กสศ

ประกาศคณะกรรมการบริหารกองทุนเพื่อความเสมอภาคทางการศึกษา
เรื่อง นโยบายการบริหารจัดการข้อมูลและธรรมาภิบาลข้อมูล

ด้วยพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ กำหนดให้หน่วยงานของรัฐจัดให้มีการบริหารงานภาครัฐและการจัดทำบริการสาธารณะเป็นไปด้วยความสะดวก รวดเร็ว มีประสิทธิภาพ และตอบสนองต่อการให้บริการและการอำนวยความสะดวกแก่ประชาชน รวมทั้งกำหนดให้หน่วยงานของรัฐจัดให้มีการบริหารจัดการและการบูรณาการข้อมูลภาครัฐ และการทำงานให้มีความสอดคล้องกันและเชื่อมโยงเข้าด้วยกันอย่างมั่นคงปลอดภัยและมีธรรมาภิบาล

อาศัยอำนาจตามความในมาตรา ๒๓ (๑) แห่งพระราชบัญญัติกองทุนเพื่อความเสมอภาคทางการศึกษา พ.ศ. ๒๕๖๑ ประกอบมติคณะกรรมการบริหารกองทุนเพื่อความเสมอภาคทางการศึกษา ในการประชุมครั้งที่ ๓/๒๕๖๘ เมื่อวันที่ ๒๔ มีนาคม ๒๕๖๘ จึงออกประกาศดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศคณะกรรมการบริหารกองทุนเพื่อความเสมอภาคทางการศึกษา เรื่อง นโยบายการบริหารจัดการข้อมูลและธรรมาภิบาลข้อมูล”

ข้อ ๒ นโยบายการบริหารจัดการข้อมูลและธรรมาภิบาลข้อมูล เป็นไปตามแนบท้ายประกาศนี้

ประกาศ ณ วันที่ ๒๔ มีนาคม พ.ศ. ๒๕๖๘

(นายประสาร ไตรรัตน์วรกุล)
ประธานกรรมการบริหารกองทุนเพื่อความเสมอภาคทางการศึกษา

แนบท้ายประกาศคณะกรรมการบริหารกองทุนเพื่อความเสมอภาคทางการศึกษา
เรื่อง นโยบายการบริหารจัดการข้อมูลและธรรมาภิบาลข้อมูล ประกาศ ณ วันที่ ๒๔ มีนาคม ๒๕๖๘

นโยบายการบริหารจัดการข้อมูลและธรรมาภิบาลข้อมูล

กองทุนเพื่อความเสมอภาคทางการศึกษามีวัตถุประสงค์เพื่อสร้างความเสมอภาคทางการศึกษา รวมถึงการส่งเสริม สนับสนุน และให้ความช่วยเหลือแก่ผู้ขาดแคลนทุนทรัพย์และผู้ด้อยโอกาส ให้ได้รับการศึกษา ตลอดจนพัฒนาให้มีความรู้ความสามารถในการประกอบอาชีพตามความถนัด มีศักยภาพที่จะพึ่งพาตนเองในการดำรงชีวิตได้ และการศึกษา วิจัย การพัฒนาองค์ความรู้เพื่อลดความเหลื่อมล้ำในการศึกษา โดยในการดำเนินงานกองทุนเพื่อความเสมอภาคทางการศึกษาตระหนักถึงความสำคัญในการบริหารจัดการข้อมูลตามพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ ดังนั้น เพื่อให้สามารถเชื่อมโยงข้อมูลเข้าด้วยกันอย่างมั่นคงปลอดภัยและเพื่อการบูรณาการข้อมูลให้เป็นไปตามภารกิจของกองทุนเพื่อความเสมอภาคทางการศึกษาอย่างมีธรรมาภิบาล จึงกำหนดนโยบายการบริหารจัดการข้อมูลและธรรมาภิบาลข้อมูล ดังนี้

๑. วัตถุประสงค์

๑.๑ เพื่อให้การบริหารจัดการข้อมูลของกองทุนเพื่อความเสมอภาคทางการศึกษาสอดคล้องกับกฎหมาย กรอบธรรมาภิบาลข้อมูลภาครัฐ และระเบียบปฏิบัติที่เกี่ยวข้อง

๑.๒ เพื่อใช้เป็นกรอบและแนวทางในการบริหารจัดการข้อมูล สำหรับบุคลากรกองทุนเพื่อความเสมอภาคทางการศึกษา และผู้ที่เกี่ยวข้อง

๒. ขอบเขต

นโยบายฉบับนี้ครอบคลุมการดำเนินงานของกองทุนเพื่อความเสมอภาคทางการศึกษาในการบริหารจัดการข้อมูลตั้งแต่การสร้างข้อมูล การจัดเก็บข้อมูล การใช้ข้อมูล การเปิดเผยข้อมูล ตลอดจนการลบหรือทำลายข้อมูล และกำกับดูแลให้เป็นไปตามธรรมาภิบาลข้อมูลอย่างเหมาะสม มีประสิทธิภาพ มีคุณภาพ มีความมั่นคงปลอดภัย มีการเชื่อมโยง และสามารถดำเนินงานได้อย่างต่อเนื่องและยั่งยืน โดยคณะกรรมการ คณะอนุกรรมการ คณะทำงาน ผู้จัดการ ผู้ปฏิบัติงาน ตลอดจนผู้ซึ่งเกี่ยวข้องกับการดำเนินงานของกองทุนเพื่อความเสมอภาคทางการศึกษา มีหน้าที่สนับสนุนและให้ความร่วมมือในการปฏิบัติตามนโยบายนี้

๓. คำนิยาม

“กองทุน” หมายความว่า กองทุนเพื่อความเสมอภาคทางการศึกษา

“สำนักงาน” หมายความว่า สำนักงานกองทุน

“คณะกรรมการ” หมายความว่า คณะกรรมการบริหารกองทุน

“กรรมการ” หมายความว่า กรรมการในคณะกรรมการ

“คณะอนุกรรมการ” หมายความว่า คณะอนุกรรมการ คณะทำงาน ที่คณะกรรมการแต่งตั้ง และคณะกรรมการตรวจสอบภายในของกองทุน

“อนุกรรมการ” หมายความว่า อนุกรรมการในคณะอนุกรรมการ

“ผู้จัดการ” หมายความว่า ผู้จัดการกองทุน

“คณะกรรมการด้านธรรมาภิบาลข้อมูล (Data Governance Committee)” หมายความว่า คณะกรรมการด้านธรรมาภิบาลข้อมูลของกองทุน ที่ผู้จัดการแต่งตั้ง

“ผู้ปฏิบัติงาน” หมายความว่า บุคลากรของสำนักงานตามระเบียบว่าด้วยการบริหารงานบุคคลของกองทุน และให้หมายความรวมถึงบุคคลภายนอกที่สำนักงานว่าจ้างให้ปฏิบัติงานให้แก่สำนักงาน

“ศูนย์ข้อมูล” หมายความว่า หน่วยงานภายในของสำนักงานที่มีหน้าที่ความรับผิดชอบเกี่ยวกับการบริหารจัดการข้อมูลของกองทุน

“ข้อมูล (Data)” หมายความว่า สิ่งที่สื่อความหมายให้รู้เรื่องราวข้อเท็จจริงหรือเรื่องอื่นใด ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใด ๆ และไม่ว่าจะได้จัดทำไว้ในรูปของเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ภาพถ่ายดาวเทียม ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ เครื่องมือตรวจวัด การสำรวจระยะไกล หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้

“ชุดข้อมูล (Data set)” หมายความว่า การนำข้อมูลจากหลายแหล่งมารวบรวม เพื่อจัดเป็นชุดให้ตรงตามลักษณะโครงสร้างของข้อมูล

“บัญชีชุดข้อมูล (Data Catalog)” หมายความว่า เอกสารแสดงบรรดารายการของชุดข้อมูลที่จำแนกแยกแยะโดยการจัดกลุ่มหรือจัดประเภทข้อมูลที่อยู่ในความครอบครองหรือควบคุมของหน่วยงานของรัฐ

“เมทาดาตา (Metadata)” หมายความว่า ข้อมูลที่ใช้อธิบายข้อมูล โดยระบุรายละเอียดแหล่งข้อมูลและคำอธิบายรายละเอียดเกี่ยวกับข้อมูล

“ผู้เกี่ยวข้อง” หมายความว่า บุคคล นิติบุคคล คณะบุคคล ที่เกี่ยวข้องกับการดำเนินงานด้านข้อมูลของกองทุน

“ทีมบริกรข้อมูล” หมายความว่า กลุ่มผู้ปฏิบัติงานซึ่งได้รับมอบหมายให้ดำเนินงานด้านธรรมาภิบาลข้อมูล

“ผู้ดูแลระบบ” หมายความว่า กองทุน หรือผู้ซึ่งได้รับมอบหมายหรือว่าจ้างจากกองทุน ให้ทำหน้าที่หรือรับผิดชอบในการพัฒนา การดูแลรักษา หรือจัดการระบบสารสนเทศของกองทุน โดยกองทุนเป็นผู้กำกับดูแล ผู้ซึ่งได้รับมอบหมายหรือว่าจ้างดังกล่าว เช่น สำนักเทคโนโลยีสารสนเทศ ส่วนงานหรือหน่วยงานภายในส่วนงาน ผู้รับจ้าง ภาคีร่วมดำเนิน

