



กองทุนบำเหน็จบำนาญข้าราชการ
ระเบียบกองทุนบำเหน็จบำนาญข้าราชการ
ว่าด้วยนโยบายการบริหารจัดการข้อมูล
พ.ศ. 2567

โดยที่เป็นการสมควรปรับปรุงนโยบายการบริหารจัดการข้อมูล เพื่อให้หน่วยงานและผู้ปฏิบัติงานที่เกี่ยวข้องกับข้อมูลทราบถึงบทบาทหน้าที่ ข้อควรปฏิบัติ และข้อห้ามปฏิบัติในการบริหารจัดการข้อมูล ซึ่งจะทำให้การปฏิบัติงานที่เกี่ยวข้องกับข้อมูลเป็นไปอย่างถูกต้อง เหมาะสม และมีประสิทธิภาพ

อาศัยอำนาจตามความในมาตรา 24 แห่งพระราชบัญญัติกองทุนบำเหน็จบำนาญข้าราชการ พ.ศ. 2539 เลขาธิการจึงออกระเบียบไว้ดังต่อไปนี้

ข้อ 1 ระเบียบนี้เรียกว่า “ระเบียบกองทุนบำเหน็จบำนาญข้าราชการ ว่าด้วยนโยบายการบริหารจัดการข้อมูล พ.ศ. 2567”

ข้อ 2 ระเบียบนี้ให้ใช้บังคับตั้งแต่วันที่ 4 กรกฎาคม 2567 เป็นต้นไป

ข้อ 3 ให้ยกเลิก “ระเบียบกองทุนบำเหน็จบำนาญข้าราชการ ว่าด้วยนโยบายการบริหารจัดการข้อมูล พ.ศ. 2563”

ข้อ 4 ให้เลขาธิการเป็นผู้รักษาการตามระเบียบนี้ รวมทั้งให้มีอำนาจตีความและวินิจฉัยปัญหาที่เกิดขึ้นจากการปฏิบัติตามระเบียบนี้

หมวด 1
บททั่วไป

ข้อ 5 ในระเบียบนี้

“ผู้ปฏิบัติงาน” หมายความว่า พนักงานหรือลูกจ้างของกองทุน

“ข้อมูล” หมายความว่า สิ่งที่สามารถทำให้รู้เรื่องราวข้อเท็จจริง ข้อมูล หรือสิ่งใด ๆ ไม่ว่า การสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใด ๆ และไม่ว่าจะได้จัดทำไว้ในรูปแบบของเอกสาร แฟ้ม รายงาน หนังสือ แผ่นผัง แผนที่ ภาพวาด ภาพถ่าย ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้

“ชุดข้อมูล (Data Set)” หมายความว่า ข้อมูลที่มีการรวบรวมจากแหล่งข้อมูลต่าง ๆ และนำมาจัดเป็นชุดให้ถูกต้องตามคุณสมบัติและลักษณะโครงสร้างของข้อมูล เพื่อให้สามารถใช้ในการประมวลผลได้

“เมทาดาตา (Meta Data)” หมายความว่า ข้อมูลที่ถูกจัดวางโครงสร้างอย่างเป็นระบบเพื่อใช้อธิบายข้อมูลหลักหรือกลุ่มข้อมูลอื่นที่เกี่ยวข้องทั้งที่เป็นกระบวนการเชิงธุรกิจและเชิงเทคโนโลยีสารสนเทศ ซึ่งจะช่วยให้สามารถเข้าใจข้อมูล กฎและข้อจำกัดของข้อมูล โครงสร้างและระบบของข้อมูล รวมทั้งขั้นตอนการทำงานได้ดียิ่งขึ้น

ข้อ 6 ข้อมูลของกองทุนที่บริหารจัดการภายใต้นโยบายที่กำหนดไว้ในระเบียบนี้ประกอบด้วย

(1) ข้อมูลเพื่อการวิเคราะห์ซึ่งจัดเก็บอยู่ในคลังข้อมูล (Data Warehouse) ที่ได้จากการรวบรวมหรือเชื่อมโยงข้อมูล (Data Integration) จากแหล่งข้อมูลต่าง ๆ โดยผ่านกระบวนการแปลงข้อมูลด้วยวิธีการเชิงคุณภาพเพื่อให้ได้ข้อมูลตรงตามความต้องการ รวมทั้งเป็นไปตามโครงสร้างหรือรูปแบบของข้อมูลที่เหมาะสม



