2568

EEC
เขตพัฒนาพิเศษภาคตะวันออก
เชื่อมโลก ให้ไทยแล่น
สำนักงานคณะกรรมการนโยบายเขตพัฒนาพิเศษภาคตะวันออก

ธรรมาภิบาลข้อมูล
(Data Governance)

รุ่นเอกสาร 1
ณ วันที่ 6 พฤษภาคม 2568

คณะกรรมการธรรมาภิบาลข้อมูล
สำนักงานคณะกรรมการนโยบายเขตพัฒนาพิเศษภาคตะวันออก
(สกพอ.)

สารบัญ

1. บทนำ

1.1. ความเป็นมา

ตามพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 ได้กำหนดให้หน่วยงานของรัฐต้องดำเนินการบริหารจัดการและบูรณาการข้อมูลให้เชื่อมโยงกันอย่างมีธรรมาภิบาล มั่นคงปลอดภัย และสอดคล้องกัน โดยให้ดำเนินการจัดทำธรรมาภิบาลข้อมูลในระดับหน่วยงาน เพื่อรองรับการเปิดเผย เชื่อมโยง และแลกเปลี่ยนข้อมูลผ่านระบบดิจิทัล ตลอดจนการขับเคลื่อนหน่วยงานให้เป็นองค์กรที่ใช้ข้อมูลอย่างมีคุณภาพ เคารพความเป็นส่วนบุคคล และปลอดภัย ทั้งนี้ ต้องดำเนินการให้สอดคล้องกับประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูล ลงวันที่ 12 มีนาคม พ.ศ. 2563

สำนักงานคณะกรรมการนโยบายเขตพัฒนาพิเศษภาคตะวันออก (สกพอ.) ได้ตระหนักถึงบทบาทและความสำคัญของข้อมูลในยุคดิจิทัล จึงได้ยกระดับประสิทธิภาพการทำงานและการให้บริการประชาชนด้วยการนำเทคโนโลยีดิจิทัลมาใช้เพื่อเพิ่มความสะดวก รวดเร็ว ลดระยะเวลา และสนับสนุนการตัดสินใจเชิงนโยบาย โดยอาศัยการวิเคราะห์ข้อมูลขนาดใหญ่ (Big Data) ที่ถูกต้องและแม่นยำ รวมถึงส่งเสริมการแลกเปลี่ยนข้อมูลกับหน่วยงานภายนอกและพัฒนาการบริการให้ตอบสนองความต้องการของประชาชนได้อย่างแท้จริง นอกจากนี้ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ยังได้กำหนดให้หน่วยงานของรัฐ รวมถึง สกพอ. ต้องดำเนินการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลอย่างเหมาะสมและปลอดภัย ส่งผลให้ สกพอ. จำเป็นต้องวิเคราะห์การดำเนินงานในด้านต่าง ๆ ที่เกี่ยวข้องกับข้อมูลในความครอบครองของหน่วยงาน เช่น การบริหารจัดการข้อมูล การคุ้มครองข้อมูลส่วนบุคคล การตรวจสอบคุณภาพข้อมูล และการจัดทำบัญชีข้อมูล (Data Catalog) เพื่อให้เกิดมาตรฐานการดำเนินงานที่สอดคล้องกับกฎหมาย

เพื่อรองรับแนวทางดังกล่าว สกพอ. จึงได้จัดทำ “ธรรมาภิบาลข้อมูล (Data Governance)” เพื่อเป็นแนวทางในการกำกับดูแลการใช้ข้อมูลอย่างมีประสิทธิภาพ สำหรับบุคลากร ผู้บริหาร และผู้มีส่วนได้ส่วนเสีย โดยเน้นการใช้ข้อมูลอย่างถูกต้อง เหมาะสม และเกิดประโยชน์สูงสุดต่อการขับเคลื่อนภารกิจของหน่วยงาน

1.2. วัตถุประสงค์

1.2.1. เพื่อกำหนดกรอบนโยบาย มาตรฐาน และแนวปฏิบัติในการบริหารจัดการข้อมูล

1.2.2. เพื่อกำหนดบทบาทและความรับผิดชอบในการบริหารจัดการข้อมูลอย่างเป็นระบบ

1.2.3. เพื่อรักษาความมั่นคงปลอดภัยของข้อมูลและปฏิบัติตามกฎหมายหรือข้อบังคับที่เกี่ยวข้อง

1.2.4. เพื่อสนับสนุนการบูรณาการและการใช้ข้อมูลร่วมกันระหว่างหน่วยงานอย่างมีประสิทธิภาพ

2. แนวคิดธรรมาภิบาลข้อมูลภาครัฐ

2.1. ธรรมาภิบาลข้อมูล (DATA GOVERNANCE)

กรอบแนวทางและกระบวนการในการบริหารจัดการข้อมูลภาครัฐอย่างเป็นระบบ โดยมีการกำหนดนโยบาย มาตรฐาน บทบาทหน้าที่ และกลไกการควบคุมที่ชัดเจน เพื่อให้ข้อมูลของรัฐมีความ ถูกต้อง เชื่อถือได้ ปลอดภัย เป็นปัจจุบัน เป็นไปตามหลักการทางกฎหมายและสามารถใช้ประโยชน์ได้อย่างเหมาะสม ทั้งในการให้บริการประชาชน การตัดสินใจเชิงนโยบาย และการบูรณาการระหว่างหน่วยงาน

ธรรมาภิบาลข้อมูลภาครัฐมีบทบาทสำคัญในการสร้างความโปร่งใส ความน่าเชื่อถือ และความเป็นธรรมในการใช้ข้อมูลของภาครัฐ โดยเน้นให้เกิดความรับผิดชอบต่อสาธารณะ สร้างความไว้วางใจ และมีการควบคุมการใช้ข้อมูลอย่างมีประสิทธิภาพ พร้อมป้องกันการละเมิดความเป็นส่วนตัวของข้อมูล ทั้งนี้เพื่อให้ภาครัฐสามารถใช้ข้อมูลในการตัดสินใจอย่างมีประสิทธิภาพและตอบสนองต่อสังคมได้อย่างเหมาะสมและเป็นธรรม

องค์ประกอบหลักของธรรมาภิบาลข้อมูลภาครัฐที่ดี ประกอบด้วย

1) มีนโยบายข้อมูลที่ชัดเจน ซึ่งสามารถนำไปใช้เป็นกรอบสำหรับการบริหารจัดการและกำกับดูแลข้อมูล
2) มีคำอธิบายชุดข้อมูลหรือเมทาดาตาที่ช่วยให้ผู้ใช้งานเข้าใจว่าข้อมูลชุดนี้คือข้อมูลที่เกี่ยวข้องกับอะไร สามารถนำไปใช้งานอย่างไร และมีข้อจำกัดอะไรบ้าง โดยมีมาตรฐานของเมทาดาตาที่เหมาะสมกับการใช้งาน
3) มีมาตรการในการรักษาความมั่นคงปลอดภัยและความเป็นส่วนบุคคลของข้อมูล ซึ่งช่วยป้องกันหรือบรรเทาความเสียหายที่จะเกิดขึ้นกับข้อมูลและการละเมิดสิทธิส่วนบุคคล
4) มีมาตรการในการควบคุมคุณภาพของข้อมูลให้มีคุณภาพสูง ซึ่งจะสนับสนุนให้การดำเนินงานของหน่วยงานเป็นไปอย่างมีประสิทธิภาพและประสิทธิผล
5) การตรวจสอบและประเมินความสัมฤทธิ์ผลของนโยบายข้อมูล และมาตรการต่าง ๆ ตลอดวงจรชีวิตของข้อมูล เป็นประจำอย่างน้อยปีละหนึ่งครั้ง
6) ข้อ (1) – (5) เป็นกรณีที่ต้องปฏิบัติได้อย่างแท้จริง (Practical)

ประโยชน์ของธรรมาภิบาลข้อมูลภาครัฐที่มีต่อองค์กร มีดังนี้

1) **เสถียรภาพและความน่าเชื่อถือของข้อมูล:** ช่วยกำหนดนโยบายและแนวทางที่ชัดเจนในการใช้ข้อมูล ส่งเสริมคุณภาพ ความถูกต้อง และความน่าเชื่อถือของข้อมูลภาครัฐ
2) **การปกป้องความเป็นส่วนตัว:** วางกรอบนโยบายและมาตรการเพื่อคุ้มครองข้อมูลส่วนบุคคล ลดความเสี่ยงในการละเมิดสิทธิ และเพิ่มความไว้วางใจของประชาชน
3) **เพิ่มประสิทธิภาพการบริหารจัดการข้อมูล:** ช่วยให้หน่วยงานมีระบบการจัดการข้อมูลที่เป็นระเบียบ มีขั้นตอนชัดเจน ตั้งแต่การเก็บรวบรวม ประมวลผล ไปจนถึงการนำข้อมูลไปใช้ในการบริหารและให้บริการ

4) **ส่งเสริมการใช้ข้อมูลในการตัดสินใจ:** สนับสนุนการวางแผน การจัดสรรทรัพยากร และการกำหนดนโยบายโดยอิงข้อมูลอย่างเป็นระบบและถูกต้องตามกฎหมาย
5) **สนับสนุนการเข้าถึงและการนำข้อมูลไปใช้:** ส่งเสริมการเปิดเผยข้อมูลภาครัฐอย่างเหมาะสม อำนวยความสะดวกให้ประชาชน ภาคเอกชน และหน่วยงานอื่นสามารถเข้าถึงและใช้ข้อมูลได้ง่ายและมีประสิทธิภาพ

2.2. การบริหารจัดการข้อมูล (DATA MANAGEMENT)

การบริหารจัดการข้อมูล คือ “คำจำกัดความที่อธิบายถึงกระบวนการที่ใช้ในการวางแผน (Plan) ระบุ (Specify) เปิดใช้งาน (Enable) สร้าง (Create) รับ (Acquire) ดูแลรักษา (Maintain) ใช้ (Use) จัดเก็บถาวร (Archive) ดึงข้อมูล (Retrieve) ควบคุม (Control) และทำลายข้อมูล (Purge)” (Cupola et al., 2014)

การบริหารจัดการข้อมูลเป็นสิ่งสำคัญสำหรับทุกหน่วยงาน ซึ่งแต่ละหน่วยงานต้องตระหนักว่าข้อมูลที่มีอยู่เป็นทรัพย์สินที่มีค่า และจากการเกิดขึ้นของข้อมูลที่มีปริมาณมหาศาล ไม่ว่าจะเป็นข้อมูลที่รวบรวมมาโดยอัตโนมัติจากระบบหรืออุปกรณ์ต่าง ๆ หรือข้อมูลที่เกิดขึ้นจากการป้อนข้อมูลหรือโต้ตอบกับผู้ใช้งาน เพื่อให้หน่วยงานสามารถนำข้อมูลเหล่านี้ไปประมวลผลหรือใช้ในการตัดสินใจได้อย่างแม่นยำ จึงต้องได้รับการบริหารจัดการอย่างถูกต้อง เหมาะสม และสอดคล้องกับวัตถุประสงค์ในการบริหารจัดการข้อมูลของหน่วยงาน

การบริหารจัดการข้อมูลเป็นกระบวนการที่มุ่งเน้นการยกระดับการใช้ประโยชน์จากข้อมูลให้เกิดประสิทธิภาพสูงสุด โดยครอบคลุมการดำเนินงานในหลากหลายด้าน ดังนี้

1) **ด้านสถาปัตยกรรมข้อมูล (Data Architecture)** เป็นส่วนหนึ่งของการพัฒนาสถาปัตยกรรมองค์กร (Enterprise Architecture) เป็นการอธิบายเกี่ยวกับกลุ่มของข้อมูลทั้งหมดที่มีในหน่วยงาน ความสัมพันธ์ระหว่างข้อมูลกับกระบวนการปฏิบัติงาน ความสัมพันธ์ระหว่างข้อมูลกับแอปพลิเคชัน สถาปัตยกรรมเทคโนโลยีข้อมูล สถาปัตยกรรมการบูรณาการข้อมูล สถาปัตยกรรมเมทาดาตา เป็นต้น สถาปัตยกรรมข้อมูลจะอยู่ในรูปแบบของแบบจำลองข้อมูลที่มองเห็นภาพรวม ความเชื่อมโยง และการไหลของข้อมูลในระดับต่างๆ ทั้งหมดของหน่วยงานทั้งที่เป็นหน่วยงานต้นน้ำ กลางน้ำ หรือปลายน้ำ สามารถอธิบายสถานะที่มีอยู่ในปัจจุบัน และกำหนดความต้องการสำหรับอนาคต เพื่อให้หน่วยงานเกิดความเข้าใจและเห็นเป็นภาพเดียวกันดังนั้นจึงเป็นพื้นฐานที่สำคัญในการวางแผนบริหารจัดการข้อมูล
2) **ด้านจำลองและการออกแบบข้อมูล (Data Modeling and Design)** เป็นวิธีการวิเคราะห์ความต้องการของผู้ใช้ รวมถึงระบุข้อกำหนดและการแก้ปัญหาต่าง ๆ ที่เกี่ยวข้อง แบบจำลองข้อมูลแสดงในรูปแบบของไดอะแกรม (Diagram) ที่มีการออกแบบลักษณะโครงสร้างของข้อมูล เพื่อใช้ในการสื่อสารภายในหน่วยงานให้เข้าใจตรงกัน แบบจำลองข้อมูลจะแสดงถึงความสัมพันธ์ระหว่างข้อมูลที่เกี่ยวข้องกันพร้อมทั้งรายละเอียดของโครงสร้างของข้อมูล โดยแบ่งออกเป็น 3 ระดับ ได้แก่ (1) แบบจำลองข้อมูลเชิงความคิด (Conceptual Data Model)

(2) แบบจำลองข้อมูลเชิงตรรกะ (Logical Data Model) และ (3) แบบจำลองข้อมูลเชิงกายภาพ (Physical Data Model)

3) **ด้านการจัดเก็บและการดำเนินงานกับข้อมูล (Data Storage and Operations)** เป็นการจัดเก็บข้อมูลที่มีโครงสร้าง โดยจัดเก็บในรูปแบบของฐานข้อมูล ซึ่งการดำเนินงานกับข้อมูลจะเกี่ยวข้องตั้งแต่การวางแผนการใช้งาน การสำรองข้อมูล (Backup) การกู้คืนข้อมูล (Restore) การจัดเก็บข้อมูลถาวร (Archive) กระบวนการที่เกี่ยวข้องกับข้อมูล (Create Read Update Delete - CRUD) ตลอดทั้งวงจรชีวิตของข้อมูล รวมถึงการปรับปรุงประสิทธิภาพของฐานข้อมูลให้พร้อมใช้งานได้ตลอดเวลา

4) **ด้านการบูรณาการและความสามารถในการทำงานร่วมกัน (Data Integration and Interoperability)** เป็นการรวบรวมข้อมูลจากแหล่งข้อมูลต่าง ๆ ในรูปแบบที่สอดคล้องกันเข้ามารวมอยู่ในแหล่งข้อมูลเดียวกัน เพื่อนำไปใช้ในการจัดทำข้อมูลหลัก (Master Data) คลังข้อมูล (Data Warehouse) ดาตาเลค (Data Lake) รวมถึงการแลกเปลี่ยนข้อมูลระหว่างหน่วยงานและสามารถในการทำงานร่วมกัน (Interoperability) นอกจากนี้ การกำหนดมาตรฐานหรือข้อตกลงร่วมกันระหว่างหน่วยงานหรือระบบ โดยมีการอ้างถึงคุณลักษณะของระบบต่าง ๆ ที่สามารถแลกเปลี่ยนข้อมูลกันหรือสื่อสารกันได้ เช่น มีการแลกเปลี่ยนข้อมูลในรูปแบบของ API (Application Programming Interfaces)

5) **ด้านการบริหารจัดการเอกสารและเนื้อหา (Document and Content Management)** เป็นการวางแผนการจัดการ การเข้าถึง การใช้งาน และการควบคุมกิจกรรมต่าง ๆ ที่เกี่ยวข้องกับข้อมูลที่ไม่มีโครงสร้างหรือกึ่งโครงสร้าง เช่น การจัดเก็บ การป้องกันความเสียหาย และการเข้าถึงข้อมูล ไม่ว่าจะอยู่ในรูปแบบกระดาษหรือไฟล์อิเล็กทรอนิกส์ที่มีลักษณะเป็นข้อความ รูปภาพ เสียง หรือภาพเคลื่อนไหว เป็นต้น

6) **ด้านข้อมูลหลักและข้อมูลอ้างอิง (Master and Reference Data)** เป็นการบริหารจัดการข้อมูลเพื่อให้หน่วยงานสามารถเข้าถึงและใช้ข้อมูลร่วมกันได้อย่างมีประสิทธิภาพ โดยจัดเก็บข้อมูลไว้ในแหล่งเดียว พร้อมกำหนดมาตรฐานข้อมูลเพื่อลดความซ้ำซ้อนและยกระดับคุณภาพข้อมูล โดยจำแนกข้อมูลออกเป็น 2 ประเภทหลัก ได้แก่ ข้อมูลอ้างอิง (Reference Data) ซึ่งเป็นข้อมูลที่เป็นสากล มีการเปลี่ยนแปลงน้อย เช่น รหัสไปรษณีย์ รหัสประเทศ หน่วยวัดต่าง ๆ และข้อมูลหลัก (Master Data) ซึ่งมีรายละเอียดมากกว่า มีโอกาสเปลี่ยนแปลงสูง และถูกใช้งานร่วมกันภายในหน่วยงาน เช่น ข้อมูลพนักงาน ลูกค้า ผู้ขาย สินค้า ครุภัณฑ์ และสถานที่

7) **ด้านคลังข้อมูล ดาตาเลค ระบบรายงานอัจฉริยะ และดาตาอนาไลติกส์ (Data Warehouse, Data Lake, Business Intelligence, and Data Analytics)** เป็นการดำเนินงานจัดการข้อมูลมุ่งเน้นการกำหนดกระบวนการในการรวบรวม จัดเก็บ และการนำไปใช้

- **คลังข้อมูล (Data Warehouse)** เป็นระบบจัดเก็บข้อมูลที่เกิดจากการรวมข้อมูลจากแหล่งต่าง ๆ ผ่านกระบวนการ Extract, Transform, Load (ETL) เพื่อจัดเก็บในรูปแบบข้อมูลที่มีโครงสร้าง พร้อมสำหรับการวิเคราะห์ เช่น รายงานอัจฉริยะ (Business Intelligence) และการวิเคราะห์ข้อมูล (Data Analytics)
- **ดาตาเลค (Data Lake)** เป็นแหล่งจัดเก็บข้อมูลทุกประเภท ทั้งข้อมูลที่มีโครงสร้าง กึ่งโครงสร้าง และไม่มีโครงสร้าง โดยจัดเก็บไว้ในรูปแบบดั้งเดิมหรือใกล้เคียงต้นฉบับ เหมาะสำหรับใช้เป็นที่สำรองข้อมูลและรองรับการนำไปวิเคราะห์ภายหลังตามความต้องการ

8) **ด้านคำอธิบายชุดข้อมูลดิจิทัล หรือเมทาดาตา (Metadata)**เป็นการจัดทำข้อมูลประกอบที่ใช้ในการอธิบายชุดข้อมูลภายใต้การดำเนินงานของหน่วยงาน โดยแบ่งเป็น 2 มิติ ได้แก่

- **เชิงธุรกิจ (Business Metadata):** เช่น ชื่อเจ้าของข้อมูล ระดับความลับของข้อมูล ขอบเขตการนำไปใช้ เป็นต้น
- **เชิงเทคนิค (Technical Metadata):** เช่น วันที่ปรับปรุงข้อมูลล่าสุด โครงสร้างของข้อมูล ฯลฯ

9) **ด้านความมั่นคงปลอดภัยและการรักษาความเป็นส่วนบุคคลของข้อมูล (Data Security and Privacy)** เป็นองค์ประกอบสำคัญของการบริหารจัดการข้อมูล โดยมีเป้าหมายเพื่อปกป้องข้อมูลจากการเข้าถึง การใช้ หรือการเปิดเผยโดยไม่ได้รับอนุญาต รวมถึงการป้องกันความเสียหาย การสูญหาย และการเปลี่ยนแปลงข้อมูลโดยไม่เหมาะสม มีองค์ประกอบ 4 ด้าน ดังนี้

- **การรักษาความลับ (Confidentiality)** หมายถึง การรักษาข้อมูลตามสภาพของการจัดชั้นความลับ และมีการกำหนดสิทธิ์การเข้าถึงข้อมูลนั้น เนื่องจากข้อมูลในหน่วยงานอาจมีหลายประเภท ข้อมูลบางประเภทเป็นข้อมูลที่มีความสำคัญ หรืออ่อนไหว จึงต้องมีการรักษาความลับเพื่อลดความเสี่ยงของการถูกคุกคาม และเป็นการป้องกันการรั่วไหลของข้อมูลโดยมิชอบ เช่น การส่งข้อมูลที่ปกปิดหรือเป็นความลับต้องมีวิธีการที่ทำให้ทราบได้ว่าบุคคลที่ต้องการส่งข้อมูลมาให้ หรือการที่ผู้ได้รับการอนุญาตให้เข้าถึงข้อมูลเท่านั้นที่สามารถอ่านข้อมูลได้
- **ความถูกต้องของข้อมูล (Integrity)** หมายถึง การคงสภาพของข้อมูลหรือการรักษาความถูกต้องสมบูรณ์ของข้อมูลให้มีความถูกต้องและน่าเชื่อถือ รวมถึงมีการปกป้องข้อมูลให้ปราศจากการถูกเปลี่ยนแปลงโดยผู้ไม่มีสิทธิ์ เช่น ข้อมูลที่ใช้จะต้องเป็นข้อมูลที่ถูกต้องอย่างแท้จริง ไม่มีการดัดแปลงหรือแก้ไขระหว่างทาง
- **ความพร้อมใช้งานของข้อมูล (Availability)** หมายถึง การพร้อมในการใช้งานอยู่เสมอ กล่าวคือข้อมูลต้องพร้อมสำหรับการใช้งานได้เสมอ รวมถึงมีการสำรองข้อมูล

ไว้เมื่อเกิดภัยพิบัติหรือเหตุการณ์ที่ไม่คาดฝัน เช่น หากต้องการใช้ข้อมูล ผู้ใช้งานสามารถใช้ข้อมูลได้ทันที และใช้ได้อย่างต่อเนื่อง

- **การรักษาความเป็นส่วนบุคคลของข้อมูล (Data Privacy)** หมายถึง การกำกับดูแลข้อมูลส่วนบุคคลตั้งแต่การรวบรวม จัดเก็บใช้ เผยแพร่ หรือดำเนินการอื่นใดเกี่ยวกับข้อมูล โดยจะต้องมีการระบุวัตถุประสงค์เป็นหลักฐานให้ชัดเจน ห้ามมิให้มีการเปิดเผย หรือแสดง หรือทำให้ปรากฏในลักษณะอื่นใดที่ไม่สอดคล้องกับวัตถุประสงค์ เว้นแต่จะได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลนั้น ๆ หรือมีกฎหมายกำหนดให้สามารถกระทำสิ่งนั้นได้

10) **ด้านคุณภาพของข้อมูล (Data Quality)** เป็นกระบวนการวัดและประเมินความน่าเชื่อถือ รวมถึงประสิทธิภาพของการนำข้อมูลไปใช้งานในหลากหลายมิติ เช่น ความถูกต้อง (Accuracy) ความครบถ้วน (Completeness) ความสอดคล้องกัน (Consistency) ความทันเวลา (Timeliness) ความตรงประเด็น (Relevancy) ความพร้อมใช้งาน (Availability) นอกจากนี้ ยังครอบคลุมถึงการปรับปรุงข้อมูลให้มีคุณภาพสูงขึ้นอย่างต่อเนื่อง เพื่อให้ตอบสนองความต้องการของผู้ใช้งานและสนับสนุนการตัดสินใจได้อย่างมีประสิทธิภาพ

การบริหารจัดการข้อมูลนั้น มีองค์ประกอบในการบริหารจัดการตลอดทั้งระบบบริหารและกระบวนการจัดการข้อมูล หรือวงจรชีวิตของข้อมูล ดังรูปที่ 1

รูปที่ 1 ระบบบริหารและกระบวนการจัดการข้อมูล หรือวงจรชีวิตของข้อมูล และองค์ประกอบในการบริหารจัดการข้อมูล

ระบบบริหารและกระบวนการจัดการข้อมูล หรือวงจรชีวิตของข้อมูล (Data Life Cycle)

ระบบบริหารและกระบวนการจัดการข้อมูล หรือวงจรชีวิตของข้อมูล คือ “ลำดับขั้นตอนของข้อมูลตั้งแต่เริ่มสร้างข้อมูลไปจนถึงการทำลายข้อมูล” ประกอบด้วย 6 ขั้นตอน ดังนี้

1) **กระบวนการสร้างข้อมูล (Create)** เป็นการสร้างข้อมูลขึ้นมาใหม่ โดยวิธีการบันทึกเข้าไปด้วยบุคคลหรือบันทึกอัตโนมัติด้วยอุปกรณ์อิเล็กทรอนิกส์ เช่น อุปกรณ์ตรวจจับสัญญาณ (Sensor) รวมถึงการซื้อข้อมูล หรือการรับข้อมูลจากหน่วยงานอื่น เพื่อนำมาจัดเก็บในภายหลัง
2) **กระบวนการจัดเก็บข้อมูล (Store)** เป็นการจัดเก็บข้อมูลที่เกิดจากกระบวนการสร้าง หรือข้อมูลที่ได้จากการแลกเปลี่ยนกับหน่วยงานอื่น เพื่อให้มีระเบียบ ง่ายต่อการใช้งาน ไม่สูญหาย หรือถูกทำลายและให้ผู้ใช้งานสามารถประมวลผลข้อมูลต่าง ๆ ตามความต้องการได้อย่างรวดเร็ว ไม่ว่าจะจัดเก็บลงแฟ้มข้อมูล (File) หรือระบบการจัดการฐานข้อมูล (Database Management System - DBMS)
3) **กระบวนการใช้ข้อมูล (Use)** เป็นการนำข้อมูลที่จัดเก็บมาประมวลผล เช่น การถ่ายโอนข้อมูล การเปลี่ยนรูปแบบการจัดเก็บข้อมูล การวิเคราะห์ข้อมูล การจัดทำรายงาน เพื่อนำข้อมูลเหล่านั้นมาใช้งานให้เกิดประโยชน์ตามวัตถุประสงค์ รวมถึงการสำรอง (Backup) ข้อมูล โดยการคัดลอกข้อมูลที่ใช้งานอยู่ในปัจจุบัน เพื่อทำสำเนา เช่น ใช้โปรแกรมในการสำรองข้อมูล เป็นการหลีกเลี่ยงความเสียหายที่จะเกิดขึ้นหากข้อมูลเกิดการเสียหายหรือสูญหาย ซึ่งสามารถนำข้อมูลที่สำรองไว้ในสื่อบันทึกข้อมูลกลับมาใช้งานได้ทันที โดยการกู้คืน (Restore)
4) **กระบวนการเผยแพร่ข้อมูล (Publish)** เป็นการแชร์ข้อมูล (Sharing) การกระจายข้อมูล (Dissemination) การควบคุมการเข้าถึง (Access Control) การแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน(Exchange) และการกำหนดเงื่อนไขในการนำข้อมูลไปใช้ (Condition)
5) **กระบวนการจัดเก็บข้อมูลถาวร (Archive)** เป็นการคัดลอกเอาข้อมูลที่มีช่วงอายุเกินช่วงใช้งานหรือไม่ได้ใช้งานแล้ว เพื่อทำสำเนาสำหรับการเก็บรักษา โดยที่ข้อมูลนั้นไม่มีการลบ ปรับปรุงหรือแก้ไขอีก และสามารถนำกลับไปใช้งานได้ใหม่เมื่อต้องการ
6) **กระบวนการทำลายข้อมูล (Destroy)** เป็นการทำลายข้อมูล ซึ่งปกติจะเป็นการทำลายข้อมูลที่มีการจัดเก็บถาวรเป็นระยะเวลานานหรือเกินกว่าระยะเวลาที่กำหนด

2.3. ความสัมพันธ์ระหว่างธรรมาภิบาลข้อมูลกับการบริหารจัดการข้อมูล

ธรรมาภิบาลข้อมูล (Data Governance) เป็นตัวกำหนดทิศทาง ควบคุม และในขณะที่การบริหารจัดการข้อมูล (Data Management) เป็นการนำหลักการไปปฏิบัติทำให้เกิดผลลัพธ์ที่เป็นรูปธรรมในทางปฏิบัติ โดยธรรมาภิบาลจะกำหนดว่าข้อมูลควรจัดการอย่างไร ส่วนการบริหารจัดการจะดำเนินการตามแนวทางที่กำหนดไว้

การวางแผนบริหารจัดการข้อมูลควรเริ่มต้นจากการจัดตั้งธรรมาภิบาลข้อมูล เพื่อเป็นกรอบในการกำหนดบทบาท หน้าที่ ความรับผิดชอบ และการตัดสินใจอย่างชัดเจน สร้างความเชื่อมั่นในความเป็นระเบียบถูกต้อง และยั่งยืน โดยธรรมาภิบาลข้อมูลต้องมีบทบาทในทุกกิจกรรมของการบริหารจัดการข้อมูล ซึ่งทั้งสอง

ด้านต่างมีเป้าหมายร่วมกันในการยกระดับคุณภาพ ความเชื่อถือได้ ความปลอดภัย และการใช้ประโยชน์จากข้อมูลอย่างมีประสิทธิภาพ องค์กรที่สามารถบริหารจัดการข้อมูลได้สำเร็จจึงต้องมีทั้งธรรมาภิบาลข้อมูลที่เข้มแข็งและการจัดการข้อมูลที่มีประสิทธิภาพควบคู่กันอย่างสอดประสาน

2.4. คำนิยามและคำจำกัดความที่สำคัญ (Key Definitions and Terminology)

สกพอ.	หมายถึง	สำนักงานคณะกรรมการนโยบายเขตพัฒนาพิเศษภาคตะวันออก
คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council)	หมายถึง	คณะกรรมการธรรมาภิบาลข้อมูลของ สกพอ.
ธรรมาภิบาลข้อมูล (Data Governance)	หมายถึง	การกำหนดสิทธิ หน้าที่ และความรับผิดชอบของผู้มีส่วนได้เสียในการบริหารจัดการข้อมูลภาครัฐทุกขั้นตอน เพื่อให้การได้มาและการนำข้อมูลของหน่วยงานไปใช้อย่างถูกต้อง ครบถ้วน เป็นปัจจุบัน รักษาความเป็นส่วนบุคคล และสามารถเชื่อมโยงแลกเปลี่ยน และบูรณาการระหว่างกันได้อย่างมีประสิทธิภาพและมั่นคงปลอดภัย โดยใช้ข้อมูลเป็นหลักในการบริหารงานภาครัฐและการบริการสาธารณะ
ข้อมูล (Data)	หมายถึง	สิ่งที่สื่อความหมายให้รู้เรื่องราวข้อเท็จจริงหรือเรื่องอื่นใด ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเอง หรือโดยผ่านวิธีการใด ๆ และไม่ว่าจะได้จัดทำไว้ในรูปของเอกสารแฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ภาพถ่ายดาวเทียม ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ เครื่องมือตรวจวัด การสำรวจระยะไกล หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้
ชุดข้อมูล (Dataset)	หมายถึง	การนำข้อมูลจากหลายแหล่งมารวบรวม เพื่อจัดเป็นชุดให้ตรงตามลักษณะโครงสร้างของข้อมูล หรือจากการใช้ประโยชน์ของข้อมูล
บัญชีข้อมูล (Data Catalog)	หมายถึง	เอกสารแสดงบรรดารายการของชุดข้อมูล ที่จำแนกแยกแยะโดยการจัดกลุ่มหรือจัดประเภทข้อมูลที่อยู่ในความครอบครองหรือควบคุมของหน่วยงาน
หมวดหมู่ของข้อมูล (Data Category)	หมายถึง	ตามกรอบธรรมาภิบาลข้อมูลภาครัฐแบ่งออกได้เป็น 4 หมวดหมู่ ได้แก่ ข้อมูลส่วนบุคคล ข้อมูลความมั่นคง ข้อมูลความลับทางราชการ และ ข้อมูลสาธารณะ
เมทาดาตา (Metadata)	หมายถึง	คำอธิบายชุดข้อมูลดิจิทัล เป็นข้อมูลที่ใช้อธิบายข้อมูลหลักหรือกลุ่มข้อมูลอื่น ๆ ที่เกี่ยวข้องทั้งกระบวนการเชิงธุรกิจและเชิงเทคโนโลยีสารสนเทศ
พจนานุกรมข้อมูล (Data Dictionary)	หมายถึง	แหล่งรวบรวมและจัดเก็บคำอธิบายหรือเมตาดาทา (Metadata) ของข้อมูลที่ใช้ภายในระบบสารสนเทศหรือฐานข้อมูลอย่างเป็นระบบ

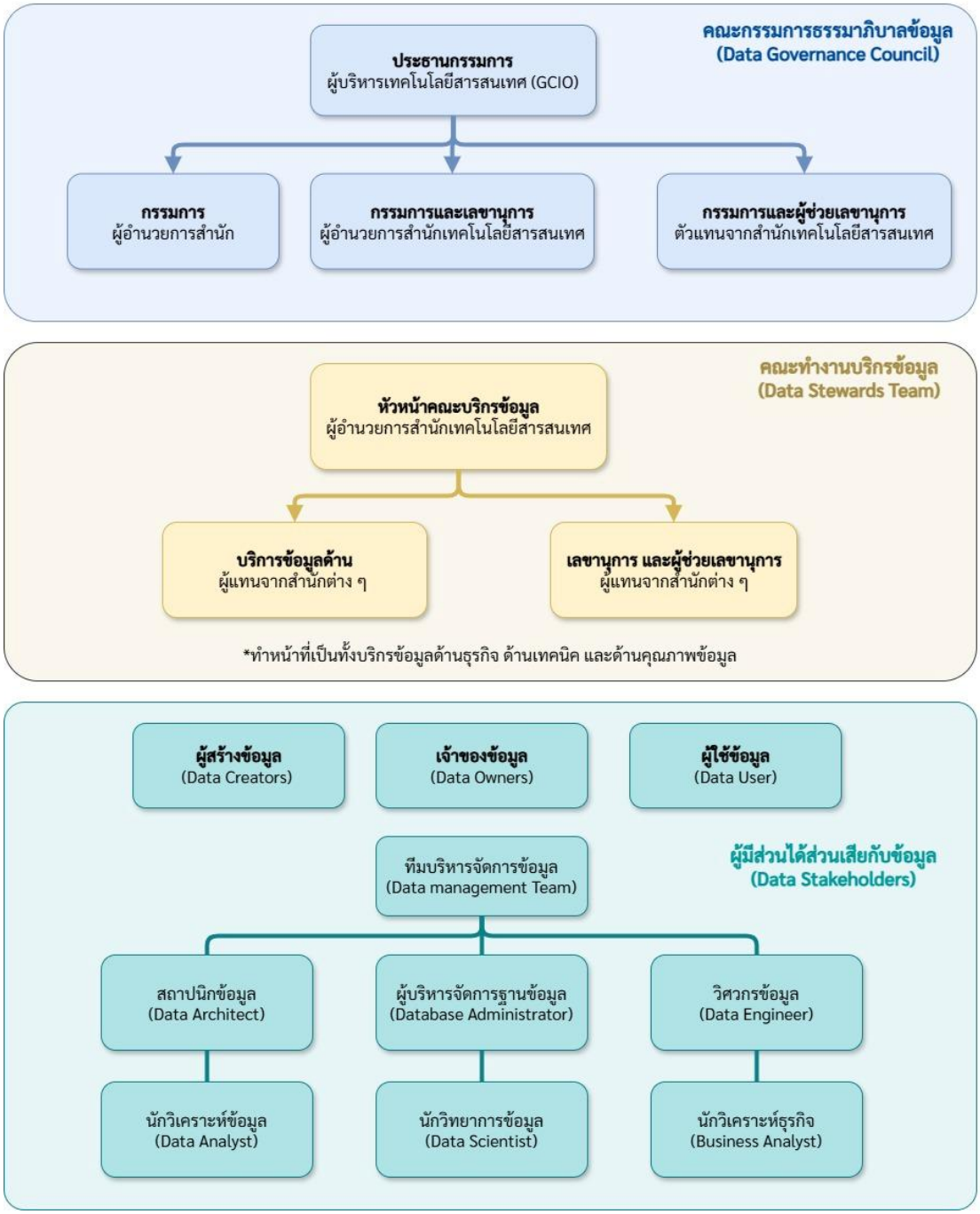
การบริหารจัดการข้อมูล (Data Management)	หมายถึง	กระบวนการอย่างเป็นระบบในการวางแผน การดำเนินการ และการควบคุมกิจกรรมต่าง ๆ ที่เกี่ยวข้องกับวงจรชีวิตของข้อมูล ตั้งแต่การรวบรวม การจัดเก็บ การจัดระเบียบ การรักษาความปลอดภัย การประมวลผล การวิเคราะห์ ไปจนถึงการนำข้อมูลไปใช้งานและการกำจัดทิ้ง
บริกรข้อมูล (Data Steward)	หมายถึง	บุคคลหรือกลุ่มบุคคลที่มีความรับผิดชอบหลักในการกำกับดูแล จัดการ และบำรุงรักษาคุณภาพและความถูกต้องของข้อมูล ภายในองค์กร
ผู้สร้างข้อมูล (Data Creator)	หมายถึง	บุคคลที่ทำหน้าที่ บันทึก แก้ไข ปรับปรุง หรือลบข้อมูลให้สอดคล้องกับโครงสร้างที่ถูกกำหนดไว้ นอกจากนี้ยังมีหน้าที่ในการทำงานร่วมกับบริกรข้อมูล เพื่อตรวจสอบและแก้ไขปัญหาด้านคุณภาพข้อมูลและความมั่นคงปลอดภัย
เจ้าของข้อมูล (Data Owner)	หมายถึง	บุคคลหรือหน่วยงานที่มีหน้าที่และความรับผิดชอบดูแลข้อมูลโดยตรง ชุดใดชุดหนึ่งภายในองค์กร โดยครอบคลุมถึงประเด็นสำคัญ เช่น การกำหนดนโยบายการเข้าถึง การใช้งาน การรักษาความปลอดภัย และคุณภาพของข้อมูลนั้น ๆ
ผู้ใช้ข้อมูล (Data User)	หมายถึง	บุคคลที่ทำหน้าที่นำข้อมูลไปใช้งานทั้งในระดับปฏิบัติงานและระดับบริหาร และสนับสนุนธรรมาภิบาลข้อมูลภาครัฐ โดยการให้ความต้องการในการใช้ข้อมูล พร้อมทั้งรายงานประเด็นปัญหาที่พบระหว่างการใช้ข้อมูล ทั้งด้านคุณภาพและความปลอดภัยของข้อมูลไปยังบริกรข้อมูล
ทีมบริหารจัดการข้อมูล (Data Management Team)	หมายถึง	ทีมตรวจสอบการปฏิบัติตามนโยบายข้อมูล ตรวจสอบคุณภาพ ตรวจสอบความมั่นคงปลอดภัยของข้อมูล วิเคราะห์ผลจากการ ตรวจสอบ
การจัดชั้นความลับของข้อมูล (Data Classification)	หมายถึง	การกำหนดประเภทและข้อกำหนดของการจัดชั้นความลับของข้อมูล เพื่อกำหนดสิทธิในการเข้าถึงและสามารถนำข้อมูลไปใช้ได้อย่างเหมาะสม ซึ่งตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 กำหนดให้มีชั้นความลับเป็น ชั้นลับ ชั้นลับมาก หรือ ชั้นลับที่สุด โดยคำนึงถึงการปฏิบัติหน้าที่ของหน่วยงานและประโยชน์แห่งรัฐประกอบกัน ดังนั้น ชั้นความลับของข้อมูลมักถูกกำหนดให้สอดคล้องกับผลกระทบต่อหน่วยงานและความมั่นคงของประเทศ อาทิ ชื่อเสียง ความต่อเนื่องของการดำเนินงาน การเงิน และทรัพยากรบุคคล

วงจรชีวิตของข้อมูล (Data Life Cycle)	หมายถึง	ลำดับขั้นตอนของข้อมูลตั้งแต่เริ่มสร้างข้อมูลไปจนถึงการทำลายข้อมูล ตามกรอบธรรมาภิบาลข้อมูลภาครัฐ
ข้อมูลหลักและข้อมูลอ้างอิง (Master and Reference Data)	หมายถึง	การบริหารจัดการข้อมูลเพื่อให้ทั้งหน่วยงานสามารถเข้าถึงและใช้ข้อมูลร่วมกันได้ โดยข้อมูลถูกจัดเก็บไว้แหล่งเดียว มีการกำหนดมาตรฐานของข้อมูล เพื่อช่วยลดความซ้ำซ้อนของข้อมูลและทำให้ข้อมูลมีคุณภาพ ซึ่ง Master data เป็นข้อมูลที่สร้างและถูกใช้งานอยู่ภายในหน่วยงาน มีโอกาสเปลี่ยนแปลงได้และมีรายละเอียดหรือจำนวนฟิลด์ข้อมูลที่มาก เช่น ข้อมูลพนักงาน ข้อมูลลูกค้า ข้อมูลผู้ขาย ข้อมูลสินค้าและบริการ ข้อมูลครุภัณฑ์ และข้อมูลสถานที่ ในขณะที่ Reference data มีความเป็นสากลถูกสร้างและใช้งานโดยทั่วไป โดยหลากหลายองค์กร หรือแม้กระทั่งใช้งานไปทั่วโลก เช่น รหัสไปรษณีย์ รหัสประเทศ หน่วยวัดระยะทาง

3. กรอบธรรมภิบาลข้อมูลของ สกพอ.