“ผู้สร้างข้อมูล (Data Creator)” หมายความว่า ผู้ซึ่งบันทึก แก้ไข ปรับปรุง หรือลบข้อมูลให้สอดคล้องกับโครงสร้างที่ถูกกำหนดไว้ โดยทำงานร่วมกับทีมบริกรข้อมูล เพื่อตรวจสอบและแก้ไขปัญหาด้านคุณภาพข้อมูลและความปลอดภัยของข้อมูล รวมทั้งผู้ซึ่งส่งข้อมูลเข้าระบบสารสนเทศโดยตรงด้วย

“ผู้ใช้ข้อมูล (Data User)” หมายความว่า ผู้ซึ่งนำข้อมูลไปใช้งานทั้งในระดับปฏิบัติงานและระดับบริหาร โดยอาจเป็นหน่วยงานเจ้าของข้อมูล หรือเป็นผู้นำข้อมูลตนเองไปใช้ รวมถึงบุคคลภายนอกซึ่งได้รับอนุญาตจากสำนักงาน โดยมีหน้าที่สนับสนุนธรรมาภิบาลข้อมูล ตลอดจนรายงานประเด็นปัญหาที่พบระหว่างการใช้ข้อมูลทั้งด้านคุณภาพและความปลอดภัยของข้อมูล

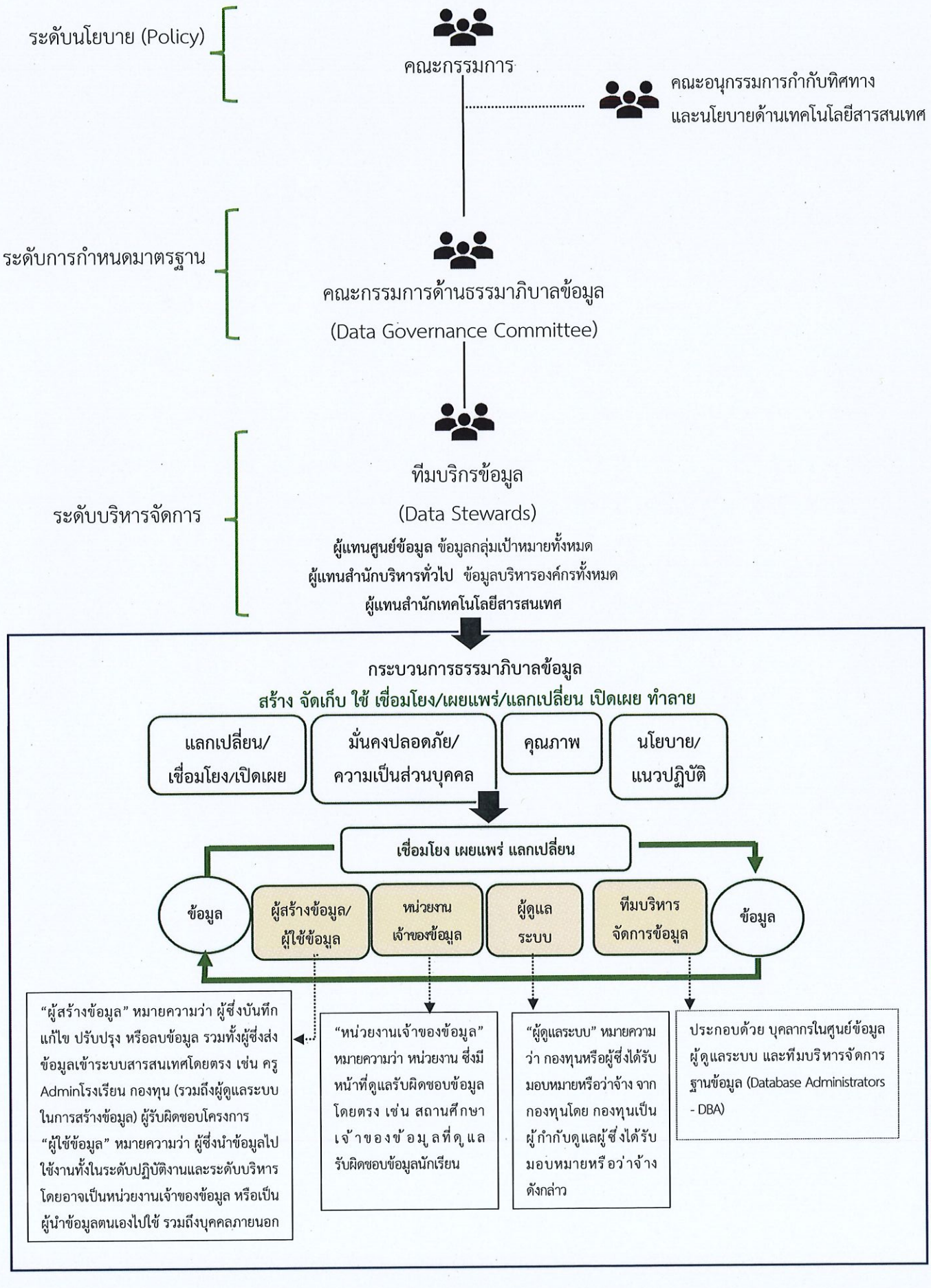
“เจ้าของข้อมูลส่วนบุคคล (Data Subject)” หมายความว่า เจ้าของข้อมูลส่วนบุคคลตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

“หน่วยงานเจ้าของข้อมูล (Data Owner)” หมายความว่า หน่วยงาน ซึ่งมีหน้าที่ดูแลรับผิดชอบข้อมูลโดยตรง เช่น สำนักบริหารกลยุทธ์งบประมาณและเงินกองทุน เป็นหน่วยงานเจ้าของข้อมูลเกี่ยวกับงบประมาณ ฝ่ายทรัพยากรบุคคล เป็นหน่วยงานเจ้าของข้อมูลบุคลากร โดยมีหน้าที่ทบทวนและอนุมัติการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับข้อมูล เช่น การเปลี่ยนแปลงเมทาดาตาและเกณฑ์การทำข้อมูลให้ถูกต้องสมบูรณ์ (Data Cleansing) การให้สิทธิในการเข้าถึงข้อมูลที่ตนเป็นเจ้าของ การจัดระดับชั้นข้อมูล

“ทีมบริหารจัดการข้อมูล (Data Management)” หมายความว่า บุคลากรในศูนย์ข้อมูลและผู้ดูแลระบบ ซึ่งมีหน้าที่หลักในการบริหารจัดการข้อมูลให้สอดคล้องกับองค์ประกอบของการบริหารจัดการข้อมูล ๑๐ ข้อ ได้แก่ สถาปัตยกรรมข้อมูล การจำลองและการออกแบบข้อมูล การจัดเก็บและการดำเนินการกับข้อมูลการบูรณาการและความสามารถในการทำงานร่วมกัน การบริหารจัดการเอกสารและเนื้อหา ข้อมูลหลักและข้อมูลอ้างอิง คำอธิบายชุดข้อมูลดิจิทัล หรือเมทาดาตา ความมั่นคงปลอดภัยและการรักษาความเป็นส่วนบุคคลของข้อมูล คุณภาพของข้อมูล รวมทั้งมีหน้าที่ในการตรวจสอบการปฏิบัติตามนโยบายข้อมูล สนับสนุนกิจกรรมของธรรมาภิบาลข้อมูล เช่น ช่วยเหลือทีมบริกรข้อมูลในการนิยามเมทาดาตา ช่วยเหลือทีมบริกรข้อมูลในการร่างนโยบายข้อมูลและมาตรฐานข้อมูล รวมทั้งกำหนดสิทธิการเข้าถึงข้อมูลโดยทีมบริหารจัดการฐานข้อมูล (Database Administrators - DBA)

“ผู้ทำลายข้อมูล” หมายความว่า บุคลากรที่ได้รับการกำหนดสิทธิจากหน่วยงานเจ้าของข้อมูลให้มีสิทธิในการทำลายข้อมูล

๔. โครงสร้างการบริหารจัดการข้อมูลและธรรมาภิบาลข้อมูล



ตารางคำอธิบายโครงสร้างการบริหารจัดการข้อมูลและธรรมาภิบาลข้อมูล

ตำแหน่ง/ชื่อ	บทบาท	หน้าที่และอำนาจ
ระดับนโยบาย (Policy)		
คณะกรรมการ	๑. กำหนดกลยุทธ์ด้านธรรมาภิบาลข้อมูล ๒. กำกับดูแลด้านธรรมาภิบาลข้อมูลของสำนักงาน	๑. กำหนดกลยุทธ์ด้านธรรมาภิบาลข้อมูล (Data Governance Strategy) ๒. กำหนดนโยบายการบริหารจัดการข้อมูลและธรรมาภิบาลข้อมูล
คณะอนุกรรมการกำกับทิศทางและนโยบายด้านเทคโนโลยีสารสนเทศและผู้จัดการ		ให้ข้อเสนอแนะต่อร่างนโยบายการบริหารจัดการข้อมูลและธรรมาภิบาลข้อมูล ก่อนเสนอคณะกรรมการ
		จัดลำดับความสำคัญของภารกิจและการดำเนินงาน (use case)
ระดับการกำหนดมาตรฐาน		
คณะกรรมการด้านธรรมาภิบาลข้อมูล (Data Governance Committee)	กำหนดกรอบมาตรฐานในการบริหารจัดการข้อมูล	๑. คัดเลือกระบบงานหรือข้อมูลชุดที่มีความสำคัญเพื่อนำมาจัดทำบัญชีข้อมูล (Data Catalog) (Catalog ตามภารกิจและการดำเนินงาน (use case)) ตามแนวทางการจัดทำบัญชีข้อมูลภาครัฐ และแนวทางการลงทะเบียนบัญชีข้อมูลภาครัฐที่สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.) กำหนด ๒. กำหนดผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องชุดข้อมูลที่สำคัญ เช่น หน่วยงานเจ้าของข้อมูล ๓. กำหนดกรอบมาตรฐานในการบริหารจัดการตามองค์ประกอบของการบริหารจัดการข้อมูล เพื่อให้จำแนกหมวดหมู่และชั้นความลับของข้อมูล รวมทั้งจัดทำคำอธิบายข้อมูล (Metadata) ได้ รวมทั้งกำหนดมาตรฐานของธรรมาภิบาลข้อมูลตามภารกิจและการดำเนินงาน (use case) ๔. ดำเนินการร่วมกับทีมบริกรข้อมูล เพื่อตรวจสอบและแก้ไขปัญหาด้านคุณภาพข้อมูลและความมั่นคงปลอดภัยของข้อมูล ๕. มีหน้าที่ในการทบทวนและอนุมัติผลที่ได้รับจากการปฏิบัติงาน

