นโยบายและแนวปฏิบัติ การบริหารจัดการข้อมูล

ของ

สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ

นโยบายและแนวปฏิบัติการบริหารจัดการข้อมูล ของสำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ

สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ

คำนำ

ตามแผนพัฒนารัฐบาลดิจิทัลของประเทศไทย พ.ศ. 2563–2565 ยุทธศาสตร์ที่ 1 การยกระดับหน่วยงานภาครัฐไปสู่องค์กรดิจิทัล มีการกำหนดกลยุทธ์ให้ปรับเปลี่ยนข้อมูลปัจจุบันให้เป็นข้อมูลดิจิทัลที่ได้มาตรฐาน โดยให้หน่วยงานภาครัฐจัดทำธรรมาภิบาลข้อมูลภาครัฐหรือมาตรฐานอื่น ๆ ที่เกี่ยวข้อง เพื่อเป็นแนวทางให้หน่วยงานภาครัฐสามารถปรับเปลี่ยนข้อมูลให้อยู่ในรูปแบบดิจิทัลตามหลักธรรมาภิบาล รวมทั้งการสร้างความรู้ความเข้าใจเกี่ยวกับหลักเกณฑ์ แนวทางหรือมาตรฐานการจัดทำข้อมูลดิจิทัล และมีมาตรการสนับสนุนการปรับเปลี่ยนข้อมูลในรูปแบบเอกสาร หรือสำเนากระดาษให้อยู่ในรูปแบบข้อมูลดิจิทัลและติดตามผลการดำเนินงานอย่างต่อเนื่อง ทั้งนี้ โดยเป็นการสมควรกำหนดนโยบายของการกำกับดูแลข้อมูล เพื่อให้เป็นไปตามพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 มาตรา 4 มาตรา 8 มาตรา 12 และกฎเกณฑ์ข้อมูลตามประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ และเพื่อให้มีกรอบนโยบายและแนวปฏิบัติเกี่ยวกับการบริหารจัดการข้อมูลให้ครอบคลุมในด้านต่าง ๆ ของธรรมาภิบาลข้อมูลและการบริหารจัดการข้อมูลภาครัฐ ที่มีประสิทธิภาพ สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ (“สดช.”) จึงได้จัดทำนโยบายและแนวปฏิบัติการบริหารจัดการข้อมูลของสำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ เพื่อให้การบริหารจัดการข้อมูลเป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีคุณภาพ มีความมั่นคงปลอดภัย มีการเชื่อมโยงและสามารถดำเนินงานได้อย่างต่อเนื่องและยั่งยืนต่อไป

สารบัญ

หน้า

คำนำ **1**

สารบัญ **2**

สารบัญตาราง **3**

สารบัญภาพ **4**

นโยบายการบริหารจัดการข้อมูล (Data Management Policy) **5**

1. วัตถุประสงค์ 5
2. ขอบเขตและการบังคับใช้ 5
3. บทบาทและความรับผิดชอบ 6
4. คำนิยาม 6
5. นโยบายการบริหารจัดการข้อมูล 7
6. ข้อกฎหมายและเอกสารอ้างอิง 12
7. ข้อมูลเพิ่มเติม 14

แนวปฏิบัติการบริหารจัดการข้อมูล (Data Management Guideline) **16**

1. คำนิยาม 16
2. หลักการและขอบเขต 17
3. วงจรชีวิตของข้อมูล 18
4. หมวดหมู่และการจัดระดับชั้นของข้อมูล 19
5. ผู้เกี่ยวข้อง 20
6. การเผยแพร่และการทบทวน 21

หมวด 1 การสร้างข้อมูล **22**

หมวด 2 การจัดเก็บข้อมูล **25**

หมวด 3 การประมวลผลข้อมูลและการใช้ข้อมูล **29**

หมวด 4 การเปิดเผยข้อมูล **32**

หมวด 5 การทำลายข้อมูล **36**

หมวด 6 การเชื่อมโยงและการแลกเปลี่ยนข้อมูล **39**

บรรณานุกรม **43**

สารบัญตาราง

หน้า

ตารางที่ 1 บทบาทและความรับผิดชอบของผู้มีส่วนเกี่ยวข้อง 14
ตารางที่ 2 ความสัมพันธ์ระหว่างกระบวนการ/กิจกรรมและผู้มีส่วนได้ส่วนเสีย 15
ตารางที่ 3 มีส่วนได้ส่วนเสียในการสร้างข้อมูล 24
ตารางที่ 4 ผู้มีส่วนได้ส่วนเสียในการประมวลผลและใช้ข้อมูล 31
ตารางที่ 5 ผู้มีส่วนได้ส่วนเสียในการเปิดเผยข้อมูล 35
ตารางที่ 6 มีส่วนได้ส่วนเสียในการทำลายข้อมูล 38
ตารางที่ 7 ผู้มีส่วนได้ส่วนเสียในการเชื่อมโยงและการแลกเปลี่ยนข้อมูล 42

สารบัญภาพ

หน้า

ภาพที่ 1 วงจรชีวิตของข้อมูล 18
ภาพที่ 2 หมวดหมู่ของข้อมูล 19
ภาพที่ 3 ระดับชั้นข้อมูลของ สดช. 20
ภาพที่ 4 แนวปฏิบัติการสร้างข้อมูล 23
ภาพที่ 5 แนวปฏิบัติการจัดเก็บข้อมูล 26
ภาพที่ 6 แนวปฏิบัติการประมวลผลข้อมูลและการใช้ข้อมูล 30
ภาพที่ 7 แนวปฏิบัติการเปิดเผยข้อมูล 33
ภาพที่ 8 แนวปฏิบัติการทำลายข้อมูล 37
ภาพที่ 9 แนวปฏิบัติการเชื่อมโยงและการแลกเปลี่ยนข้อมูล 40

นโยบายการบริหารจัดการข้อมูล (Data Management Policy)

สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ (“สดช.”) มีภารกิจในการดำเนินงานเกี่ยวกับคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ และคณะกรรมการเฉพาะด้าน โดยมีการขับเคลื่อนเศรษฐกิจและสังคมดิจิทัลอย่างยั่งยืนเพื่อยกระดับคุณภาพชีวิตของประชาชน และเพิ่มขีดความสามารถในการแข่งขันในเวทีประชาคมโลก เพื่อให้เป็นไปตามพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 รวมถึงกฎหมายที่เกี่ยวข้อง โดยให้ครอบคลุมการบริหารจัดการและการบูรณาการ ตลอดจนให้เกิดความสอดคล้องกับกรอบธรรมาภิบาลข้อมูลภาครัฐ จึงเห็นสมควรกำหนดนโยบายข้อมูล โดยกำหนดให้มีนโยบาย (Policies) มาตรฐาน (Standard) แนวปฏิบัติ (Guideline) ขั้นตอนการปฏิบัติงาน (Procedure) และวิธีการปฏิบัติ (Work Instruction) ให้ครอบคลุมในด้านต่าง ๆ ของธรรมาภิบาลข้อมูลและการบริหารจัดการข้อมูล

1. วัตถุประสงค์

1. เพื่อให้การบริหารจัดการข้อมูลของ สดช. สอดคล้องกับกฎหมาย กรอบธรรมาภิบาลข้อมูลภาครัฐ และระเบียบปฏิบัติที่เกี่ยวข้อง

2. เพื่อใช้เป็นกรอบและแนวทางในการบริหารจัดการข้อมูลของหน่วยงาน สำหรับผู้บริหาร เจ้าหน้าที่ สดช. และผู้ที่เกี่ยวข้อง

3. เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติ และวิธีการปฏิบัติให้แก่ผู้บริหาร เจ้าหน้าที่ ลูกจ้าง และผู้ที่เกี่ยวข้องให้เกิดความตระหนักถึงความสำคัญของธรรมาภิบาลข้อมูลและการบริหารจัดการข้อมูลและปฏิบัติตามอย่างเคร่งครัด

4. เพื่อใช้เป็นหลักในการพัฒนาและปรับปรุงธรรมาภิบาลข้อมูลและการบริหารจัดการข้อมูลเพื่อให้ข้อมูลมีคุณภาพ และมีความมั่นคงปลอดภัยตามหลักมาตรฐานสากล

2. ขอบเขตและการบังคับใช้

1. การจัดทำนโยบายการดำเนินการด้านธรรมาภิบาลข้อมูลมีขอบเขตครอบคลุมการบริหารจัดการข้อมูลให้เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีคุณภาพ มีความมั่นคงปลอดภัย มีการเชื่อมโยงและสามารถดำเนินงานได้อย่างต่อเนื่องและยั่งยืน

2. นโยบายนี้จะต้องทำการเผยแพร่ให้เจ้าหน้าที่ทุกระดับใน สดช. ได้รับทราบ และเจ้าหน้าที่ทุกคนจะต้องถือปฏิบัติตามนโยบายอย่างเคร่งครัด

3. นโยบายนี้ต้องมีการดำเนินการตรวจสอบและประเมินผลการปฏิบัติเพื่อปรับนโยบายตามระยะเวลา 1 ครั้งต่อปี

3. บทบาทและความรับผิดชอบ

1. หัวหน้าหน่วยงานของรัฐหรือผู้ที่ได้รับมอบหมายต้องควบคุมและกำกับดูแลให้บุคลากรในหน่วยงาน และผู้ที่เกี่ยวข้องดำเนินการตามนโยบายการบริหารจัดการข้อมูลอย่างเคร่งครัด

2. ผู้บังคับบัญชา/ผู้ที่ได้รับมอบหมายต้องตรวจสอบให้แน่ใจว่าบุคลากรในหน่วยงานและบุคคลอื่น ๆ เช่น บริษัทหรือผู้รับจ้าง ที่ได้รับมอบหมายจากหน่วยงานให้ทำหน้าที่บริหารจัดการข้อมูลได้รับความรู้เกี่ยวกับนโยบายนี้อย่างเหมาะสม และนำนโยบายไปปฏิบัติตามอย่างมีประสิทธิภาพและประสิทธิผล บุคลากรในหน่วยงานและบุคคลอื่น ๆ เช่น บริษัทหรือผู้รับจ้าง ที่ได้รับมอบหมายจากหน่วยงานให้ทำหน้าที่บริหารจัดการข้อมูลต้องปฏิบัติตามนโยบาย มาตรการ วิธีการ และแนวปฏิบัติต่าง ๆ ที่เกี่ยวข้องกับข้อมูลและระบบข้อมูลสารสนเทศที่หน่วยงานกำหนด

3. คณะกรรมการธรรมาภิบาลข้อมูล/คณะทำงานด้านข้อมูล/เจ้าของข้อมูลและผู้ดูแลข้อมูลต้องปฏิบัติหน้าที่ที่ได้รับมอบหมายภายใต้นโยบายนี้ (รายละเอียดตามข้อ 7)

4. คำนิยาม

1. ข้อมูล (Data) หมายถึง สิ่งที่สื่อความหมายให้รู้เรื่องราวข้อเท็จจริงหรือเรื่องอื่นใด ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเอง หรือโดยผ่านวิธีการใด ๆ และไม่ว่าจะได้จัดทำไว้ในรูปของ เอกสารแฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ภาพถ่ายดาวเทียม ฟิล์ม การบันทึกภาพหรือ เสียง การบันทึกโดยเครื่องคอมพิวเตอร์ เครื่องมือตรวจวัด การสำรวจระยะไกล หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้

2. ชุดข้อมูล (Dataset) คือ การนำข้อมูลจากหลายแหล่งมารวบรวม เพื่อจัดเป็นชุดให้ตรงตามลักษณะโครงสร้างของข้อมูล

3. บัญชีข้อมูล (Data Catalog) คือ เอกสารแสดงบรรดารายการของชุดข้อมูล ที่จำแนกแยกแยะโดยการจัดกลุ่มหรือจัดประเภทข้อมูลที่อยู่ในความครอบครองหรือควบคุมของสำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ

4. ธรรมาภิบาลข้อมูลภาครัฐ (Data Governance for Government) หมายถึง การกำหนดสิทธิ หน้าที่ และความรับผิดชอบของผู้มีส่วนได้เสียในการบริหารจัดการข้อมูลทุกขั้นตอน เพื่อให้การได้มาและการนำไปใช้ข้อมูลของหน่วยงานภาครัฐถูกต้อง ครบถ้วน เป็นปัจจุบัน รักษาความเป็นส่วนตัว และสามารถเชื่อมโยงกันได้อย่างมีประสิทธิภาพและมั่นคงปลอดภัย

5. หมวดหมู่ของข้อมูล (Data Category) ตามกรอบธรรมาภิบาลข้อมูลภาครัฐแบ่งออกได้เป็น 4 หมวดหมู่ ได้แก่ ข้อมูลส่วนบุคคล ข้อมูลความมั่นคง ข้อมูลความลับทางราชการ และข้อมูลสาธารณะ

6. การจัดชั้นความลับของข้อมูล คือ การกำหนดประเภทและข้อกำหนดของการจัดชั้นความลับของข้อมูล เพื่อกำหนดสิทธิในการเข้าถึงและสามารถนำข้อมูลไปใช้ได้อย่างเหมาะสม ซึ่งตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 กำหนดให้มีชั้นความลับเป็น ชั้นลับ ชั้นลับมาก หรือชั้นลับที่สุด

โดยคำนึงถึงการปฏิบัติหน้าที่ของหน่วยงานและประโยชน์แห่งรัฐประกอบกัน ดังนั้น ชั้นความลับของข้อมูลมักถูกกำหนดให้สอดคล้องกับผลกระทบต่อหน่วยงานและความมั่นคงของประเทศ อาทิ ชื่อเสียง ความต่อเนื่องของการดำเนินงาน การเงิน และทรัพยากรบุคคล

7. วงจรชีวิตของข้อมูล (Data Life Cycle) คือ ลำดับขั้นตอนของข้อมูลตั้งแต่เริ่มสร้างข้อมูลไปจนถึงการทำลายข้อมูล ตามกรอบธรรมาภิบาลข้อมูลภาครัฐ

8. ข้อมูลหลักและข้อมูลอ้างอิง (Master and Reference Data) เป็นการบริหารจัดการข้อมูลเพื่อให้ทั้งหน่วยงานสามารถเข้าถึงและใช้ข้อมูลร่วมกันได้ โดยข้อมูลถูกจัดเก็บไว้แหล่งเดียว มีการกำหนดมาตรฐานของข้อมูล เพื่อช่วยลดความซ้ำซ้อนของข้อมูลและทำให้ข้อมูลมีคุณภาพ ซึ่ง Master data เป็นข้อมูลที่สร้างและถูกใช้งานอยู่ภายในหน่วยงาน มีโอกาสเปลี่ยนแปลงได้และมีรายละเอียดหรือจำนวนฟิลด์ข้อมูลที่มาก เช่น ข้อมูลพนักงาน ข้อมูลลูกค้า ข้อมูลผู้ขาย ข้อมูลสินค้าและบริการ ข้อมูลครุภัณฑ์ และข้อมูลสถานที่ ในขณะที่ Reference data มีความเป็นสากลถูกสร้างและใช้งานโดยทั่วไปโดยหลากหลายองค์กร หรือแม้กระทั่งใช้งานไปทั่วโลก เช่น รหัสไปรษณีย์ รหัสประเทศ หน่วยวัดระยะทาง