3.1. โครงสร้างธรรมาภิบาลข้อมูล (Data Governance Structure)

สกพอ. กำหนดโครงสร้างธรรมาภิบาลข้อมูลภาครัฐ เพื่อให้การบริหารจัดการข้อมูลของหน่วยงานเป็นไปอย่างมีประสิทธิภาพ โปร่งใส และมีความรับผิดชอบ จึงกำหนดบทบาทและความรับผิดชอบของผู้เกี่ยวข้องในระดับต่าง ๆ ดังนี้



จากรูป โครงสร้างธรรมาภิบาลข้อมูลของ สกพอ. แบ่งลำดับขั้นออกเป็นระดับที่ 1 คณะกรรมการธรรมาธิบาลข้อมูล ระดับที่ 2 คณะทำงานบริกรข้อมูล และระดับที่ 3 ผู้มีส่วนได้เสียกับข้อมูล ตามลำดับ โดยมีผู้บริหารเทคโนโลยีสารสนเทศเป็นประธานกรรมการ

3.2. บทบาทและความรับผิดชอบ (Roles and Responsibilities)

3.2.1. คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council)

คณะกรรมการธรรมาภิบาลข้อมูลของ สกพอ. ประกอบด้วย รองเลขาธิการ ที่ได้รับการแต่งตั้งให้เป็นผู้บริหารเทคโนโนโลยีสารสนเทศระดับกรมและดำรงตำแหน่งเป็นประธานคณะกรรมการธรรมาภิบาลข้อมูล โดยมีผู้อำนวยการสำนักเทคโนโลยีสารสนเทศเป็นกรรมการและเลขานุการ และผู้แทนจากสำนักต่าง ๆ เป็นกรรมการ โดยมีบทบาทหน้าที่ ตามรายละเอียดตารางที่ 1

ตารางที่ 1 ตำแหน่งและบทบาทหน้าที่ของคณะกรรมการธรรมาภิบาลข้อมูล

ลำดับ	ตำแหน่ง	บทบาทหน้าที่
1	ประธานกรรมการ ● ผู้บริหารเทคโนโนโลยีสารสนเทศระดับกรม (GCIO)	(1) กำหนดนโยบายธรรมาภิบาลข้อมูล (Data Governance Policy) แนวปฏิบัติ และแผนการดำเนินงานด้านธรรมภิบาลข้อมูลภาครัฐของ สกพอ. ให้สอดคล้องกับประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ (2) ส่งเสริมและสนับสนุนการดำเนินการตามนโยบายและแผนการดำเนินงานด้านธรรมาภิบาลข้อมูลตาม (1) เพื่อให้สามารถดำเนินการไปได้อย่างลุล่วง โดยจัดให้มีกลไกการตรวจสอบ วัดผล และรายงาน ตลอดจนการปรับปรุงอย่างต่อเนื่อง (3) กำกับดูแลการดำเนินการธรรมาภิบาลข้อมูล เพื่อให้ข้อมูลของสำนักงานมีความถูกต้อง ครบถ้วน เป็นปัจจุบัน มีความมั่นคงปลอดภัย และข้อมูลส่วนบุคคลได้รับการคุ้มครองอย่างเหมาะสม (4) กำกับดูแลการดำเนินงานของคณะทำงานบริกรข้อมูล (Data Steward Team) (5) กำกับดูแลการดำเนินการเกี่ยวกับข้อมูลของสำนักงาน เพื่อให้เป็นไปตามกฎหมายข้อมูลข่าวสารของราชการ กฎหมายคุ้มครองข้อมูลส่วนบุคคล กฎหมายการบริหารงานและการให้บริการภาครัฐผ่าน
2	กรรมการ ประกอบด้วย ● ผู้อำนวยการสำนักกฎหมาย ● ผู้อำนวยการสำนักยุทธศาสตร์องค์กร ● ผู้อำนวยการสำนักพัฒนาเขตส่งเสริมเศรษฐกิจพิเศษ ● ผู้อำนวยการสำนักพัฒนาพื้นที่และชุมชน 2 ● ผู้อำนวยการสำนักพัฒนาโครงสร้างพื้นฐานและสาธารณูปโภค ● ผู้อำนวยการสำนักยุทธศาสตร์การส่งเสริมและชักชวนนักลงทุน	
3	กรรมการและเลขานุการ ● ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ	
4	ผู้ช่วยเลขานุการ ● ผู้แทนสำนักเทคโนโลยีสารสนเทศ	

ลำดับ	ตำแหน่ง	บทบาทหน้าที่
		ระบบดิจิทัล และกฎหมายอื่น ๆ ที่เกี่ยวข้อง (6) แต่งตั้งคณะทำงานเพื่อสนับสนุนการดำเนินการธรรมาภิบาลข้อมูลและการปฏิบัติตามข้อกำหนดของกฎหมายที่เกี่ยวข้องตามความเหมาะสม

3.2.2. **คณะบริกรข้อมูล (Data Steward Team)**

คณะบริการข้อมูลของ สกพอ. ประกอบด้วย ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ ที่ได้รับการแต่งตั้งเป็นหัวหน้าคณะบริกรข้อมูล ผู้แทนสำนักต่าง ๆ ทำหน้าที่เป็นบริกรข้อมูลและเลขานุการ โดยมีอำนาจหน้าที่ให้ความรู้เกี่ยวกับนโยบายข้อมูลและความรู้อื่น ๆ ที่จะสนับสนุนให้เกิดธรรมาภิบาลข้อมูลภาครัฐที่ดีภายใน สกพอ. และคณะบริกรข้อมูลรับคำสั่งโดยตรงจากคณะกรรมการธรรมาภิบาลข้อมูลของ สกพอ. แต่ในขณะเดียวกันมีการให้ข้อมูลสนับสนุนในการตัดสินใจต่อคณะกรรมการธรรมาภิบาลข้อมูลของ สกพอ. ด้วย ตามรายละเอียดตารางที่ 2

ตารางที่ 2 ตำแหน่งและบทบาทหน้าที่ของคณะบริการข้อมูล

ลำดับ	ตำแหน่ง	บทบาทหน้าที่
1	หัวหน้าคณะบริกรข้อมูล (Lead Data Steward) ● ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ	(1) จัดทำร่างธรรมาภิบาลข้อมูลโดยกำหนดนโยบายข้อมูล จำแนกหมวดหมู่ของข้อมูล มาตรการ ควบคุมและพัฒนาคุณภาพข้อมูล เพื่อให้ข้อมูลมีความถูกต้อง ครบถ้วน เป็นปัจจุบัน มั่นคงปลอดภัย และไม่ละเมิดความเป็นส่วนบุคคลรวมทั้งสามารถเชื่อมโยงข้อมูลแลกเปลี่ยนบูรณาการ และใช้ประโยชน์ได้อย่างมีประสิทธิภาพ (2) กำหนดความต้องการด้านคุณภาพข้อมูล และความมั่นคงปลอดภัยจากผู้ใช้ข้อมูลหรือผู้มีส่วนได้ส่วนเสียกับข้อมูล (3) กำหนดนิยามพร้อมจัดทำคำอธิบายชุดข้อมูลดิจิทัล หรือเมทาดาตา และบัญชีข้อมูลให้ครบถ้วน ตามความจำเป็นในการใช้งาน และ
2	บริกรข้อมูลซึ่งทำหน้าที่เป็นบริกรข้อมูลด้านธุรกิจ (Business Data Stewards) บริกรข้อมูลด้านเทคนิค (Technical Data Stewards) และบริกรข้อมูลด้านคุณภาพข้อมูล (Data Quality Stewards) เป็นผู้แทนจากสำนักต่าง ๆ ประกอบด้วย ● สำนักกฎหมาย ● สำนักยุทธศาสตร์องค์กร ● สำนักพัฒนาเขตส่งเสริมเศรษฐกิจพิเศษ ● สำนักพัฒนาพื้นที่และชุมชน 2 ● สำนักพัฒนาโครงสร้างพื้นฐานและสาธารณูปโภค	

ลำดับ	ตำแหน่ง	บทบาทหน้าที่
	● สำนักยุทธศาสตร์การส่งเสริมและชักชวนนักลงทุน ● สำนักเทคโนโลยีสารสนเทศ นอกจากนี้ มีผู้เกี่ยวข้องเพิ่มเติมได้แก่ ผู้ดูแลความปลอดภัยข้อมูล (Information Security Officer) และผู้ดูแลข้อมูลส่วนบุคคล (Data Protection Officer)	ตรงตามความต้องการของผู้มีส่วนได้ส่วนเสียกับข้อมูล (4) วิเคราะห์ความพร้อมของธรรมาภิบาลข้อมูลภาครัฐของ สกพอ. ความต้องการด้านคุณภาพข้อมูล การรักษาความเป็นส่วนบุคคลและความมั่นคงปลอดภัย ให้เหมาะสมกับสถานการณ์ปัจจุบัน เพื่อวางแผนการวัดและประเมินผล (5) ดำเนินงานให้สอดคล้องกับนโยบายเป้าประสงค์ความต้องการของผู้มีส่วนได้ส่วนเสียกับข้อมูลรวมทั้งติดตามการดำเนินงานตามแผนที่กำหนดเพื่อตรวจสอบการปฏิบัติตามนโยบายข้อมูล (6) ตรวจสอบ วิเคราะห์ และวัดผลการดำเนินงาน (7) ทบทวนและปรับปรุงกระบวนการ เพื่อนำมาปรับปรุงกระบวนการทำงาน (8) กำหนดรายละเอียดที่เกี่ยวข้องกับการออกแบบระบบเทคโนโลยีสารสนเทศรวมถึงโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ เพื่อคุ้มครองข้อมูลและรักษาความมั่นคงปลอดภัย (9) รายงานผลลัพธ์ไปยังคณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council) ของ สกพอ. และผู้ที่เกี่ยวข้อง (10) สนับสนุนการดำเนินงานด้านเทคโนโลยีสารสนเทศและอื่น ๆ ที่เกี่ยวข้อง รวมทั้งให้ข้อเสนอแนะเชิงเทคนิคที่สอดคล้องกับนโยบายและเป้าประสงค์ ความต้องการของผู้มีส่วนได้ส่วนเสียกับข้อมูล (11) ปฏิบัติงานอื่นที่คณะกรรมการธรรมาภิบาลของ สกพอ. มอบหมาย
3	เลขานุการ และผู้ช่วยเลขานุการ ● สำนักเทคโนโลยีสารสนเทศ	

3.2.3. ผู้มีส่วนได้ส่วนเสียกับข้อมูล (Data Stakeholders)

ผู้มีส่วนได้เสียกับข้อมูลมีส่วนร่วมในการดำเนินงานด้านธรรมาภิบาลข้อมูล โดยมีบทบาทสำคัญในการจัดการข้อมูลในองค์กรโดยตรง หรือโดยอ้อมกับวงจรชีวิตของข้อมูล ตั้งแต่การจัดเก็บ การจัดการ การใช้ การวิเคราะห์ การรักษาความปลอดภัย ไปจนถึงการนำข้อมูลไปใช้ในการตัดสินใจหรือการบริการ ซึ่งประกอบด้วย ผู้สร้างข้อมูล (Data Creators) เจ้าของข้อมูล (Data Owners) ทีมบริหารจัดการข้อมูล (Data Management Team) และผู้ใช้ข้อมูล (Data Users) โดยมีบทบาทหน้าที่ ดังนี้

ลำดับ	ตำแหน่ง	บทบาทหน้าที่
1	ผู้สร้างข้อมูล (Data Creators)	ทำหน้าที่ สร้าง บันทึกข้อมูลใหม่ แก้ไข ปรับปรุง หรือลบข้อมูลเข้าสู่ระบบหรือแหล่งจัดเก็บข้อมูลขององค์กรให้สอดคล้องกับโครงสร้างที่ถูกกำหนดไว้ นอกจากนี้ยังมีหน้าที่ในการทำงานร่วมกับบริกรข้อมูล เพื่อตรวจสอบ และแก้ไขปัญหาด้านคุณภาพข้อมูลและความมั่นคงปลอดภัย เช่น เจ้าหน้าที่รับคำขอสิทธิประโยชน์ เจ้าหน้าที่รับคำขออนุมัติ อนุญาตก่อสร้าง เป็นต้น
2	เจ้าของข้อมูล (Data Owners)	บุคคลที่มีหน้าที่และความรับผิดชอบดูแลข้อมูลโดยตรง สร้างความมั่นใจได้ว่าการบริหารจัดการข้อมูลสอดคล้องกับนโยบาย มาตรฐาน กฎระเบียบ หรือกฎหมาย เจ้าของข้อมูลทำการทบทวนและอนุมัติการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับข้อมูล เช่น การเปลี่ยนแปลงเมทาดาตาและเกณฑ์ การทำดาตาคลีนซิ่ง (Data Cleansing) นอกจากนี้ยังมีหน้าที่ในการให้สิทธิในการเข้าถึงข้อมูลและจัดชั้นความลับ ของข้อมูล เจ้าของข้อมูลมักจะอยู่ในตำแหน่งบริหาร เช่น ผู้อำนวยการสำนัก เป็นต้น
3	ทีมบริหารจัดการข้อมูล (Data Management Team)	มีหน้าที่หลักในการบริหารจัดการข้อมูล สอดคล้องกับหลักการบริหารจัดการข้อมูล 10 องค์ประกอบ ● สถาปัตยกรรมข้อมูล (Data Architecture) ● การจำลองและการออกแบบข้อมูล (Data Modeling and Design) ● การจัดเก็บและการดำเนินการกับข้อมูล (Data Storage and Operations) ● การบูรณาการและความสามารถในการทำงานร่วมกัน (Data Integration and Interoperability)

ลำดับ	ตำแหน่ง	บทบาทหน้าที่
		● การบริหารจัดการเอกสาร และเนื้อหา (Document and Content Management) ● ข้อมูลหลักและข้อมูลอ้างอิง (Master and Reference Data) ● คลังข้อมูล ดาตาเลค ระบบรายงานอัจฉริยะ และดาตาอนาไลติกส์ (Data Warehouse, Data Lake, Business Intelligence, and Data Analytics) ● คำอธิบายชุดข้อมูลดิจิทัล หรือเมทาดาตา (Metadata) ความมั่นคงปลอดภัยและการรักษาความเป็นส่วนบุคคลของข้อมูล (Data Security and Privacy) ● คุณภาพของข้อมูล (Data Quality) นอกจากนี้ ทำหน้าที่ตรวจสอบการปฏิบัติตามนโยบายข้อมูล ทีมบริหารจัดการข้อมูลสนับสนุนกิจกรรมของธรร มาภิบาลข้อมูลภาครัฐ เช่น ช่วยเหลือในการนิยามเมทาดาตา ร่างนโยบายข้อมูล และ มาตรฐานข้อมูล และกำหนดสิทธิการเข้าถึงข้อมูล รายละเอียดบทบาทและความรับผิดชอบของทีมบริหาร จัดการข้อมูล
4	ผู้ใช้ข้อมูล (Data Users)	บุคคลที่ทำหน้าที่นำข้อมูลไปใช้งานทั้งในระดับปฏิบัติงานและระดับบริหาร และสนับสนุนธรรมาภิบาลข้อมูลภาครัฐโดยการให้ความต้องการในการใช้ข้อมูล พร้อมทั้งรายงานประเด็นปัญหาที่พบระหว่างการใช้ข้อมูล ทั้งด้านคุณภาพและความปลอดภัยของข้อมูลไปยังบริกรข้อมูล ซึ่งบทบาทผู้ใช้ข้อมูลนี้ครอบคลุมถึงผู้บริหาร ผู้เชี่ยวชาญเฉพาะด้าน ตลอดจนเจ้าหน้าที่ทั้งหมดภายใน สกพอ.

4. กระบวนการธรรมาภิบาลข้อมูลภาครัฐ (Data Governance Processes)

กระบวนการธรรมาภิบาลข้อมูลภาครัฐเป็นขั้นตอนที่ใช้สำหรับกำกับดูแลการดำเนินการ บริหารและกระบวนการจัดการข้อมูลตั้งแต่ การสร้างข้อมูล การจัดเก็บข้อมูล (รวมการจัดเก็บถาวร) การประมวลผลข้อมูลและการใช้ข้อมูล การเปิดเผยข้อมูล การทำลายข้อมูล และการเชื่อมโยงและการแลกเปลี่ยนข้อมูล โดยสร้างกลไกในการกำหนดแนวทาง เพื่อควบคุมข้อมูลให้เป็นไปตาม กฎ ระเบียบ ข้อบังคับ หรือนโยบายที่เกี่ยวข้องกับข้อมูล มี 4 ขั้นตอนดังรายละเอียดดังนี้

4.1. การวางแผน (Plan) เป็นขั้นตอนการกำหนดเป้าหมาย กำหนดนโยบาย และวางแผนการดำเนินการทั้งหมดที่เกี่ยวข้องกับธรรมาภิบาลข้อมูล

4.1.1. กำหนดเป้าหมาย วัตถุประสงค์ และขอบเขตของธรรมาภิบาลข้อมูล

4.1.2. กำหนดโครงสร้างองค์กรและกำหนดบทบาทความรับผิดชอบ ได้แก่ การแต่งตั้งคณะกรรมการธรรมาภิบาลข้อมูล การแต่งตั้งคณะบริการข้อมูล

4.1.3. การพัฒนานโยบาย มาตรฐาน และแนวปฏิบัติของข้อมูล ได้แก่ การกำหนดนิยามข้อมูล กำหนดนโยบายข้อมูล (Data Policy) มาตรฐานข้อมูล และการจัดทำแนวทางปฏิบัติ/ขั้นตอนปฏิบัติสำหรับการปฏิบัติงาน เช่น มาตรฐานเมทาดาตา มาตรฐานชุดข้อมูล และมาตรฐานการจัดชั้นความลับของข้อมูล

4.1.4. การยกร่างนโยบายข้อมูล (Data Policy) ซึ่งประกอบไปด้วยร่างนโยบายการบริหารจัดการข้อมูล และร่างแนวปฏิบัติการบริหารจัดการข้อมูล

4.1.5. การกำหนดชุดข้อมูลตั้งต้นพร้อมจัดทำบัญชีข้อมูล และคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตา

4.1.6. การวางแผนการสื่อสารและการฝึกอบรมกับผู้ที่เกี่ยวข้อง

4.2. การปฏิบัติ (Do) ขั้นตอนการนำแผนที่วางไว้ไปปฏิบัติจริง

4.2.1. การประกาศใช้อย่างเป็นทางการ และการปฏิบัติตามนโยบายและมาตรฐานที่กำหนดไว้ ได้แก่ การบังคับใช้นโยบายข้อมูล (Data Policy) มาตรฐานข้อมูล และแนวทางปฏิบัติ/ขั้นตอนปฏิบัติสำหรับการปฏิบัติงาน

4.2.2. การดำเนินการจัดการด้านข้อมูล ได้แก่ คุณภาพข้อมูล (Data Quality) เมทาดาตา (Metadata) ลำดับข้อมูล (Data Lineage) การเผยแพร่ Data Catalog และ Data Dictionary ให้ผู้ที่เกี่ยวข้องเข้าถึง และการจัดการความปลอดภัยและการบังคับใช้มาตรการควบคุมการเข้าถึงข้อมูลตามบทบาท และการจัดชั้นความลับของข้อมูล (Data Classification)

4.2.3. การสื่อสารและการฝึกอบรมกับผู้ที่เกี่ยวข้อง ได้แก่ การติดประกาศ เว็บไซต์ บันทึกภายใน การสื่อสารในที่ประชุมของ สกพอ. การอบรมให้กับพนักงานตามแผนที่วางไว้ ตลอดจนการสื่อสารข้อมูลที่สำคัญเกี่ยวกับการบริหารจัดการข้อมูลอย่างต่อเนื่อง

4.3. **การติดตามดำเนินงาน/ตรวจสอบ/วัดผล และรายงานผล (Check, Measure and Report)** ขั้นตอนของการตรวจสอบและประเมินว่าผลการปฏิบัติงานตามแผนที่วางไว้และเกิดผลลัพธ์ตามที่คาดหวัง

4.3.1. การติดตาม ตรวจสอบการปฏิบัติตามนโยบาย เช่น การทำตรวจสอบภายในเป็นระยะ ๆ ให้มั่นใจว่าพนักงานได้ปฏิบัติตามนโยบายและขั้นตอนที่กำหนด

4.3.2. การวัดผลตามเกณฑ์การตรวจสอบและประเมินที่ได้กำหนดไว้ เช่น วัดผลคุณภาพข้อมูลอัตราความถูกต้อง ความครบถ้วน เป็นต้น

4.3.3. การรวบรวมข้อมูลเสนอแนะและปัญหาที่เกี่ยวกับการบริหารจัดการข้อมูล เพื่อนำมาเสนอคณะทำงานที่เกี่ยวข้องในการปรับปรุงให้นโยบายและแนวปฏิบัติ

4.4. การปรับปรุงอย่างต่อเนื่อง (Continual Improvement) ขั้นตอนการนำผลการดำเนินงานมาวิเคราะห์และปรับปรุงแก้ไข เพื่อให้นโยบายและการปฏิบัติมีประสิทธิภาพมากยิ่งขึ้น และจะนำข้อเสนอแนะไปสู่ขั้นตอนการวานแผน (Plan)

4.4.1. การจัดทำรายงานผลการตรวจสอบความสอดคล้องของการดำเนินงานต่อนโยบายข้อมูล รายงานคุณภาพข้อมูล และรายงานผลการประเมินความเสี่ยงข้อมูล

4.4.2. กำหนดแนวทางแก้ไขและปรับปรุงพัฒนาให้สอดคล้องกับความต้องการทางธุรกิจและสภาพแวดล้อมที่เปลี่ยนแปลงไปเสมอ เช่น แก้ไขนโยบาย ปรับปรุงขั้นตอน ปรับปรุงระบบหรือเครื่องมือที่ใช้ในการบริหารจัดการข้อมูล เพิ่มการสื่อสารและการฝึกอบรม เป็นต้น

5. แนวทางการจัดการกระบวนการธรรมาภิบาลข้อมูลภาครัฐ (Data Governance Process Guidelines)

แนวทางการจัดการกระบวนการธรรมาภิบาลข้อมูลภาครัฐมีความสำคัญที่จะช่วยให้เราเข้าใจถึงกระบวนการทั้งหมด และนำไปประยุกต์ใช้ได้อย่างมีประสิทธิภาพยิ่งขึ้น โดยจะแนวทางนี้จะแสดงให้เห็นถึงความสัมพันธ์ ที่ชัดเจนระหว่างองค์ประกอบหลัก ได้แก่

- **กระบวนการธรรมาภิบาลข้อมูล:** ขั้นตอนและกิจกรรมที่เกี่ยวข้องกับการบริหารจัดการข้อมูล
- **เครื่องมือและเอกสาร:** สิ่งที่ใช้ในการดำเนินงานธรรมาภิบาลข้อมูล (เช่น นโยบาย, มาตรฐาน, คู่มือ)
- **ผลลัพธ์:** ประโยชน์หรือสิ่งที่องค์กรได้รับจากการมีธรรมาภิบาลข้อมูลที่ดี
- **ผู้เกี่ยวข้อง/ผู้มีส่วนได้เสีย:** บุคคลหรือหน่วยงานที่เกี่ยวข้องกับข้อมูลและได้รับผลกระทบจากธรรมาภิบาลข้อมูล

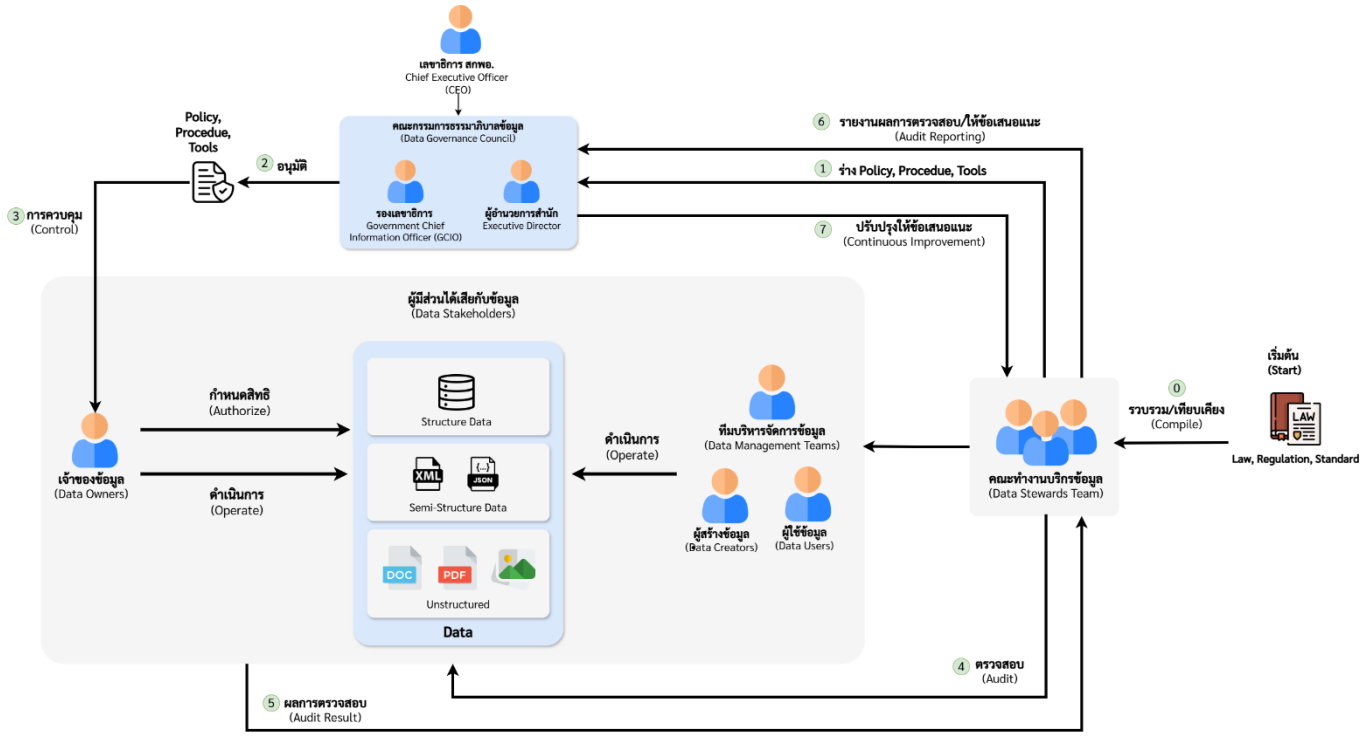
นอกจากนี้ แนวทางดังกล่าวจะมีรายละเอียดการดำเนินงานธรรมาภิบาลข้อมูลภาครัฐ โดยเน้นย้ำถึงความสัมพันธ์ระหว่าง กระบวนการ (Process) ส่วนนำเข้า (Inputs) ส่วนนำออก (Outputs) และ ผู้มีส่วนได้เสีย (Stakeholders) ที่เกี่ยวข้องกับข้อมูลอย่างเป็นระบบ

ตารางที่ 3 ความสัมพันธ์ระหว่างกระบวนการ ส่วนนำเข้า ส่วนนำออก และผู้มีส่วนได้เสียกับข้อมูล

กระบวนการ (Processes)	ส่วนนำเข้า (Input)	ส่วนนำออก (Output)	ผู้มีส่วนได้เสียกับข้อมูล (Data Stakeholder)
1. การวางแผน (Plan)	1) นโยบาย กฎ ระเบียบ ข้อบังคับ และกฎหมายที่เกี่ยวข้องกับข้อมูล 2) รายการชุดข้อมูล 3) รายการประเด็นปัญหาจากรายงานผลการตรวจสอบความสอดคล้องของการดำเนินงานต่อนโยบายข้อมูลรายงานคุณภาพข้อมูล รายงานความมั่นคงปลอดภัยต่อข้อมูล และรายงานความเสี่ยงต่อข้อมูล	1) แผนดำเนินการ (กิจกรรมบุคลากร งบประมาณ และระยะเวลาในการดำเนินการ) 2) โครงสร้างธรรมาภิบาลข้อมูล 3) กระบวนการธรรมาภิบาลข้อมูล 4) เกณฑ์การประเมินความพร้อมของธรรมาภิบาลข้อมูลระดับคุณภาพข้อมูล	1) ผู้บริหารระดับสูง 2) คณะกรรมการธรรมาภิบาลข้อมูล 3) คณะบริกรข้อมูล
2. การปฏิบัติ (Do)	1) นโยบาย กฎ ระเบียบ ข้อบังคับ และกฎหมายที่เกี่ยวข้องกับข้อมูล 2) แผนดำเนินการ (ขอบเขต เวลา และต้นทุน)	1) รายงานความก้าวหน้าในการปฏิบัติงาน 2) ผลการปฏิบัติงาน 3) ประเด็นปัญหาที่พบระหว่างปฏิบัติงาน	1) ผู้บริหารงาน 2) คณะกรรมการธรรมาภิบาลข้อมูล 3) คณะบริกรข้อมูล 4) ผู้ปฏิบัติงานที่เกี่ยวข้อง
3. การติดตามดำเนินงาน/ตรวจสอบ/วัดผล และรายงานผล (Check, Measure and Report)	1) นโยบาย กฎ ระเบียบ ข้อบังคับ และกฎหมายที่เกี่ยวข้องกับข้อมูล 2) เกณฑ์การประเมินความพร้อมของธรรมาภิบาลข้อมูลภาครัฐ ระดับคุณภาพข้อมูล	1) รายงานผลการตรวจสอบความสอดคล้องของการดำเนินงานต่อนโยบายข้อมูล 2) รายงานคุณภาพข้อมูล 3) รายงานความมั่นคงปลอดภัยต่อข้อมูล 4) รายงานความเสี่ยงต่อข้อมูล	1) คณะบริกรข้อมูล
4. การปรับปรุงอย่างต่อเนื่อง (Continual Improvement)	1) นโยบาย กฎ ระเบียบ ข้อบังคับ และกฎหมายที่เกี่ยวข้องกับข้อมูล 2) โครงสร้างธรรมาภิบาลข้อมูลภาครัฐ	1) กระบวนการธรรมาภิบาลข้อมูล 2) นโยบาย กฎ ระเบียบ ข้อบังคับและกฎหมาย ที่เกี่ยวข้องกับข้อมูล 3) เกณฑ์การประเมินความพร้อม	1) ผู้บริหารระดับสูง 2) คณะกรรมการธรรมาภิบาลข้อมูล 3) คณะบริกรข้อมูล

กระบวนการ (Processes)	ส่วนนำเข้า (Input)	ส่วนนำออก (Output)	ผู้มีส่วนได้เสียกับข้อมูล (Data Stakeholder)
	3) เกณฑ์การประเมินความพร้อมของธรรมาภิบาลข้อมูลภาครัฐ และระดับคุณภาพข้อมูล 4) รายงานผลการตรวจสอบความสอดคล้องของการดำเนินงานต่อนโยบายข้อมูล รายงานความมั่นคงปลอดภัยต่อข้อมูล และรายงานความเสี่ยงต่อข้อมูล 5) รายการความต้องการจากผู้บริหารและผู้มีส่วนได้ส่วนเสีย	ของธรรมาภิบาลข้อมูล และระดับคุณภาพข้อมูล 4) โครงสร้างธรรมาภิบาลข้อมูล	

แผนภาพแสดงความสัมพันธ์การทำงานระหว่างตามโครงสร้างธรรมาภิบาลข้อมูล อ้างอิงตาม สพร.



6. นโยบายข้อมูล (Data Policies) ของ สกพอ.

