ประกาศกรมกิจการสตรีและสถาบันครอบครัว
เรื่อง นโยบายการบริหารจัดการข้อมูล กรมกิจการสตรีและสถาบันครอบครัว

ด้วยพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ มาตรา ๘ (๔) การกำหนดนโยบายหรือกฎเกณฑ์การเข้าถึงและใช้ประโยชน์จากข้อมูลที่ชัดเจนและมีระบบบริหารจัดการ รวมทั้งมีมาตรการและหลักประกันในการคุ้มครองข้อมูลที่อยู่ในความครอบครองให้มีความมั่นคงปลอดภัยและมิให้ข้อมูลส่วนบุคคลถูกละเมิด และกฎเกณฑ์ข้อมูล และตามประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ ข้อ ๔ (๕) การจำแนกหมวดหมู่ของข้อมูล เพื่อกำหนดนโยบายข้อมูลหรือกฎเกณฑ์เกี่ยวกับผู้มีสิทธิเข้าถึงและใช้ประโยชน์จากข้อมูลต่าง ๆ ภายในหน่วยงาน สำหรับให้ผู้ซึ่งมีหน้าที่เกี่ยวข้องปฏิบัติตามนโยบายหรือกฎเกณฑ์ได้อย่างถูกต้องและสอดคล้องตามกฎหมายที่เกี่ยวข้อง อันจะนำไปสู่การบริหารจัดการข้อมูลภาครัฐอย่างเป็นระบบ รวมทั้งสนับสนุนการจัดทำบัญชีข้อมูลหน่วยงานให้ได้มาตรฐานและเป็นไปในทิศทางเดียวกัน สอดคล้องตามกรอบธรรมาภิบาลข้อมูลภาครัฐ

นโยบายการบริหารจัดการข้อมูล กรมกิจการสตรีและสถาบันครอบครัว ประกอบด้วย ข้อกำหนดทั่วไป การจัดหมวดหมู่และชั้นความลับของข้อมูล การบริหารจัดการข้อมูลตามวงจรชีวิตของข้อมูล คุณภาพข้อมูล ข้อกฎหมายและเอกสารอ้างอิง เพื่อให้หน่วยงานในสังกัดกรมกิจการสตรีและสถาบันครอบครัวใช้เป็นกรอบและแนวทางในการบริหารจัดการข้อมูลให้มีความมั่นคงปลอดภัย มีความโปร่งใส และสามารถตรวจสอบได้ รวมทั้งเพื่อให้ข้อมูลของหน่วยงานมีคุณภาพ เป็นที่ยอมรับเชื่อถือ และสามารถนำไปบูรณาการกับหน่วยงานต่าง ๆ ได้อย่างมีประสิทธิภาพ จึงได้กำหนดใช้นโยบายการบริหารจัดการข้อมูล กรมกิจการสตรีและสถาบันครอบครัว รายละเอียดตามแนบท้ายประกาศนี้

จึงประกาศให้ทราบโดยทั่วกัน

ประกาศ ณ วันที่ ๒๔ สิงหาคม พ.ศ. ๒๕๖๖

(นางจินตนา จันทร์บำรุง)
อธิบดีกรมกิจการสตรีและสถาบันครอบครัว

นโยบายการบริหารจัดการข้อมูล (Data Management Policy)

ของกรมกิจการสตรีและสถาบันครอบครัว

เวอร์ชั่น	ผู้อนุมัติ	วันที่อนุมัติ	วันที่มีผลบังคับใช้	การปรับปรุงครั้งถัดไป
1.0	นางจินตนา จันทร์บำรุง (อธิบดีกรมกิจการสตรีและสถาบันครอบครัว)	28 ส.ค. 2566	28 ส.ค. 2566	

ด้วยพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 มาตรา 8 (4) การกำหนดนโยบายหรือกฎเกณฑ์การเข้าถึงและใช้ประโยชน์จากข้อมูลที่ชัดเจนและมีระบบบริหารจัดการรวมทั้งมีมาตรการและหลักประกันในการคุ้มครองข้อมูลที่อยู่ในความครอบครองให้มีความมั่นคงปลอดภัยและมิให้ข้อมูลส่วนบุคคลถูกละเมิด และกฎเกณฑ์ข้อมูล และตามประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ ข้อ 4 (5) การจำแนกหมวดหมู่ของข้อมูล เพื่อกำหนดนโยบายข้อมูลหรือกฎเกณฑ์ เกี่ยวกับผู้มีสิทธิเข้าถึงและใช้ประโยชน์จากข้อมูลต่าง ๆ ภายในหน่วยงาน สำหรับให้ผู้ซึ่งมีหน้าที่เกี่ยวข้อง ปฏิบัติตามนโยบายหรือกฎเกณฑ์ได้อย่างถูกต้อง และสอดคล้องตามกฎหมายที่เกี่ยวข้อง อันจะนำไปสู่การบริหารจัดการข้อมูลภาครัฐอย่างเป็นระบบ รวมทั้งสนับสนุนการจัดทำบัญชีข้อมูลหน่วยงานให้ได้มาตรฐาน และเป็นไปในทิศทางเดียวกัน สอดคล้องตามกรอบธรรมาภิบาลข้อมูลภาครัฐ