5. นโยบายการบริหารจัดการข้อมูล

5.1 ข้อกำหนดทั่วไป

นโยบาย

1) กำหนดให้มีโครงสร้างคณะกรรมการธรรมาภิบาลข้อมูล และกำหนดบทบาท หน้าที่และความรับผิดชอบของแต่ละบุคคลตามโครงสร้างธรรมาภิบาลข้อมูลภาครัฐ โดยต้องได้รับการมอบอำนาจและการอนุมัติจากผู้บริหาร พร้อมทั้งกำหนดหน่วยงานที่เป็นเจ้าของข้อมูล เพื่อทำหน้าที่ในการบริหารจัดการข้อมูลนั้น ๆ

2) กำหนดมาตรฐาน (Data Standard) และระเบียบปฏิบัติมาตรฐานและการบริหารจัดการคำอธิบายชุดข้อมูล (Metadata) ครอบคลุมบทบาทหน้าที่ความรับผิดชอบ กระบวนการจัดทำคำอธิบายชุดข้อมูลการควบคุมดูแลและสอบทานคำอธิบายชุดข้อมูล

3) จัดทำนโยบายการบริหารจัดการข้อมูลเป็นลายลักษณ์อักษร อนุมัติเผยแพร่เพื่อประกาศใช้และถือปฏิบัติ โดยให้มีผลบังคับใช้กับบุคลากรในหน่วยงาน ตลอดจนหน่วยงาน/บุคคลภายนอกที่เกี่ยวข้องกับการได้มาและการใช้ข้อมูลของหน่วยงาน พร้อมทั้งจัดทำแนวปฏิบัติและมาตรฐานที่เกี่ยวกับข้อมูลเพื่อสนับสนุนการปฏิบัติงานให้สอดคล้องตามนโยบายดังกล่าว

4) กำหนดมาตรการ วิธีการ และแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของข้อมูลเพื่อป้องกันการละเมิด การเข้าถึง การสูญหาย การทำลาย หรือการเปลี่ยนแปลงข้อมูล โดยปราศจากอำนาจโดยมิชอบหรือโดยมิได้รับอนุญาต (อ้างอิงตามนโยบายความมั่นคงปลอดภัยสารสนเทศของ สดช. หรือเป็นไปตามมาตรฐานสากล)

5) กำหนดมาตรการ วิธีการ และแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลที่สอดคล้องกับกฎหมาย ระเบียบ และแนวปฏิบัติของหน่วยงาน (อ้างอิงตามนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) ของ สดช. และเป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562)

6) ตรวจสอบความมีอยู่และรายละเอียดของข้อมูลที่สำคัญ เช่น คำอธิบายข้อมูลหรือเมทาดาตา ชุดข้อมูล การจัดชั้นความลับข้อมูล และรายงานผลให้แก่ผู้รับผิดชอบตามโครงสร้างธรรมาภิบาลข้อมูลภาครัฐและดำเนินการตามกระบวนการธรรมาภิบาลข้อมูลภาครัฐ

7) ตรวจสอบ ติดตาม และประเมินผลการปฏิบัติตามนโยบายการบริหารจัดการข้อมูลโดยผู้ตรวจประเมินที่คณะกรรมการธรรมภิบาลข้อมูลของ สดช. กำหนด พร้อมทั้งกำหนดให้มีการทบทวนนโยบาย รวมถึง มาตรการ วิธีการ และแนวปฏิบัติต่าง ๆ เกี่ยวกับข้อมูล อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญตามความเหมาะสม

8) ตรวจสอบ ติดตาม และประเมินผลการดำเนินงานธรรมาภิบาลข้อมูลของหน่วยงานอย่างน้อยปีละ 1 ครั้ง ในเรื่อง (1) การประเมินความพร้อมธรรมาภิบาลข้อมูล (2) การประเมินคุณภาพข้อมูล และ (3) การประเมินความมั่นคงปลอดภัยของข้อมูล เป็นอย่างน้อย (อ้างอิงตามมาตรฐานและหลักเกณฑ์ที่ สพร. กำหนด หรือ เป็นไปตามมาตรฐานสากล)

9) จัดให้มีทรัพยากรด้านงบประมาณ ทรัพยากรบุคคล และเทคโนโลยีที่เพียงพอต่อการบริหารจัดการข้อมูล พร้อมทั้งสนับสนุนการฝึกอบรมธรรมาภิบาลข้อมูลภาครัฐและการบริหารจัดการข้อมูลให้ครอบคลุมทั้งวงจรชีวิตของข้อมูลแก่บุคลากรของ สดช. อย่างน้อยปีละ 1 ครั้ง

5.2 การจัดหมวดหมู่และชั้นความลับของข้อมูล

<u>นโยบาย</u>

1) กำหนดหมวดหมู่และประเภทชั้นความลับของข้อมูลที่ใช้กับข้อมูลทุกรูปแบบของหน่วยงาน ทั้งเอกสารกระดาษและข้อมูลดิจิทัล ด้วยการประเมินผลกระทบของข้อมูลหน่วยงาน เพื่อระบุหมวดหมู่และประเภทชั้นความลับของข้อมูล รวมทั้งกำหนดระดับความปลอดภัยที่เหมาะสมสำหรับการสร้าง/จัดเก็บ การใช้ และการเข้าถึงชุดข้อมูล และเพื่อใช้กับบุคลากรรวมถึงตัวแทนบุคคลที่สามที่ได้รับอนุญาตให้เข้าถึงข้อมูลในหน่วยงาน พร้อมทั้งกำหนดบทบาทหน้าที่ของบุคลากรในการจัดหมวดหมู่และชั้นความลับ เพื่อป้องกัน จัดการ และกำกับดูแลข้อมูลให้เหมาะสม

2) ติดป้ายกำกับชุดข้อมูล (Labeling/Tagging Dataset) ตามผลประเมินและระบุหมวดหมู่และประเภทชั้นความลับอย่างเหมาะสม และป้ายกำกับสำรองชั้นความลับข้อมูล (ถ้ามี) เช่น ลับ ลับมาก ลับที่สุด เป็นต้น เพื่อจำแนกความแตกต่างของชุดข้อมูลภายในหน่วยงานหรือแนวปฏิบัติตามข้อกำหนดอื่น ๆ

3) กำหนดแนวปฏิบัติและมาตรฐานของการประมวลผลข้อมูล และทำการสื่อสารให้แก่ผู้ที่เกี่ยวข้องรับทราบ

4) ห้ามเปิดเผยข้อมูลที่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง หลักเกณฑ์ นโยบายและแนวปฏิบัติของ สดช. ที่ประกาศใช้ในปัจจุบัน ไม่ว่าข้อมูลจะอยู่ในรูปแบบใดหรือสถานที่ใดก็ตาม

5) การดำเนินการประมวลผลข้อมูลที่เป็นความลับ เช่น ข้อมูลส่วนบุคคล ให้เป็นไปตามขอบเขตเงื่อนไขหรือวัตถุประสงค์ในการยินยอมให้ดำเนินการกับข้อมูลส่วนบุคคลนั้น

6) ต้องมีการเก็บบันทึกประวัติการเข้าถึงและการใช้ข้อมูล (Log Files) เพื่อให้สามารถตรวจสอบย้อนกลับได้

7) คณะบริกรข้อมูล เจ้าของข้อมูล และผู้มีส่วนได้ส่วนเสียกับข้อมูลที่เกี่ยวข้องต้องร่วมกันจัดทำเมทาดาตาพร้อมคำอธิบาย (Metadata) สำหรับข้อมูลที่จัดเก็บอยู่ในฐานข้อมูล (Database) ในทุกชุดข้อมูล

8) กำกับดูแลและติดตามอย่างต่อเนื่อง โดยตรวจสอบความปลอดภัยการใช้งานและรูปแบบการเข้าถึงของระบบและข้อมูล ทั้งผ่านกระบวนการอัตโนมัติหรือโดยบุคคล เพื่อระบุภัยคุกคามภายนอก การบำรุงรักษา การทำงานของระบบตามปกติ และการติดตั้งโปรแกรมเพื่อปรับปรุงและติดตามการเปลี่ยนแปลงของสภาพแวดล้อมของระบบและข้อมูล

9) ต้องมีการทบทวนระดับชั้นความลับข้อมูล อย่างน้อยปีละ 1 ครั้ง และให้ดำเนินการปรับปรุงอย่างต่อเนื่อง

5.3 การบริหารจัดการข้อมูลตามวงจรชีวิตของข้อมูล

นโยบาย

1) กำหนดนโยบาย แนวปฏิบัติ และสภาพแวดล้อมการบริหารจัดการข้อมูลตามวงจรชีวิตของข้อมูลที่เอื้อต่อการรักษาความมั่นคงปลอดภัย คุ้มครองความเป็นส่วนตัวของข้อมูล และเพื่อให้ได้ข้อมูลที่มีคุณภาพ

2) จัดทำแนวปฏิบัติการจัดการชุดข้อมูล รวมถึงการรักษาความปลอดภัยตามหมวดหมู่และประเภทชั้นความลับตามแนวทางที่เหมาะสม และปรับปรุงอย่างต่อเนื่องให้สอดคล้องกับสถานการณ์

3) จัดเก็บข้อมูลให้สอดคล้องกับแนวทางหรือมาตรฐานการจัดชั้นความลับของข้อมูลที่กำหนดไว้ โดยข้อมูลต้องมีความถูกต้อง สมบูรณ์ และเป็นปัจจุบัน พร้อมทั้งกำหนดสิทธิและจัดหาระบบ/เครื่องมือ ที่ใช้ในการเข้าถึงข้อมูลเพื่อรักษาความมั่นคงปลอดภัยและคุณภาพข้อมูล และทำลายข้อมูลตามแนวปฏิบัติและกฎหมายที่เกี่ยวข้อง

4) จัดทำแนวปฏิบัติและมาตรฐานการประมวลผลและใช้ข้อมูล เพื่อผู้ใช้นำข้อมูลไปใช้อย่างถูกต้องตามวัตถุประสงค์ที่ต้องการเพื่อให้เกิดประโยชน์สูงสุด

5) ห้ามเปิดเผยข้อมูลที่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง นโยบาย และแนวปฏิบัติ ไม่ว่าข้อมูลจะอยู่ในรูปแบบใดหรือสถานที่ใดก็ตาม และต้องได้รับการอนุญาตจากตัวแทนหน่วยงานหรือเจ้าของข้อมูลก่อนการเปิดเผยข้อมูล รวมทั้งจัดให้มีช่องทางการเปิดเผยข้อมูลที่เข้าถึงและนำไปใช้ได้ง่าย (อ้างอิงตามมาตรฐานและหลักเกณฑ์ที่ สดช. กำหนด หรือเป็นไปตามมาตรฐานสากล)

6) กำหนดกระบวนการ เทคโนโลยี และมาตรฐานทางเทคนิคที่ใช้ในการแลกเปลี่ยนข้อมูลและจัดทำสัญญาอนุญาตหรือข้อตกลงในการแลกเปลี่ยนข้อมูลและการนำข้อมูลไปใช้

7) จัดทำแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัย ด้านคุณภาพข้อมูล และด้านคุ้มครองความเป็นส่วนตัวของข้อมูล รวมถึงแนวปฏิบัติให้กับผู้ประสานงานหรือศูนย์ติดต่อ (Contact Center) และตรวจสอบให้แน่ใจว่าได้บริหารจัดการข้อมูลอย่างเหมาะสมตามแนวทางหรือแนวปฏิบัติที่กำหนดไว้

8) สร้างความรู้ความเข้าใจในการบริหารจัดการข้อมูลตามวงจรชีวิตของข้อมูล ให้แก่ผู้เกี่ยวข้องทั้งภายในและภายนอกหน่วยงาน

5.4 คุณภาพข้อมูล

นโยบาย

1) กำหนดนโยบายการจัดการคุณภาพข้อมูล เพื่อใช้เป็นกรอบแนวทางในการจัดการข้อมูลของหน่วยงานให้มีคุณภาพเป็นตามเกณฑ์หรือคุณสมบัติที่กำหนด เช่น ความถูกต้องสมบูรณ์ ความสอดคล้องกัน (Consistency) ความเป็นปัจจุบัน (Timeliness) ตรงตามความต้องการใช้งาน และความพร้อมใช้ เป็นต้น โดยผู้ดูแลข้อมูล มีหน้าที่จัดการและกำกับดูแลข้อมูลให้มีคุณภาพเพื่อสร้างความมั่นใจให้กับผู้ใช้ข้อมูล ในขณะที่ผู้ใช้ข้อมูล มีบทบาทในการให้ข้อเสนอแนะแก่ผู้ดูแลข้อมูลเพื่อการปรับปรุงคุณภาพให้ดียิ่งขึ้น

2) กำหนดมาตรฐานข้อมูลให้เป็นแบบเดียวกัน และมีการควบคุมคุณภาพข้อมูลตลอดทั้งวงจรชีวิตข้อมูล (Data Life Cycle) ของข้อมูลที่ตนเองมีหน้าที่รับผิดชอบนั้น

3) กำหนดให้มีข้อกำหนดพื้นฐานของการบริหารจัดการคุณภาพข้อมูล (Data Quality Management) รวมถึงแนวทางการควบคุมและการปรับปรุงอย่างต่อเนื่อง

4) การกำหนดตัวชี้วัดคุณภาพข้อมูล เช่น ความถูกต้อง ความครบถ้วน ความต้องกัน ความเป็นปัจจุบันตรงตามความต้องการของผู้ใช้และพร้อมใช้งาน

5) จัดทำเกณฑ์คุณภาพข้อมูลที่สามารถวัดผลได้ พร้อมทั้งจัดทำแผนพัฒนาคุณภาพข้อมูลที่สามารถระบุตัวชี้วัดคุณภาพและแผนปฏิบัติการเพื่อจัดการคุณภาพข้อมูลได้อย่างมีประสิทธิภาพ โดยออกแบบการเก็บรวบรวมข้อมูลเพื่อให้ได้ข้อมูลสำหรับประเมินคุณภาพตามเกณฑ์ดังกล่าวให้รวมอยู่ในระบบเทคโนโลยีสารสนเทศและกระบวนการทำงาน (Quality by design) เพื่อลดข้อผิดพลาดและปรับปรุงคุณภาพตั้งแต่จุดการป้อนข้อมูลหรือการสร้างข้อมูลไปจนถึงการประมวลผลข้อมูล (อ้างอิงตามมาตรฐานและหลักเกณฑ์ที่ สพร. หรือเป็นไปตามมาตรฐานสากล)

6) รายงานคุณภาพข้อมูล ประกอบด้วยการกำหนดระดับมิติตัวชี้วัด และค่าเป้าหมายในการประเมินคุณภาพข้อมูลจะต้องแนบไปกับการใช้ชุดข้อมูล (Dataset) และชุดคำอธิบายข้อมูล