และสามารถนำไปใช้วิเคราะห์หรือใช้ประโยชน์ในกิจการของกองทุนต่อไปได้ เช่น รายงานอัจฉริยะ (Business Intelligence) หรือดาตาอานาไลติกส์ (Data Analytics)

(2) ข้อมูลเพื่อการเปิดเผย แลกเปลี่ยน และเชื่อมโยงระหว่างกองทุนกับหน่วยงานภายนอกภายใต้ขอบเขตที่กำหนดอย่างชัดเจนโดยนิติกรรมสัญญา

ข้อ 7 ในการบริหารจัดการข้อมูลของกองทุนจะต้องคำนึงถึงปัจจัยดังต่อไปนี้

(1) การบริหารจัดการข้อมูลให้เป็นไปตามหลักธรรมาภิบาลข้อมูลดังต่อไปนี้

(ก) ต้องกำหนดนโยบายและแนวปฏิบัติสำหรับการบริหารจัดการข้อมูล เพื่อให้ข้อมูลมีความถูกต้อง ครบถ้วน เป็นปัจจุบัน พร้อมใช้งาน

(ข) ต้องกำหนดมาตรฐานด้านข้อมูลและเป้าหมายการปฏิบัติงานที่เกี่ยวกับข้อมูล ซึ่งครอบคลุมมาตรการความมั่นคงปลอดภัยของข้อมูล (Data Security) และการคุ้มครองข้อมูลส่วนบุคคล เพื่อป้องกันการเข้าถึง การทำลายหรือทำให้สูญหาย หรือการเปลี่ยนแปลงข้อมูลโดยไม่ชอบด้วยกฎหมายหรือโดยไม่ได้รับอนุญาต

(ค) ต้องนำระบบเทคโนโลยีสารสนเทศมาใช้ในการจัดทำเมทาดาตา (Meta Data) และเผยแพร่รายละเอียดชุดข้อมูล (Data Set) ผ่านเว็บท่า (Portal) โดยจัดให้มีช่องทางสำหรับให้บริการและให้คำปรึกษา แนะนำเกี่ยวกับการใช้ข้อมูลที่ถูกต้อง

(ง) ต้องตรวจสอบทบทวนความเหมาะสมของนโยบายและแนวปฏิบัติสำหรับการบริหารจัดการข้อมูล รวมทั้งมาตรฐานด้านข้อมูลและเป้าหมายการปฏิบัติงานที่เกี่ยวกับข้อมูลอย่างต่อเนื่องไม่น้อยกว่าปีละหนึ่งครั้ง เพื่อให้สอดคล้องกับกฎหมายที่เกี่ยวข้องและการบริหารจัดการข้อมูลของกองทุนที่มีประสิทธิภาพ

(จ) ต้องสื่อสารและเผยแพร่ นโยบายและแนวปฏิบัติสำหรับการบริหารจัดการข้อมูล รวมทั้งมาตรฐานด้านข้อมูลและเป้าหมายการปฏิบัติงานที่เกี่ยวกับข้อมูลให้ผู้ปฏิบัติงานและหน่วยงานต่าง ๆ ที่เกี่ยวข้อง ทั้งภายในและภายนอกกองทุน รับทราบและถือปฏิบัติ

(ฉ) จัดฝึกอบรมเพื่อสร้างความตระหนักถึงหลักธรรมาภิบาลข้อมูลตามระเบียบนี้ให้แก่ผู้ปฏิบัติงานอย่างสม่ำเสมอ

(2) การรักษาความมั่นคงปลอดภัยของข้อมูลตามกฎหมาย รวมทั้งระเบียบ ประกาศ และนโยบาย ที่กองทุนกำหนด

(3) การคุ้มครองข้อมูลส่วนบุคคลตามกฎหมาย รวมทั้งระเบียบ ประกาศ และนโยบายที่กองทุนกำหนด

หมวด 2

บทบาทและอำนาจหน้าที่ของผู้ที่เกี่ยวข้อง

ข้อ 8 เพื่อให้สามารถบริหารจัดการข้อมูลของกองทุนให้เป็นไปตามหลักธรรมาภิบาลข้อมูล กองทุนจึงกำหนดบทบาทและอำนาจหน้าที่ของผู้ที่เกี่ยวข้องดังต่อไปนี้