เพื่อให้ธรรมาภิบาลข้อมูลภาครัฐมีประสิทธิภาพ จึงต้องมีการกำหนดนโยบาย สอดคล้องกับพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ ประกาศ ณ วันที่ 12 มีนาคม 2563 ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล และกฎหมายหรือข้อกำหนดอื่น ๆ ที่เกี่ยวข้อง โดยผ่านการอนุมัติจากคณะกรรมการธรรมาภิบาลข้อมูลของ สกพอ. และมีการเผยแพร่และสื่อสารให้กับเจ้าหน้าที่ สกพอ. และผู้ที่เกี่ยวข้องทั้งภายในและภายนอกหน่วยงาน

เพื่อให้นโยบายข้อมูลได้ถูกนำมาปฏิบัติอย่างมีประสิทธิภาพและต่อเนื่อง และให้เจ้าหน้าที่ทุกระดับได้รับทราบและถือปฏิบัติ ตามนโยบายนี้อย่างเคร่งครัด โดยนโยบายนี้ต้องได้รับการทบทวนอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ หรือเมื่อคณะกรรมการธรรมาภิบาลข้อมูลของ สกพอ. เห็นสมควร โดยนโยบายข้อมูลควรจะครอบคลุมระบบบริหารและกระบวนการจัดการข้อมูลหรือวงจรชีวิตของข้อมูล ซึ่งอาจจะประกอบไปด้วยนโยบาย และแนวปฏิบัติต่าง ๆ ทั้งนี้ สกพอ. จัดทำนโยบายและแนวปฏิบัติ ได้แก่ นโยบายข้อมูล (Data Policy) นโยบายการบริหารจัดการข้อมูล (Data Management Policy) และแนวปฏิบัติการบริหารจัดการข้อมูล (Data Management Guideline) รายละเอียดดังนี้

6.1. นโยบายข้อมูล (Data Policy)

เป็นนโยบายระดับสูง ที่กำหนดแนวทาง กระบวนการ และหลักเกณฑ์ในการจัดการข้อมูลตลอดวงจรชีวิตของข้อมูล โดยมีเป้าหมายเพื่อกำหนดทิศทางและเป้าหมายในการใช้ข้อมูลภายในองค์กรให้เป็นไปอย่างมีธรรมาภิบาล สร้างคุณค่า และเพิ่มประสิทธิภาพในการดำเนินงาน นโยบายนี้จะกำหนดหลักการทั่วไป ความคาดหวัง และแนวปฏิบัติในการใช้ข้อมูล เพื่อให้มั่นใจว่าข้อมูลได้รับการจัดการอย่างเหมาะสม ครอบคลุมตั้งแต่การจัดเก็บ ใช้งาน ไปจนถึงการทำลายข้อมูลอย่างปลอดภัย

รายละเอียดนโยบายข้อมูล (Data Policy) สกพอ. ดังภาคผนวก ข

6.2. นโยบายการบริหารจัดการข้อมูล (Data Management Policy)

เป็นแนวนโยบายระดับหลักการ/ข้อกำหนด ที่ชัดเจนในการจัดการข้อมูลตลอดวงจรชีวิต โดยอ้างอิงถึงมาตรฐาน แนวทาง และเครื่องมือที่ใช้ในการบริหารจัดการข้อมูลอย่างเป็นระบบ มีวัตถุประสงค์เพื่อถ่ายทอดหลักการจากนโยบายข้อมูล (Data Policy) ไปสู่การปฏิบัติให้เกิดผลอย่างเป็นรูปธรรม เพื่อให้ข้อมูลมีคุณภาพ เข้าถึงได้ ปลอดภัย และเป็นไปตามกฎหมาย/ข้อบังคับที่เกี่ยวข้อง

รายละเอียดนโยบายการบริหารจัดการข้อมูล สกพอ. ดังภาคผนวก ค

6.3. แนวปฏิบัติการบริหารจัดการข้อมูล (Data Management Guideline)

เป็นเป็นเอกสารระดับปฏิบัติการ ทำหน้าที่เป็นคู่มือการปฏิบัติงานที่อธิบายขั้นตอนและวิธีการปฏิบัติงานเพื่อให้เป็นไปตามนโยบายในการบริหารจัดการข้อมูล เพื่อให้บรรลุตามที่นโยบายกำหนด จึงต้องสอดคล้องกันและใช้ร่วมกันเพื่อให้การจัดการข้อมูลเป็นไปอย่างมีประสิทธิภาพและถูกต้องตามมาตรฐาน

ภายในเอกสารจะแบ่งออกเป็น 6 หมวด ได้แก่ การสร้างข้อมูล การจัดเก็บข้อมูล (รวมการจัดเก็บถาวร) การประมวลผลข้อมูลและการใช้ข้อมูล การเปิดเผยข้อมูล การทำลายข้อมูล และการเชื่อมโยงและการแลกเปลี่ยนข้อมูล ในแต่ละหมวดจะระบุ วัตถุประสงค์ ผู้รับผิดชอบงาน อ้างอิง และข้อปฏิบัติ ทั้งนี้ เอกสารสามารถปรับปรุงได้ตามความเหมาะสม

รายละเอียดแนวปฏิบัติการบริหารจัดการข้อมูล สกพอ. ดังภาคผนวก ง

7. มาตรฐานข้อมูล (Data Standards)

มาตรฐานข้อมูล สกพอ. ออกแบบให้ผู้เกี่ยวข้องสามารถบริหารจัดการข้อมูลและใช้ข้อมูล มีวัตถุประสงค์เพื่อสร้างให้เกิดความเข้าใจร่วมกัน และสามารถทำงานร่วมกันได้อย่างราบรื่นของข้อมูล ประกอบไปด้วย 3 ด้าน ได้แก่ 1) มาตรฐานเมทาดาตา (Metadata Standard) 2) มาตรฐานชุดข้อมูล (Datasets Standard) และ 3) มาตรฐานการจัดชั้นความลับของข้อมูล (Data Classification Standard)

7.1. มาตรฐานเมทาดาตา (Metadata Standard)

ชุดของข้อกำหนด กฎเกณฑ์ แนวทางที่ใช้ในการจัดระเบียบและอธิบายข้อมูลเกี่ยวกับข้อมูล (metadata) เพื่อให้สามารถแลกเปลี่ยน ใช้งาน และจัดการข้อมูลได้อย่างมีประสิทธิภาพ ถูกต้อง และสอดคล้องกันระหว่างระบบ องค์กร หรือหน่วยงานต่าง ๆ สามารถทำงานร่วมกันได้ โดยมาตรฐานเมทาดาตาที่ สกพอ. กำหนดได้อ้างอิงตามประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่องมาตรฐานรัฐบาลดิจิทัลว่าด้วยแนวทางการจัดทำบัญชีข้อมูลภาครัฐและแนวทางการลงทะเบียนบัญชีข้อมูลภาครัฐประกาศ ณ วันที่ 15 กุมภาพันธ์ พ.ศ. 2566 ประกอบด้วยคำอธิบายข้อมูลจำนวน 14 รายการรายละเอียดตาม “ภาคผนวก ฉ. คำอธิบายข้อมูลหรือเมทาดาตาสำหรับชุดข้อมูลภาครัฐ (Metadata Standard)”

7.2. มาตรฐานชุดข้อมูล (Datasets Standard)

ข้อกำหนดรูปแบบ และแนวทางที่กำหนดขึ้นเพื่อสร้าง จัดโครงสร้าง อธิบาย และเผยแพร่ชุดข้อมูล (Dataset) ให้มีความสอดคล้องกัน เข้าใจตรงกัน และสามารถใช้งานร่วมกันได้อย่างมีประสิทธิภาพ

มาตรฐานชุดข้อมูลจะระบุรายละเอียดที่จำเป็นเพื่อให้ผู้ใช้ข้อมูลสามารถทำความเข้าใจโครงสร้าง ความหมาย และคุณลักษณะของข้อมูลทั้งหมดในชุดนั้น โดย สกพอ. ได้กำหนดมาตรฐานชุดข้อมูลดังนี้

1) ข้อมูลบุคคล
2) ข้อมูลนิติบุคคล
3) ข้อมูลผู้ประกอบกิจการในเขตส่งเสริมเศรษฐกิจพิเศษ
4) ข้อมูลผู้ได้รับสิทธิประโยชน์
5) ข้อมูลผู้ได้รับอนุมัติ อนุญาต
6) ข้อมูลเขตส่งเสริมเศรษฐกิจพิเศษ
7) ข้อมูลผังการใช้ประโยชน์ที่ดิน สกพอ.
8) ข้อมูลกฎหมายที่เกี่ยวข้อง สกพอ.

7.3. มาตรฐานการจัดชั้นระดับชั้นข้อมูล (Data Classification Standard)

การกำหนดรูปแบบและข้อกำหนดของการจัดชั้นระดับชั้นข้อมูล เพื่อป้องกันการเข้าถึงและสามารถนำข้อมูลไปใช้ได้อย่างเหมาะสม ระดับชั้นของข้อมูลมักถูกกำหนดให้สอดคล้องกับผลกระทบต่อหน่วยงานและความมั่นคงของประเทศ และผลประโยชน์ของชาติ อ้างอิงจาก มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมาหาชน) ว่าด้วยหลักเกณฑ์การจัดระดับชั้นและการแบ่งปันข้อมูลภาครัฐ เวอร์ชัน 1.0 โดยแบ่งเกณฑ์การแบ่งระดับชั้นข้อมูลภาครัฐ ดังนี้

1) **ชั้นเปิดเผย (Open) สู่สาธารณะ** เป็นข้อมูลข่าวสารของราชการที่หน่วยงานของรัฐต้องเปิดเผยให้ประชาชนได้รับรู้ รับทราบ หรือตรวจสอบได้โดยไม่จำเป็นต้องร้องขอ เช่น กฎ มติคณะรัฐมนตรีข้อบังคับ รายงานผลการ ศึกษาทางวิชาการ และข้อมูลเปิดภาครัฐ ฯลฯ
2) **ชั้นเผยแพร่ภายในองค์กร (Private) เปิดเผยเมื่อได้รับอนุญาต** เป็นข้อมูลที่องค์กรไม่ได้เผยแพร่โดยอิสระ โดยทั่วไปจะเกี่ยวข้องกับข้อมูลที่มีลักษณะเป็นส่วนตัว (Private) ไม่ว่าจะเป็นข้อมูลบุคคลหรือองค์กร **และแม้ว่าการสูญเสียข้อมูลหรือการเปิดเผยข้อมูลอาจไม่ส่งผลให้เกิดผลกระทบที่สำคัญแต่ก็ไม่พึงประสงค์ที่ให้เปิดเผยโดยไม่ได้รับอนุญาต** เช่น ข้อมูลระเบียน ข้อมูลพนักงาน เอกสารประกอบการปฏิบัติงาน และวิธีปฏิบัติภายในหน่วยงาน ฯลฯ
3) **ชั้นลับ (Confidential)** เปิดเผยเมื่อได้รับอนุญาต เป็นข้อมูลที่มีระดับ Confidential หรือ Sensitive จะก่อให้เกิดความสูญเสีย หากมีการเปิดเผยต่อบุคคล/องค์กรที่ไม่ได้รับอนุญาต และส่งผลให้เกิดความอับอายอย่างมากต่อบุคคล/องค์กร และอาจเป็นผลทางกฎหมาย หรือจะก่อให้เกิดความเสียหายแก่ผลประโยชน์แห่งรัฐ เช่น ข้อมูลการฟ้องคดี และความเห็นภายในหน่วยงานที่ยังไม่ได้ข้อยุติ ฯลฯ
4) **ชั้นลับมาก (Secret)** เปิดเผยเมื่อได้รับอนุญาต เป็นข้อมูลที่จัดระดับ Secret หรือ Medium Sensitive สงวนไว้สำหรับข้อมูลที่จะก่อให้เกิดความสูญเสีย/ผลกระทบร้ายแรง อาจทำให้เสียชื่อเสียงและการสูญเสียทางการเงิน/ทรัพย์สิน ต่อความมั่นคงและ**ผลประโยชน์แห่งรัฐอย่างร้ายแรง หรือ ที่มีนัยสำคัญ (Importance)** หากสูญหายหรือเปิดเผยอย่างไม่ถูกต้องเหมาะสม เช่น รายงานการแพทย์ ข้อมูลความสัมพันธ์ระหว่างประเทศ และนโยบายสำคัญที่ใช้ปฏิบัติต่อรัฐต่างประเทศ ฯลฯ
5) **ชั้นลับที่สุด (Top Secret) เปิดเผยไม่ได้** เป็นข้อมูลที่จัดระดับ Top Secret หรือ Highly Sensitive จำกัดการใช้/ไม่เปิดเผยสำหรับข้อมูลที่จะ**ก่อให้เกิดความสูญเสีย/ผลกระทบร้ายแรงที่สุด** หรือที่สำคัญยิ่งยวด (Vital) หากสูญหายหรือเปิดเผยอย่างไม่ถูกต้องเหมาะสม **ซึ่งในกรณีข้อมูลที่อยู่ในชั้น “ลับที่สุด”จะไม่สามารถนำเข้าในระบบสารสนเทศได้ ต้องดำเนินการในรูปแบบเอกสาร (Hard Copy) เท่านั้น** เช่น ข้อมูลกำลังรบ ข้อมูลด้านการข่าวกรองยุทธศาสตร์ ข้อมูลความมั่นคงเชิงนโยบาย

ทั้งนี้ นิยามการกำหนดข้อมูลข่าวสารลับ ให้อ้างอิงตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม สำหรับนิยามศัพท์ที่เกี่ยวข้องกับหลักเกณฑ์ฯ ฉบับนี้ สามารถดูรายละเอียดได้ที่ **อภิธานศัพท์**

8. การประเมินคุณภาพของข้อมูล (Data Quality Assessment)

การประเมินคุณภาพข้อมูลเป็นหนึ่งในกระบวนการสำคัญของการรับประกันคุณภาพข้อมูลภายในของ สกพอ. และเป็นการตรวจสอบผลลัพธ์หรือความสำเร็จจากธรรมาภิบาลข้อมูลภาครัฐ เพื่อยกระดับคุณภาพข้อมูลภายใน สกพอ. จึงควรมีการควบคุมและบริหารจัดการคุณภาพข้อมูลอย่างเป็นระบบ โดยมีกระบวนการสำคัญ ดังนี้

- **กำหนดตัวชี้วัดคุณลักษณะผลผลิตข้อมูล** ตามมิติคุณภาพข้อมูล
- **ดำเนินการประเมินและตรวจสอบคุณภาพข้อมูล** ภายในหน่วยงาน
- **จัดทำรายงานสถานะคุณภาพข้อมูล** พร้อมเสนอแนวทางการพัฒนา

ซึ่งมีโดยองค์ประกอบในการประเมินคุณภาพข้อมูลภาครัฐ (DQAF: Data Quality Assessment Framework) เป็นกรอบเบื้องต้นในการประเมิน โดยอิงจาก กรอบธรรมาภิบาลข้อมูลภาครัฐ ซึ่งกำหนด 5 มิติคุณภาพข้อมูลหลัก ได้แก่

องค์ประกอบในการประเมินคุณภาพข้อมูล ตามแนวคิดของ สพร.

1) **ความถูกต้อง และสมบูรณ์ (Accuracy and Completeness)** หมายความว่า ข้อมูลมีความถูกต้องแม่นยำสูง มีความครบถ้วนสมบูรณ์ของข้อมูลที่เก็บรวบรวมมา และมีการตรวจสอบความถูกต้องระหว่างข้อมูลในส่วนต่าง ๆ ในทุกขั้นตอน เพื่อให้ข้อมูลถูกต้องเชื่อถือได้และให้ผลลัพธ์ตรงตามความต้องการผู้ใช้ (ข้อมูลครบถ้วน ข้อมูลไม่ขาดหาย กว้างพอและลึกพอสำหรับการใช้งาน)
2) **ความสอดคล้องกัน (Consistency)** หมายความว่า ข้อมูลมีความสอดคล้องกันของ แนวคิดคำนิยาม วิธีการ รหัส และการนำเสนอที่ทำให้ข้อมูลจากต่างแหล่ง ต่างเวลา สามารถเปรียบเทียบข้ามช่วงเวลาและบูรณาการข้อมูลเพื่อใช้ประโยชน์ร่วมกันได้

3) **ความเป็นปัจจุบัน (Timeliness)** หมายความว่า ข้อมูลเป็นปัจจุบันทันสมัยเพียงพอต่อการใช้งาน และพร้อมใช้งานตามที่กำหนดและในกรอบเวลาที่กำหนดไว้ หรือมีข้อมูลทันต่อการใช้งานทุกครั้งตามที่ผู้ใช้ต้องการ
4) **ตรงตามความต้องการของผู้ใช้ (Relevancy)** หมายความว่า ข้อมูลสามารถนำไปใช้ได้กับงานที่ทำอยู่ เป็นข้อมูลที่ผู้ใช้งานต้องการ หรือเป็นข้อมูลที่จำเป็นต้องทราบ มีมุมมองและความละเอียดเพียงพอต่อการนำไปใช้งาน
5) **ความพร้อมใช้ (Availability)** หมายความว่า ข้อมูลเข้าถึงได้ง่าย หรือมีข้อมูลนั้นอยู่สามารถใช้งานได้จริง และสามารถใช้งานได้ตลอดเวลา

ทั้งนี้ สกพอ. ได้กำหนดขอบเขตการวัดและประเมินคุณภาพของข้อมูล จำแนกตามองค์ประกอบในการประเมินคุณภาพข้อมูล รายละเอียดดังนี้

1. **ข้อมูลที่จัดเก็บในระบบบริหารจัดการฐานข้อมูล** เป็นข้อมูลที่อยู่ในระบบบริหารจัดการฐานข้อมูล (Database Management System) ที่มีโครงสร้างเป็นตารางข้อมูล (Table) การวัดคุณภาพของข้อมูลสำหรับแต่ละชุดข้อมูล ในทั้ง 5 ด้าน มีรายละเอียดดังนี้
   หมายเหตุ : กำหนดให้ชุดข้อมูลพนักงาน มีจำนวน 1,000 แถว (คน) แต่ละแถวประกอบด้วย 100 คอลัมน์ (ฟิลด์)

ตัวอย่างการวัดคุณภาพข้อมูลที่เป็นโครงสร้างสำหรับแต่ละชุดข้อมูล

คุณภาพข้อมูล	รูปแบบการวัด	หน่วยวัด	ตัวอย่าง
ความถูกต้องและสมบูรณ์ (Accuracy and Completeness)	1) แถว xฟิลด์ 2.1) แถว 2.2) แถวx ฟิลด์ 2.3) แถวx ฟิลด์ที่จำเป็น	ร้อยละ	**กรณีที่ 1 : พิจารณาเฉพาะแถวข้อมูล** ถ้าพบว่ามี 80 ฟิลด์ที่มีความถูกต้องตลอดทั้ง 1,000 คน ดังนั้นชุดข้อมูลนี้มี ความถูกต้อง = (1,000 x 80) / (1,000 x 100) x 100 = 80 **กรณีที่ 2.1 : พิจารณาเฉพาะแถวข้อมูล** ถ้าพบว่ามีการบันทึกข้อมูล 900 คน โดยไม่สนใจจำนวนฟิลด์ที่มีการบันทึก ดังนั้นข้อมูลชุดนี้มีความครบถ้วน = (900 /1,000) x 100 = 90 **กรณีที่ 2.2 : พิจารณาแถวและฟิลด์ข้อมูล** ถ้าพบว่ามี 60 ฟิลด์จาก 100 ฟิลด์ ที่มีการบันทึกข้อมูลทั้ง 1,000 คน ดังนั้นข้อมูลชุดนี้มีความครบถ้วน = (1,000 x 60) / (1,000 x 100) x 100 = 60 **กรณีที่ 2.3 : พิจารณาแถวและฟิลด์ข้อมูลที่มีความจำเป็นเท่านั้น**

คุณภาพข้อมูล	รูปแบบการวัด	หน่วยวัด	ตัวอย่าง
			ถ้ากำหนดให้มี 80 ฟิลด์ที่มีความจำเป็นต้องบันทึกข้อมูล แล้วพบว่ามี 60 ฟิลด์จาก 80 ฟิลด์ ที่มีการบันทึกข้อมูลทั้ง 1,000 คน ดังนั้นข้อมูลชุดนี้มี ความครบถ้วน = (1,000 x 60) / (1,000 x 80) x 100 = 75
ความสอดคล้องกัน (Consistency)	ฟิลด์	ร้อยละ	ถ้าพบว่ามี 20 ฟิลด์ที่เก็บซ้ำซ้อนกับชุดข้อมูลอื่นและมีรูปแบบของฟิลด์ที่ แตกต่างกัน เช่น รูปแบบวันที่ รูปแบบรหัส ดังนั้นข้อมูลชุดนี้มีความสอดคล้องกัน = (100-20 / 100) x 100 = 80
ความเป็นปัจจุบัน (Timeliness)	1) แถว 2) แถวxฟิลด์	ร้อยละ	**กรณีที่ 1 : พิจารณาเฉพาะแถวข้อมูล** ถ้ามีพนักงานใหม่ 10 คน และมีพนักงานเก่า 5 คนที่มีการเปลี่ยนข้อมูล ซึ่งยังไม่มีการบันทึกหรือปรับปรุงให้เป็นปัจจุบัน ดังนั้นข้อมูลชุดนี้มีความเป็นปัจจุบัน = 100 – [(10 + 5) / (1,000+10) x 100] = 98.51 **กรณีที่ 2 : พิจารณาแถวและฟิลด์ข้อมูล** ถ้ามีพนักงานใหม่ 10 คน และมีพนักงานเก่า 5 คนที่มีการเปลี่ยนชื่อและ บ้านเลขที่ ซึ่งยังไม่มีการบันทึกหรือปรับปรุงให้เป็นปัจจุบัน ดังนั้นข้อมูลชุดนี้มีความเป็นปัจจุบัน = 100 – [[(10 x 100) + (5 x 2)] / [(1,000 + 10) x 100] x 100] = 99.00 **หมายเหตุ** : ชื่อและบ้านเลขที่นับเป็น 2 ฟิลด์
ตรงตามความต้องการใช้ (Relevancy)	ฟิลด์	ร้อยละ	ถ้าพบว่ามี 20 ฟิลด์ที่ไม่เคยถูกนำไปใช้ ดังนั้นข้อมูลชุดนี้มีความตรงตามความต้องการใช้ = [(100-20) / 100] x 100 = 80
ความพร้อมใช้ (Availability)	ชุดข้อมูล	ร้อยละ	= 100 ถ้าข้อมูลเก็บอยู่ในรูปแบบ ฐานข้อมูล กำหนดให้ = 66.67 ถ้าข้อมูลเก็บอยู่ในรูปแบบ XML JSON และ CSV = 33.33 ถ้าข้อมูลเก็บอยู่ในรูปแบบ WORD PDF **หมายเหตุ** : ข้อมูลที่อยู่ในระดับที่ต่ำกว่าสามารถจัดให้อยู่ในระดับที่สูงขึ้นได้ ถ้ามีเครื่องมือหรือวิธีการที่ทำให้การนำข้อมูลไปใช้งานสะดวกมากขึ้น

2. **ข้อมูลที่ไม่ได้จัดเก็บในระบบบริหารจัดการฐานข้อมูล** เช่น เป็นไฟล์ Word, Excel, PowerPoint หรือเอกสาร PDF) การประเมินข้อมูลดังกล่าวไม่สามารถใช้หลักการเชิงเทคนิค เช่น โครงสร้างตารางหรือฟิลด์ข้อมูลได้เหมือนกับฐานข้อมูลเชิงสัมพันธ์ จึงต้องใช้แนวทางที่แตกต่าง โดยสามารถดำเนินการประเมินได้ตามหัวข้อต่อไปนี้

ตัวอย่างการวัดคุณภาพข้อมูลที่ไม่ได้จัดเก็บในระบบบริหารจัดการฐานข้อมูล

คุณภาพข้อมูล	การตรวจสอบ	ผลการตรวจสอบ
ความถูกต้องและสมบูรณ์ (Accuracy and Completeness)	1) พิจารณาว่าเอกสารมีเนื้อหาครบถ้วนตามวัตถุประสงค์หรือไม่ 2) ตรวจสอบว่าข้อมูลที่ควรมี (เช่น ชื่อผู้รับผิดชอบ วันเวลา รายละเอียดหลัก) ปรากฏอยู่ครบถ้วนหรือไม่ 3) เปรียบเทียบกับแบบฟอร์มหรือรายการตรวจสอบ (Checklist) ที่กำหนดไว้ในกระบวนงาน 4) ตรวจสอบความถูกต้องของเนื้อหาภายในเอกสาร เช่น ค่าตัวเลข สถิติ หรือข้อความ 5) หากมีแหล่งข้อมูลอ้างอิง ควรตรวจสอบว่าเนื้อหาในเอกสารสอดคล้องกับแหล่งข้อมูลนั้นหรือไม่	
	1) ตรวจสอบความสอดคล้องของข้อมูลระหว่างเอกสารหลายฉบับในเรื่องเดียวกัน 2) ตรวจสอบรูปแบบการจัดทำเอกสารว่ามีมาตรฐานเดียวกันหรือไม่	
ความเป็นปัจจุบัน (Timeliness)	1) พิจารณาว่าเอกสารเป็นข้อมูลที่เป็นปัจจุบันหรือไม่ โดยดูจากวันที่จัดทำหรือปรับปรุงล่าสุด 2) ตรวจสอบว่าข้อมูลในเอกสารยังคงมีความเกี่ยวข้องและสามารถนำมาใช้ประกอบการตัดสินใจได้หรือไม่	
ความสามารถในการเข้าถึงและใช้งาน (Accessibility & Availability)	1) ข้อมูลในเอกสารสามารถเปิดอ่านได้หรือไม่ (ไม่มีรหัสผ่านหรือข้อจำกัดในการเข้าถึง) 2) ข้อมูลจัดเรียงอย่างเข้าใจง่าย และมีโครงสร้างที่สนับสนุนการค้นหาและใช้งาน	

9. การประเมินความมั่นคงปลอดภัยของข้อมูล (Data Security Assessment)

การประเมินความมั่นคงปลอดภัยของข้อมูลเป็นอีกหนึ่งวิธีในการวัดความสำเร็จจากธรรมาภิบาลข้อมูลภาครัฐ โดยใช้หลักเกณฑ์ในด้านต่าง ๆ ดังนี้

1) จัดทำนโยบายด้านความมั่นคงปลอดภัยของข้อมูลที่รวมถึงการป้องกันข้อมูลในบริบทของการรักษาความลับ ความถูกต้องของข้อมูล ความพร้อมใช้งานของข้อมูล
2) ข้อมูลมีการจัดระดับชั้นข้อมูล (Data Classification) ข้อมูลควรมีการจำแนกชั้นของข้อมูลในบริบทของการรักษาความปลอดภัยข้อมูลตามระดับของความอ่อนไหวและผลกระทบที่จะเกิดขึ้นต่อบุคคลองค์กร และประเทศ หากมีการเปิดเผย เปลี่ยนแปลง หรือทำลายข้อมูลโดยไม่ได้รับอนุญาต
3) กำหนดมาตรการควบคุมและป้องกันการเข้าถึงข้อมูล (Data Protection) การกำหนดมาตรการควบคุมและป้องกันการเข้าถึงข้อมูลต้องคำนึงถึงระดับชั้นข้อมูล เช่น ข้อมูลที่มีความอ่อนไหวต้องมีการกำหนดมาตรการควบคุมและป้องกันการเข้าถึงข้อมูลแบบพิเศษ เพื่อป้องกันการเข้าถึงเพื่อเปิดเผยข้อมูลที่อ่อนไหวนั้นรวมถึงเพื่อป้องกันการดัดแปลง แก้ไข แต่งเติมข้อมูลโดยไม่ได้รับอนุญาต
4) ข้อมูลถูกใช้งานอย่างเหมาะสม การนำข้อมูลไปใช้ควรดำเนินการให้สอดคล้องกับสัญญาอนุญาต และไม่ขัดต่อกฎหมาย
5) ข้อมูลต้องมีความพร้อมใช้อยู่เสมอ ต้องมีการดำเนินการเตรียมความพร้อมไม่ว่าข้อมูลจะอยู่ใน ประเภทใดก็ตาม เช่น ข้อมูลในรูปแบบกระดาษต้องมีสถานที่จัดเก็บดูแล และสามารถเข้าถึงโดยผู้มีสิทธิได้ อย่างสม่ำเสมอ ข้อมูลในรูปแบบอิเล็กทรอนิกส์ต้องมีการเตรียมความพร้อมเรื่องระบบงาน การสำรองข้อมูล รวมถึงมีแผนการดำเนินการในกรณีฉุกเฉินใด ๆ ที่อาจมีผลต่อการใช้ข้อมูลด้วย

ตัวอย่างการการวัดความมั่นคงปลอดภัยของข้อมูล

ความมั่นคงปลอดภัยของข้อมูล	หน่วยวัด	ตัวอย่าง
ความลับ ความถูกต้อง ความพร้อมใช้	จำนวนครั้ง	• จำนวนการพิจารณาทบทวนนโยบายความมั่นคงปลอดภัยสารสนเทศและมาตรการควบคุมและป้องกันการเข้าถึงข้อมูล • จำนวนการส่งเสริมสื่อสารสร้างความตระหนักด้านความมั่นคงปลอดภัย • จำนวนการทดสอบความต่อเนื่องของการให้บริการและการนำข้อมูลกลับมาใช้

ความมั่นคงปลอดภัยของข้อมูล	หน่วยวัด	ตัวอย่าง
ความลับ ความถูกต้อง ความพร้อมใช้	ร้อยละ	• ร้อยละของการปฏิบัติตามนโยบายข้อมูลที่ได้กำหนดไว้ $= \frac{\text{จำนวนข้อกำหนดของนโยบายที่เป็นไปตามที่กำหนด}}{\text{จำนวนข้อกำหนดของนโยบายทั้งหมด}} \times 100$ • ร้อยละของจำนวนเหตุละเมิดความมั่นคงปลอดภัยที่ควบคุมได้ เช่น ร้อยละของการถูกเผยแพร่ข้อมูลโดยไม่ได้รับอนุญาต สูตรการคำนวณ $= \frac{\text{จำนวนเหตุละเมิดความมั่นคงปลอดภัยที่ควบคุมได้}}{\text{จำนวนเหตุละเมิดความมั่นคงปลอดภัยทั้งหมด}} \times 100$ • ร้อยละของจำนวนข้อร้องเรียนด้านความมั่นคงปลอดภัยข้อมูลที่ลดลง เช่น ร้อยละของจำนวนข้อร้องเรียนจากการเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับการอนุญาต สูตรการคำนวณ $= \frac{\text{จำนวนข้อร้องเรียนปีปัจจุบัน} - \text{ปีที่ผ่านมา}}{\text{จำนวนข้อร้องเรียนปีที่ผ่านมา}} \times 100$ • ร้อยละของความสำเร็จในการกู้คืนข้อมูลเมื่อมีเหตุฉุกเฉิน $= \frac{\text{จำนวนกู้คืนข้อมูลที่ความสำเร็จ}}{\text{จำนวนกู้คืนข้อมูลทั้งหมด}} \times 100$

ตัวอย่างหลักเกณฑ์การประเมินคุณภาพข้อมูลสำหรับหน่วยงานภาครัฐ

อ้างอิง สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.) ได้จัดทำหลักเกณฑ์การประเมินคุณภาพข้อมูลสำหรับหน่วยงานภาครัฐฉบับนี้ขึ้นเพื่อเป็นกรอบและเครื่องมือในการประเมินคุณภาพข้อมูลของหน่วยงานภาครัฐในการตรวจสอบและควบคุมการบริหารจัดการข้อมูล โดยประกอบด้วยเกณฑ์ด้านคุณภาพข้อมูลดังนี้

มิติคุณภาพข้อมูล	รายละเอียด	รายการตัวชี้วัด
ความถูกต้องและสมบูรณ์ (Accuracy and Completeness)	ประเมินเรื่องความถูกต้องแม่นยำ แหล่งข้อมูลที่น่าเชื่อถือ และมีกระบวนการตรวจสอบ	• มีแหล่งข้อมูลที่น่าเชื่อถือ • มีกระบวนการหรือเครื่องมือตรวจสอบจุดผิดพลาดของข้อมูล • มีการตรวจสอบความครบถ้วนของข้อมูล

มิติคุณภาพข้อมูล	รายละเอียด	รายการตัวชี้วัด
		● มีวิธีเก็บข้อมูลมีความเป็นกลาง น่าเชื่อถือ และไม่สร้างข้อมูลที่มีอคติ ● มีการระบุคำนิยามและลักษณะข้อมูลที่ต้องการ
ความสอดคล้องกัน (Consistency)	ประเมินเรื่องรูปแบบของข้อมูลความสอดคล้องกัน และมาตรฐานในการจัดทำข้อมูลของหน่วยงาน	● มีการเก็บข้อมูลภายใต้มาตรฐานข้อมูลเดียวกันหรือมาตรฐานข้อมูลที่สอดคล้องกัน ทำให้สามารถใช้ประโยชน์ข้อมูลร่วมกันได้ ● มีการตรวจสอบรูปแบบข้อมูลภายในชุดข้อมูลเดียวกัน ● ข้อมูลมีความเชื่อมโยงและไม่ขัดแย้งกัน ● มีการใช้กฎ วิธีการตรวจวัดที่สอดคล้องกันทั้งหน่วยงาน รวมถึงหน่วยงานภายนอก ● มีการกำหนดบทบาทและผู้รับผิดชอบข้อมูล
ตรงตามความต้องการของผู้ใช้ (Relevancy)	ประเมินว่า เป็นข้อมูลที่ผู้ใช้ต้องการหรือเป็นข้อมูลที่จำเป็นต้องทราบ มีความละเอียดเพียงพอต่อการนำไปใช้งาน	● ข้อมูลตรงตามความต้องการและวัตถุประสงค์ของการใช้งาน ● มีผลประเมินความพึงพอใจของผู้ใช้ และมีการปรับปรุงคุณภาพให้ตรงตามความต้องการของผู้ใช้
ความเป็นปัจจุบัน (Timeliness)	ประเมินเรื่องการเผยแพร่ข้อมูลการปรับปรุงข้อมูล และแผนเรื่องระยะเวลา	● ข้อมูลมีการเผยแพร่ ส่งต่อตรงเวลา ● ข้อมูลมีความเป็นปัจจุบัน ● ข้อมูลมีการเผยแพร่ข้อมูลในเวลาที่เหมาะสม ● มีการจัดทำปฏิทินเผยแพร่ข้อมูล
ความพร้อมใช้ (Availability)	ประเมินความพร้อมใช้ของข้อมูลรวมไปถึงช่องทางในการขอ หรือใช้ข้อมูล	● ข้อมูลถูกจัดในรูปแบบที่พร้อมนำไปใช้งานและเหมาะสมกับผู้ใช้งาน ● มีการเผยแพร่ข้อมูลที่เหมาะสมและสามารถเข้าถึงได้ โดยผู้ใช้สามารถเข้าถึงข้อมูลได้สะดวกตามสิทธิที่เหมาะสม ● ข้อมูลสามารถอ่านด้วยโปรแกรมคอมพิวเตอร์ได้ ● มีคำอธิบายข้อมูลที่ชัดเจน ● มีคำอธิบายขั้นตอนการขอข้อมูลที่ไม่เผยแพร่

นอกจากนี้ สพร. ยังได้จัดทำเครื่องมือการประเมินคุณภาพข้อมูลมีวัตถุประสงค์เพื่อให้หน่วยงานภาครัฐใช้ในการตรวจสอบและควบคุมการบริหารจัดการข้อมูลเพื่อให้ได้ข้อมูลที่มีคุณภาพ น่าเชื่อถือ สามารถนำไปใช้ประกอบการวิเคราะห์และตัดสินใจในเชิงนโยบายและการดำเนินงานได้อย่างถูกต้องเหมาะสม รวมทั้งสามารถนำไปใช้ประโยชน์เพื่อเพิ่มประสิทธิภาพในการทำงาน เพิ่มคุณค่าในการให้บริการภาครัฐ และต่อยอดการพัฒนาของประเทศในมิติต่าง ๆ ได้ ตลอดจนสร้างความเชื่อมั่นให้กับผู้ใช้ข้อมูลภาครัฐ ประกอบด้วย

1) **แบบตรวจประเมินคุณภาพ (*DQA Checklist*)** เพื่อตรวจสอบกระบวนการเตรียมข้อมูลที่มีคุณภาพ สำหรับ ผู้ประเมินคุณภาพข้อมูล
2) **แบบประเมินคุณภาพข้อมูลด้วยตนเอง (*DQA Self-Assessment*)** เพื่อวัดผลลัพธ์ข้อมูล (*Data Output*) ตามมิติคุณภาพข้อมูล สำหรับ เจ้าของข้อมูล (*Data Owner*)
3) **แบบตรวจประเมินการควบคุมและติดตามคุณภาพข้อมูล (*DQC Checklist*)** ตามกระบวนการจัดทำธรรมาภิบาลข้อมูลภาครัฐ สำหรับ ผู้ประเมินคุณภาพข้อมูล / เจ้าของข้อมูล (*Data Owner*) โดยใช้สำหรับประเมินคุณภาพข้อมูลในประเภทข้อมูลระเบียน (*Record*) และ/หรือ *Tabular Format Data* ที่อยู่ใน *Database* ซึ่งเป็นข้อมูลที่สำคัญและหน่วยงานภาครัฐมีการใช้งานเป็นประจำ เพื่อส่งเสริมให้มีการนำเกณฑ์การประเมินคุณภาพข้อมูลไปปฏิบัติจริงในหน่วยงาน

<u>คำแนะนำในการใช้งาน</u>

1) ผู้ประเมินคุณภาพข้อมูลควรต้องทำความเข้าใจข้อเสนอแนะสำหรับดำเนินการประเมินคุณภาพข้อมูล และดำเนินการ กรอกรายละเอียดในรายงานคุณภาพ จากนั้นดำเนินการตรวจประเมินคุณภาพข้อมูลตามรายการในแต่ละมิติของตัวชี้วัดใน *DQA Checklist* โดยสามารถนำผลจากประเมิน *DQA Self-Assessment* มาประกอบการตรวจประเมิน และใช้เป็นหลักฐานประกอบใน *DQC Checklist*
2) เจ้าของข้อมูล (*Data Owner*) ควรพิจารณาข้อมูลภาพรวมของหน่วยงาน และทำความเข้าใจ *DQA Self-Assessment* ในส่วนที่ 1 เกณฑ์และคำอธิบาย จากนั้นทำการประเมินคุณภาพข้อมูลในส่วนที่ 2 โดยกรอกค่าคะแนนในแต่ละมิติของตัวชี้วัด (*Indicators*) จากนั้นให้นำค่าคะแนนที่ได้จากการประเมินไปกรอกใน *Sheet* การแสดงผล ระบบจะประมวลผลตามเกณฑ์ประเมินคุณภาพข้อมูลในแต่ละมิติ และจะแสดงผลในรูปแบบ *Radar Graph* ทั้งนี้ กรุณานำส่งผลการประเมินให้ผู้ประเมินคุณภาพข้อมูลเพื่อใช้ประกอบการตรวจประเมินคุณภาพข้อมูล

3) ผู้ประเมินคุณภาพข้อมูล / เจ้าของข้อมูล (*Data Owner)* ทำความเข้าใจคำชี้แจงและกรอก *DQC-Checklist* ให้ครบถ้วนสมบูรณ์ด้วยระบบอิเล็กทรอนิกส์ และเจ้าของข้อมูลกรุณาส่งกลับให้ผู้ประเมินผลภายในระยะเวลาที่กำหนด เพื่อจัดทำรายงานสรุปผลการตรวจประเมินให้ผู้บริหารรับทราบและดำเนินการตามแผนปฏิบัติการจัดการคุณภาพข้อมูลของหน่วยงานต่อไปทั้งนี้ สามารถสแกน *QR Code* เพื่อดาวน์โหลดเอกสารเครื่องมือการประเมินคุณภาพข้อมูลด้วยตนเองสำหรับหน่วยงานภาครัฐ และดูตัวอย่างรายงานการประเมินคุณภาพข้อมูลด้วยตนเองได้ด้านล่างนี้

เครื่องมือการประเมินคุณภาพข้อมูล

ตัวอย่างรายงานการประเมินคุณภาพข้อมูล

ภาคผนวก ก.