7) ประเมินผลและจัดการคุณภาพข้อมูลอย่างสม่ำเสมอตลอดวงจรชีวิตของข้อมูล โดยเจ้าของข้อมูล และคณะบริกรข้อมูลควรกำหนดกรอบคุณภาพข้อมูลเฉพาะหมวดหมู่ข้อมูลหรือโดเมน (Domain) เช่น Quality Assurance Framework of the European Statistical System (ESS. QAF) ที่เป็นกรอบคุณภาพข้อมูลสถิติของ the European Statistical System ที่สามารถนำมาใช้อ้างอิงได้

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

5.5 การเชื่อมโยงและแลกเปลี่ยนข้อมูล

นโยบาย

1) กำหนดแนวปฏิบัติในการจัดการเรื่องความมั่นคงปลอดภัย คุณภาพข้อมูล และผู้ประสานงานหรือศูนย์ติดต่อ (Contact Center)

2) กำหนดกระบวนการในการเชื่อมโยงและแลกเปลี่ยนข้อมูลให้ชัดเจน เริ่มตั้งแต่ขั้นตอนการเตรียมการ ขั้นตอนเริ่มดำเนินการ ขั้นตอนระหว่างดำเนินการ และขั้นตอนสิ้นสุดการดำเนินการ

3) กำหนดเมทาดาตาของชุดข้อมูลที่ต้องการเชื่อมโยงและแลกเปลี่ยนที่จำเป็นให้ครบถ้วน

4) ทำสัญญาอนุญาต บันทึกข้อตกลง (Memorandum of Understanding : MOU) สัญญารักษาความลับ (Non-Disclosure Agreement : NDA) หรือข้อตกลงอื่นใดว่าด้วยการเชื่อมโยงข้อมูลของ สดช. หรือข้อตกลงในการแลกเปลี่ยนข้อมูลและการนำข้อมูลไปใช้

5) กำหนดเทคโนโลยีและมาตรฐานทางเทคนิคที่ใช้ในการแลกเปลี่ยนและเชื่อมโยงข้อมูล รวมถึงการรักษาความมั่นคงปลอดภัยของข้อมูล ให้เป็นไปตามมาตรฐานและกฎหมายที่เกี่ยวข้อง

6) ให้มีการตรวจสอบการสอดคล้องกัน (Integrity) ของข้อมูลระหว่างหน่วยงานที่เกี่ยวข้อง

7) บันทึกรายละเอียดและจัดเก็บข้อมูลการดำเนินงานที่เกิดขึ้นในแต่ละครั้งที่มีการเชื่อมโยงและแลกเปลี่ยนข้อมูล (Log File) ระหว่างหน่วยงาน เพื่อให้สามารถตรวจสอบย้อนกลับได้

8) สามารถตรวจสอบได้ว่าการเชื่อมโยงและแลกเปลี่ยนข้อมูลได้ดำเนินการอย่างเหมาะสมหรือเป็นไปตามแนวทางปฏิบัติ กระบวนการการเชื่อมโยงและแลกเปลี่ยน และมาตรฐานตามที่กำหนด

9) ตรวจสอบชั้นความลับของข้อมูล (Data Classification) ว่าอยู่ในชั้นความลับที่สามารถเปิดเผยได้หรือไม่ เช่น ไม่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ ความมั่นคงของประเทศ ความลับทางราชการ และความเป็นส่วนบุคคล เป็นต้น พร้อมทั้งตรวจสอบสิทธิของหน่วยงานที่สามารถนำข้อมูลไปใช้ได้ตามบทบาทและภารกิจตามกฎหมายของหน่วยงานนั้น ๆ

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

5.6 นโยบายการเปิดเผยข้อมูล

นโยบาย

1) ห้ามเปิดเผยข้อมูลที่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง หลักเกณฑ์ นโยบาย แนวปฏิบัติของ สดช. ที่ประกาศใช้ในปัจจุบัน ไม่ว่าข้อมูลจะอยู่ในรูปแบบใดหรือสถานที่ใดก็ตาม

2) การเปิดเผยข้อมูลต้องได้รับความยินยอมจากเจ้าของข้อมูล

3) ให้มีการจัดเตรียมข้อมูลที่อยู่ในรูปแบบที่ง่ายต่อการนำไปใช้

4) ให้มีการคัดเลือกชุดข้อมูลที่ต้องการเผยแพร่

5) ให้มีการระบุช่องทางการเปิดเผยข้อมูลที่เข้าถึงและนำไปใช้ได้ง่าย

6) ให้มีการเปิดเผยคำอธิบายชุดข้อมูล (Metadata) ควบคู่ไปกับข้อมูลที่เปิดเผย

7) ให้สามารถตรวจสอบว่าการเปิดเผยข้อมูลได้ถูกดำเนินการอย่างเหมาะสมหรือเป็นไปตามแนวทางที่ได้กำหนดไว้

8) ให้มีการกำหนดผู้รับผิดชอบหลัก ขั้นตอน และวิธีการนำชุดข้อมูลขึ้นเผยแพร่สู่สาธารณะ

9) เก็บประวัติการเปิดเผยข้อมูล เพื่อให้สามารถตรวจสอบ ติดตามการดำเนินงานให้มีคุณภาพและเป็นไปอย่างเหมาะสม

10) ต้องปฏิบัติตามอย่างเคร่งครัด และป้องกันมิให้มีการเปิดเผยข้อมูล โดยไม่ได้รับอนุญาต

6. ข้อกฎหมายและเอกสารอ้างอิง

1) พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562
2) พระราชบัญญัติการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม พ.ศ. 2560
3) พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
4) พระราชบัญญัติการอำนวยความสะดวกในการพิจารณาอนุญาตของทางราชการ พ.ศ. 2558
5) พระราชบัญญัติข้อมูลข่าวกรองแห่งชาติ พ.ศ. 2562
6) พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540
7) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
8) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม
9) พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544
10) พระราชกฤษฎีการกำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549
11) พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553
12) ระเบียบสำนักนายกรัฐมนตรีว่าด้วยงานสารบรรณ พ.ศ. 2526 และที่แก้ไขเพิ่มเติม
13) ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม

14) ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ ลงวันที่ 12 มีนาคม พ.ศ. 2563

15) ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง มาตรฐานและหลักเกณฑ์การเปิดเผยข้อมูลเปิดภาครัฐในรูปแบบข้อมูลดิจิทัลต่อสาธารณะ ลงวันที่ 11 มิถุนายน พ.ศ. 2563

16) ประกาศ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ที่ 3/2564 เรื่อง มาตรฐานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ว่าด้วยแนวทางการจัดทำบัญชีข้อมูลภาครัฐ (มสพร. 1-2564)

17) ประกาศ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ที่ 4/2564 เรื่อง นโยบายความมั่นคงปลอดภัยสารสนเทศของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

18) ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2564

19) ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ แก้ไขเพิ่มเติมถึง (ฉบับที่ ๒) พ.ศ. ๒๕๕๖

20) มาตรฐานรัฐบาลดิจิทัล ว่าด้วย กรอบแนวทางการพัฒนามาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ (THAILAND GOVERNMENT INFORMATION EXCHANGE STANDARD DEVELOPMENT FRAMEWORK) พ.ศ. 2565

21) ชุดเอกสารแม่แบบ (template) สำหรับการดำเนินการของผู้ดูแลข้อมูลส่วนบุคคลภาครัฐ (Version 1.0) จัดทำโดย สพร.

7. ข้อมูลเพิ่มเติม

7.1 การกำหนดบทบาทและความรับผิดชอบของผู้มีส่วนเกี่ยวข้อง

ตารางที่ 1 บทบาทและความรับผิดชอบของผู้มีส่วนเกี่ยวข้อง

บทบาท	ความรับผิดชอบ
คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Committee)	• ประกอบไปด้วย ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer) ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer) ผู้บริหารข้อมูลระดับสูง (Chief Data Officer) ผู้บริหารด้านการรักษาความปลอดภัยระดับสูง (Chief Security Officer) ผู้บริหารจากส่วนงานต่าง ๆ ทั้งจากฝ่ายบริหารและฝ่ายเทคโนโลยีสารสนเทศ รวมไปถึงหัวหน้าคณะบริกรข้อมูล (Lead Data Steward) • มีอำนาจสูงสุดในธรรมาภิบาลข้อมูลภายในหน่วยงาน ทำหน้าที่ตัดสินใจเชิงนโยบาย แก้ไขปัญหา และบริหารจัดการข้อมูลของหน่วยงาน ทั้งนี้ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงอาจจะทำหน้าที่แทนผู้บริหารข้อมูลระดับสูง
คณะบริกรข้อมูล (Data Stewards)	ดำเนินการกำกับดูแล ติดตาม และรายงานผลการดำเนินการธรรมาภิบาลข้อมูล ประกอบด้วย • บริหารจัดการ ควบคุมการดำเนินงานตามนโยบายจากคณะกรรมการธรรมาภิบาลข้อมูล • ติดตามการดำเนินงานและข้อเสนอแนะ เพื่อเป็นข้อมูลให้แก่ผู้บริหารระดับสูงด้านข้อมูลหรือคณะกรรมการธรรมาภิบาลข้อมูล • ตรวจสอบความสอดคล้องกันระหว่างนโยบายกับการดำเนินการต่อข้อมูล ตรวจสอบคุณภาพข้อมูล วิเคราะห์ผลจากการตรวจสอบและรายงานผลไปยังคณะกรรมการธรรมาภิบาลข้อมูลและผู้ที่เกี่ยวข้องอื่น ๆ • ประสานงานในปัญหาด้านข้อมูลจากบุคลากรในส่วนงานเดียวกัน โดยทั้งหมดนี้จะควบคุมผ่านคณะกรรมการธรรมาภิบาลข้อมูล
เจ้าของข้อมูล (Data Owner)	• ตรวจสอบ ดูแล และรักษาคุณภาพของข้อมูล • ทบทวนและอนุมัติการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับข้อมูล
ผู้สร้างข้อมูล (Data Creator)	• บันทึก แก้ไข ปรับปรุง หรือลบข้อมูลให้สอดคล้องกับโครงสร้างที่ถูกกำหนดไว้ • ทำงานร่วมกับคณะบริกรข้อมูล เพื่อตรวจสอบและแก้ไขปัญหาด้านคุณภาพข้อมูลและความปลอดภัยของข้อมูล
ผู้ใช้ข้อมูล (Data User)	• นำข้อมูลไปใช้งานทั้งในระดับปฏิบัติงานและระดับบริหาร • สนับสนุนการกำกับดูแลข้อมูล • รายงานประเด็นปัญหาที่พบระหว่างการใช้ข้อมูล ทั้งด้านคุณภาพ และความปลอดภัยของข้อมูล

7.2 ความสัมพันธ์ระหว่างกระบวนการ/กิจกรรมและผู้มีส่วนได้ส่วนเสีย

ตารางที่ 2 ความสัมพันธ์ระหว่างกระบวนการ/กิจกรรมและผู้มีส่วนได้ส่วนเสีย

กิจกรรม	ผู้มีส่วนได้ส่วนเสีย				
	คณะกรรมการธรรมาภิบาลข้อมูล	คณะบริกรข้อมูล	เจ้าของข้อมูล	ผู้สร้างข้อมูล	ผู้ใช้ข้อมูล
1. ประเมินความพร้อมของธรรมาภิบาลข้อมูลของหน่วยงาน	I	A/R	S/C	S	S
2. กำหนดนโยบายและแนวทางปฏิบัติการบริหารจัดการข้อมูลของหน่วยงาน	A	R	S	I	I
3. ตรวจสอบการปฏิบัติตามนโยบายและแนวทางปฏิบัติการบริหารจัดการข้อมูลของหน่วยงาน	I	A/R	R	S	S
4. ประเมินและวัดผลข้อมูลของหน่วยงาน	I	R	S	S	S
5. รายงานผลการดำเนินงานต่อคณะกรรมการธรรมาภิบาลข้อมูล	I	A/R	I	I	I
6. ทบทวนและปรับปรุงนโยบายและแนวทางปฏิบัติการบริหารจัดการข้อมูลของหน่วยงานในภาพรวม	A	R	S	I	I

หมายเหตุ

R (Responsible) หมายถึง ผู้มีหน้าที่ในการปฏิบัติงานตามกระบวนการหรือกิจกรรมที่กำหนดไว้

A (Accountable) หมายถึง ผู้มีหน้าที่ในการทบทวนและอนุมัติผลที่ได้รับจากปฏิบัติงาน

S (Supportive) หมายถึง ผู้ที่มีหน้าที่ในการสนับสนุนหรือให้การช่วยเหลือต่อปฏิบัติงาน

C (Consulted) หมายถึง ผู้ที่ทำหน้าที่ให้คำปรึกษาต่อผู้ปฏิบัติงาน

I (Informed) หมายถึง ผู้ที่ทำหน้าที่รับทราบผลการปฏิบัติงาน

แนวปฏิบัติการบริหารจัดการข้อมูล (Data Management Guideline)

1. คำนิยาม

1. “สดช.” หมายความว่า สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ

2. “คณะกรรมการ” หมายความว่า คณะกรรมการธรรมาภิบาลข้อมูลสำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ

3. “ข้อมูล” หมายความว่า สิ่งที่สื่อความหมายให้รู้เรื่องราวข้อเท็จจริง หรือเรื่องอื่นใด ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใด ๆ และไม่ว่าจะได้จัดทำไว้ในรูปของเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ภาพถ่ายดาวเทียม ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ เครื่องมือตรวจวัด การสำรวจระยะไกล หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้

4. “ชุดข้อมูล” หมายความว่า การนำข้อมูลจากหลายแหล่งมารวบรวมเพื่อจัดเป็นชุดให้ตรงตามลักษณะโครงสร้างของข้อมูล

5. “บัญชีข้อมูล” หมายความว่า เอกสารแสดงบรรดารายการของชุดข้อมูลที่จำแนกแยกแยะโดยการจัดกลุ่มหรือจัดประเภทข้อมูลที่อยู่ในความครอบครองหรือควบคุมของสำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ

6. “ธรรมาภิบาลข้อมูลภาครัฐ” หมายความว่า การกำหนดสิทธิ หน้าที่ และความรับผิดชอบของผู้มีส่วนได้เสียในการบริหารจัดการข้อมูลทุกขั้นตอน เพื่อให้การได้มาและการนำไปใช้ข้อมูลของหน่วยงานภาครัฐถูกต้อง ครบถ้วน เป็นปัจจุบัน รักษาความเป็นส่วนตัว และสามารถเชื่อมโยงกันได้อย่างมีประสิทธิภาพและมั่นคงปลอดภัย

7. “พจนานุกรมข้อมูล” หมายความว่า ตารางหรือข้อมูลที่ใช้อธิบายรายละเอียดของข้อมูลในแต่ละแถวหรือคอลัมภ์

