DATA GOVERNANCE

# DATA MANAGEMENT POLICY AND GUIDELINE

## นโยบายบริหารจัดการข้อมูล และแนวปฏิบัติการบริหารจัดการข้อมูล ของสำนักงานป้องกันและปราบปรามการฟอกเงิน

กุมภาพันธ์ 2568
ศูนย์เทคโนโลยีสารสนเทศ

# คำนำ

นโยบายการบริหารจัดการข้อมูล (Data Management Policy) และแนวปฏิบัติการบริหารจัดการข้อมูล (Data Management Guideline) ของสำนักงานป้องกันและปราบปรามการฟอกเงินฉบับนี้ จัดทำขึ้นเพื่อประมวลนโยบายและแนวปฏิบัติดังกล่าว รวมถึงประกาศที่เกี่ยวข้องให้อยู่ในรูปเล่มรายงานอิเล็กทรอนิกส์และเผยแพร่ตามข้อสั่งการเลขาธิการสำนักงานป้องกันและปราบปรามการฟอกเงิน ต่อผู้บริหารและหน่วยงานในสำนักงาน ปปง. รับทราบและถือปฏิบัติโดยเคร่งครัด

ศูนย์เทคโนโลยีสารสนเทศ สำนักงานป้องกันและปราบปรามการฟอกเงิน จึงได้ประมวลนโยบายและแนวปฏิบัติต่าง ๆ ที่เกี่ยวข้อง โดยมีโครงสร้างเนื้อหา ประกอบด้วย

1. นโยบายการบริหารจัดการข้อมูล (Data Management Policy)
2. แนวปฏิบัติการบริหารจัดการข้อมูล (Data Management Guideline)

<u>ประกาศที่เกี่ยวข้อง</u>

- ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง มาตรฐานรัฐบาลดิจิทัลว่าด้วยข้อเสนอแนะสำหรับการจัดทำนโยบายและแนวปฏิบัติการบริหารจัดการข้อมูล ลงวันที่ 15 กุมภาพันธ์ 2566
- ประกาศสำนักงานป้องกันและปราบปรามการฟอกเงิน เรื่อง นโยบายธรรมาภิบาลข้อมูลของสำนักงานป้องกันและปราบปรามการฟอกเงิน ลงวันที่ 26 กันยายน 2567
- คำสั่งสำนักงานป้องกันและปราบปรามการฟอกเงิน ที่ 352/2567 เรื่อง แต่งตั้งคณะกรรมการธรรมาภิบาลข้อมูลของสำนักงานป้องกันและปราบปรามการฟอกเงิน ลงวันที่ 8 สิงหาคม 2567
- หนังสือ ศท. ที่ ปง 0014.5/119 ลงวันที่ 17 กุมภาพันธ์ 2568 เรื่อง ขอความเห็นชอบนโยบายการบริหารจัดการข้อมูล และแนวปฏิบัติการบริหารจัดการข้อมูลของสำนักงานป้องกันและปราบปรามการฟอกเงิน

หวังว่ารายงานฉบับนี้ จะช่วยให้ผู้บริหารและเจ้าหน้าที่ของสำนักงานป้องกันและปราบปรามการฟอกเงิน ขับเคลื่อนด้านธรรมาภิบาลข้อมูลของสำนักงานป้องกันและปราบปรามการฟอกเงิน บรรลุผลตามตัวชี้วัดยุทธศาสตร์ 3.3.1 ระดับความสำเร็จของการดำเนินงานด้านธรรมาภิบาลข้อมูล (Data Governance) เพื่อสนับสนุนจัดทำฐานข้อมูลด้าน AML/CFT/CPF ภายใต้แผนยุทธศาสตร์และแผนปฏิบัติราชการ 5 ปี (พ.ศ. 2566 – 2570) ได้อย่างมีประสิทธิภาพยิ่งขึ้น

ส่วนนโยบายและแผนยุทธศาสตร์เทคโนโลยีสารสนเทศ
ศูนย์เทคโนโลยีสารสนเทศ
กุมภาพันธ์ 2568

# นโยบายการบริหารจัดการข้อมูล
# (Data Management Policy)
# สำนักงานป้องกันและปราบปรามการฟอกเงิน

| เวอร์ชัน | ผู้อนุมัติ | ลงนาม | วันที่อนุมัติ | วันที่มีผลบังคับใช้ |
|---|---|---|---|---|
| ๑.๐ | นายเทพสุ บวรโชติดารา |  | กุมภาพันธ์ ๒๕๖๘ | กุมภาพันธ์ ๒๕๖๘ |

**๑. วัตถุประสงค์**

๑) เพื่อให้การบริหารจัดการข้อมูลของสำนักงานป้องกันและปราบปรามการฟอกเงิน สอดคล้องกับกฎหมาย กรอบธรรมาภิบาลข้อมูลภาครัฐ และระเบียบปฏิบัติที่เกี่ยวข้อง

๒) เพื่อใช้เป็นกรอบและแนวทางในการบริหารจัดการข้อมูลของหน่วยงาน สำหรับผู้บริหาร เจ้าหน้าที่สำนักงานป้องกันและปราบปรามการฟอกเงิน และผู้ที่เกี่ยวข้อง

**๒. ขอบเขตและการบังคับใช้**

นโยบายการบริหารจัดการข้อมูลฉบับนี้ จัดทำโดยสำนักงานป้องกันและปราบปรามการฟอกเงิน มีผลบังคับใช้กับข้อมูลทั้งหมดที่อยู่ในความรับผิดชอบของ สำนักงานป้องกันและปราบปรามการฟอกเงิน โดยผู้ทำหน้าที่ดูแลข้อมูล ผู้ใช้ข้อมูล คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Committee) คณะทำงาน บริกรข้อมูล (Data Stewards) และบุคลากรอื่น ๆ ของหน่วยงาน มีหน้าที่โดยตรงที่จะต้องสนับสนุนดำเนินการและปฏิบัติตามนโยบายอย่างเคร่งครัด ผู้ใช้อื่นที่เกี่ยวข้องแต่ไม่มีหน้าที่ในการดูแลข้อมูลจะต้องให้ความร่วมมือในการดำเนินการตามนโยบายนี้ ผู้ฝ่าฝืนนโยบายนี้มีความผิดและจะต้องได้รับการดำเนินการตามระเบียบของหน่วยงาน

**๓. ข้อยกเว้น**

นโยบายนี้อาจมีการขยายผลหรือมีการยกเว้น โดยปฏิบัติตามขั้นตอนการยกเว้นนโยบายของรัฐด้านอื่น ๆ หรือนโยบายของหน่วยงานร่วมด้วย

**๔. บทบาทและความรับผิดชอบ**

๑) หัวหน้าหน่วยงานของรัฐหรือผู้ที่ได้รับมอบหมายต้องควบคุมและกำกับดูแลให้บุคลากรในหน่วยงานและผู้ที่เกี่ยวข้องดำเนินการตามนโยบายการบริหารจัดการข้อมูลอย่างเคร่งครัด

๒) ผู้บังคับบัญชา/ผู้ที่ได้รับมอบหมายต้องตรวจสอบให้แน่ใจว่าบุคลากรในหน่วยงานและบุคคลอื่น ๆ เช่น บริษัทหรือผู้รับจ้าง ที่ได้รับมอบหมายจากหน่วยงานให้ทำหน้าที่บริหารจัดการข้อมูลได้รับความรู้เกี่ยวกับนโยบายนี้อย่างเหมาะสม และนำนโยบายไปปฏิบัติตามอย่างมีประสิทธิภาพและประสิทธิผล เป็นต้น

๓) บุคลากรในหน่วยงานและบุคคลอื่น ๆ เช่น บริษัทหรือผู้รับจ้าง ที่ได้รับมอบหมายจากหน่วยงานให้ทำหน้าที่บริหารจัดการข้อมูลต้องปฏิบัติตามนโยบาย มาตรการ วิธีการ และแนวปฏิบัติต่าง ๆ ที่เกี่ยวข้องกับข้อมูลและระบบข้อมูลสารสนเทศที่หน่วยงานกำหนด เป็นต้น

๔) คณะกรรมการธรรมาภิบาลข้อมูล/คณะทำงานด้านข้อมูล/เจ้าของข้อมูลและผู้ดูแลข้อมูล ต้องปฏิบัติหน้าที่ที่ได้รับมอบหมายภายใต้นโยบายนี้ (รายละเอียดตามข้อ ๘. ข้อมูลเพิ่มเติม)

**๕. 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 ที่จำแนกแยกแยะโดยการจัดกลุ่มหรือจัดประเภทข้อมูลที่อยู่ในความครอบครองหรือควบคุมของหน่วยงาน

**ธรรมาภิบาลข้อมูลภาครัฐ** (Data Governance for Government) หมายความว่า การกำหนดสิทธิ หน้าที่ และความรับผิดชอบของผู้มีส่วนได้เสียในการบริหารจัดการข้อมูลทุกขั้นตอน เพื่อให้การได้มาและการนำไปใช้ข้อมูลของหน่วยงานภาครัฐถูกต้อง ครบถ้วน เป็นปัจจุบัน รักษาความเป็นส่วนตัวและสามารถเชื่อมโยงกันได้อย่างมีประสิทธิภาพและมั่นคงปลอดภัย

**หมวดหมู่ของข้อมูล** (Data Category) หมายความว่า ตามกรอบธรรมาภิบาลข้อมูลภาครัฐแบ่งออกได้เป็น ๔ หมวดหมู่ ได้แก่ ข้อมูลส่วนบุคคล ข้อมูลความมั่นคง ข้อมูลความลับทางราชการ และ ข้อมูลสาธารณะ

**การจัดชั้นความลับของข้อมูล** (Data Classification) หมายความว่า การกำหนดประเภทและข้อกำหนดของการจัดชั้นความลับของข้อมูล เพื่อกำหนดสิทธิในการเข้าถึงและสามารถนำข้อมูลไปใช้ได้อย่างเหมาะสม ซึ่งตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ กำหนดให้มีชั้นความลับเป็น ชั้นลับ ชั้นลับมาก หรือ ชั้นลับที่สุด โดยคำนึงถึงการปฏิบัติหน้าที่ของหน่วยงานและประโยชน์แห่งรัฐประกอบกัน 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 เป็นข้อมูลที่สร้างและถูกใช้งานอยู่ภายในหน่วยงาน มีโอกาสเปลี่ยนแปลงได้และมีรายละเอียดหรือจำนวนฟิลด์ข้อมูลที่มาก เช่น ข้อมูลพนักงาน ข้อมูลลูกค้า ข้อมูลผู้ขาย ข้อมูลสินค้าและบริการ ข้อมูลครุภัณฑ์ และข้อมูลสถานที่ เป็นต้น ในขณะที่ Reference data มีความเป็นสากลถูกสร้างและใช้งานโดยทั่วไป โดยหลากหลายองค์กรหรือแม้กระทั่งใช้งานไปทั่วโลก เช่น รหัสไปรษณีย์ รหัสประเทศ หน่วยวัดระยะทาง เป็นต้น

**๖. นโยบายการบริหารจัดการข้อมูล**

**ข้อกำหนดทั่วไป**

๑) กำหนดบทบาท หน้าที่ และความรับผิดชอบของแต่ละบุคคลตามโครงสร้างธรรมาภิบาลข้อมูลภาครัฐ โดยต้องได้รับการมอบอำนาจและการอนุมัติจากผู้บริหาร พร้อมทั้งกำหนดหน่วยงานเจ้าของข้อมูลเพื่อทำหน้าที่ในการบริหารจัดการข้อมูลนั้น ๆ

๒) จัดทำนโยบายการบริหารจัดการข้อมูลเป็นลายลักษณ์อักษร อนุมัติเผยแพร่เพื่อประกาศใช้ และถือปฏิบัติโดยให้มีผลบังคับใช้กับบุคลากรในหน่วยงาน ตลอดจนหน่วยงาน/บุคคลภายนอกที่เกี่ยวข้องกับการได้มาและการใช้ข้อมูลของหน่วยงาน พร้อมทั้งจัดทำแนวปฏิบัติและมาตรฐานที่เกี่ยวกับข้อมูลเพื่อสนับสนุนการปฏิบัติงานให้สอดคล้องตามนโยบายดังกล่าว

๓) กำหนดมาตรการ วิธีการ และแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของข้อมูล เพื่อป้องกันการละเมิด การเข้าถึง การสูญหาย การทำลาย หรือการเปลี่ยนแปลงข้อมูล โดยปราศจากอำนาจโดยมิชอบหรือโดยมิได้รับอนุญาต

๔) กำหนดมาตรการ วิธีการ และแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลที่สอดคล้องกับกฎหมายระเบียบ และแนวปฏิบัติของหน่วยงาน

๕) ตรวจสอบความมีอยู่และรายละเอียดของข้อมูลที่สำคัญ เช่น คำอธิบายข้อมูลหรือเมทาดาตา ชุดข้อมูล การจัดชั้นความลับข้อมูล และรายงานผลให้แก่ผู้รับผิดชอบตามโครงสร้างธรรมาภิบาลข้อมูลภาครัฐและดำเนินการตามกระบวนการธรรมาภิบาลข้อมูลภาครัฐ เป็นต้น

๖) ตรวจสอบ ติดตาม และประเมินผลการปฏิบัติตามนโยบายการบริหารจัดการข้อมูลโดยผู้ตรวจประเมินที่คณะกรรมการธรรมาภิบาลข้อมูลของสำนักงานป้องกันและปราบปรามการฟอกเงินกำหนด พร้อมทั้งกำหนดให้มีการทบทวนนโยบาย รวมถึงมาตรการ วิธีการ และแนวปฏิบัติต่าง ๆ เกี่ยวกับข้อมูล อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญตามความเหมาะสม

๗) ตรวจสอบ ติดตาม และประเมินผลการดำเนินงานธรรมาภิบาลข้อมูลของหน่วยงานอย่างน้อยปีละ ๑ ครั้ง ในเรื่อง (๑) การประเมินความพร้อมธรรมาภิบาลข้อมูล (๒) การประเมินคุณภาพข้อมูล และ (๓) การประเมินความมั่นคงปลอดภัยของข้อมูล เป็นอย่างน้อย

๘) จัดให้มีทรัพยากรด้านงบประมาณ ทรัพยากรบุคคล และเทคโนโลยีที่เพียงพอต่อการบริหารจัดการข้อมูล พร้อมทั้งสนับสนุนการฝึกอบรมธรรมาภิบาลข้อมูลภาครัฐและการบริหารจัดการข้อมูลให้ครอบคลุมทั้งวงจรชีวิตของข้อมูลแก่บุคลากรในหน่วยงาน อย่างน้อยปีละ ๑ ครั้ง

**การจัดหมวดหมู่และชั้นความลับของข้อมูล**

๑) กำหนดหมวดหมู่และประเภทชั้นความลับของข้อมูลที่ใช้กับข้อมูลทุกรูปแบบของหน่วยงาน ทั้งเอกสารกระดาษและข้อมูลดิจิทัล ด้วยการประเมินผลกระทบของข้อมูลหน่วยงาน เพื่อระบุหมวดหมู่และประเภทชั้นความลับของข้อมูล รวมทั้งกำหนดระดับความปลอดภัยที่เหมาะสมสำหรับการสร้าง/จัดเก็บ การใช้และการเข้าถึงชุดข้อมูล และเพื่อใช้กับบุคลากรรวมถึงตัวแทนบุคคลที่สามที่ได้รับอนุญาตให้เข้าถึงข้อมูลในหน่วยงาน พร้อมทั้งกำหนดบทบาทหน้าที่ของบุคลากรในการจัดหมวดหมู่และชั้นความลับ เพื่อป้องกันจัดการ และกำกับดูแลข้อมูลให้เหมาะสม

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

๓) กำกับดูแลและติดตามอย่างต่อเนื่อง โดยตรวจสอบความปลอดภัยการใช้งานและรูปแบบการเข้าถึงของระบบและข้อมูล ทั้งผ่านกระบวนการอัตโนมัติหรือโดยบุคคล เพื่อระบุภัยคุกคามภายนอก การบำรุงรักษาการทำงานของระบบตามปกติ และการติดตั้งโปรแกรมเพื่อปรับปรุงและติดตามการเปลี่ยนแปลงของสภาพแวดล้อมของระบบและข้อมูล