(1) “ผู้บริหารข้อมูลระดับสูง (Chief Data Officer)” ซึ่งเป็นผู้บริหารสูงสุดของกลุ่มงานเทคโนโลยีสารสนเทศ มีอำนาจหน้าที่ดังต่อไปนี้

(ก) จัดทำวิสัยทัศน์และพันธกิจเพื่อให้การบริหารจัดการข้อมูลเป็นไปตามหลักธรรมาภิบาลข้อมูล



(ข) จัดทำนโยบายและแนวปฏิบัติสำหรับการบริหารจัดการข้อมูลให้มีความสอดคล้องกันและเป็นไปตามหลักธรรมาภิบาลข้อมูล รวมทั้งจัดให้มีการทบทวนและปรับปรุงนโยบายและแนวปฏิบัติสำหรับการบริหารจัดการข้อมูลของกองทุนอย่างต่อเนื่อง

(ค) จัดทำเป้าหมายและการวัดความสำเร็จของการดำเนินการธรรมาภิบาลข้อมูล รวมทั้งให้คำปรึกษาและข้อเสนอแนะเกี่ยวกับการบริหารจัดการข้อมูล มาตรฐานข้อมูล การจัดลำดับความสำคัญของข้อมูล

(ง) กำหนดหรือเสนอแนะแนวทางในการสรรหาเทคโนโลยี เครื่องมือ หรือวิธีการในการนำข้อมูลไปใช้เพื่อประโยชน์ของกองทุน

(จ) บริหารจัดการข้อมูลให้มีคุณภาพ เพื่อให้ข้อมูลมีความถูกต้องครบถ้วน เป็นปัจจุบัน และพร้อมใช้งาน เพื่อให้เป็นไปตามหลักการธรรมาภิบาลข้อมูล

(ฉ) ประสานงานระหว่างหน่วยงานภาครัฐในการแลกเปลี่ยนและเชื่อมโยงข้อมูลระหว่างกัน

(ช) ส่งเสริมและมอบหมายให้ผู้ปฏิบัติงานในสังกัดกลุ่มงานเทคโนโลยีสารสนเทศปฏิบัติตามความเหมาะสม

(2) “คณะกรรมการธรรมาภิบาลข้อมูล” ที่เลขาธิการแต่งตั้ง ประกอบด้วยผู้บริหารข้อมูลระดับสูง (Chief Data Officer) เป็นประธาน ผู้บริหารสูงสุดของทุกกลุ่มงานของกองทุน เป็นกรรมการ และให้ผู้บริหารสูงสุดของฝ่ายระบบงานสารสนเทศเป็นเลขานุการ โดยมีอำนาจหน้าที่ดังต่อไปนี้

(ก) พิจารณาให้ความเห็นชอบวิสัยทัศน์และพันธกิจเพื่อให้การบริหารจัดการข้อมูลเป็นไปตามหลักธรรมาภิบาลข้อมูล

(ข) พิจารณาให้ความเห็นชอบนโยบายและแนวปฏิบัติสำหรับการบริหารจัดการข้อมูลให้มีความสอดคล้องกันและเป็นไปตามหลักธรรมาภิบาลข้อมูล รวมทั้งกำกับดูแลให้มีการทบทวนและปรับปรุงนโยบายและแนวปฏิบัติสำหรับการบริหารจัดการข้อมูลของกองทุนอย่างต่อเนื่อง

(ค) พิจารณากำหนดเป้าหมายและการวัดความสำเร็จของการดำเนินการธรรมาภิบาลข้อมูล

(ง) พิจารณากำหนดให้หน่วยงานที่ขอให้มีและใช้งานระบบสารสนเทศที่มีความสำคัญเป็นเจ้าของระบบ (System Owner) หรือหน่วยงานที่รับผิดชอบในการเก็บรวบรวมหรือใช้ข้อมูลที่มีความสำคัญเป็นเจ้าของข้อมูล (Data Owner)

(จ) กำกับดูแลและติดตามให้การบริหารจัดการข้อมูลของกองทุนให้เป็นไปตามหลักธรรมาภิบาลข้อมูล รวมทั้งให้คำปรึกษาและวินิจฉัยปัญหาที่เกี่ยวกับการบริหารจัดการข้อมูลของกองทุน