8. “เมทาดาตา” หมายความว่า คำอธิบายชุดข้อมูล เพื่อให้ทราบรายละเอียดเกี่ยวกับโครงสร้างของข้อมูล เนื้อหาสาระ รูปแบบการจัดเก็บ แหล่งข้อมูล และสิทธิในการเข้าถึงข้อมูล

9. “หมวดหมู่ของข้อมูล” หมายความว่า การกำหนดหมวดหมู่ของข้อมูลตามกรอบธรรมาภิบาลข้อมูลภาครัฐแบ่งออกได้เป็น 4 หมวดหมู่ ได้แก่ ข้อมูลส่วนบุคคล ข้อมูลความมั่นคง ข้อมูลความลับทางราชการ และข้อมูลสาธารณะ

10. “การจัดชั้นความลับของข้อมูล” หมายความว่า การกำหนดประเภทและข้อกำหนดของการจัดชั้นความลับของข้อมูล เพื่อกำหนดสิทธิในการเข้าถึงและสามารถนำข้อมูลไปใช้ได้อย่างเหมาะสม ซึ่งตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 กำหนดให้มีชั้นความลับเป็น ชั้นลับ ชั้นลับมาก หรือ ชั้นลับที่สุด โดยคำนึงถึงการปฏิบัติหน้าที่ของหน่วยงานและประโยชน์แห่งรัฐประกอบกัน ดังนั้น ชั้น

ความลับของข้อมูลมักถูกกำหนดให้สอดคล้องกับผลกระทบต่อหน่วยงานและความมั่นคงของประเทศ อาทิ ชื่อเสียง ความต่อเนื่องของการดำเนินงาน การเงิน และทรัพยากรบุคคล

11. “วงจรชีวิตของข้อมูล” หมายความว่า ลำดับขั้นตอนของข้อมูลตั้งแต่เริ่มสร้างข้อมูลไปจนถึงการทำลายข้อมูลตามกรอบธรรมาภิบาลข้อมูลภาครัฐ

12. “การบริหารจัดการข้อมูล” หมายความว่า ขั้นตอนการสร้างข้อมูล การรวบรวมข้อมูล การจัดเก็บ การจัดเก็บถาวร การทำลายข้อมูล การประมวลผลข้อมูล การใช้ข้อมูล การแลกเปลี่ยน การเชื่อมโยงข้อมูล และการเปิดเผยข้อมูลต่อสาธารณะ

13. “เจ้าของข้อมูล” หมายความว่า ผู้ที่ได้รับมอบหมายในปฏิบัติงานให้รับผิดชอบข้อมูลที่ระบุไว้ ซึ่งรวมถึงผู้บังคับบัญชาของเจ้าของข้อมูลนั้นด้วย โดยทำหน้าที่กำกับดูแลตามธรรมาภิบาลข้อมูลตลอดวงจรชีวิตของข้อมูลนั้น ๆ รวมทั้งทำหน้าที่กำหนดสิทธิในการเข้าถึงข้อมูลและจัดชั้นความลับของข้อมูล

14. “เจ้าหน้าที่” หมายความว่า ข้าราชการ พนักงานราชการ หรือบุคลากรอื่นใด ที่สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ มอบหมายในการบริหารจัดการข้อมูล

15. “คณะบริกรข้อมูล” หมายความว่า เจ้าหน้าที่ซึ่งได้รับการแต่งตั้งจากคณะกรรมการ ให้ปฏิบัติหน้าที่ติดตาม ตรวจสอบ ประเมินผล และจัดทำรายงานผลการดำเนินงานด้านธรรมาภิบาลข้อมูล หรือหน้าที่อื่นใดตามที่คณะกรรมการมอบหมาย

16. “ผู้ดูแลข้อมูล” หมายความว่า ผู้ที่ทำงานร่วมกับเจ้าของข้อมูลโดยตรง ทำหน้าที่ จัดเก็บรักษาข้อมูลและทำลายข้อมูล รวมถึงป้องกันภัยคุกคาม ทำการสำรองข้อมูล

17. “ผู้ดูแลระบบสารสนเทศ” หมายความว่า บุคลากรของศูนย์ข้อมูลเศรษฐกิจและสังคมดิจิทัล ที่มีหน้าที่ดูแลรับผิดชอบระบบสารสนเทศของหน่วยงาน

2. หลักการและขอบเขต

แนวปฏิบัติเกี่ยวกับข้อมูล จัดเป็นหนึ่งในองค์ประกอบตามกรอบธรรมาภิบาลข้อมูลภาครัฐเพื่อเป็นแนวทางให้ผู้มีส่วนได้ส่วนเสียเกี่ยวกับข้อมูลปฏิบัติตาม เพื่อให้ข้อมูลภายในหน่วยงานมีคุณภาพและมีความมั่นคงปลอดภัย ทั้งนี้ แนวปฏิบัติการดำเนินงานด้านธรรมาภิบาลข้อมูลจะต้องสอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง หรือข้อกำหนดอื่น ๆ ที่เกี่ยวข้องตลอดจนผ่านการอนุมัติจากผู้บริหาร มีการเผยแพร่และสื่อสารให้กับเจ้าหน้าที่และผู้ที่เกี่ยวข้องทั้งภายในและภายนอกหน่วยงานอย่างทั่วถึง และจะต้องมีการทบทวนแนวปฏิบัตินี้อย่างสม่ำเสมอ เพื่อให้แนวปฏิบัติการดำเนินงานด้านธรรมาภิบาลข้อมูลนี้ได้ถูกนำไปปฏิบัติอย่างมีประสิทธิภาพและต่อเนื่อง โดยแนวปฏิบัติการดำเนินงานด้านธรรมาภิบาลข้อมูลจะต้องครอบคลุมตลอดทั้งวงจรชีวิตของข้อมูล ดังนี้

3. วงจรชีวิตของข้อมูล

ภาพที่ 1 วงจรชีวิตของข้อมูล

1. การสร้างข้อมูล (Create) เป็นการสร้างข้อมูลขึ้นมาใหม่ หรือปรับปรุงข้อมูลขึ้นใหม่ โดยวิธีการบันทึกเข้าไปด้วยบุคคล หรือบันทึกอัตโนมัติด้วยอุปกรณ์อิเล็กทรอนิกส์ เช่น อุปกรณ์ตรวจจับสัญญาณ (Sensor) รวมถึงการซื้อข้อมูล หรือการรับข้อมูลจากหน่วยงานอื่น เพื่อนำมาจัดเก็บในภายหลัง

2. การจัดเก็บข้อมูล (Store) เป็นการจัดเก็บข้อมูลที่เกิดจากกระบวนการสร้างหรือข้อมูลที่ได้จากการเชื่อมโยงและ/หรือแลกเปลี่ยนกับหน่วยงานอื่น ไม่ว่าจะจัดเก็บลงแฟ้มข้อมูล (File) หรือระบบการจัดการฐานข้อมูล (Database Management System - DBMS) เพื่อให้เกิดความมีระเบียบง่ายต่อการใช้งานข้อมูล ไม่สูญหายหรือถูกทำลาย และช่วยให้ผู้ใช้งานสามารถประมวลผลข้อมูลต่าง ๆ ตามความต้องการได้อย่างรวดเร็ว

3. การประมวลผลและใช้ข้อมูล (Processing and Use) เป็นการนำข้อมูลที่จัดเก็บมาประมวลผล เช่น การถ่ายโอนข้อมูล การเปลี่ยนรูปแบบการจัดเก็บข้อมูล การวิเคราะห์ข้อมูล การจัดทำรายงาน เพื่อนำข้อมูลเหล่านั้นมาใช้งานให้เกิดประโยชน์ตามวัตถุประสงค์ รวมถึงการสำรอง (Backup) ข้อมูล โดยการคัดลอก ข้อมูลที่ใช้งานอยู่ในปัจจุบัน เพื่อทำสำเนา เช่น ใช้โปรแกรมในการสำรองข้อมูล เป็นการหลีกเลี่ยง

ความเสียหายที่จะเกิดขึ้นหากข้อมูลเกิดการเสียหายหรือสูญหาย ซึ่งสามารถนำข้อมูลที่สำรองไว้ในสื่อบันทึกข้อมูลกลับมาใช้งานได้ทันที โดยการกู้คืน (Restore)

4. การเผยแพร่ข้อมูล (Disclosure) เป็นการนำข้อมูลที่อยู่ในความครอบครองของหน่วยงานเผยแพร่ตามช่องทางต่าง ๆ อย่างเหมาะสม อาทิ การเปิดเผยข้อมูล (Open data) การแชร์ข้อมูล (Sharing) การกระจายข้อมูล (Dissemination) การควบคุมการเข้าถึง (Access Control) การแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน (Exchange) และการกำหนดเงื่อนไขในการนำข้อมูลไปใช้ (Condition)

5. กระบวนการจัดเก็บข้อมูลถาวร (Archive) เป็นการย้ายข้อมูลที่มีช่วงอายุเกินช่วงใช้งานหรือไม่ได้ใช้งานแล้ว เพื่อเก็บรักษาถาวรโดยที่ข้อมูลนั้นไม่มีการลบ ปรับปรุง หรือแก้ไขอีก และสามารถนำกลับไปใช้งานได้ใหม่เมื่อต้องการ

6. การทำลายข้อมูล (Destroy) เป็นการทำลายข้อมูลที่มีการจัดเก็บถาวรเป็นระยะเวลานานหรือเกินกว่าระยะเวลาที่กำหนด

7. การเชื่อมโยงและแลกเปลี่ยนข้อมูล (Linkage and Exchange) การเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงานทั้งภายในและภายนอกให้มีความมั่นคงปลอดภัยและข้อมูลมีคุณภาพ สามารถนำไปใช้ประโยชน์ได้อย่างมีประสิทธิภาพ

4. หมวดหมู่และการจัดระดับชั้นของข้อมูล

ข้อมูลของหน่วยงานสามารถแบ่งหมวดหมู่ตามกรอบธรรมาภิบาลข้อมูลและการใช้งานภายในสำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคม (สดช.) ดังนี้

1. ข้อมูลสาธารณะ
2. ข้อมูลส่วนบุคคล
3. ข้อมูลความมั่นคง
4. ข้อมูลความลับทางราชการ

ภาพที่ 2 หมวดหมู่ของข้อมูล

โดยมีการจัดระดับชั้นความลับของข้อมูล ดังนี้

- ข้อมูลใช้ภายใน (Internal Use Only) ได้แก่ ข้อมูลสำหรับใช้ในการดำเนินกิจการภายในของหน่วยงาน ซึ่งไม่อนุญาตให้นำไปใช้งานภายนอกก่อนได้รับอนุญาต เช่น นโยบาย มาตรฐาน และขั้นตอนการปฏิบัติงาน ประกาศ และบันทึกภายในหน่วยงาน เป็นต้น
- ข้อมูลที่มีชั้นความลับ (Secret) แบ่งเป็นข้อมูลลับที่สุด (Top Secret) ข้อมูลลับมาก (Secret) และข้อมูลลับ (Confidential)
- ข้อมูลเปิดเผยได้ (Public) ได้แก่ ข้อมูลที่สามารถเปิดเผยได้แก่บุคคลทั่วไป โดยไม่ก่อให้เกิดความเสียหายใด ๆ แก่ สดช. เช่น ข้อมูลเผยแพร่บนเว็บไซต์ ข้อมูลจากการแถลงข่าว หรือรายงานประจำปีของ สดช. เป็นต้น

ภาพที่ 3 ระดับชั้นข้อมูลของ สดช.

5. ผู้เกี่ยวข้อง

ทั้งนี้แนวปฏิบัติเกี่ยวกับข้อมูลนี้บังคับใช้กับผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับข้อมูลตามประกาศแนวปฏิบัติการกำกับดูแลและบริหารจัดการข้อมูลของ สดช. รวมถึงผู้เกี่ยวข้องอื่น ๆ ที่ไม่ได้ระบุไว้ในแนวปฏิบัติ ดังนี้

1. ผู้สร้างข้อมูล (Data Creators)
2. ผู้ใช้ข้อมูล (Data Users)
3. เจ้าของข้อมูล (Data Owners)
4. คณะบริกรข้อมูล (Data Stewards)
5. ผู้ดูแลระบบสารสนเทศ (System Administrators)
6. ผู้ทำลายข้อมูล (Data Disposer)

6. การเผยแพร่และการทบทวน

แนวปฏิบัติเกี่ยวกับข้อมูลนี้จะต้องทำการเผยแพร่โดยการประกาศเวียนในระบบอินทราเน็ตและจดหมายอิเล็กทรอนิกส์ เพื่อให้เจ้าหน้าที่ทุกระดับใน สดช. ได้รับทราบ และถือปฏิบัติตามแนวปฏิบัตินี้อย่างเคร่งครัด โดยแนวปฏิบัติที่จัดขึ้นนี้เมื่อเริ่มนำไปใช้ในระยะแรกสามารถทบทวนได้บ่อยครั้งเป็นราย ไตรมาส เพื่อให้เหมาะสมกับบริบทการปฏิบัติงานจริง และจะต้องมีการทบทวนเป็นประจำอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ รวมถึงเมื่อมีข้อเสนอแนะคณะกรรมการธรรมาภิบาลข้อมูลของ สดช. เห็นสมควร

หมวด 1 การสร้างข้อมูล

การสร้างข้อมูลเป็นขั้นตอนแรกของวงจรชีวิตข้อมูล เป็นการสร้างข้อมูลขึ้นมาใหม่ หรือปรับปรุงข้อมูลด้วยการบันทึกเข้าไปโดยบุคคล บันทึกอัตโนมัติด้วยอุปกรณ์อิเล็กทรอนิกส์ หรือการรับข้อมูลจากหน่วยงานอื่น

วัตถุประสงค์

เพื่อกำหนดแนวปฏิบัติสำหรับผู้ที่เกี่ยวข้องในการสร้างข้อมูลให้มีคุณภาพ มีความมั่นคงปลอดภัย และเป็นประโยชน์ต่อผู้ใช้ข้อมูล

ผู้รับผิดชอบงาน

1. ผู้สร้างข้อมูล (Data Creators)
2. เจ้าของข้อมูล (Data Owners)
3. คณะบริกรข้อมูล (Data Stewards)
4. ผู้ดูแลระบบสารสนเทศ (System Administrators)

อ้างอิง

1. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 แก้ไขเพิ่มเติมถึง (ฉบับที่ 2) พ.ศ. 2556
2. พระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537 และที่แก้ไขเพิ่มเติม
3. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม
4. พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562
5. ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ พ.ศ. 2563