คำสั่งแต่งตั้งคณะกรรมการธรรมาภิบาลข้อมูล สกพอ.

คำสั่งสำนักงานคณะกรรมการนโยบายเขตพัฒนาพิเศษภาคตะวันออก

ที่ ๗๗ /2568

เรื่อง แต่งตั้งคณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council)

ด้วยพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 กำหนดให้หน่วยงานของรัฐจัดให้มีการบริหารงานภาครัฐและการจัดทำบริการสาธารณะเป็นไปด้วยความสะดวก รวดเร็ว มีประสิทธิภาพ และตอบสนองต่อการให้บริการและการอำนวยความสะดวกแก่ประชาชน รวมทั้งกำหนดให้หน่วยงานของรัฐจัดให้มีการบริหารจัดการและการบูรณาการข้อมูลภาครัฐและการทำงานให้มีความสอดคล้องกันและเชื่อมโยงเข้าด้วยกันอย่างมั่นคงปลอดภัยและมีธรรมาภิบาล

เพื่อให้การดำเนินการด้านธรรมาภิบาลข้อมูลภาครัฐของสำนักงานคณะกรรมการนโยบายเขตพัฒนาพิเศษภาคตะวันออกเป็นไปอย่างมีประสิทธิภาพ อาศัยอำนาจตามความในมาตรา 20 วรรคหนึ่ง (1) แห่งพระราชบัญญัติเขตพัฒนาพิเศษภาคตะวันออก พ.ศ. 2561 เลขาธิการคณะกรรมการนโยบายเขตพัฒนาพิเศษภาคตะวันออก จึงมีคำสั่งดังต่อไปนี้

ข้อ 1 ให้มีคณะกรรมการธรรมาภิบาลข้อมูลภาครัฐ (Data Governance Council) ประกอบด้วย

(1) ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง	ประธานกรรมการ
(2) ผู้อำนวยการสำนักกฎหมาย	กรรมการ
(3) ผู้อำนวยการสำนักยุทธศาสตร์องค์กร	กรรมการ
(4) ผู้อำนวยการสำนักพัฒนาเขตส่งเสริมเศรษฐกิจพิเศษ	กรรมการ
(5) ผู้อำนวยการสำนักพัฒนาพื้นที่และชุมชน 2	กรรมการ
(6) ผู้อำนวยการสำนักพัฒนาโครงสร้างพื้นฐานและสาธารณูปโภค	กรรมการ
(7) ผู้อำนวยการสำนักยุทธศาสตร์การส่งเสริมและชักชวนนักลงทุน	กรรมการ
(8) ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ	กรรมการและเลขานุการ
(9) ผู้แทนสำนักเทคโนโลยีสารสนเทศ	ผู้ช่วยเลขานุการ

ข้อ 2 ให้คณะกรรมการตามข้อ 1 มีหน้าที่และอำนาจดังต่อไปนี้

(1) กำหนดกรอบธรรมาภิบาลข้อมูล (Data Governance) เพื่อจัดทำนโยบายข้อมูล (Data Policy) รวมถึงแนวปฏิบัติ มาตรฐาน และแผนการดำเนินงานด้านธรรมภิบาลข้อมูลภาครัฐของ สกพอ. ให้สอดคล้องกับประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ ลงวันที่ 12 มีนาคม 2563

(2) ส่งเสริมและสนับสนุนการดำเนินการตามนโยบายและแผนการดำเนินงานด้านธรรมาภิบาลข้อมูลตาม (1) เพื่อให้สามารถดำเนินการไปได้อย่างลุล่วง โดยจัดให้มีกลไกการตรวจสอบ วัดผล และรายงานตลอดจนการปรับปรุงอย่างต่อเนื่อง

(3) กำกับดูแลการดำเนินการธรรมาภิบาลข้อมูล เพื่อให้ข้อมูลของ สกพอ. มีความถูกต้องครบถ้วน เป็นปัจจุบัน มีความมั่นคงปลอดภัย และข้อมูลส่วนบุคคลได้รับการคุ้มครองอย่างเหมาะสม

(4) กำกับดูแลการดำเนินการเกี่ยวกับข้อมูลของ สกพอ. เพื่อให้เป็นไปตามกฎหมายว่าด้วยข้อมูลข่าวสารของราชการ กฎหมายว่าด้วยคุ้มครองข้อมูลส่วนบุคคล กฎหมายว่าด้วยการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล และกฎหมายอื่น ๆ ที่เกี่ยวข้อง

(5) เสนอแนะต่อเลขาธิการแต่งตั้งคณะทำงาน เพื่อสนับสนุนการดำเนินการธรรมาภิบาลข้อมูล คณะบริกรข้อมูล (Data Steard Team) และการปฏิบัติตามข้อกำหนดของกฎหมายที่เกี่ยวข้องตามความเหมาะสม

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

สั่ง ณ วันที่ 23 พฤษภาคม พ.ศ. 2568

(นายจุฬา สุขมานพ)
เลขาธิการคณะกรรมการนโยบายเขตพัฒนาพิเศษภาคตะวันออก

ภาคผนวก ข.

นโยบายข้อมูล สกพอ.

2568

นโยบายข้อมูล

(Data Policy)

รุ่นเอกสาร1

ณ วันที่ 6 พฤษภาคม 2568

สำนักเทคโนโลยีสารสนเทศ
สำนักงานคณะกรรมการนโยบายเขตพัฒนาพิเศษภาคตะวันออก (สกพอ.)

สารบัญ

1. บทนำ (Introduction)

1.1. วัตถุประสงค์ของนโยบาย (Policy Purpose)

1.1.1 กำหนดหลักการและกรอบแนวทางในการใช้ จัดเก็บ และแบ่งปันข้อมูลอย่างมีธรรมาภิบาล

1.1.2 กำหนดกรอบแนวทางในการจัดการและใช้ข้อมูลภายในหน่วยงาน

1.1.3 ส่งเสริมการใช้ข้อมูลอย่างมีประสิทธิภาพ ถูกต้อง ปลอดภัย และโปร่งใส

1.1.4 สนับสนุนการเชื่อมโยงข้อมูลระหว่างหน่วยงานภาครัฐตามหลักธรรมาภิบาลข้อมูล

1.1.5 ปฏิบัติตามกฎหมายและมาตรฐานที่เกี่ยวข้อง เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA)

1.2. ขอบเขตการบังคับใช้ (Scope of Application)

นโยบายฉบับนี้ครอบคลุมการบริหารจัดการข้อมูลในทุกกระบวนการ ตั้งแต่การจัดทำ การจัดเก็บ การประมวลผล การใช้ การแลกเปลี่ยน การเปิดเผย ตลอดจนการจัดเก็บถาวรและการทำลายข้อมูล โดยใช้บังคับกับ:

1) หน่วยงานทุกส่วนภายในองค์กร ที่มีหน้าที่เกี่ยวข้องกับการสร้าง ใช้ จัดเก็บ และจัดการข้อมูล
2) ข้อมูลทุกประเภท ที่อยู่ในความรับผิดชอบขององค์กร ทั้งข้อมูลภายใน ข้อมูลภายนอก ข้อมูลส่วนบุคคล ข้อมูลเปิด และข้อมูลที่มีความอ่อนไหว
3) ระบบงาน ฐานข้อมูล โครงสร้างพื้นฐานดิจิทัล และแพลตฟอร์มที่เกี่ยวข้อง กับการบริหารจัดการข้อมูล
4) บุคลากรทุกระดับ ที่มีหน้าที่หรือเกี่ยวข้องกับการใช้หรือจัดการข้อมูล รวมถึงเจ้าหน้าที่ภายนอกหรือผู้รับจ้างที่ได้รับสิทธิ์เข้าถึงข้อมูลขององค์กร
5) การดำเนินงานที่เกี่ยวข้องกับพันธมิตร หรือหน่วยงานภายนอก ที่มีการแลกเปลี่ยนหรือเชื่อมโยงข้อมูลกับองค์กร

นโยบายนี้ใช้เป็นแนวทางหลักในการควบคุมดูแลข้อมูลขององค์กรให้เป็นไปตามหลักธรรมาภิบาลข้อมูล (Data Governance) และข้อกำหนดของกฎหมาย ระเบียบ ข้อบังคับ หรือมาตรฐานที่เกี่ยวข้อง

1.3. บทบาทและความรับผิดชอบ

1) ผู้บริหารเทคโนโลยีสารสนเทศหรือผู้ที่ได้รับมอบหมายต้องควบคุมและกำกับดูแลให้บุคลากรใน สกพอ. และผู้ที่เกี่ยวข้องดำเนินการตามนโยบายการบริหารจัดการข้อมูลอย่างเคร่งครัด
2) ผู้บริหารเทคโนโลยีสารสนเทศหรือผู้ที่ได้รับมอบหมายต้องตรวจสอบให้แน่ใจว่าบุคลากรใน สกพอ. และบุคคลอื่น ๆ เช่น บริษัทหรือผู้รับจ้าง ที่ได้รับมอบหมายจาก สกพอ. ให้ทำหน้าที่บริหารจัดการข้อมูลได้รับความรู้เกี่ยวกับนโยบายนี้อย่างเหมาะสม และนำนโยบายไปปฏิบัติตามอย่างมีประสิทธิภาพและประสิทธิผล

3) บุคลากรใน สกพอ. และบุคคลอื่น ๆ เช่น บริษัทหรือผู้รับจ้าง ที่ได้รับมอบหมายจาก สกพอ. ให้ทำหน้าที่บริหารจัดการข้อมูลต้องปฏิบัติตามนโยบาย มาตรการ วิธีการ และแนวปฏิบัติต่าง ๆ ที่เกี่ยวข้องกับข้อมูลและระบบข้อมูลสารสนเทศที่ สกพอ. กำหนด
4) คณะกรรมการธรรมาภิบาลข้อมูล/คณะทำงานด้านข้อมูล/เจ้าของข้อมูลและผู้ดูแลข้อมูลต้องปฏิบัติหน้าที่ที่ได้รับมอบหมายภายใต้นโยบายนี้

1.4. คำนิยามและคำจำกัดความที่สำคัญ (Key Definitions and Terminology)

ข้อมูล (Data) หมายความว่า สิ่งที่สื่อความหมายให้รู้เรื่องราวข้อเท็จจริงหรือเรื่องอื่นใด ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเอง หรือโดยผ่านวิธีการใด ๆ และไม่ว่าจะได้จัดทำไว้ในรูปของเอกสารแฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ภาพถ่ายดาวเทียม ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ เครื่องมือตรวจวัด การสำรวจระยะไกล หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้

ชุดข้อมูล (Dataset) หมายความว่า การนำข้อมูลจากหลายแหล่งมารวบรวม เพื่อจัดเป็นชุดให้ตรงตามลักษณะโครงสร้างของข้อมูล หรือจากการใช้ประโยชน์ของข้อมูล

บัญชีข้อมูล (Data Catalog) หมายความว่า เอกสารแสดงบรรดารายการของชุดข้อมูล ที่จำแนกแยกแยะโดยการจัดกลุ่มหรือจัดประเภทข้อมูลที่อยู่ในความครอบครองหรือควบคุมของ สกพอ.

ธรรมาภิบาลข้อมูลภาครัฐ (Data Governance for Government) หมายความว่า การกำหนดสิทธิ หน้าที่และความรับผิดชอบของผู้มีส่วนได้เสียในการบริหารจัดการข้อมูลทุกขั้นตอน เพื่อให้การได้มาและการนำไปใช้ข้อมูลของ สกพอ. ภาครัฐถูกต้อง ครบถ้วน เป็นปัจจุบัน รักษาความเป็นส่วนตัวและสามารถเชื่อมโยงกันได้อย่างมีประสิทธิภาพและมั่นคงปลอดภัย

หมวดหมู่ของข้อมูล (Data Category) ตามกรอบธรรมาภิบาลข้อมูลภาครัฐแบ่งออกได้เป็น 4 หมวดหมู่ ได้แก่ ข้อมูลส่วนบุคคล ข้อมูลความมั่นคง ข้อมูลความลับทางราชการ และ ข้อมูลสาธารณะ

การจัดชั้นความลับของข้อมูล (Data Classification) หมายความว่า การกำหนดประเภทและข้อกำหนดของการจัดชั้นความลับของข้อมูล เพื่อกำหนดสิทธิในการเข้าถึงและสามารถนำข้อมูลไปใช้ได้อย่างเหมาะสม ซึ่งตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 กำหนดให้มีชั้นความลับเป็น ชั้นลับ ชั้นลับมาก หรือ ชั้นลับที่สุด โดยคำนึงถึงการปฏิบัติหน้าที่ของ สกพอ. และประโยชน์แห่งรัฐประกอบกัน ดังนั้น ชั้นความลับของข้อมูลมักถูกกำหนดให้สอดคล้องกับผลกระทบต่อหน่วยงานและความมั่นคงของประเทศ อาทิ ชื่อเสียง ความต่อเนื่องของการดำเนินงาน การเงิน และทรัพยากรบุคคล

วงจรชีวิตของข้อมูล (Data Life Cycle) หมายความว่า ลำดับขั้นตอนของข้อมูลตั้งแต่เริ่มสร้างข้อมูลไปจนถึงการทำลายข้อมูล ตามกรอบธรรมาภิบาลข้อมูลภาครัฐ

ข้อมูลหลักและข้อมูลอ้างอิง (Master and Reference Data) หมายความว่า การบริหารจัดการข้อมูลเพื่อให้ทั้งหน่วยงานสามารถเข้าถึงและใช้ข้อมูลร่วมกันได้ โดยข้อมูลถูกจัดเก็บไว้แหล่งเดียว มีการกำหนดมาตรฐานของข้อมูล เพื่อช่วยลดความซ้ำซ้อนของข้อมูลและทำให้ข้อมูลมีคุณภาพ ซึ่ง Master data เป็นข้อมูลที่สร้างและถูกใช้งานอยู่ภายใน สกพอ. มีโอกาสเปลี่ยนแปลงได้และมีรายละเอียดหรือจำนวนฟิลด์ข้อมูลที่มาก เช่น ข้อมูลพนักงาน ข้อมูลลูกค้า ข้อมูลผู้ขาย ข้อมูลสินค้าและบริการ ข้อมูลครุภัณฑ์ และข้อมูลสถานที่ ในขณะที่ Reference data มีความเป็นสากลถูกสร้างและใช้งานโดยทั่วไป โดยหลากหลายองค์กร หรือแม้กระทั่งใช้งานไปทั่วโลก เช่น รหัสไปรษณีย์ รหัสประเทศ หน่วยวัดระยะทาง

นโยบายข้อมูล (Data Policy)

หมวด 1 หมวดทั่วไป

(General)

วัตถุประสงค์

เพื่อกำหนดแนวทางการดำเนินงานด้านธรรมาภิบาลข้อมูลอย่างชัดเจนและมีประสิทธิภาพ จำเป็นต้องจัดทำนโยบายข้อมูลที่สอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ และข้อกำหนดที่เกี่ยวข้อง โดยผ่านการอนุมัติจากผู้บริหาร พร้อมเผยแพร่และสื่อสารให้ผู้มีส่วนได้ส่วนเสียรับทราบ รวมถึงมีการทบทวนอย่างสม่ำเสมอ เพื่อให้การบริหารจัดการข้อมูลเป็นไปอย่างต่อเนื่องและมีประสิทธิผล

นโยบาย

1. กำหนดโครงสร้างการกำกับดูแลข้อมูล พร้อมระบุบทบาทและความรับผิดชอบของผู้มีส่วนเกี่ยวข้อง โดยเฉพาะเจ้าของข้อมูลที่ต้องรับผิดชอบและอนุมัติการดำเนินการต่าง ๆ ต่อข้อมูล
2. ระบุขอบเขตชุดข้อมูลและข้อมูลที่อยู่ภายใต้กรอบธรรมาภิบาลข้อมูล โดยให้เหมาะสมกับบริบทและความเสี่ยงของ สกพอ.
3. กำหนดแนวทางการดำเนินกิจกรรมที่สนับสนุนธรรมาภิบาลข้อมูล ครอบคลุมการวางแผน การดำเนินการ การตรวจทาน และการปรับปรุงอย่างต่อเนื่อง
4. วางนโยบายและมาตรการป้องกันการเข้าถึง การสูญหาย การทำลาย หรือการเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต รวมถึงคุ้มครองข้อมูลส่วนบุคคล
5. กำหนดมาตรฐานข้อมูล (Data Standard) ที่ครอบคลุมรูปแบบการจัดเก็บ การแลกเปลี่ยน และการจัดลำดับชั้นความลับของข้อมูล
6. สนับสนุนการใช้ทรัพยากรและเทคโนโลยีสารสนเทศในการบริหารจัดการข้อมูลให้มีประสิทธิภาพและเป็นไปตามหลักธรรมาภิบาล
7. ส่งเสริมภาวะผู้นำในการใช้ประโยชน์จากข้อมูล รวมถึงการสร้างนวัตกรรมเพื่อสนับสนุนภารกิจของ สกพอ.
8. กำหนดให้มีการสื่อสารและเผยแพร่นโยบายด้านข้อมูลแก่ผู้เกี่ยวข้อง ทั้งภายในและภายนอกองค์กร
9. จัดให้มีการฝึกอบรมเพื่อสร้างความตระหนักด้านการกำกับดูแลและการบริหารจัดการข้อมูล โดยครอบคลุมกระบวนการธรรมาภิบาลและวงจรชีวิตข้อมูล
10. กำหนดให้มีการประเมินผลการดำเนินงานด้านธรรมาภิบาลข้อมูล พร้อมทั้งติดตามและรายงานผลอย่างน้อยปีละ 1 ครั้ง
11. กำหนดให้มีการตรวจสอบความสอดคล้องระหว่างนโยบายข้อมูลกับการดำเนินงานของผู้มีส่วนได้ส่วนเสียอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่านโยบายถูกนำไปใช้จริงอย่างมีประสิทธิภาพ
12. กำหนดให้มีการทบทวนนโยบายข้อมูลอย่างน้อยปีละ 1 ครั้ง และดำเนินการปรับปรุงต่อเนื่อง หากพบว่าการกำกับดูแลข้อมูลยังไม่มีประสิทธิภาพเพียงพอ

หมวด 2 การสร้างข้อมูลและการจัดเก็บข้อมูล
(Data Creation and Data Storage)

วัตถุประสงค์

เพื่อกำหนดแนวทางการสร้างและจัดเก็บข้อมูลให้ถูกต้องเป็นระบบ ปลอดภัย และสามารถนำไปใช้ประโยชน์ได้อย่างมีประสิทธิภาพ โดยยึดหลักมาตรฐานข้อมูลและการกำกับดูแลข้อมูลที่เหมาะสม ครอบคลุมตลอดวงจรชีวิตข้อมูล

นโยบาย

การสร้างข้อมูล (Data Creation)

1. การสร้างข้อมูลต้องดำเนินการด้านการรักษาความปลอดภัยของข้อมูล (Data Security) โดย
   1.1. ต้องมีการควบคุมการเข้าถึง (Access Control) โดยกำหนดบุคคลที่สามารถสร้างข้อมูลได้ หากบุคคลดังกล่าวมีสิทธิ์แค่การเห็นข้อมูลเพียงอย่างเดียว จะไม่สามารถสร้างข้อมูลได้
   1.2. ต้องมีการบันทึกเหตุการณ์และการติดตามความเคลื่อนไหว (Logging and Monitoring) ของข้อมูลที่ถูกสร้างขึ้น
2. ต้องกำหนดมาตรฐานในการสร้างข้อมูลให้มีคุณภาพเหมาะสมกับข้อมูลแต่ละประเภท (Preventive Data Quality) โดยต้องมีการตรวจสอบให้ข้อมูลที่ถูกสร้างเป็นไปตามมาตรฐานที่กำหนดก่อนทำการบันทึกข้อมูลเช่น การกำหนดโครงสร้างของข้อมูล การกำหนดข้อมูลในฟิลด์บังคับที่ต้องกรอกอย่างครบถ้วน (Mandatory Field) เป็นต้น
3. ต้องกำหนดเจ้าของข้อมูลทำหน้าที่รับผิดชอบดูแลข้อมูลดังกล่าว
4. ต้องกำหนดผู้กรอกข้อมูลทำหน้าที่รับผิดชอบการนำเข้าข้อมูล
5. มีการจัดทำเมทาดาตา (Metadata) ของข้อมูล เพื่อใช้เป็นคำอธิบาย ข้อมูล

การจัดเก็บข้อมูล (Data Storage)

1. มีการมอบหมายผู้ดูแลข้อมูล (Data Administrator)
2. การรวบรวมและจัดเก็บข้อมูลต้องทำให้เหมาะสมกับชั้นความลับของ ข้อมูล ความต้องการ และวัตถุประสงค์ในการดำเนินงาน
   2.1. ต้องเก็บข้อมูลตามสถาปัตยกรรมข้อมูลอย่างเหมาะสม
   2.2. ต้องจัดระเบียบข้อมูลให้เหมาะแก่การใช้งาน
   2.3. ต้องมีการระบุเวอร์ชันของข้อมูลเมื่อมีการแก้ไข หรือปรับปรุงให้เป็นปัจจุบัน
3. การจัดเก็บข้อมูลต้องดำเนินการผ่านการรักษาความปลอดภัยของข้อมูล (Dala Security) โดยต้องมี
   3.1. การควบคุมการเข้าถึง (Access Control)
   3.2. การบันทึกเหตุการณ์และการติดตามความเคลื่อนไหว (Logging and Monitoring)

3.3. การจัดและกู้คืนข้อมูล (Backup and Restore)

4. ข้อมูลที่ถูกจัดเก็บต้องได้รับการระบุสิทธิ์การเข้าถึงข้อมูล (Data Access) เพื่อให้ผู้มีสิทธิ์สามารถเข้าถึงข้อมูลโดยไม่ต้องทำเรื่องร้องขอ (Access by Default)
5. ข้อมูลที่ถูกจัดเก็บต้องได้รับการตรวจวัดคุณภาพข้อมูล (Data Quality) ในมิติต่าง ๆ เช่น ความครบถ้วนสมบูรณ์ของข้อมูล Completeness)
6. ความถูกต้องแม่นยำของข้อมูล (Accuracy) ความสอดคล้อง (Consistency) และความเป็นปัจจุบันของข้อมูล (Timeliness) หากพบว่าข้อมูลมีคุณภาพไม่ผ่านเกณฑ์ที่กำหนดจะต้องดำเนินการแก้ไข คุณภาพข้อมูลให้ผ่านเกณฑ์ (Corrective Data Quality) ตามกรอบเวลาที่กำหนด หรือชี้แจงให้คณะธรรมาภิบาลข้อมูลรับทราบ เพื่อหารือถึงแนวทางในการแก้ปัญหา
7. ข้อมูลที่ถูกจัดเก็บต้องได้รับการจัดการดูแลโครงสร้างข้อมูล (Data Stucture) ให้เหมาะสมผ่านการทำแบบจำลองข้อมูล (Data Modeing) ทั้งการปรับเปลี่ยนโครงสร้างข้อมูลให้สอดคล้องกับความต้องการหาง ธุรกิจ ความต้องการทางระบบ และความต้องการทางสถาปัตยกรรมข้อมูล
8. ข้อมูลที่ถูกจัดเก็บต้องได้รับการสำรองข้อมูลอย่างสม่ำเสมอ เพื่อให้พร้อมต่อการกู้คืนเมื่อเกิดเหตุฉุกเฉิน
9. กำหนดให้มีการจัดทำรายงานการตรวจสอบ และกำกับดูแลแนวทางปฏิบัติในการจัดเก็บข้อมูลอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง

หมวด 3 การประมวลผลข้อมูลและการใช้ข้อมูล
(Data Processing and Data Usage)

วัตถุประสงค์

เพื่อกำหนดแนวทางการประมวลผลและการใช้ข้อมูลอย่างถูกต้อง โปร่งใส และเป็นไปตามวัตถุประสงค์ที่กำหนด โดยคำนึงถึงความถูกต้องของข้อมูล ความปลอดภัย และสิทธิของเจ้าของข้อมูลตามหลักธรรมาภิบาลข้อมูล

แนวนโยบาย

1. ข้อมูลจะต้องผ่านการประเมินชั้นความลับของข้อมูลก่อนถูกนำไปใช้งาน
2. ข้อมูลจะต้องได้รับการประเมินคุณภาพของข้อมูล และผ่านเกณฑ์มาตรฐานในมิติต่าง ๆ ขององค์กร เว้นเสียแต่ได้รับการอนุมัติจากคณะธรรมาภิบาลข้อมูล
3. การใช้ข้อมูลต้องดำเนินการด้านการรักษาความปลอดภัยของข้อมูล (Data Security) โดยต้องมี
   3.1. การควบคุมการเข้าถึง (Access Control) ในทุกกรณี
   3.2. ต้องมีการบันทึกเหตุการณ์และการติดตามความเคลื่อนไหว (Logging and Monitoring) ในกรณีที่มีการร้องขอเข้าใช้ข้อมูล
   3.3. การจัดเก็บข้อมูลสำรองและกู้คืนข้อมูล (Backup and Restore) ในกรณีที่มีการร้องขอเข้าใช้ข้อมูล
   3.4. การจัดเก็บข้อมูลถาวรและทำลายข้อมูล (Archive and Destroy) ในกรณีที่มีการร้องขอเข้าใช้ข้อมูล
4. ข้อมูลพร้อมใช้งานต้องได้รับการจัดทำเมทาดาตา (Metadata) ให้ผู้ใช้ข้อมูลสามารถสืบค้นได้อย่างชัดเจน
5. ข้อมูลพร้อมใช้งานต้องได้รับการจัดทำเส้นทางของข้อมูล (Data Lineage) เพื่อให้ผู้ใช้ข้อมูลสามารถรู้ว่าข้อมูลที่ตนเองใช้มีที่มาและที่ไปเป็นอย่างไร
6. ผู้ที่มีสิทธิ์เข้าถึงข้อมูลสามารถใช้ข้อมูลดังกล่าวได้โดยไม่ต้องทำเรื่องร้องขอ ในทางกลับกันหากมีเหตุจำเป็นต้องใช้ข้อมูล แต่ไม่มีสิทธิ์เข้าถึง ข้อมูลต้องทำเรื่องร้องขอสิทธิ์เข้าถึงข้อมูล โดยกระบวนการอนุมัติคำร้องจะอ้างอิงตามชั้นความลับของข้อมูลดังกล่าว
7. การร้องขอสิทธิ์เข้าถึงข้อมูลต้องระบุ
   7.1. ระบุตัวตน ตำแหน่งงาน แผนกงานของผู้ขอใช้ข้อมูล
   7.2. ขอบเขตการใช้ข้อมูลภายในหรือภายนอกองค์กร
   7.3. วัตถุประสงค์ในการใช้ข้อมูล
   7.4. ระยะเวลาในการใช้ข้อมูล
   7.5. รายละเอียดเพิ่มเติม ที่สามารถช่วยตัดสินใจในการอนุมัติข้อมูลได้ง่ายขึ้น

8. การร้องขอสิทธิ์ในการเข้าถึงข้อมูลต้องแนบเอกสารที่เกี่ยวข้องตามกฎระเบียบ กฎหมาย และข้อบังคับที่เกี่ยวข้องให้ครบถ้วน เช่น ใบคำร้อง สัญญาห้ามเปิดเผยข้อมูล สัญญาการใช้หรือประมวลผลข้อมูลส่วนบุคคล เอกสารยินยอมให้ใช้ข้อมูลส่วนบุคคลจากเจ้าของข้อมูล เป็นต้น
9. ในการร้องขอข้อมูล อย่างน้อยต้องได้รับการเก็บบันทึกรายละเอียด (Log)
   9.1. ผู้ร้องขอ ผู้อนุมัติ และผู้เปิดสิทธิ์เข้าถึงข้อมูล
   9.2. วันที่ทำการร้องขอ วันที่ทำการอนุมัติ และวันที่ทำการเปิดสิทธิ์เข้าถึงข้อมูล
   9.3. วันที่สิทธิ์การเข้าถึงสิ้นสุด และวันที่ทำการปิดสิทธิ์เข้าถึงข้อมูล
   9.4. ระยะเวลาการเปิดสิทธิ์
10. ผู้ใช้ข้อมูลต้องใช้ตามวัตถุประสงค์ที่ได้ยื่นคำร้องไป และต้องปฏิบัติตามกฎระเบียบ กฎหมาย และข้อบังคับที่เกี่ยวข้องเท่านั้น
11. ข้อมูลที่ประกอบไปด้วยข้อมูลส่วนบุคคล จะต้องได้รับการประเมินถึงความเหมาะสมในการนำข้อมูลไปใช้ ตามวัตถุประสงค์ของการเก็บ ข้อมูลนั้น ๆ โดยเจ้าของข้อมูลเป็นผู้ประเมิน ในกรณีที่ผู้ใช้งานได้แจ้ง วัตถุประสงค์ในการใช้ซึ่งเป็นการใช้ที่ไม่จำเป็นต้องมีการระบุตัวตนเจ้าของข้อมูล จะต้องพิจารณาการทำข้อมูลนิรนาม (Anonymous Data)
12. ต้องมีบัญชีข้อมูล (Data Catalog) เป็นแหล่งแสดงผลข้อมูลพร้อมใช้ทุกชุด เพื่อเป็นแหล่งสืบค้นแก่ผู้ใช้ข้อมูล
13. บัญชีข้อมูล (Data Catalog) ต้องได้รับการปรับให้เป็นปัจจุบันเพื่อสอดคล้องกับความต้องการใช้ข้อมูลอยู่เสมอ โดยต้องได้รับการจัดกลุ่มข้อมูล (Collection) อย่างเหมาะสม เพื่อสะดวกในการค้นหา ข้อมูล
14. ต้องมีการระบุบทบาทหน้าที่ผู้รับผิดชอบในการใช้งานและดูแลบัญชีข้อมูล เพื่อจัดการบัญชีข้อมูลให้ถูกต้องเหมาะสมอยู่เสมอ
15. กำหนดให้มีการจัดทำรายงานการตรวจสอบ และกำกับดูแลแนวทางปฏิบัติในการใช้ข้อมูลอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง

หมวด 4 การจัดเก็บข้อมูลถาวรและการทำลายข้อมูล

(Data archive and Data Destruction)

วัตถุประสงค์

เพื่อกำหนดแนวทางการจัดเก็บข้อมูลถาวรและการทำลายข้อมูลอย่างเหมาะสม ปลอดภัย และตรวจสอบได้ โดยยึดตามวงจรชีวิตข้อมูล ระยะเวลาการจัดเก็บ และข้อกำหนดทางกฎหมายที่เกี่ยวข้อง

แนวนโยบาย

1. เมื่อครบกำหนดระยะเวลาต้องทำการจัดเก็บข้อมูลถาวร โดยต้องกำหนดผู้รับผิดชอบ กรอบระยะเวลาในการจัดเก็บข้อมูลถาวรอย่าง ชัดเจน และแหล่งจัดเก็บข้อมูลถาวร ซึ่งกระบวนการทั้งหมดต้องไม่ขัด ต่อ กฎระเบียบ กฎหมาย และข้อบังคับที่เกี่ยวข้อง
2. การจัดเก็บข้อมูลถาวรและการทำลายต้องดำเนินการด้านการรักษาความปลอดภัยของข้อมูล (Data Security) โดยต้องมี
   2.1. การควบคุมการเข้าถึง (Access Control)
   2.2. การควบคุมการเคลื่อนไหวของข้อมูล (Movement Control)
   2.3. การบันทึกเหตุการณ์และการติดตามความเคลื่อนไหว (Logging and Monitoring)
   2.4. การจัดเก็บข้อมูลสำรองและกู้คืนข้อมูล (Backup and Restore) โดยสำหรับการทำลายข้อมูลต้องมีการกำหนดระยะเวลาในการสำรองและกู้คืนข้อมูล (Backup and Restore) ก่อนทำการลบข้อมูลถาวร (Permanently Delete)
3. ต้องมีการแสดงผลคำอธิบายชุดข้อมูลหลัก (Mandatory Metadata) ที่จำเป็นของข้อมูลที่ถูกจัดเก็บถาวรและทำลาย เช่น ชื่อข้อมูล คำอธิบาย ข้อมูล ชั้นความลับของข้อมูล เจ้าของข้อมูล และบริกรข้อมูล เป็นต้นเพื่อเป็นสารสนเทศประกอบการตัดสินใจ และกำหนดระยะเวลาในการจัดเก็บถาวรและทำลายข้อมูล
4. ต้องเก็บรักษาคำอธิบายชุดข้อมูลหลัก (Mandatory Metadata) ของ ข้อมูลที่ถูกจัดเก็บถาวรและข้อมูลที่ถูกทำลายให้ครบถ้วน เพื่อประโยชน์ในการกำกับดูแลและตรวจสอบ หรือการเรียกคืนข้อมูลในภายหลัง
5. การจัดเก็บถาวรและทำลายข้อมูล ต้องมีการระบุ
   5.1. แหล่งจัดเก็บข้อมูลถาวรของข้อมูลที่ถูกจัดเก็บไว้
   5.2. เจ้าของข้อมูล ผู้กำหนดระยะเวลาการจัดเก็บถาวรและทำลายข้อมูล
   5.3. นักเทคโนโลยีสารสนเทศ ผู้ดำเนินการจัดเก็บถาวรและทำลายข้อมูล
   5.4. ระยะเวลาในการจัดเก็บข้อมูลถาวรก่อนถึงขันตอนการทำลายข้อมูล
   5.5. วันที่จัดเก็บข้อมูลถาวร และวันที่ทำลายข้อมูล