ตำแหน่ง/ชื่อ	บทบาท	หน้าที่และอำนาจ
ระดับบริหารจัดการ (Operation)		
ทีมบริกรข้อมูล (Data Steward) ประกอบด้วย ๑. ผู้แทนสำนักผู้จัดการ (ข้อมูลกลุ่มเป้าหมายทั้งหมด) ๒. ผู้แทนสำนักบริหารทั่วไป (ข้อมูลการดำเนินงานทั้งหมด) ๓. ผู้แทนสำนักเทคโนโลยีสารสนเทศ รวมถึงผู้สร้างข้อมูล ผู้ใช้ข้อมูลหน่วยงานเจ้าของข้อมูล ผู้ดูแลระบบ ทีมบริหารจัดการข้อมูล	ดำเนินงานให้ข้อมูลได้ตามมาตรฐานที่กำหนด	๑. ดำเนินงานให้ข้อมูลได้ตามมาตรฐานที่กำหนดเพื่อนำไปดำเนินการตามภารกิจ (use case) ๒. ให้ข้อมูลสนับสนุนในการตัดสินใจต่อคณะกรรมการด้านธรรมาภิบาลข้อมูล ๓. ดำเนินงานเกี่ยวกับด้านข้อมูลของกองทุน เช่น ๓.๑ ร่างนโยบายข้อมูล มาตรฐาน และแนวปฏิบัติต่าง ๆ ที่เกี่ยวข้องกับข้อมูล ด้วยการช่วยเหลือจากทีมบริหารจัดการข้อมูล เพื่อเสนอต่อคณะกรรมการด้านธรรมาภิบาลข้อมูล ๓.๒ ตรวจสอบการปฏิบัติตามนโยบายข้อมูล ตรวจสอบคุณภาพตรวจสอบความมั่นคงปลอดภัยของข้อมูล วิเคราะห์ผลจากการตรวจสอบแล้วรายงานผลไปยังคณะกรรมการด้านธรรมาภิบาลข้อมูล ๓.๓ สนับสนุนด้านเทคโนโลยีสารสนเทศตลอดจนรักษาและดูแลข้อมูลที่อยู่บนระบบเทคโนโลยีสารสนเทศต่าง ๆ ๓.๔ ดำเนินการในเรื่องคุณภาพข้อมูล เช่น กำหนดนโยบายข้อมูลด้านคุณภาพ การตรวจวัดคุณภาพข้อมูล และการวิเคราะห์คุณภาพข้อมูล ๔. ดำเนินการอื่น ๆ ตามที่คณะกรรมการด้านธรรมาภิบาลข้อมูลกำหนด

ตำแหน่ง/ชื่อ	บทบาท	หน้าที่และอำนาจ

ความสัมพันธ์ระหว่างกระบวนการ/กิจกรรมกับผู้มีส่วนได้เสียกับข้อมูล

กระบวนการ/กิจกรรม	คณะกรรมการ	คณะอนุกรรมการกำกับทิศทางฯ	คกก. ธรรมาภิบาลข้อมูล	ทีมบริกรข้อมูล				เจ้าของข้อมูลส่วนบุคคล
				หน่วยงานเจ้าของข้อมูล	ทีมบริหารจัดการข้อมูล	ผู้สร้างและผู้ใช้งาน	ผู้ดูแลระบบ	
กำหนดและปรับปรุงนโยบายและมาตรฐานข้อมูล	A	C	C	S	R	S	S	-
ตรวจสอบการปฏิบัติตามนโยบาย	I	I	A	S	R	S	S	-
การประเมินความพร้อมของธรรมาภิบาลข้อมูลภาครัฐ	I	I	R	S	R	S	S	-
ประเมินความมั่นคงปลอดภัยและคุณภาพข้อมูล	I	I	I	S	R	S	R	-
รายงานผลการตรวจสอบความมั่นคงปลอดภัย และคุณภาพข้อมูล	I	I	I	I	R	I	R	-
กำหนดสิทธิในการเข้าถึงข้อมูล	I	I	I	A	R	I	S	-
ขอแก้ไขข้อมูลส่วนบุคคลเฉพาะระบบที่เปิดสิทธิให้มีการร้องขอแก้ไข	I	I	I	S	I	I	S	R

หมายเหตุ

R (Responsible) หมายถึง ผู้มีหน้าที่ในการปฏิบัติงานตามกระบวนการหรือกิจกรรมที่กำหนดไว้

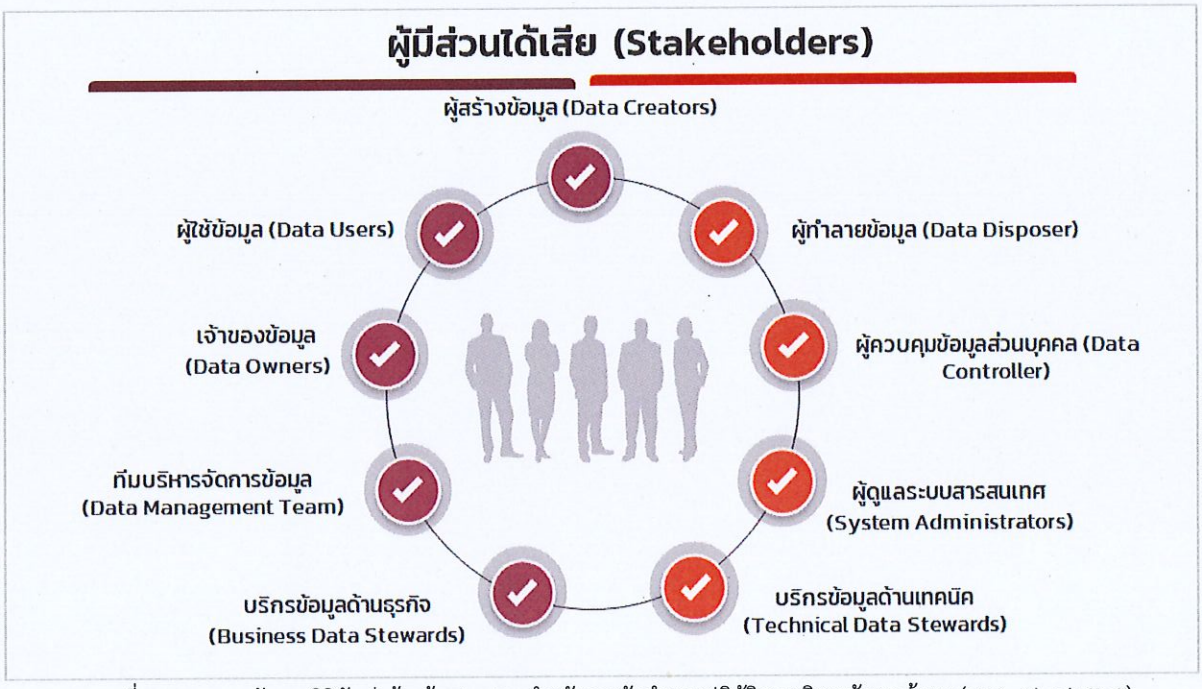
A (Accountable) หมายถึง ผู้มีหน้าที่ในการทบทวนและอนุมัติผลที่ได้รับจากปฏิบัติงาน

S (Supportive) หมายถึง ผู้ที่มีหน้าที่ในการสนับสนุนหรือให้การช่วยเหลือต่อผู้ปฏิบัติงาน

C (Consulted) หมายถึง ผู้ที่ทำหน้าที่ให้คำปรึกษาต่อผู้ปฏิบัติงาน

I (Informed) หมายถึง ผู้ที่ทำหน้าที่รับทราบผลการปฏิบัติงาน

ที่มา: ประกาศธรรมาภิบาลข้อมูลภาครัฐ



ที่มา: มาตรฐานรัฐบาลดิจิทัล ว่าด้วยข้อเสนอแนะสำหรับการจัดทำแนวปฏิบัติการบริหารจัดการข้อมูล (มรด. ๔-๒ : ๒๕๖๕) สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

ตารางความสัมพันธ์ตามวงจรชีวิตข้อมูลกับผู้มีส่วนได้เสีย (Stakeholders)