ภาพที่ 4 แนวปฏิบัติการสร้างข้อมูล

แนวปฏิบัติ

1. เจ้าของข้อมูลต้องมีการกำหนดผู้มีสิทธิในการสร้างข้อมูล และจะต้องทบทวนสิทธินั้นอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ เช่น การลาออก เปลี่ยนตำแหน่ง โอนย้าย สิ้นสุดการจ้าง การปรับโครงสร้าง หรือเมื่อมีการปรับปรุงระบบสารสนเทศ เป็นต้น
2. เจ้าของข้อมูลเป็นผู้กำหนดหมวดหมู่และชั้นความลับของข้อมูลที่ถูกสร้างขึ้นตามวิธีปฏิบัติการจำแนกชั้นความลับของข้อมูล
3. ผู้ดูแลระบบสารสนเทศจะต้องกำหนดสิทธิในการสร้างข้อมูลในระบบให้แก่ผู้สร้างข้อมูลตามที่เจ้าของข้อมูลกำหนด
4. เจ้าของข้อมูล และคณะบริกรข้อมูล ร่วมจัดทำคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตา (Metadata) เมื่อมีการสร้างชุดข้อมูล (Datasets) ตามมาตรฐานขั้นต่ำ คำอธิบายชุดข้อมูลดิจิทัลที่สำนักงานพัฒนารัฐบาลดิจิทัล (สพร.) กำหนด และกำหนดให้ทำการประเมินคุณค่าของชุดข้อมูลดิจิทัลตามแบบฟอร์มประเมินคุณค่าชุดข้อมูลที่ สพร. หรือ สดช. กำหนด เพื่อสนับสนุนการคัดเลือกเป็นชุดข้อมูลคุณค่าสูง (High Value Dataset) และเผยแพร่เป็นข้อมูลเปิดของหน่วยงานต่อสาธารณะตามกฎหมายว่าด้วยข้อมูลข่าวสารของราชการในรูปแบบข้อมูลดิจิทัล
5. ห้ามมิให้ผู้สร้างข้อมูลนำข้อมูลที่มีลักษณะดังต่อไปนี้เข้าสู่ระบบคอมพิวเตอร์ที่ขัดต่อกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์

- ข้อมูลที่บิดเบือน หรือปลอมไม่ว่าทั้งหมดหรือบางส่วน

- ข้อมูลอันเป็นเท็จที่น่าจะเกิดความเสียหายต่อการรักษาความมั่นคงปลอดภัย ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจ หรือโครงสร้างพื้นฐาน หรือก่อให้เกิดความตื่นตระหนก

- ข้อมูลอันเป็นความผิดเกี่ยวกับความมั่นคง หรือความผิดเกี่ยวกับการก่อการร้าย

- ข้อมูลที่มีลักษณะอันลามก และคนทั่วไปอาจเข้าถึงได้

- ข้อมูลที่ปรากฏภาพของผู้อื่น และเป็นภาพที่สร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ ทำให้ผู้อื่นเสียชื่อเสียง ถูกดูหมิ่นถูกเกลียดชัง หรือได้รับความอับอาย

6. ห้ามมิให้ผู้สร้างข้อมูล ทำการสร้าง/ทำซ้ำต่อข้อมูลที่ขัดต่อกฎหมายว่าด้วยลิขสิทธิ์หรือทรัพย์สินทางปัญญาของผู้อื่น เว้นแต่จะเป็นไปตามอำนาจที่กฎหมายรับรอง
7. กำหนดให้ผู้สร้างข้อมูลสร้างข้อมูลที่มาจากแหล่งข้อมูลที่เชื่อถือได้เท่านั้น
8. กำหนดให้เจ้าของข้อมูลตรวจสอบความถูกต้องของข้อมูลที่ถูกสร้างขึ้น
9. กำหนดให้มีวิธีปฏิบัติเกี่ยวกับสร้างข้อมูลให้มีความปลอดภัย และเป็นประโยชน์ต่อผู้ใช้ข้อมูล

ตารางที่ 3 มีส่วนได้ส่วนเสียในการสร้างข้อมูล

กิจกรรม	ผู้มีส่วนได้ส่วนเสีย			
	ผู้สร้างข้อมูล	เจ้าของข้อมูล	คณะบริกรข้อมูล	ผู้ดูแลระบบสารสนเทศ
กำหนดผู้มีสิทธิในการสร้างข้อมูล และกำหนดหมวดหมู่และชั้นความลับ	I	R	C	S
กำหนดสิทธิในการสร้างข้อมูลในระบบให้แก่ผู้สร้างข้อมูล	I	S	I	R
สร้างข้อมูลที่ไม่ขัดต่อกฎหมายและจากแหล่งข้อมูลที่เชื่อถือได้เท่านั้น	R	C	C	S
จัดทำคำอธิบายชุดข้อมูลดิจิทัล	S	R	R	S
ประเมินคุณค่าของชุดข้อมูลดิจิทัล	I	R	R	I
ตรวจสอบความถูกต้องของข้อมูล	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

หมวด 2 การจัดเก็บข้อมูล

การจัดเก็บข้อมูล เป็นการจัดเก็บข้อมูลที่ได้จากกระบวนการสร้าง หรือกระบวนการเชื่อมโยงและแลกเปลี่ยนข้อมูลกับหน่วยงานอื่น เพื่อให้เกิดความมีระเบียบ ง่ายต่อการใช้งาน ข้อมูลไม่สูญหายหรือถูกทำลายและช่วยให้ผู้ใช้งานสามารถประมวลผลข้อมูลต่าง ๆ ตามความต้องการได้อย่างรวดเร็ว

วัตถุประสงค์

เพื่อกำหนดแนวปฏิบัติสำหรับผู้ที่เกี่ยวข้องในการจัดเก็บข้อมูล ให้มีคุณภาพ เข้าถึงและใช้งานได้อย่างมั่นคงปลอดภัย

ผู้รับผิดชอบงาน

1. เจ้าของข้อมูล (Data Owners)
2. ผู้สร้างข้อมูล (Data Creators)
3. คณะบริกรข้อมูล (Data Stewards)
4. ผู้ใช้ข้อมูล (Data Users)
5. ผู้ดูแลระบบสารสนเทศ (System Administrators)

อ้างอิง

1. ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2564

2. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 แก้ไขเพิ่มเติมถึง (ฉบับที่ 2) พ.ศ. 2556

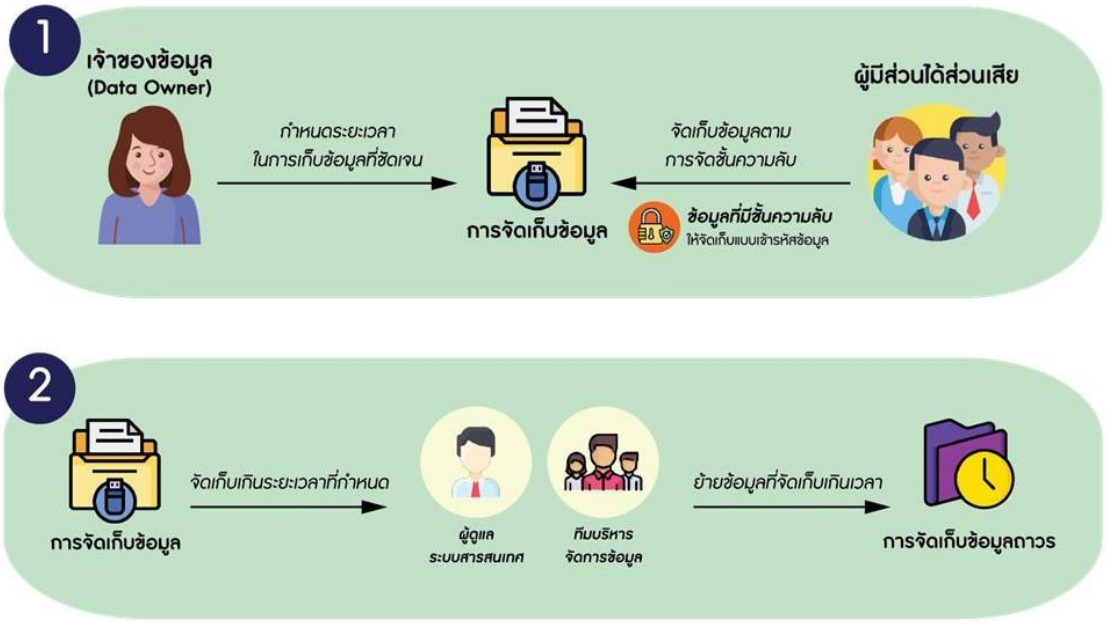
4. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม

5. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

6. พระราชกำหนดว่าด้วยการประชุมผ่านสื่ออิเล็กทรอนิกส์ พ.ศ. 2563

7. ระเบียบสำนักนายกรัฐมนตรี ว่าด้วยงานสารบรรณ พ.ศ. 2526 และที่แก้ไขเพิ่มเติม

8. มาตรฐานรัฐบาลดิจิทัล ว่าด้วย กรอบแนวทางการพัฒนามาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ (THAILAND GOVERNMENT INFORMATION EXCHANGE STANDARD DEVELOPMENT FRAMEWORK) พ.ศ. 2565



ภาพที่ 5 แนวปฏิบัติการจัดเก็บข้อมูล

ข้อปฏิบัติ

1. กำหนดให้เจ้าของข้อมูลจะต้องกำหนดระยะเวลาในการจัดเก็บข้อมูลที่ชัดเจน

2. กำหนดให้คณะบริกรข้อมูล และผู้ดูแลระบบสารสนเทศทำการย้ายข้อมูลที่มีการจัดเก็บเกินระยะเวลาที่กำหนดแล้วเพื่อจัดเก็บเป็นข้อมูลถาวร

3. กำหนดให้การจัดเก็บชุดข้อมูลจะต้องมีคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตา หากไม่มีหรือไม่ครบถ้วน ทีมบริหารจัดการข้อมูลจะต้องแจ้งผู้รับผิดชอบ ได้แก่ เจ้าของข้อมูล และคณะบริกรข้อมูลร่วมกันจัดทำและปรับปรุงให้เป็นปัจจุบัน

4. ผู้มีส่วนได้ส่วนเสียเกี่ยวข้องกับข้อมูล ทั้งเจ้าของข้อมูล ผู้สร้างข้อมูล ผู้ใช้ข้อมูล และคณะบริกรข้อมูล จะต้องจัดเก็บข้อมูลตามการจัดชั้นความลับของหน่วยงาน โดยทำการเข้ารหัสข้อมูล เพื่อป้องกันการเข้าถึงหรือแก้ไขข้อมูลโดยไม่ได้รับอนุญาต ทั้งนี้การเข้ารหัสข้อมูลให้ปฏิบัติตาม วิธีการเข้ารหัสข้อมูล แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

4.1 ในกรณีที่ในตารางฐานข้อมูลเดียวกันมีฟิลด์ข้อมูลที่มีชั้นความลับและไม่มีชั้นความลับอยู่ร่วมกัน ให้ทำการเข้ารหัสข้อมูลเฉพาะฟิลด์ข้อมูลที่มีชั้นความลับเท่านั้น

4.2 ในกรณีข้อมูลที่จัดเก็บในรูปแบบเอกสาร ให้มีการจัดเก็บ ดังนี้

- เก็บในสถานที่เหมาะสม สามารถปิดล็อคได้เมื่อไม่ใช้งาน
- เก็บแยกออกจากอุปกรณ์ประมวลผลต่าง ๆ เช่น เครื่องพิมพ์ เครื่องถ่ายเอกสาร เป็นต้น โดยทันที เพื่อเป็นการป้องกันไม่ให้ผู้ไม่มีสิทธิในการเข้าถึงข้อมูล เข้าถึงข้อมูลได้

5. กำหนดให้มีวิธีปฏิบัติการกู้คืนข้อมูลที่จัดเก็บถาวร สำหรับข้อมูลที่มีความสำคัญมากต่อการดำเนินงานของหน่วยงาน เพื่อสอบทานความถูกต้อง ครบถ้วน ความพร้อมใช้งาน คุณภาพข้อมูล

6. ในการจัดเก็บข้อมูลส่วนบุคคลให้เก็บรวบรวมได้เท่าที่จำเป็น ภายใต้อำนาจหน้าที่และวัตถุประสงค์อันชอบด้วยกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล และไม่เก็บรวบรวมข้อมูลส่วนบุคคลดังต่อไปนี้ เว้นแต่ได้รับการยินยอมจากเจ้าของข้อมูลส่วนบุคคล หรือพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล หรือกฎหมายอื่นบัญญัติให้กระทำได้

- เชื้อชาติ
- เผ่าพันธุ์
- ความคิดเห็นทางการเมือง
- ความเชื่อในลัทธิ ศาสนาหรือปรัชญา
- พฤติกรรมทางเพศ
- ประวัติอาชญากรรม
- ข้อมูลสุขภาพ ความพิการ หรือข้อมูลสุขภาพจิต
- ข้อมูลสหภาพแรงงาน
- ข้อมูลพันธุกรรม
- ข้อมูลชีวภาพ
- ข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลในทำนองเดียวกันตามที่หน่วยงานกำหนด

7. กำหนดให้มีการยกเลิกการจัดเก็บข้อมูลส่วนบุคคลกรณีเจ้าของข้อมูลส่วนบุคคลถอนความยินยอมตามที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลกำหนด

8. ในกรณีที่มีการประชุมหรือธุรกรรมออนไลน์ กำหนดให้มีการจัดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่า 90 วัน นับแต่วันที่ข้อมูลเข้าสู่ระบบคอมพิวเตอร์ โดยจัดเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการนับแต่เริ่มใช้บริการให้สอดคล้องตามกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์และในการจัดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ให้สอดคล้องตามกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ ผู้ให้บริการจะต้องใช้วิธีการที่มั่นคงปลอดภัยอย่างน้อย ดังนี้

- เก็บลงในสื่อที่รักษาความครบถ้วนถูกต้องแท้จริง (Integrity) และระบุตัวตน (Identification) ที่เข้าถึงสื่อได้
- มีการรักษาความลับของข้อมูล และกำหนดชั้นความลับในการเข้าถึงและจัดเก็บข้อมูล เพื่อรักษาความน่าเชื่อถือของข้อมูล และไม่อนุญาตให้ผู้ดูแลระบบแก้ไขข้อมูลที่จัดเก็บไว้ได้
- การจัดเก็บข้อมูลระบุรายละเอียดผู้ใช้บริการเป็นรายบุคคลได้ (Identification and Authentication) เช่น Proxy Server NAT และอื่น ๆ

9. กำหนดให้มีมาตรการรักษาความปลอดภัยในการจัดเก็บข้อมูล รวมทั้งกรณีที่มีการเคลื่อนย้ายอุปกรณ์ที่จัดเก็บข้อมูล เพื่อป้องกันมิให้มีการเข้าถึงโดยมิได้รับอนุญาต หรือลักลอบนำข้อมูลไปใช้ที่ก่อให้เกิดความเสียหายต่อหน่วยงาน

10. กำหนดมาตรการรักษาความปลอดภัยของข้อมูลที่จัดเก็บถาวร เพื่อป้องกันข้อมูลไม่ให้มีการลบ ปรับปรุง แก้ไขได้ รวมทั้งป้องกันมิให้ข้อมูลที่จัดเก็บถาวรรั่วไหลไปยังบุคคลที่ไม่ได้รับอนุญาต