**การบริหารจัดการข้อมูลตามวงจรชีวิตของข้อมูล**

๑) กำหนดนโยบาย แนวปฏิบัติ และสภาพแวดล้อมการบริหารจัดการข้อมูลตามวงจรชีวิตของข้อมูลที่เอื้อต่อการรักษาความมั่นคงปลอดภัย คุ้มครองความเป็นส่วนตัวของข้อมูล และเพื่อให้ได้ข้อมูลที่มีคุณภาพ

๒) จัดทำแนวปฏิบัติการจัดการชุดข้อมูล รวมถึงการรักษาความปลอดภัยตามหมวดหมู่และประเภทชั้นความลับตามแนวทางที่เหมาะสม และปรับปรุงอย่างต่อเนื่องให้สอดคล้องกับสถานการณ์

๓) จัดเก็บข้อมูลให้สอดคล้องกับแนวทางหรือมาตรฐานการจัดชั้นความลับของข้อมูลที่กำหนดไว้ โดยข้อมูลต้องมีความถูกต้อง สมบูรณ์ และเป็นปัจจุบัน พร้อมทั้งกำหนดสิทธิและจัดหาระบบ/เครื่องมือที่ใช้ในการเข้าถึงข้อมูลเพื่อรักษาความมั่นคงปลอดภัยและคุณภาพข้อมูล และทำลายข้อมูลตามแนวปฏิบัติและกฎหมายที่เกี่ยวข้อง

๔) จัดทำแนวปฏิบัติและมาตรฐานการประมวลผลและใช้ข้อมูล เพื่อผู้ใช้นำข้อมูลไปใช้อย่างถูกต้องตามวัตถุประสงค์ที่ต้องการเพื่อให้เกิดประโยชน์สูงสุด

๕) ห้ามเปิดเผยข้อมูลที่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง นโยบาย และแนวปฏิบัติ ไม่ว่าข้อมูลจะอยู่ในรูปแบบใดหรือสถานที่ใดก็ตาม และต้องได้รับการอนุญาตจากตัวแทนหน่วยงานหรือเจ้าของข้อมูลก่อนการเปิดเผยข้อมูล รวมทั้ง จัดให้มีช่องทางการเปิดเผยข้อมูลที่เข้าถึงและนำไปใช้ได้ง่าย

๖) กำหนดกระบวนการ เทคโนโลยี และมาตรฐานทางเทคนิคที่ใช้ในการแลกเปลี่ยนข้อมูล และจัดทำสัญญาอนุญาตหรือข้อตกลงในการแลกเปลี่ยนข้อมูลและการนำข้อมูลไปใช้

๗) จัดทำแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัย ด้านคุณภาพข้อมูล และด้านคุ้มครองความเป็นส่วนตัวของข้อมูล รวมถึงแนวปฏิบัติให้กับผู้ประสานงานหรือศูนย์ติดต่อ (Contact Center) และตรวจสอบให้แน่ใจว่าได้บริหารจัดการข้อมูลอย่างเหมาะสมตามแนวทางหรือแนวปฏิบัติที่กำหนดไว้

๘) สร้างความรู้ความเข้าใจในการบริหารจัดการข้อมูลตามวงจรชีวิตของข้อมูล ให้แก่ผู้เกี่ยวข้องทั้งภายในและภายนอกหน่วยงาน

**คุณภาพข้อมูล**

๑) กำหนดนโยบายการจัดการคุณภาพข้อมูล เพื่อใช้เป็นกรอบแนวทางในการจัดการข้อมูลของหน่วยงานให้มีคุณภาพเป็นตามเกณฑ์หรือคุณสมบัติที่กำหนด เช่น ความถูกต้องสมบูรณ์ ความสอดคล้องกัน (Consistency) ความเป็นปัจจุบัน ตรงตามความต้องการใช้งาน และความพร้อมใช้ เป็นต้น โดยผู้ดูแลข้อมูลมีหน้าที่จัดการและกำกับดูแลข้อมูลให้มีคุณภาพเพื่อสร้างความมั่นใจให้กับผู้ใช้ข้อมูล ในขณะที่ผู้ใช้ข้อมูลมีบทบาทในการให้ข้อเสนอแนะแก่ผู้ดูแลข้อมูลเพื่อการปรับปรุงคุณภาพให้ดียิ่งขึ้น

๒) จัดทำเกณฑ์คุณภาพข้อมูลที่สามารถวัดผลได้ พร้อมทั้งจัดทำแผนพัฒนาคุณภาพข้อมูลที่สามารถระบุตัวชี้วัดคุณภาพและแผนปฏิบัติการเพื่อจัดการคุณภาพข้อมูลได้อย่างมีประสิทธิภาพ โดยออกแบบการเก็บรวบรวมข้อมูลเพื่อให้ได้ข้อมูลสำหรับประเมินคุณภาพตามเกณฑ์ดังกล่าวให้รวมอยู่ในระบบเทคโนโลยีสารสนเทศและกระบวนการทำงาน (Quality by design) เพื่อลดข้อผิดพลาดและปรับปรุงคุณภาพตั้งแต่จุดการป้อนข้อมูลหรือการสร้างข้อมูลไปจนถึงการประมวลผลข้อมูล

๓) ประเมินผลและจัดการคุณภาพข้อมูลอย่างสม่ำเสมอตลอดวงจรชีวิตของข้อมูล โดยเจ้าของข้อมูลและบริกรข้อมูลควรกำหนดกรอบคุณภาพข้อมูลเฉพาะหมวดหมู่ข้อมูลหรือโดเมน (Domain) เช่น Quality Assurance Framework of the European Statistical System (ESS. QAF) ที่เป็นกรอบคุณภาพข้อมูลสถิติของ the European Statistical System ที่สามารถนำมาใช้อ้างอิงได้ เป็นต้น

๔) พัฒนากระบวนการหรือกลไกให้ผู้ใช้สามารถให้ข้อเสนอแนะหรือ Feedback เพื่อรายงานปัญหาให้กับเจ้าของข้อมูลโดยเฉพาะข้อมูลสำคัญ เช่น ข้อมูลหลัก (Master data) และข้อมูลอ้างอิง (Reference data) เป็นต้น

**๗. ข้อกฎหมายและเอกสารอ้างอิง**

๑) ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ และที่แก้ไขเพิ่มเติม

๒) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

๓) ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ

๔) ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง มาตรฐานและหลักเกณฑ์การเปิดเผยข้อมูลเปิดภาครัฐในรูปแบบข้อมูลดิจิทัลต่อสาธารณะ

๕) ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง มาตรฐานรัฐบาลดิจิทัลว่าด้วยแนวทางการจัดทำบัญชีข้อมูลภาครัฐ (มรด. ๓-๑:๒๕๖๕)

๖) ประกาศสำนักงานป้องกันและปราบปรามการฟอกเงิน เรื่อง นโยบายธรรมาภิบาลข้อมูลของสำนักงานป้องกันและปราบปรามการฟอกเงิน

**๘. ข้อมูลเพิ่มเติม**

๑) บทบาทและความรับผิดชอบของผู้มีส่วนเกี่ยวข้อง

| บทบาท | ความรับผิดชอบ |
|---|---|
| คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Committee) | ● มีอำนาจสูงสุดในธรรมาภิบาลข้อมูลภายในหน่วยงาน ทำหน้าที่ตัดสินใจเชิงนโยบาย แก้ไขปัญหา และบริหารจัดการข้อมูลของหน่วยงาน ทั้งนี้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงอาจจะทำหน้าที่แทนผู้บริหารข้อมูลระดับสูง |
| บริกรข้อมูลด้านธุรกิจ (Business Data Stewards) | ● นิยามความต้องการด้านคุณภาพและความมั่นคงปลอดภัย<br>● นิยามเมทาดาตา (Metadata)<br>● ร่างนโยบายข้อมูล มาตรฐาน และแนวปฏิบัติต่าง ๆ ที่เกี่ยวข้องกับข้อมูล<br>● ตรวจสอบการปฏิบัติตามนโยบายข้อมูล ตรวจสอบคุณภาพ ตรวจสอบความมั่นคงปลอดภัยของข้อมูล วิเคราะห์ผลจากการตรวจสอบ |
| บริกรข้อมูลด้านเทคนิค (Technical Data Stewards) | ● ให้การสนับสนุนด้านเทคโนโลยีสารสนเทศแก่บริกรข้อมูล<br>● รักษา และดูแลข้อมูลที่อยู่บนระบบเทคโนโลยีสารสนเทศต่าง ๆ ในหน่วยงาน |
| บริกรข้อมูลด้านคุณภาพข้อมูล (Data Quality Stewards) | ● ดำเนินการในเรื่องคุณภาพข้อมูล เช่น กำหนดนโยบายข้อมูลด้านคุณภาพ การตรวจวัดคุณภาพข้อมูล และการวิเคราะห์คุณภาพข้อมูล |
| ทีมบริหารจัดการข้อมูล (Data Management Team) | ● บริหารจัดการข้อมูลให้เป็นไปตามองค์ประกอบในการบริหารจัดการข้อมูล |
| เจ้าของข้อมูล (Data Owner) | ● ตรวจสอบ ดูแล และรักษาคุณภาพของข้อมูล<br>● ทบทวนและอนุมัติการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับข้อมูล |
| ผู้สร้างข้อมูล (Data Creator) | ● บันทึก แก้ไข ปรับปรุง หรือลบข้อมูลให้สอดคล้องกับโครงสร้างที่ถูกกำหนดไว้<br>● ทำงานร่วมกับบริกรข้อมูล เพื่อตรวจสอบและแก้ไขปัญหาด้านคุณภาพข้อมูลและความปลอดภัยของข้อมูล |
| ผู้บริหารจัดการฐานข้อมูล (Database Administrator) | ● บริหารจัดการ และควบคุมเกี่ยวกับระบบฐานข้อมูลภายในหน่วยงาน<br>● กำหนดนโยบาย มาตรการ และมาตรฐานของระบบฐานข้อมูล ทั้งหมดภายในหน่วยงาน เช่น รายละเอียดและวิธีการจัดเก็บข้อมูล การใช้งานฐานข้อมูล การรักษาความปลอดภัยของข้อมูล การสำรองข้อมูล การกู้คืนข้อมูล เป็นต้น |

| บทบาท | ความรับผิดชอบ |
|---|---|
| ผู้ใช้ข้อมูล (Data User) | ● นำข้อมูลไปใช้งานทั้งในระดับปฏิบัติงานและระดับบริหาร<br>● สนับสนุนการกำกับดูแลข้อมูล<br>● รายงานประเด็นปัญหาที่พบระหว่างการใช้ข้อมูล |

๒) ความสัมพันธ์ระหว่างกระบวนการ/กิจกรรมและผู้มีส่วนได้ส่วนเสีย

| กิจกรรม | ผู้มีส่วนได้ส่วนเสีย | | | | | |
|---|---|---|---|---|---|---|
| | คณะกรรมการธรรมาภิบาลข้อมูล | ทีมบริกรข้อมูล | เจ้าของข้อมูล | ผู้สร้างข้อมูล | ทีมบริหารจัดการข้อมูล | ผู้ใช้ข้อมูล |
| ๑. ประเมินความพร้อมของธรรมาภิบาลข้อมูลของหน่วยงาน | I | A/R | S/C | S | R | S |
| ๒. กำหนดนโยบายและแนวทางปฏิบัติการบริหารจัดการข้อมูลของหน่วยงาน | A | R | S | I | I | I |
| ๓. ตรวจสอบการปฏิบัติตามนโยบายและแนวทางปฏิบัติการบริหารจัดการข้อมูลของหน่วยงาน | I | A/R | R | S | R | S |
| ๔. ประเมินและวัดผลข้อมูลของหน่วยงาน | I | R | S | S | S | S |
| ๕. รายงานผลการดำเนินงานต่อคณะกรรมการธรรมาภิบาลข้อมูล | I | A/R | I | I | I | I |
| ๗. ทบทวนและปรับปรุงนโยบายและแนวทางปฏิบัติการบริหารจัดการข้อมูลของหน่วยงาน ในภาพรวม | 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

# แนวปฏิบัติการบริหารจัดการข้อมูล
# (Data Management Guideline)
## สำนักงานป้องกันและปราบปรามการฟอกเงิน

จัดทำโดย
ศูนย์เทคโนโลยีสารสนเทศ

# การอนุมัติเอกสาร

| ชื่อเอกสาร | | | |
|---|---|---|---|
| แนวปฏิบัติการบริหารจัดการข้อมูล | | | เวอร์ชัน ๑.๐ |
| **การอนุมัติ** | **ชื่อ - สกุล** | **ตำแหน่ง** | **ลงนาม** |
| **ผู้อนุมัติ** | นายเทพสุ บวรโชติดารา | เลขาธิการคณะกรรมการป้องกันและปราบปรามการฟอกเงิน | |
| **ผู้ตรวจสอบ** | นายศิวัช ชาวบางงาม | ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ | |
| **ผู้จัดทำ** | นายวีรยุทธ เจริญสุวรรณกิจ | ผู้อำนวยการส่วนนโยบายและแผนยุทธศาสตร์เทคโนโลยีสารสนเทศ | |
| | นางสาวกุลนันทน์ ศรีเจริญ | นักวิชาการคอมพิวเตอร์ชำนาญการ | |
| | นายสุเมธ วนาลีสุขสันต์ | นักวิชาการคอมพิวเตอร์ชำนาญการ | สุเมธ |
| **วันที่อนุมัติ** | กุมภาพันธ์ ๒๕๖๘ | **วันที่บังคับใช้** | กุมภาพันธ์ ๒๕๖๘ |

# บันทึกประวัติการแก้ไขเอกสาร

| ครั้งที่แก้ไข | วันที่แก้ไข | รายการเปลี่ยนแปลง | ผู้จัดทำ |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

# สารบัญ

หน้า

# บทนำ

**หลักการและขอบเขต**

แนวปฏิบัติการบริหารจัดการข้อมูล ได้กำหนดขึ้นให้สอดคล้องตามนโยบายข้อมูล (Data Policy) ซึ่งเป็นหนึ่งในองค์ประกอบตามกรอบธรรมาภิบาลข้อมูลภาครัฐ จัดทำโดยศูนย์เทคโนโลยีสารสนเทศ สำนักงานป้องกันและปราบปรามการฟอกเงิน มีผลบังคับใช้กับผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับข้อมูลตามแนวปฏิบัติการบริหารจัดการข้อมูลที่สำนักงานป้องกันและปราบปรามการฟอกเงินประกาศ ซึ่งมีหน้าที่โดยตรงที่จะต้องสนับสนุน ดำเนินการและปฏิบัติตามอย่างเคร่งครัด และผู้ใช้อื่นที่เกี่ยวข้องแต่ไม่มีหน้าที่ในการดูแลข้อมูลจะต้องให้ความร่วมมือในการดำเนินการตามแนวปฏิบัตินี้ ผู้ฝ่าฝืนมีความผิดและจะต้องได้รับการดำเนินการตามระเบียบของหน่วยงาน โดยแนวปฏิบัติดังกล่าวจะต้องครอบคลุมระบบบริหารและกระบวนการจัดการข้อมูล หรือวงจรชีวิตของข้อมูลและองค์ประกอบในการบริหารจัดการข้อมูล ดังรูปต่อไปนี้

**วงจรชีวิตของข้อมูล**


ที่มา : ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัลเรื่อง ธรรมาภิบาลข้อมูลภาครัฐ

**๑. การสร้างข้อมูล (Create)** เป็นการสร้างข้อมูลขึ้นมาใหม่ หรือปรับปรุงข้อมูลขึ้นใหม่ โดยวิธีการบันทึกเข้าไปด้วยบุคคลหรือบันทึกอัตโนมัติด้วยอุปกรณ์อิเล็กทรอนิกส์ เช่น อุปกรณ์ตรวจจับสัญญาณ (Sensor) เป็นต้น รวมถึงการซื้อข้อมูล หรือการรับข้อมูลจากหน่วยงานอื่น เพื่อนำมาจัดเก็บในภายหลัง