วงจรชีวิตข้อมูล	ผู้เกี่ยวข้อง	ข้อปฏิบัติ
๑. การสร้างข้อมูล	๑. ทีมบริกรข้อมูล ได้แก่ ๑.๑ ผู้สร้างข้อมูล ๑.๒ ทีมบริหารจัดการข้อมูล ๑.๓ หน่วยงานเจ้าของข้อมูล ๑.๔ ผู้ดูแลระบบ	๑. หน่วยงานเจ้าของข้อมูล กำหนดหมวดหมู่ สิทธิ และชั้นความลับของข้อมูล ๒. ผู้ดูแลระบบจะต้องกำหนดสิทธิในระบบให้แก่ผู้สร้างข้อมูลตามที่หน่วยงานเจ้าของข้อมูลกำหนด ๓. หน่วยงานเจ้าของข้อมูล ทีมบริกรข้อมูล และทีมบริหารจัดการข้อมูล ร่วมจัดทำคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตา (Metadata) ตามมาตรฐานขั้นต่ำคำอธิบายชุดข้อมูลดิจิทัลที่สำนักงานพัฒนารัฐบาลดิจิทัล (สพร.) กำหนด และกำหนดให้ทำการประเมินคุณค่าของชุดข้อมูลดิจิทัลตามแบบฟอร์มประเมินคุณค่าชุดข้อมูลที่ สพร. หรือหน่วยงานกำหนด เพื่อสนับสนุนการคัดเลือกเป็นชุดข้อมูลคุณค่าสูง (High Value Dataset) และเผยแพร่เป็นข้อมูลเปิดของหน่วยงานต่อสาธารณะตามกฎหมายว่าด้วยข้อมูลข่าวสารของราชการในรูปแบบข้อมูลดิจิทัล ๔. ห้ามมิให้ผู้สร้างข้อมูลนำข้อมูลที่มีลักษณะดังต่อไปนี้เข้าสู่ระบบคอมพิวเตอร์ ๔.๑ ข้อมูลที่บิดเบือน หรือปลอมไม่ว่าทั้งหมดหรือบางส่วน ๔.๒ ข้อมูลอันเป็นเท็จ ที่น่าจะเกิดความเสียหายต่อการรักษาความมั่นคงปลอดภัย ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจ หรือ โครงสร้างพื้นฐาน หรือ ก่อให้เกิดความตื่นตระหนก ๔.๓ ข้อมูลอันเป็นความผิดเกี่ยวกับความมั่นคง หรือ ความผิดเกี่ยวกับการก่อการร้าย ๔.๔ ข้อมูลที่มีลักษณะอันลามก และคนทั่วไปอาจเข้าถึงได้ ๔.๕ ข้อมูลที่ปรากฏภาพของผู้อื่น และเป็นภาพที่สร้างขึ้น ตัดต่อเติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ ทำให้ผู้อื่นเสียชื่อเสียง ถูกดูหมิ่นถูกเกลียดชัง หรือ ได้รับความอับอาย ๕. ผู้สร้างข้อมูลสร้างข้อมูลที่มาจากแหล่งข้อมูลที่เชื่อถือได้เท่านั้น ๖. หน่วยงานเจ้าของข้อมูลตรวจสอบความถูกต้องของข้อมูลที่ถูกสร้างขึ้น ๗. การสร้างข้อมูล เป็นการสร้างข้อมูลขึ้นมาใหม่ โดยวิธีการบันทึกเข้าไปด้วยบุคคล หรือบันทึกอัตโนมัติด้วยอุปกรณ์อิเล็กทรอนิกส์ เช่น อุปกรณ์ตรวจจับสัญญาณ (Sensor) รวมถึงการซื้อข้อมูล หรือการรับข้อมูลจากหน่วยงานอื่น เพื่อนำมาจัดเก็บในภายหลัง

<table>
<tr><th>วงจรชีวิตข้อมูล</th><th>ผู้เกี่ยวข้อง</th><th>ข้อปฏิบัติ</th></tr>
<tr><td colspan="3">

ผู้มีส่วนได้ส่วนเสียในการสร้างข้อมูล

<table>
<tr><th rowspan="3">กิจกรรมตามวงจรชีวิตข้อมูล
(การสร้าง การจัดเก็บ การใช้ การเปิดเผย การลบหรือทำลาย)</th><th colspan="4">ผู้มีส่วนได้ส่วนเสีย</th></tr>
<tr><th colspan="4">ทีมบริกรข้อมูล</th></tr>
<tr><th>ผู้สร้างข้อมูล</th><th>ทีมบริหารจัดการข้อมูล</th><th>หน่วยงานเจ้าของข้อมูล</th><th>ผู้ดูแลระบบ</th></tr>
<tr><td>กำหนดผู้มีสิทธิในการสร้างข้อมูล และกำหนดหมวดหมู่และชั้นความลับ</td><td>I</td><td>I</td><td>A</td><td>S</td></tr>
<tr><td>กำหนดสิทธิในการสร้างข้อมูลในระบบให้แก่ผู้สร้างข้อมูล</td><td>I</td><td>I</td><td>A</td><td>R</td></tr>
<tr><td>สร้างข้อมูลที่ไม่ขัดต่อกฎหมายและจากแหล่งข้อมูลที่เชื่อถือได้</td><td>R</td><td>I</td><td>C</td><td>S</td></tr>
<tr><td>จัดทำคำอธิบายชุดข้อมูลดิจิทัล</td><td>R</td><td>S</td><td>A</td><td>S</td></tr>
<tr><td>ประเมินคุณค่าของชุดข้อมูลดิจิทัล</td><td>I</td><td>I</td><td>R</td><td>I</td></tr>
<tr><td>ตรวจสอบความถูกต้องของข้อมูล</td><td>I</td><td>I</td><td>A</td><td>I</td></tr>
</table>

หมายเหตุ

R (Responsible) หมายถึง ผู้มีหน้าที่ในการปฏิบัติงานตามกระบวนการหรือกิจกรรมที่กำหนดไว้

A (Accountable) หมายถึง ผู้มีหน้าที่ในการทบทวนและอนุมัติผลที่ได้รับจากปฏิบัติงาน

S (Supportive) หมายถึง ผู้ที่มีหน้าที่ในการสนับสนุนหรือให้การช่วยเหลือต่อปฏิบัติงาน

C (Consulted) หมายถึง ผู้ที่ทำหน้าที่ให้คำปรึกษาต่อผู้ปฏิบัติงาน

I (Informed) หมายถึง ผู้ที่ทำหน้าที่รับทราบผลการปฏิบัติงาน

</td></tr>
<tr><td>๒. การจัดเก็บข้อมูล</td><td>๑. ทีมบริกรข้อมูล ได้แก่
๑.๑ หน่วยงานเจ้าของข้อมูล
๑.๒ ผู้ดูแลระบบ
๑.๓ ผู้สร้างข้อมูล
๑.๔ ผู้ใช้ข้อมูล
๑.๕ ทีมบริหารจัดการข้อมูล</td><td>๑. หน่วยงานเจ้าของข้อมูลต้องจำแนกหมวดหมู่ข้อมูลและกำหนดชั้นความลับของข้อมูล พร้อมกำหนดระยะเวลาในการจัดเก็บข้อมูลที่ชัดเจน ตามแนวทางการจำแนกหมวดหมู่ข้อมูลและชั้นความลับข้อมูลของสำนักงาน
๒. ทีมบริกรข้อมูลและผู้ดูแลระบบ ทำการย้ายข้อมูลที่มีการจัดเก็บเกินระยะเวลาที่กำหนดแล้วเพื่อจัดเก็บเป็นข้อมูลถาวร
๓. การจัดเก็บชุดข้อมูลจะต้องมีคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตา หากไม่มีหรือไม่ครบถ้วน ทีมบริหารจัดการข้อมูลจะต้องแจ้งผู้รับผิดชอบ ได้แก่ หน่วยงานเจ้าของข้อมูล ทีมบริกรข้อมูล โดยทีมบริหารจัดการข้อมูลร่วมกันจัดทำและปรับปรุงให้เป็นปัจจุบัน
๔. ผู้มีส่วนได้ส่วนเสียเกี่ยวข้องกับข้อมูล ทั้งหน่วยงานเจ้าของข้อมูล ผู้สร้างข้อมูล ผู้ใช้ข้อมูล และทีมบริหารจัดการข้อมูล จะต้องจัดเก็บข้อมูลตามการจัดชั้นความลับของสำนักงาน โดยทำการเข้ารหัสข้อมูลเพื่อป้องกันการเข้าถึงหรือแก้ไขข้อมูลโดยไม่ได้รับอนุญาต ทั้งนี้การเข้ารหัสข้อมูลให้ปฏิบัติตามวิธีการเข้ารหัสข้อมูลตามนโยบายหรือหลักเกณฑ์ที่สำนักงานกำหนด และสอดคล้องกับหลักเกณฑ์หรือกฎหมายที่เกี่ยวข้อง</td></tr>
</table>