11. กำหนดให้มีมาตรการรักษาความปลอดภัยของการถ่ายโอนข้อมูลกับหน่วยงานภายนอกที่ผ่านช่องทางการสื่อสารทุกชนิด โดยต้องสอดคล้องตามนโยบายความมั่นคงปลอดภัยสารสนเทศ

12. ห้ามมิให้จัดเก็บข้อมูลส่วนตัวหรือข้อมูลที่ไม่เกี่ยวข้องกับการดำเนินงานของหน่วยงาน สำหรับการจัดเก็บข้อมูลถาวรบนเครื่องแม่ข่ายที่หน่วยงานจัดสรรไว้

13. กำหนดให้มีการทบทวนเกี่ยวกับช่วงระยะเวลาการจัดเก็บข้อมูล มาตรการ และวิธีปฏิบัติที่เกี่ยวข้องกับการจัดเก็บข้อมูลถาวร อย่างน้อยปีละ 1 ครั้ง

ตารางที่ 2 ผู้มีส่วนได้ส่วนเสียในการจัดเก็บข้อมูล

กิจกรรม	ผู้มีส่วนได้ส่วนเสีย				
	เจ้าของข้อมูล	ผู้ดูแลระบบสารสนเทศ	ผู้สร้างข้อมูล	ผู้ใช้ข้อมูล	คณะบริกรข้อมูล
กำหนดระยะเวลาในการจัดเก็บข้อมูล	R	S	S	I	I
ย้ายข้อมูลที่มีการจัดเก็บเกินระยะเวลาที่กำหนด	I	R	I	I	I
จัดทำคำอธิบายชุดข้อมูลดิจิทัลและปรับปรุงให้เป็นปัจจุบัน	R	S	S	I	R
จัดเก็บข้อมูลตามการจัดชั้นความลับของหน่วยงาน	R	S	R	I	C
จัดเก็บข้อมูลส่วนบุคคลเท่าที่จำเป็น	R	R/S	S	R	C
ยกเลิกการจัดเก็บข้อมูลส่วนบุคคลกรณีเจ้าของข้อมูลส่วนบุคคลถอนความยินยอม	R	R	I	R	I
จัดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์	I	R	I	I	I

หมายเหตุ

R (Responsible) หมายถึง ผู้มีหน้าที่ในการปฏิบัติงานตามกระบวนการหรือกิจกรรมที่กำหนดไว้

A (Accountable) หมายถึง ผู้มีหน้าที่ในการทบทวนและอนุมัติผลที่ได้รับจากปฏิบัติงาน

S (Supportive) หมายถึง ผู้ที่มีหน้าที่ในการสนับสนุนหรือให้การช่วยเหลือต่อปฏิบัติงาน

C (Consulted) หมายถึง ผู้ที่ทำหน้าที่ให้คำปรึกษาต่อผู้ปฏิบัติงาน

I (Informed) หมายถึง ผู้ที่ทำหน้าที่รับทราบผลการปฏิบัติงาน

หมวด 3 การประมวลผลข้อมูลและการใช้ข้อมูล

การประมวลผลและการใช้ข้อมูล เป็นการนำข้อมูลที่ได้จากการจัดเก็บมาประมวลผล ได้แก่ การเปลี่ยนรูปแบบการจัดเก็บข้อมูล การวิเคราะห์ข้อมูล แสดงผลในรูปแบบตามวัตถุประสงค์ที่กำหนด เพื่อนำข้อมูลเหล่านั้น มาใช้งานให้เกิดประโยชน์ตามวัตถุประสงค์ที่จำเป็น

วัตถุประสงค์

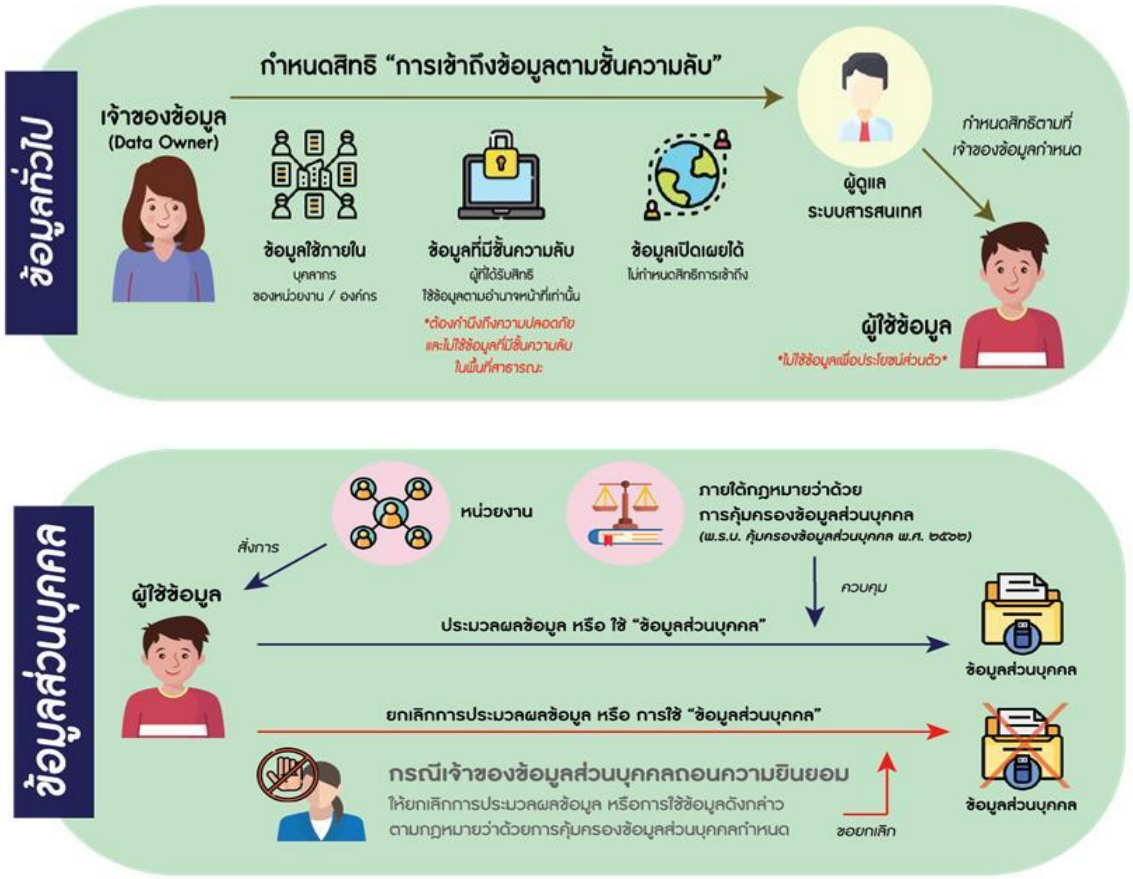
เพื่อกำหนดแนวปฏิบัติในการประมวลผลข้อมูลและการใช้ข้อมูลที่มีประสิทธิภาพถูกต้องตรงตามวัตถุประสงค์ เพื่อให้เกิดประโยชน์สูงสุด

ผู้รับผิดชอบงาน

1. เจ้าของข้อมูล (Data Owners)
2. ผู้ใช้ข้อมูล (Data Users)
3. ผู้ดูแลระบบสารสนเทศ (System Administrators)

อ้างอิง

1. พระราชบัญญัติข้อมูลข่าวสารราชการ พ.ศ. 2540
2. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 แก้ไขเพิ่มเติมถึง (ฉบับที่ 2) พ.ศ. 2556
3. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562



ภาพที่ 6 แนวปฏิบัติการประมวลผลข้อมูลและการใช้ข้อมูล

ข้อปฏิบัติ

1. เจ้าของข้อมูลจะต้องกำหนดผู้มีสิทธิเข้าถึงเพื่อประมวลผลและใช้ข้อมูลตามชั้นความลับ ดังนี้

- ข้อมูลเปิดเผยได้ ไม่กำหนดสิทธิการเข้าถึงเพื่อประมวลผลและใช้งานข้อมูล
- ข้อมูลที่มีชั้นความลับ กำหนดให้ผู้ใช้งานที่ได้รับสิทธิเข้าถึงและใช้ข้อมูลตามอำนาจหน้าที่เท่านั้น
- ข้อมูลใช้ภายใน กำหนดให้บุคลากรของหน่วยงานเท่านั้นที่มีสิทธิเข้าถึงเพื่อประมวลผลและใช้งานข้อมูลได้

2. ผู้ดูแลระบบสารสนเทศจะต้องกำหนดสิทธิในการเข้าถึงข้อมูลในระบบเพื่อประมวลผลและใช้ข้อมูลของผู้ใช้งานตามที่เจ้าของข้อมูลกำหนด

3. เจ้าของข้อมูลจะต้องทบทวนสิทธิการเข้าถึงเพื่อประมวลผลและใช้ข้อมูลของผู้ใช้งานอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ เช่น การลาออก เปลี่ยนตำแหน่ง โอนย้าย สิ้นสุดการจ้าง การปรับโครงสร้าง หรือเมื่อมีการปรับปรุงระบบสารสนเทศ

4. ผู้ที่มีสิทธิเข้าใช้งานข้อมูลที่มีชั้นความลับตามที่กำหนดโดยเจ้าของข้อมูลจะต้องใช้ข้อมูลอย่างระมัดระวัง โดยคำนึงถึงความปลอดภัยและต้องไม่ใช้งานข้อมูลที่มีชั้นความลับในพื้นที่สาธารณะ

5. ผู้ใช้ข้อมูลจะประมวลผลข้อมูลหรือใช้ข้อมูลส่วนบุคคลเท่าที่จำเป็นภายใต้อำนาจหน้าที่และวัตถุประสงค์อันชอบด้วยกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล หรือตามคำสั่งที่ได้รับจากหน่วยงานเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคล

6. หน่วยงานต้องยกเลิกการประมวลผลข้อมูลหรือการใช้ข้อมูลส่วนบุคคล กรณีที่เจ้าของข้อมูลส่วนบุคคลถอนความยินยอมตามที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลกำหนด

7. ผู้ใช้ข้อมูลจะต้องไม่ใช้ข้อมูลในเครือข่ายของหน่วยงานเพื่อประโยชน์ในเชิงธุรกิจเป็นการส่วนตัว หรือเพื่อเข้าสู่เว็บไซต์ที่ไม่เหมาะสมหรือใช้ข้อมูลอันก่อให้เกิดความเสียหายต่อหน่วยงาน

ตารางที่ 4 ผู้มีส่วนได้ส่วนเสียในการประมวลผลและใช้ข้อมูล

กิจกรรม	ผู้มีส่วนได้ส่วนเสีย		
	เจ้าของข้อมูล	ผู้ใช้ข้อมูล	ผู้ดูแลระบบสารสนเทศ
กำหนดสิทธิในการประมวลผลและใช้งานข้อมูลตามชั้นความลับ	R	I	I
กำหนดสิทธิในการประมวลผลและเข้าใช้งานข้อมูลในระบบ	C	I	R
ไม่ใช้ข้อมูลในเครือข่ายของหน่วยงานเพื่อประโยชน์ ในเชิงธุรกิจเป็นการส่วนตัว	C	R	S
ประมวลผลข้อมูลหรือใช้ข้อมูลส่วนบุคคลเท่าที่จำเป็น	C	R	S
ยกเลิกการประมวลผลข้อมูลหรือการใช้ข้อมูลส่วนบุคคล กรณีที่เจ้าของข้อมูลส่วนบุคคลถอนความยินยอม	C	R	S

หมายเหตุ

R (Responsible) หมายถึง ผู้มีหน้าที่ในการปฏิบัติงานตามกระบวนการหรือกิจกรรมที่กำหนดไว้

A (Accountable) หมายถึง ผู้มีหน้าที่ในการทบทวนและอนุมัติผลที่ได้รับจากปฏิบัติงาน

S (Supportive) หมายถึง ผู้ที่มีหน้าที่ในการสนับสนุนหรือให้การช่วยเหลือต่อปฏิบัติงาน

C (Consulted) หมายถึง ผู้ที่ทำหน้าที่ให้คำปรึกษาต่อผู้ปฏิบัติงาน

I (Informed) หมายถึง ผู้ที่ทำหน้าที่รับทราบผลการปฏิบัติงาน

หมวด 4 การเปิดเผยข้อมูล

เป็นการนำข้อมูลที่อยู่ในความครอบครองของ สดช. เผยแพร่ตามช่องทางต่าง ๆ อย่างเหมาะสม อาทิเช่น การเปิดเผยข้อมูล (Open data) การแชร์ข้อมูล (Sharing) การกระจายข้อมูล (Dissemination) การควบคุมการเข้าถึง (Access Control) การแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน (Exchange) และการกำหนดเงื่อนไขในการนำข้อมูลไปใช้ (Condition)

วัตถุประสงค์

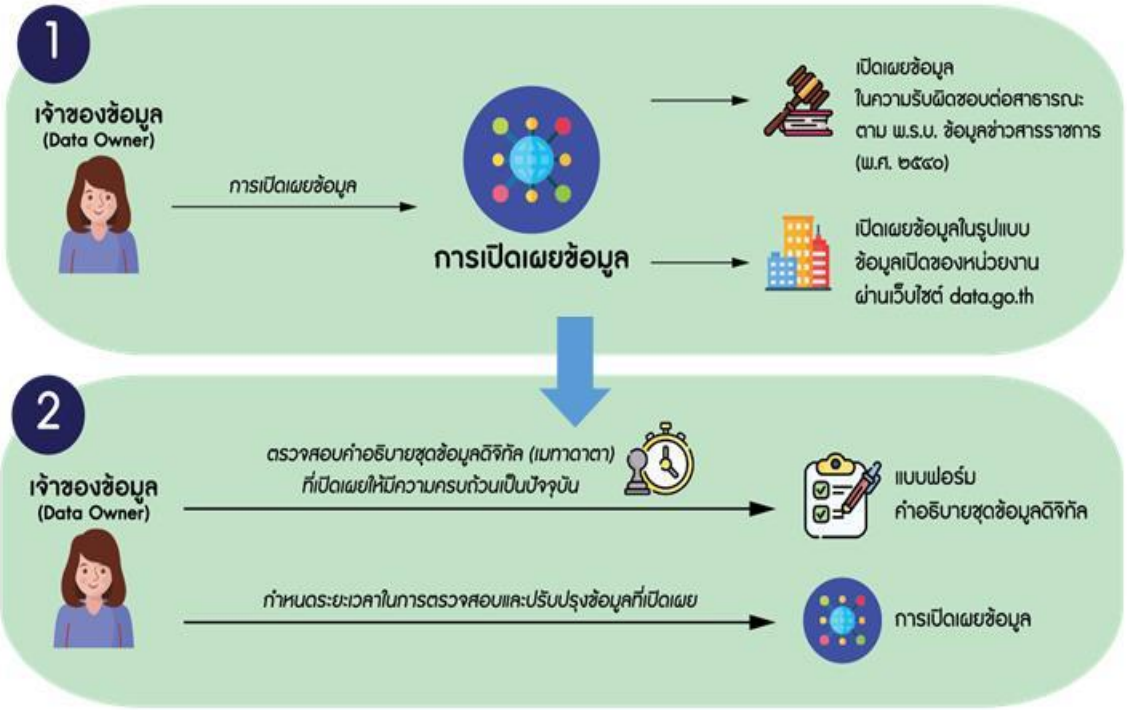
กำหนดแนวปฏิบัติการเปิดเผยข้อมูลต่อสาธารณะโดยอิงจากกฎหมาย กฎเกณฑ์ และแนวปฏิบัติที่เกี่ยวข้อง ทั้งนี้ข้อมูลที่เปิดเผยควรเป็นประโยชน์ สามารถนำไปประมวลผลและใช้ต่อยอดในการพัฒนาในรูปแบบต่าง ๆ ได้