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

**๓. การประมวลผลและใช้ข้อมูล (Processing and Use)** เป็นการนำข้อมูลที่จัดเก็บมาประมวลผล เช่น การถ่ายโอนข้อมูล การเปลี่ยนรูปแบบการจัดเก็บข้อมูล การวิเคราะห์ข้อมูล การจัดทำรายงาน เป็นต้น

เพื่อนำข้อมูลเหล่านั้นมาใช้งานให้เกิดประโยชน์ตามวัตถุประสงค์ รวมถึง การสำรองข้อมูล (Backup) โดยการคัดลอกข้อมูลที่ใช้งานอยู่ในปัจจุบัน เพื่อทำสำเนา เช่น ใช้โปรแกรมในการสำรองข้อมูล เป็นต้น เป็นการหลีกเลี่ยงความเสียหายที่จะเกิดขึ้นหากข้อมูลเกิดการเสียหายหรือสูญหาย ซึ่งสามารถนำข้อมูลที่สำรองไว้ในสื่อบันทึกข้อมูลกลับมาใช้งานได้ทันที โดยการกู้คืน (Restore)

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

**๕. กระบวนการจัดเก็บข้อมูลถาวร (Archive)** เป็นการย้ายข้อมูลที่มีช่วงอายุเกินช่วงใช้งานหรือไม่ได้ใช้งานแล้ว เพื่อเก็บรักษาถาวรโดยที่ข้อมูลนั้นไม่มีการลบ ปรับปรุง หรือแก้ไขอีก และสามารถนำกลับไปใช้งานได้ใหม่เมื่อต้องการ

**๖. การทำลายข้อมูล (Destroy)** เป็นการทำลายข้อมูลที่มีการจัดเก็บถาวรเป็นระยะเวลานานหรือเกินกว่าระยะเวลาที่กำหนด

**๗. การเชื่อมโยงและแลกเปลี่ยนข้อมูล (Linkage and Exchange)** การเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงานทั้งภายในและภายนอกให้มีความมั่นคงปลอดภัยและข้อมูลมีคุณภาพ สามารถนำไปใช้ประโยชน์ได้อย่างมีประสิทธิภาพ

**หมวดหมู่และการจัดระดับชั้นของข้อมูล**

ข้อมูลของหน่วยงานสามารถแบ่งหมวดหมู่ตามกรอบธรรมาภิบาลข้อมูลและการใช้งานภายในได้ ดังนี้

๑. ข้อมูลสาธารณะ
๒. ข้อมูลส่วนบุคคล
๓. ข้อมูลความมั่นคง
๔. ข้อมูลความลับทางราชการ
๕. ข้อมูลใช้ภายในหน่วยงาน (ที่ยังไม่แบ่งหมวดหมู่)

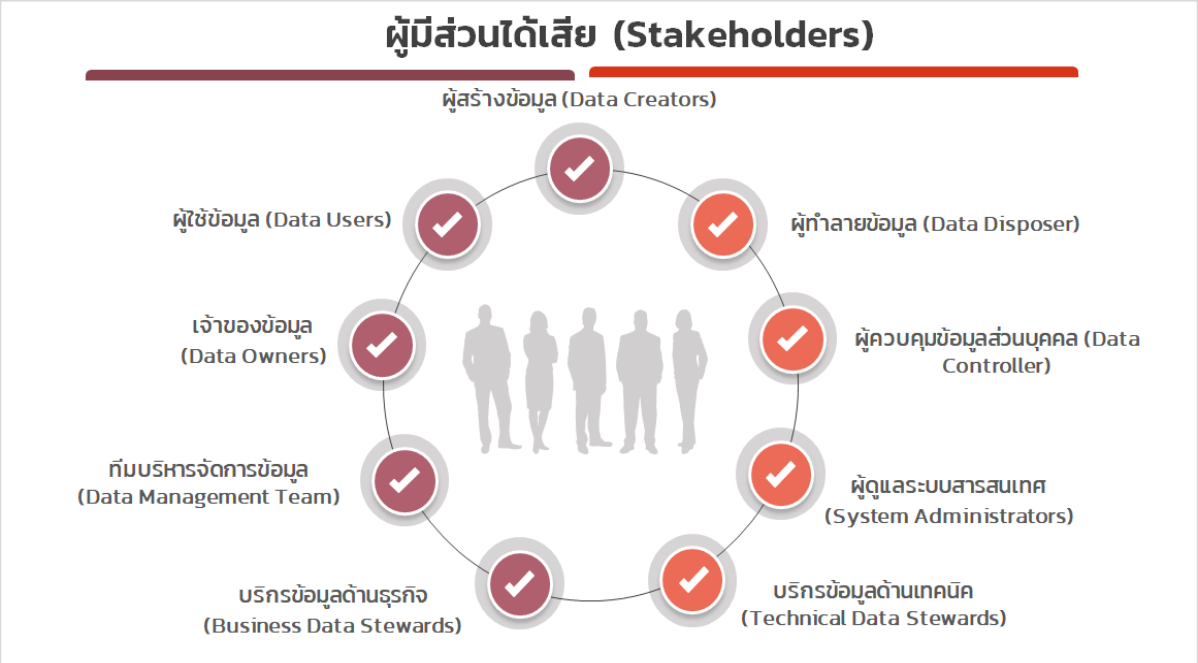
โดยมีการจัดระดับชั้นความลับของข้อมูลดังภาพ โดยสรุปได้ดังนี้

- ข้อมูลใช้ภายใน (Internal Use Only) ได้แก่ ข้อมูลสำหรับใช้ในการดำเนินกิจการภายในของหน่วยงาน ซึ่งไม่อนุญาตให้นำไปใช้งานภายนอกก่อนได้รับอนุญาต เช่น นโยบาย มาตรฐาน และขั้นตอนการปฏิบัติงาน ประกาศ และบันทึกภายในหน่วยงาน เป็นต้น
- ข้อมูลที่มีชั้นความลับ (Secret) แบ่งเป็น ข้อมูลลับที่สุด (Top Secret) ข้อมูลลับมาก (Secret) และ ข้อมูลลับ (Confidential)
- ข้อมูลเปิดเผยได้ (Public) ได้แก่ ข้อมูลที่สามารถเปิดเผยได้แก่บุคคลทั่วไป เช่น ข้อมูลเผยแพร่บนเว็บไซต์ ข้อมูลจากการแถลงข่าว หรือรายงานประจำปีของหน่วยงาน เป็นต้น


**ผู้เกี่ยวข้อง**

แนวปฏิบัติเกี่ยวกับข้อมูลนี้บังคับใช้กับผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับข้อมูลตามประกาศแนวปฏิบัติการกำกับดูแลและบริหารจัดการข้อมูลของหน่วยงาน รวมถึงผู้เกี่ยวข้องอื่น ๆ ที่ไม่ได้ระบุไว้ใน แนวปฏิบัติ 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** | สำนักงานป้องกันและปราบปรามการฟอกเงิน |
| **คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Committee)** | คณะกรรมการธรรมาภิบาลข้อมูลของสำนักงานป้องกันและปราบปรามการฟอกเงิน มีอำนาจสูงสุดในธรรมาภิบาลข้อมูลภายในหน่วยงาน ซึ่งทำหน้าที่ตัดสินใจเชิงนโยบาย แก้ไขปัญหา และบริหารจัดการข้อมูลของหน่วยงาน ประกอบไปด้วย ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer) ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer) ผู้บริหารจากส่วนงานต่าง ๆ ทั้งจากฝ่ายบริหารและฝ่ายเทคโนโลยีสารสนเทศ รวมไปถึงหัวหน้าทีมบริกรข้อมูล (Lead Data Steward) |
| **หัวหน้าหน่วยงานของรัฐ** | เลขาธิการคณะกรรมการป้องกันและปราบปรามการฟอกเงิน |
| **ผู้บริหาร** | ผู้บริหารที่เกี่ยวข้องกับการบริหารจัดการข้อมูล ตามคณะกรรมการ/คณะทำงานที่เกี่ยวข้อง |
| **ข้าราชการ/เจ้าหน้าที่/พนักงาน** | บุคคลผู้ที่หน่วยงานบรรจุและแต่งตั้งเป็นเจ้าหน้าที่ของหน่วยงาน |
| **ลูกจ้าง** | บุคคลผู้ที่หน่วยงานบรรจุและแต่งตั้งเป็นลูกจ้าง โดยมีสัญญาจ้างให้ปฏิบัติงานเป็นการชั่วคราวและมีกำหนดระยะเวลาและสิ้นสุดที่แน่นอน |
| **ผู้บังคับบัญชา** | ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของสำนักงาน |
| **ผู้สร้างข้อมูล (Data Creators)** | บุคลากรจากกอง/ศูนย์/กลุ่ม/สำนักของสำนักงานป้องกันและปราบปรามการฟอกเงิน ที่ทำหน้าที่บันทึก แก้ไข ปรับปรุง หรือลบข้อมูลให้สอดคล้องกับโครงสร้างที่ถูกกำหนดไว้ |
| **ผู้ใช้ข้อมูล (Data Users)** | คณะกรรมการ ผู้อำนวยการ ข้าราชการ/เจ้าหน้าที่/พนักงาน ลูกจ้าง รวมถึงหน่วยงานภายนอกที่ได้รับอนุญาต (Authorized Users) ให้สามารถเข้าใช้ข้อมูลของหน่วยงานตามสิทธิและหน้าที่ความรับผิดชอบ พร้อมทั้งรายงานประเด็นปัญหาที่พบระหว่างการใช้ข้อมูล |
| **สิทธิของผู้ใช้งานข้อมูล** | - สิทธิและหน้าที่ตามบทบาท (Role) ที่เกี่ยวข้องกับข้อมูลและระบบสารสนเทศของหน่วยงาน มีดังนี้<br>- สิทธิใช้งานทั่วไป หมายถึง คณะกรรมการ ผู้อำนวยการ ข้าราชการ/เจ้าหน้าที่/พนักงาน ลูกจ้าง ที่ใช้งานระบบสารสนเทศพื้นฐานของสำนักงาน ผู้ใช้งานข้อมูลต้องขออนุญาตจาก ผู้บังคับบัญชา โดยให้ใช้แบบฟอร์มเพื่อขออนุมัติตามที่หน่วยงานกำหนด<br>- สิทธิจำเพาะ หมายถึง สิทธิเฉพาะตามหน้าที่ความรับผิดชอบที่เกี่ยวข้องกับการปฏิบัติงาน ผู้ใช้งานข้อมูลต้องได้รับสิทธิจากผู้บังคับบัญชา<br>- สิทธิพิเศษ หมายถึง สิทธิที่ได้รับมอบหมายเพิ่มเติมจากผู้บังคับบัญชาเป็นกรณีพิเศษ ผู้ใช้งานต้องได้รับมอบหมายจากผู้บังคับบัญชาเป็นครั้งคราว |
| **เจ้าของข้อมูล (Data Owner)** | ผู้ที่ได้รับมอบหมายในการปฏิบัติงานให้รับผิดชอบข้อมูลที่ระบุไว้ ซึ่งรวมถึงผู้บังคับบัญชาของเจ้าของข้อมูลนั้นด้วย โดยทำหน้าที่กำกับดูแลตามธรรมาภิบาลข้อมูลตลอดวงจรชีวิตของข้อมูลนั้น ๆ รวมทั้งทำหน้าที่กำหนดสิทธิในการเข้าถึงข้อมูลและจัดชั้นความลับของข้อมูล |

| คำศัพท์ | ความหมาย |
|---|---|
| **เจ้าของข้อมูลส่วนบุคคล (Data Subject)** | บุคคลธรรมดาที่ข้อมูลส่วนบุคคลเกี่ยวกับบุคคลนั้นระบุถึง |
| **เจ้าของระบบงาน (System Owner)** | ผู้ที่มีหน้าที่รับผิดชอบในการใช้งาน ดูแลและบำรุงรักษา หรือปรับปรุงระบบงานที่ใช้ในหน่วยงาน |
| **ทีมบริหารจัดการข้อมูล (Data Management Team)** | กลุ่มบุคคลภายในฝ่ายเทคโนโลยีสารสนเทศของหน่วยงานที่ทำหน้าที่รับผิดชอบดูแลรักษาข้อมูลในระบบสารสนเทศของหน่วยงาน และสนับสนุนกิจกรรมของธรรมาภิบาลข้อมูลภาครัฐ เช่น ช่วยเหลือในการนิยาม Metadata ร่างนโยบายข้อมูลและมาตรฐานข้อมูล และกำหนดสิทธิการเข้าถึงข้อมูลโดย DBA เป็นต้น |
| **บริกรข้อมูลด้านธุรกิจ (Business Data Stewards)** | บุคลากรระดับหัวหน้ากลุ่ม/ส่วนงานจากทุกกอง/ศูนย์/กลุ่ม/สำนักของสำนักงานป้องกันและปราบปรามการฟอกเงิน ที่ได้รับมอบหมายให้ทำหน้าที่กำหนดนิยามความต้องการด้านคุณภาพและความมั่นคงปลอดภัยซึ่งอาจจะได้รับมาจากผู้ใช้ข้อมูล (Data Users) หรือผู้มีส่วนได้เสียอื่น ๆ นิยามคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตาโดยการสนับสนุนจากผู้ใช้ข้อมูล ร่างนโยบายข้อมูลด้วยการช่วยเหลือจากทีมบริหารจัดการข้อมูล (Data Management Team) ตรวจสอบการปฏิบัติตามนโยบายข้อมูล ตรวจสอบคุณภาพ ตรวจสอบความมั่นคงปลอดภัยของข้อมูล วิเคราะห์ผลจากการตรวจสอบ แล้วรายงานผลลัพธ์ไปยังคณะกรรมการธรรมาภิบาลข้อมูลและผู้ที่เกี่ยวข้องอื่น ๆ ให้ทราบ |
| **บริกรข้อมูลด้านเทคนิค (Technical Data Stewards)** | บุคลากรจากศูนย์เทคโนโลยีสารสนเทศ ที่ทำหน้าที่ให้การสนับสนุนด้านเทคโนโลยีสารสนเทศแก่บริกรข้อมูลด้านธุรกิจ เช่น นิยาม Metadata เชิงเทคนิค ซึ่งอาจจะได้รับการช่วยเหลือจากทีมบริหารจัดการข้อมูล ให้ข้อเสนอแนะเชิงเทคนิคในการร่างนโยบายข้อมูล ตรวจสอบคุณภาพข้อมูล ความมั่นคงปลอดภัยของข้อมูล และการปฏิบัติตามนโยบายข้อมูลในเชิงเทคนิค |
| **ผู้ดูแลระบบสารสนเทศ (System Administrators)** | บุคลากรของศูนย์เทคโนโลยีสารสนเทศ ที่มีหน้าที่ดูแลรับผิดชอบระบบสารสนเทศของหน่วยงาน |
| **ผู้ดูแลระบบแม่ข่าย (Server Administrators)** | บุคลากรที่มีหน้าที่ดูแลรับผิดชอบระบบแม่ข่ายของหน่วยงาน |
| **ผู้จัดการโครงการ (Project Managers)** | บุคลากรจากกอง/ศูนย์/กลุ่ม/สำนักของสำนักงานป้องกันและปราบปรามการฟอกเงิน ของหน่วยงานหลักที่ได้รับมอบหมายบริหารจัดการโครงการตามแผนดำเนินงาน |
| **ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)** | บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจ เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล |
| **ผู้ทำลายข้อมูล (Data Disposer)** | บุคลากรที่ได้รับการกำหนดสิทธิจากเจ้าของข้อมูลให้มีสิทธิในการทำลายข้อมูล |