6. ต้องกำหนดกระบวนการในการจัดเก็บข้อมูลถาวรและทำลายข้อมูลอย่างชัดเจนเหมาะสม โดยอ้างอิงตามชั้นความลับของข้อมูล
7. ต้องกำหนดกระบวนการในการร้องขอให้ดำเนินการจัดเก็บข้อมูลถาวรและทำลายข้อมูลอย่างชัดเจนเหมาะสม โดยอ้างอิงตามชั้นความลับของ ข้อมูล
8. ต้องกำหนดกระบวนการในการร้องขอเพื่อเรียกคืนข้อมูลที่ถูกจัดเก็บถาวร (Retention) อย่างชัดเจนเหมาะสม โดยอ้างอิงตามชั้นความลับของข้อมูล
9. การเรียกคืนข้อมูลที่ถูกจัดเก็บถาวร (Retention) ต้องระบุ
    9.1. ระบุตัวตน ตำแหน่งงาน แผนกงานของผู้ขอใช้ข้อมูล
    9.2. ขอบเขตการใช้ข้อมูลภายในหรือภายนอกองค์กร
    9.3. วัตถุประสงค์ในการใช้ข้อมูล
    9.4. ระยะเวลาในการเรียกคืน (Retention Period)
    9.5. เวอร์ชั่นของการเรียกคืน (Retention Version)
    9.6. รายละเอียดเพิ่มเติมที่สามารถช่วยตัดสินใจในการอนุมัติข้อมูลได้ง่ายขึ้น
10. ในการเรียกคืนข้อมูลที่ถูกจัดเก็บถาวร (Retention) อย่างน้อยต้องได้รับการเก็บบันทึกรายละเอียด (Log) ดังนี้
    10.1. ผู้ร้องขอ ผู้อนุมัติ และผู้เรียกคืนข้อมูล
    10.2. วันที่ทำการร้องขอ วันที่ทำการอนุมัติ และวันที่ทำการเรียก คืนข้อมูล
    10.3. วันที่สิทธิ์การเข้าถึงสิ้นสุด และวันที่ทำการยกเลิกการเรียก คืนข้อมูล
    10.4. ระยะเวลาการเรียกคืนข้อมูล
11. กำหนดให้มีการจัดทำรายงานการตรวจสอบ และกำกับดูแลแนวทางปฏิบัติในการจัดเก็บข้อมูลถาวรและทำลายข้อมูลอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง

หมวด 5 การเชื่อมโยงและแลกเปลี่ยนข้อมูล

(Data Integration and Exchange Policy)

วัตถุประสงค์

เพื่อกำหนดแนวทางการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างระบบหรือหน่วยงานอย่างมีมาตรฐาน ปลอดภัย และเชื่อถือได้ โดยส่งเสริมการใช้ข้อมูลร่วมกันอย่างมีประสิทธิภาพ ภายใต้กรอบกฎหมายและการควบคุมสิทธิ์การเข้าถึงข้อมูล

แนวนโยบาย

1. กำหนดแนวปฏิบัติในการแลกเปลี่ยนและเชื่อมโยงข้อมูล (Data Integration) จากหน่วยงานภายนอก ทั้งภาครัฐและเอกชน โดยแนวปฏิบัติต้องกำหนดกลไกหรือเทคโนโลยีที่ใช้ในการแลกเปลี่ยนและเชื่อมโยงข้อมูล ตั้งแต่ขั้นตอนการเตรียมการ ขั้นตอนการเริ่มดำเนินการ ขั้นตอนระหว่างดำเนินการ ตลอดจนการสิ้นสุดการดำเนินการ แลกเปลี่ยนหรือเชื่อมโยงข้อมูล
2. กำหนดและจัดทำคำอธิบายข้อมูล (Meta Data) ของชุดข้อมูลที่ต้องการแลกเปลี่ยนและเชื่อมโยงข้อมูล โดยครอบคลุมถึงผู้รับผิดชอบเมื่อมีการเปลี่ยนแปลงของชุดข้อมูล
3. กำหนดให้มีการจัดทำสัญญาอนุญาต บันทึกข้อตกลง (Memorandum of Understanding :MOU) สัญญารักษาความลับ (Non-disclosure agreement : NDA) หรือข้อตกลงอื่นใดว่าด้วยการแลกเปลี่ยนและเชื่อมโยงข้อมูลระหว่างองค์กรก่อนการแลกเปลี่ยนและเชื่อมโยงข้อมูล
4. กำหนดเทคโนโลยีและมาตรฐานทางเทคนิคที่ใช้ในการแลกเปลี่ยนและเชื่อมโยงข้อมูล
5. กำหนดให้มีบันทึกรายละเอียดและจัดเก็บข้อมูลการดำเนินงานที่เกิดขึ้นในแต่ละครั้งที่มีการแลกเปลี่ยนและเชื่อมโยงข้อมูล (Log) ระหว่างหน่วยงาน เพื่อให้สามารถตรวจสอบย้อนกลับได้ว่าการแลกเปลี่ยนและเชื่อมโยงข้อมูล ได้ดำเนินการอย่างเหมาะสม หรือเป็นไปตามแนวทางปฏิบัติและมาตรฐานตามที่กำหนดร่วมกัน

หมวด 6 การเปิดเผยข้อมูล

(Open Data)

วัตถุประสงค์

เพื่อส่งเสริมการเปิดเผยข้อมูลภาครัฐอย่างโปร่งใส ตรวจสอบได้ และนำไปใช้ประโยชน์ต่อยอดได้อย่างกว้างขวาง โดยคำนึงถึงความถูกต้องของข้อมูล สิทธิส่วนบุคคล และข้อจำกัดทางกฎหมายที่เกี่ยวข้อง

แนวนโยบาย

1. กระบวนการในการเปิดเผยข้อมูล และเทคโนโลยีที่ใช้ต้องไม่ขัดกฎระเบียบ กฎหมาย และข้อบังคับที่เกี่ยวข้อง และต้องสอดคล้องกับขั้นความลับของข้อมูล
2. การเปิดเผยข้อมูลต้องสอดคล้องกับวัตถุประสงค์ในการใช้งานข้อมูล
3. ข้อมูลที่ถูกเปิดเผยต้องได้รับการจัดทำชั้นความลับของข้อมูลแล้วท่านั้นหากยังไม่ได้รับการจัดทำชั้นความลับของข้อมูล จะไม่สามารถเปิดเผยข้อมูลดังกล่าว
4. ข้อมูลที่ถูกเปิดเผยต้องได้รับการตรวจวัดและแสดงผลผ่านเกณฑ์คุณภาพของข้อมูลเท่านั้น หากคุณภาพข้อมูลไม่ผ่านเกณฑ์ จะไม่สามารถเปิดเผยข้อมูลดังกล่าวได้ ยกเว้นได้รับการยกเว้นพิเศษจากคณะกรรมการธรรมาภิบาลข้อมูล
5. การเปิดเผยข้อมูลต้องมีการกำหนดระยะเวลาในการเปิดเผย โดยหากครบกำหนดระยะเวลาแล้ว นักเทคโนโลยีสารสนเทศต้องดำเนินการยกเลิกแชร์ข้อมูลในทันที
6. การเปิดเผยข้อมูลต้องดำเนินการด้านการรักษาความปลอดภัยของ ข้อมูล (Data Security) โดยต้องมี
   6.1. การควบคุมการเข้าถึง (Access Control) ยกเว้นข้อมูลในระดับชั้นสาธารณะ
   6.2. การควบคุมการเคลื่อนไหวของข้อมูล (Movement Control)
   6.3. การบันทึกเหตุการณ์และการติดตามความเคลื่อนไหว (Logging and Monitoring)
   6.4. การจัดเก็บข้อมูลสำรองและกู้คืนข้อมูล (Backup and Restore)
   6.5. การจัดเก็บข้อมูลถาวรและทำลายข้อมูล (Archive and Destroy) ต้องทำลายข้อมูลทันทีที่ครบกำหนดระยะเวลาเปิดเผยข้อมูล
7. ในกระบวนการเปิดเผยข้อมูล ต้องควบคุมการเคลื่อนไหวของข้อมูล (Movement Control) โดยอ้างอิงกับชั้นความลับของข้อมูลดังกล่าว
8. ต้องดำเนินการป้องกันไม่ให้มีการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต
9. เมื่อมีการเปิดเผยข้อมูลต้องเปิดเผยคำอธิบายชุดข้อมูล (Metadata) ควบคู่ไปพร้อมกัน
10. ต้องกำหนดช่องทางในการเปิดเผยข้อมูลที่สามารถเข้าถึง และนำไปใช้ได้ง่าย แต่ยังอยู่ในสภาพแวดล้อม (Environment) ที่สามารถควบคุมได้
11. กำหนดให้มีการจัดทำรายงานการตรวจสอบ และกำกับดูแลแนวทางปฏิบัติในการเปิดเผยข้อมูลอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง

หมวด 7 ความน่าเชื่อถือและคุณภาพข้อมูล
(Data Reliability and Data Quality)

วัตถุประสงค์

เพื่อกำหนดแนวทางการดูแลข้อมูลให้มีความถูกต้อง ครบถ้วน ทันสมัย และเชื่อถือได้ตลอดวงจรชีวิตข้อมูล และสนุนการใช้ข้อมูลในการตัดสินใจเชิงนโยบายและการดำเนินงานอย่างมีประสิทธิภาพ

แนวนโยบาย

1. กำหนดให้มีบทบาทหน้าที่และผู้รับผิดชอบที่เกี่ยวข้องกับการควบคุมคุณภาพข้อมูลและชุดข้อมูล โดยต้องครอบคลุมตลอดทั้งวงจรชีวิตข้อมูล (Data Lifecycle)
2. กำหนดให้มีชุดข้อมูลและข้อมูลต้องมีคุณภาพในมิติขั้นต่ำ ดังต่อไปนี้
   2.1. ความครบถ้วน (Completeness) เป็นการวัดค่าในชุดข้อมูลของเราว่ามีความครบถ้วนมากน้อยแค่ไหน ไม่ได้มีค่าว่าง ในช่องที่ควรมีข้อมูลครบถ้วน
   2.2. ความเป็นเอกลักษณ์ (Uniqueness) เป็นการวัดความไม่ซ้ำซ้อนกันของค่าในชุดข้อมูล ที่ไม่ควรมีการซ้ำซ้อนกัน เช่น ข้อมูลเลขบัตรประจำตัวประชาชน ในทะเบียนข้อมูลประชาชนควรมีหนึ่งข้อมูลต่อประชาชนหนึ่งคน ไม่ควรมีเลขบัตรที่ซ้ำกัน
   2.3. ความเป็นปัจจุบัน (Timeliness) เป็นการวัดค่าความเป็นปัจจุบันในชุดข้อมูลว่ามีความทันสมัยเพียงพอต่อการใช้งานและพร้อมใช้งานตามที่กำหนดและในกรอบเวลาที่กำหนดไว้ หรือมีข้อมูลทันต่อการใช้งานทุกครั้งตามที่ผู้ใช้ต้องการ
   2.4. ความเที่ยงตรง (Validity) เป็นการวัดค่าในชุดข้อมูลว่าเก็บรวบรวมตามรูปแบบที่องค์กรหรือมาตรฐานกำหนดไว้ หรืออยู่ในช่วงที่เหมาะสมหรือไม่
   2.5. ความถูกต้อง (Accuracy) เป็นการวัดค่าในชุดข้อมูลว่าตรงกับความเป็นจริงมากน้อยเพียงใด เพื่อบ่งชี้ความมีคุณภาพของข้อมูลที่สามารถสะท้อนถึงสถานการณ์ที่เกิดขึ้นจริงได้
   2.6. ความสอดคล้องกัน (Consistency) เป็นการวัดค่าความสอดคล้องในชุดข้อมูลเมื่อเคลื่อนผ่านเครือข่ายและแอปพลิเคชันต่าง ๆ ค่าของข้อมูลเดียวกันที่จัดเก็บไว้ในตำแหน่งที่แตกต่างกันไม่ควรขัดแย้งกัน เช่น ข้อมูลรหัสไปรษณีย์ของแต่ละพื้นที่ ที่แสดงแต่ละระบบควรจะจัดเก็บไว้อย่างสอดคล้องตรงกัน
3. กำหนดตัวชีวัดและค่าเป้าหมายของคุณภาพของข้อมูลและชุดข้อมูล และวัดวิเคราะห์คุณภาพข้อมูลตามตัวชี้วัดคุณภาพ ดำเนินการปรับปรุงแก้ไขเมื่อคุณภาพของข้อมูลและชุดข้อมูลไม่ตรงตามค่าเป้าหมายที่กำหนดไว้
4. กำหนดสภาพแวดล้อมเทคโนโลยี กลไกวิธีการ ในการจัดเก็บข้อมูล ใช้ และทำลายข้อมูลที่เอื้อต่อการรักษาระดับคุณภาพของข้อมูลและชุดข้อมูล
5. ข้อมูลหรือชุดข้อมูลจากแหล่งอื่น นอกเหนือการกำกับดูแลของ สกพอ. ต้องมีการวัดวิเคราะห์คุณภาพข้อมูลก่อนนำมาใช้งาน

6. ต้องมีการทบทวนตัวชี้วัดและค่าเป้าหมายของคุณภาพข้อมูล อย่างน้อยปีละ 1 ครั้ง และให้ดำเนินการปรับปรุง อย่างต่อเนื่อง

หมวด 8 มาตรฐานการจัดขั้นความลับข้อมูล

(Data Classification Standard)

วัตถุประสงค์

เพื่อกำหนดมาตรฐานการจัดชั้นความลับของข้อมูลตามระดับความสำคัญและความเสี่ยง เพื่อควบคุมการเข้าถึงและการใช้ข้อมูลอย่างเหมาะสม โดยคำนึงถึงความปลอดภัยของข้อมูล การปฏิบัติตามกฎหมาย และการบริหารจัดการข้อมูลอย่างมีประสิทธิภาพ

แนวนโยบาย

1. ข้อมูลทุกชุดต้องมีการจัดชั้นความลับของข้อมูล ดังนี้
    1.1. ระดับที่ 1 ข้อมูลสาธารณะ คือข้อมูลที่เปิดเผยต่อบุคคลภายนอก โดยข้อมูลนั้นต้องไม่ส่งผลกระทบต่อการดำเนินงานอย่างมีนัยสำคัญ อย่างไรก็ตาม ข้อมูลประเภทนี้ต้องได้รับการปกป้องดูแลเพื่อให้มั่นใจได้ว่า ข้อมูลจะมีความสมบูรณ์พร้อมเมื่อมีการเปิดเผย เพื่อสร้างความน่าเชื่อถือให้ผู้ใช้งาน และเป็นการรักษาภาพลักษณ์ดีของบริษัทฯ
    1.2. ระดับที่ 2 ข้อมูลใช้ภายในองค์กร คือข้อมูลที่ได้รับอนุญาตให้ใช้ภายในหน่วยงานที่เฉพาะเจาะจงเท่านั้น การเข้าถึงหรือการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตอาจนำไปสู่ผลกระทบต่อการดำเนินการประจำวันของหน่วยงาน แต่ไม่กระทบต่อการดำเนินงานโดยรวมขององค์กร
    1.3. ระดับที่ 3 ข้อมูลลับ คือข้อมูลที่มีความสำคัญและจำเป็นต่อการดำเนินธุรกิจของบริษัทฯ ซึ่งสามารถเข้าถึง หรือใช้งานได้โดยกลุ่มบุคคลที่ได้รับอนุญาตเท่านั้น การเข้าถึงหรือการเปิดเผยข้อมูลเหล่านี้โดยไม่ได้รับอนุญาตสามารถส่งผลกระทบต่อบริษัท สร้างความเสียหายในเรื่องต่าง ๆ เช่น ผลขาดทุนทางการเงิน การติดขัดในการดำเนินงานรายวัน รวมถึงอุปสรรคในความก้าวหน้าทาง ธุรกิจ และชื่อเสียงของบริษัทฯ
    1.4. ระดับที่ 4 ข้อมูลลับมาก คือข้อมูลที่มีความสำคัญและจำเป็นอย่างยิ่งต่อการดำเนิน ธุรกิจของบริษัทฯ สามารถเข้าถึง หรือใช้งานได้โดยเจ้าของ ข้อมูลหรือบุคคลที่ได้รับอนุญาตเท่านั้น การเข้าถึงหรือการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตสามารถส่งผลกระทบอย่างใหญ่หลวงต่อกลยุทธ์ในการดำเนินธุรกิจของบริษัทฯ และอาจนำไปสู่การสูญเสียความสามารถในการแข่งขันกับคู่แข่งได้
2. ข้อมูลทุกชุดต้องได้รับการติดป้ายกำกับแสดงชั้นความลับของ ข้อมูล และมีการแสดงผลชั้นความลับข้อมูลใน Metadata
3. ชุดข้อมูลที่ไม่ได้รับการจัดชั้นความลับจะไม่สามารถใช้งานได้
4. การจัดชั้นความลับจะต้องได้รับการดำเนินการโดยบริกรข้อมูล ได้รับการตรวจสอบโดยเจ้าของข้อมูล และผ่านการอนุมัติโดยคณะธรรมาภิบาลข้อมูล

5. ข้อมูลระดับชั้นใช้ภายในองค์กร ข้อมูลความลับ และข้อมูลความลับมาก ต้องมีการระบุผู้ใช้ผู้มีสิทธิ์เข้าถึงข้อมูลตามบทบาทหน้าที่ในการดำเนินงานอย่างเหมาะสม
6. ข้อมูลใช้ภายในองค์กร ข้อมูลความลับ และข้อมูลความลับมาก ต้องได้รับการกำหนดกระบวนการในการร้องขอ อนุมัติ เผยแพร่ และปกป้องข้อมูลอย่างเหมาะสม โดยยิ่งมีระดับของชั้นความลับข้อมูลสูง ยิ่งต้องมีกระบวนการที่เข้มงวดให้สอดคล้องกัน
7. การพิจารณาข้อมูลส่วนบุคคล จะต้องเป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยชุดข้อมูลที่มีข้อมูลส่วน บุคคลเป็นส่วนประกอบ จะถูกจัดชั้นความลับในระดับลับเป็นต้นไป
8. ชั้นความลับของข้อมูลต้องได้รับการดำเนินการโดยเจ้าของข้อมูลบริกรข้อมูล และผู้มีส่วนเกี่ยวข้องอื่นทุกคน โดยบริกรข้อมูลเป็นผู้ประเมินหลัก และต้องได้รับการตรวจสอบ หรือข้อเสนอแนะจากเจ้าของข้อมูล หรือผู้มีส่วนเกี่ยวข้องกับข้อมูล
9. กำหนดให้มีการจัดทำรายงานการตรวจสอบตามคำร้อง และมีการ จัดทำรายงานแนวทางกำกับและการปฏิบัติด้านชั้นความลับข้อมูลอย่างน้อยปีละ 1 ครั้ง

หมวด 9 มาตรฐาน Metadata ในหน่วยงานภาครัฐ

วัตถุประสงค์

เพื่อกำหนดมาตรฐานการจัดทำ Metadata ที่สอดคล้องกันในระดับหน่วยงาน เพื่อให้สามารถจัดการค้นหา และเชื่อมโยงข้อมูลได้อย่างมีประสิทธิภาพ โดยสนับสนุนการบูรณาการข้อมูลภาครัฐและการเปิดเผยข้อมูลตามหลักธรรมาภิบาลและมาตรฐานกลางของประเทศ

นโยบาย

1. ข้อมูลพร้อมใช้ทุกชุดต้องได้รับการจัดทำ Metadata ให้ครบถ้วน
2. Metadata แบ่งออกเป็น คำอธิบายชุดข้อมูลส่วนหลัก หรือ Mandatory Metadata และคำอธิบายชุดข้อมูลทางเลือก หรือ Optional Metadata โดยทีมบริกรข้อมูลมีหน้าที่ออกแบบหัวข้อต่างๆ ซึ่งผู้มีส่วนได้ส่วนเสียจะต้องให้ความร่วมมือในการกรอกรายละเอียดให้ครบถ้วน โดยเฉพาะคำอธิบายชุดข้อมูลส่วนหลักที่จะต้องมีความครบถ้วนเพื่อให้ชุดข้อมูลนั้นมีความพร้อมใช้
3. เพื่อให้ผู้ใช้งานมีความเข้าใจในเชิงโครงสร้างของข้อมูล สามารถมีการ จัดทำพจนานุกรมข้อมูล (Data Dictionar) เพิ่มเติมได้ โดยบริกร ข้อมูลมีหน้าที่ออกแบบ และผู้ดูแลข้อมูลมีหน้าที่กรอกรายละเอียดดังกล่าว
4. คำอธิบายชุดข้อมูลเชิงธุรกิจ หรือ Business Metadata ต้องได้รับการดำเนินการโดยเจ้าของข้อมูล หรือตัวแทนเจ้าของข้อมูล ภายใต้การสนับสนุนและกำกับดูแลของบริกรข้อมูล
5. Metadata ต้องได้รับการเผยแพร่ให้ผู้เกี่ยวข้องกับข้อมูลทุกคนได้รับรู้และสามารถเข้าถึงได้
6. เมื่อมีการเผยแพร่ชุดข้อมูล ต้องเผยแพร่ Metadata ของข้อมูลดังกล่าวไปพร้อมกันด้วย
7. Metadata ต้องถูกต้อง เป็นปัจจุบัน และสอดคล้องกับชุดข้อมูลตลอดเวลา
8. ต้องมีการกำหนดกระบวนการในการจัดทำ Metadata
9. การเปลี่ยนแปลง Metadata ต้องเป็นการกระทำร่วมกันระหว่างเจ้าของข้อมูล และบริกรข้อมูล ทั้งนี้หากมีผู้มีส่วนได้ส่วนเสียอื่นที่เกี่ยวข้อง ต้องเชิญบุคคลดังกล่าวมาเข้าร่วมการตัดสินใจด้วย
10. เมื่อมีการเปลี่ยนแปลง Metadata ต้องระบุผู้ดำเนินการเปลี่ยนแปลง ผู้อนุมัติการเปลี่ยนแปลง และวันที่ที่ทำการเปลี่ยนแปลง
11. กำหนดให้มีการจัดทำรายงานการตรวจสอบตามคำร้อง และมีการ จัดทำรายงานแนวทางกำกับและการปฏิบัติด้าน

ภาคผนวก ค.

นโยบายการบริหารจัดการข้อมูล (Data Management Policy)

2568

EEC
เขตพัฒนาพิเศษภาคตะวันออก
เชื่อมโลก ให้ไทยแล่น
สำนักงานคณะกรรมการนโยบายเขตพัฒนาพิเศษภาคตะวันออก

นโยบายการบริหารจัดการข้อมูล (Data Management Policy)

รุ่นเอกสาร 1
ณ วันที่ 3 มีนาคม 2568

สำนักบริการผู้ลงทุน
สายงานเขตส่งเสริมเศรษฐกิจพิเศษ
สำนักงานคณะกรรมการนโยบายเขตพัฒนาพิเศษภาคตะวันออก (สกพอ.)

สารบัญ

นโยบายการบริหารจัดการข้อมูล
(Data Management Policy)
สำนักงานคณะกรรมการนโยบายเขตพัฒนาพิเศษภาคตะวันออก (สกพอ.)

เวอร์ชัน	ผู้อนุมัติ	วันที่อนุมัติ	วันที่มีผลบังคับใช้	การปรับปรุงครั้งถัดไป
1.0	เลขาธิการ สกพอ.	3 มี.ค. 2568	3 มี.ค. 2568	พ.ศ. 2569

1. วัตถุประสงค์

1) เพื่อให้การบริหารจัดการข้อมูลของ สกพอ. สอดคล้องกับกฎหมาย กรอบธรรมาภิบาลข้อมูลภาครัฐ และระเบียบปฏิบัติที่เกี่ยวข้อง

2) เพื่อใช้เป็นกรอบและแนวทางในการบริหารจัดการข้อมูลของ สกพอ. สำหรับผู้บริหาร เจ้าหน้าที่ สกพอ. และผู้ที่เกี่ยวข้อง

2. ขอบเขตและการบังคับใช้

นโยบายการบริหารจัดการข้อมูลฉบับนี้จัดทำโดยคณะบริกรข้อมูลของ สกพอ. มีผลบังคับใช้กับข้อมูลทั้งหมดที่อยู่ในความรับผิดชอบของ สกพอ. โดยผู้ทำหน้าที่ดูแลข้อมูล ผู้ใช้ข้อมูล คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Committee) คณะทำงาน บริกรข้อมูล (Data Stewards) และบุคลากรอื่น ๆ ของ สกพอ. มีหน้าที่โดยตรงที่จะต้องสนับสนุน ดำเนินการและปฏิบัติตามนโยบายอย่างเคร่งครัด ผู้ใช้อื่นที่เกี่ยวข้องแต่ไม่มีหน้าที่ในการดูแลข้อมูลจะต้องให้ความร่วมมือในการดำเนินการตามนโยบายนี้ ผู้ฝ่าฝืนนโยบายนี้มีความผิดและจะต้องได้รับการดำเนินการตามระเบียบของ สกพอ.

3. ข้อยกเว้น

นโยบายนี้อาจมีการขยายผลหรือมีการยกเว้นโดยปฏิบัติตามขั้นตอนการยกเว้นนโยบายของรัฐด้านอื่น ๆ หรือนโยบายของ สกพอ. ร่วมด้วย

4. บทบาทและความรับผิดชอบ

1) ผู้บริหารเทคโนโลยีสารสนเทศหรือผู้ที่ได้รับมอบหมายต้องควบคุมและกำกับดูแลให้บุคลากรใน สกพอ. และผู้ที่เกี่ยวข้องดำเนินการตามนโยบายการบริหารจัดการข้อมูลอย่างเคร่งครัด

2) ผู้บริหารเทคโนโลยีสารสนเทศหรือผู้ที่ได้รับมอบหมายต้องตรวจสอบให้แน่ใจว่าบุคลากรใน สกพอ. และบุคคลอื่น ๆ เช่น บริษัทหรือผู้รับจ้าง ที่ได้รับมอบหมายจาก สกพอ. ให้ทำหน้าที่บริหารจัดการข้อมูลได้รับความรู้เกี่ยวกับนโยบายนี้อย่างเหมาะสม และนำนโยบายไปปฏิบัติตามอย่างมีประสิทธิภาพและประสิทธิผล

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

4) คณะกรรมการธรรมาภิบาลข้อมูล/คณะทำงานด้านข้อมูล/เจ้าของข้อมูลและผู้ดูแลข้อมูล ต้องปฏิบัติหน้าที่ที่ได้รับมอบหมายภายใต้นโยบายนี้ *(รายละเอียดตามข้อ 9. ข้อมูลเพิ่มเติม)*

5. คำนิยาม

ข้อมูล (Data) หมายความว่า สิ่งที่สื่อความหมายให้รู้เรื่องราวข้อเท็จจริงหรือเรื่องอื่นใด ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเอง หรือโดยผ่านวิธีการใด ๆ และไม่ว่าจะได้จัดทำไว้ในรูปของเอกสารแฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ภาพถ่ายดาวเทียม ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ เครื่องมือตรวจวัด การสำรวจระยะไกล หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้

ชุดข้อมูล (Dataset) หมายความว่า การนำข้อมูลจากหลายแหล่งมารวบรวม เพื่อจัดเป็นชุดให้ตรงตามลักษณะโครงสร้างของข้อมูล หรือจากการใช้ประโยชน์ของข้อมูล

บัญชีข้อมูล (Data Catalog) หมายความว่า เอกสารแสดงบรรดารายการของชุดข้อมูล ที่จำแนกแยกแยะโดยการจัดกลุ่มหรือจัดประเภทข้อมูลที่อยู่ในความครอบครองหรือควบคุมของ สกพอ.

ธรรมาภิบาลข้อมูลภาครัฐ (Data Governance for Government) หมายความว่า การกำหนดสิทธิ หน้าที่และความรับผิดชอบของผู้มีส่วนได้เสียในการบริหารจัดการข้อมูลทุกขั้นตอน เพื่อให้การได้มาและการนำไปใช้ข้อมูลของ สกพอ. ภาครัฐถูกต้อง ครบถ้วน เป็นปัจจุบัน รักษาความเป็นส่วนตัวและสามารถเชื่อมโยงกันได้อย่างมีประสิทธิภาพและมั่นคงปลอดภัย

หมวดหมู่ของข้อมูล (Data Category) ตามกรอบธรรมาภิบาลข้อมูลภาครัฐแบ่งออกได้เป็น 4 หมวดหมู่ ได้แก่ ข้อมูลส่วนบุคคล ข้อมูลความมั่นคง ข้อมูลความลับทางราชการ และ ข้อมูลสาธารณะ

การจัดชั้นความลับของข้อมูล (Data Classification) หมายความว่า การกำหนดประเภทและข้อกำหนดของการจัดชั้นความลับของข้อมูล เพื่อกำหนดสิทธิในการเข้าถึงและสามารถนำข้อมูลไปใช้ได้อย่างเหมาะสม ซึ่งตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 กำหนดให้มีชั้นความลับเป็น ชั้นลับ ชั้นลับมาก หรือ ชั้นลับที่สุด โดยคำนึงถึงการปฏิบัติหน้าที่ของ สกพอ. และประโยชน์แห่งรัฐประกอบกัน ดังนั้น ชั้นความลับของข้อมูลมักถูกกำหนดให้สอดคล้องกับผลกระทบต่อหน่วยงานและความมั่นคงของประเทศ อาทิ ชื่อเสียง ความต่อเนื่องของการดำเนินงาน การเงิน และทรัพยากรบุคคล

วงจรชีวิตของข้อมูล (Data Life Cycle) หมายความว่า ลำดับขั้นตอนของข้อมูลตั้งแต่เริ่มสร้างข้อมูลไปจนถึงการทำลายข้อมูล ตามกรอบธรรมาภิบาลข้อมูลภาครัฐ

ข้อมูลหลักและข้อมูลอ้างอิง (Master and Reference Data) หมายความว่า การบริหารจัดการข้อมูลเพื่อให้ทั้งหน่วยงานสามารถเข้าถึงและใช้ข้อมูลร่วมกันได้ โดยข้อมูลถูกจัดเก็บไว้แหล่งเดียว มีการกำหนดมาตรฐานของข้อมูล เพื่อช่วยลดความซ้ำซ้อนของข้อมูลและทำให้ข้อมูลมีคุณภาพ ซึ่ง Master data เป็นข้อมูลที่สร้างและถูกใช้งานอยู่ภายใน สกพอ. มีโอกาสเปลี่ยนแปลงได้และมีรายละเอียดหรือจำนวนฟิลด์ข้อมูลที่มาก เช่น ข้อมูลพนักงาน ข้อมูลลูกค้า ข้อมูลผู้ขาย ข้อมูลสินค้าและบริการ ข้อมูลครุภัณฑ์ และข้อมูลสถานที่ ในขณะที่ Reference data มีความเป็นสากลถูกสร้างและใช้งานโดยทั่วไป โดยหลากหลายองค์กร หรือแม้กระทั่งใช้งานไปทั่วโลก เช่น รหัสไปรษณีย์ รหัสประเทศ หน่วยวัดระยะทาง

6. นโยบายการบริหารจัดการข้อมูล

ข้อกำหนดทั่วไป

1) กำหนดบทบาท หน้าที่ และความรับผิดชอบของแต่ละบุคคลตามโครงสร้างธรรมาภิบาลข้อมูลภาครัฐ โดยต้องได้รับการมอบอำนาจและการอนุมัติจากผู้บริหารเทคโนโลยีสารสนเทศ พร้อมทั้งกำหนดหน่วยงานเจ้าของข้อมูล เพื่อทำหน้าที่ในการบริหารจัดการข้อมูลนั้น ๆ

2) จัดทำนโยบายการบริหารจัดการข้อมูลเป็นลายลักษณ์อักษร อนุมัติเผยแพร่เพื่อประกาศใช้ และถือปฏิบัติ โดยให้มีผลบังคับใช้กับบุคลากรใน สกพอ. ตลอดจนหน่วยงาน/บุคคลภายนอกที่เกี่ยวข้องกับการได้มาและการใช้ข้อมูลของ สกพอ. พร้อมทั้งจัดทำแนวปฏิบัติและมาตรฐานที่เกี่ยวกับข้อมูลเพื่อสนับสนุนการปฏิบัติงานให้สอดคล้องตามนโยบายดังกล่าว

3) กำหนดมาตรการ วิธีการ และแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของข้อมูล เพื่อป้องกันการละเมิด การเข้าถึง การสูญหาย การทำลาย หรือการเปลี่ยนแปลงข้อมูล โดยปราศจากอำนาจโดยมิชอบหรือโดยมิได้รับอนุญาต *(อ้างอิงตามนโยบายความมั่นคงปลอดภัยสารสนเทศของ สกพอ.)*

4) กำหนดมาตรการ วิธีการ และแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลที่สอดคล้องกับกฎหมายระเบียบ และแนวปฏิบัติของ สกพอ. *(อ้างอิงตามนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) สกพอ. และเป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562)*

5) ตรวจสอบความมีอยู่และรายละเอียดของข้อมูลที่สำคัญ เช่น คำอธิบายข้อมูลหรือเมทาดาตา ชุดข้อมูล การจัดชั้นความลับข้อมูล และรายงานผลให้แก่ผู้รับผิดชอบตามโครงสร้างธรรมาภิบาลข้อมูลภาครัฐและดำเนินการตามกระบวนการธรรมาภิบาลข้อมูลภาครัฐ

6) ตรวจสอบ ติดตาม และประเมินผลการปฏิบัติตามนโยบายการบริหารจัดการข้อมูลโดยผู้ตรวจประเมินที่คณะกรรมการธรรมภิบาลข้อมูลของ สกพอ. กำหนด พร้อมทั้งกำหนดให้มีการทบทวนนโยบาย รวมถึงมาตรการ วิธีการ และแนวปฏิบัติต่าง ๆ เกี่ยวกับข้อมูล อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญตามความเหมาะสม

7) ตรวจสอบ ติดตาม และประเมินผลการดำเนินงานธรรมาภิบาลข้อมูลของ สกพอ. อย่างน้อยปีละ 1 ครั้ง ในเรื่อง (1) การประเมินความพร้อมธรรมาภิบาลข้อมูล (2) การประเมินคุณภาพข้อมูล และ (3) การประเมินความมั่นคงปลอดภัยของข้อมูล เป็นอย่างน้อย *(อ้างอิงตามมาตรฐานและหลักเกณฑ์ที่สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) กำหนด)*

8) จัดให้มีทรัพยากรด้านงบประมาณ ทรัพยากรบุคคล และเทคโนโลยีที่เพียงพอต่อการบริหารจัดการข้อมูล พร้อมทั้งสนับสนุนการฝึกอบรมธรรมาภิบาลข้อมูลภาครัฐและการบริหารจัดการข้อมูลให้ครอบคลุมทั้งวงจรชีวิตของข้อมูลแก่บุคลากรใน สกพอ. อย่างน้อยปีละ 1 ครั้ง

การจัดหมวดหมู่และชั้นความลับของข้อมูล

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

2) ติดป้ายกำกับชุดข้อมูล (Labeling/Tagging Dataset) ตามผลประเมินและระบุหมวดหมู่และประเภทชั้นความลับอย่างเหมาะสม และป้ายกำกับสำรองชั้นความลับข้อมูล (ถ้ามี) เช่น ลับ ลับมาก ลับที่สุด เป็นต้น เพื่อจำแนกความแตกต่างของชุดข้อมูลภายใน สกพอ. หรือแนวปฏิบัติตามข้อกำหนดอื่น ๆ

3) กำกับดูแลและติดตามอย่างต่อเนื่อง โดยตรวจสอบความปลอดภัยการใช้งานและรูปแบบการเข้าถึงของระบบและข้อมูล ทั้งผ่านกระบวนการอัตโนมัติหรือโดยบุคคล เพื่อระบุภัยคุกคามภายนอก การบำรุงรักษาการทำงานของระบบตามปกติ และการติดตั้งโปรแกรมเพื่อปรับปรุงและติดตามการเปลี่ยนแปลงของสภาพแวดล้อมของระบบและข้อมูล

4) แนวทางอื่น ๆ ตามที่หน่วยงานกำหนดเพิ่มเติม

การบริหารจัดการข้อมูลตามวงจรชีวิตของข้อมูล

1) กำหนดนโยบาย แนวปฏิบัติ และสภาพแวดล้อมการบริหารจัดการข้อมูลตามวงจรชีวิตของข้อมูลที่เอื้อต่อการรักษาความมั่นคงปลอดภัย คุ้มครองความเป็นส่วนตัวของข้อมูล และเพื่อให้ได้ข้อมูลที่มีคุณภาพ

2) จัดทำแนวปฏิบัติการจัดการชุดข้อมูล รวมถึงการรักษาความปลอดภัยตามหมวดหมู่และประเภทชั้นความลับตามแนวทางที่เหมาะสม และปรับปรุงอย่างต่อเนื่องให้สอดคล้องกับสถานการณ์

3) จัดเก็บข้อมูลให้สอดคล้องกับแนวทางหรือมาตรฐานการจัดชั้นความลับของข้อมูลที่กำหนดไว้ โดยข้อมูลต้องมีความถูกต้อง สมบูรณ์ และเป็นปัจจุบัน พร้อมทั้งกำหนดสิทธิและจัดหาระบบ/เครื่องมือที่ใช้ในการเข้าถึงข้อมูลเพื่อรักษาความมั่นคงปลอดภัยและคุณภาพข้อมูล และทำลายข้อมูลตามแนวปฏิบัติและกฎหมายที่เกี่ยวข้อง

4) จัดทำแนวปฏิบัติและมาตรฐานการประมวลผลและใช้ข้อมูล เพื่อผู้ใช้นำข้อมูลไปใช้อย่างถูกต้องตามวัตถุประสงค์ที่ต้องการเพื่อให้เกิดประโยชน์สูงสุด

5) ห้ามเปิดเผยข้อมูลที่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง นโยบาย และแนวปฏิบัติ ไม่ว่าข้อมูลจะอยู่ในรูปแบบใดหรือสถานที่ใดก็ตาม และต้องได้รับการอนุญาตจากตัวแทนหน่วยงานหรือเจ้าของข้อมูลก่อนการเปิดเผยข้อมูล รวมทั้งจัดให้มีช่องทางการเปิดเผยข้อมูลที่เข้าถึงและนำไปใช้ได้ง่าย

6) กำหนดกระบวนการ เทคโนโลยี และมาตรฐานทางเทคนิคที่ใช้ในการแลกเปลี่ยนข้อมูล และจัดทำสัญญาอนุญาตหรือข้อตกลงในการแลกเปลี่ยนข้อมูลและการนำข้อมูลไปใช้

7) จัดทำแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัย ด้านคุณภาพข้อมูล และด้านคุ้มครองความเป็นส่วนตัวของข้อมูล รวมถึงแนวปฏิบัติให้กับผู้ประสานงานหรือศูนย์ติดต่อ (Contact Center) และตรวจสอบให้แน่ใจว่าได้บริหารจัดการข้อมูลอย่างเหมาะสมตามแนวทางหรือแนวปฏิบัติที่กำหนดไว้

8) สร้างความรู้ความเข้าใจในการบริหารจัดการข้อมูลตามวงจรชีวิตของข้อมูล ให้แก่ผู้เกี่ยวข้องทั้งภายในและภายนอก สกพอ.

