่าระยะเวลาที่กำหนด แต่จะต้องทบทวนเหตุผลความจำเป็นดังกล่าวทุกปี

ซ. สร้างความรู้ความเข้าใจในการจัดเก็บและทำลายข้อมูลแก่ผู้ที่เกี่ยวข้องภายในธนาคาร

(3) การทำลายข้อมูลจะต้องครอบคลุมถึงข้อมูลที่เป็นเอกสารต้นฉบับและสำเนา รวมทั้งข้อมูลอิเล็กทรอนิกส์ด้วย

6.7 การแลกเปลี่ยนและการเชื่อมโยงข้อมูล

เพื่อให้การแลกเปลี่ยนและการเชื่อมโยงข้อมูลระหว่างธนาคารกับหน่วยงานภายนอก มีความมั่นคงปลอดภัยและมีประสิทธิภาพ ให้หน่วยงานที่เกี่ยวข้องถือปฏิบัติตามหลักการดังต่อไปนี้

(1) กำหนดแนวปฏิบัติในการจัดการเรื่องความมั่นคงปลอดภัย คุณภาพข้อมูล และผู้ประสานงานหรือศูนย์ติดต่อ (Contact Center)

(2) ทำสัญญาอนุญาต บันทึกข้อตกลง (Memorandum of Understanding : MOU) สัญญารักษาความลับ (Non-disclosure agreement : NDA) หรือข้อตกลงอื่นใดว่าด้วยการเชื่อมโยงข้อมูลของธนาคารหรือข้อตกลงในการแลกเปลี่ยนข้อมูล รวมทั้งแนวปฏิบัติในการเก็บรวบรวม ใช้และเปิดเผยข้อมูล การจัดการเรื่องความมั่นคงปลอดภัย คุณภาพข้อมูล รวมทั้งผู้ประสานงานหรือผู้ติดต่ออย่างชัดเจน

(3) กำหนดกระบวนการแลกเปลี่ยนและการเชื่อมโยงข้อมูลระหว่างกันให้ชัดเจน ตั้งแต่ขั้นตอนการเตรียมการ ขั้นตอนเริ่มดำเนินการ ขั้นตอนระหว่างดำเนินการ และขั้นตอนสิ้นสุดการดำเนินการ

(4) กำหนดบุคคลหรือกลุ่มบุคคลในการดำเนินการเชื่อมโยงและแลกเปลี่ยนข้อมูล เช่น บุคคลที่ทำหน้าที่ออกแบบกระบวนการและเทคโนโลยีในการเชื่อมโยงและแลกเปลี่ยนข้อมูล (Data Integration Architect) บุคคลที่ทำหน้าที่ดำเนินการเชื่อมโยงและแลกเปลี่ยนข้อมูลให้สอดคล้องกับที่ได้ออกแบบไว้ (Data Integration Specialist)

(5) กำหนดเทคโนโลยีและมาตรฐานทางเทคนิคที่จำเป็นในการแลกเปลี่ยนข้อมูล และเชื่อมโยงข้อมูล

(6) กำหนดเมทาดาตา (Meta Data) ของชุดข้อมูล (Data Set) ที่ต้องการแลกเปลี่ยนและ เชื่อมโยงข้อมูลที่จำเป็นให้ครบถ้วน บันทึกประวัติรายละเอียดการแลกเปลี่ยนและเชื่อมโยงข้อมูลแต่ละครั้ง เพื่อประโยชน์ในการตรวจสอบ

(7) บันทึกรายละเอียดและจัดเก็บข้อมูลการดำเนินงานที่เกิดขึ้นในแต่ละครั้งที่มีการแลกเปลี่ยนข้อมูล (Log File) ระหว่างธนาคารกับหน่วยงานภายนอก เพื่อให้สามารถตรวจสอบย้อนกลับได้

(8) สามารถตรวจสอบได้ว่าการแลกเปลี่ยนข้อมูลได้ดำเนินการอย่างเหมาะสมหรือเป็นไปตามแนวทางปฏิบัติ กระบวนการแลกเปลี่ยน และมาตรฐานตามที่กำหนด

(9) ตรวจสอบว่าการแลกเปลี่ยนและเชื่อมโยงข้อมูลได้ดำเนินการตามกฎหมาย ระเบียบ และแนวปฏิบัติในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูล การจัดการเรื่องความมั่นคงปลอดภัย และคุณภาพข้อมูลตามที่ได้กำหนดไว้ร่วมกัน

6.8 การรักษาความมั่นคงปลอดภัยของข้อมูลและการรักษาความเป็นข้อมูลส่วนบุคคล

(1) ธนาคารต้องมีการรักษาความมั่นคงปลอดภัยของข้อมูล ครอบคลุมการรับส่งข้อมูลผ่านเครือข่ายการสื่อสาร การจัดเก็บหรือใช้ข้อมูลบนระบบงานและสื่อบันทึกข้อมูลต่างๆ การเก็บรักษาและการทำลายข้อมูล รวมถึงกรณีที่มีการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก ให้สอดคล้องกับระดับความเสี่ยงของข้อมูล และดำเนินการตามนโยบายด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ (IT Security Policy) และคำสั่งเรื่องแนวปฏิบัติการรักษาความมั่นคงปลอดภัยสารสนเทศ (IT Security Guideline) รวมถึงกฎเกณฑ์และกฎหมายที่เกี่ยวข้อง