วงจรชีวิตข้อมูล	ผู้เกี่ยวข้อง	ข้อปฏิบัติ
		๔.๑.๑ ในกรณีที่ในตารางฐานข้อมูลเดียวกันมีฟิลด์ข้อมูลที่มีชั้นความลับและไม่มีชั้นความลับอยู่ร่วมกันให้ทำการเข้ารหัสข้อมูลเฉพาะฟิลด์ข้อมูลที่มีชั้นความลับเท่านั้น ๔.๑.๒ ในกรณีข้อมูลที่จัดเก็บในรูปแบบเอกสาร ให้มีการจัดเก็บดังนี้ (๑) เก็บในสถานที่เหมาะสม สามารถปิดล็อกได้เมื่อไม่ใช้งาน (๒) เก็บแยกออกจากอุปกรณ์ประมวลผลต่าง ๆ เช่น เครื่องพิมพ์ เครื่องถ่ายเอกสาร เป็นต้น โดยทันที เพื่อเป็นการป้องกันไม่ให้ผู้ไม่มีสิทธิในการเข้าถึงข้อมูล เข้าถึงข้อมูลได้ ๕. ทีมบริกรข้อมูลและผู้ดูแลระบบกำหนดให้มีวิธีปฏิบัติการกู้คืนข้อมูลที่จัดเก็บถาวร สำหรับข้อมูลที่มีความสำคัญมากต่อการดำเนินงานของสำนักงาน เพื่อสอบทานความถูกต้อง ครบถ้วน ความพร้อมใช้งาน คุณภาพข้อมูล ๖. ในกรณีที่มีการประชุมออนไลน์ กำหนดให้มีการจัดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่า ๙๐ วัน นับแต่วันที่ข้อมูลเข้าสู่ระบบคอมพิวเตอร์ โดยจัดเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการนับแต่เริ่มใช้บริการ ให้สอดคล้องตามกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ และในการจัดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ให้สอดคล้องตามกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ จะต้องใช้วิธีการที่มั่นคงปลอดภัยอย่างน้อย ดังนี้ ๖.๑ เก็บลงในสื่อที่รักษาความครบถ้วนถูกต้องแท้จริง (Integrity) และระบุตัวตน (Identification) ที่เข้าถึงสื่อได้ ๖.๒ มีการรักษาความลับของข้อมูล และกำหนดชั้นความลับในการเข้าถึงและจัดเก็บข้อมูล เพื่อรักษาความน่าเชื่อถือของข้อมูล และไม่อนุญาตให้ผู้ดูแลระบบแก้ไขข้อมูลที่จัดเก็บไว้ได้ ๖.๓ การจัดเก็บข้อมูลระบุรายละเอียดผู้ใช้บริการเป็นรายบุคคลได้ เช่น Proxy Server NAT และอื่น ๆ ๗. ทีมบริกรข้อมูลและผู้ดูแลระบบกำหนดให้มีมาตรการรักษาความปลอดภัยในการจัดเก็บข้อมูล รวมทั้งกรณีที่มีการเคลื่อนย้ายอุปกรณ์ที่จัดเก็บข้อมูล เพื่อป้องกันมิให้มีการเข้าถึงโดยมิได้รับอนุญาต หรือลักลอบนำข้อมูลไปใช้ที่ก่อให้เกิดความเสียหายต่อสำนักงาน

วงจรชีวิตข้อมูล	ผู้เกี่ยวข้อง	ข้อปฏิบัติ
		๘. ทีมบริกรข้อมูลและผู้ดูแลระบบ กำหนดมาตรการรักษาความปลอดภัยของข้อมูลที่จัดเก็บถาวรเพื่อป้องกันข้อมูลไม่ให้มีการลบ ปรับปรุง แก้ไขได้ รวมทั้งป้องกันมิให้ข้อมูลที่จัดเก็บถาวรรั่วไหลไปยังบุคคลที่ไม่ได้รับอนุญาต ๙. ทีมบริกรข้อมูล ทีมบริหารจัดการข้อมูล และผู้ดูแลระบบ กำหนดให้มีมาตรการรักษาความปลอดภัยของการถ่ายโอนข้อมูลกับหน่วยงานภายนอกที่ผ่านช่องทางการสื่อสารทุกชนิด โดยต้องสอดคล้องตามนโยบายความมั่นคงปลอดภัยสารสนเทศ ๑๐. ห้ามมิให้ผู้ปฏิบัติและผู้เกี่ยวข้องจัดเก็บข้อมูลส่วนตัวหรือข้อมูลที่ไม่เกี่ยวข้องกับการดำเนินงานของสำนักงาน สำหรับการจัดเก็บข้อมูลถาวรบนเครื่องแม่ข่ายที่สำนักงานจัดสรรไว้ ๑๑. ทีมบริกรข้อมูลกำหนดให้มีการทบทวนเกี่ยวกับช่วงระยะเวลาการจัดเก็บข้อมูล มาตรการ และวิธีปฏิบัติที่เกี่ยวข้องกับการจัดเก็บข้อมูลถาวร อย่างสม่ำเสมอ หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ

ผู้มีส่วนได้ส่วนเสียในการจัดเก็บข้อมูล

กิจกรรมตามวงจรชีวิตข้อมูล (การสร้าง การจัดเก็บ การใช้ การเปิดเผย การลบหรือทำลาย)	ผู้มีส่วนได้ส่วนเสีย				
	ทีมบริกรข้อมูล				
	หน่วยงานเจ้าของข้อมูล	ผู้ดูแลระบบ	ผู้สร้างข้อมูล	ผู้ใช้ข้อมูล	ทีมบริหารจัดการข้อมูล
กำหนดระยะเวลาในการจัดเก็บข้อมูล	A	S	S	I	S
ย้ายข้อมูลที่มีการจัดเก็บเกินระยะเวลาที่กำหนด	I	R	I	I	R
จัดทำคำอธิบายชุดข้อมูลดิจิทัลและปรับปรุงให้เป็นปัจจุบัน	R	S	S	I	R
จัดเก็บข้อมูลตามการจัดชั้นความลับของหน่วยงาน	R	S	R	I	C/S
จัดเก็บข้อมูลส่วนบุคคลเท่าที่จำเป็น	R	R/S	S	R	C/S
ยกเลิกการจัดเก็บข้อมูลส่วนบุคคลกรณีเจ้าของข้อมูลส่วนบุคคลถอนความยินยอม	R	R	I	R	I
จัดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์	I	R	I	I	I
ตรวจสอบให้มั่นใจว่าสภาพแวดล้อมการจัดเก็บข้อมูลมีคุณภาพและความปลอดภัย	I	R	I	I	A

หมายเหตุ R = Responsible A = Accountable S = Supportive C = Consulted และ I = Informed

<table>
<tr><th>วงจรชีวิตข้อมูล</th><th>ผู้เกี่ยวข้อง</th><th>ข้อปฏิบัติ</th></tr>
<tr><td>๓. การใช้ข้อมูล</td><td>๑. ทีมบริกรข้อมูล ได้แก่
๑.๑ หน่วยงานเจ้าของข้อมูล
๑.๒ ผู้ใช้ข้อมูล
๑.๓ ผู้ดูแลระบบ</td><td>๑. หน่วยงานเจ้าของข้อมูลจะต้องกำหนดผู้มีสิทธิเข้าถึงเพื่อประมวลผลและใช้ข้อมูลตามชั้นความลับตามแนวทางการจำแนกหมวดหมู่ข้อมูลและชั้นความลับข้อมูลของสำนักงาน
๒. ผู้ดูแลระบบจะต้องกำหนดสิทธิในการเข้าถึงข้อมูลในระบบเพื่อประมวลผลและใช้ข้อมูลของผู้ใช้งานตามที่หน่วยงานเจ้าของข้อมูลกำหนด
๓. หน่วยงานเจ้าของข้อมูลจะต้องทบทวนสิทธิการเข้าถึงเพื่อประมวลผลและใช้ข้อมูลของผู้ใช้งานอย่างสม่ำเสมอ หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ เช่น การลาออก เปลี่ยนตำแหน่ง โอนย้าย สิ้นสุดการจ้างการปรับโครงสร้าง สิ้นสุดสัญญา หรือเมื่อมีการปรับปรุงระบบสารสนเทศ
๔. ผู้ใช้ข้อมูลที่มีชั้นความลับจะต้องใช้ข้อมูลอย่างระมัดระวัง โดยคำนึงถึงความปลอดภัยและความเป็นส่วนตัวของข้อมูล และต้องไม่ใช้งานข้อมูลที่มีชั้นความลับในเครือข่ายสาธารณะ</td></tr>
<tr><td colspan="3">ผู้มีส่วนได้ส่วนเสียในการใช้ข้อมูล
<table>
<tr><th rowspan="3">กิจกรรมตามวงจรชีวิตข้อมูล
(การสร้าง การจัดเก็บ การใช้ การเปิดเผย การลบหรือทำลาย)</th><th colspan="3">ผู้มีส่วนได้ส่วนเสีย</th></tr>
<tr><th colspan="3">ทีมบริกรข้อมูล</th></tr>
<tr><th>หน่วยงานเจ้าของข้อมูล</th><th>ผู้ใช้ข้อมูล</th><th>ผู้ดูแลระบบ</th></tr>
<tr><td>กำหนดสิทธิในการใช้งานข้อมูลตามชั้นความลับ</td><td>A</td><td>I</td><td>I</td></tr>
<tr><td>กำหนดสิทธิในการเข้าใช้งานข้อมูลในระบบ</td><td>A</td><td>I</td><td>R</td></tr>
<tr><td>ไม่ใช้ข้อมูลในเครือข่ายของสำนักงานเพื่อประโยชน์ส่วนตัว</td><td>C</td><td>R</td><td>S</td></tr>
<tr><td>ยกเลิกการประมวลผลข้อมูลหรือการใช้ข้อมูลส่วนบุคคล กรณีที่เจ้าของข้อมูลส่วนบุคคลถอนความยินยอม</td><td>C</td><td>R</td><td>S</td></tr>
</table>
หมายเหตุ R = Responsible A = Accountable S = Supportive C = Consulted และ I = Informed</td></tr>
<tr><td>๔. การเปิดเผยข้อมูล</td><td>๑. ทีมบริกรข้อมูล ได้แก่
๑.๑ หน่วยงานเจ้าของข้อมูล
๑.๒ ผู้ใช้ข้อมูล
๑.๓ ทีมบริหารจัดการข้อมูล</td><td>๑. การเปิดเผยข้อมูลในความรับผิดชอบของหน่วยงานเจ้าของข้อมูลในรูปแบบข้อมูลเปิดของสำนักงาน โดยดำเนินการดังนี้
๑.๑ กำหนดลักษณะของข้อมูลที่เผยแพร่กำหนดให้อยู่ในรูปแบบที่เครื่องสามารถประมวลผลได้
๑.๒ กำหนดให้มีคำอธิบายข้อมูลหรือเมทาดาตาสำหรับข้อมูลที่ต้องเปิดเผย
๑.๓ ข้อมูลที่เผยแพร่จะต้องมีการบันทึกเวลา (Timestamps) ที่ช่วยให้ผู้ใช้งานสามารถระบุได้ว่าข้อมูลนั้นเป็นปัจจุบัน</td></tr>
</table>