| คำศัพท์ | ความหมาย |
|---|---|
| **ข้อมูล (Data)** | สิ่งที่สื่อความหมายให้รู้เรื่องราวข้อเท็จจริงหรือเรื่องอื่นใด ไม่ว่าการสื่อความหมายจะทำได้โดยสภาพของสิ่งนั้นเอง 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 |
| **สารสนเทศ (Information)** | ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบข้อมูล ซึ่งอาจอยู่ในรูปของตัวเลข ข้อความหรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้งานสามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ |
| **ระบบสารสนเทศ (Information System)** | ระบบงานที่นำเทคโนโลยีมาช่วยในการสร้างสารสนเทศที่สามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนา และควบคุมการติดต่อสื่อสาร 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)** | สิ่งที่มีคุณค่าหรือมูลค่าต่อหน่วยงานและเป็นทรัพย์สินที่เกี่ยวข้องกับการประมวลผลสารสนเทศที่หน่วยงานเป็นเจ้าของ เช่า ว่าจ้าง พัฒนา หรือจัดซื้อ โดยแบ่งแยกออกเป็นประเภทต่าง ๆ ได้แก่ สารสนเทศ (Information) ซอฟต์แวร์ (Software) ทรัพย์สินที่มีรูปร่าง (Physical Asset) บริการสาธารณูปโภคพื้นฐาน (Service) และบุคลากร (People) |
| **ข้อมูลของหน่วยงาน** | ข้อมูลที่อยู่ในความครอบครองหรือควบคุมดูแลของหน่วยงาน |
| **ข้อมูลสาธารณะ (Public Data)** | ข้อมูลที่สามารถเปิดเผยได้ สามารถนำไปใช้ได้อย่างอิสระ ไม่ว่าจะเป็นข้อมูลข่าวสาร ข้อมูลส่วนบุคคล ข้อมูลอิเล็กทรอนิกส์ เป็นต้น |

| คำศัพท์ | ความหมาย |
|---|---|
| **ข้อมูลส่วนบุคคล (Personal Data)** | ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ (พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒) |
| **ข้อมูลความมั่นคง (National Security Data)** | ข้อมูลเกี่ยวกับความมั่นคงของรัฐ ที่ทำให้เกิดความสงบเรียบร้อย การมีเสถียรภาพความเป็นปึกแผ่น ปลอดภัยจากภัยคุกคาม เป็นต้น |
| **ข้อมูลความลับทางราชการ (Confidential Government Data)** | ข้อมูลที่อยู่ในความครอบครองหรือควบคุมดูแลของหน่วยงานของรัฐที่มีคำสั่งไม่ให้มีการเปิดเผย และมีการกำหนดชั้นความลับของข้อมูล |
| **ข้อมูลลับ (Confidential)** | ข้อมูลข่าวสารซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์ของรัฐซึ่งผู้ที่สามารถเข้าถึงได้ต้องเป็นบุคคลที่มีสิทธิเท่านั้นและห้ามเผยแพร่ต่อบุคคลภายนอกเว้นแต่จะได้รับอนุมัติเป็นลายลักษณ์อักษรโดย เลขาธิการคณะกรรมการป้องกันและปราบปรามการฟอกเงิน ขึ้นไปโดยต้องมีการลงนามในเอกสารข้อตกลงการไม่เปิดเผยข้อมูล (Non-Disclosure Agreement) เว้นแต่การเผยแพร่ดังกล่าวเป็นไปตามอำนาจที่กฎหมายให้การรับรอง |
| **ข้อมูลลับมาก (Secret)** | ข้อมูลข่าวสารซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรงซึ่งผู้ที่สามารถเข้าถึงได้ต้องเป็นบุคคลที่มีสิทธิเท่านั้นและห้ามเผยแพร่ต่อบุคคลภายนอก เว้นแต่จะได้รับอนุมัติเป็นลายลักษณ์อักษรโดย เลขาธิการคณะกรรมการป้องกันและปราบปรามการฟอกเงิน ที่เป็นเจ้าของข้อมูลขึ้นไปโดยต้องมีการลงนามในเอกสารข้อตกลงการไม่เปิดเผยข้อมูล (Non-Disclosure Agreement) เว้นแต่การเผยแพร่ดังกล่าวเป็นไปตามอำนาจที่กฎหมายให้การรับรอง |
| **ข้อมูลลับที่สุด (Top Secret)** | ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรงที่สุดซึ่งผู้ที่สามารถเข้าถึงได้ต้องเป็นบุคคลที่มีสิทธิเท่านั้นและห้ามเผยแพร่ต่อบุคคลภายนอกเว้นแต่จะได้รับอนุมัติเป็นลายลักษณ์อักษรโดย เลขาธิการคณะกรรมการป้องกันและปราบปรามการฟอกเงิน ขึ้นไปโดยต้องมีการลงนามในเอกสารข้อตกลงการไม่เปิดเผยข้อมูล (Non-Disclosure Agreement) เว้นแต่การเผยแพร่ดังกล่าวเป็นไปตามอำนาจที่กฎหมายให้การรับรอง |
| **ข้อมูลใช้ภายใน (Internal Use Only)** | ข้อมูลสำหรับใช้ในการดำเนินกิจการภายในของหน่วยงานซึ่งไม่อนุญาตให้นำไปใช้งานภายนอกก่อนได้รับอนุญาต เช่น นโยบาย มาตรฐาน และขั้นตอนการปฏิบัติงาน ประกาศ และบันทึกภายในหน่วยงาน เป็นต้น |

**การเผยแพร่และการทบทวน**

แนวปฏิบัติเกี่ยวกับข้อมูลนี้จะต้องทำการเผยแพร่โดยการประกาศเวียนในระบบสารบรรณ ระบบเว็บไซต์ของหน่วยงาน เพื่อให้เจ้าหน้าที่ทุกระดับในหน่วยงาน ได้รับทราบ และถือปฏิบัติตามแนวปฏิบัตินี้อย่างเคร่งครัด โดยแนวปฏิบัติที่จัดขึ้นนี้เมื่อเริ่มนำไปใช้ในระยะแรกสามารถทบทวนได้บ่อยครั้งเป็นรายไตรมาส เพื่อให้เหมาะสมกับบริบทการปฏิบัติงานจริง และจะต้องมีการทบทวนเป็นประจำอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ รวมถึงเมื่อมีข้อเสนอแนะคณะกรรมการธรรมาภิบาลข้อมูลเห็นสมควร

# แนวปฏิบัติการบริหารจัดการข้อมูล

**หมวด ๑ การสร้างข้อมูล**

**วัตถุประสงค์**

กำหนดแนวปฏิบัติสำหรับผู้ที่เกี่ยวข้องในการสร้างข้อมูลให้มีคุณภาพ มีความมั่นคงปลอดภัย และเป็นประโยชน์ต่อผู้ใช้ข้อมูล

**ผู้รับผิดชอบงาน**

๑. ผู้สร้างข้อมูล (Data Creators)
๒. ทีมบริหารจัดการข้อมูล (Data Management Team)
๓. เจ้าของข้อมูล (Data Owners)
๔. บริกรข้อมูล (Data Stewards)
๕. ผู้ดูแลระบบสารสนเทศ (System Administrators)

**อ้างอิง**

๑. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓
๒. พระราชบัญญัติลิขสิทธิ์ (ฉบับที่ ๒) พ.ศ. ๒๕๕๘
๓. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐
๔. พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒
๕. ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ พ.ศ ๒๕๖๓

**ข้อปฏิบัติ**

๑. เจ้าของข้อมูล
   ๑.๑ กำหนดผู้มีสิทธิในการสร้างข้อมูล และจะต้องทบทวนสิทธินั้น อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ เช่น การลาออก เปลี่ยนตำแหน่ง โอนย้าย สิ้นสุดการจ้าง การปรับโครงสร้าง หรือเมื่อมีการปรับปรุงระบบสารสนเทศ เป็นต้น
   ๑.๒ กำหนดหมวดหมู่และชั้นความลับของข้อมูล
๒. ผู้ดูแลระบบสารสนเทศจะต้องกำหนดสิทธิในการสร้างข้อมูลในระบบให้แก่ผู้สร้างข้อมูลตามที่เจ้าของข้อมูลกำหนด
๓. เจ้าของข้อมูล บริกรข้อมูลธุรกิจ บริกรข้อมูลเทคนิค และทีมบริหารจัดการข้อมูล ร่วมจัดทำคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตา (Metadata) เมื่อมีการสร้างชุดข้อมูล (Datasets) ตามมาตรฐานขั้นต่ำคำอธิบายชุดข้อมูลดิจิทัลที่สำนักงานพัฒนารัฐบาลดิจิทัล (สพร.) กำหนด และกำหนดให้ทำการประเมินคุณค่าของชุดข้อมูลดิจิทัลตามแบบฟอร์มประเมินคุณค่าชุดข้อมูลที่ สพร. หรือหน่วยงานกำหนด เพื่อสนับสนุนการคัดเลือกเป็นชุดข้อมูลคุณค่าสูง (High Value Dataset) และเผยแพร่เป็นข้อมูลเปิดของหน่วยงานต่อสาธารณะตามกฎหมายว่าด้วยข้อมูลข่าวสารของราชการในรูปแบบข้อมูลดิจิทัล
๔. 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


๕. ห้ามมิให้ผู้สร้างข้อมูล ทำการสร้าง/ทำซ้ำต่อข้อมูลที่ขัดต่อกฎหมายว่าด้วยลิขสิทธิ์หรือทรัพย์สินทางปัญญาของผู้อื่น เว้นแต่จะเป็นไปตามอำนาจที่กฎหมายรับรอง

๖. กำหนดให้ผู้สร้างข้อมูลสร้างข้อมูลที่มาจากแหล่งข้อมูลที่เชื่อถือได้เท่านั้น

๗. 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 ๒ การจัดเก็บข้อมูล

**วัตถุประสงค์**

กำหนดแนวปฏิบัติสำหรับผู้ที่เกี่ยวข้องในการจัดเก็บข้อมูล ให้มีคุณภาพ เข้าถึงและใช้งานได้อย่างมั่นคงปลอดภัย

**ผู้รับผิดชอบงาน**

๑. เจ้าของข้อมูล (Data Owners)
๒. ผู้ดูแลระบบสารสนเทศ (System Administrators)
๓. ผู้สร้างข้อมูล (Data Creators)
๔. บริกรข้อมูล (Data Stewards)
๕. ผู้ใช้ข้อมูล (Data Users)
๖. ทีมบริหารจัดการข้อมูล (Data Management Team)

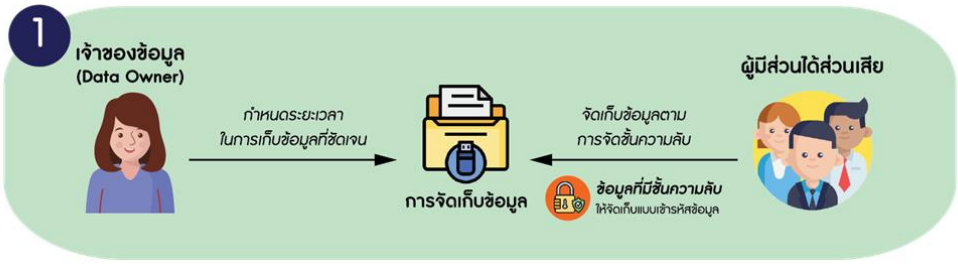
**อ้างอิง**

๑. ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๕๐
๒. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓
๓. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐
๔. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒
๕. พระราชกำหนดว่าด้วยการประชุมผ่านสื่ออิเล็กทรอนิกส์ พ.ศ. ๒๕๖๓
๖. ระเบียบสำนักนายกรัฐมนตรี ว่าด้วยงานสารบรรณ (ฉบับที่ ๔) พ.ศ. ๒๕๖๔

**ข้อปฏิบัติ**

๑. กำหนดให้เจ้าของข้อมูลจะต้องกำหนดระยะเวลาในการจัดเก็บข้อมูลที่ชัดเจน
๒. กำหนดให้ทีมบริหารจัดการข้อมูล และผู้ดูแลระบบสารสนเทศทำการย้ายข้อมูลที่มีการจัดเก็บเกินระยะเวลาที่กำหนดแล้วเพื่อจัดเก็บเป็นข้อมูลถาวร
๓. กำหนดให้การจัดเก็บชุดข้อมูลจะต้องมีคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตา หากไม่มีหรือไม่ครบถ้วน ทีมบริหารจัดการข้อมูลจะต้องแจ้งผู้รับผิดชอบ ได้แก่ เจ้าของข้อมูล บริกรข้อมูลด้านเทคนิค และบริกรข้อมูลด้านธุรกิจ โดยทีมบริหารจัดการข้อมูลร่วมกันจัดทำและปรับปรุงให้เป็นปัจจุบัน
๔. ผู้มีส่วนได้ส่วนเสียเกี่ยวข้องกับข้อมูล ทั้งเจ้าของข้อมูล ผู้สร้างข้อมูล ผู้ใช้ข้อมูล และทีมบริหารจัดการข้อมูล จะต้องจัดเก็บข้อมูลตามการจัดชั้นความลับของหน่วยงาน โดยทำการเข้ารหัสข้อมูลเพื่อป้องกันการเข้าถึงหรือแก้ไขข้อมูลโดยไม่ได้รับอนุญาต ทั้งนี้การเข้ารหัสข้อมูลให้ปฏิบัติตามวิธีการเข้ารหัสข้อมูลแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน
    ๔.๑ในกรณีที่ในตารางฐานข้อมูลเดียวกันมีฟิลด์ข้อมูลที่มีชั้นความลับและไม่มีชั้นความลับอยู่ร่วมกันให้ทำการเข้ารหัสข้อมูลเฉพาะฟิลด์ข้อมูลที่มีชั้นความลับเท่านั้น
    ๔.๒ในกรณีข้อมูลที่จัดเก็บในรูปแบบเอกสาร ให้มีการจัดเก็บ ดังนี้
        - เก็บในสถานที่เหมาะสม สามารถปิดล็อกได้เมื่อไม่ใช้งาน
        - เก็บแยกออกจากอุปกรณ์ประมวลผลต่าง ๆ เช่น เครื่องพิมพ์ เครื่องถ่ายเอกสาร เป็นต้น โดยทันที เพื่อเป็นการป้องกันไม่ให้ผู้ไม่มีสิทธิในการเข้าถึงข้อมูล เข้าถึงข้อมูลได้

๕. กำหนดให้มีวิธีปฏิบัติการกู้คืนข้อมูลที่จัดเก็บถาวร สำหรับข้อมูลที่มีความสำคัญมากต่อการดำเนินงานของหน่วยงาน เพื่อสอบทานความถูกต้อง ครบถ้วน ความพร้อมใช้งาน คุณภาพข้อมูล





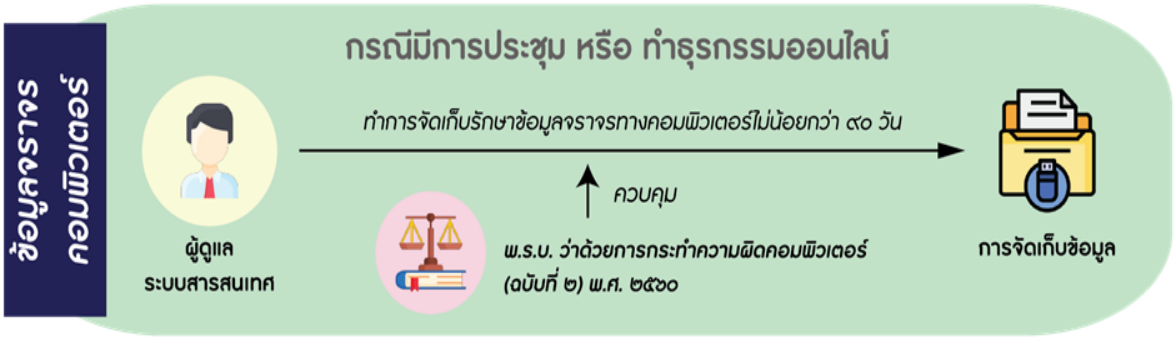
๖. ในการจัดเก็บข้อมูลส่วนบุคคล**ให้เก็บรวบรวมได้เท่าที่จำเป็น** ภายใต้อำนาจหน้าที่และวัตถุประสงค์อันชอบด้วยกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล และ**ไม่เก็บรวบรวมข้อมูลส่วนบุคคล**ดังต่อไปนี้ เว้นแต่ได้รับการยินยอมจากเจ้าของข้อมูลส่วนบุคคล หรือพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล หรือกฎหมายอื่นบัญญัติให้กระทำได้