(ฉ) ส่งเสริมและสนับสนุนการดำเนินงานด้านธรรมาภิบาลข้อมูลให้สอดคล้องกับมาตรฐานรัฐบาลดิจิทัลว่าด้วยกรอบธรรมาภิบาลข้อมูลภาครัฐ โดยจะนำมาปรับใช้อย่างเหมาะสมและเกิดประโยชน์สูงสุดต่อกองทุน

(ช) สนับสนุน ส่งเสริม และผลักดันการบริหารจัดการข้อมูลของกองทุนให้เป็นตามหลักธรรมาภิบาลข้อมูลอย่างทั่วถึงและต่อเนื่อง

(ช) รายงานสรุปผลการดำเนินงานที่เกี่ยวข้องกับธรรมาภิบาลข้อมูลให้เลขาธิการทราบอย่างน้อยปีละหนึ่งครั้ง

(3) “คณะบริการข้อมูล” ที่เลขาธิการแต่งตั้ง ประกอบด้วยผู้บริหารสูงสุดของฝ่ายระบบงานสารสนเทศ เป็นประธานคณะบริการข้อมูล (Lead Data Steward) ผู้ปฏิบัติงานซึ่งเป็นผู้แทนจากกลุ่มงานที่เป็นเจ้าของระบบ (System Owner) และเจ้าของข้อมูล (Data Owner) เป็นบริการข้อมูลด้านธุรกิจ (Business Data Steward)



ผู้ปฏิบัติงานด้านความมั่นคงปลอดภัยของข้อมูลที่เป็นผู้แทนจากฝ่ายบริหารเทคโนโลยีสารสนเทศ และผู้ปฏิบัติงานที่เป็นผู้แทนของฝ่ายระบบงานสารสนเทศ เป็นบริการข้อมูลด้านเทคนิค (Technical Data Steward) และเลขานุการ โดยมีอำนาจหน้าที่ดังต่อไปนี้

(ก) ปฏิบัติงานด้านธรรมาภิบาลข้อมูลให้เป็นไปตามนโยบายและแนวปฏิบัติสำหรับการบริหารจัดการข้อมูลที่คณะกรรมการธรรมาภิบาลข้อมูลให้ความเห็นชอบ

(ข) ให้ข้อมูลสนับสนุนแก่การพิจารณาของคณะกรรมการธรรมาภิบาลข้อมูล

(ค) เสนอแนะโจทย์จากเป้าหมายทางยุทธศาสตร์ แผนดำเนินงาน หรือความท้าทายของแต่ละหน่วยงาน เพื่อระบุชุดข้อมูลสำคัญในการดำเนินงาน

(ง) ดำเนินการตามกระบวนการบริหารจัดการข้อมูลให้เป็นไปตามที่กำหนดไว้ในระเบียบนี้

(4) “เจ้าของระบบ (System Owner)” ซึ่งเป็นหน่วยงานที่ขอให้มีและใช้งานระบบสารสนเทศ นอกจากจะมีหน้าที่และความรับผิดชอบตามที่กำหนดไว้ในระเบียบว่าด้วยนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศแล้ว เจ้าของระบบ (System Owner) ยังมีหน้าที่และความรับผิดชอบดังต่อไปนี้

(ก) ตรวจสอบและดูแลข้อมูล เพื่อสร้างความมั่นใจได้ว่าการบริหารจัดการข้อมูลสอดคล้องกับกฎหมาย ระเบียบ นโยบาย มาตรฐานและแนวปฏิบัติสำหรับการบริหารจัดการข้อมูลของกองทุน

(ข) ทบทวนและอนุมัติการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับข้อมูล เช่น การเปลี่ยนแปลงเมทาดาตา และเกณฑ์การทำดาตาคลีนซิง (Data Cleansing)

(ค) กำหนดสิทธิในการให้ผู้ปฏิบัติงานหรือบุคคลอื่นใดเข้าถึงข้อมูลและจัดชั้นความลับของข้อมูล

(5) “บริการข้อมูลด้านธุรกิจ (Business Data Steward)” ซึ่งเป็นผู้ปฏิบัติงานที่เป็นผู้แทนจากกลุ่มงานที่เป็นเจ้าของระบบ (System Owner) และเจ้าของข้อมูล (Data Owner) มีหน้าที่และความรับผิดชอบดังต่อไปนี้

