ประกาศสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

ที่ ๓/๒๕๖๙

เรื่อง นโยบายการบริหารจัดการข้อมูล (Data Management Policy)

ของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

โดยที่เป็นการสมควรปรับปรุงนโยบายการบริหารจัดการข้อมูล (Data Management Policy) ของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) เพื่อให้มีความครบถ้วน เหมาะสม เป็นปัจจุบัน สอดคล้องกับกรอบธรรมาภิบาลข้อมูลภาครัฐ กฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง สำหรับใช้เป็นกรอบและแนวทางในการบริหารจัดการข้อมูลของหน่วยงานสำหรับผู้บริหาร เจ้าหน้าที่และผู้ปฏิบัติงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ต่อไป

อาศัยอำนาจตามความในมาตรา ๘ (๒) มาตรา ๒๙ และมาตรา ๓๐ แห่งพระราชกฤษฎีกาจัดตั้งสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) พ.ศ. ๒๕๖๑ ประกอบกับมติคณะทำงานขับเคลื่อนธรรมาภิบาลข้อมูลและคุ้มครองข้อมูลส่วนบุคคล ในการประชุมครั้งที่ ๑/๒๕๖๘ เมื่อวันที่ ๙ ธันวาคม ๒๕๖๘ จึงให้ยกเลิกประกาศสำนักงานพัฒนารัฐบาลดิจิทัล (องคการมหาชน) ที่ ๙/๒๕๖๖ เรื่อง นโยบายการบริหารจัดการข้อมูล (Data Management Policy) ของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ฉบับลงวันที่ ๗ พฤศจิกายน ๒๕๖๖ และให้ออกประกาศเรื่องนโยบายการบริหารจัดการข้อมูล (Data Management Policy) ของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) โดยมีรายละเอียดตามที่แนบท้ายประกาศฉบับนี้

จึงประกาศให้ทราบโดยทั่วกัน ทั้งนี้ ให้มีผลนับตั้งแต่บัดนี้เป็นต้นไป จนกว่าจะมีประกาศเปลี่ยนแปลง

ประกาศ ณ วันที่ ๒๑ เมษายน พ.ศ. ๒๕๖๙

(นางไอรดา เหลืองวิไล)

รองผู้อำนวยการ รักษาการแทน

ผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

นโยบายการบริหารจัดการข้อมูล (Data Management Policy) ของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

เวอร์ชัน	ผู้อนุมัติ	วันที่อนุมัติ	วันที่มีผลบังคับใช้
0.1	ผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล	7 พฤศจิกายน พ.ศ. 2566	7 พฤศจิกายน พ.ศ. 2566
0.2	รักษาการผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล	21 เมษายน พ.ศ. 2569	21 เมษายน พ.ศ. 2569

1. วัตถุประสงค์

1) เพื่อให้การบริหารจัดการข้อมูลของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) หรือ สพร. สอดคล้องกับกฎหมาย กรอบธรรมาภิบาลข้อมูลภาครัฐ และระเบียบปฏิบัติที่เกี่ยวข้อง

2) เพื่อใช้เป็นกรอบและแนวทางในการบริหารจัดการข้อมูลของหน่วยงาน สำหรับผู้บริหาร เจ้าหน้าที่และผู้ปฏิบัติงานของ สพร. และผู้ที่เกี่ยวข้อง

2. ขอบเขตและการบังคับใช้

นโยบายการบริหารจัดการข้อมูลฉบับนี้จัดทำโดยฝ่ายบริหารจัดการและเชื่อมโยงข้อมูลภาครัฐ มีผลบังคับใช้กับข้อมูลดิจิทัลทั้งหมดที่อยู่ในความครอบครองหรือควบคุมของ สพร. เพื่อให้การบริหารจัดการข้อมูลมีประสิทธิภาพและสอดคล้องกับทรัพยากรของหน่วยงาน

โดยการบังคับใช้นโยบายฉบับนี้ ให้พิจารณาดำเนินการตามลำดับความสำคัญกับชุดข้อมูลเป้าหมายตามที่คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Committee) กำหนดก่อนและให้ดำเนินการทบทวนชุดข้อมูลเป้าหมายดังกล่าวเป็นประจำทุกปี ดังนี้

(1) กลุ่มข้อมูลสำหรับรายงานผู้บริหาร เช่น ข้อมูลสำหรับการวิเคราะห์แนวโน้มและการรับรู้รายได้และข้อมูลสำหรับการวิเคราะห์ความสัมพันธ์ระหว่าง งาน เงิน และคน