วงจรชีวิตข้อมูล	ผู้เกี่ยวข้อง	ข้อปฏิบัติ
		๑.๔ ข้อมูลที่เผยแพร่ต้องมาจากแหล่งที่เก็บข้อมูลโดยตรงด้วยระดับความละเอียดสูงโดยไม่มีการปรับแต่งหรือเป็นข้อมูลรูปแบบสรุป ๑.๕ ชุดข้อมูลและรายการชุดข้อมูลที่เผยแพร่จะต้องมีการจัดรูปแบบที่กำหนดเป็นมาตรฐาน และกำหนดภายใต้หมวดหมู่เดียวกัน เพื่อให้ผู้ใช้ข้อมูลสามารถค้นหาและเข้าถึงข้อมูลได้ง่าย ๒. หน่วยงานเจ้าของข้อมูลห้ามเปิดเผยข้อมูลลับและข้อมูลความมั่นคงที่อยู่ในความครอบครองของสำนักงาน รวมทั้งห้ามเปิดเผยข้อมูลที่การเปิดเผยแล้วจะเป็นความผิดตามกฎหมาย นโยบาย และแนวปฏิบัติอันทำให้เกิดความเสียหายต่อสำนักงาน ๓. หน่วยงานเจ้าของข้อมูลต้องคัดเลือกข้อมูลที่จะเปิดเผยในรูปแบบข้อมูลเปิดจากลำดับชั้นความสำคัญของชุดข้อมูลที่มีคุณค่าสูง (High Value Dataset) ๔. หน่วยงานเจ้าของข้อมูลต้องกำหนดรอบระยะเวลาในการตรวจสอบและปรับปรุงข้อมูลที่เปิดเผยเพื่อให้ข้อมูลถูกต้อง และเป็นปัจจุบัน ๕. หากข้อมูลที่เปิดเผยไม่ครบถ้วนตามข้อ ๑ หรือไม่เป็นปัจจุบัน ให้ผู้ที่พบแจ้งหน่วยงานเจ้าของข้อมูล ทีมบริกรข้อมูล และทีมบริหารจัดการข้อมูล เพื่อจัดทำหรือปรับปรุงให้เป็นปัจจุบัน

ผู้มีส่วนได้ส่วนเสียในการเปิดเผยข้อมูล

กิจกรรมตามวงจรชีวิตข้อมูล (การสร้าง การจัดเก็บ การใช้ การเปิดเผย การลบหรือทำลาย)	ผู้มีส่วนได้ส่วนเสีย			
	ทีมบริกรข้อมูล			
	หน่วยงานเจ้าของข้อมูล	ผู้ใช้ข้อมูล	ทีมบริหารจัดการข้อมูล	ผู้ดูแลระบบ
จะต้องเปิดเผยข้อมูลในความรับผิดชอบต่อสาธารณะตามกฎหมาย/มาตรฐานที่เกี่ยวข้อง	A	I	S/C	S/C
คัดเลือกข้อมูลที่จะเปิดเผยในรูปแบบข้อมูลเปิดจากลำดับชั้นความสำคัญของ High Value Dataset	A	I	S/C	S/C
ตรวจสอบคำอธิบายชุดข้อมูลดิจิทัลที่จะทำการเปิดเผยให้มีความครบถ้วนเป็นปัจจุบัน	S	I	A	R
เปิดเผยข้อมูลส่วนบุคคลตามข้อกำหนดของกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล และห้ามเปิดเผยข้อมูลความมั่นคงและข้อมูลความลับทางราชการ รวมถึงข้อมูลที่เป็นการกระทำความผิดตามกฎหมาย	A	R	S/C	S/C
กำหนดรอบระยะเวลาในการตรวจสอบและปรับปรุงข้อมูลที่เปิดเผย	A	I	I	S/C

หมายเหตุ R = Responsible A = Accountable S = Supportive C = Consulted และ I = Informed

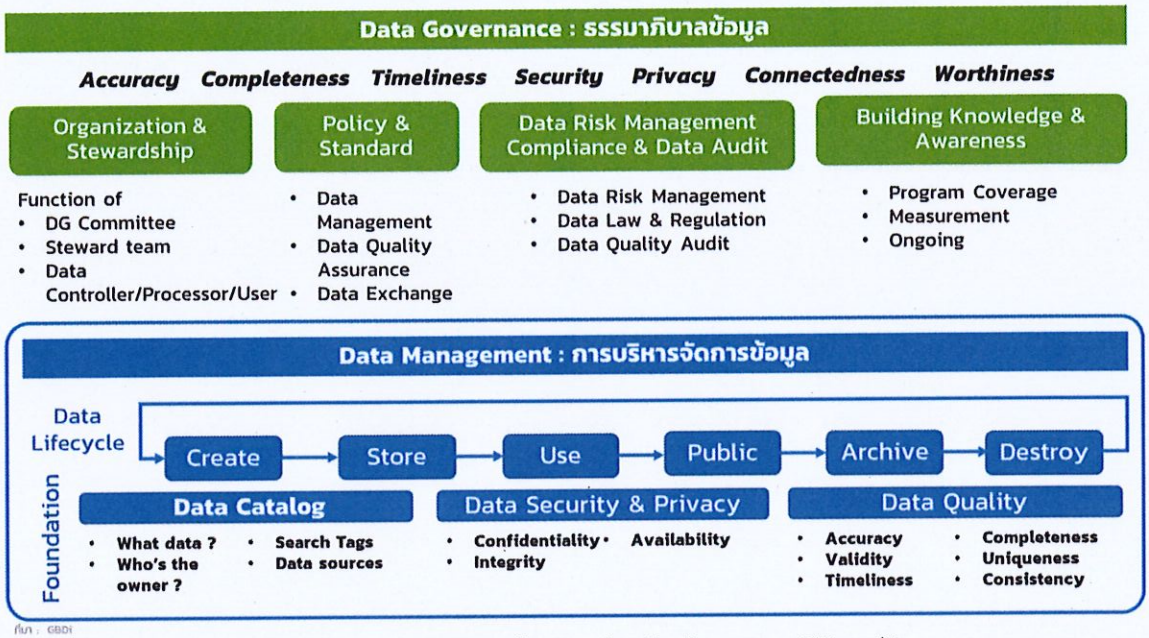
วงจรชีวิตข้อมูล	ผู้เกี่ยวข้อง	ข้อปฏิบัติ
๕. การลบหรือทำลายข้อมูล	๑. ทีมบริกรข้อมูล ได้แก่ ๑.๑ หน่วยงานเจ้าของข้อมูล ๑.๒ ผู้ทำลายข้อมูล ๑.๓ ผู้ดูแลระบบ	๑. หน่วยงานเจ้าของข้อมูลเป็นผู้กำหนดผู้มีสิทธิในการทำลายข้อมูล และทบทวนสิทธินั้นอย่างสม่ำเสมอ หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ เช่น การลาออก เปลี่ยนตำแหน่ง โอนย้าย สิ้นสุดการจ้าง การปรับโครงสร้าง สิ้นสุดสัญญา หรือเมื่อมีการปรับปรุงระบบสารสนเทศ ๒. ผู้ดูแลระบบจะต้องกำหนดสิทธิในการทำลายข้อมูลในระบบให้แก่ผู้ทำลายข้อมูลตามที่หน่วยงานเจ้าของข้อมูลกำหนด ๓. ผู้ทำลายข้อมูลต้องทำลายข้อมูลตามนโยบายหรือหลักเกณฑ์ที่สำนักงานกำหนด และสอดคล้องกับหลักเกณฑ์หรือกฎหมายที่เกี่ยวข้องกับการทำลายข้อมูล ๔. หน่วยงานเจ้าของข้อมูลต้องจัดเก็บคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตาที่ทำลายสำหรับตรวจสอบในภายหลัง ๕. ผู้ทำลายข้อมูลจัดเก็บบันทึกรายละเอียดการทำลายข้อมูลไว้ในทะเบียนควบคุมและบันทึกการทำลายข้อมูล โดยให้เก็บรักษาไว้เป็นหลักฐานไม่น้อยกว่า ๑ ปี

ผู้มีส่วนได้ส่วนเสียในการทำลายข้อมูล

กิจกรรมตามวงจรชีวิตข้อมูล (การสร้าง การจัดเก็บ การใช้ การเปิดเผย การลบหรือทำลาย)	ผู้มีส่วนได้ส่วนเสีย				
	ทีมบริกรข้อมูล				
	หน่วยงานเจ้าของข้อมูล	ทีมบริหารจัดการข้อมูล	ผู้ดูแลระบบ	ผู้ทำลายข้อมูล	ผู้ใช้ข้อมูล
กำหนดผู้มีสิทธิในการทำลายข้อมูล	A	I	R	I	I
ทำลายข้อมูลตามนโยบายหรือหลักเกณฑ์ที่สำนักงานกำหนด และสอดคล้องกับหลักเกณฑ์หรือกฎหมายที่เกี่ยวข้องกับการทำลายข้อมูล	C	I	S	R	I
จัดเก็บคำอธิบายข้อมูลที่ทำลายสำหรับตรวจสอบในภายหลัง	R	I	S	R	I
จัดเก็บบันทึกรายละเอียดการทำลายข้อมูล	I	I	S	R	I
ทำลายข้อมูลส่วนบุคคลเมื่อเจ้าของข้อมูลส่วนบุคคลร้องขอตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล	C	I	S	I	I
ตรวจสอบเพื่อให้มั่นใจว่าข้อมูลถูกลบอย่างปลอดภัยและไม่สามารถกู้คืนได้	I	A	S	R	I