9) แนวทางอื่น ๆ ตามที่หน่วยงานกำหนดเพิ่มเติม

คุณภาพข้อมูล

1) กำหนดนโยบายการจัดการคุณภาพข้อมูล เพื่อใช้เป็นกรอบแนวทางในการจัดการข้อมูลของ สกพอ. ให้มีคุณภาพเป็นตามเกณฑ์หรือคุณสมบัติที่กำหนด เช่น ความถูกต้องสมบูรณ์ ความสอดคล้องกัน (Consistency) ความเป็นปัจจุบัน ตรงตามความต้องการใช้งาน และความพร้อมใช้ เป็นต้น โดยผู้ดูแลข้อมูลมีหน้าที่จัดการและกำกับดูแลข้อมูลให้มีคุณภาพเพื่อสร้างความมั่นใจให้กับผู้ใช้ข้อมูล ในขณะที่ผู้ใช้ข้อมูลมีบทบาทในการให้ข้อเสนอแนะแก่ผู้ดูแลข้อมูลเพื่อการปรับปรุงคุณภาพให้ดียิ่งขึ้น

2) จัดทำเกณฑ์คุณภาพข้อมูลที่สามารถวัดผลได้ พร้อมทั้งจัดทำแผนพัฒนาคุณภาพข้อมูลที่สามารถระบุตัวชี้วัดคุณภาพและแผนปฏิบัติการเพื่อจัดการคุณภาพข้อมูลได้อย่างมีประสิทธิภาพ โดยออกแบบการเก็บรวบรวมข้อมูลเพื่อให้ได้ข้อมูลสำหรับประเมินคุณภาพตามเกณฑ์ดังกล่าวให้รวมอยู่ในระบบเทคโนโลยีสารสนเทศและกระบวนการทำงาน (Quality by design) เพื่อลดข้อผิดพลาดและปรับปรุงคุณภาพตั้งแต่จุดการป้อนข้อมูลหรือการสร้างข้อมูลไปจนถึงการประมวลผลข้อมูล *(อ้างอิงตามมาตรฐานและหลักเกณฑ์ที่สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) กำหนด)*

3) ประเมินผลและจัดการคุณภาพข้อมูลอย่างสม่ำเสมอตลอดวงจรชีวิตของข้อมูล โดยเจ้าของข้อมูลและบริกรข้อมูลควรกำหนดกรอบคุณภาพข้อมูลเฉพาะหมวดหมู่ข้อมูลหรือโดเมน (Domain) *(อ้างอิงตามมาตรฐานและหลักเกณฑ์ที่สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) กำหนด)*

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

5) แนวทางอื่น ๆ ตามที่หน่วยงานกำหนดเพิ่มเติม

7. ข้อกฎหมายและเอกสารอ้างอิง

1) ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม

2) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

3) ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ

4) ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง มาตรฐานและหลักเกณฑ์การเปิดเผยข้อมูลเปิดภาครัฐในรูปแบบข้อมูลดิจิทัลต่อสาธารณะ

5) ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง มาตรฐานรัฐบาลดิจิทัลว่าด้วยแนวทางการจัดทำบัญชีข้อมูลภาครัฐ (มรด. 3-1:2565)

6) ประกาศสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ที่ 4/2564 เรื่อง นโยบายความมั่นคงปลอดภัยสารสนเทศของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

7) ชุดเอกสารแม่แบบ (template) สำหรับการดำเนินการของผู้ควบคุมข้อมูลส่วนบุคคลภาครัฐ (Version 1.0) จัดทำโดย สพร.

8. ประวัติการแก้ไขเอกสาร

เวอร์ชัน	ผู้จัดทำ	ผู้อนุมัติ	วันที่แก้ไขข้อมูล	รายละเอียดแก้ไข
1.0	[ใส่ชื่อผู้จัดทำ]	[ใส่ชื่อผู้อนุมัติ]	XX เดือน ปี พ.ศ.	เวอร์ชันเริ่มต้น

9. ข้อมูลเพิ่มเติม

1) ตัวอย่างการกำหนดบทบาทและความรับผิดชอบของผู้มีส่วนเกี่ยวข้อง

บทบาท	ความรับผิดชอบ
คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Committee)	• กำหนดกรอบธรรมาภิบาลข้อมูล (Data Governance) เพื่อจัดทำนโยบายข้อมูล (Data Policy) รวมถึงแนวปฏิบัติ มาตรฐาน และแผนการดำเนินงานด้านธรรมภิบาลข้อมูลภาครัฐของ สกพอ. ให้สอดคล้องกับประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ ลงวันที่ 12 มีนาคม 2563 • ส่งเสริมและสนับสนุนการดำเนินการตามนโยบายและแผนการดำเนินงานด้านธรรมาภิบาลข้อมูลตาม (1) เพื่อให้สามารถดำเนินการไปได้อย่างลุล่วง โดยจัดให้มีกลไกการตรวจสอบ วัดผล และรายงาน ตลอดจนการปรับปรุงอย่างต่อเนื่อง • กำกับดูแลการดำเนินการธรรมาภิบาลข้อมูล เพื่อให้ข้อมูลของ สกพอ. มีความถูกต้อง ครบถ้วน เป็นปัจจุบัน มีความมั่นคงปลอดภัย และข้อมูลส่วนบุคคลได้รับการคุ้มครองอย่างเหมาะสม • กำกับดูแลการดำเนินการเกี่ยวกับข้อมูลของ สกพอ. เพื่อให้เป็นไปตามกฎหมายว่าด้วยข้อมูลข่าวสารของราชการ กฎหมายว่าด้วยคุ้มครองข้อมูล

บทบาท	ความรับผิดชอบ
	ส่วนบุคคล กฎหมายว่าด้วยการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล และกฎหมายอื่น ๆ ที่เกี่ยวข้อง ● (5) เสนอแนะต่อเลขาธิการแต่งตั้งคณะทำงาน เพื่อสนับสนุนการดำเนินการธรรมาภิบาลข้อมูล คณะบริกรข้อมูล (Data Steard Team) และการปฏิบัติตามข้อกำหนดของกฎหมายที่เกี่ยวข้องตามความเหมาะสม
บริกรข้อมูลด้านธุรกิจ (Business Data Stewards)	● นิยามความต้องการด้านคุณภาพและความมั่นคงปลอดภัย ● นิยามเมทาดาตา ● ร่างนโยบายข้อมูล มาตรฐาน และแนวปฏิบัติต่าง ๆ ที่เกี่ยวข้องกับข้อมูล ● ตรวจสอบการปฏิบัติตามนโยบายข้อมูล ตรวจสอบคุณภาพ ตรวจสอบความมั่นคงปลอดภัยของข้อมูล วิเคราะห์ผลจากการตรวจสอบ
บริกรข้อมูลด้านเทคนิค (Technical Data Stewards)	● ให้การสนับสนุนด้านเทคโนโลยีสารสนเทศแก่บริกรข้อมูล ● รักษา และดูแลข้อมูลที่อยู่บนระบบเทคโนโลยีสารสนเทศต่าง ๆ ในหน่วยงาน
บริกรข้อมูลด้านคุณภาพข้อมูล (Data Quality Stewards)	● ดำเนินการในเรื่องคุณภาพข้อมูล เช่น กำหนดนโยบายข้อมูลด้านคุณภาพ การตรวจวัดคุณภาพข้อมูล และการวิเคราะห์คุณภาพข้อมูล
ทีมบริหารจัดการข้อมูล (Data Management Team)	● บริหารจัดการข้อมูลให้เป็นไปตามองค์ประกอบในการบริหารจัดการข้อมูล *(เจ้าหน้าที่ภายในสำนักเทคโนโลยีสารสนเทศของ สกพอ.)*
เจ้าของข้อมูล (Data Owner)	● ตรวจสอบ ดูแล และรักษาคุณภาพของข้อมูล ● ทบทวนและอนุมัติการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับข้อมูล
ผู้สร้างข้อมูล (Data Creator)	● บันทึก แก้ไข ปรับปรุง หรือลบข้อมูลให้สอดคล้องกับโครงสร้างที่ถูกกำหนดไว้ ● ทำงานร่วมกับบริกรข้อมูล เพื่อตรวจสอบและแก้ไขปัญหาด้านคุณภาพข้อมูล และความปลอดภัยของข้อมูล
ผู้บริหารจัดการฐานข้อมูล (Database Administrator)	● บริหารจัดการ และควบคุมเกี่ยวกับระบบฐานข้อมูลภายในหน่วยงาน ● กำหนดนโยบาย มาตรการ และมาตรฐานของระบบฐานข้อมูล ทั้งหมดภายในหน่วยงาน เช่น รายละเอียดและวิธีการจัดเก็บข้อมูล การใช้งานฐานข้อมูล การรักษาความปลอดภัยของข้อมูล การสำรองข้อมูล การกู้คืนข้อมูล เป็นต้น
ผู้ใช้ข้อมูล (Data User)	● นำข้อมูลไปใช้งานทั้งในระดับปฏิบัติงานและระดับบริหาร ● สนับสนุนการกำกับดูแลข้อมูล ● รายงานประเด็นปัญหาที่พบระหว่างการใช้ข้อมูล ทั้งด้านคุณภาพ และความปลอดภัยของข้อมูล

2) ตัวอย่างความสัมพันธ์ระหว่างกระบวนการ/กิจกรรมและผู้มีส่วนได้ส่วนเสีย

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

หมายเหตุ

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

ภาคผนวก ง.

แนวปฏิบัติการบริหารจัดการข้อมูล (Data Management Guideline)

2568

EEC
เขตพัฒนาพิเศษภาคตะวันออก
เชื่อมโลก ให้ไทยแล่น
สำนักงานคณะกรรมการนโยบายเขตพัฒนาพิเศษภาคตะวันออก

แนวปฏิบัติการบริหารจัดการข้อมูล

(Data Management Guideline)

รุ่นเอกสาร 1

ณ วันที่ 6 พฤษภาคม 2568

สำนักเทคโนโลยีสารสนเทศ
สำนักงานคณะกรรมการนโยบายเขตพัฒนาพิเศษภาคตะวันออก (สกพอ.)

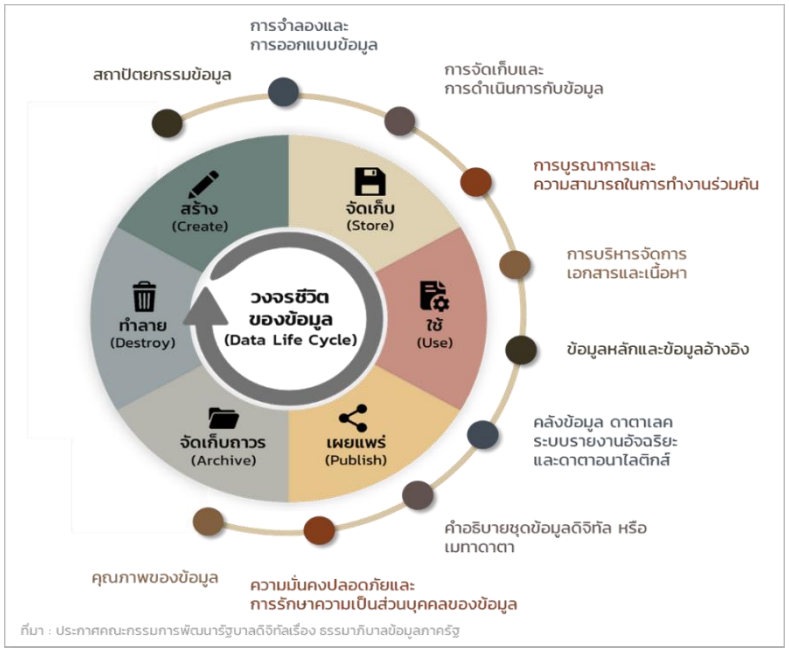
สารบัญ

บทนำ

แนวปฏิบัติการบริหารจัดการข้อมูลฉบับนี้จัดทำขึ้นโดย สกพอ. เพื่อกำหนดมาตรฐานและแนวทางปฏิบัติที่เป็นระบบในการบริหารจัดการข้อมูลขององค์กร ให้สอดคล้องกับหลักการธรรมาภิบาลข้อมูล (Data Governance) และกฎหมายที่เกี่ยวข้อง โดยมุ่งเน้นการใช้ประโยชน์จากข้อมูลอย่างมีประสิทธิภาพ รักษาความปลอดภัย และปกป้องสิทธิส่วนบุคคล

หลักการและขอบเขต

แนวปฏิบัติการบริหารจัดการข้อมูล ได้กำหนดขึ้นให้สอดคล้องตามนโยบายข้อมูล (Data Policy) ที่หน่วยงานประกาศ ซึ่งเป็นหนึ่งในองค์ประกอบตามกรอบธรรมาภิบาลข้อมูลภาครัฐ จัดทำโดยสำนักเทคโนโลยีสารสนเทศ มีผลบังคับใช้กับผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับข้อมูลตามแนวปฏิบัติที่ สกพอ. ประกาศ ซึ่งมีหน้าที่โดยตรงที่จะต้องสนับสนุน ดำเนินการและปฏิบัติตามอย่างเคร่งครัด และผู้ใช้อื่นที่เกี่ยวข้องแต่ไม่มีหน้าที่ในการดูแลข้อมูลจะต้องให้ความร่วมมือในการดำเนินการตามแนวปฏิบัตินี้ ผู้ฝ่าฝืนมีความผิดและจะต้องได้รับการดำเนินการตามระเบียบของหน่วยงาน โดยแนวปฏิบัติจะต้องครอบคลุมระบบบริหารและกระบวนการจัดการข้อมูล หรือวงจรชีวิตของข้อมูลและองค์ประกอบในการบริหารจัดการข้อมูล ดังรูปต่อไปนี้



ที่มา : ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัลเรื่อง ธรรมาภิบาลข้อมูลภาครัฐ

วงจรชีวิตของข้อมูล

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

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

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

หมวดหมู่และการจัดระดับชั้นของข้อมูล

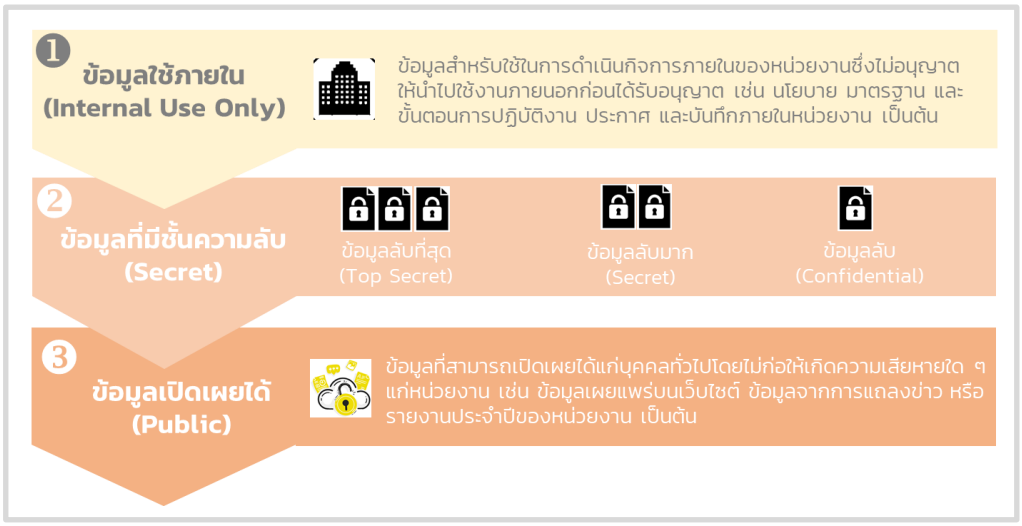
ข้อมูลของหน่วยงานสามารถแบ่งหมวดหมู่ตามกรอบธรรมาภิบาลข้อมูลและการใช้งานภายในหน่วยงาน ดังนี้

1. ข้อมูลสาธารณะ
2. ข้อมูลส่วนบุคคล
3. ข้อมูลความมั่นคง
4. ข้อมูลความลับทางราชการ
5. ข้อมูลใช้ภายในหน่วยงาน (ที่ยังไม่แบ่งหมวดหมู่)

โดยมีการจัดระดับชั้นความลับของข้อมูล ดังนี้

- ข้อมูลใช้ภายใน (Internal Use Only) ได้แก่ ข้อมูลสำหรับใช้ในการดำเนินกิจการภายในของหน่วยงานซึ่งไม่อนุญาตให้นำไปใช้งานภายนอกก่อนได้รับอนุญาต เช่น นโยบาย มาตรฐาน และขั้นตอนการปฏิบัติงาน ประกาศ และบันทึกภายในหน่วยงาน เป็นต้น
- ข้อมูลที่มีชั้นความลับ (Secret) แบ่งเป็น ข้อมูลลับที่สุด (Top Secret) ข้อมูลลับมาก (Secret) และข้อมูลลับ (Confidential)

- ข้อมูลเปิดเผยได้ (Public) ได้แก่ ข้อมูลที่สามารถเปิดเผยได้แก่บุคคลทั่วไป เช่น ข้อมูลเผยแพร่บนเว็บไซต์ ข้อมูลจากการแถลงข่าว หรือรายงานประจำปีของหน่วยงาน เป็นต้น

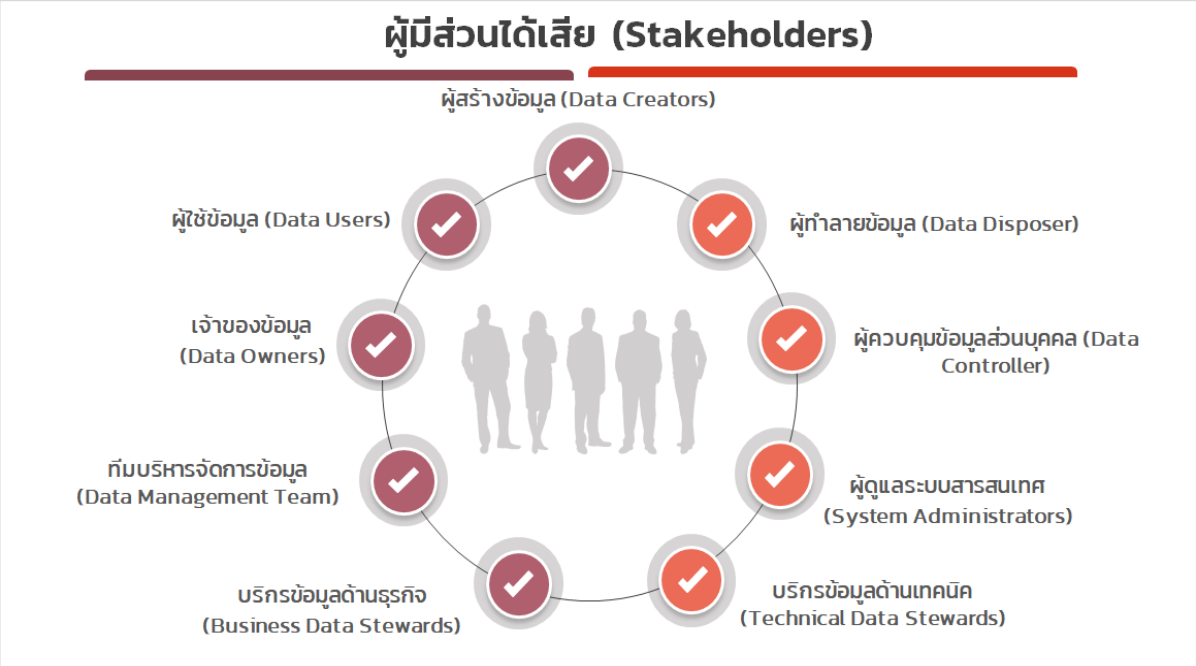


ผู้เกี่ยวข้อง

ทั้งนี้แนวปฏิบัติเกี่ยวกับข้อมูลนี้บังคับใช้กับผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับข้อมูลตามประกาศแนวปฏิบัติการกำกับดูแลและบริหารจัดการข้อมูลของหน่วยงาน รวมถึงผู้เกี่ยวข้องอื่น ๆ ที่ไม่ได้ระบุไว้ในแนวปฏิบัติ ดังนี้

- ผู้สร้างข้อมูล (Data Creators)
- ผู้ใช้ข้อมูล (Data Users)
- เจ้าของข้อมูล (Data Owners)
- ทีมบริหารจัดการข้อมูล (Data Management Team)
- บริกรข้อมูลด้านธุรกิจ (Business Data Stewards)
- บริกรข้อมูลด้านเทคนิค (Technical Data Stewards)
- ผู้ดูแลระบบสารสนเทศ (System Administrators)
- ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)

- ผู้ทำลายข้อมูล (Data Disposer)



คำนิยาม

คำศัพท์	ความหมาย
สำนักงาน / กรม	สำนักงานคณะกรรมการนโยบายเขตพัฒนาพิเศษภาคตะวันออก (สกพอ.)
คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Committee)	ประกอบไปด้วย ผู้บริหารระดับสูงสุดของ สกพอ. (Chief Executive Officer) ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer) ผู้บริหารข้อมูลระดับสูง (Chief Data Officer) ผู้บริหารด้านการรักษาความปลอดภัยระดับสูง (Chief Security Officer) ผู้บริหารจากส่วนงานต่าง ๆ ทั้งจากฝ่ายบริหารและฝ่ายเทคโนโลยีสารสนเทศ รวมไปถึงหัวหน้าทีม บริกรข้อมูล (Lead Data Steward) คณะกรรมการธรรมาภิบาลข้อมูลมีอำนาจสูงสุดในธรรมาภิบาลข้อมูลภายใน สกพอ. หรือ คณะกรรมการ/คณะทำงาน ซึ่งทำหน้าที่ตัดสินใจเชิงนโยบาย แก้ไขปัญหา และบริหารจัดการข้อมูลของ สกพอ. ทั้งนี้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงอาจจะทำหน้าที่แทนผู้บริหารข้อมูลระดับสูง
หัวหน้าหน่วยงานของรัฐ	เลขาธิการคณะกรรมการนโยบายเขตพัฒนาพิเศษภาคตะวันออก
ผู้บริหาร	ผู้บริหารที่เกี่ยวข้องกับการบริหารจัดการข้อมูล ตามคณะกรรมการ/คณะทำงานที่เกี่ยวข้อง
เจ้าหน้าที่/พนักงาน	บุคคลผู้ที่ สกพอ. บรรจุและแต่งตั้งเป็นเจ้าหน้าที่ของหน่วยงาน
ลูกจ้าง	บุคคลผู้ที่ สกพอ. บรรจุและแต่งตั้งเป็นลูกจ้าง โดยมีสัญญาจ้างให้ปฏิบัติงานเป็นการชั่วคราวและมีกำหนดระยะเวลาและสิ้นสุดที่แน่นอน
ผู้บังคับบัญชา	ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของสำนักงาน
ผู้สร้างข้อมูล (Data Creators)	บุคลากรของทุก สำนัก/กลุ่มงาน ที่ทำหน้าที่บันทึก แก้ไข ปรับปรุง หรือลบข้อมูลให้สอดคล้องกับโครงสร้างที่ถูกกำหนดไว้
ผู้ใช้ข้อมูล (Data Users)	คณะกรรมการ ผู้อำนวยการ เจ้าหน้าที่/พนักงาน ลูกจ้าง รวมถึงหน่วยงานภายนอกที่ได้รับอนุญาต (Authorized Users) ให้สามารถเข้ามาใช้ข้อมูลของ สกพอ. ตามสิทธิและหน้าที่ความรับผิดชอบ พร้อมทั้งรายงานประเด็นปัญหาที่พบระหว่างการใช้ข้อมูล
สิทธิของผู้ใช้งานข้อมูล	สิทธิและหน้าที่ตามบทบาท (Role) ที่เกี่ยวข้องกับข้อมูลและระบบสารสนเทศของ สกพอ. มีดังนี้ - สิทธิใช้งานทั่วไป หมายถึง คณะกรรมการ ผู้อำนวยการ ข้าราชการ/เจ้าหน้าที่/พนักงาน ลูกจ้าง ที่ใช้งานระบบสารสนเทศพื้นฐานของสำนักงาน ผู้ใช้งานข้อมูลต้องขออนุญาตจาก ผู้บังคับบัญชา โดยให้ใช้แบบฟอร์มเพื่อขออนุมัติตามที่ สกพอ. กำหนด - สิทธิจำเพาะ หมายถึง สิทธิเฉพาะตามหน้าที่ความรับผิดชอบที่เกี่ยวข้องกับการปฏิบัติงาน ผู้ใช้งานข้อมูลต้องได้รับสิทธิจากผู้บังคับบัญชา - สิทธิพิเศษ หมายถึง สิทธิที่ได้รับมอบหมายเพิ่มเติมจากผู้บังคับบัญชาเป็นกรณีพิเศษ ผู้ใช้งานต้องได้รับมอบหมายจากผู้บังคับบัญชาเป็นครั้งคราว
เจ้าของข้อมูล (Data Owner)	ผู้ที่ได้รับมอบหมายในการปฏิบัติงานให้รับผิดชอบข้อมูลที่ระบุไว้ ซึ่งรวมถึงผู้บังคับบัญชาของเจ้าของข้อมูลนั้นด้วย โดยทำหน้าที่กำกับดูแลตามธรรมาภิบาลข้อมูลตลอดวงจรชีวิตของข้อมูลนั้นๆ รวมทั้งทำหน้าที่กำหนดสิทธิในการเข้าถึงข้อมูลและจัดชั้นความลับของข้อมูล
เจ้าของข้อมูลส่วนบุคคล (Data Subject)	บุคคลธรรมดาที่ข้อมูลส่วนบุคคลเกี่ยวกับบุคคลนั้นระบุถึง

คำศัพท์	ความหมาย
เจ้าของระบบงาน (System Owner)	ผู้ที่มีหน้าที่รับผิดชอบในการใช้งาน ดูแลและบำรุงรักษา หรือปรับปรุงระบบงานที่ใช้ใน สกพอ.
ทีมบริหารจัดการข้อมูล (Data Management Team)	กลุ่มบุคคลภายในฝ่ายเทคโนโลยีสารสนเทศของ สกพอ. ที่ทำหน้าที่รับผิดชอบดูแลรักษาข้อมูลในระบบสารสนเทศของ สกพอ. และสนับสนุนกิจกรรมของธรรมาภิบาลข้อมูลภาครัฐ เช่น ช่วยเหลือในการนิยามเมทาดาตา ร่างนโยบายข้อมูลและมาตรฐานข้อมูล และกำหนดสิทธิการเข้าถึงข้อมูลโดย DBA เป็นต้น
บริกรข้อมูลด้านธุรกิจ (Business Data Stewards)	เจ้าหน้าที่ในสำนักเทคโนโลยีสารสนเทศที่ได้รับมอบหมายให้ทำหน้าที่ กำหนดนิยามความต้องการด้านคุณภาพและความมั่นคงปลอดภัยซึ่งอาจจะได้รับมาจากผู้ใช้ข้อมูล (Data Users) หรือผู้มีส่วนได้เสียอื่น ๆ นิยามคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตาโดยการสนับสนุนจากผู้ใช้ข้อมูล ร่างนโยบายข้อมูลด้วยการช่วยเหลือจากทีมบริหารจัดการข้อมูล (Data Management Team) ตรวจสอบการปฏิบัติตามนโยบายข้อมูล ตรวจสอบคุณภาพ ตรวจสอบความมั่นคงปลอดภัยของข้อมูล วิเคราะห์ผลจากการตรวจสอบ แล้วรายงานผลลัพธ์ไปยังคณะกรรมการธรรมาภิบาลข้อมูลและผู้ที่เกี่ยวข้องอื่น ๆ ให้ทราบ
บริกรข้อมูลด้านเทคนิค (Technical Data Stewards)	เจ้าหน้าที่ในสำนักเทคโนโลยีสารสนเทศที่ทำหน้าที่ให้การสนับสนุนด้านเทคโนโลยีสารสนเทศแก่บริกรข้อมูลด้านธุรกิจ เช่น นิยามเมทาดาตาเชิงเทคนิคซึ่งอาจจะได้รับการช่วยเหลือจากทีมบริหารจัดการข้อมูล ให้ข้อเสนอแนะเชิงเทคนิคในการร่างนโยบายข้อมูล ตรวจสอบคุณภาพข้อมูล ความมั่นคงปลอดภัยของข้อมูล และการปฏิบัติตามนโยบายข้อมูลในเชิงเทคนิค
ผู้ดูแลระบบสารสนเทศ (System Administrators)	เจ้าหน้าที่ในสำนักเทคโนโลยีสารสนเทศที่มีหน้าที่ดูแลรับผิดชอบระบบสารสนเทศของ สกพอ.
ผู้ดูแลระบบแม่ข่าย (Server Administrators)	บุคลากรที่มีหน้าที่ดูแลรับผิดชอบระบบแม่ข่ายของ สกพอ.
ผู้จัดการโครงการ (Project Managers)	เจ้าหน้าที่ของ สกพอ. หลักที่ได้รับมอบหมายบริหารจัดการโครงการตามแผนดำเนินงาน
ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)	บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจ เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
ผู้ทำลายข้อมูล (Data Disposer)	บุคลากรที่ได้รับการกำหนดสิทธิจากเจ้าของข้อมูลให้มีสิทธิในการทำลายข้อมูล
ข้อมูล (Data)	สิ่งที่สื่อความหมายให้รู้เรื่องราวข้อเท็จจริงหรือเรื่องอื่นใด ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเอง หรือโดยผ่านวิธีการใด ๆ และไม่ว่าจะได้จัดทำไว้ในรูปของเอกสารแฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ภาพถ่ายดาวเทียม ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ เครื่องมือตรวจวัด การสำรวจระยะไกล หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้
ข้อมูลดิจิทัล (Digital Data)	ข้อมูลที่ได้จัดทำ จัดเก็บ จำแนกหมวดหมู่ ประมวลผล ใช้ ปกปิด เปิดเผย ตรวจสอบ ทำลาย ด้วยเครื่องมือหรือวิธีการทางเทคโนโลยีดิจิทัล
ชุดข้อมูล (Dataset)	การนำข้อมูลจากหลายแหล่งมารวม เพื่อจัดเป็นชุดให้ตรงตามลักษณะโครงสร้างของข้อมูล

คำศัพท์	ความหมาย
สารสนเทศ (Information)	ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบข้อมูล ซึ่งอาจอยู่ในรูปของตัวเลข ข้อความหรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้งานสามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่นๆ
ระบบสารสนเทศ (Information System)	ระบบงานที่นำเทคโนโลยีมาช่วยในการสร้างสารสนเทศที่สามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งประกอบด้วยเทคโนโลยีคอมพิวเตอร์และเทคโนโลยีการสื่อสารโทรคมนาคม ได้แก่ ระบบคอมพิวเตอร์ (Computer System) ระบบเครือข่าย (Network System) ซอฟต์แวร์ (Software) ข้อมูล (Data) และสารสนเทศ (Information) เป็นต้น
อินทราเน็ต (Intranet)	เป็นระบบเครือข่ายที่สามารถเข้าถึงได้โดยผู้ใช้งานภายในสำนักงานเท่านั้น โดยมีจุดประสงค์เพื่อการติดต่อสื่อสาร แลกเปลี่ยนข้อมูลและสารสนเทศภายในสำนักงาน
การเข้าถึงและควบคุมการใช้งานข้อมูล	การเข้าถึงและการใช้งานข้อมูลทั้งทางอิเล็กทรอนิกส์หรือกายภาพ รวมทั้งการอนุญาต การกำหนดสิทธิในเข้าถึงและใช้งานข้อมูล การปรับปรุงข้อมูล การเพิกถอนหรือการยกเลิกสิทธิการเข้าถึงข้อมูล
การเข้าถึงและควบคุมการใช้งานระบบสารสนเทศ	การเข้าถึงและการใช้งานระบบสารสนเทศ รวมทั้งการตรวจสอบ การอนุมัติ การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ และการเพิกถอนหรือการยกเลิกสิทธิการเข้าถึงเครือข่ายหรือระบบสารสนเทศ
ทรัพย์สิน (Asset)	สิ่งที่มีคุณค่าหรือมูลค่าต่อหน่วยงานและเป็นทรัพย์สินที่เกี่ยวข้องกับการประมวลผลสารสนเทศที่ สกพอ. เป็นเจ้าของ เช่า ว่าจ้าง พัฒนา หรือจัดซื้อ โดยแบ่งแยกออกเป็นประเภทต่าง ๆ ได้แก่ สารสนเทศ (Information) ซอฟต์แวร์ (Software) ทรัพย์สินที่มีรูปร่าง (Physical Asset) บริการสาธารณูปโภคพื้นฐาน (Service) และบุคลากร (People)
ข้อมูลของหน่วยงาน	ข้อมูลที่อยู่ในความครอบครองหรือควบคุมดูแลของ สกพอ.
ข้อมูลสาธารณะ (Public Data)	ข้อมูลที่สามารถเปิดเผยได้ สามารถนำไปใช้ได้อย่างอิสระ ไม่ว่าจะเป็นข้อมูลข่าวสาร ข้อมูลส่วนบุคคล ข้อมูลอิเล็กทรอนิกส์ เป็นต้น
ข้อมูลส่วนบุคคล (Personal Data)	ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ (พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562)
ข้อมูลความมั่นคง (National Security Data)	ข้อมูลเกี่ยวกับความมั่นคงของรัฐ ที่ทำให้เกิดความสงบเรียบร้อย การมีเสถียรภาพความเป็นปึกแผ่น ปลอดภัยจากภัยคุกคาม เป็นต้น
ข้อมูลความลับทางราชการ (Confidential Government Data)	ข้อมูลที่อยู่ในความครอบครองหรือควบคุมดูแลของ สกพอ. ของรัฐที่มีคำสั่งไม่ให้มีการเปิดเผย และมีการกำหนดชั้นความลับของข้อมูล

คำศัพท์	ความหมาย
ข้อมูลลับ (Confidential)	ข้อมูลข่าวสารซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์ของรัฐซึ่งผู้ที่สามารถเข้าถึงได้ต้องเป็นบุคคลที่มีสิทธิเท่านั้นและห้ามเผยแพร่ต่อบุคคลภายนอกเว้นแต่จะได้รับอนุมัติเป็นลายลักษณ์อักษรโดย ผู้อำนวยการสำนักส่วนงานเจ้าของข้อมูล ขึ้นไปโดยต้องมีการลงนามในเอกสารข้อตกลงการไม่เปิดเผยข้อมูล (Non-Disclosure Agreement) เว้นแต่การเผยแพร่ดังกล่าวเป็นไปตามอำนาจที่กฎหมายให้การรับรอง
ข้อมูลลับมาก (Secret)	ข้อมูลข่าวสารซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรงซึ่งผู้ที่สามารถเข้าถึงได้ต้องเป็นบุคคลที่มีสิทธิเท่านั้นและห้ามเผยแพร่ต่อบุคคลภายนอก เว้นแต่จะได้รับอนุมัติเป็นลายลักษณ์อักษรโดย รองเลขาธิการ สกพอ. สายงาน ที่เป็นเจ้าของข้อมูลขึ้นไปโดยต้องมีการลงนามในเอกสารข้อตกลงการไม่เปิดเผยข้อมูล (Non-Disclosure Agreement) เว้นแต่การเผยแพร่ดังกล่าวเป็นไปตามอำนาจที่กฎหมายให้การรับรอง
ข้อมูลลับที่สุด (Top Secret)	ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรงที่สุดซึ่งผู้ที่สามารถเข้าถึงได้ต้องเป็นบุคคลที่มีสิทธิเท่านั้นและห้ามเผยแพร่ต่อบุคคลภายนอกเว้นแต่จะได้รับอนุมัติเป็นลายลักษณ์อักษรโดยรองเลขาธิการ สกพอ. สายงานขึ้นไป โดยต้องมีการลงนามในเอกสารข้อตกลงการไม่เปิดเผยข้อมูล (Non-Disclosure Agreement) เว้นแต่การเผยแพร่ดังกล่าวเป็นไปตามอำนาจที่กฎหมายให้การรับรอง
ข้อมูลใช้ภายใน (Internal Use Only)	ข้อมูลสำหรับใช้ในการดำเนินกิจการภายในของ สกพอ. ซึ่งไม่อนุญาตให้นำไปใช้งานภายนอกก่อนได้รับอนุญาต เช่น นโยบาย มาตรฐาน และขั้นตอนการปฏิบัติงาน ประกาศ และบันทึกภายใน สกพอ. เป็นต้น