(2) กลุ่มข้อมูลในบัญชีรายการสินทรัพย์สารสนเทศ (Asset Inventory) เช่น ฝ่ายบริหารจัดการและเชื่อมโยงข้อมูลภาครัฐ ฝ่ายมาตรฐานดิจิทัลภาครัฐ ฝ่ายกลยุทธ์องค์กร ส่วนการเงิน บัญชี และควบคุมงบประมาณ

3. ข้อยกเว้น

นโยบายนี้อาจมีการขยายผลหรือมีการยกเว้น โดยปฏิบัติตามขั้นตอนการขยายผลหรือยกเว้นนโยบายของรัฐด้านอื่น ๆ หรือนโยบายของ สพร. ร่วมด้วย

4. บทบาทและความรับผิดชอบ

1) ผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัลหรือผู้ที่ได้รับมอบหมายต้องควบคุมและกำกับดูแลให้บุคลากรใน สพร. ผู้ใช้ข้อมูล และผู้ที่เกี่ยวข้องดำเนินการตามนโยบายการบริหารจัดการข้อมูลอย่างเคร่งครัด

2) ผู้บังคับบัญชา/ผู้ที่ได้รับมอบหมายต้องตรวจสอบให้แน่ใจว่าบุคลากรในหน่วยงาน ภายใต้บังคับบัญชาทำหน้าที่บริหารจัดการข้อมูล และได้รับความรู้เกี่ยวกับนโยบายนี้อย่างเหมาะสม รวมถึงสามารถนำนโยบายไปปฏิบัติตามอย่างมีประสิทธิภาพและประสิทธิผล

3) บุคลากรใน สพร. และบุคคลอื่น ๆ เช่น บริษัทหรือผู้รับจ้าง ที่ได้รับมอบหมายจาก สพร. ให้ทำหน้าที่บริหารจัดการข้อมูลต้องปฏิบัติตามนโยบาย มาตรการ วิธีการ และแนวปฏิบัติต่าง ๆ ที่เกี่ยวข้องกับข้อมูลและระบบข้อมูลสารสนเทศที่ สพร. กำหนด

4) ผู้ดูแลบริหารจัดการข้อมูล ได้แก่ คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Committee) บรรณาธิการข้อมูล เจ้าของข้อมูล ทีมบริกรข้อมูล ผู้ใช้ข้อมูล ผู้บริหารจัดการฐานข้อมูล ผู้ดูแลระบบสารสนเทศ ผู้ทำลายข้อมูล ต้องปฏิบัติหน้าที่ที่ได้รับมอบหมายภายใต้นโยบายนี้ (รายละเอียดตามข้อ 8 ข้อมูลเพิ่มเติม)

ทั้งนี้ ผู้ที่ฝ่าฝืนนโยบายนี้ถือว่าเป็นการกระทำความผิดและจะต้องได้รับการดำเนินการตามระเบียบหรือข้อบังคับของ สพร.

5. คำนิยาม

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

ชุดข้อมูล (Dataset) หมายความว่า การนำข้อมูลจากหลายแหล่งมารวบรวม เพื่อจัดเป็นชุดให้ตรงตามลักษณะโครงสร้างของข้อมูล

บัญชีข้อมูล (Data Catalog) หมายความว่า เอกสารแสดงบรรดารายการของชุดข้อมูล ที่จำแนกแยกแยะโดยการจัดกลุ่มหรือจัดประเภทข้อมูลที่อยู่ในความครอบครองหรือควบคุมของหน่วยงาน

บัญชีข้อมูลภาครัฐ (Government Data Catalog) หมายความว่า เอกสารแสดงบรรดารายการของชุดข้อมูลสำคัญที่รวบรวมจากบัญชีข้อมูลของหน่วยงานภาครัฐ

คำอธิบายชุดข้อมูลดิจิทัล หรือเมทาดาทา (Metadata) หมายความว่า ข้อมูลที่ใช้อธิบายข้อมูลหลักหรือกลุ่มข้อมูลอื่น ๆ ที่เกี่ยวข้องทั้งกระบวนการเชิงธุรกิจ ในที่นี้หมายถึง กระบวนการทำงานตามภารกิจของหน่วยงานและเชิงเทคโนโลยีสารสนเทศ กฎและข้อจำกัดของข้อมูล และโครงสร้างของข้อมูลเมทาดาตาช่วยให้หน่วยงานสามารถเข้าใจข้อมูล ระบบ และขั้นตอนการทำงานได้ดียิ่งขึ้น โดยการบริหารจัดการเมทาดาตา (Metadata Management) เริ่มตั้งแต่ การเก็บรวบรวม การจัดกลุ่ม การดูแล และการควบคุมเมทาดาตา ทั้งนี้ข้อมูลแต่ละ