(ก) นิยามความต้องการด้านคุณภาพของข้อมูล

(ข) นิยามคำอธิบายชุดข้อมูล (Data Set) และเมทาดาตา (Meta Data)

(ค) ตรวจสอบการปฏิบัติตามนโยบายและแนวปฏิบัติสำหรับการบริหารจัดการข้อมูล

(ง) ตรวจสอบและวิเคราะห์คุณภาพ รวมทั้งความมั่นคงปลอดภัยของข้อมูลและการปฏิบัติตามนโยบายและแนวปฏิบัติสำหรับการบริหารจัดการข้อมูล

(จ) ให้ความรู้และคำแนะนำแก่ผู้ปฏิบัติงานและหน่วยงานอื่นเพื่อให้เกิดความเข้าใจและสามารถใช้ประโยชน์จากข้อมูลได้โดยถูกต้องและเป็นไปตามกฎหมาย รวมทั้งนโยบายและแนวปฏิบัติสำหรับการบริหารจัดการข้อมูล

(ฉ) วิเคราะห์ผลการตรวจสอบจากผู้ตรวจสอบภายในหรือผู้ตรวจสอบภายนอก และรายงานผลการดำเนินการแก่ผู้บริหารข้อมูลระดับสูง (Chief Data Officer) เจ้าของข้อมูล (Data Owner) และผู้บริหารกลุ่มงานที่เกี่ยวข้อง

(6) “บริการข้อมูลด้านเทคนิค (Technical Data Steward)” ซึ่งเป็นผู้ปฏิบัติงานที่เป็นผู้แทนของฝ่ายระบบงานสารสนเทศที่ให้การสนับสนุนด้านเทคโนโลยีสารสนเทศแก่บริการข้อมูลด้านธุรกิจ (Business Data Steward) มีหน้าที่และความรับผิดชอบดังต่อไปนี้

(ก) นิยามเชิงเทคนิคและจัดทำเมทาดาตา (Meta Data)



(ข) ให้คำปรึกษาและข้อเสนอแนะเชิงเทคนิคในการจัดทำและแก้ไขปรับปรุงนโยบายและแนวปฏิบัติสำหรับการบริหารจัดการข้อมูล

(ค) ตรวจสอบคุณภาพ ความมั่นคงปลอดภัยของข้อมูล และการปฏิบัติตามนโยบายและแนวปฏิบัติสำหรับการบริหารจัดการข้อมูลในเชิงเทคนิค

(ง) ให้คำปรึกษาและข้อเสนอแนะในการพัฒนาเทคโนโลยีสารสนเทศสำหรับการบริหารจัดการข้อมูลเพื่อให้ข้อมูลมีคุณภาพ ถูกต้องครบถ้วน เป็นปัจจุบัน และพร้อมใช้งาน รวมทั้งมีความมั่นคงปลอดภัยเป็นไปตามมาตรฐานที่กำหนด

(จ) จัดทำนโยบายด้านคุณภาพของข้อมูล รวมทั้งการตรวจวัดและการวิเคราะห์คุณภาพข้อมูล เพื่อเสนอขอความเห็นชอบจากกลุ่มงานเทคโนโลยีสารสนเทศและคณะกรรมการธรรมาภิบาลข้อมูลตามลำดับ

หมวด 3 การสร้างข้อมูล

ข้อ 9 ให้เจ้าของข้อมูล (Data Owner) กำหนดหมวดหมู่ของข้อมูลสำหรับชุดข้อมูล (Data Set) เพื่อให้เกิดความเข้าใจ รวมทั้งสามารถกำหนดการเข้าถึงและใช้งานข้อมูลได้อย่างเหมาะสม เพื่อรักษาความเป็นส่วนตัวและความมั่นคงปลอดภัยของข้อมูล ตลอดจนสามารถจัดการข้อมูลในกระบวนการที่เกี่ยวข้องกับภารกิจของกองทุนได้อย่างมีประสิทธิภาพ

ข้อมูลสามารถแบ่งออกเป็น 5 ประเภท ดังต่อไปนี้

- (1) ข้อมูลสาธารณะ
- (2) ข้อมูลใช้ภายใน
- (3) ข้อมูลส่วนบุคคล
- (4) ข้อมูลความลับทางราชการ
- (5) ข้อมูลความมั่นคง