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

๗. กำหนดให้มีการยกเลิกการจัดเก็บข้อมูลส่วนบุคคลกรณีเจ้าของข้อมูลส่วนบุคคลถอนความยินยอมตามที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลกำหนด

๘. ในกรณีที่มีการประชุมหรือธุรกรรมออนไลน์ กำหนดให้มีการจัดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่า ๙๐ วัน นับแต่วันที่ข้อมูลเข้าสู่ระบบคอมพิวเตอร์ โดยจัดเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการนับแต่เริ่มใช้บริการให้สอดคล้องตามกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์และในการจัดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ให้สอดคล้องตามกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ ผู้ให้บริการจะต้องใช้วิธีการที่มั่นคงปลอดภัยอย่างน้อย ดังนี้

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




๙. กำหนดให้มีมาตรการรักษาความปลอดภัยในการจัดเก็บข้อมูล รวมทั้งกรณีที่มีการเคลื่อนย้ายอุปกรณ์ที่จัดเก็บข้อมูล เพื่อป้องกันมิให้มีการเข้าถึงโดยมิได้รับอนุญาต หรือลักลอบนำข้อมูลไปใช้ที่ก่อให้เกิดความเสียหายต่อหน่วยงาน

๑๐. กำหนดมาตรการรักษาความปลอดภัยของข้อมูลที่จัดเก็บถาวร เพื่อป้องกันข้อมูลไม่ให้มีการลบปรับปรุง แก้ไขได้ รวมทั้งป้องกันมิให้ข้อมูลที่จัดเก็บถาวรรั่วไหลไปยังบุคคลที่ไม่ได้รับอนุญาต

๑๑. กำหนดให้มีมาตรการรักษาความปลอดภัยของการถ่ายโอนข้อมูลกับหน่วยงานภายนอกที่ผ่านช่องทางการสื่อสารทุกชนิด โดยต้องสอดคล้องตามนโยบายความมั่นคงปลอดภัยสารสนเทศ

๑๒. ห้ามมิให้จัดเก็บข้อมูลส่วนตัวหรือข้อมูลที่ไม่เกี่ยวข้องกับการดำเนินงานของหน่วยงาน สำหรับการจัดเก็บข้อมูลถาวรบนเครื่องแม่ข่ายที่หน่วยงานจัดสรรไว้

๑๓. กำหนดให้มีการทบทวนเกี่ยวกับช่วงระยะเวลาการจัดเก็บข้อมูล มาตรการ และวิธีปฏิบัติที่เกี่ยวข้องกับการจัดเก็บข้อมูลถาวร อย่างน้อยปีละ ๑ 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 |

| กิจกรรม | ผู้มีส่วนได้ส่วนเสีย | | | | | |
|---|---|---|---|---|---|---|
| | เจ้าของข้อมูล | ผู้ดูแลระบบสารสนเทศ | ผู้สร้างข้อมูล | ผู้ใช้ข้อมูล | บริกรข้อมูล | ทีมบริหารจัดการข้อมูล |
| 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 ๓ การประมวลผลข้อมูลและการใช้ข้อมูล

### วัตถุประสงค์

กำหนดแนวปฏิบัติในการประมวลผลข้อมูลและการใช้ข้อมูลที่มีประสิทธิภาพถูกต้อง ตรงตามวัตถุประสงค์ เพื่อให้เกิดประโยชน์สูงสุด

### ผู้รับผิดชอบงาน

๑. เจ้าของข้อมูล (Data Owners)
๒. ผู้ใช้ข้อมูล (Data Users)
๓. ผู้ดูแลระบบสารสนเทศ (System Administrators)

### อ้างอิง

๑. พระราชบัญญัติข้อมูลข่าวสารราชการ พ.ศ. ๒๕๔๐
๒. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓
๓. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

### ข้อปฏิบัติ

๑. เจ้าของข้อมูลจะต้องกำหนดผู้มีสิทธิเข้าถึงเพื่อประมวลผลและใช้ข้อมูลตามชั้นความลับ ดังนี้
   - ข้อมูลเปิดเผยได้ ไม่กำหนดสิทธิการเข้าถึงเพื่อประมวลผลและใช้งานข้อมูล
   - ข้อมูลที่มีชั้นความลับ กำหนดให้ผู้ใช้งานที่ได้รับสิทธิเข้าถึงและใช้ข้อมูลตามอำนาจหน้าที่เท่านั้น
   - ข้อมูลใช้ภายใน กำหนดให้บุคลากรของหน่วยงานเท่านั้นที่มีสิทธิเข้าถึงเพื่อประมวลผลและใช้งานข้อมูลได้

๒. ผู้ดูแลระบบสารสนเทศจะต้องกำหนดสิทธิในการเข้าถึงข้อมูลในระบบเพื่อประมวลผลและใช้ข้อมูลของผู้ใช้งานตามที่เจ้าของข้อมูลกำหนด

๓. เจ้าของข้อมูลจะต้องทบทวนสิทธิการเข้าถึงเพื่อประมวลผลและใช้ข้อมูลของผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ เช่น การลาออก เปลี่ยนตำแหน่ง โอนย้าย สิ้นสุดการจ้าง การปรับโครงสร้าง หรือเมื่อมีการปรับปรุงระบบสารสนเทศ

๔. ผู้ที่มีสิทธิเข้าใช้งานข้อมูลที่มีชั้นความลับตามที่กำหนดโดยเจ้าของข้อมูลจะต้องใช้ข้อมูลอย่างระมัดระวัง โดยคำนึงถึงความปลอดภัยและต้องไม่ใช้งานข้อมูลที่มีชั้นความลับในพื้นที่สาธารณะ

๕. ผู้ใช้ข้อมูลจะประมวลผลข้อมูลหรือใช้ข้อมูลส่วนบุคคลเท่าที่จำเป็นภายใต้อำนาจหน้าที่และวัตถุประสงค์อันชอบด้วยกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล หรือตามคำสั่งที่ได้รับจากหน่วยงานเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคล

๖. หน่วยงานต้องยกเลิกการประมวลผลข้อมูลหรือการใช้ข้อมูลส่วนบุคคล กรณีที่เจ้าของข้อมูลส่วนบุคคลถอนความยินยอมตามที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลกำหนด

๗. 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 ๔ การเปิดเผยข้อมูล

### วัตถุประสงค์

กำหนดแนวปฏิบัติการเปิดเผยข้อมูลต่อสาธารณะโดยอิงจากกฎหมาย กฎเกณฑ์และแนวปฏิบัติที่เกี่ยวข้อง ทั้งนี้ข้อมูลที่เปิดเผยควรเป็นประโยชน์ สามารถนำไปประมวลผลและใช้ต่อยอดในการพัฒนาในรูปแบบต่าง ๆ ได้

### ผู้รับผิดชอบงาน

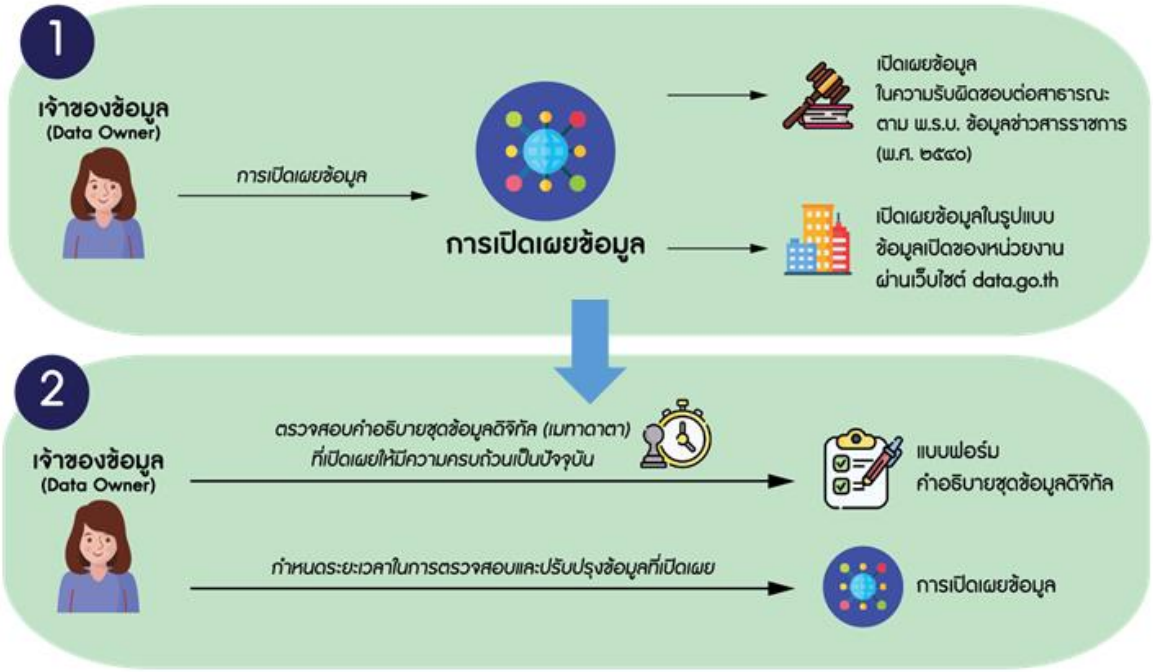
๑. เจ้าของข้อมูล (Data Owners)
๒. ผู้ใช้ข้อมูล (Data Users)
๓. บริกรข้อมูล (Data Stewards)
๔. ทีมบริหารจัดการข้อมูล (Data Management Team)

### อ้างอิง

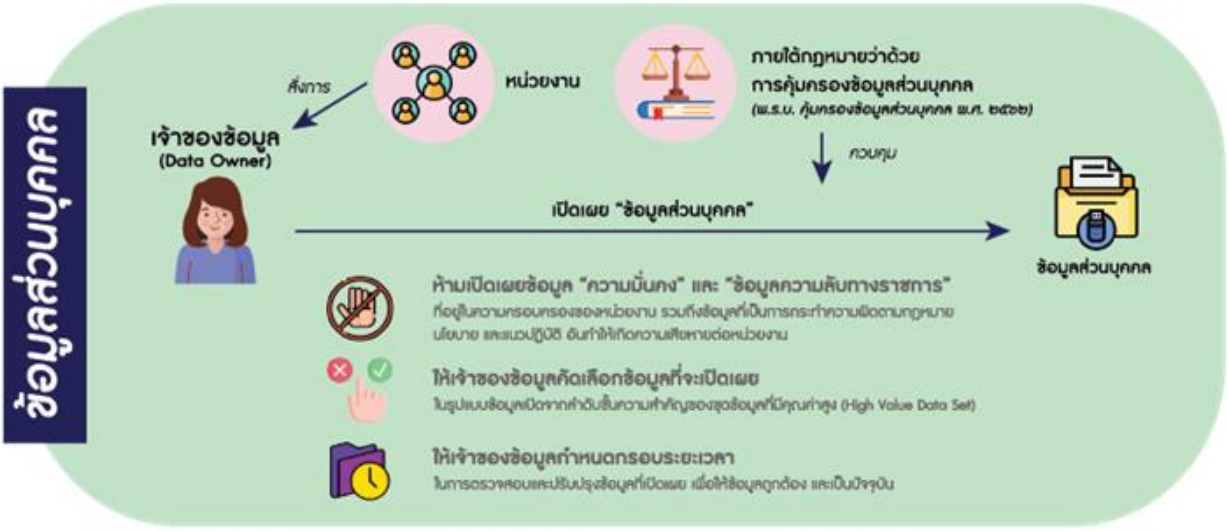
๑. พระราชบัญญัติข้อมูลข่าวสารราชการ พ.ศ. ๒๕๔๐
๒. พระราชบัญญัติการอำนวยความสะดวกในการพิจารณาอนุญาตของทางราชการ พ.ศ. ๒๕๕๘
๓. พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒
๔. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒
๕. ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง มาตรฐานและหลักเกณฑ์การเปิดเผยข้อมูลเปิดภาครัฐในรูปแบบข้อมูลดิจิทัลต่อสาธารณะ

### ข้อปฏิบัติ

๑. เจ้าของข้อมูลจะต้องเปิดเผยข้อมูลในความรับผิดชอบต่อสาธารณะตามกฎหมายว่าด้วยข้อมูลข่าวสารของราชการ และมาตรฐานและหลักเกณฑ์การเปิดเผยข้อมูลเปิดภาครัฐในรูปแบบข้อมูลดิจิทัลต่อสาธารณะ



๒. เจ้าของข้อมูลทำการเปิดเผยข้อมูลในความรับผิดชอบในรูปแบบข้อมูลเปิดของหน่วยงานโดยดำเนินการดังนี้
   - กำหนดลักษณะของข้อมูลที่เผยแพร่กำหนดให้อยู่ในรูปแบบที่เครื่องสามารถประมวลผลได้
   - กำหนดให้มีคำอธิบายข้อมูลหรือเมทาดาตาสำหรับข้อมูลที่ต้องเปิดเผย
   - ข้อมูลที่เผยแพร่จะต้องมีการบันทึกเวลา (Timestamps) ที่ช่วยให้ผู้ใช้งานสามารถระบุได้ว่าข้อมูลนั้นเป็นปัจจุบัน
   - ข้อมูลที่เผยแพร่ต้องมาจากแหล่งที่เก็บข้อมูลโดยตรง ด้วยระดับความละเอียดสูงโดยไม่มีการปรับแต่งหรือเป็นข้อมูลรูปแบบสรุป (Summary data)
   - ชุดข้อมูลและรายการชุดข้อมูลที่เผยแพร่จะต้องมีการจัดรูปแบบที่กำหนดเป็นมาตรฐานและกำหนดภายใต้หมวดหมู่เดียวกัน เพื่อให้ผู้ใช้ข้อมูลสามารถค้นหาและเข้าถึงข้อมูลได้ง่าย
๓. กำหนดให้เงื่อนไขและข้อกำหนดของข้อมูลที่นำมาเปิดเผยภายในเครือข่ายของหน่วยงาน ข้อมูลที่เผยแพร่ต้องไม่ขัดต่อกฎหมายว่าด้วยทรัพย์สินทางปัญญา เว้นแต่การเปิดเผยข้อมูลจะเป็นไปตามอำนาจที่กฎหมายรับรอง
๔. สนับสนุนการจัดทำบัญชีข้อมูลหน่วยงานและการลงทะเบียนบัญชีข้อมูลภาครัฐ โดยบริหารจัดการข้อมูลสำคัญ จัดทำบัญชีข้อมูลของหน่วยงาน และทำการลงทะเบียนบัญชีข้อมูลของหน่วยงานและชุดข้อมูลสำคัญ เข้าสู่ระบบบัญชีข้อมูลภาครัฐ (Government Data Catalog หรือ GD Catalog) เพื่อการเปิดเผยข้อมูลภาครัฐที่เป็นระบบ และมีเอกภาพ สามารถสืบค้นชุดข้อมูล คำอธิบายชุดข้อมูล รวมไปถึงแหล่งต้นทางของชุดข้อมูลภาครัฐที่สำคัญ สนับสนุนการใช้ประโยชน์ข้อมูลร่วมกัน
๕. สนับสนุนการเผยแพร่ข้อมูลผ่านช่องทางที่ง่ายต่อการเข้าถึงข้อมูล และสนับสนุนการเปิดเผยข้อมูลในรูปแบบดิจิทัลต่อสาธารณะที่ศูนย์กลางข้อมูลเปิดภาครัฐ (Government Open Data) ผ่านเว็บไซต์ data.go.th โดย
   - กำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัยในการเปิดเผยข้อมูลที่กำหนดลำดับชั้นข้อมูลตั้งแต่ลับขึ้นไป อย่างเพียงพอและมีประสิทธิภาพ
   - มีการตรวจสอบข้อมูลที่เผยแพร่จากหน่วยงานทั้งภายในและภายนอกหน่วยงาน เพื่อให้มั่นใจว่าหน่วยงานได้มีข้อมูลที่เผยแพร่ที่มีคุณค่า
   - การเผยแพร่ข้อมูล ต้องมีการตรวจสอบรูปแบบข้อมูลที่เผยแพร่ให้สอดคล้องกับมาตรฐานที่หน่วยงานกำหนด
   - หากการเปิดเผยนั้นเป็นการเปิดเผยบนช่องทางที่ดูแลรับผิดชอบโดยหน่วยงานอื่นที่ให้ปฏิบัติตามเอกสาร/คู่มือการนำข้อมูลขึ้นเผยแพร่ของหน่วยงานนั้น
   - หากการเปิดเผยข้อมูลไม่ครบถ้วน หรือไม่เป็นปัจจุบัน ให้แจ้งเจ้าของข้อมูล บริกรข้อมูลธุรกิจ บริกรข้อมูลเทคนิค และทีมบริหารจัดการข้อมูลทำการจัดทำ/ปรับปรุงให้เป็นปัจจุบัน
๖. กำหนดให้เปิดเผยข้อมูลส่วนบุคคลตามข้อกำหนดของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ หรือตามคำสั่งที่ได้รับจากหน่วยงานเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติในกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล




๗. เจ้าของข้อมูลห้ามเปิดเผยข้อมูลความมั่นคงและข้อมูลความลับทางราชการที่อยู่ในความครอบครองของหน่วยงานรวมทั้งห้ามเปิดเผยข้อมูลที่เป็นการกระทำความผิดตามกฎหมาย นโยบาย และแนวปฏิบัติอันทำให้เกิดความเสียหายต่อหน่วยงาน

๘. กำหนดให้เจ้าของข้อมูลคัดเลือกข้อมูลที่จะเปิดเผยในรูปแบบข้อมูลเปิดจากลำดับชั้นความสำคัญของชุดข้อมูลที่มีคุณค่าสูง (High Value Dataset)

๙. 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. ๒๕๖๒ 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 ๕ การทำลายข้อมูล

**วัตถุประสงค์**

กำหนดแนวปฏิบัติการทำลายข้อมูล และการพิจารณาอนุมัติทำลายโดยเจ้าของข้อมูลเพื่อเป็นการรักษาความมั่นคงปลอดภัยของข้อมูล

**ผู้รับผิดชอบงาน**

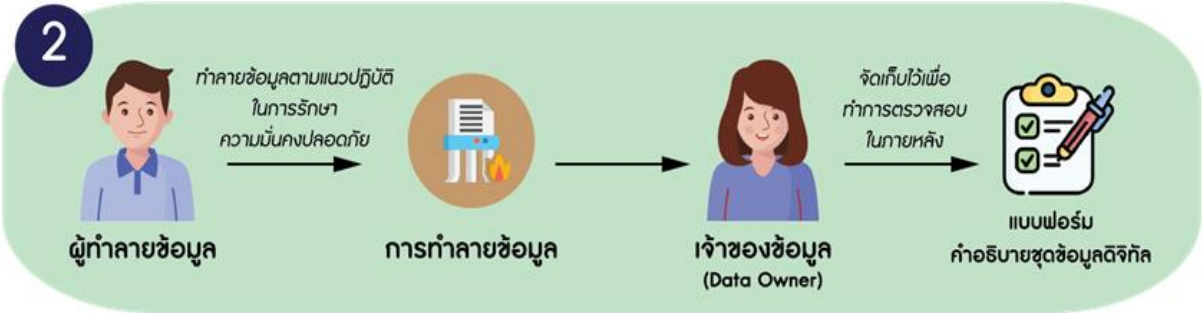
๑. เจ้าของข้อมูล (Data Owners)
๒. ผู้ทำลายข้อมูล (Data Disposer)
๓. ผู้ดูแลระบบสารสนเทศ (Systems Administrators)

**อ้างอิง**

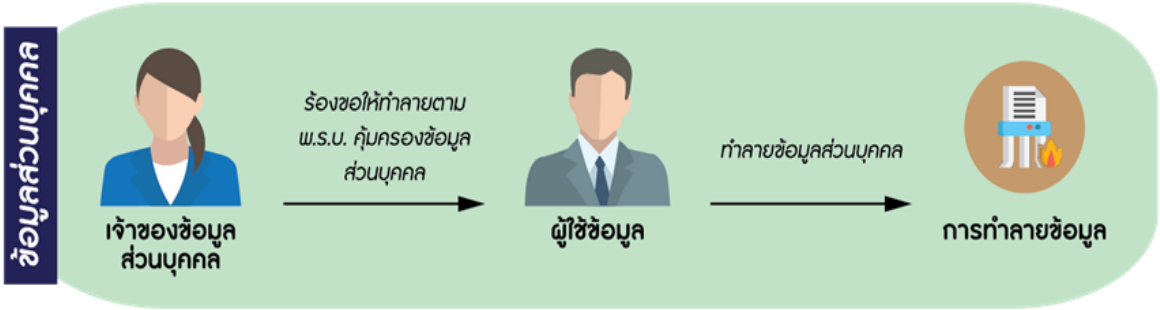
๑. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓
๒. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

**ข้อปฏิบัติ**

๑. เจ้าของข้อมูลเป็นผู้กำหนดผู้มีสิทธิในการทำลายข้อมูล และจะต้องทบทวนสิทธินั้น อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ เช่น การลาออก เปลี่ยนตำแหน่ง โอนย้าย สิ้นสุดการจ้าง การปรับโครงสร้าง หรือเมื่อมีการปรับปรุงระบบสารสนเทศ เป็นต้น
๒. ผู้ดูแลระบบสารสนเทศจะต้องกำหนดสิทธิในการทำลายข้อมูลในระบบให้แก่ผู้ทำลายข้อมูลตามที่เจ้าของข้อมูลกำหนด
๓. ผู้ทำลายข้อมูลต้องทำลายข้อมูลตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน
๔. กำหนดให้เจ้าของข้อมูลต้องจัดเก็บคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตาที่ทำลายสำหรับตรวจสอบในภายหลัง
๕. กำหนดให้ผู้ทำลายข้อมูลจัดเก็บบันทึกรายละเอียดการทำลายข้อมูลไว้ในทะเบียนควบคุมและบันทึกการทำลายข้อมูล โดยให้เก็บรักษาไว้เป็นหลักฐานไม่น้อยกว่า ๑ ปี

๖. กำหนดให้ผู้ใช้ข้อมูลส่วนบุคคลทำลายข้อมูลส่วนบุคคลเมื่อเจ้าของข้อมูลส่วนบุคคล ร้องขอตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒




| 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 | C | S | I | R |

*ตารางที่: 5 ตัวอย่างผู้มีส่วนได้ส่วนเสียในการทำลายข้อมูล*

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

## หมวด ๖ การเชื่อมโยงและการแลกเปลี่ยนข้อมูล

**วัตถุประสงค์**

เพื่อกำหนดแนวปฏิบัติและมาตรฐานด้านเทคนิคในการเชื่อมโยงและการแลกเปลี่ยนข้อมูลดิจิทัลทั้งภายในหน่วยงานและระหว่างหน่วยงาน อย่างมีประสิทธิภาพและก่อให้เกิดประโยชน์ต่อภาคประชาชน ภาครัฐ และภาคเอกชน

**ผู้รับผิดชอบงาน**

๑. ผู้จัดการโครงการ (Project Managers)
๒. ผู้ดูแลระบบแม่ข่าย (Server Administrators)
๓. เจ้าของข้อมูล (Data Owners)
๔. บริกรข้อมูล (Data Stewards)
๕. ทีมบริหารจัดการข้อมูล (Data Management Team)

**อ้างอิง**

๑. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓
๒. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐
๓. พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒
๔. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

**ข้อปฏิบัติ**

๑. กำหนดให้ผู้จัดการโครงการกำหนดวิธีปฏิบัติและมาตรฐานทางด้านเทคนิคที่จำเป็นต้องใช้เกี่ยวกับการเชื่อมโยงและแลกเปลี่ยนข้อมูลของโครงการในความรับผิดชอบ ดังนี้
   - การเชื่อมโยงและแลกเปลี่ยนข้อมูลภายในหน่วยงาน กำหนดให้ใช้รูปแบบที่เป็นมาตรฐานเปิด (Open Format) ทั้งในส่วนมาตรฐานข้อมูล เช่น XML และ JSON เป็นต้น มาตรฐานโปรโตคอลสื่อสาร เช่น SOAP REST หรืออื่น ๆ ที่ได้รับการยอมรับจากมาตรฐานสากล
   - การเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน ให้ดำเนินการตามมาตรฐานกลางของหน่วยงานหลักที่เป็นผู้รับผิดชอบ

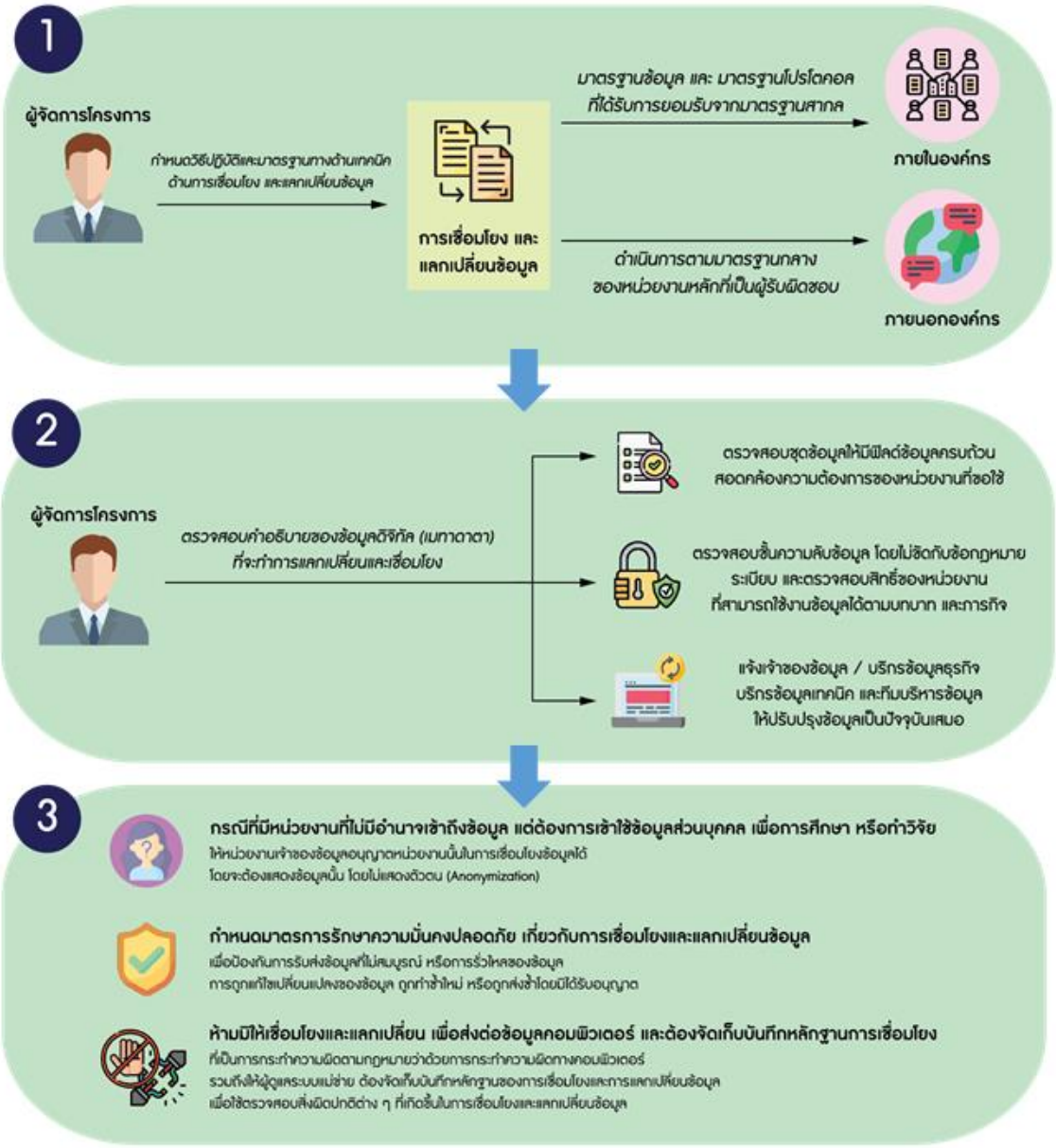
๒. กำหนดให้ผู้จัดการโครงการตรวจสอบคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตาที่จะทำการเชื่อมโยงและแลกเปลี่ยนให้ครบถ้วน ดังนี้
   - ตรวจสอบเมทาดาตาของชุดข้อมูลดิจิทัลที่จัดเก็บให้มีฟิลด์ข้อมูลครบถ้วนสอดคล้องกับความต้องการของหน่วยงานที่ขอใช้ หากไม่ครบถ้วนต้องจัดทำเพิ่มเติมตามความต้องการของหน่วยงานที่ขอใช้
   - ตรวจสอบชั้นความลับของข้อมูลว่าอยู่ในชั้นความลับที่สามารถเปิดเผยได้หรือไม่ นั่นคือ ต้องไม่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ ความมั่นคงของประเทศ ความลับทางราชการ และความเป็นส่วนตัว พร้อมทั้งตรวจสอบสิทธิของหน่วยงานที่สามารถนำข้อมูลไปใช้ได้ตามบทบาทและภารกิจตามกฎหมายของหน่วยงานนั้น ๆ
   - หากไม่ครบถ้วน หรือไม่เป็นปัจจุบัน ให้แจ้งเจ้าของข้อมูล บริกรข้อมูลธุรกิจ บริกรข้อมูลเทคนิค และทีมบริหารจัดการข้อมูลทำการจัดทำ/ปรับปรุงให้เป็นปัจจุบัน

๓. ในกรณีที่มีหน่วยงานอื่นที่ไม่มีอำนาจในการเข้าถึงข้อมูลส่วนบุคคลแต่ต้องการใช้ข้อมูลส่วนบุคคลในการครอบครองของหน่วยงาน เพื่อทำการศึกษาหรือวิจัย ซึ่งเป็นข้อยกเว้นตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ให้หน่วยงานเจ้าของข้อมูลอนุญาตหน่วยงานนั้นในการเชื่อมโยงข้อมูลได้ โดยจะต้องแสดงข้อมูลนั้นด้วยวิธีไม่แสดงตัวตน (Anonymization)

๔. กำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัยเกี่ยวกับการเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัล เพื่อป้องกันมิให้มีการรับส่งข้อมูลที่ไม่สมบูรณ์ หรือส่งข้อมูลไปผิดที่หรือมีการรั่วไหลของข้อมูล หรือ ข้อมูลถูกแก้ไขเปลี่ยนแปลง ถูกทำซ้ำใหม่ ถูกส่งซ้ำโดยมิได้รับอนุญาต

๕. ห้ามมิให้เชื่อมโยงและแลกเปลี่ยนเพื่อส่งต่อข้อมูลคอมพิวเตอร์ที่เป็นการกระทำความผิดตามกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์

๖. 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

# ประกาศที่เกี่ยวข้อง

# ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล

เรื่อง มาตรฐานรัฐบาลดิจิทัลว่าด้วยข้อเสนอแนะ
สำหรับการจัดทำนโยบายและแนวปฏิบัติการบริหารจัดการข้อมูล

---

ด้วยพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ มีวัตถุประสงค์เพื่อให้หน่วยงานของรัฐจัดให้มีการบริหารงานภาครัฐและการจัดทำบริการสาธารณะเป็นไปด้วยความสะดวก รวดเร็ว มีประสิทธิภาพ และตอบสนองต่อการให้บริการและการอำนวยความสะดวกแก่ประชาชน ให้หน่วยงานของรัฐจัดให้มีการบริหารงานและการจัดทำบริการสาธารณะในรูปแบบและช่องทางดิจิทัล โดยมีการบริหารจัดการและการบูรณาการข้อมูลภาครัฐและการทำงานให้มีความสอดคล้องกันและเชื่อมโยงเข้าด้วยกันอย่างมั่นคงปลอดภัยและมีธรรมาภิบาล ประกอบกับตามประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ กำหนดให้หน่วยงานของรัฐจัดให้มีการจำแนกหมวดหมู่ของข้อมูล เพื่อกำหนดนโยบายข้อมูลหรือกฎเกณฑ์เกี่ยวกับผู้มีสิทธิเข้าถึงและใช้ประโยชน์จากข้อมูลต่าง ๆ ภายในหน่วยงาน สำหรับให้ผู้ซึ่งมีหน้าที่เกี่ยวข้องปฏิบัติตามนโยบายหรือกฎเกณฑ์ได้อย่างถูกต้องและสอดคล้องตามกฎหมายที่เกี่ยวข้อง อันจะนำไปสู่การบริหารจัดการข้อมูลภาครัฐอย่างเป็นระบบ รวมทั้งสนับสนุนการจัดทำบัญชีข้อมูลหน่วยงานให้ได้มาตรฐานและเป็นไปในทิศทางเดียวกัน สอดคล้องตามกรอบธรรมาภิบาลข้อมูลภาครัฐ