ชุดควรมีเมทาดาตาเพื่อให้ผู้ใช้งานทราบเกี่ยวกับชุดข้อมูล เช่น รายละเอียดชุดข้อมูล สิ่งที่เกี่ยวข้องกับชุดข้อมูล วัตถุประสงค์การนำไปใช้ ฟิลด์ข้อมูล

ธรรมาภิบาลข้อมูลภาครัฐ (Data Governance for Government) หมายความว่า การกำหนดสิทธิ หน้าที่ และความรับผิดชอบของผู้มีส่วนได้ส่วนเสียทั้งหมดที่เกี่ยวข้องในการบริหารจัดการข้อมูลของหน่วยงานภาครัฐ ในทุกขั้นตอนของวงจรชีวิตข้อมูล เพื่อให้การได้มา การจัดเก็บ การประมวลผล การใช้ การแลกเปลี่ยน และการเปิดเผยข้อมูลเป็นไปอย่างถูกต้องตามกฎหมาย ครบถ้วน เป็นปัจจุบัน มีคุณภาพ น่าเชื่อถือ มีความมั่นคงปลอดภัย เคารพความเป็นส่วนตัวของเจ้าของข้อมูล เพื่อสนับสนุนการใช้ข้อมูลในการบริหารงานภาครัฐและการบริการสาธารณะ

หมวดหมู่ของข้อมูล (Data Category) หมายความว่า ตามกรอบธรรมาภิบาลข้อมูลภาครัฐแบ่งออก ได้เป็น 5 หมวดหมู่ ได้แก่ ข้อมูลสาธารณะ ข้อมูลใช้ภายใน ข้อมูลส่วนบุคคล ข้อมูลความลับทางราชการ และ ข้อมูลความมั่นคง

การจัดระดับชั้นข้อมูล (Data Classification) หมายความว่า การจัดระดับชั้นของข้อมูลในบริบทของการรักษาความปลอดภัยข้อมูลตามระดับของความอ่อนไหวและผลกระทบต่อบุคคล องค์กร และประเทศ หากมีการเปิดเผย เปลี่ยนแปลง หรือทำลายข้อมูลโดยไม่ได้รับอนุญาต โดยการจัดระดับชั้นข้อมูลจะช่วยกำหนดการควบคุมความปลอดภัยพื้นฐานที่เหมาะสมสำหรับการปกป้องข้อมูลนั้นๆ ทั้งนี้ ข้อมูลสำคัญของบุคคล องค์กร และประเทศทั้งหมด ควรจัดชั้นตามระดับความอ่อนไหวของระดับชั้นข้อมูลหรือตามที่หน่วยงานกำหนด เพื่อให้หน่วยงานของรัฐสามารถจัดการข้อมูลในกระบวนงานที่เกี่ยวข้องกับภารกิจของหน่วยงานได้อย่างมีประสิทธิภาพ

การควบคุมการเข้าถึง (Access Control) หมายความว่า นโยบาย กระบวนการ และกลไกทางเทคนิคที่ใช้ในการจำกัดและควบคุมสิทธิ์ของผู้ใช้หรือระบบในการเข้าถึง (เช่น ดู อ่าน เขียน แก้ไข ลบ) ข้อมูล ทรัพย์สินสารสนเทศ หรือระบบงานต่าง ๆ โดยยึดหลักการให้สิทธิ์น้อยที่สุดเท่าที่จำเป็น (Least Privilege) และหลักความจำเป็นต้องรู้ (Need-to-Know)

สินทรัพย์ข้อมูล (Data Asset) หมายความว่า ข้อมูลที่ครอบครองหรือมีสิทธิในการใช้ ซึ่งมีมูลค่าในเชิงกลยุทธ์หรือการดำเนินงาน โดยถือเป็นทรัพย์สินที่ต้องได้รับการบริหารจัดการอย่างเหมาะสม ครอบคลุมถึงการจัดเก็บ การรักษาความปลอดภัย การควบคุมการเข้าถึง และการใช้ประโยชน์อย่างมีประสิทธิภาพ

วงจรชีวิตของข้อมูล (Data Life Cycle) หมายความว่า ลำดับขั้นตอนของข้อมูลตั้งแต่เริ่มสร้างข้อมูลไปจนถึงการทำลายข้อมูลตามกรอบธรรมาภิบาลข้อมูลภาครัฐ

คุณภาพข้อมูล (Data Quality) หมายความว่า ข้อมูลที่ดี ได้มาตรฐานตามที่กำหนด และตรงกับความต้องการของผู้ใช้ กล่าวคือ ผลรวมของคุณลักษณะและคุณสมบัติของผลิตผลข้อมูลที่พึงประสงค์ทุกประการของผลการปฏิบัติงานตามดัชนีตัวชี้วัดคุณภาพและองค์ประกอบที่กำหนดไว้