หมายเหตุ R = Responsible A = Accountable S = Supportive C = Consulted และ I = Informed

๕. การบริหารจัดการข้อมูลภาครัฐตามกรอบธรรมาภิบาลข้อมูลภาครัฐ



ที่มา: มาตรฐานรัฐบาลดิจิทัล ว่าด้วยกรอบธรรมาภิบาลข้อมูลภาครัฐ ฉบับปรับปรุง: แนวปฏิบัติ เวอร์ชัน ๒.๐ มรด. ๖: ๒๕๖๖

๕.๑ การบริหารจัดการข้อมูล

สำนักงานบริหารจัดการข้อมูลตามวงจรชีวิตข้อมูล โดยเริ่มตั้งแต่การสร้างข้อมูล การจัดเก็บข้อมูล การใช้ข้อมูล การเปิดเผย การจัดเก็บข้อมูล ไปจนถึงการทำลายข้อมูล โดยมีการดำเนินการดังนี้

๕.๑.๑ การจัดทำบัญชีชุดข้อมูล (Data Catalog) โดยมีขั้นตอนดังนี้

(๑) สำนักงานเลือกชุดข้อมูลที่สำคัญตามพันธกิจของสำนักงานเพื่อนำมาจัดทำบัญชีชุดข้อมูล (Data Catalog) เพื่อให้ทราบว่าข้อมูลนี้เป็นข้อมูลอะไร ผู้ใดเป็นหน่วยงานเจ้าของข้อมูลหรือเป็นผู้รับผิดชอบดูแลข้อมูล แหล่งที่มาของข้อมูลมาจากแหล่งใด และมีคำสำคัญอะไร เพื่อความสะดวกในการค้นหาและนำข้อมูลไปใช้ประโยชน์

(๒) สำนักงานอาจจัดทำเมทาดาตา (Metadata) ประกอบด้วย เพื่อช่วยให้ผู้ใช้สามารถเข้าใจและเข้าถึงข้อมูลได้ง่ายขึ้น

๕.๑.๒ การรักษาข้อมูลให้มีความมั่นคงปลอดภัยและคุ้มครองความเป็นส่วนตัว (Data Security & Privacy) และบรรลุวัตถุประสงค์ด้านความปลอดภัย (CIA) ซึ่งประกอบด้วย ๓ มิติ ได้แก่

(๑) ด้านความลับ (Confidentiality) เพื่อเป็นการจำกัดการเข้าถึงเฉพาะผู้ที่มีสิทธิหรือได้รับอนุญาตเท่านั้น โดยกำหนดมาตรการการเข้าถึงข้อมูล เช่น การเข้ารหัสข้อมูล การใช้ระบบยืนยันตัวตน (เช่น กำหนดรหัสผ่าน การตรวจสอบแบบสองขั้นตอน (Two-Factor Authentication)) เป็นต้น

(๒) ด้านความถูกต้อง ครบถ้วนสมบูรณ์ ความคงสภาพ (Integrity) เพื่อป้องกันมิให้ข้อมูลถูกดัดแปลง หรือถูกทำลายโดยวิธีที่ไม่เหมาะสม และรวมถึงการรับรองว่าข้อมูลจะไม่ถูกปฏิเสธ (non-repudiation) และเป็นข้อมูลที่ถูกต้องเป็นความจริง (authenticity) เช่น การบันทึกเวลา (Timestamping) เพื่อบันทึกวันที่และเวลาที่มีการส่งข้อมูล ให้สามารถพิสูจน์ได้ว่าเหตุการณ์เกิดขึ้นในช่วงเวลาใด หรือการใช้ระบบ

ที่มีการตรวจสอบ (Audit Trails) เพื่อการบันทึกกิจกรรมทั้งหมดที่เกี่ยวข้องกับการเข้าถึงและการจัดการข้อมูล เพื่อให้สามารถติดตามและตรวจสอบได้ เป็นต้น

(๓) ด้านความพร้อมใช้งาน (Availability) เพื่อให้ผู้ใช้ข้อมูลที่มีสิทธิในการเข้าถึงข้อมูลสามารถเข้าถึงข้อมูลหรือระบบสารสนเทศได้อย่างทันท่วงทีเมื่อจำเป็น เช่น การควบคุมการเข้าถึง (Access Control) เพื่อกำหนดสิทธิในการเข้าถึงข้อมูลให้แน่ใจว่าเฉพาะผู้ที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงข้อมูลสำคัญได้ หรือการสำรองข้อมูล (Data Backup) และการบำรุงรักษาระบบเพื่อให้แน่ใจว่าผู้ใช้ที่ได้รับอนุญาตสามารถเข้าถึงข้อมูลได้อย่างต่อเนื่อง เป็นต้น

๕.๑.๓ คุณภาพของข้อมูล (Data Quality) เพื่อให้สำนักงานได้ข้อมูลที่ถูกต้อง สมบูรณ์ และ สามารถนำมาใช้ประโยชน์ได้ โดยมีเกณฑ์การประเมินคุณภาพข้อมูล ๕ มิติ ดังนี้

(๑) ความถูกต้องและสมบูรณ์ (Accuracy and Completeness)

(๒) ความถูกต้องตามมาตรฐาน (Validity)

(๓) ความเป็นปัจจุบัน (Timeliness)

(๔) ความเป็นเอกลักษณ์ (Uniqueness)

(๕) ความสอดคล้องกัน (Consistency)

๕.๒ ธรรมาภิบาลข้อมูล (Data Governance) มีองค์ประกอบที่สำคัญ ได้แก่ ข้อมูลมีความถูกต้องและเชื่อถือได้ (Accuracy) ข้อมูลต้องมีความครบถ้วน (Completeness) ข้อมูลมีความเป็นปัจจุบันและพร้อมใช้งานเมื่อต้องการ (Timeliness) ข้อมูลต้องมีความปลอดภัย (Security) ข้อมูลมีความเป็นส่วนตัว (Privacy) ข้อมูลต้องมีความเชื่อมโยงกัน (Connectedness) และข้อมูลมีคุณค่าและสามารถนำมาใช้ประโยชน์ได้ (Worthiness) ทั้งนี้ เพื่อให้การดำเนินการด้านธรรมาภิบาลข้อมูลของสำนักงานมีประสิทธิภาพ สำนักงานจะมีการดำเนินการ ดังนี้

๕.๒.๑ การวางโครงสร้างบุคลากรและผู้ดูแล (Organization and Stewardship) โดยสำนักงานกำหนดโครงสร้างธรรมาภิบาลข้อมูลภาครัฐ แบ่งออกเป็น ๓ ระดับ ดังนี้

(๑) ระดับนโยบาย (Policy) ได้แก่ คณะกรรมการบริหารกองทุน คณะอนุกรรมการกำกับทิศทางและนโยบายด้านเทคโนโลยีสารสนเทศ และผู้จัดการกองทุน

(๒) ระดับการกำหนดมาตรฐาน ได้แก่ คณะกรรมการด้านธรรมาภิบาลข้อมูลของกองทุนเพื่อความเสมอภาคทางการศึกษา (Data Governance Committee)

(๓) ระดับบริหารจัดการ (Operation) ได้แก่ ทีมบริกรข้อมูล (Data Steward Team)

๕.๒.๒ การจัดทำนโยบายและมาตรฐาน (Policy & Standard) เพื่อเป็นกรอบในการกำหนด กฎเกณฑ์นโยบาย และการวางระบบสารสนเทศเพื่อการกำกับดูแลข้อมูล ทั้งนี้ สำนักงานจะกำหนดนโยบายหรือมาตรฐานด้านข้อมูล ดังนี้

(๑) แนวทางการบริหารจัดการข้อมูล (Data Management) เพื่อให้ข้อมูลมีการดูแลตลอดวงจรชีวิตข้อมูล

(๒) การประกันคุณภาพของข้อมูล (Data Quality Assurance) เพื่อให้แน่ใจว่าข้อมูลที่จัดเก็บและใช้งานในสำนักงานมีคุณภาพสูง ซึ่งรวมถึงการตรวจสอบความถูกต้อง ความครบถ้วน ความสอดคล้อง และความทันเวลาของข้อมูล เพื่อให้สามารถใช้ข้อมูลในการตัดสินใจและดำเนินงานได้อย่างมีประสิทธิภาพ

(๓) การแลกเปลี่ยนข้อมูล (Data Exchange)

(๔) การประเมินความพร้อมของธรรมาภิบาลข้อมูลภาครัฐ (Data Governance Readiness Assessment) ตามหลักเกณฑ์ที่สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.) กำหนด

๕.๒.๓ การตรวจประเมินการบริหารจัดการความเสี่ยงด้านข้อมูลและการตรวจสอบข้อมูล (Data Risk Management Compliance & Data Audit) เพื่อเป็นการประกันคุณภาพโดยการตรวจสอบผลลัพธ์และความสำเร็จจากการกำกับดูแลข้อมูล โดยมีการตรวจสอบเรื่องดังนี้

(๑) การบริหารจัดการความเสี่ยงด้านข้อมูล (Data Risk Management)

(๒) กฎหมายและกฎระเบียบที่เกี่ยวข้อง (Data Law & Regulation)