อาศัยอำนาจตามความในมาตรา ๗ (๓) และ (๙) แห่งพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ ประกอบมติที่ประชุมคณะกรรมการพัฒนารัฐบาลดิจิทัล ในคราวการประชุมครั้งที่ ๒/๒๕๖๕ เมื่อวันที่ ๒๙ กันยายน พ.ศ. ๒๕๖๕ จึงมีมติให้ออกประกาศไว้ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง มาตรฐานรัฐบาลดิจิทัลว่าด้วยข้อเสนอแนะสำหรับการจัดทำนโยบายและแนวปฏิบัติการบริหารจัดการข้อมูล”

ข้อ ๒ ในประกาศนี้

“หน่วยงานของรัฐ” หมายความว่า ราชการส่วนกลาง ราชการส่วนภูมิภาค ราชการส่วนท้องถิ่น รัฐวิสาหกิจ องค์การมหาชน รัฐสภา ศาล องค์กรอิสระตามรัฐธรรมนูญ องค์กรอัยการ สถาบันอุดมศึกษาของรัฐ และหน่วยงานอิสระของรัฐ

“การกำหนดนโยบายข้อมูล” หมายความว่า การกำหนดนโยบายที่ระบุอย่างชัดเจนที่ครอบคลุมระบบบริหารและกระบวนการจัดการข้อมูลหรือวงจรชีวิตของข้อมูล ซึ่งอาจจะประกอบไปด้วยนโยบายต่าง ๆ ที่สอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง หรือข้อกำหนดอื่น ๆ ที่เกี่ยวข้อง โดยผ่านการอนุมัติจากหัวหน้าหน่วยงานของรัฐ มีการเผยแพร่และสื่อสารให้กับเจ้าหน้าที่และผู้ที่เกี่ยวข้องทั้งภายในและภายนอกหน่วยงานของรัฐ รวมถึงควรมีการทบทวนนโยบายอย่างสม่ำเสมอ เพื่อให้นโยบายข้อมูลได้ถูกนำมาปฏิบัติอย่างมีประสิทธิภาพและต่อเนื่อง

“เอกสารแม่แบบนโยบายการบริหารจัดการข้อมูล” หมายความว่า เนื้อหาสาระที่เกี่ยวข้องกับการจัดทำนโยบายข้อมูล ประกอบด้วยหมวด/หัวข้อ และตัวอย่าง ซึ่งหน่วยงานของรัฐสามารถกำหนดให้สอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง หรือข้อกำหนดอื่น ๆ ที่เกี่ยวข้อง สอดคล้องกับสภาพแวดล้อม ความต้องการและความคาดหวังของผู้มีส่วนได้เสียกับข้อมูล และเป้าประสงค์ของธรรมาภิบาลข้อมูลภาครัฐในหน่วยงาน รวมทั้งข้อกำหนดด้านคุณภาพข้อมูล การรักษาความเป็นส่วนตัว และความมั่นคงปลอดภัยที่หน่วยงานได้จัดทำขึ้น

“การจัดทำแนวปฏิบัติการบริหารจัดการข้อมูล” หมายความว่า การจัดทำแนวปฏิบัติการบริหารจัดการข้อมูลให้สอดคล้องตามนโยบายข้อมูล (Data Policy) ที่หน่วยงานของรัฐประกาศและใช้เป็นแนวทางให้ผู้มีส่วนได้ส่วนเสียเกี่ยวกับข้อมูลปฏิบัติตาม เพื่อให้ข้อมูลภายในหน่วยงานของรัฐมีคุณภาพ และมีความมั่นคงปลอดภัย

“เอกสารแม่แบบแนวปฏิบัติการบริหารจัดการข้อมูล” หมายความว่า เอกสารที่ประกอบด้วยหัวข้อและตัวอย่างเนื้อหาสาระที่เกี่ยวข้องกับการจัดทำแนวปฏิบัติการบริหารจัดการข้อมูลตามวงจรชีวิตของข้อมูล โดยแบ่งออกเป็น ๖ หมวด ได้แก่ การสร้างข้อมูล การจัดเก็บข้อมูล (รวมการจัดเก็บถาวร) การประมวลผลข้อมูลและการใช้ข้อมูล การเปิดเผยข้อมูล การทำลายข้อมูล และการเชื่อมโยงและการแลกเปลี่ยนข้อมูล ในแต่ละหมวดจะระบุ วัตถุประสงค์ ผู้รับผิดชอบงาน อ้างอิง และข้อปฏิบัติ ซึ่งหน่วยงานสามารถกำหนดข้อปฏิบัติอื่น ๆ เพิ่มเติมให้สอดคล้องสภาพแวดล้อมและวัฒนธรรมองค์กร และจะต้องสอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง หรือข้อกำหนดอื่น ๆ ที่เกี่ยวข้อง

ข้อ ๓ เพื่อให้หน่วยงานของรัฐมีการกำหนดนโยบายข้อมูลหรือกฎเกณฑ์เกี่ยวกับการบริหารจัดการข้อมูล กำหนดผู้มีสิทธิเข้าถึงและใช้ประโยชน์จากข้อมูลต่าง ๆ ภายในหน่วยงาน สำหรับให้ผู้ซึ่งมีหน้าที่เกี่ยวข้องปฏิบัติตามนโยบายหรือกฎเกณฑ์ได้อย่างถูกต้อง และสอดคล้องตามกฎหมายที่เกี่ยวข้อง อันจะนำไปสู่การบริหารจัดการข้อมูลภาครัฐอย่างเป็นระบบ ให้เป็นไปตามกรอบแนวทางมาตรฐานที่กำหนดแนบท้ายประกาศดังนี้

(๑) มาตรฐานรัฐบาลดิจิทัลว่าด้วยข้อเสนอแนะสำหรับการจัดทำนโยบายการบริหารจัดการข้อมูล เลขที่ มรด. ๔-๑ : ๒๕๖๕

(๒) มาตรฐานรัฐบาลดิจิทัลว่าด้วยข้อเสนอแนะสำหรับการจัดทำแนวปฏิบัติการบริหารจัดการข้อมูล เลขที่ มรด. ๔-๒ : ๒๕๖๕

ทั้งนี้ เพื่อเป็นตัวอย่างในการจัดทำนโยบายและแนวปฏิบัติการบริหารจัดการข้อมูลของหน่วยงานของรัฐ ซึ่งจะเป็นกรอบและแนวทางให้การบริหารจัดการข้อมูลภายในหน่วยงานของรัฐมีความมั่นคงปลอดภัย มีความโปร่งใส และสามารถตรวจสอบได้ รวมทั้งเพื่อให้ข้อมูลของหน่วยงานของรัฐมีคุณภาพ เป็นที่ยอมรับและเชื่อถือของผู้ใช้งาน และสามารถนำไปบูรณาการกับหน่วยงานต่าง ๆ ได้อย่างมีประสิทธิภาพ

ข้อ ๔ ให้นำมาตรฐานและหลักเกณฑ์ตามประกาศนี้มาใช้บังคับกับหน่วยงานของรัฐนับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ประกาศ ณ วันที่ ๑๕ กุมภาพันธ์ พ.ศ. ๒๕๖๖
ดอน ปรมัตถ์วินัย
รองนายกรัฐมนตรี
ประธานกรรมการพัฒนารัฐบาลดิจิทัล

# ข้อมูลมาตรฐานรัฐบาลดิจิทัล
# เอกสารแนบท้ายฉบับที่ ๑ มาตรฐานรัฐบาลดิจิทัลว่าด้วยข้อเสนอแนะ สำหรับการจัดทำนโยบายการบริหารจัดการข้อมูล

| | | |
|---|---|---|
| ชื่อมาตรฐาน | : | มาตรฐานรัฐบาลดิจิทัลว่าด้วย<br>ข้อเสนอแนะสำหรับการจัดทำนโยบายการบริหารจัดการข้อมูล<br>RECOMMENDATION for WRITING DATA MANAGEMENT POLICY |
| มาตรฐานเลขที่ | : | เลขที่ มรด. ๔-๑ : ๒๕๖๕ |
| ผู้จัดทำ | : | สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) |
| กรรมการวิชาการ | : | คณะกรรมการจัดทำร่างมาตรฐาน ข้อกำหนด และหลักเกณฑ์ ภายใต้พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒<br>คณะทำงานเทคนิคด้านมาตรฐานการบริหารจัดการข้อมูลภาครัฐ<br>(วาระดำรงตำแหน่ง กันยายน ๒๕๖๔ - กันยายน ๒๕๖๕)<br>คณะทำงานเทคนิคด้านมาตรฐานการจัดทำบัญชีข้อมูลภาครัฐ<br>(วาระดำรงตำแหน่ง กันยายน ๒๕๖๓ - กันยายน ๒๕๖๔) |
| ขอบข่าย | : | พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒<br>ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ |
| เนื้อหาประกอบด้วย | : | ข้อเสนอแนะสำหรับการจัดทำนโยบายการบริหารจัดการข้อมูล เอกสารแม่แบบนโยบายการบริหารจัดการข้อมูล ประกอบด้วย วัตถุประสงค์ ขอบเขตและการบังคับใช้ ข้อยกเว้น บทบาทและความรับผิดชอบ คำนิยาม นโยบายการบริหารจัดการข้อมูล ข้อกฎหมายและเอกสารอ้างอิง ประวัติการแก้ไขเอกสาร และ ข้อมูลเพิ่มเติม |
| จำนวนหน้า | : | ๒๐ หน้า |
| สถานที่จัดเก็บ | : | https://standard.dga.or.th/category/dg-std/ |
| สถานที่ติดต่อ | : | สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)<br>อาคารบางกอกไทยทาวเวอร์ ชั้น ๑๗ เลขที่ ๑๐๘ ถนนรางน้ำ แขวงถนนพญาไท เขตราชเทวี กรุงเทพมหานคร ๑๐๔๐๐ หมายเลขโทรศัพท์ ๐ ๒๖๑๒ ๖๐๐๐ |

# ข้อมูลมาตรฐานรัฐบาลดิจิทัล
# เอกสารแทบท้ายฉบับที่ ๒ มาตรฐานรัฐบาลดิจิทัลว่าด้วยข้อเสนอแนะสำหรับการจัดทำแนวปฏิบัติการบริหารจัดการข้อมูล

| | | |
|---|---|---|
| ชื่อมาตรฐาน | : | มาตรฐานรัฐบาลดิจิทัลว่าด้วย<br>ข้อเสนอแนะสำหรับการจัดทำแนวปฏิบัติการบริหารจัดการข้อมูล<br>RECOMMENDATION for WRITING DATA MANAGEMENT GUIDELINE |
| มาตรฐานเลขที่ | : | เลขที่ มรด. ๔-๒ : ๒๕๖๕ |
| ผู้จัดทำ | : | สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) |
| กรรมการวิชาการ | : | คณะกรรมการจัดทำร่างมาตรฐาน ข้อกำหนด และหลักเกณฑ์ ภายใต้พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒<br>คณะทำงานเทคนิคด้านมาตรฐานการบริหารจัดการข้อมูลภาครัฐ<br>(วาระดำรงตำแหน่ง กันยายน ๒๕๖๔ - กันยายน ๒๕๖๕)<br>คณะทำงานเทคนิคด้านมาตรฐานการจัดทำบัญชีข้อมูลภาครัฐ<br>(วาระดำรงตำแหน่ง กันยายน ๒๕๖๓ - กันยายน ๒๕๖๔) |
| ขอบข่าย | : | พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒<br>ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ |
| เนื้อหาประกอบด้วย | : | ข้อเสนอแนะสำหรับการจัดทำแนวปฏิบัติการบริหารจัดการข้อมูล เอกสารแม่แบบแนวปฏิบัติการบริหารจัดการข้อมูล ประกอบด้วย บทนำ แนวปฏิบัติการบริหารจัดการข้อมูล และ ภาคผนวก |
| จำนวนหน้า | : | ๓๖ หน้า |
| สถานที่จัดเก็บ | : | https://standard.dga.or.th/category/dg-std/ |
| สถานที่ติดต่อ | : | สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)<br>อาคารบางกอกไทยทาวเวอร์ ชั้น ๑๗ เลขที่ ๑๐๘ ถนนรางน้ำ แขวงถนนพญาไท<br>เขตราชเทวี กรุงเทพมหานคร ๑๐๔๐๐ หมายเลขโทรศัพท์ ๐ ๒๖๑๒ ๖๐๐๐ |

ประกาศสำนักงานป้องกันและปราบปรามการฟอกเงิน
เรื่อง นโยบายธรรมาภิบาลข้อมูลของสำนักงานป้องกันและปราบปรามการฟอกเงิน
---

โดยที่พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ กำหนดให้หน่วยงานของรัฐบริหารจัดการข้อมูลในรูปแบบข้อมูลดิจิทัลตามหลักธรรมาภิบาลข้อมูลภาครัฐ เพื่อส่งเสริมการบูรณาการและใช้ประโยชน์ข้อมูลร่วมกันระหว่างหน่วยงานของรัฐ ยกระดับการบริการ ที่ทันสมัย และสร้างการมีส่วนร่วมของทุกภาคส่วนในการเข้าถึงข้อมูลเปิดภาครัฐ เพื่อตรวจสอบการดำเนินงาน และใช้ประโยชน์ข้อมูลดังกล่าวไปพัฒนานวัตกรรมที่สร้างประโยชน์ต่อประเทศ ประกอบกับประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ ลงวันที่ ๑๒ มีนาคม พ.ศ. ๒๕๖๓ กำหนดให้หน่วยงานของรัฐดำเนินการให้เป็นไปตามธรรมาภิบาลข้อมูลภาครัฐ และจัดทำธรรมาภิบาลข้อมูลของหน่วยงานให้สอดคล้องกับธรรมาภิบาลข้อมูลภาครัฐ

เพื่อให้การดำเนินการจัดทำธรรมาภิบาลข้อมูลของสำนักงานป้องกันและปราบปรามการฟอกเงินเป็นไปด้วยความเรียบร้อยและสอดคล้องกับประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัลข้างต้น อาศัยอำนาจตามความใน มาตรา ๔๑ แห่งพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. ๒๕๔๒ ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน (ฉบับที่ ๕) พ.ศ. ๒๕๕๘ เลขาธิการคณะกรรมการป้องกันและปราบปรามการฟอกเงินจึงออกประกาศสำนักงานป้องกันและปราบปรามการฟอกเงิน เรื่อง นโยบายธรรมาภิบาลข้อมูลของสำนักงานป้องกันและปราบปรามการฟอกเงิน ดังนี้

ข้อ ๑ จัดให้มีกระบวนการธรรมาภิบาลข้อมูลของสำนักงานป้องกันและปราบปรามการฟอกเงิน

ข้อ ๒ จัดให้มีนโยบาย หลักเกณฑ์ มาตรการ และแนวปฏิบัติที่เกี่ยวข้องกับกระบวนการธรรมาภิบาลข้อมูลของสำนักงานป้องกันและปราบปรามการฟอกเงิน

ข้อ ๓ จัดให้มีโครงสร้างธรรมาภิบาลข้อมูลของสำนักงานป้องกันและปราบปรามการฟอกเงิน อาทิ คณะกรรมการธรรมาภิบาลข้อมูล และคณะบริกรข้อมูล