ข้อมูลส่วนบุคคล (Personal Data - PII) หมายความว่า ข้อมูลใด ๆ ที่เกี่ยวกับบุคคลธรรมดาซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าโดยทางตรงหรือทางอ้อม เช่น ชื่อ-นามสกุล เลขประจำตัวประชาชน ที่อยู่ เบอร์โทรศัพท์ อีเมล แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

ข้อมูลส่วนบุคคลอ่อนไหว (Sensitive Personal Data) หมายความว่า ข้อมูลส่วนบุคคลที่เกี่ยวกับเชื้อชาติ, เผ่าพันธุ์, ความคิดเห็นทางการเมือง, ความเชื่อในลัทธิ, ศาสนาหรือปรัชญา, พฤติกรรมทางเพศ, ประวัติอาชญากรรม, ข้อมูลสุขภาพ, ความพิการ, ข้อมูลสหภาพแรงงาน, ข้อมูลพันธุกรรม, ข้อมูลชีวภาพ (Biometric Data) หรือข้อมูลอื่นใดที่อาจกระทบต่อเจ้าของข้อมูลในทำนองเดียวกันตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด ซึ่งการเก็บรวบรวม ใช้ หรือเปิดเผยต้องอยู่ภายใต้เงื่อนไขที่เข้มงวดกว่าข้อมูลส่วนบุคคลทั่วไป

บุคลากรใน สพร. หมายความว่า เจ้าหน้าที่ ลูกจ้าง หรือผู้ปฏิบัติงาน ไม่ว่าจะเป็นการแต่งตั้งในฐานะเป็นกรรมการหรือฐานะอื่นใด

6. นโยบายการบริหารจัดการข้อมูล

ข้อกำหนดทั่วไป

1) กำหนดบทบาท หน้าที่ และความรับผิดชอบของแต่ละบุคคลตามโครงสร้างธรรมาภิบาลข้อมูลภาครัฐ โดยต้องได้รับการมอบอำนาจและการอนุมัติจากผู้บริหาร พร้อมทั้งกำหนดหน่วยงานเจ้าของข้อมูล เพื่อทำหน้าที่ในการบริหารจัดการข้อมูลนั้น ๆ

2) กำหนดการจัดทำนโยบายการบริหารจัดการข้อมูลเป็นลายลักษณ์อักษร อนุมัติเผยแพร่เพื่อประกาศใช้และถือปฏิบัติ โดยให้มีผลบังคับใช้กับบุคลากรใน สพร. ตลอดจนหน่วยงาน/บุคคลภายนอกที่เกี่ยวข้องกับการได้มาและการใช้ข้อมูลของ สพร. พร้อมทั้งจัดทำแนวปฏิบัติและมาตรฐานที่เกี่ยวกับข้อมูลเพื่อสนับสนุนการปฏิบัติงานให้สอดคล้องตามนโยบายดังกล่าว

3) กำหนดมาตรการ วิธีการ และแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของข้อมูล เพื่อป้องกันการละเมิดการเข้าถึง การสูญหาย การทำลาย หรือการเปลี่ยนแปลงข้อมูล โดยปราศจากอำนาจโดยมิชอบหรือโดยมิได้รับอนุญาต โดยให้สอดคล้องกับนโยบายความมั่นคงปลอดภัยสารสนเทศของ สพร.

4) กำหนดมาตรการ วิธีการ และแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลที่สอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล ตลอดจนถึงระเบียบ และแนวปฏิบัติของ สพร.

5) ดำเนินการตรวจสอบ ติดตาม และประเมินผลการปฏิบัติตามนโยบายการบริหารจัดการข้อมูลโดยทีมบริกรข้อมูล พร้อมทั้งกำหนดให้มีการทบทวนนโยบาย รวมถึงมาตรการ วิธีการ และแนวปฏิบัติต่าง ๆ เกี่ยวกับข้อมูลต่อคณะกรรมการธรรมาภิบาลข้อมูลของ สพร. อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญตามความเหมาะสม

6) กำหนดเกี่ยวกับการจัดให้มีทรัพยากรด้านงบประมาณ ทรัพยากรบุคคล และเทคโนโลยีที่เพียงพอต่อการบริหารจัดการข้อมูล พร้อมทั้งสนับสนุนการฝึกอบรมธรรมาภิบาลข้อมูลภาครัฐและการบริหารจัดการข้อมูลให้ครอบคลุมทั้งวงจรชีวิตของข้อมูลแก่บุคลากรใน สพร. อย่างน้อยปีละ 1 ครั้ง