(2) ธนาคารต้องมีการรักษาความเป็นส่วนบุคคลของข้อมูลให้เป็นไปตามนโยบายคุ้มครองข้อมูลส่วนบุคคล และให้สอดคล้องกับกฎเกณฑ์และกฎหมายที่เกี่ยวข้อง

(3) ธนาคารต้องมีการดูแลข้อมูลของลูกค้าให้เป็นไปตามมาตรฐานขั้นต่ำสำหรับการดูแลข้อมูลของลูกค้าตามนโยบายการบริหารจัดการด้านการให้บริการแก่ลูกค้าอย่างเป็นธรรม (Market Conduct Policy)

6.9 การบริหารจัดการประเด็นปัญหาด้านข้อมูล

(1) ธนาคารต้องมีกระบวนการติดตามและบริหารจัดการประเด็นปัญหาด้านข้อมูล ทั้งการตรวจจับการระบุ การยับยั้งปัญหา การวิเคราะห์หาสาเหตุ การรวบรวมหลักฐานหรือเอกสาร การแก้ไขปัญหาการบริหารจัดการให้สามารถกลับมาดำเนินธุรกิจได้ตามปกติ รวมถึงการปรับปรุงกระบวนการควบคุมเพื่อลดโอกาสที่จะเกิดปัญหาที่คล้ายกันในอนาคต

(2) ในกรณีที่เกิดประเด็นปัญหากับธนาคาร และส่งผลกระทบต่อความต่อเนื่องในการดำเนินธุรกิจ ฝ่ายจัดการ พนักงาน และผู้เกี่ยวข้อง จะต้องปฏิบัติตามนโยบายการบริหารความต่อเนื่องทางธุรกิจ และแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan) ของธนาคาร

(3) กรณีเกิดเหตุการณ์ละเมิดข้อมูลขึ้น ฝ่ายจัดการ พนักงาน และผู้เกี่ยวข้อง จะต้องปฏิบัติตามวิธีปฏิบัติงาน เรื่องการขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลและการดำเนินการเมื่อข้อมูลส่วนบุคคลถูกละเมิด

7. การวัดการดำเนินการและความสำเร็จของธรรมาภิบาลข้อมูล

กำหนดให้มีการติดตาม ตรวจสอบ และประเมินผล รวมทั้งการทบทวนการปฏิบัติตามนโยบายธรรมาภิบาลข้อมูลในทุกปี เพื่อให้เห็นระดับการดำเนินการของธรรมาภิบาลข้อมูล ซึ่งจะส่งผลต่อความสำเร็จของการดำเนินการหรือคุณภาพของข้อมูลธนาคาร การควบคุมและตรวจสอบการดำเนินงานที่เกี่ยวข้องกับข้อมูล

8. การทบทวนและเปลี่ยนแปลงนโยบาย

กำหนดให้มีการทบทวนนโยบายอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงกฎเกณฑ์ คำสั่ง แนวปฏิบัตินโยบายจากคณะกรรมการ และจากหน่วยงานภายนอกที่กำกับดูแลธนาคารอย่างมีนัยสำคัญ

9. การปฏิบัติตามนโยบาย

กำหนดให้ผู้จัดการมีอำนาจในการออกระเบียบธนาคาร ระเบียบปฏิบัติงาน ประกาศ คำสั่ง หลักเกณฑ์ หรือคู่มือปฏิบัติงานเพื่อให้หน่วยงานใช้ในการปฏิบัติงานตามนโยบายฉบับนี้ บรรดาระเบียบ ประกาศ คำสั่ง คู่มือปฏิบัติงาน หรือหลักเกณฑ์ที่ใช้บังคับอยู่ก่อนวันที่นโยบายฉบับนี้มีผลใช้บังคับ ให้ยังคงใช้บังคับได้ต่อไปเท่าที่ไม่ขัดหรือแย้งกับนโยบายฉบับนี้จนกว่าจะมีระเบียบ ประกาศ คำสั่ง คู่มือปฏิบัติงานหรือหลักเกณฑ์ที่ออกตามนโยบายฉบับนี้ใช้บังคับแทน

ทั้งนี้ ให้มีผลบังคับใช้ตั้งแต่บัดนี้เป็นต้นไป และให้ยกเลิกประกาศนโยบายธรรมาภิบาลข้อมูล (Data Governance Policy) ฉบับลงวันที่ 16 ธันวาคม พ.ศ. 2563 และให้ใช้นโยบายฉบับนี้แทน

ให้ไว้ ณ วันที่ 30 ธันวาคม พ.ศ. 2567

(นายยงยุทธ ชัยพรหมประสิทธิ์)
ประธานกรรมการ
ธนาคารอิสลามแห่งประเทศไทย