(๓) การประเมินคุณภาพข้อมูล (Data Quality Audit)

๕.๒.๔ การสร้างความตระหนักและองค์ความรู้ในองค์กร (Building Knowledge and Awareness) ผ่านกลไกต่าง ๆ เช่น จัดหลักสูตรอบรมด้านธรรมาภิบาลข้อมูลภาครัฐ จัดทำคู่มือประกอบแนวปฏิบัติให้ผู้ที่เกี่ยวข้องเพื่อให้ผู้ปฏิบัติงานรับทราบและเข้าใจแนวปฏิบัติการบริหารจัดการข้อมูล เป็นต้น

๖. ความมั่นคงปลอดภัยและคุณภาพของข้อมูล

สำนักงานต้องจัดให้มีการรักษาความมั่นคงปลอดภัยและคุณภาพของข้อมูล ดังนี้

๖.๑ จัดให้มีข้อกำหนดในการรักษาความมั่นคงปลอดภัยและความเป็นส่วนตัวของข้อมูล เพื่อให้มั่นใจว่าข้อมูลของสำนักงานได้รับการปกป้องดูแลให้มีความปลอดภัย เป็นไปตามกฎหมาย กฎเกณฑ์ที่เกี่ยวข้อง และนำไปใช้งานอย่างเหมาะสม

๖.๒ ตรวจสอบชั้นความลับของข้อมูลภายในสำนักงาน พร้อมทั้งตรวจสอบสิทธิของสำนักงานที่สามารถนำข้อมูลไปใช้ได้ตามบทบาทและภารกิจตามกฎหมายของหน่วยงานนั้น ๆ และจำแนกหมวดหมู่และระดับชั้นความลับของข้อมูล รวมถึงต้องมีมาตรการในการป้องกัน การเข้าถึง การบริหารจัดการข้อมูลและอุปกรณ์ที่จัดเก็บข้อมูลอย่างเหมาะสม สอดคล้องตามหมวดหมู่และชั้นความลับของข้อมูล

๖.๓ กำหนดสิทธิการเข้าถึงข้อมูล วิธี และเครื่องมือที่ใช้ในการเข้าถึงข้อมูล และกำหนด ระยะเวลาในการทบทวนสิทธิและวิธีในการเข้าถึงข้อมูล

๖.๔ จัดให้มีกระบวนการรักษาคุณภาพ ความครบถ้วน และความถูกต้องของข้อมูล รวมถึงจัดให้มีกระบวนการปรับปรุงข้อมูลให้มีความเป็นปัจจุบัน ตรงตามความต้องการของผู้ใช้ และพร้อมใช้งาน

๖.๕ กำหนดหลักเกณฑ์ในการประเมินคุณภาพของข้อมูล แผนการตรวจสอบและปรับปรุง ข้อมูลอย่างต่อเนื่อง รวมถึงกำหนดเครื่องมือและทรัพยากรในการปรับปรุงคุณภาพข้อมูลอย่างเหมาะสม เพื่อให้การปรับปรุงคุณภาพของข้อมูลมีความต่อเนื่อง

๗. การแลกเปลี่ยนหรือเชื่อมโยงข้อมูล

๗.๑ ให้ทีมบริหารจัดการข้อมูลร่วมกับทีมบริกรข้อมูล กำหนดวิธีปฏิบัติหรือคู่มือหรือแนวทางการดำเนินงาน และมาตรฐานทางด้านเทคนิคที่จำเป็นต้องใช้เกี่ยวกับการเชื่อมโยงและแลกเปลี่ยนข้อมูล ดังนี้

๗.๑.๑ การเชื่อมโยงและแลกเปลี่ยนข้อมูลภายในหน่วยงาน กำหนดให้ใช้รูปแบบที่เป็นมาตรฐานเปิด (Open Format) ทั้งในส่วนมาตรฐานข้อมูล เช่น XML และ JSON เป็นต้น มาตรฐานโปรโตคอลสื่อสาร เช่น SOAP REST หรืออื่น ๆ ที่ได้รับการยอมรับจากมาตรฐานสากล

๗.๑.๒ การเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน ให้ดำเนินการตามมาตรฐานกลางของหน่วยงานหลักที่เป็นผู้รับผิดชอบ

๗.๒ ให้ทีมบริหารจัดการข้อมูลร่วมกับทีมบริกรข้อมูล ตรวจสอบคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตาที่จะทำการเชื่อมโยงและแลกเปลี่ยนให้ครบถ้วน ดังนี้

๗.๒.๑ ตรวจสอบเมทาดาตาของชุดข้อมูลดิจิทัลที่จัดเก็บให้มีฟิลด์ข้อมูลครบถ้วนสอดคล้องกับความต้องการของหน่วยงานที่ขอใช้ หากไม่ครบถ้วนต้องจัดทำเพิ่มเติมตามความต้องการของหน่วยงานที่ขอใช้

๗.๒.๒ ตรวจสอบชั้นความลับของข้อมูลว่าอยู่ในชั้นความลับที่สามารถเปิดเผยได้หรือไม่ กล่าวคือต้องไม่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ ความมั่นคงของประเทศ ความลับทางราชการ และความเป็นส่วนตัว พร้อมทั้งตรวจสอบสิทธิของหน่วยงานที่สามารถนำข้อมูลไปใช้ได้ตามบทบาทและภารกิจตามกฎหมายของหน่วยงานนั้น ๆ

๗.๒.๓ หากไม่ครบถ้วน หรือไม่เป็นปัจจุบัน ให้แจ้งหน่วยงานเจ้าของข้อมูล ทีมบริกรข้อมูล และทีมบริหารจัดการข้อมูล เพื่อจัดทำหรือปรับปรุงให้เป็นปัจจุบัน

๗.๓ ในการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน ให้สำนักงานจัดทำสัญญาอนุญาต หรือบันทึกข้อตกลง หรือสัญญารักษาความลับ หรือข้อตกลงอื่นใด เพื่อรองรับการแลกเปลี่ยนข้อมูลหรือเชื่อมโยงข้อมูลด้วย

๗.๔ ให้สำนักงาน จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยเกี่ยวกับการเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัล เพื่อป้องกันมิให้มีการรับ-ส่งข้อมูลที่ไม่สมบูรณ์ หรือส่งข้อมูลไปผิดที่หรือมีการรั่วไหลของข้อมูล หรือข้อมูลถูกแก้ไขเปลี่ยนแปลง ถูกทำซ้ำใหม่ ถูกส่งซ้ำ โดยมิได้รับอนุญาต

๗.๕ ห้ามมิให้มีการเชื่อมโยงและแลกเปลี่ยนหรือส่งต่อ ข้อมูลที่เข้าข่ายการกระทำความผิดตามกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์

๗.๖ กำหนดให้ผู้ดูระบบต้องจัดเก็บบันทึกหลักฐานของการเชื่อมโยงและการแลกเปลี่ยนข้อมูลดิจิทัล เพื่อใช้ตรวจสอบสิ่งผิดปกติต่าง ๆ ที่เกิดขึ้นในการเชื่อมโยงและแลกเปลี่ยนข้อมูล

ผู้มีส่วนได้ส่วนเสียในการเชื่อมโยงหรือแลกเปลี่ยนข้อมูล

กิจกรรมตามวงจรชีวิตข้อมูล (การสร้าง การจัดเก็บ การใช้ การเปิดเผย การลบหรือทำลาย)	ผู้มีส่วนได้ส่วนเสีย		
	ทีมบริกรข้อมูล		
	ผู้ดูแลระบบ	หน่วยงานเจ้าของข้อมูล	ทีมบริหารจัดการข้อมูล
กำหนดวิธีปฏิบัติและมาตรฐานทางด้านเทคนิคที่จำเป็นในการเชื่อมโยงหรือแลกเปลี่ยนข้อมูล	S	I	A
ตรวจสอบคำอธิบายชุดข้อมูลดิจิทัล และชั้นความลับของข้อมูล	S	C	A

จัดทำแนวทางการทำงานร่วมกันทั้งระหว่างภายในสำนักงานและหน่วยงานภายนอกในการเชื่อมโยงและแลกเปลี่ยนข้อมูล	S	S	A
จัดเก็บบันทึกหลักฐานของการเชื่อมโยงและการแลกเปลี่ยนข้อมูลดิจิทัล	R	I	I

หมายเหตุ R = Responsible A = Accountable S = Supportive C = Consulted และ I = Informed

๘. การจัดเก็บและการทำลายข้อมูล

สำนักงานต้องจัดให้มีการจัดเก็บและการทำลายข้อมูล ดังนี้

๘.๑ กำหนดระยะเวลาในการจัดเก็บข้อมูลที่เหมาะสมกับข้อมูลแต่ละประเภท

๘.๒ กำหนดเครื่องมือและกระบวนการที่จะใช้ในการจัดเก็บข้อมูล ระหว่างระยะเวลาในการจัดเก็บข้อมูล

๘.๓ กำหนดขั้นตอนและวิธีการทำลายข้อมูล

๘.๔ กำหนดอำนาจอนุมัติ สิทธิ และยืนยันตัวบุคคลในการทำลายข้อมูล

๘.๕ กำหนดวิธีและแนวทางในการทำลายข้อมูล เมื่อข้อมูลนั้นไม่มีการใช้งานหรือมีการเก็บ ข้อมูลไว้นานเกินกว่าระยะเวลาที่กำหนด

๘.๖ ให้มีการสร้างความรู้ความเข้าใจในการจัดเก็บและทำลายข้อมูลแก่ผู้ที่เกี่ยวข้องทั้งภายในและภายนอกหน่วยงาน