ข้อ 10 ให้เจ้าของข้อมูล (Data Owner) กำหนดให้มีการจัดระดับชั้นของข้อมูลดังต่อไปนี้

- (1) เปิดเผยภายในองค์กรหรือเปิดเผยสาธารณะ
- (2) เปิดเผยเมื่อได้รับอนุญาต ประกอบด้วย

(ก) “ลับ (Confidential)” หมายความว่า ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐในระดับบุคคลทั้งที่เป็นบุคคลธรรมดาและนิติบุคคล

(ข) “ลับมาก (Secret)” หมายความว่า ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรงในระดับองค์กรไม่ว่าจะเป็นส่วนราชการ รัฐวิสาหกิจ หน่วยงานอื่นของรัฐ หรือกองทุน ซึ่งอาจทำให้ไม่สามารถปฏิบัติหน้าที่ตามภารกิจให้บรรลุวัตถุประสงค์ที่กำหนดไว้ได้ หรืออาจส่งผลกระทบต่อความปลอดภัยของบุคคลสำคัญของชาติหรือต่างชาติ

(ค) “ลับที่สุด (Top Secret)” หมายความว่า ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรงที่สุดในระดับชาติ หรือส่งผลกระทบต่อความอยู่รอดปลอดภัยและความมั่นคงแห่งชาติ เช่น เอกราช อธิปไตย บุรณภาพแห่งดินแดน สถาบันหลักของชาติ เกียรติภูมิของประเทศ หรือผลประโยชน์แห่งชาติ



ข้อ 11 ผู้ปฏิบัติงานที่ได้รับสิทธิในการสร้างข้อมูลในระบบสารสนเทศจากเจ้าของระบบ (System Owner) จะต้องถือปฏิบัติดังต่อไปนี้

- (1) บันทึก แก้ไข ปรับปรุง หรือลบข้อมูลให้สอดคล้องกับโครงสร้างที่ถูกระบุไว้
- (2) ทำงานร่วมกับบริการข้อมูลด้านธุรกิจ (Business Data Steward) และบริการข้อมูลด้านเทคนิค (Technical Data Steward) เพื่อตรวจสอบและแก้ไขปัญหาด้านคุณภาพข้อมูลและความมั่นคงปลอดภัย
- (3) ไม่นำเข้าข้อมูลที่ขัดต่อกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ ไม่ว่าจะทั้งหมดหรือบางส่วน
- (4) ไม่ทำการสร้างหรือทำซ้ำต่อข้อมูลที่ขัดต่อกฎหมายว่าด้วยทรัพย์สินทางปัญญา

หมวด 4 การจัดเก็บข้อมูล

ข้อ 12 กลุ่มงานเทคโนโลยีสารสนเทศจะเป็นผู้รับผิดชอบในการพิจารณากำหนดนโยบายการจัดเก็บข้อมูลที่มีคุณภาพ โดยมีการกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลและกำหนดสภาพแวดล้อมของการจัดเก็บข้อมูลให้เป็นไปตามข้อกำหนดการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของกองทุนภายใต้หลักการดังต่อไปนี้

- (1) กำหนดคุณภาพของข้อมูล โดยคำนึงถึงความถูกต้องครบถ้วน เป็นปัจจุบัน และพร้อมใช้งานอยู่เสมอ
- (2) กำหนดชั้นความลับของข้อมูล และจัดเก็บให้สอดคล้องกับมาตรฐานการจัดชั้นความลับของข้อมูลที่กองทุนกำหนด
- (3) กำหนดสิทธิและควบคุมการเข้าถึงข้อมูลเฉพาะผู้ปฏิบัติงานที่เกี่ยวข้องและได้รับอนุญาตเท่านั้นที่จะมีสิทธิเข้าถึงข้อมูลได้ภายในระยะเวลาและขอบเขตการปฏิบัติงานที่กำหนด
- (4) กำหนดเครื่องมือที่ใช้ในการเข้าถึงข้อมูลเฉพาะที่เป็นของผู้ปฏิบัติงานที่เกี่ยวข้องและได้รับอนุญาตเท่านั้นที่จะมีสิทธิใช้ในการเข้าถึงข้อมูลได้ภายในระยะเวลาและขอบเขตการปฏิบัติงานที่กำหนด