ข้อ ๔ จัดให้มีการดำเนินการ กำกับ ตรวจสอบ ติดตาม วัดผล และประเมินผลตามนโยบาย หลักเกณฑ์ มาตรการ และแนวปฏิบัติที่เกี่ยวข้องกับกระบวนการธรรมาภิบาลข้อมูลของสำนักงานป้องกันและปราบปรามการฟอกเงิน

ข้อ ๕ จัดให้มีนโยบายกฎเกณฑ์ของข้อมูลและมาตรฐานข้อมูลของสำนักงานป้องกันและปราบปรามการฟอกเงิน

ประกาศ ณ วันที่ ๒๖ กันยายน พ.ศ. ๒๕๖๗

(นายเทพสุ บวรโชติดารา)
เลขาธิการคณะกรรมการป้องกันและปราบปรามการฟอกเงิน

คำสั่งสำนักงานป้องกันและปราบปรามการฟอกเงิน
ที่ ๓๕๒ /๒๕๖๗
เรื่อง แต่งตั้งคณะกรรมการธรรมาภิบาลข้อมูล
ของสำนักงานป้องกันและปราบปรามการฟอกเงิน

---

โดยที่พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ กำหนดให้หน่วยงานของรัฐบริหารจัดการข้อมูลในรูปแบบข้อมูลดิจิทัลตามหลักธรรมาภิบาลข้อมูลภาครัฐ เพื่อส่งเสริมการบูรณาการและใช้ประโยชน์ข้อมูลร่วมกันระหว่างหน่วยงานของรัฐ ยกระดับการบริการ ที่ทันสมัย และสร้างการมีส่วนร่วมของทุกภาคส่วนในการเข้าถึงข้อมูลเปิดภาครัฐ เพื่อตรวจสอบการดำเนินงาน และใช้ประโยชน์ข้อมูลดังกล่าวไปพัฒนานวัตกรรมที่สร้างประโยชน์ต่อประเทศ ประกอบกับประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล ลงวันที่ ๑๒ มีนาคม พ.ศ. ๒๕๖๓ เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ กำหนดให้หน่วยงานของรัฐดำเนินการให้เป็นไปตามธรรมาภิบาลข้อมูลภาครัฐ และจัดทำธรรมาภิบาลข้อมูลของหน่วยงานให้สอดคล้องกับธรรมาภิบาลข้อมูลภาครัฐ

เพื่อให้การดำเนินการเกี่ยวกับข้อมูลข่าวสารของราชการ ข้อมูลดิจิทัล และข้อมูลตามภารกิจของสำนักงานป้องกันและปราบปรามการฟอกเงิน สามารถบรรลุเป้าหมายได้อย่างมีประสิทธิภาพและเป็นไปด้วยความเรียบร้อย เลขาธิการคณะกรรมการป้องกันและปราบปรามการฟอกเงิน อาศัยอำนาจตามความใน มาตรา ๔๑ แห่งพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. ๒๕๔๒ ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน (ฉบับที่ ๕) พ.ศ. ๒๕๕๘ จึงแต่งตั้งคณะกรรมการธรรมาภิบาลข้อมูลของสำนักงานป้องกันและปราบปรามการฟอกเงิน โดยมีองค์ประกอบ หน้าที่และอำนาจ ดังนี้

**องค์ประกอบ**

| | | |
|---|---|---|
| ๑) | เลขาธิการคณะกรรมการป้องกันและปราบปรามการฟอกเงิน | ประธานคณะกรรมการ |
| ๒) | รองเลขาธิการคณะกรรมการป้องกันและปราบปรามการฟอกเงิน | รองประธานคณะกรรมการคนที่หนึ่ง |
| ๓) | รองเลขาธิการคณะกรรมการป้องกันและปราบปรามการฟอกเงิน | รองประธานคณะกรรมการคนที่สอง |
| ๔) | ผู้ช่วยเลขาธิการคณะกรรมการป้องกันและปราบปรามการฟอกเงิน | กรรมการ |
| ๕) | เลขานุการกรม หรือผู้แทน | กรรมการ |
| ๖) | ผู้อำนวยการกองกฎหมาย หรือผู้แทน | กรรมการ |
| ๗) | ผู้อำนวยการกองกำกับและตรวจสอบ หรือผู้แทน | กรรมการ |
| ๘) | ผู้อำนวยการกองข่าวกรองทางการเงิน หรือผู้แทน | กรรมการ |
| ๙) | ผู้อำนวยการกองคดี ๑ หรือผู้แทน | กรรมการ |

๑๐) ผู้อำนวยการ...

| | | |
|---|---|---|
| ๑๐) | ผู้อำนวยการกองคดี ๒ หรือผู้แทน | กรรมการ |
| ๑๑) | ผู้อำนวยการกองคดี ๓ หรือผู้แทน | กรรมการ |
| ๑๒) | ผู้อำนวยการกองคดี ๔ หรือผู้แทน | กรรมการ |
| ๑๓) | ผู้อำนวยการกองคดี ๕ หรือผู้แทน | กรรมการ |
| ๑๔) | ผู้อำนวยการกองความร่วมมือและพัฒนามาตรฐาน หรือผู้แทน | กรรมการ |
| ๑๕) | ผู้อำนวยการกองนโยบายและยุทธศาสตร์ หรือผู้แทน | กรรมการ |
| ๑๖) | ผู้อำนวยการกองป้องกันและปราบปรามการสนับสนุนทางการเงินแก่การก่อการร้าย หรือผู้แทน | กรรมการ |
| ๑๗) | ผู้อำนวยการกองบริหารจัดการทรัพย์สิน หรือผู้แทน | กรรมการ |
| ๑๘) | ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ หรือผู้แทน | กรรมการ |
| ๑๙) | ผู้อำนวยการกลุ่มพัฒนาระบบบริหาร หรือผู้แทน | กรรมการ |
| ๒๐) | ผู้อำนวยการส่วนวิจัยและพัฒนานวัตกรรมทางเทคโนโลยี หรือผู้แทน | กรรมการและเลขานุการ |
| ๒๑) | ผู้อำนวยการส่วนบริหารงานเทคโนโลยีสารสนเทศ หรือผู้แทน | กรรมการและผู้ช่วยเลขานุการ |

**หน้าที่และอำนาจ**

๑) จัดทำธรรมาภิบาลข้อมูลของสำนักงานป้องกันและปราบปรามการฟอกเงิน โดยกำหนดวิสัยทัศน์ ยุทธศาสตร์ นโยบายข้อมูล และแนวปฏิบัติ ให้สอดคล้องกับภารกิจของหน่วยงาน และเป็นไปตามกรอบธรรมาภิบาลข้อมูลภาครัฐ รวมทั้ง ทบทวนและปรับปรุงธรรมาภิบาลข้อมูลให้มีความเหมาะสมอย่างต่อเนื่อง

๒) กำหนดนโยบาย มาตรฐาน หลักเกณฑ์ แนวปฏิบัติ ระเบียบและข้อบังคับอื่น ๆ ที่เกี่ยวข้องกับการดำเนินการธรรมาภิบาลข้อมูล เป็นไปอย่างมีประสิทธิภาพ

๓) แต่งตั้งคณะบริกรข้อมูลหรือคณะทำงานอื่น เพื่อปฏิบัติงานตามที่คณะกรรมการมอบหมาย

๔) จัดลำดับความสำคัญและแก้ไขปัญหาที่เกี่ยวข้องกับข้อมูล การส่งเสริมการใช้ประโยชน์ข้อมูล และให้ข้อเสนอแนะแก่คณะบริกรข้อมูลหรือคณะทำงานอื่นที่แต่งตั้ง

๕) กำกับ ดูแล ขับเคลื่อน ติดตาม ตรวจสอบ และประเมินผลการปฏิบัติงานของหน่วยงานที่เกี่ยวข้องกับการดำเนินการธรรมาภิบาลข้อมูลของสำนักงานป้องกันและปราบปรามการฟอกเงิน และรายงานผลการดำเนินการต่อผู้บริหารสำนักงานป้องกันและปราบปรามการฟอกเงิน

๖) ประสานความร่วมมือระหว่างหน่วยงานที่เกี่ยวข้อง หรือให้มีอำนาจเชิญเจ้าหน้าที่ผู้เกี่ยวข้องมาชี้แจง เสนอข้อมูล และ/หรือเอกสารประกอบการพิจารณาได้ตามความจำเป็น

๗) ปฏิบัติงานอื่นใดตามที่ได้รับมอบหมายจากเลขาธิการคณะกรรมการป้องกันและปราบปรามการฟอกเงิน

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

สั่ง ณ วันที่ ๘ สิงหาคม พ.ศ. ๒๕๖๗

(นายเทพสุ บวรโชติดารา)
เลขาธิการคณะกรรมการป้องกันและปราบปรามการฟอกเงิน

# บันทึกข้อความ



**ส่วนราชการ** ศูนย์เทคโนโลยีสารสนเทศ (ศท.) ส่วนนโยบายและแผนยุทธศาสตร์ฯ (สนท.) โทร. ๗๐๑๒

**ที่** ปง ๐๐๑๔.๕/๑๑๙ **วันที่** ๑๗ กุมภาพันธ์ ๒๕๖๘

**เรื่อง** ขอความเห็นชอบนโยบายการบริหารจัดการข้อมูล และแนวปฏิบัติการบริหารจัดการข้อมูลของสำนักงานป้องกันและปราบปรามการฟอกเงิน



เรียน ลปง. ผ่าน รอง ลปง. (นายกมลสิษฐ์ฯ)

**๑. เรื่องเดิม**

๑.๑ คณะกรรมการพัฒนารัฐบาลดิจิทัล ได้ประกาศมาตรฐานดิจิทัลว่าด้วยข้อเสนอแนะสำหรับการจัดทำนโยบายและแนวปฏิบัติการบริหารจัดการข้อมูล ลงวันที่ ๑๕ กุมภาพันธ์ ๒๕๖๖ เพื่อให้หน่วยงานภาครัฐประยุกต์ใช้เป็นมาตรฐานในการบริหารจัดการข้อมูลตามบริบทของหน่วยงาน รวมทั้งสอดคล้องตามกรอบธรรมาภิบาลข้อมูลภาครัฐ (เอกสารแนบ ๑)

๑.๒ หนังสือ ศท. ที่ ปง ๐๐๑๔.๖/ว ๕๙๐ ลงวันที่ ๓๐ กันยายน ๒๕๖๗ เรื่อง ร่างนโยบายการบริหารจัดการข้อมูล และร่างแนวปฏิบัติการบริหารจัดการข้อมูลของสำนักงานป้องกันและปราบปรามการฟอกเงิน เพื่อให้หน่วยงานในสำนักงาน ปปง. พิจารณาร่างนโยบายและแนวปฏิบัติดังกล่าว (เอกสารแนบ ๒)

**๒. ข้อเท็จจริง**

ตามข้อ ๑.๒ ทุกหน่วยงานในสำนักงาน ปปง. ได้รับทราบและเห็นชอบกับร่างนโยบายการบริหารจัดการข้อมูลของสำนักงาน ปปง. และร่างแนวปฏิบัติการบริหารจัดการข้อมูลของสำนักงาน ปปง. (เอกสารแนบ ๓) โดย ปกร. ขอแก้ไข “ตัดคำว่า Template ออกจากหน้าปก” ทั้งนี้ ศท. ได้ดำเนินการแก้ไขตามความเห็นดังกล่าวแล้ว และขอสรุปสาระสำคัญของนโยบายฯ และแนวปฏิบัติฯ ดังนี้

๒.๑ นโยบายการบริหารจัดการข้อมูล (Data Management Policy) (เอกสารแนบ ๔)

กรอบและแนวทางในการบริหารจัดการข้อมูลให้มีความมั่นคงปลอดภัย มีความโปร่งใสและสามารถตรวจสอบได้ เพื่อให้ข้อมูลของหน่วยงานมีคุณภาพ เป็นที่ยอมรับและเชื่อถือของผู้ใช้งาน โดยในนโยบายฉบับนี้ แสดงถึง วัตถุประสงค์ ขอบเขตและการบังคับใช้ ข้อยกเว้น บทบาทและความรับผิดชอบ คำนิยาม การจัดหมวดหมู่และชั้นความลับของข้อมูล การบริหารจัดการข้อมูลตามวงจรชีวิตข้อมูล (Data Life Cycle) และคุณภาพของข้อมูล

๒.๒ แนวปฏิบัติการบริหารจัดการข้อมูล (Data Management Guideline) (เอกสารแนบ ๕)

แนวปฏิบัติตามนโยบายการบริหารจัดการข้อมูล จำนวน ๖ หมวด ได้แก่ ๑) การสร้างข้อมูล ๒) การจัดเก็บข้อมูล ๓) การประมวลผลข้อมูลและการใช้ข้อมูล ๔) การเปิดเผยข้อมูล ๕) การทำลายข้อมูล และ ๖) การเชื่อมโยงและการแลกเปลี่ยนข้อมูล

**๓. ข้อกฎหมาย**

ประกาศสำนักงาน ปปง. เรื่อง นโยบายธรรมาภิบาลข้อมูลของสำนักงานป้องกันและปราบปรามการฟอกเงิน ลงวันที่ ๒๖ กันยายน ๒๕๖๗ ข้อ ๒ จัดให้มีนโยบาย หลักเกณฑ์ มาตรการ และแนวปฏิบัติที่เกี่ยวข้องกับกระบวนการธรรมาภิบาลข้อมูลของสำนักงานป้องกันและปราบปรามการฟอกเงิน (เอกสารแนบ ๖)

**๔. ข้อพิจารณา**

เพื่อให้การดำเนินงานด้านธรรมาภิบาลข้อมูลของสำนักงาน ปปง. เป็นไปตามข้อ ๑.๑ สอดคล้องตามข้อกฎหมาย และบรรลุผลตามตัวชี้วัดยุทธศาสตร์ ๓.๓.๑ ระดับความสำเร็จของการดำเนินงาน

ด้านธรรมาภิบาล...

ด้านธรรมาภิบาลข้อมูล (Data Governance) เพื่อสนับสนุนจัดทำฐานข้อมูลด้าน AML/CFT/CPF ภายใต้แผนยุทธศาสตร์และแผนปฏิบัติราชการ ๕ ปี (พ.ศ. ๒๕๖๖ – ๒๕๗๐) ของสำนักงาน ปปง. ศท. พิจารณาแล้ว เห็นควร

๔.๑ ให้ความเห็นชอบนโยบายการบริหารจัดการข้อมูล (Data Management Policy) ตามข้อ ๒.๑ และแนวปฏิบัติการบริหารจัดการข้อมูล (Data Management Guideline) ตามข้อ ๒.๒

๔.๒ ให้ ศท. เผยแพร่นโยบายและแนวปฏิบัติดังกล่าว ต่อผู้บริหารและหน่วยงานในสำนักงาน ปปง. รับทราบและถือปฏิบัติโดยเคร่งครัด

**๕. ข้อเสนอ**

จึงเรียนมาเพื่อโปรดพิจารณาตามข้อ ๔.๑ หากเห็นชอบ ขอได้โปรดลงนามตามเอกสารที่เสนอมาพร้อมนี้ และโปรดพิจารณาอนุมัติตามข้อ ๔.๒ เพื่อ ศท. จะได้ดำเนินการในส่วนที่เกี่ยวข้องต่อไป

(นายศิวัช ชาวบางงาม)
ผอ.ศท.

- เห็นชอบ ตามข้อ ๔.๑
- อนุมัติ ตามข้อ ๔.๒
- ลงนามแล้ว

(นายเทพสุ บวรโชติดารา)
เลขาธิการ ปปง.
20 ก.พ. 2568

เรียน ลปง.

เพื่อโปรดพิจารณาตามข้อ ๔.๑ - ๔.๒
หากเห็นชอบตามข้อ ๔.๑ โปรดลงนามในเอกสารตามเสนอ

(นายกมลสิษฐ์ วงศ์บุตรน้อย)
รอง ลปง.
๑๙ ก.พ. ๒๕๖๘

ผอ.ศท.
- ดำเนินการ

(นายศิวัช ชาวบางงาม)
ผอ.ศท.
๒๐ ก.พ. ๒๕๖๘