ผู้รับผิดชอบงาน

1. เจ้าของข้อมูล (Data Owners)
2. ผู้ใช้ข้อมูล (Data Users)
3. คณะบริกรข้อมูล (Data Stewards)

อ้างอิง

1. พระราชบัญญัติข้อมูลข่าวสารราชการ พ.ศ. 2540
2. พระราชบัญญัติการอำนวยความสะดวกในการพิจารณาอนุญาตของทางราชการ พ.ศ. 2558
3. พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562
4. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
5. ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง มาตรฐานและหลักเกณฑ์การเปิดเผยข้อมูลเปิดภาครัฐในรูปแบบข้อมูลดิจิทัลต่อสาธารณะ พ.ศ. 2563



ภาพที่ 7 แนวปฏิบัติการเปิดเผยข้อมูล

ข้อปฏิบัติ

1. เจ้าของข้อมูลจะต้องเปิดเผยข้อมูลในความรับผิดชอบต่อสาธารณะตามกฎหมายว่าด้วยข้อมูลข่าวสารของราชการ และมาตรฐานและหลักเกณฑ์การเปิดเผยข้อมูลเปิดภาครัฐในรูปแบบข้อมูลดิจิทัลต่อสาธารณะ

2. เจ้าของข้อมูลทำการเปิดเผยข้อมูลในความรับผิดชอบในรูปแบบข้อมูลเปิดของหน่วยงาน โดยดำเนินการดังนี้

- กำหนดลักษณะของข้อมูลที่เผยแพร่กำหนดให้อยู่ในรูปแบบที่เครื่องสามารถประมวลผลได้
- กำหนดให้มีคำอธิบายข้อมูลหรือเมทาดาตาสำหรับข้อมูลที่ต้องเปิดเผย
- ข้อมูลที่เผยแพร่จะต้องมีการบันทึกเวลา (Timestamps) ที่ช่วยให้ผู้ใช้งานสามารถระบุได้ว่าข้อมูลนั้นเป็นปัจจุบัน
- ข้อมูลที่เผยแพร่ต้องมาจากแหล่งที่เก็บข้อมูลโดยตรงด้วยระดับความละเอียดสูง โดยไม่มีการปรับแต่งหรือเป็นข้อมูลรูปแบบสรุป (Summary data)
- ชุดข้อมูลและรายการชุดข้อมูลที่เผยแพร่จะต้องมีการจัดรูปแบบที่กำหนดเป็นมาตรฐาน และกำหนดภายใต้หมวดหมู่เดียวกัน เพื่อให้ผู้ใช้ข้อมูลสามารถค้นหาและเข้าถึงข้อมูลได้ง่าย

3. กำหนดให้เงื่อนไขและข้อกำหนดของข้อมูลที่นำมาเปิดเผยภายในเครือข่ายของหน่วยงานข้อมูลที่เผยแพร่ต้องไม่ขัดต่อกฎหมายว่าด้วยทรัพย์สินทางปัญญา เว้นแต่การเปิดเผยข้อมูลจะเป็นไปตามอำนาจที่กฎหมายรับรอง

4. สนับสนุนการจัดทำบัญชีข้อมูลหน่วยงานและการลงทะเบียนบัญชีข้อมูลภาครัฐ โดยบริหารจัดการข้อมูลสำคัญ จัดทำบัญชีข้อมูลของหน่วยงาน และทำการลงทะเบียนบัญชีข้อมูลของหน่วยงานและชุดข้อมูลสำคัญ เข้าสู่ระบบบัญชีข้อมูลภาครัฐ (Government Data Catalog หรือ GD Catalog) เพื่อการเปิดเผยข้อมูลภาครัฐที่เป็นระบบและมีเอกภาพ สามารถสืบค้นชุดข้อมูล คำอธิบายชุดข้อมูล รวมไปถึงแหล่งต้นทางของชุดข้อมูลภาครัฐที่สำคัญ สนับสนุนการใช้ประโยชน์ข้อมูลภาครัฐร่วมกัน

5. สนับสนุนการเผยแพร่ข้อมูลผ่านช่องทางที่ง่ายต่อการเข้าถึงข้อมูล และสนับสนุนการเปิดเผยข้อมูลในรูปแบบดิจิทัลต่อสาธารณะที่ศูนย์กลางข้อมูลเปิดภาครัฐ (Government Open Data) ผ่านเว็บไซต์ data.go.th โดย

- กำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัยในการเปิดเผยข้อมูลที่กำหนดลำดับชั้นข้อมูล ตั้งแต่ลับขึ้นไปอย่างเพียงพอและมีประสิทธิภาพ
- มีการตรวจสอบข้อมูลที่เผยแพร่จากหน่วยงานทั้งภายในและภายนอกหน่วยงาน เพื่อให้มั่นใจว่าหน่วยงานได้มีข้อมูลที่เผยแพร่ที่มีคุณค่า
- การเผยแพร่ข้อมูลต้องมีการตรวจสอบรูปแบบข้อมูลที่เผยแพร่ให้สอดคล้องกับมาตรฐานที่หน่วยงานกำหนด
- หากการเปิดเผยนั้นเป็นการเปิดเผยบนช่องทางที่ดูแลรับผิดชอบโดยหน่วยงานอื่นที่ให้ปฏิบัติตาม เอกสาร คู่มือ การนำข้อมูลขึ้นเผยแพร่ของหน่วยงานนั้น
- หากการเปิดเผยข้อมูลไม่ครบถ้วนหรือไม่เป็นปัจจุบัน ให้แจ้งเจ้าของข้อมูลและคณะบริกรข้อมูล ทำการจัดทำ/ปรับปรุงให้เป็นปัจจุบัน

6. กำหนดให้เปิดเผยข้อมูลส่วนบุคคลตามข้อกำหนดของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือตามคำสั่งที่ได้รับจากหน่วยงานเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติในกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

7. เจ้าของข้อมูลห้ามเปิดเผยข้อมูลความมั่นคงและข้อมูลความลับทางราชการที่อยู่ในความครอบครองของหน่วยงาน รวมทั้งห้ามเปิดเผยข้อมูลที่เป็นการกระทำความผิดตามกฎหมาย นโยบายและแนวปฏิบัติอันทำให้เกิดความเสียหายต่อหน่วยงาน

8. กำหนดให้เจ้าของข้อมูลคัดเลือกข้อมูลที่จะเปิดเผยในรูปแบบข้อมูลเปิดจากลำดับชั้นความสำคัญของชุดข้อมูลที่มีคุณค่าสูง (High Value Dataset)

9. กำหนดให้เจ้าของข้อมูลต้องกำหนดรอบระยะเวลาในการตรวจสอบและปรับปรุงข้อมูลที่เปิดเผย เพื่อให้ข้อมูลถูกต้องและเป็นปัจจุบัน

ตารางที่ 5 ผู้มีส่วนได้ส่วนเสียในการเปิดเผยข้อมูล

กิจกรรม	ผู้มีส่วนได้ส่วนเสีย		
	เจ้าของข้อมูล	ผู้ใช้ข้อมูล	คณะบริกรข้อมูล
จะต้องเปิดเผยข้อมูลในความรับผิดชอบต่อสาธารณะตามกฎหมาย/มาตรฐานที่เกี่ยวข้อง	R	I	C
คัดเลือกข้อมูลที่จะเปิดเผยในรูปแบบข้อมูลเปิดจากลำดับชั้นความสำคัญของ High Value Dataset	R	I	C
ตรวจสอบคำอธิบายชุดข้อมูลดิจิทัลที่จะทำการเปิดเผยให้มีความครบถ้วนเป็นปัจจุบัน	R	I	R
เปิดเผยข้อมูลส่วนบุคคลตามข้อกำหนดของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และห้ามเปิดเผยข้อมูลความมั่นคงและข้อมูลความลับทางราชการ รวมถึงข้อมูลที่เป็นการกระทำความผิดตามกฎหมาย	R	R	C
กำหนดรอบระยะเวลาในการตรวจสอบและปรับปรุงข้อมูลที่เปิดเผย	R	I	I

หมายเหตุ

R (Responsible) หมายถึง ผู้มีหน้าที่ในการปฏิบัติงานตามกระบวนการหรือกิจกรรมที่กำหนดไว้

A (Accountable) หมายถึง ผู้มีหน้าที่ในการทบทวนและอนุมัติผลที่ได้รับจากปฏิบัติงาน

S (Supportive) หมายถึง ผู้ที่มีหน้าที่ในการสนับสนุนหรือให้การช่วยเหลือต่อปฏิบัติงาน

C (Consulted) หมายถึง ผู้ที่ทำหน้าที่ให้คำปรึกษาต่อผู้ปฏิบัติงาน

I (Informed) หมายถึง ผู้ที่ทำหน้าที่รับทราบผลการปฏิบัติงาน

หมวด 5 การทำลายข้อมูล

เป็นการทำลายข้อมูลที่มีการจัดเก็บถาวรเป็นระยะเวลานานหรือเกินกว่าระยะเวลาที่กำหนด

วัตถุประสงค์

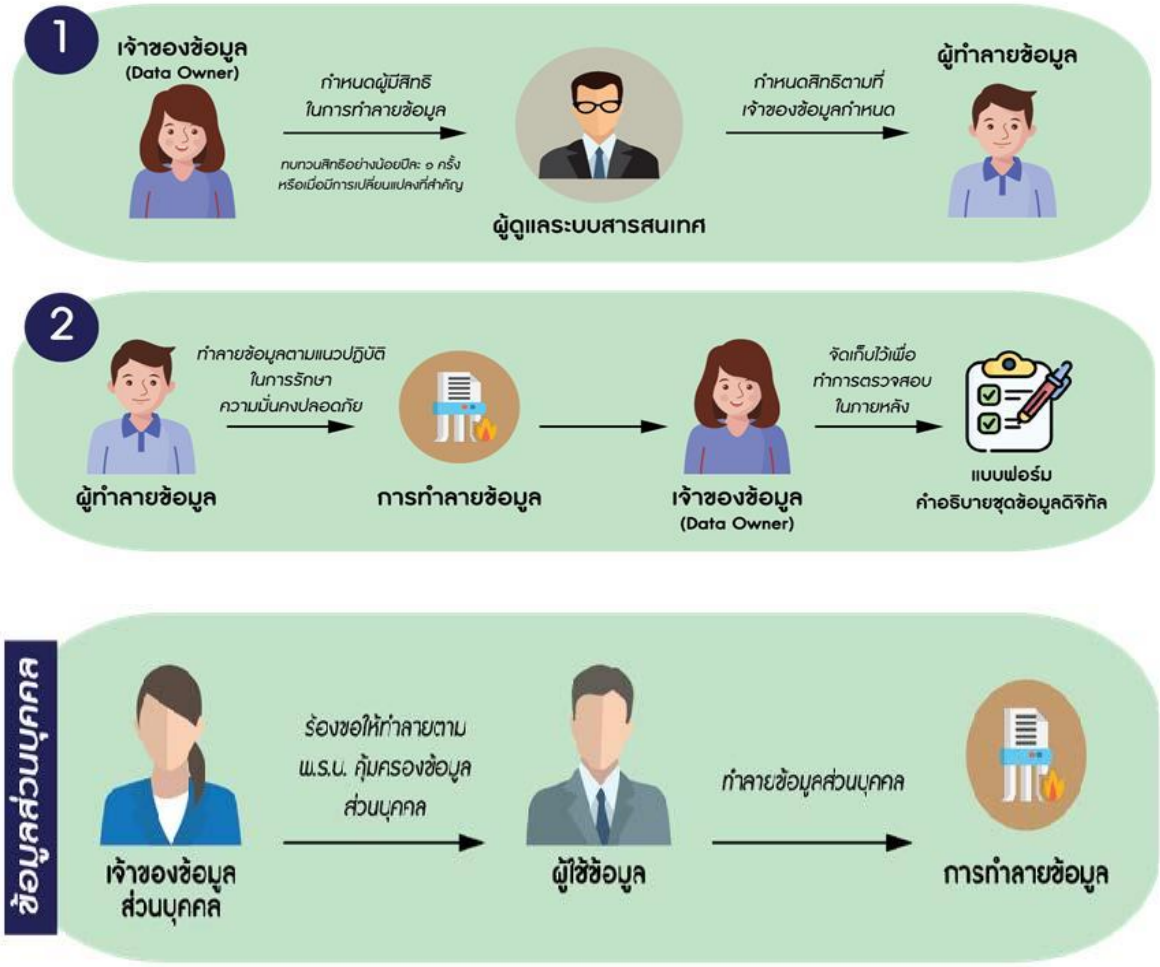
เพื่อกำหนดแนวปฏิบัติการทำลายข้อมูล และการพิจารณาอนุมัติทำลายโดยเจ้าของข้อมูล เพื่อเป็นการรักษาความมั่นคงปลอดภัยของข้อมูล

ผู้รับผิดชอบงาน

1. เจ้าของข้อมูล (Data Owners)
2. ผู้ใช้ข้อมูล (Data Users)
3. ผู้ทำลายข้อมูล (Data Destroyers)
4. ผู้ดูแลระบบสารสนเทศ (Systems Administrators)

อ้างอิง

1. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 แก้ไขเพิ่มเติมถึง (ฉบับที่ 2) พ.ศ. 2556
2. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562



ภาพที่ 8 แนวปฏิบัติการทำลายข้อมูล

ข้อปฏิบัติ

1. เจ้าของข้อมูลเป็นผู้กำหนดผู้มีสิทธิในการทำลายข้อมูล และจะต้องทบทวนสิทธินั้น อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ เช่น การลาออก เปลี่ยนตำแหน่ง โอนย้าย สิ้นสุดการจ้าง การปรับโครงสร้าง หรือเมื่อมีการปรับปรุงระบบสารสนเทศ เป็นต้น

2. ผู้ดูแลระบบสารสนเทศจะต้องกำหนดสิทธิในการทำลายข้อมูลในระบบให้แก่ผู้ทำลายข้อมูลตามที่เจ้าของข้อมูลกำหนด

3. ผู้ทำลายข้อมูลต้องทำลายข้อมูลตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

4. กำหนดให้เจ้าของข้อมูลต้องจัดเก็บคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตาที่ทำลายสำหรับตรวจสอบในภายหลัง