ข้อ 13 ผู้ปฏิบัติงานที่มีหน้าที่รับผิดชอบการเก็บรวบรวมหรือใช้ข้อมูลเพื่อการปฏิบัติงานให้แก่กองทุนจะต้องถือปฏิบัติดังต่อไปนี้

- (1) จัดเก็บข้อมูลภายใต้สภาพแวดล้อมและการควบคุมตามที่กลุ่มงานเทคโนโลยีสารสนเทศกำหนด
- (2) จัดเก็บข้อมูลส่วนบุคคลหรือข้อมูลข่าวสารลับไว้ในสถานที่ปกปิดซึ่งบุคคลที่ไม่เกี่ยวข้องกับข้อมูลดังกล่าวไม่สามารถเข้าถึงได้
- (3) ใช้อุปกรณ์หรือระบบเทคโนโลยีสารสนเทศที่ได้รับอนุญาตในการเข้าถึงข้อมูลภายในระยะเวลาและขอบเขตการปฏิบัติงานที่กำหนด เพื่อป้องกันการสูญหายของข้อมูลหรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

หมวด 5 การใช้ข้อมูล

ข้อ 14 ผู้ปฏิบัติงานและหน่วยงานที่ทำการประมวลผลข้อมูลและใช้ข้อมูลเพื่อการวิเคราะห์จะต้อง

- (1) ปฏิบัติตามแนวปฏิบัติและมาตรฐานของการประมวลผลข้อมูล รวมทั้งการใช้ข้อมูลเพื่อการวิเคราะห์ตามที่กลุ่มงานเทคโนโลยีสารสนเทศกำหนด



(2) ดำเนินการให้เป็นไปโดยถูกต้องและมีประสิทธิภาพตรงตามวัตถุประสงค์และเงื่อนไขที่เจ้าของข้อมูลส่วนบุคคลได้ให้ความยินยอมในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไว้ เว้นแต่เป็นกรณีที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลกำหนดให้กระทำได้ รวมทั้งปฏิบัติตามนโยบายและแนวปฏิบัติสำหรับการบริหารจัดการข้อมูลที่คณะกรรมการธรรมาภิบาลข้อมูลให้ความเห็นชอบ

(3) บันทึกข้อมูลประวัติการดำเนินการไว้เพื่อประโยชน์ในการตรวจสอบด้วย

หมวด 6

การแลกเปลี่ยน เชื่อมโยง และเปิดเผยข้อมูล

ข้อ 15 ในการแลกเปลี่ยนและการเชื่อมโยงข้อมูลระหว่างหน่วยงานให้มีความมั่นคงปลอดภัยและมีประสิทธิภาพ ให้หน่วยงานที่เกี่ยวข้องถือปฏิบัติตามหลักการดังต่อไปนี้

(1) เป็นการแลกเปลี่ยนข้อมูลตามที่กำหนดในกฎหมายที่เกี่ยวข้อง หรือมีการจัดทำนิติกรรมสัญญา หรือจัดให้มีข้อตกลงที่ระบุข้อกำหนดเกี่ยวกับการแลกเปลี่ยนและการเชื่อมโยงข้อมูลระหว่างกัน รวมทั้งแนวปฏิบัติในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูล การจัดการเรื่องความมั่นคงปลอดภัย คุณภาพข้อมูล รวมทั้งผู้ประสานงานหรือผู้ติดต่ออย่างชัดเจน

(2) กำหนดกระบวนการแลกเปลี่ยนและการเชื่อมโยงข้อมูลระหว่างกันให้ชัดเจนตั้งแต่ขั้นตอนการเตรียมการ ขั้นตอนเริ่มดำเนินการ ขั้นตอนระหว่างดำเนินการ และขั้นตอนสิ้นสุดการดำเนินการ

(3) กำหนดเมทาดาทา (Meta Data) ของชุดข้อมูล (Data Set) ที่ต้องการแลกเปลี่ยนและเชื่อมโยงข้อมูล ที่จำเป็นให้ครบถ้วน

(4) กำหนดเทคโนโลยีและมาตรฐานทางเทคนิคที่จำเป็นในการแลกเปลี่ยนข้อมูลและเชื่อมโยงข้อมูล

(5) บันทึกรายละเอียดการแลกเปลี่ยนและเชื่อมโยงข้อมูลแต่ละครั้งเพื่อประโยชน์ในการตรวจสอบ