7) ข้อกำหนดอื่น ๆ ตามที่ สพร. กำหนดเพิ่มเติม

การจัดหมวดหมู่และชั้นความลับของข้อมูล

1) กำหนดหมวดหมู่และประเภทชั้นความลับของข้อมูลที่ใช้กับข้อมูลทุกรูปแบบของ สพร. ทั้งเอกสารกระดาษและข้อมูลดิจิทัล ด้วยการประเมินผลกระทบของข้อมูลของ สพร. เพื่อระบุหมวดหมู่และประเภทชั้นความลับของข้อมูล รวมทั้งกำหนดระดับความปลอดภัยที่เหมาะสมสำหรับการสร้าง/จัดเก็บ การใช้ และการเข้าถึงชุดข้อมูล และเพื่อใช้กับบุคลากรรวมถึงตัวแทนบุคคลที่สามที่ได้รับอนุญาตให้เข้าถึงข้อมูลใน สพร. พร้อมทั้งกำหนดบทบาทหน้าที่ของบุคลากรในการจัดหมวดหมู่และชั้นความลับ เพื่อป้องกัน จัดการ และกำกับดูแลข้อมูลให้เหมาะสม

2) การจัดหมวดหมู่ของข้อมูลเป็นไปตามกรอบธรรมาภิบาลข้อมูลภาครัฐ ได้แก่ ข้อมูลสาธารณะ ข้อมูลใช้ภายใน ข้อมูลส่วนบุคคล ข้อมูลความลับทางราชการ และข้อมูลความมั่นคง และพิจารณาการจัดระดับชั้นความลับของข้อมูลภาครัฐที่มีความอ่อนไหวให้สอดคล้องตามแนวมาตรฐานสากลและเป็นไปตามข้อกฎหมายที่เกี่ยวข้อง โดยระดับชั้นความลับแบ่งออกเป็น 1.ชั้นเปิดเผย (Open) สู่สาธารณะ 2.เปิดเผยเมื่อได้รับอนุญาต ได้แก่ ชั้นเผยแพร่ภายในองค์กร (Private) ชั้นลับ (Confidential) และ ชั้นลับมาก (Secret) และ 3.เปิดเผยไม่ได้/ปกปิด ได้แก่ ชั้นลับที่สุด (Top Secret) ทั้งนี้ ข้อมูลใช้ภายในควรมีการจัดแบ่งหมวดหมู่ ก่อนจัดแบ่งระดับชั้นความลับของข้อมูล โดยประยุกต์ใช้หลักเกณฑ์ฯ ตามแนวทางการจัดระดับชั้นข้อมูลภาครัฐ หรือมาตรฐานข้อมูลที่บังคับใช้ในอนาคต

3) กำกับดูแลและติดตามอย่างต่อเนื่อง โดยตรวจสอบความปลอดภัยการใช้งานและรูปแบบการเข้าถึงของระบบและข้อมูล ทั้งผ่านกระบวนการอัตโนมัติหรือโดยบุคคล เพื่อระบุภัยคุกคามภายนอก การบำรุงรักษาการทำงานของระบบตามปกติ และการติดตั้งโปรแกรมเพื่อปรับปรุงและติดตามการเปลี่ยนแปลงของสภาพแวดล้อมของระบบและข้อมูล

การบริหารจัดการข้อมูลตามวงจรชีวิตของข้อมูล

1) กำหนดแนวปฏิบัติในการสร้างข้อมูลให้มีคุณภาพ มีความมั่นคงปลอดภัย และเป็นประโยชน์ต่อผู้ใช้ข้อมูล ดำเนินการตรวจสอบความมีอยู่และรายละเอียดของข้อมูลที่สำคัญ เช่น คำอธิบายข้อมูลหรือเมทาดาตา ชุดข้อมูล การจัดชั้นความลับข้อมูล รายงานผลให้แก่ผู้รับผิดชอบตามโครงสร้างธรรมาภิบาลข้อมูลภาครัฐและดำเนินการตามกระบวนการธรรมาภิบาลข้อมูลภาครัฐ

2) กำหนดแนวปฏิบัติการจัดเก็บข้อมูลให้สอดคล้องกับแนวทางหรือมาตรฐานการจัดชั้นความลับของข้อมูลที่กำหนดไว้ โดยข้อมูลต้องมีความถูกต้อง สมบูรณ์ และเป็นปัจจุบัน พร้อมทั้งกำหนดสิทธิและจัดหาระบบ/เครื่องมือที่ใช้ในการเข้าถึงข้อมูลเพื่อรักษาความมั่นคงปลอดภัยและคุณภาพข้อมูล และทำลายข้อมูลเมื่อพ้นระยะเวลาการจัดเก็บตามแนวปฏิบัติและกฎหมายที่เกี่ยวข้อง

3) กำหนดแนวปฏิบัติและมาตรฐานการประมวลผลและใช้ข้อมูล เพื่อผู้ใช้นำข้อมูลไปใช้อย่างถูกต้องตามวัตถุประสงค์ที่ต้องการเพื่อให้เกิดประโยชน์สูงสุด