5. กำหนดให้ผู้ทำลายข้อมูลจัดเก็บบันทึกรายละเอียดการทำลายข้อมูลไว้ในทะเบียนควบคุมและบันทึกการทำลายข้อมูล โดยให้เก็บรักษาไว้เป็นหลักฐานไม่น้อยกว่า 1 ปี

6. กำหนดให้ผู้ใช้ข้อมูลส่วนบุคคลทำลายข้อมูลส่วนบุคคลเมื่อเจ้าของข้อมูลส่วนบุคคล ร้องขอตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ตารางที่ 6 มีส่วนได้ส่วนเสียในการทำลายข้อมูล

กิจกรรม	ผู้มีส่วนได้ส่วนเสีย			
	เจ้าของข้อมูล	**ผู้ดูแลระบบสารสนเทศ**	**ผู้ทำลายข้อมูล**	**ผู้ใช้ข้อมูล**
กำหนดผู้มีสิทธิในการทำลายข้อมูล	R	R	I	I
ทำลายข้อมูลตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน	C	S	R	I
จัดเก็บคำอธิบายข้อมูลที่ทำลายสำหรับตรวจสอบในภายหลัง	R	S	R	I
จัดเก็บบันทึกรายละเอียดการทำลายข้อมูล	I	S	R	I
ทำลายข้อมูลส่วนบุคคลเมื่อเจ้าของข้อมูลส่วนบุคคลร้องขอ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562	C	S	I	R

หมายเหตุ

R (Responsible) หมายถึง ผู้มีหน้าที่ในการปฏิบัติงานตามกระบวนการหรือกิจกรรมที่กำหนดไว้

A (Accountable) หมายถึง ผู้มีหน้าที่ในการทบทวนและอนุมัติผลที่ได้รับจากปฏิบัติงาน

S (Supportive) หมายถึง ผู้ที่มีหน้าที่ในการสนับสนุนหรือให้การช่วยเหลือต่อปฏิบัติงาน

C (Consulted) หมายถึง ผู้ที่ทำหน้าที่ให้คำปรึกษาต่อผู้ปฏิบัติงาน

I (Informed) หมายถึง ผู้ที่ทำหน้าที่รับทราบผลการปฏิบัติงาน

หมวด 6 การเชื่อมโยงและการแลกเปลี่ยนข้อมูล

การเชื่อมโยงและแลกเปลี่ยนข้อมูล เป็นการนำข้อมูล สดช. แลกเปลี่ยนทั้งระหว่างหน่วยงานภายในและภายนอกให้มีความมั่นคงปลอดภัยและข้อมูลมีคุณภาพ สามารถนำไปใช้ประโยชน์ได้อย่างมีประสิทธิภาพ

วัตถุประสงค์

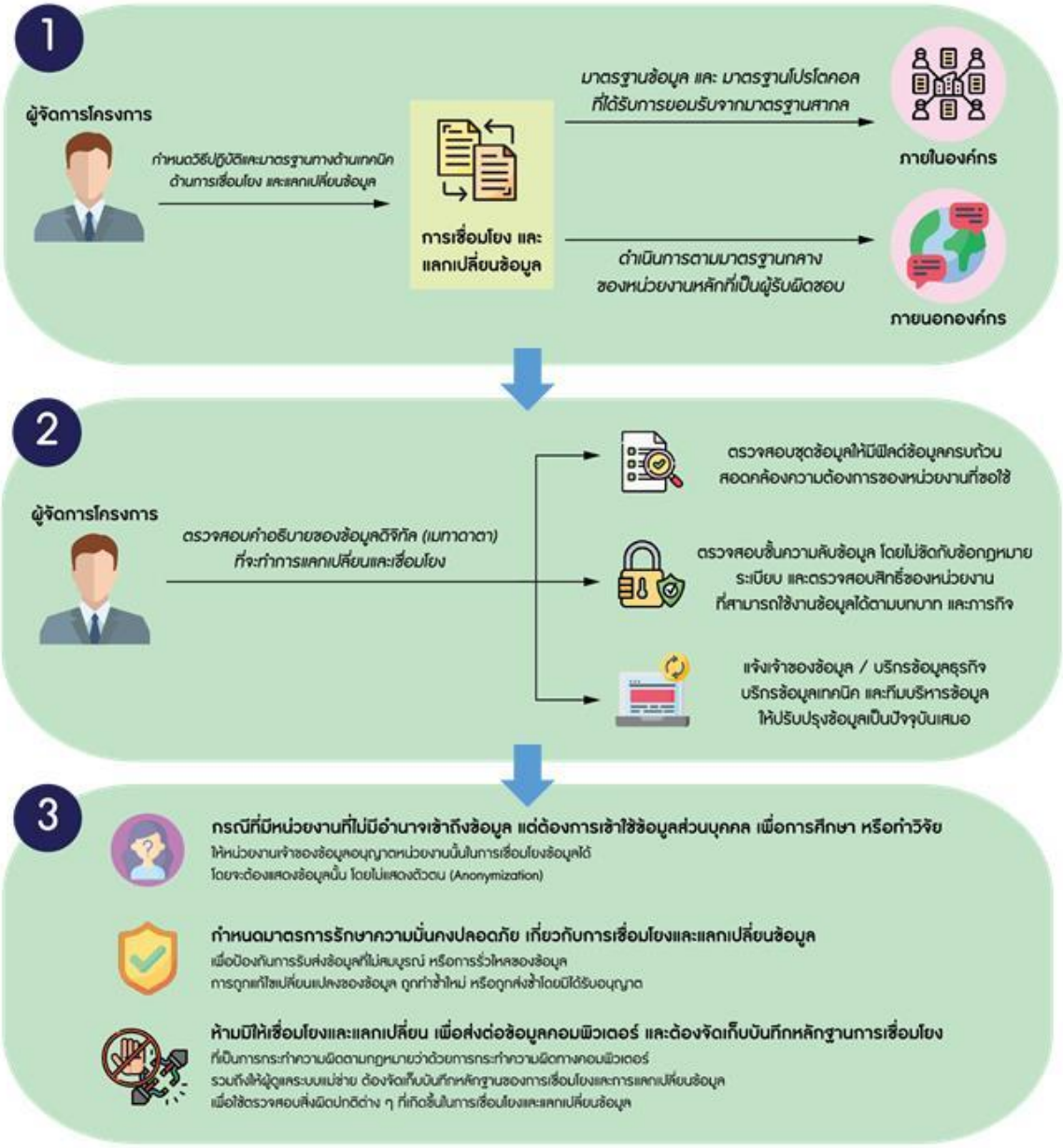
เพื่อกำหนดแนวปฏิบัติและมาตรฐานด้านเทคนิคในการเชื่อมโยงและการแลกเปลี่ยนข้อมูลดิจิทัลทั้งภายในหน่วยงานและระหว่างหน่วยงานอย่างมีประสิทธิภาพและก่อให้เกิดประโยชน์ต่อภาคประชาชน ภาครัฐ และภาคเอกชน

ผู้รับผิดชอบงาน

1. เจ้าของข้อมูล (Data Owners)
2. คณะบริกรข้อมูล (Data Stewards)
3. ผู้ดูแลระบบ (Admin)
4. ผู้จัดการโครงการ (Project Managers)

อ้างอิง

1. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 แก้ไขเพิ่มเติมถึง (ฉบับที่ 2) พ.ศ. 2556
2. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม
3. พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562
4. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
5. มาตรฐานรัฐบาลดิจิทัล ว่าด้วย กรอบแนวทางการพัฒนามาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ (THAILAND GOVERNMENT INFORMATION EXCHANGE STANDARD DEVELOPMENT FRAMEWORK) พ.ศ. 2565



ภาพที่ 9 แนวปฏิบัติการเชื่อมโยงและการแลกเปลี่ยนข้อมูล

ข้อปฏิบัติ

1. กำหนดให้ผู้จัดการโครงการกำหนดวิธีปฏิบัติและมาตรฐานทางด้านเทคนิคที่จำเป็นต้องใช้เกี่ยวกับการเชื่อมโยงและแลกเปลี่ยนข้อมูลของโครงการในความรับผิดชอบ ดังนี้

- การเชื่อมโยงและแลกเปลี่ยนข้อมูลภายในหน่วยงาน กำหนดให้ใช้รูปแบบที่เป็นมาตรฐานเปิด (Open Format) ทั้งในส่วนมาตรฐานข้อมูล เช่น XML และ JSON เป็นต้น มาตรฐานโปรโตคอล สื่อสาร เช่น SOAP REST หรืออื่น ๆ ที่ได้รับการยอมรับจากมาตรฐานสากล
- การเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน ให้ดำเนินการตามมาตรฐานกลางของหน่วยงานหลักที่เป็นผู้รับผิดชอบ

2. กำหนดให้ผู้จัดการโครงการตรวจสอบคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตาที่จะทำการเชื่อมโยงและแลกเปลี่ยนให้ครบถ้วน ดังนี้

- ตรวจสอบเมทาดาตาของชุดข้อมูลดิจิทัลที่จัดเก็บให้มีฟิลด์ข้อมูลครบถ้วนสอดคล้องกับความต้องการของหน่วยงานที่ขอใช้ หากไม่ครบถ้วนต้องจัดทำเพิ่มเติมตามความต้องการของหน่วยงานที่ขอใช้
- ตรวจสอบชั้นความลับของข้อมูลว่าอยู่ในชั้นความลับที่สามารถเปิดเผยได้หรือไม่ นั่นคือ ต้องไม่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ ความมั่นคงของประเทศ ความลับทางราชการ และความเป็นส่วนตัว พร้อมทั้งตรวจสอบสิทธิของหน่วยงานที่สามารถนำข้อมูลไปใช้ได้ตามบทบาทและภารกิจตามกฎหมายของหน่วยงานนั้น ๆ
- หากไม่ครบถ้วน หรือไม่เป็นปัจจุบัน ให้แจ้งเจ้าของข้อมูล คณะบริกรข้อมูล และทีมบริหารจัดการข้อมูลทำการจัดทำ/ปรับปรุงให้เป็นปัจจุบัน

3. ในกรณีที่มีหน่วยงานอื่นที่ไม่มีอำนาจในการเข้าถึงข้อมูลส่วนบุคคลแต่ต้องการใช้ข้อมูลส่วนบุคคลในการครอบครองของหน่วยงาน เพื่อทำการศึกษาหรือวิจัย ซึ่งเป็นข้อยกเว้นตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ให้หน่วยงานเจ้าของข้อมูลอนุญาตหน่วยงานนั้นในการเชื่อมโยงข้อมูลได้ โดยจะต้องแสดงข้อมูลนั้นด้วยวิธีไม่แสดงตัวตน (Anonymization)

4. กำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัยเกี่ยวกับการเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัล เพื่อป้องกันมิให้มีการรับส่งข้อมูลที่ไม่สมบูรณ์ หรือส่งข้อมูลไปผิดที่หรือมีการรั่วไหลของข้อมูล หรือข้อมูลถูกแก้ไขเปลี่ยนแปลง ถูกทำซ้ำใหม่ ถูกส่งซ้ำโดยมิได้รับอนุญาต

5. ห้ามมิให้เชื่อมโยงและแลกเปลี่ยนเพื่อส่งต่อข้อมูลคอมพิวเตอร์ที่เป็นการกระทำความผิดตามกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์

6. กำหนดให้ผู้ดูแลระบบแม่ข่ายต้องจัดเก็บบันทึกหลักฐานของการเชื่อมโยงและการแลกเปลี่ยนข้อมูลดิจิทัล เพื่อใช้ตรวจสอบสิ่งผิดปกติต่าง ๆ ที่เกิดขึ้นในการเชื่อมโยงและแลกเปลี่ยนข้อมูล

ตารางที่ 7 ผู้มีส่วนได้ส่วนเสียในการเชื่อมโยงและการแลกเปลี่ยนข้อมูล

กิจกรรม	ผู้มีส่วนได้ส่วนเสีย			
	ผู้จัดการโครงการ	ผู้ดูแลระบบแม่ข่าย	เจ้าของข้อมูล	คณะบริกรข้อมูล
กำหนดวิธีปฏิบัติและมาตรฐานทางด้าน เทคนิคที่จำเป็นในการเชื่อมโยงและแลกเปลี่ยนข้อมูลของโครงการ	R	S	I	I
ตรวจสอบคำอธิบายชุดข้อมูลดิจิทัลและชั้นความลับของข้อมูล	R	R	C	C
จัดทำแนวทางการทำงานร่วมกันทั้งระหว่างหน่วยงานภายในและหน่วยงานภายนอกในการเชื่อมโยงและแลกเปลี่ยนข้อมูล	R	S	S	S
จัดเก็บบันทึกหลักฐานของการเชื่อมโยง และการแลกเปลี่ยนข้อมูลดิจิทัล	I	R	I	I

หมายเหตุ

R (Responsible) หมายถึง ผู้มีหน้าที่ในการปฏิบัติงานตามกระบวนการหรือกิจกรรมที่กำหนดไว้

A (Accountable) หมายถึง ผู้มีหน้าที่ในการทบทวนและอนุมัติผลที่ได้รับจากปฏิบัติงาน

S (Supportive) หมายถึง ผู้ที่มีหน้าที่ในการสนับสนุนหรือให้การช่วยเหลือต่อปฏิบัติงาน

C (Consulted) หมายถึง ผู้ที่ทำหน้าที่ให้คำปรึกษาต่อผู้ปฏิบัติงาน

I (Informed) หมายถึง ผู้ที่ทำหน้าที่รับทราบผลการปฏิบัติงาน

บรรณานุกรม

1. แบบฟอร์มรายชื่อชุดข้อมูลที่สัมพันธ์กับกระบวนการทำงานตามภารกิจของหน่วยงาน https://gdhelppage.nso.go.th/p00_03_001.html

2. แบบฟอร์มคำอธิบายชุดข้อมูล (Metadata) ที่สอดคล้องตามมาตรฐานที่ สพร. กำหนด https://gdhelppage.nso.go.th/p00_03_006.html

3. แบบฟอร์มชุดข้อมูลที่มีคุณค่าสูง High Value Datasets Checklist ที่ สพร. จัดทำขึ้น https://data.go.th/pages/high-value-criteria

4. มาตรฐานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ว่าด้วยข้อเสนอแนะสำหรับการจัดทำนโยบายการบริหารจัดการข้อมูล (RECOMMENDATION for WRITING DATA MANAGEMENT POLICY) (มสพร. 2-1:2564 และ มสพร. 2-2:2564) https://standard.dga.or.th/dga-std/3671/

5. มาตรฐานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ว่าด้วยแนวทางการจัดทำบัญชีข้อมูลภาครัฐ (GOVERNMENT DATA CATALOG GUIDELINE) (มสพร. 1-2564) https://standard.dga.or.th/dga-std/2594/

6. มาตรฐานรัฐบาลดิจิทัล ว่าด้วยกรอบแนวทางการพัฒนามาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ (THAILAND GOVERNMENT INFORMATION EXCHANGE STANDARD DEVELOPMENT FRAMEWORK) พ.ศ. 2565

นโยบายและแนวปฏิบัติการบริหารจัดการข้อมูล ของสำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