(6) ตรวจสอบว่าการแลกเปลี่ยนและเชื่อมโยงข้อมูลได้ดำเนินการตามกฎหมาย ระเบียบและแนวปฏิบัติในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูล การจัดการเรื่องความมั่นคงปลอดภัย และคุณภาพข้อมูลตามที่ได้กำหนดไว้ร่วมกัน

ข้อ 16 ให้หน่วยงานและผู้ปฏิบัติงานที่เกี่ยวข้องถือปฏิบัติในการเปิดเผยข้อมูลให้เป็นไปโดยถูกต้องตรงตามวัตถุประสงค์ของการนำข้อมูลไปใช้ประโยชน์ของเจ้าของข้อมูล ผู้ปฏิบัติงาน หรือหน่วยงานที่เกี่ยวข้องภายใต้หลักการดังต่อไปนี้

(1) ไม่เปิดเผยข้อมูลที่ขัดต่อกฎหมาย ระเบียบ และคำสั่งของกองทุน

(2) การเปิดเผยข้อมูลส่วนบุคคลต้องได้รับอนุญาตจากเจ้าของข้อมูลส่วนบุคคลก่อน เว้นแต่เป็นกรณีที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลกำหนดให้กระทำได้

(3) กำหนดกระบวนการเปิดเผยข้อมูลให้ชัดเจนตั้งแต่ขั้นตอนการเตรียมการ ขั้นตอนเริ่มดำเนินการ ขั้นตอนระหว่างดำเนินการ และขั้นตอนสิ้นสุดการดำเนินการ

(4) บันทึกรายละเอียดการเปิดเผยข้อมูลแต่ละครั้งเพื่อประโยชน์ในการตรวจสอบ

(5) ตรวจสอบว่าการเปิดเผยข้อมูลได้ดำเนินการโดยถูกต้องตามกฎหมาย ระเบียบ และแนวปฏิบัติที่กำหนดอย่างเหมาะสม



หมวด 7 การทำลายข้อมูล

ข้อ 17 ให้หน่วยงานที่เกี่ยวข้องการทำลายข้อมูลในกรณีดังต่อไปนี้

(1) เมื่อเจ้าของข้อมูลส่วนบุคคลร้องขอให้ทำลายข้อมูลส่วนบุคคลของตนหรือเมื่อพ้นกำหนดระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคลตามนโยบายการคุ้มครองข้อมูลส่วนบุคคลที่กองทุนกำหนด เว้นแต่มีความจำเป็นตามที่กฎหมายหรือนโยบายของกองทุนกำหนด

(2) เมื่อหน่วยงานที่เป็นเจ้าของข้อมูลร้องขอให้ทำลายข้อมูลที่จัดเก็บไว้โดยไม่มีการใช้ประโยชน์อีกต่อไป

(3) เมื่อบริการข้อมูลด้านเทคนิค (Technical Data Steward) แจ้งให้หน่วยงานที่เป็นเจ้าของข้อมูลทำลายข้อมูลที่จัดเก็บไว้เกินกว่าระยะเวลาที่กำหนด เว้นแต่หน่วยงานที่เป็นเจ้าของข้อมูลจะมีเหตุผลความจำเป็นในการจัดเก็บข้อมูลเกินกว่าระยะเวลาที่กำหนด แต่จะต้องทบทวนเหตุผลความจำเป็นดังกล่าวทุกปี

ข้อ 18 การทำลายข้อมูลจะต้องดำเนินการโดยเร็วและถูกต้องตามหลักเกณฑ์และวิธีการที่กำหนดโดยกฎหมาย รวมทั้งนโยบาย ระเบียบ และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของกองทุน รวมทั้งนโยบาย ระเบียบ และแนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคล และให้บริการข้อมูลด้านเทคนิค (Technical Data Steward) หรือฝ่ายงานที่เกี่ยวข้อง บันทึกประวัติการทำลายข้อมูลดังกล่าวไว้เพื่อประโยชน์ในการตรวจสอบด้วย

การทำลายข้อมูลอาจครอบคลุมถึงข้อมูลที่เป็นเอกสารต้นฉบับและสำเนาด้วย

ประกาศ ณ วันที่ ๕ กรกฎาคม พ.ศ. 2567

(นายทรงพล ชีวะปัญญาโรจน์)
เลขาธิการคณะกรรมการ กบข.