4) กำหนดแนวปฏิบัติการเปิดเผยข้อมูลต่อสาธารณะ โดยข้อมูลที่เปิดเผยควรเป็นประโยชน์ สามารถนำไปประมวลผลและใช้ต่อยอดในการพัฒนาในรูปแบบต่าง ๆ ได้ เว้นแต่มีกฎหมายกำหนดไว้เป็นอย่างอื่น การเปิดเผยข้อมูลส่วนบุคคล หรือข้อมูลที่มีชั้นความลับ ต้องได้รับการพิจารณาจากคณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Committee) ก่อนการเปิดเผยข้อมูล รวมทั้งจัดให้มีช่องทางการเปิดเผยข้อมูลที่เข้าถึงและนำไปใช้อย่างเหมาะสม

5) จัดทำสัญญาอนุญาตหรือข้อตกลงในการแลกเปลี่ยนข้อมูลและการนำข้อมูลไปใช้ ในกรณีที่จำเป็น

6) กำหนดแนวปฏิบัติการรักษาความมั่นคงปลอดภัย ด้านคุณภาพข้อมูล และด้านคุ้มครองความเป็นส่วนตัวของข้อมูล รวมถึงแนวปฏิบัติให้กับผู้ประสานงานหรือศูนย์ติดต่อ (Contact Center) และตรวจสอบให้แน่ใจว่าได้บริหารจัดการข้อมูลอย่างเหมาะสมตามแนวทางหรือแนวปฏิบัติที่กำหนดไว้

7) กำหนดแนวปฏิบัติการทำลายข้อมูล และการพิจารณาอนุมัติทำลายข้อมูลเพื่อเป็นการรักษาความมั่นคงปลอดภัยของข้อมูล

คุณภาพข้อมูล

1) กำหนดนโยบายการจัดการคุณภาพข้อมูล เพื่อใช้เป็นกรอบแนวทางในการจัดการข้อมูลของ สพร. ให้มีคุณภาพตามเกณฑ์หรือคุณสมบัติที่กำหนด เช่น ความถูกต้องสมบูรณ์ ความครบถ้วน ความสอดคล้องกัน ความเป็นปัจจุบัน ตรงตามความต้องการใช้งาน และความพร้อมใช้ เป็นต้น โดยบรรณาธิการข้อมูลมีหน้าที่จัดการและกำกับดูแลข้อมูลให้มีคุณภาพเพื่อสร้างความมั่นใจให้กับผู้ใช้ข้อมูล ในขณะที่ผู้ใช้ข้อมูลมีบทบาทในการให้ข้อเสนอแนะแก่บรรณาธิการข้อมูลเพื่อการปรับปรุงคุณภาพให้ดียิ่งขึ้น

2) จัดทำเกณฑ์คุณภาพข้อมูลที่สามารถวัดผลได้ พร้อมทั้งจัดทำแผนพัฒนาคุณภาพข้อมูลที่สามารถระบุตัวชี้วัดคุณภาพและแผนปฏิบัติการเพื่อจัดการคุณภาพข้อมูลได้อย่างมีประสิทธิภาพ โดยออกแบบการเก็บรวบรวมข้อมูลเพื่อให้ได้ข้อมูลสำหรับประเมินคุณภาพตามเกณฑ์ดังกล่าวให้รวมอยู่ในระบบเทคโนโลยีสารสนเทศและกระบวนการทำงาน (Quality by Design) เพื่อลดข้อผิดพลาดและปรับปรุงคุณภาพตั้งแต่จุดการป้อนข้อมูลหรือการสร้างข้อมูลไปจนถึงการประมวลผลข้อมูล

3) ประเมินผลและจัดการคุณภาพข้อมูลอย่างสม่ำเสมอตลอดวงจรชีวิตของข้อมูล โดยเจ้าของข้อมูลและทีมบริกรข้อมูลควรกำหนดกรอบคุณภาพข้อมูลเฉพาะหมวดหมู่ข้อมูลหรือโดเมน (Domain) เช่น Quality Assurance Framework of the European Statistical System (ESS. QAF) ที่เป็นกรอบคุณภาพข้อมูลสถิติของ the European Statistical System ที่สามารถนำมาใช้อ้างอิงได้ หรือ กรอบตัวชี้วัดคุณภาพข้อมูล (Data Quality Metrics) ในระบบตรวจสอบคุณภาพข้อมูลแบบอัตโนมัติที่ สพร. พัฒนาขึ้น