การเผยแพร่และการทบทวน

แนวปฏิบัติเกี่ยวกับข้อมูลนี้จะต้องทำการเผยแพร่โดยการประกาศเวียนในระบบอินทราเน็ต ระบบ Sharepoint EECO Information เว็บไซต์ของ สกพอ. และจดหมายอิเล็กทรอนิกส์เพื่อให้เจ้าหน้าที่ทุกระดับในหน่วยงาน ได้รับทราบ และถือปฏิบัติตามแนวปฏิบัตินี้อย่างเคร่งครัด โดยแนวปฏิบัติที่จัดขึ้นนี้เมื่อเริ่มนำไปใช้ในระยะแรกสามารถทบทวนได้บ่อยครั้งเป็นรายไตรมาสเพื่อให้เหมาะสมกับบริบทการปฏิบัติงานจริง และจะต้องมีการทบทวนเป็นประจำอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ รวมถึงเมื่อมีข้อเสนอแนะคณะกรรมการธรรมาภิบาลข้อมูลเห็นสมควร

แนวปฏิบัติการบริหารจัดการข้อมูล

หมวด 1 การสร้างข้อมูล

วัตถุประสงค์

กำหนดแนวปฏิบัติสำหรับผู้ที่เกี่ยวข้องในการสร้างข้อมูลให้มีคุณภาพ มีความมั่นคงปลอดภัย และเป็นประโยชน์ต่อผู้ใช้ข้อมูล

ผู้รับผิดชอบงาน

1. ผู้สร้างข้อมูล (Data Creators)
2. ทีมบริหารจัดการข้อมูล (Data Management Team)
3. เจ้าของข้อมูล (Data Owners)
4. บริกรข้อมูล (Data Stewards)
5. ผู้ดูแลระบบสารสนเทศ (System Administrators)

อ้างอิง

1. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553
2. พระราชบัญญัติลิขสิทธิ์ (ฉบับที่ 2) พ.ศ. 2558
3. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560
4. พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562
5. ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ 2563

ข้อปฏิบัติ

1. เจ้าของข้อมูล
   1.1. กำหนดผู้มีสิทธิในการสร้างข้อมูล และจะต้องทบทวนสิทธินั้น อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ เช่น การลาออก เปลี่ยนตำแหน่ง โอนย้าย สิ้นสุดการจ้าง การปรับโครงสร้าง หรือเมื่อมีการปรับปรุงระบบสารสนเทศ เป็นต้น
   1.2. กำหนดหมวดหมู่และชั้นความลับของข้อมูล
2. ผู้ดูแลระบบสารสนเทศจะต้องกำหนดสิทธิในการสร้างข้อมูลในระบบให้แก่ผู้สร้างข้อมูลตามที่เจ้าของข้อมูลกำหนด
3. เจ้าของข้อมูล บริกรข้อมูลธุรกิจ บริกรข้อมูลเทคนิค และทีมบริหารจัดการข้อมูล ร่วมจัดทำคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตา (Metadata) เมื่อมีการสร้างชุดข้อมูล (Datasets) ตามมาตรฐานขั้นต่ำคำอธิบายชุดข้อมูลดิจิทัลที่สำนักงานพัฒนารัฐบาลดิจิทัล (สพร.) กำหนด และกำหนดให้ทำการประเมินคุณค่าของชุดข้อมูลดิจิทัลตามแบบฟอร์มประเมินคุณค่าชุดข้อมูลที่ สพร. หรือหน่วยงานกำหนด เพื่อสนับสนุนการคัดเลือกเป็นชุดข้อมูลคุณค่าสูง (High Value Dataset) และเผยแพร่เป็นข้อมูลเปิดของหน่วยงานต่อสาธารณะตามกฎหมายว่าด้วยข้อมูลข่าวสารของราชการในรูปแบบข้อมูลดิจิทัล
4. ห้ามมิให้ผู้สร้างข้อมูลนำข้อมูลที่มีลักษณะดังต่อไปนี้เข้าสู่ระบบคอมพิวเตอร์ที่ขัดต่อกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์
   - ข้อมูลที่บิดเบือน หรือปลอมไม่ว่าทั้งหมดหรือบางส่วน
   - ข้อมูลอันเป็นเท็จ ที่น่าจะเกิดความเสียหายต่อการรักษาความมั่นคงปลอดภัย ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจ หรือ โครงสร้างพื้นฐาน หรือ ก่อให้เกิดความตื่นตระหนก

- ข้อมูลอันเป็นความผิดเกี่ยวกับความมั่นคง หรือ ความผิดเกี่ยวกับการก่อการร้าย
- ข้อมูลที่มีลักษณะอันลามก และคนทั่วไปอาจเข้าถึงได้
- ข้อมูลที่ปรากฏภาพของผู้อื่น และเป็นภาพที่สร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ ทำให้ผู้อื่นเสียชื่อเสียง ถูกดูหมิ่นถูกเกลียดชัง หรือ ได้รับความอับอาย

5. ห้ามมิให้ผู้สร้างข้อมูล ทำการสร้าง/ทำซ้ำต่อข้อมูลที่ขัดต่อกฎหมายว่าด้วยลิขสิทธิ์หรือทรัพย์สินทางปัญญาของผู้อื่น เว้นแต่จะเป็นไปตามอำนาจที่กฎหมายรับรอง
6. กำหนดให้ผู้สร้างข้อมูลสร้างข้อมูลที่มาจากแหล่งข้อมูลที่เชื่อถือได้เท่านั้น
7. กำหนดให้เจ้าของข้อมูลตรวจสอบความถูกต้องของข้อมูลที่ถูกสร้างขึ้น

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

ตารางที่: 1 ตัวอย่างผู้มีส่วนได้ส่วนเสียในการสร้างข้อมูล

หมายเหตุ

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

หมวด 2 การจัดเก็บข้อมูล

วัตถุประสงค์

กำหนดแนวปฏิบัติสำหรับผู้ที่เกี่ยวข้องในการจัดเก็บข้อมูล ให้มีคุณภาพ เข้าถึงและใช้งานได้อย่างมั่นคงปลอดภัย

ผู้รับผิดชอบงาน

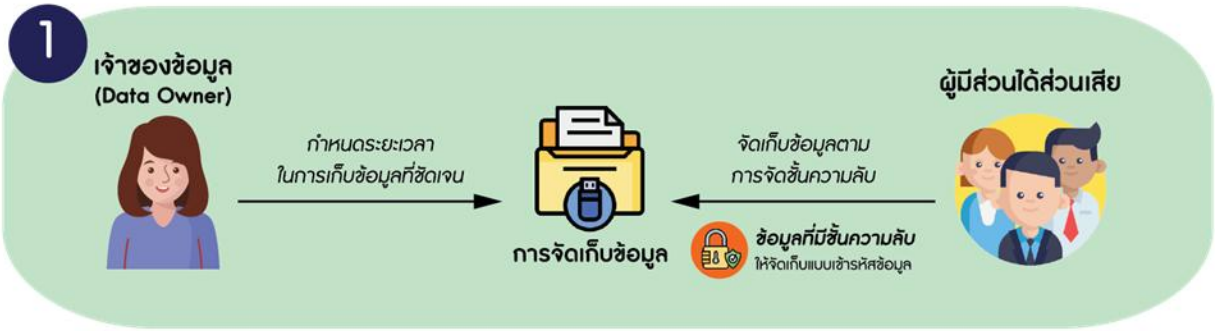
1. เจ้าของข้อมูล (Data Owners)
2. ผู้ดูแลระบบสารสนเทศ (System Administrators)
3. ผู้สร้างข้อมูล (Data Creators)
4. บริกรข้อมูล (Data Stewards)
5. ผู้ใช้ข้อมูล (Data Users)
6. ทีมบริหารจัดการข้อมูล (Data Management Team)

อ้างอิง

1. ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550
2. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553
3. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560
4. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
5. พระราชกำหนดว่าด้วยการประชุมผ่านสื่ออิเล็กทรอนิกส์ พ.ศ. 2563
6. ระเบียบสำนักนายกรัฐมนตรี ว่าด้วยงานสารบรรณ (ฉบับที่ 4) พ.ศ. 2564

ข้อปฏิบัติ

1. กำหนดให้เจ้าของข้อมูลจะต้องกำหนดระยะเวลาในการจัดเก็บข้อมูลที่ชัดเจน
2. กำหนดให้ทีมบริหารจัดการข้อมูล และผู้ดูแลระบบสารสนเทศทำการย้ายข้อมูลที่มีการจัดเก็บเกินระยะเวลาที่กำหนดแล้วเพื่อจัดเก็บเป็นข้อมูลถาวร
3. กำหนดให้การจัดเก็บชุดข้อมูลจะต้องมีคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตา หากไม่มีหรือไม่ครบถ้วน ทีมบริหารจัดการข้อมูลจะต้องแจ้งผู้รับผิดชอบ ได้แก่ เจ้าของข้อมูล บริกรข้อมูลด้านเทคนิค และบริกรข้อมูลด้านธุรกิจ โดยทีมบริหารจัดการข้อมูลร่วมกันจัดทำและปรับปรุงให้เป็นปัจจุบัน
4. ผู้มีส่วนได้ส่วนเสียเกี่ยวข้องกับข้อมูล ทั้งเจ้าของข้อมูล ผู้สร้างข้อมูล ผู้ใช้ข้อมูล และทีมบริหารจัดการข้อมูล จะต้องจัดเก็บข้อมูลตามการจัดชั้นความลับของหน่วยงาน โดยทำการเข้ารหัสข้อมูลเพื่อป้องกันการเข้าถึงหรือแก้ไขข้อมูลโดยไม่ได้รับอนุญาต ทั้งนี้การเข้ารหัสข้อมูลให้ปฏิบัติตามวิธีการเข้ารหัสข้อมูลแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน
   4.1. ในกรณีที่ในตารางฐานข้อมูลเดียวกันมีฟิลด์ข้อมูลที่มีชั้นความลับและไม่มีชั้นความลับอยู่ร่วมกันให้ทำการเข้ารหัสข้อมูลเฉพาะฟิลด์ข้อมูลที่มีชั้นความลับเท่านั้น
   4.2. ในกรณีข้อมูลที่จัดเก็บในรูปแบบเอกสาร ให้มีการจัดเก็บ ดังนี้
      - เก็บในสถานที่เหมาะสม สามารถปิดล็อกได้เมื่อไม่ใช้งาน
      - เก็บแยกออกจากอุปกรณ์ประมวลผลต่าง ๆ เช่น เครื่องพิมพ์ เครื่องถ่ายเอกสาร เป็นต้น โดยทันที เพื่อเป็นการป้องกันไม่ให้ผู้ไม่มีสิทธิในการเข้าถึงข้อมูล เข้าถึงข้อมูลได้
5. กำหนดให้มีวิธีปฏิบัติการกู้คืนข้อมูลที่จัดเก็บถาวร สำหรับข้อมูลที่มีความสำคัญมากต่อการดำเนินงานของหน่วยงาน เพื่อสอบทานความถูกต้อง ครบถ้วน ความพร้อมใช้งาน คุณภาพข้อมูล

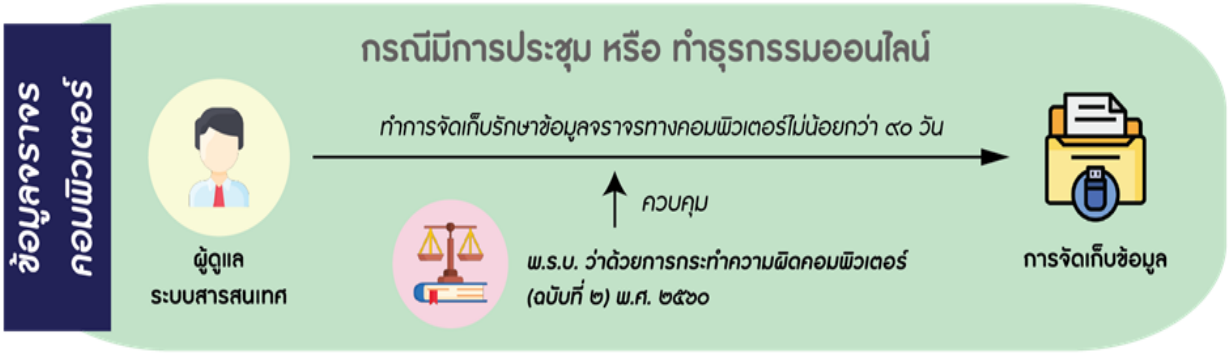


6. ในการจัดเก็บข้อมูลส่วนบุคคล**ให้เก็บรวบรวมได้เท่าที่จำเป็น** ภายใต้อำนาจหน้าที่และวัตถุประสงค์อันชอบด้วยกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล และ**ไม่เก็บรวบรวมข้อมูลส่วนบุคคล**ดังต่อไปนี้ เว้นแต่ได้รับการยินยอมจากเจ้าของข้อมูลส่วนบุคคล หรือพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล หรือกฎหมายอื่นบัญญัติให้กระทำได้

- 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

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

ตารางที่: 2 ตัวอย่างผู้มีส่วนได้ส่วนเสียในการจัดเก็บข้อมูล

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

หมวด 3 การประมวลผลข้อมูลและการใช้ข้อมูล

วัตถุประสงค์

กำหนดแนวปฏิบัติในการประมวลผลข้อมูลและการใช้ข้อมูลที่มีประสิทธิภาพถูกต้อง ตรงตามวัตถุประสงค์ 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
3. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

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. ผู้ใช้ข้อมูลจะต้องไม่ใช้ข้อมูลในเครือข่ายของหน่วยงานเพื่อประโยชน์ในเชิงธุรกิจเป็นการส่วนตัวหรือเพื่อเข้าสู่เว็บไซต์ที่ไม่เหมาะสมหรือใช้ข้อมูลอันก่อให้เกิดความเสียหายต่อหน่วยงาน

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

ตารางที่: 3 ตัวอย่างผู้มีส่วนได้ส่วนเสียในการประมวลผลและใช้ข้อมูล

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

หมวด 4 การเปิดเผยข้อมูล

วัตถุประสงค์

กำหนดแนวปฏิบัติการเปิดเผยข้อมูลต่อสาธารณะโดยอิงจากกฎหมาย กฎเกณฑ์และแนวปฏิบัติที่เกี่ยวข้อง ทั้งนี้ข้อมูลที่เปิดเผยควรเป็นประโยชน์ สามารถนำไปประมวลผลและใช้ต่อยอดในการพัฒนาในรูปแบบต่าง ๆ ได้

ผู้รับผิดชอบงาน

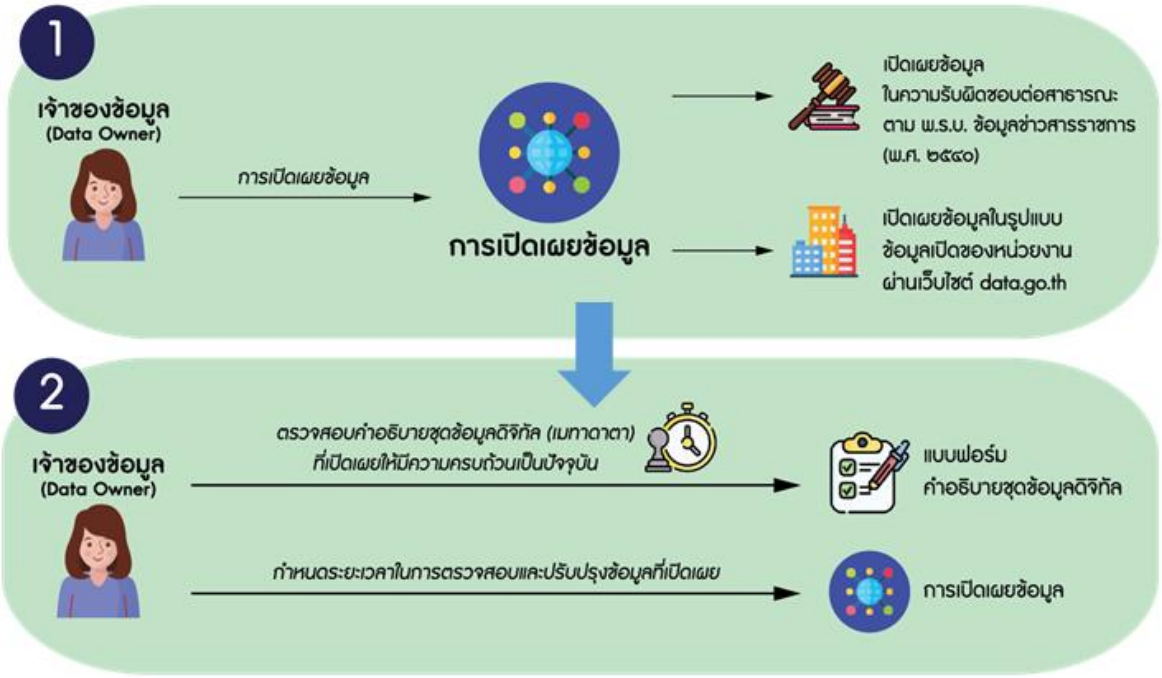
1. เจ้าของข้อมูล (Data Owners)
2. ผู้ใช้ข้อมูล (Data Users)
3. บริกรข้อมูล (Data Stewards)
4. ทีมบริหารจัดการข้อมูล (Data Management Team)

อ้างอิง

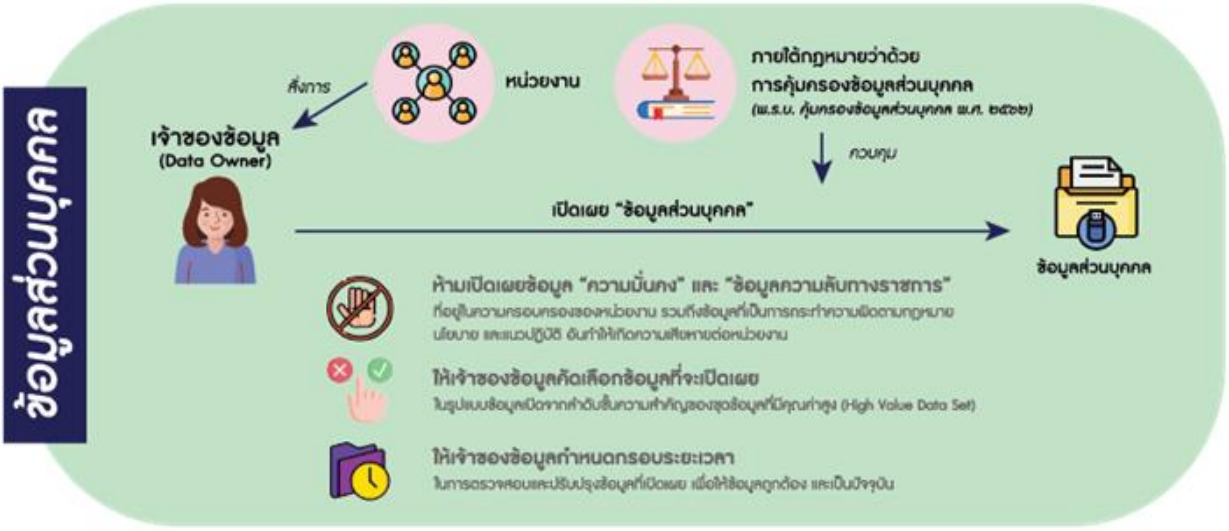
1. พระราชบัญญัติข้อมูลข่าวสารราชการ พ.ศ. 2540
2. พระราชบัญญัติการอำนวยความสะดวกในการพิจารณาอนุญาตของทางราชการ พ.ศ. 2558
3. พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562
4. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
5. ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง มาตรฐานและหลักเกณฑ์การเปิดเผยข้อมูลเปิดภาครัฐในรูปแบบข้อมูลดิจิทัลต่อสาธาร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

ข้อปฏิบัติ

1. เจ้าของข้อมูลจะต้องเปิดเผยข้อมูลในความรับผิดชอบต่อสาธารณะตามกฎหมายว่าด้วยข้อมูลข่าวสารของราชการ และมาตรฐานและหลักเกณฑ์การเปิดเผยข้อมูลเปิดภาครัฐในรูปแบบข้อมูลดิจิทัลต่อสาธารณะ



2. เจ้าของข้อมูลทำการเปิดเผยข้อมูลในความรับผิดชอบในรูปแบบข้อมูลเปิดของหน่วยงานโดยดำเนินการดังนี้
   - กำหนดลักษณะของข้อมูลที่เผยแพร่กำหนดให้อยู่ในรูปแบบที่เครื่องสามารถประมวลผลได้
   - กำหนดให้มีคำอธิบายข้อมูลหรือเมทาดาตาสำหรับข้อมูลที่ต้องเปิดเผย
   - ข้อมูลที่เผยแพร่จะต้องมีการบันทึกเวลา (Timestamps) ที่ช่วยให้ผู้ใช้งานสามารถระบุได้ว่าข้อมูลนั้นเป็นปัจจุบัน
   - ข้อมูลที่เผยแพร่ต้องมาจากแหล่งที่เก็บข้อมูลโดยตรง ด้วยระดับความละเอียดสูงโดยไม่มีการปรับแต่งหรือเป็นข้อมูลรูปแบบสรุป (Summary data)
   - ชุดข้อมูลและรายการชุดข้อมูลที่เผยแพร่จะต้องมีการจัดรูปแบบที่กำหนดเป็นมาตรฐาน และกำหนดภายใต้หมวดหมู่เดียวกัน เพื่อให้ผู้ใช้ข้อมูลสามารถค้นหาและเข้าถึงข้อมูลได้ง่าย
3. กำหนดให้เงื่อนไขและข้อกำหนดของข้อมูลที่นำมาเปิดเผยภายในเครือข่ายของหน่วยงาน ข้อมูลที่เผยแพร่ต้องไม่ขัดต่อกฎหมายว่าด้วยทรัพย์สินทางปัญญา เว้นแต่การเปิดเผยข้อมูลจะเป็นไปตามอำนาจที่กฎหมายรับรอง
4. สนับสนุนการจัดทำบัญชีข้อมูลหน่วยงานและการลงทะเบียนบัญชีข้อมูลภาครัฐ โดยบริหารจัดการข้อมูลสำคัญ จัดทำบัญชีข้อมูลของหน่วยงาน และทำการลงทะเบียนบัญชีข้อมูลของหน่วยงานและชุดข้อมูลสำคัญ เข้าสู่ระบบบัญชีข้อมูลภาครัฐ (Government Data Catalog หรือ GD Catalog) เพื่อการเปิดเผยข้อมูลภาครัฐที่เป็นระบบ และมีเอกภาพ สามารถสืบค้นชุดข้อมูล คำอธิบายชุดข้อมูล รวมไปถึงแหล่งต้นทางของชุดข้อมูลภาครัฐที่สำคัญ สนับสนุนการใช้ประโยชน์ข้อมูลภาครัฐร่วมกัน
5. สนับสนุนการเผยแพร่ข้อมูลผ่านช่องทางที่ง่ายต่อการเข้าถึงข้อมูล และสนับสนุนการเปิดเผยข้อมูลในรูปแบบดิจิทัลต่อสาธารณะที่ศูนย์กลางข้อมูลเปิดภาครัฐ (Government Open Data) ผ่านเว็บไซต์ data.go.th โดย
   - กำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัยในการเปิดเผยข้อมูลที่กำหนดลำดับชั้นข้อมูลตั้งแต่ลับขึ้นไป อย่างเพียงพอและมีประสิทธิภาพ
   - มีการตรวจสอบข้อมูลที่เผยแพร่จากหน่วยงานทั้งภายในและภายนอกหน่วยงาน เพื่อให้มั่นใจว่าหน่วยงานได้มีข้อมูลที่เผยแพร่ที่มีคุณค่า
   - การเผยแพร่ข้อมูล ต้องมีการตรวจสอบรูปแบบข้อมูลที่เผยแพร่ให้สอดคล้องกับมาตรฐานที่หน่วยงานกำหนด
   - หากการเปิดเผยนั้นเป็นการเปิดเผยบนช่องทางที่ดูแลรับผิดชอบโดยหน่วยงานอื่นที่ให้ปฏิบัติตามเอกสาร คู่มือ การนำข้อมูลขึ้นเผยแพร่ของหน่วยงานนั้น
   - หากการเปิดเผยข้อมูลไม่ครบถ้วน หรือไม่เป็นปัจจุบัน ให้แจ้งเจ้าของข้อมูล บริกรข้อมูลธุรกิจ บริกรข้อมูลเทคนิค และทีมบริหารจัดการข้อมูลทำการจัดทำ/ปรับปรุงให้เป็นปัจจุบัน
6. กำหนดให้เปิดเผยข้อมูลส่วนบุคคลตามข้อกำหนดของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือตามคำสั่งที่ได้รับจากหน่วยงานเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติในกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล



7. เจ้าของข้อมูลห้ามเปิดเผยข้อมูลความมั่นคงและข้อมูลความลับทางราชการที่อยู่ในความครอบครองของหน่วยงานรวมทั้งห้ามเปิดเผยข้อมูลที่เป็นการกระทำความผิดตามกฎหมาย นโยบาย และแนวปฏิบัติอันทำให้เกิดความเสียหายต่อหน่วยงาน
8. กำหนดให้เจ้าของข้อมูลคัดเลือกข้อมูลที่จะเปิดเผยในรูปแบบข้อมูลเปิดจากลำดับชั้นความสำคัญของชุดข้อมูลที่มีคุณค่าสูง (High Value Dataset)
9. กำหนดให้เจ้าของข้อมูลต้องกำหนดรอบระยะเวลาในการตรวจสอบและปรับปรุงข้อมูลที่เปิดเผยเพื่อให้ข้อมูลถูกต้อง และเป็นปัจจุบัน

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

ตารางที่: 4 ตัวอย่างผู้มีส่วนได้ส่วนเสียในการเปิดเผยข้อมูล

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

หมวด 5 การทำลายข้อมูล

วัตถุประสงค์

กำหนดแนวปฏิบัติการทำลายข้อมูล และการพิจารณาอนุมัติทำลายโดยเจ้าของข้อมูลเพื่อเป็นการรักษาความมั่นคงปลอดภัยของข้อมูล

ผู้รับผิดชอบงาน

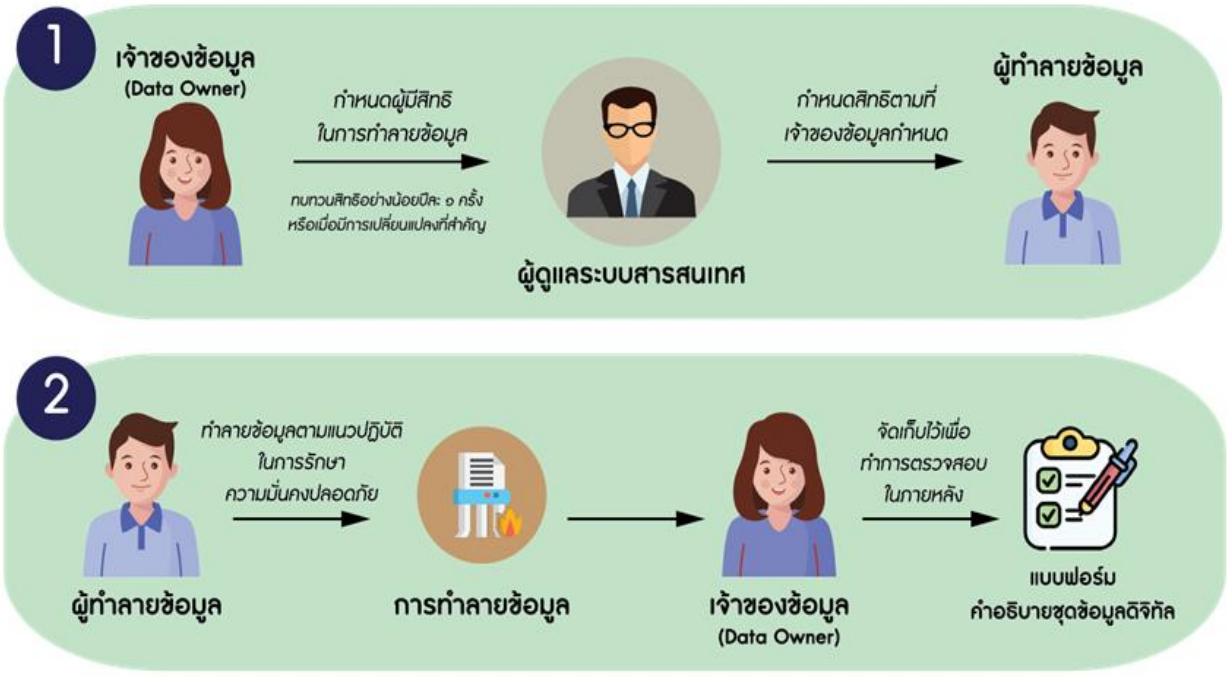
1. เจ้าของข้อมูล (Data Owners)
2. ผู้ทำลายข้อมูล (Data Disposer)
3. ผู้ดูแลระบบสารสนเทศ (Systems Administrators)

อ้างอิง

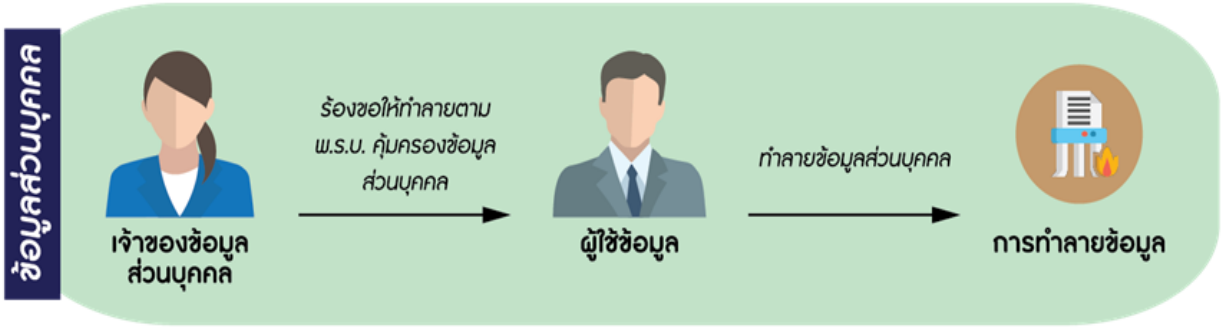
1. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553
2. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

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



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

ตารางที่: 5 ตัวอย่างผู้มีส่วนได้ส่วนเสียในการทำลายข้อมูล

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

หมวด 6 การเชื่อมโยงและการแลกเปลี่ยนข้อมูล

วัตถุประสงค์

เพื่อกำหนดแนวปฏิบัติและมาตรฐานด้านเทคนิคในการเชื่อมโยงและการแลกเปลี่ยนข้อมูลดิจิทัลทั้งภายในหน่วยงานและระหว่างหน่วยงาน อย่างมีประสิทธิภาพและก่อให้เกิดประโยชน์ต่อภาคประชาชน ภาครัฐ และภาคเอกชน

ผู้รับผิดชอบงาน

1. ผู้จัดการโครงการ (Project Managers)
2. ผู้ดูแลระบบแม่ข่าย (Server Administrators)
3. เจ้าของข้อมูล (Data Owners)
4. บริกรข้อมูล (Data Stewards)
5. ทีมบริหารจัดการข้อมูล (Data Management Team)

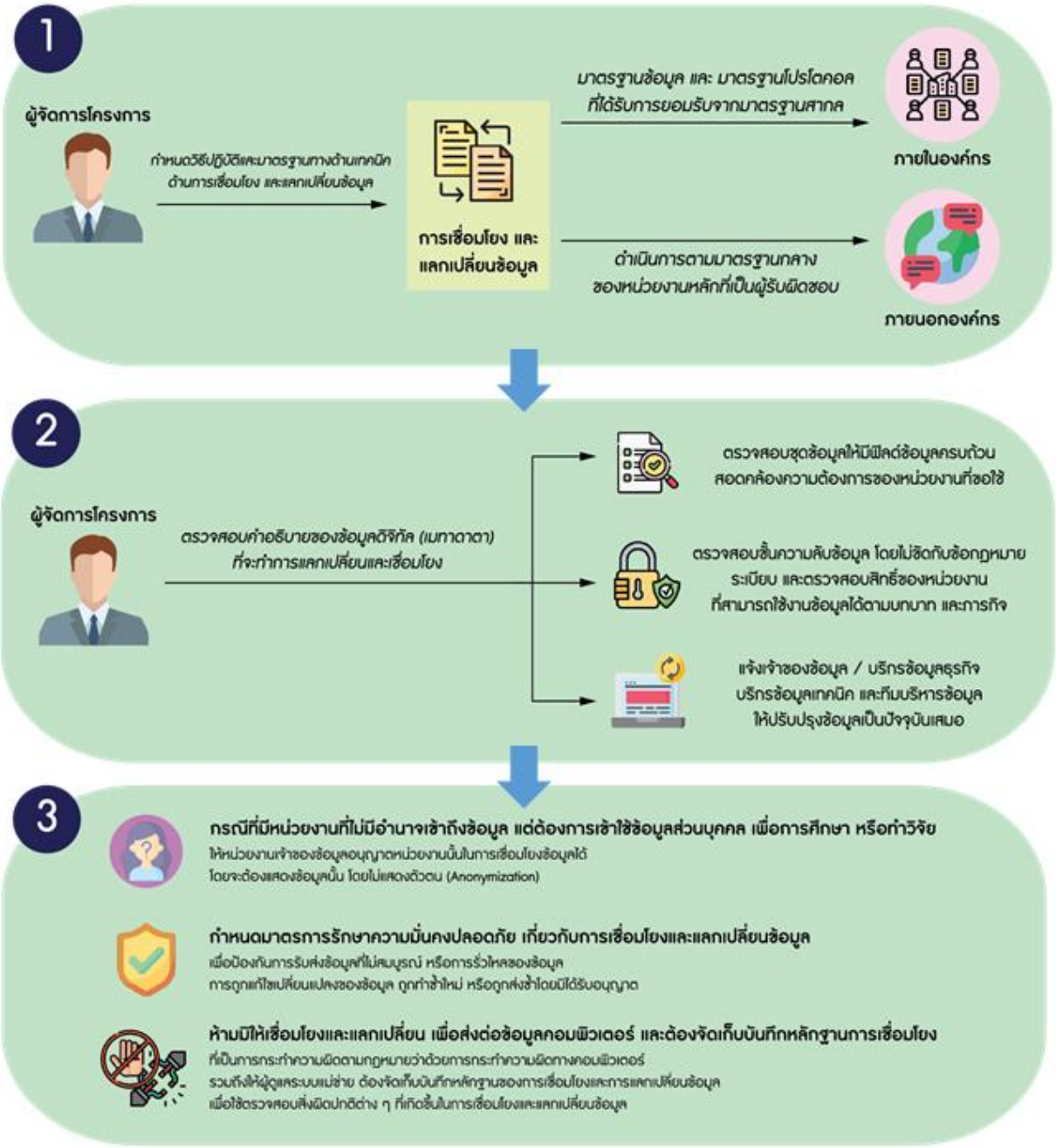
อ้างอิง

1. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553
2. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560

3. พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562
4. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ข้อปฏิบัติ

1. กำหนดให้ผู้จัดการโครงการกำหนดวิธีปฏิบัติและมาตรฐานทางด้านเทคนิคที่จำเป็นต้องใช้เกี่ยวกับการเชื่อมโยงและแลกเปลี่ยนข้อมูลของโครงการในความรับผิดชอบ ดังนี้
   - การเชื่อมโยงและแลกเปลี่ยนข้อมูลภายในหน่วยงาน กำหนดให้ใช้รูปแบบที่เป็นมาตรฐานเปิด (Open Format) ทั้งในส่วนมาตรฐานข้อมูล เช่น XML และ JSON เป็นต้น มาตรฐานโปรโตคอลสื่อสาร 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 บริกรข้อมูลธุรกิจ บริกรข้อมูลเทคนิค 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. กำหนดให้ผู้ดูระบบแม่ข่ายต้องจัดเก็บบันทึกหลักฐานของการเชื่อมโยงและการแลกเปลี่ยนข้อมูลดิจิทัล เพื่อใช้ตรวจสอบสิ่งผิดปกติต่าง ๆ ที่เกิดขึ้นในการเชื่อมโยงและแลกเปลี่ยนข้อมูล