4) พัฒนากระบวนการหรือกลไกให้ผู้ใช้สามารถให้ข้อเสนอแนะหรือ Feedback เพื่อรายงานปัญหาให้กับเจ้าของข้อมูลโดยเฉพาะข้อมูลสำคัญ เช่น ข้อมูลหลัก (Master data) และข้อมูลอ้างอิง (Reference data)

7. ข้อกฎหมายและเอกสารอ้างอิง

1) ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม

2) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

3) มาตรฐานรัฐบาลดิจิทัล มรด.3-1 : 2565 ว่าด้วยแนวทางการจัดทำบัญชีข้อมูลภาครัฐ GOVERNMENT DATA CATALOG GUIDELINE เวอร์ชัน 1.0

4) มาตรฐานรัฐบาลดิจิทัล มรด.5 : 2565 ว่าด้วยหลักเกณฑ์การประเมินคุณภาพข้อมูลสำหรับหน่วยงานภาครัฐ DATA QUALITY ASSESSMENT FRAMEWORK for GOVERNMENT AGENCY เวอร์ชัน 1.0

5) มาตรฐานรัฐบาลดิจิทัล มรด.6 : 2566 ว่าด้วยกรอบธรรมาภิบาลข้อมูลภาครัฐ ฉบับปรับปรุง: แนวปฏิบัติ DATA GOVERNANCE FRAMEWORK REVISED : GUILDELINE เวอร์ชัน 2.0

6) มาตรฐานรัฐบาลดิจิทัล มรด.8 : 2567 ว่าด้วยแนวทางการเปิดเผยข้อมูลเปิดภาครัฐในรูปแบบดิจิทัลต่อสาธารณะ OPEN GOVERNMENT DATA GUIDELINE เวอร์ชัน 2.0

7) มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) มสพร. 8-2565 ว่าด้วยหลักเกณฑ์ การจัดระดับชั้นและการแบ่งปันข้อมูลภาครัฐ (GOVERNMENT DATA CLASSIFICATION AND DATA SHARING FRAMEWORK) เวอร์ชัน 1.0

8. ข้อมูลเพิ่มเติม

1) บทบาทและอำนาจ/หน้าที่ของผู้ดูแลบริหารจัดการข้อมูล

บทบาท	อำนาจ/หน้าที่
คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Committee) ประกอบไปด้วย ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer) ผู้บริหารข้อมูลระดับสูง (Chief Data Officer) ผู้บริหารจากส่วนงานต่าง ๆ ทั้งจากฝ่ายบริหารและฝ่ายเทคโนโลยีสารสนเทศที่เกี่ยวข้อง	● มีอำนาจสูงสุดในธรรมาภิบาลข้อมูลภายในหน่วยงาน ทำหน้าที่ตัดสินใจเชิงนโยบาย แก้ไขปัญหา และบริหารจัดการข้อมูลของหน่วยงาน
บรรณาธิการข้อมูล (Editor)	● ดูแลจัดทำข้อมูลของส่วนงานให้พร้อมใช้ ● กำหนดนิยามเมทาดาตา ● ตรวจสอบ ดูแล และรักษาคุณภาพของข้อมูล ● ทำงานร่วมกับบริกรข้อมูล เพื่อตรวจสอบและแก้ไขปัญหาด้านคุณภาพข้อมูลและความปลอดภัยของข้อมูล
เจ้าของข้อมูล (Data Owner)	● ผู้อำนวยการฝ่ายหรือหัวหน้าส่วนงาน ● รับผิดชอบดูแลข้อมูล สร้างความมั่นใจว่าการบริหารจัดการข้อมูลสอดคล้องกับนโยบาย มาตรฐาน กฎระเบียบ หรือกฎหมาย

บทบาท	อำนาจ/หน้าที่
	● ทบทวนและอนุมัติการดำเนินการที่เกี่ยวข้องกับข้อมูล เช่น การเปลี่ยนแปลงเมทาดาตา การเปลี่ยนแปลงข้อมูล ● กำหนดให้สิทธิในการเข้าถึงข้อมูลและจัดชั้นความลับของข้อมูล
ทีมบริกรข้อมูล (Data Steward Team)	● ดำเนินการในเรื่องคุณภาพข้อมูล เช่น กำหนดนโยบายข้อมูลด้านคุณภาพ การตรวจวัดคุณภาพข้อมูล และการวิเคราะห์คุณภาพข้อมูล ● บริหารจัดการข้อมูลให้เป็นไปตามองค์ประกอบในการบริหารจัดการข้อมูล ● ติดตามประเมินผลการจัดการข้อมูล ● ให้คำแนะนำและอบรมบุคลากรในองค์กรเกี่ยวกับการจัดการข้อมูล
ผู้ใช้ข้อมูล (Data User)	● นำข้อมูลไปใช้งานทั้งในระดับปฏิบัติงานและระดับบริหาร ● สนับสนุนการกำกับดูแลข้อมูล ● รายงานประเด็นปัญหาที่พบระหว่างการใช้ข้อมูล ทั้งด้านคุณภาพ และความปลอดภัยของข้อมูล
ผู้บริหารจัดการฐานข้อมูล (Database Administrator)	● บริหารจัดการ และควบคุมเกี่ยวกับระบบฐานข้อมูลภายในหน่วยงาน ● กำหนดนโยบาย มาตรการ และมาตรฐานของระบบฐานข้อมูล ทั้งหมดภายในหน่วยงาน เช่น รายละเอียดและวิธีการจัดเก็บข้อมูล การใช้งานฐานข้อมูล การรักษาความปลอดภัยของข้อมูล การสำรองข้อมูล การกู้คืนข้อมูล เป็นต้น
ผู้ดูแลระบบสารสนเทศ (System Administrators)	● ดูแลและบำรุงรักษาระบบสารสนเทศให้สามารถทำงานได้อย่างสม่ำเสมอ ● กำหนดสิทธิ์การเข้าถึงข้อมูลในระบบต่างๆ ● ตรวจสอบแก้ไขปัญหาที่เกี่ยวกับระบบสารสนเทศ รวมถึงด้านความปลอดภัยไซเบอร์ ● สำรองและกู้คืนข้อมูลเมื่อเกิดเหตุการณ์ฉุกเฉิน หรือข้อมูลสูญหาย ● กำหนดมาตรการความปลอดภัยของระบบ
ผู้ทำลายข้อมูล (Data Disposer)	● ดูแลกระบวนการทำลายข้อมูลที่ไม่จำเป็น หรือหมดอายุการใช้งาน ● เสนอวิธีการและแนวทางการทำลายข้อมูลให้เป็นไปตามนโยบายข้อมูล แก่คณะกรรมการและ

บทบาท	อำนาจ/หน้าที่
	คณะทำงานที่เกี่ยวข้อง โดยพิจารณาความเหมาะสมตามลำดับชั้นข้อมูล หากมีข้อมูลส่วนบุคคลให้ขอความเห็นจาก DPO ก่อนดำเนินการ ● ปฏิบัติตามแนวทางที่ได้รับอนุมัติ และทำให้ข้อมูลไม่สามารถกู้คืนหรือใช้งานได้อีก ● บันทึกและจัดทำรายงานการทำลายข้อมูล

2) ความสัมพันธ์ระหว่างกระบวนการ/กิจกรรมและผู้มีส่วนได้ส่วนเสีย

กระบวนการ/กิจกรรม	ผู้มีส่วนได้ส่วนเสีย							
	คณะกรรมการธรรมาภิบาลข้อมูล	บรรณาธิการข้อมูล	เจ้าของข้อมูล	ทีมบริกรข้อมูล	ผู้ใช้ข้อมูล	ผู้บริหารจัดการฐานข้อมูล	ผู้ดูแลระบบสารสนเทศ	ผู้ทำลายข้อมูล
1. ประเมินความพร้อมของธรรมาภิบาลข้อมูลของหน่วยงาน	I	S	S/C	A/R	S	S	S	S
2. กำหนดนโยบายและแนวทางปฏิบัติการบริหารจัดการข้อมูลของหน่วยงาน	A	I	S	R	I	I	I	I
3. ตรวจสอบการปฏิบัติตามนโยบายและแนวทางปฏิบัติการบริหารจัดการข้อมูลของหน่วยงาน	I	S	R	A/R	S	S	S	S
4. ประเมินและวัดผลข้อมูลของหน่วยงาน	I	S	S	R	S	S	S	S
5. รายงานผลการดำเนินงานต่อคณะกรรมการธรรมาภิบาลข้อมูล	I	I	I	R	I	I	I	R
6. ทบทวนและปรับปรุงนโยบายและแนวทางปฏิบัติการบริหารจัดการข้อมูลของหน่วยงานในภาพรวม	A	I	S	R	I	R	R	I

หมายเหตุ

R (Responsible) หมายถึง ผู้มีหน้าที่ในการปฏิบัติงานตามกระบวนการหรือกิจกรรมที่กำหนดไว้
A (Accountable) หมายถึง ผู้มีหน้าที่ในการทบทวนและอนุมัติผลที่ได้รับจากปฏิบัติงาน
S (Supportive) หมายถึง ผู้ที่มีหน้าที่ในการสนับสนุนหรือให้การช่วยเหลือต่อปฏิบัติงาน
C (Consulted) หมายถึง ผู้ที่ทำหน้าที่ให้คำปรึกษาต่อผู้ปฏิบัติงาน
I (Informed) หมายถึง ผู้ที่ทำหน้าที่รับทราบผลการปฏิบัติงาน