กิจกรรม	ผู้มีส่วนได้ส่วนเสีย				
	ผู้จัดการโครงการ	ผู้ดูแลระบบแม่ข่าย	เจ้าของข้อมูล	บริกรข้อมูล	ทีมบริหารจัดการข้อมูล
กำหนดวิธีปฏิบัติและมาตรฐานทางด้านเทคนิคที่จำเป็นในการเชื่อมโยงและแลกเปลี่ยนข้อมูลของโครงการ	R	S	I	I	I
ตรวจสอบคำอธิบายชุดข้อมูลดิจิทัล และชั้นความลับของข้อมูล	R	R	C	C	S
จัดทำแนวทางการทำงานร่วมกันทั้งระหว่างหน่วยงานภายในและหน่วยงานภายนอกในการเชื่อมโยงและแลกเปลี่ยนข้อมูล	R	S	S	S	S
จัดเก็บบันทึกหลักฐานของการเชื่อมโยงและการแลกเปลี่ยนข้อมูลดิจิทัล	I	R	I	I	I

ตารางที่: 6 ตัวอย่างผู้มีส่วนได้ส่วนเสียในการเชื่อมโยงและแลกเปลี่ยนข้อมูล

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

ภาคผนวก

การเลือกภารกิจ/กระบวนงานของหน่วยงาน

ลิงก์สำหรับดาวน์โหลดแบบฟอร์มรายชื่อชุดข้อมูลที่สัมพันธ์กับกระบวนการทำงานตามภารกิจของหน่วยงาน https://gdhelppage.nso.go.th/p00_03_001.html

การจัดทำคำอธิบายชุดข้อมูล (Metadata)

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

แนวทางในการพิจารณาชุดข้อมูลที่มีคุณค่าสูง

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

ภาคผนวก ฉ.
คำอธิบายข้อมูลหรือเมทาดาตาสำหรับชุดข้อมูลภาครัฐ
(Metadata Standard Guideline)

ภาคผนวก ก
คำอธิบายข้อมูลหรือเมทาดาตาสำหรับชุดข้อมูลภาครัฐ (Metadata Standard)

ตารางที่: 1 คำอธิบายข้อมูลส่วนหลัก (Mandatory Metadata) สำหรับชุดข้อมูลภาครัฐ

No.	ชื่อรายการไทย	ชื่อทางเทคนิค	คำอธิบาย	ตัวเลือก / รูปแบบ	ตัวอย่าง	
1	ประเภทข้อมูล	data_type	ชุดข้อมูลนี้เป็นข้อมูลประเภทใด	Code (Character 1 digits (1-9)) ดูรายละเอียด “ภาคผนวก ข.”	1 = ข้อมูลระเบียน	2 = ข้อมูลสถิติ
2	ชื่อชุดข้อมูล	title	ชื่อของชุดข้อมูลที่กำหนดโดยองค์กรที่รับผิดชอบข้อมูล	Text (150 Characters)	รายได้จากการท่องเที่ยว	จำนวนกำลังแรงงานรวม
3.1	รหัสองค์กร	Org_ID	รหัสองค์กรที่รับผิดชอบข้อมูล	Code (Character 4 digits) ดูรายละเอียด “ภาคผนวก ข.”	0304 - กรมบัญชีกลาง	S702 - ธนาคารกรุงไทย
3.2	ชื่อองค์กร	Org_standard_name	ชื่อองค์กรที่รับผิดชอบข้อมูล	Text (255 Characters)	สำนักงานปลัดกระทรวงการท่องเที่ยวและกีฬา	สำนักงานสถิติแห่งชาติ
4	ชื่อฝ่ายงานสำหรับติดต่อ	maintainer	ชื่อกอง สำนัก หรือฝ่าย ที่ได้รับการมอบหมายให้รับผิดชอบข้อมูล	Text (150 Characters)	กลุ่มสารสนเทศด้านเศรษฐกิจ	กองสถิติสังคม
5	อีเมลสำหรับติดต่อ	maintainer_email	อีเมลกอง สำนัก หรือฝ่าย ที่ได้รับการมอบหมายให้รับผิดชอบข้อมูล	Text (50 Characters)	bets@mots.go.th	slaborfs@nso.go.th

No.	ชื่อรายการไทย	ชื่อทางเทคนิค	คำอธิบาย	ตัวเลือก / รูปแบบ	ตัวอย่าง	
6	คำสำคัญ	tag_string	หัวข้อ คำ วลี หรือแท็ก (tag) ที่ใช้ระบุคำสำคัญในชุดข้อมูล	Text แยกแต่ละ keywords ด้วย “,” (comma) (200 Characters)	รายได้, ท่องเที่ยว, จังหวัด	แรงงาน, กำลังแรงงาน
7	รายละเอียด	notes	คำอธิบายรายละเอียดที่สำคัญของชุดข้อมูลอย่างสั้น เช่น คำนิยาม ชุดข้อมูลเกี่ยวกับอะไร มีวิธีการจัดเก็บแบบใด กลุ่มเป้าหมายผู้ใช้งานข้อมูลเป็นใคร	Text (1,000 Characters)	รายได้จากการท่องเที่ยวจำแนกรายจังหวัด	กำลังแรงงานรวม หมายถึง บุคคลทุกคนที่มี อายุ 15 ปีขึ้นไป ในสัปดาห์แห่งการสำรวจเป็นผู้อยู่ในกำลังแรงงานปัจจุบัน และเป็นผู้ถูกจัดจำแนกอยู่ในประเภทกำลังแรงงานที่รอฤดูกาล
8	วัตถุประสงค์	objective	อธิบายที่มาและวัตถุประสงค์ของการจัดทำชุดข้อมูล เช่น กฎหมาย ภารกิจ โครงการตามแผนยุทธศาสตร์ และเพื่อใช้ในการวิเคราะห์หรือตอบโจทย์ในประเด็นยุทธศาสตร์ในเรื่องใดที่ผู้ใช้ต้องการ	Code (Character 2 digits (01-99)) ดูรายละเอียด “ภาคผนวก ข.”	04 = แผนพัฒนาการท่องเที่ยวแห่งชาติ ฉบับที่ 2 (พ.ศ. 2560-2564) 11 = พันธกิจของ สป.กก. - เพื่อรายงานสถานการณ์ด้านการท่องเที่ยว	10 = กฎกระทรวง 11 = พันธกิจของสำนักงานสถิติแห่งชาติ - เพื่อประมาณจำนวนและลักษณะของกำลังแรงงานภายในประเทศ
9.1	หน่วยความถี่ของการปรับปรุงข้อมูล	update_frequency_unit	<u>สำหรับข้อมูลระเบียน</u> <u>และข้อมูลภูมิสารสนเทศเชิงพื้นที่</u> : ความถี่ที่ข้อมูลในระบบคลังข้อมูลถูกปรับปรุง/เพิ่ม หรือเปลี่ยนแปลง <u>สำหรับข้อมูลสถิติ</u>: ความถี่ในการเผยแพร่ต่อผู้ใช้ข้อมูล	Code (1 Character (A-Z)) ดูรายละเอียด “ภาคผนวก ข.”	A	M

No.	ชื่อรายการไทย	ชื่อทางเทคนิค	คำอธิบาย	ตัวเลือก / รูปแบบ	ตัวอย่าง	
9.2	ค่าความถี่ของการปรับปรุงข้อมูล	update_frequency_interval	ใช้คุณสมบัตินี้ประกอบกับหน่วยความถี่ในการปรับปรุงข้อมูล ตัวอย่างเช่น ถ้าชุดข้อมูลมีการปรับปรุงทุก ๆ 2 ปี ท่านสามารถใส่ “2” สำหรับค่าความถี่ และ “รายปี” สำหรับหน่วยความถี่	Number หรือ เว้นว่างไว้	2	1
10	ขอบเขตเชิงภูมิศาสตร์หรือเชิงพื้นที่	geo_coverage	สำหรับข้อมูลระเบียน และข้อมูลภูมิสารสนเทศเชิงพื้นที่: มิติการจัดจำแนกข้อมูลพื้นที่ในระดับย่อยที่สุดในการจัดเก็บข้อมูล สำหรับข้อมูลสถิติ: มิติการจัดจำแนกข้อมูลพื้นที่ในระดับย่อยที่สุดในการนำเสนอข้อมูล	Code (Character 2 digits (00-99)) ดูรายละเอียด “ภาคผนวก ข.”	06 = จังหวัด	06 = จังหวัด
11	แหล่งที่มา	data_source	แหล่งที่มาของข้อมูลที่นำมาจัดทำชุดข้อมูล พร้อมองค์กรที่จัดทำ เช่น สำรวจภาวะการทำงานของประชากร (สำนักงานสถิติแห่งชาติ) ฐานข้อมูลทะเบียนราษฎร์ (กรมการปกครอง)	Text (200 Characters)	รายงานสถานการณ์ด้านการท่องเที่ยว (สป.กก.)	สำรวจภาวะการทำงานของประชากร (สำนักงานสถิติแห่งชาติ)
12	รูปแบบการเก็บข้อมูล	data_format	รูปแบบของการจัดเก็บข้อมูล	Code (Character 2 digits (01-99)) ดูรายละเอียด “ภาคผนวก ข.”	02 = csv 07 = text	01 = Database 10 = XLS 07 = text 99 = อื่น ๆ ระบุ SPSS

No.	ชื่อรายการไทย	ชื่อทางเทคนิค	คำอธิบาย	ตัวเลือก / รูปแบบ	ตัวอย่าง	
13	หมวดหมู่ข้อมูลตามธรรมาภิบาลข้อมูลภาครัฐ	data_category	หมวดหมู่ข้อมูลตามธรรมาภิบาลข้อมูลภาครัฐ	Code (Character 1 digits (1-4)) ดูรายละเอียด “ภาคผนวก ข.”	1 = ข้อมูลสาธารณะ	1 = ข้อมูลสาธารณะ
14	สัญญาอนุญาตให้ใช้ข้อมูล	license_id	สัญญาอนุญาตให้ใช้ข้อมูล ต้องสอดคล้องกับหมวดหมู่ข้อมูลตามธรรมาภิบาลข้อมูลภาครัฐ	Code (G0 – G6) ดูรายละเอียด “ภาคผนวก ข.”	G0 = Open Data Common	G6 = Others License

ตารางที่: 2 คำอธิบายข้อมูลส่วนที่เป็นทางเลือก (Optional Metadata) สำหรับชุดข้อมูลภาครัฐ: ประเภทข้อมูลระเบียน

No.	ชื่อรายการไทย	ชื่อทางเทคนิค	คำอธิบาย	ตัวเลือก / รูปแบบ
15	ระดับชั้นข้อมูล	Data_Classification	ระดับชั้นข้อมูลเพื่อจัดการข้อมูลในกระบวนงานที่เกี่ยวข้องกับภารกิจ โดยข้อมูลที่มีความอ่อนไหวแบ่งระดับชั้นออกเป็น ชั้นเปิดเผย (Open) ชั้นเผยแพร่ภายในองค์กร (Private) ชั้นลับ (Confidential) ชั้นลับมาก (Secret) และ ชั้นลับที่สุด (Top Secret)	ดูรายละเอียด “ภาคผนวก ข.”
	เงื่อนไขในการเข้าถึงข้อมูล	accessible_condition	เงื่อนไขเพื่อให้สามารถเข้าถึงหรือใช้ข้อมูลได้ ในกรณีที่เลือกหมวดหมู่ข้อมูลตามธรรมาภิบาลข้อมูลภาครัฐในรายการที่ 13 เป็นข้อมูลใช้ภายใน ข้อมูลความมั่นคง ข้อมูลความลับทางราชการ ข้อมูลส่วนบุคคล	ดูรายละเอียด “ภาคผนวก ข.”
16	วันที่เริ่มต้นสร้าง	created_date	วัน เดือน ปี ที่เริ่มต้นสร้างหรือจัดทำข้อมูล โดยระบบสร้างขึ้นอัตโนมัติ หรือดึงข้อมูลจากฐานข้อมูล	DATE: YYYY-MM-DD ในรูปแบบปี พ.ศ.
17	วันที่ปรับปรุงข้อมูลล่าสุด	last_updated_date	วัน เดือน ปี ที่ปรับปรุงหรือเผยแพร่ข้อมูลล่าสุด โดยระบบสร้างขึ้นอัตโนมัติ หรือดึงข้อมูลจากฐานข้อมูล	DATE: YYYY-MM-DD ในรูปแบบปี พ.ศ.
18	URL	url	URL ที่สามารถเข้าถึงชุดข้อมูลได้	Text โดยมีชื่อ Domain ที่เป็นทางการ
19	ผู้สนับสนุนหรือผู้ร่วมดำเนินการ	data_support	องค์กรสนับสนุนหรือร่วมดำเนินการ นอกเหนือจากองค์กรที่รับผิดชอบข้อมูล	Code (Character 1 digits (0-9)) ดูรายละเอียด “ภาคผนวก ข.”
20	หน่วยที่ย่อยที่สุดของการจัดเก็บข้อมูล	data_collect	หน่วยที่ย่อยที่สุดของการจัดเก็บข้อมูล เช่น บุคคล สถานประกอบการ ประเทศ	Code (Character 2 digits (0-9)) ดูรายละเอียด “ภาคผนวก ข.”
21	ภาษาที่ใช้	data_language	ภาษาที่ใช้ในชุดข้อมูล เช่น ภาษาไทย ภาษาอังกฤษ ภาษาจีน ภาษาญี่ปุ่น	Code (Character 2 digits (0-9)) ดูรายละเอียด “ภาคผนวก ข.”
22	ชุดข้อมูลที่มีคุณค่าสูง	high_value_dataset	ชุดข้อมูลที่มีคุณค่าสูง โดยองค์กรที่นำเข้าข้อมูลไม่ต้องกรอก	BOOLEAN (เป็น และ ไม่เป็น)
23	ข้อมูลอ้างอิง	reference_data	ข้อมูลอ้างอิง โดยองค์กรที่นำเข้าข้อมูลไม่ต้องกรอก	BOOLEAN (เป็น และ ไม่เป็น)

ตารางที่: 3 คำอธิบายข้อมูลส่วนที่เป็นทางเลือก (Optional Metadata) สำหรับชุดข้อมูลภาครัฐ: ประเภทข้อมูลสถิติ

No.	ชื่อรายการไทย	ชื่อทางเทคนิค	คำอธิบาย	ตัวเลือก / รูปแบบ
15	ระดับชั้นข้อมูล	Data_Classification	ระดับชั้นข้อมูลเพื่อจัดการข้อมูลในกระบวนงานที่เกี่ยวข้องกับภารกิจ โดยข้อมูลที่มีความอ่อนไหวแบ่งระดับชั้นออกเป็น ชั้นเปิดเผย (Open) ชั้นเผยแพร่ภายในองค์กร (Private) ชั้นลับ (Confidential) ชั้นลับมาก (Secret) และ ชั้นลับที่สุด (Top Secret) ซึ่งข้อมูลที่มีระดับชั้น ลับ (Confidential) ลับมาก (Secret) และ ลับที่สุด (Top Secret)	ดูรายละเอียด “ภาคผนวก ข.”
	เงื่อนไขในการเข้าถึงข้อมูล	accessible_condition	เงื่อนไขเพื่อให้สามารถเข้าถึงหรือใช้ข้อมูลได้ ในกรณีที่เลือกหมวดหมู่ข้อมูลตามธรรมาภิบาลข้อมูลภาครัฐในรายการที่ 13 เป็นข้อมูลใช้ภายใน ข้อมูลความมั่นคง ข้อมูลความลับทางราชการ ข้อมูลส่วนบุคคล	ดูรายละเอียด “ภาคผนวก ข.”
16	ปีข้อมูลที่เริ่มต้นจัดทำ	first_year_of_data	ปีข้อมูลที่เริ่มต้นจัดทำ ในกรณีความถี่ในการจัดทำมากกว่าปีละครั้ง ให้ระบุ วันที่หรือเดือนหรือไตรมาสที่เริ่มต้นจัดทำ เช่น มี.ค./2540	DATE: YYYY-MM-DD โดยในกรณีที่ไม่สามารถระบุวัน หรือเดือน ให้แสดงเฉพาะปี (ในรูปแบบปี พ.ศ.) หรือเดือนที่เลือก
17	ปีข้อมูลล่าสุดที่เผยแพร่	last_year_of_data	ปีข้อมูลล่าสุดที่เผยแพร่ ในกรณีที่ความถี่ในการเผยแพร่มากกว่าปีละครั้ง ให้ระบุ วันที่หรือเดือนหรือไตรมาสล่าสุดที่เผยแพร่ เช่น มี.ค./2562	DATE: YYYY-MM-DD โดยในกรณีที่ไม่สามารถระบุวัน หรือเดือน ให้แสดงเฉพาะปี (ในรูปแบบปี พ.ศ.) หรือเดือนที่เลือก
18	วันที่กำหนดเผยแพร่ข้อมูล	data_release_ calendar	แสดงกำหนดการเผยแพร่วัน เดือน ปี หรือในกรณีที่สามารถระบุเป็นชั่วโมงหรือนาทีได้ให้ระบุ ทั้งนี้ขึ้นกับลักษณะของสถิติทางการ	DATETIME: YYYY-MM-DD-hh-mm ในกรณีกำหนดการเผยแพร่เป็น ปี-เดือน-วัน-ชั่วโมง-นาที หากสามารถระบุได้ชัดเจน หรือ ระบุ..... ในกรณีที่ไม่สามารถกำหนดเป็นวันเวลาที่ชัดเจน เช่น ทุกวันที่ 3 ของเดือน หรือ เวลา 9.00 น. ของวันที่ 1 ของทุกเดือนเป็นต้น

No.	ชื่อรายการไทย	ชื่อทางเทคนิค	คำอธิบาย	ตัวเลือก / รูปแบบ
19	วันที่ปรับปรุงข้อมูลล่าสุด	last_updated_date	วัน เดือน ปี ที่ปรับปรุงหรือเผยแพร่ข้อมูลล่าสุด โดยระบบสร้างขึ้นอัตโนมัติ หรือดึงข้อมูลจากฐานข้อมูล	DATE: YYYY-MM-DD ในรูปแบบปี พ.ศ.
20	การจัดจำแนก	disaggregation	การจัดจำแนกที่ใช้ในการจัดทำสถิติทางการ เช่น เพศ อายุ ศาสนา ระดับการศึกษา อาชีพ ประเทศ	Code (Character 2 digits (0-9)) ดูรายละเอียด “ภาคผนวก ข.”
21	หน่วยวัด	unit_of_measure	หน่วยนับจำนวน เช่น บาท ไร่ ครัวเรือน คน คดี ชิ้น อัน เครื่อง งาน กิโลกรัม กิโลเมตร ต่อประชากร 1,000 คน หรือไม่มีหน่วยในกรณีที่เป็นดัชนี	Text (100 Characters)
22	หน่วยตัวคูณ	unit_of_multiplier	ตัวคูณของหน่วยวัด เช่น ข้อมูลมูลค่าการลงทุน หน่วย: ล้านบาท หน่วยวัดคือ บาท หน่วยตัวคูณคือ 1 ล้าน	Code (Character 2 digits (0-9)) ดูรายละเอียด “ภาคผนวก ข.”
23	วิธีการคำนวณ	calculation_method	วิธีการคำนวณหรือสูตรในการคำนวณที่ใช้ในการจัดทำสถิติหรือตัวชี้วัด	Text (500 Characters)
24	มาตรฐานการจัดทำข้อมูล	standard	มาตรฐานต่าง ๆ ทั้งที่เป็นมาตรฐานสากลและมาตรฐานในประเทศที่นำมาใช้อ้างอิงในการจัดทำสถิติทางการทั้งวิธีการจัดทำ รหัส การเผยแพร่ เช่น มาตรฐานการจัดทำตามSNA, มาตรฐาน ISO, มาตรฐานรหัสTSIC, มาตรฐานรหัสHS มาตรฐานการเผยแพร่ SDDS	Text (200 Characters)
25	URL	url	URL ที่สามารถเข้าถึงชุดข้อมูลได้	ใช้คำอธิบายข้อมูลส่วนที่เป็นทางเลือก (Optional Metadata) สำหรับชุดข้อมูลภาครัฐ: ประเภทข้อมูลระเบียน ในรายการที่ 18 URL
26	ภาษาที่ใช้	data_language	ภาษาที่ใช้ในชุดข้อมูล เช่น ภาษาไทย ภาษาอังกฤษ ภาษาจีน ภาษาญี่ปุ่น	ใช้คำอธิบายข้อมูลส่วนที่เป็นทางเลือก (Optional Metadata) สำหรับชุดข้อมูลภาครัฐ: ประเภทข้อมูลระเบียน ในรายการที่ 21 ภาษาที่ใช้
27	สถิติทางการ	official_statistics	ข้อความ หรือตัวเลขที่เป็นตัวแทนแสดงถึงคุณลักษณะของสิ่งต่าง ๆ ในประเทศ ที่ประมวลตามความเป็นจริงจากข้อมูลที่เก็บรวบรวมได้ตามหลักวิชาการทางสถิติ	Boolean (ใช่ และ ไม่ใช่)

No.	ชื่อรายการไทย	ชื่อทางเทคนิค	คำอธิบาย	ตัวเลือก / รูปแบบ
			และเป็นสถิติที่มีความสำคัญต่อการใช้ในการกำหนดนโยบายเพื่อการพัฒนาประเทศ โดยองค์กรที่นำเข้าข้อมูลไม่ต้องกรอก	

ตารางที่: 4 คำอธิบายข้อมูลส่วนที่เป็นทางเลือก (Optional Metadata) สำหรับชุดข้อมูลภาครัฐ: ประเภทข้อมูลภูมิศาสตร์สารสนเทศ

No.	ชื่อรายการภาษาไทย	ชื่อรายการทางเทคนิค	คำอธิบาย	ตัวเลือก/รูปแบบ
15	ระดับชั้นข้อมูล	Data_Classification	ระดับชั้นข้อมูลเพื่อจัดการข้อมูลในกระบวนงานที่เกี่ยวข้องกับภารกิจ โดยข้อมูลที่มีความอ่อนไหวแบ่งระดับชั้นออกเป็น ชั้นเปิดเผย (Open) ชั้นเผยแพร่ภายในองค์กร (Private) ชั้นลับ (Confidential) ชั้นลับมาก (Secret) และ ชั้นลับที่สุด (Top Secret) ซึ่งข้อมูลที่มีระดับชั้น ลับ (Confidential) ลับมาก (Secret) และ ลับที่สุด (Top Secret)	ดูรายละเอียด “ภาคผนวก ข.”
	เงื่อนไขในการเข้าถึงข้อมูล	accessible_condition	เงื่อนไขเพื่อให้สามารถเข้าถึงหรือใช้ข้อมูลได้ ในกรณีที่เลือกหมวดหมู่ข้อมูลตามธรรมาภิบาลข้อมูลภาครัฐในรายการที่ 13 เป็นข้อมูลใช้ภายใน ข้อมูลความมั่นคง ข้อมูลความลับทางราชการ ข้อมูลส่วนบุคคล	ดูรายละเอียด “ภาคผนวก ข.”
16	ชุดข้อมูลภูมิศาสตร์	geographic_data_set	ชุดข้อมูลภูมิศาสตร์จำแนกเป็นลักษณะเฉพาะด้านต่าง ๆ ของชั้นข้อมูลโดยแบ่งออกเป็น 13 ชุดข้อมูล ตามข้อกำหนดของมาตรฐาน โครงสร้าง เนื้อหา คุณลักษณะ คุณภาพของชุดข้อมูลภูมิศาสตร์พื้นฐาน (Fundamental Geographic Data Set : FGDS)	Code (Character 2 digits (0-9)) ดูรายละเอียด “ภาคผนวก ข”
17	มาตราส่วน	equivalent_scale	แสดงอัตราส่วนเปรียบเทียบระหว่างระยะทางที่วัดได้บนแผนที่ 1 หน่วยกับระยะทางที่วัดได้จริงบนภูมิประเทศ	Code (Character 1 digits (0-9)) ดูรายละเอียด “ภาคผนวก ข”
18.1	ค่าพิกัดกรอบพื้นที่ด้านทิศตะวันตก	west_bound_longitude	เส้นรอยตัดระหว่างผิวโลกกับพื้นราบที่ตั้งฉากกับแกนขั้วโลกเหนือ รอยตัดนี้จะเป็นวงกลมที่ขนานกับเส้นศูนย์สูตร ค่าลองจิจูดนับออกจากเมริเดียนแรกไปทางตะวันตก โดยวัดไปตามเส้นศูนย์สูตร เป็นมุมที่ศูนย์กลางโลก	Text (20 Characters)

No.	ชื่อรายการภาษาไทย	ชื่อรายการทางเทคนิค	คำอธิบาย	ตัวเลือก/รูปแบบ
18.2	ค่าพิกัดกรอบพื้นที่ด้านทิศตะวันออก	east_bound_longitude	เส้นรอยตัดระหว่างผิวโลกกับพื้นราบที่ตั้งฉากกับแกนขั้วโลกเหนือ รอยตัดนี้จะเป็นวงกลมที่ขนานกับเส้นศูนย์สูตร ค่าลองจิจูดนับออกจากเมริเดียนแรกไปทางตะวันออก โดยวัดไปตามเส้นศูนย์สูตร เป็นมุมที่ศูนย์กลางโลก	Text (20 Characters)
18.3	ค่าพิกัดกรอบพื้นที่ด้านทิศเหนือ	north_bound_longitude	เส้นรอยตัดระหว่างผิวโลกกับพื้นราบที่ตั้งฉากกับแกนขั้วโลกเหนือ รอยตัดนี้จะเป็นวงกลมที่ขนานกับเส้นศูนย์สูตร ค่าของละติจูดนับออกจากเส้นศูนย์สูตรไปทางขั้วโลกเหนือ โดยวัดไปตามเส้นเมริเดียน เป็นมุมที่ศูนย์กลางของโลก	Text (20 Characters)
18.4	ค่าพิกัดกรอบพื้นที่ด้านทิศใต้	south_bound_longitude	เส้นรอยตัดระหว่างผิวโลกกับพื้นราบที่ตั้งฉากกับแกนขั้วโลกใต้ รอยตัดนี้จะเป็นวงกลมที่ขนานกับเส้นศูนย์สูตร ค่าของละติจูดนับออกจากเส้นศูนย์สูตรไปทางขั้วโลกใต้ โดยวัดไปตามเส้นเมริเดียน เป็นมุมที่ศูนย์กลางของโลก	Text (20 Characters)
19	ความถูกต้องของตำแหน่ง	positional_accuracy	มีการควบคุมความถูกต้องของข้อมูล เช่น การวัดความถูกต้องของตำแหน่งทางราบด้วยค่า Accuacy$_H$(CE95) ของข้อมูล FGDS ของชั้นข้อมูล และ/หรือ การวัดความถูกต้องเชิงตำแหน่งทางราบด้วย RMSEH ของข้อมูล FGDS ของชั้นข้อมูล	Text (100 Characters) กรณีที่มีการควบคุมความคลาดเคลื่อนของข้อมูล กำหนดเป็นค่า “มี” พร้อมระบุวิธีการที่ใช้และค่าที่คำนวณได้ (ถ้ามี) ดูรายละเอียด “ภาคผนวก ข.” กรณีที่ไม่มีการควบคุมความคลาดเคลื่อนของข้อมูล กำหนดเป็นค่า “ไม่มี” การระบุความถูกต้องของตำแหน่งต้องสอดคล้องกับรายการที่ 16 ชุดข้อมูลภูมิศาสตร์ (geographic_data_set)

No.	ชื่อรายการภาษาไทย	ชื่อรายการทางเทคนิค	คำอธิบาย	ตัวเลือก/รูปแบบ
20	เวลาอ้างอิง	reference_period	แสดง วัน เดือน ปี ที่ใช้อ้างอิง/อธิบายข้อมูลภูมิสารสนเทศเชิงพื้นที่ เพื่อให้ทราบว่าภูมิสารสนเทศเชิงพื้นที่ที่รวบรวมได้เป็นของช่วงเวลาใดหรืออ้างอิงขณะใด หรือในกรณีที่สามารถระบุเป็นชั่วโมงหรือนาทีได้ให้ระบุ ทั้งนี้ขึ้นกับลักษณะของข้อมูล เช่น วันสุดท้ายของเดือน สัปดาห์แรกของเดือนปีปฏิทิน	DATETIME: YYYY-MM-DD-hh-mm ในกรณีกำหนดการเผยแพร่เป็น ปี-เดือน-วัน-ชั่วโมง-นาที หากสามารถระบุได้ชัดเจน หรือ ระบุ..... ในกรณีที่ไม่สามารถกำหนดเป็นวันเวลาที่ชัดเจน เช่น ทุกวันที่ 3 ของเดือน หรือ เวลา 9.00 น. ของวันที่ 1 ของทุกเดือน เป็นต้น
21	วันที่ปรับปรุงข้อมูลล่าสุด	last_updated_date	วัน เดือน ปี ที่ปรับปรุงหรือเผยแพร่ข้อมูลล่าสุด โดยระบบสร้างขึ้นอัตโนมัติ หรือดึงข้อมูลจากฐานข้อมูล	DATE: YYYY-MM-DD ในรูปแบบปี พ.ศ.
22	วันที่กำหนดเผยแพร่ข้อมูล	data_release_ calendar	แสดงกำหนดการเผยแพร่วัน เดือน ปี หรือในกรณีที่สามารถระบุเป็นชั่วโมงหรือนาทีได้ให้ระบุ ทั้งนี้ขึ้นกับลักษณะของข้อมูล	DATETIME: YYYY-MM-DD-hh-mm ในกรณีกำหนดการเผยแพร่เป็น ปี-เดือน-วัน-ชั่วโมง-นาที หากสามารถระบุได้ชัดเจน หรือ ระบุ..... ในกรณีที่ไม่สามารถกำหนดเป็นวันเวลาที่ชัดเจน เช่น ทุกวันที่ 3 ของเดือนหรือเวลา 9.00 น. ของวันที่ 1 ของทุกเดือนเป็นต้น
23	วันที่เผยแพร่ข้อมูล	data_release_date	แสดง วัน เดือน ปี ที่มีการเผยแพร่ข้อมูลหรือในกรณีที่สามารถระบุเป็นชั่วโมงหรือนาทีได้ให้ระบุ ทั้งนี้ขึ้นกับลักษณะของภูมิสารสนเทศเชิงพื้นที่	DATETIME: YYYY-MM-DD-hh-mm ในกรณีที่เผยแพร่เป็น ปี-เดือน-วัน-ชั่วโมง-นาที หากสามารถระบุได้ชัดเจน หรือ ระบุ..... ในกรณีที่ไม่สามารถกำหนดเป็นวันเวลาที่ชัดเจน เช่น ทุกวันที่ 3 ของเดือน หรือเวลา 9.00 น. ของวันที่ 1 ของทุกเดือนเป็นต้น
24	URL	url	URL ที่สามารถเข้าถึงชุดข้อมูลได้	Text (100 Characters)

No.	ชื่อรายการภาษาไทย	ชื่อรายการทางเทคนิค	คำอธิบาย	ตัวเลือก/รูปแบบ
25	ภาษาที่ใช้	data_language	ภาษาที่ใช้ในชุดข้อมูล เช่น ภาษาไทย ภาษาอังกฤษ ภาษาจีน ภาษาญี่ปุ่น	Code (Character 2 digits (0-9)) ดูรายละเอียด “ภาคผนวก ข”

ตารางที่: 5 รายการพจนานุกรมข้อมูล (Data Dictionary)

No.	ชื่อรายการ	คำอธิบาย	ตัวเลือก / รูปแบบ
1	Name	ชื่อตัวแปรข้อมูล	Text
2	Data Type	ชนิดของตัวแปรข้อมูล	เลือกใช้ตัวอย่างกลุ่มของชนิดข้อมูลสำหรับ Data Dictionary จากแหล่งต่าง ๆ เช่น MariaDB Data Types, Microsoft Access Data Types, JSON Data Types เป็นต้น
3	Description	คำอธิบายตัวแปรข้อมูล	Text
4	Required	ข้อมูลไม่สามารถเป็นค่าว่าง (null) ได้หรือไม่	สำหรับฐานข้อมูลเลือก YES / NO สำหรับชุดข้อมูลอื่น ๆ เลือก true / false
5	Example	แสดงข้อมูลจริงจากหนึ่งตัวอย่างข้อมูล (sample)	ขึ้นอยู่กับตัวอย่างข้อมูล

หมายเหตุ : รายการ 1 - 3 เป็นรายการแบบ Mandatory ที่องค์กรภาครัฐจำเป็นต้องจัดทำและระบุรายละเอียด

1) รายการชนิดข้อมูล (Data Type) สำหรับพจนานุกรมข้อมูล ที่ใช้อาจแตกต่างกันไปขึ้นอยู่กับรูปแบบการเก็บของข้อมูล และระบบการจัดการข้อมูลที่ใช้งานจริงภายในแต่ละองค์กร คณะผู้จัดทำจึงไม่กำหนดมาตรฐานสำหรับตัวเลือกของชนิดข้อมูลนี้ แต่ผู้จัดทำ Data Dictionary สามารถศึกษาและเลือกใช้ตัวอย่างกลุ่มของชนิดข้อมูลจาก “ตัวเลือก / รูปแบบ”
2) รายการบ่งบอกว่าข้อมูลไม่สามารถเป็นค่าว่างได้หรือไม่ (Required) มีมาตรฐานการเลือกใช้อย่างแตกต่างกันไป ขึ้นอยู่กับรูปแบบการเก็บของข้อมูล และระบบการจัดการข้อมูลที่ใช้งานจริง คณะผู้จัดทำจึงกำหนดมาตรฐาน 2 ชุดตัวเลือก ตามปรากฏใน “ตัวเลือก / รูปแบบ”

เอกสารอ้างอิง

มาตรฐานรัฐบาลดิจิทัล ว่าด้วยกรอบธรรมาภิบาลข้อมูลภาครัฐ ฉบับปรับปรุงแนวปฏิบัติ (Data Governance Framework Revised : Guideline) เวอร์ชั่น 2.0. สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน).

ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ (2563, 12 มีนาคม). ราชกิจจานุเบกษา. เล่ม 137 ตอนพิเศษ 74 ง.

ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง มาตรฐานรัฐบาลดิจิทัลว่าด้วยหลักเกณฑ์การประเมินคุณภาพข้อมูลสาหรับหน่วยงานภาครัฐ (2566, 15 กุมภาพันธ์). ราชกิจจานุเบกษา. เล่ม 140 ตอนพิเศษ 69 ง.

ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง มาตรฐานและหลักเกณฑ์การเปิดเผยข้อมูลเปิดภาครัฐในรูปแบบข้อมูลดิจิทัลต่อสาธารณะ (2563, 24 มิถุนายน). ราชกิจจานุเบกษา. เล่ม 137 ตอนพิเศษ 148 ง.

ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่องมาตรฐานรัฐบาลดิจิทัลว่าด้วยแนวทางการจัดทาบัญชีข้อมูลภาครัฐและแนวทางการลงทะเบียนบัญชีข้อมูลภาครัฐ (2566, 15 กุมภาพันธ์). ราชกิจจานุเบกษา. เล่ม 140 ตอนพิเศษ 69 ง.

ประกาศสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ที่ 18 /2564 เรื่อง มาตรฐานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ว่าด้วยข้อเสนอแนะสำหรับการจัดทำนโยบายและแนวปฏิบัติการบริหารจัดการข้อมูล (2564, 26 ตุลาคม). สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน).

ประกาศสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ที่ 3 /2564 เรื่อง มาตรฐานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ว่าด้วยแนวทางการจัดทำบัญชีข้อมูลภาครัฐ (2564, 15 มีนาคม). สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน).

พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 (2549, 26 พฤศจิกายน). ราชกิจจานุเบกษา. เล่ม 128 ตอนที่ 4 ก.

พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 (2562, 19 พฤษภาคม).ราชกิจจานุเบกษา. เล่ม 136 ตอนที่ 67 ก.

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 (2562, 24 พฤษภาคม). ราชกิจจานุเบกษา.เล่ม 136 ตอนที่ 69 ก.

พระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. 2540 (2540, 2 กันยายน). ภูมิพลอดุลยเดช ป.ร..

พระราชบัญญัติข่าวกรองแห่งชาติ พ.ศ. 2562 (2562, 15 เมษายน). ราชกิจจานุเบกษา. เล่ม 136 ตอนที่ 50 ก.

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (2562, 27 พฤษภาคม). ราชกิจจานุเบกษา. เล่ม 136 ตอนที่ 69 ก.

ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 (2544, 5 กุมภาพันธ์). คณะรัฐมนตรี.