กรมกิจการสตรีและสถาบันครอบครัว (สค.) จึงได้กำหนดนโยบายการบริหารจัดการข้อมูลของ สค. ซึ่งจะเป็นกรอบและแนวทางในการบริหารจัดการข้อมูลให้มีความมั่นคงปลอดภัย มีความโปร่งใส และสามารถตรวจสอบได้ รวมทั้งเพื่อให้ข้อมูลของ สค. มีคุณภาพ เป็นที่ยอมรับและเชื่อถือของผู้ใช้งาน และสามารถนำไปบูรณาการกับหน่วยงานต่าง ๆ ได้อย่างมีประสิทธิภาพ

1. วัตถุประสงค์

1) เพื่อให้การบริหารจัดการข้อมูลของ สค. สอดคล้องกับกฎหมาย กรอบธรรมาภิบาลข้อมูลภาครัฐ และระเบียบปฏิบัติที่เกี่ยวข้อง รวมถึงการบริหารความเสี่ยงที่อาจเกิดขึ้นอันเนื่องมาจากการใช้ข้อมูล

2) เพื่อใช้เป็นกรอบและแนวทางสำหรับผู้บริหาร เจ้าหน้าที่ของ สค. และผู้ที่เกี่ยวข้องในการบริหารจัดการข้อมูลของหน่วยงานให้มีความมั่นคงปลอดภัย มีความโปร่งใส และสามารถตรวจสอบได้รวมทั้งเพื่อให้ข้อมูลของหน่วยงานมีคุณภาพ เป็นที่ยอมรับและเชื่อถือของผู้ใช้งาน และสามารถนำไปบูรณาการกับหน่วยงานต่าง ๆ ได้อย่างมีประสิทธิภาพ

3) เพื่อส่งเสริมการขับเคลื่อนองค์กรด้วยข้อมูล (Data Driven Organization) อย่างมีประสิทธิภาพและไปในทิศทางเดียวกัน

2. ขอบเขตและการบังคับใช้

1) นโยบายการบริหารจัดการข้อมูลฉบับนี้จัดทำโดยคณะอนุกรรมการธรรมาภิบาลข้อมูลภาครัฐ สค. และผ่านความเห็นชอบจาก คณะกรรมการธรรมาภิบาลข้อมูลภาครัฐ สค. มีผลบังคับใช้กับบัญชีข้อมูลที่แนบท้ายประกาศกรมกิจการสตรีและสถาบันครอบครัว

2) คณะกรรมการธรรมาภิบาลข้อมูลภาครัฐ สค. (DWF Data Governance Council) คณะอนุกรรมการธรรมาภิบาลข้อมูลภาครัฐ สค. ผู้ดูแลข้อมูล ผู้สร้างข้อมูล ผู้ใช้ข้อมูล ผู้บริหารจัดการฐานข้อมูล และบุคลากรที่เกี่ยวข้อง มีหน้าที่จะต้องสนับสนุน ดำเนินการ และปฏิบัติตามนโยบายอย่างเคร่งครัด

3. ข้อยกเว้น

นโยบายนี้อาจมีการขยายผลหรือมีการยกเว้นไม่ต้องปฏิบัติตามนโยบายดังกล่าวได้ ถ้ามีกฎหมายหรือระเบียบอื่นกำหนดไว้โดยเฉพาะ ให้บังคับตามบทบัญญัติแห่งกฎหมายนั้น

4. บทบาทและความรับผิดชอบ

1) อธิบดีกรมกิจการสตรีและสถาบันครอบครัวหรือผู้ที่ได้รับมอบหมาย ควบคุมและกำกับดูแลและส่งเสริมให้บุคลากรและผู้ที่เกี่ยวข้องมีความรู้และสามารถดำเนินการให้เป็นไปตามนโยบายการบริหารจัดการข้อมูลอย่างเคร่งครัด

2) บุคลากรในหน่วยงานและบุคคลอื่น ๆ เช่น บริษัทหรือผู้รับจ้าง ที่ได้รับมอบหมายจากหน่วยงานให้ทำหน้าที่บริหารจัดการข้อมูลต้องปฏิบัติตามกฎหมาย นโยบาย มาตรการ วิธีการ และแนวปฏิบัติต่าง ๆ ที่เกี่ยวข้องกับข้อมูลและระบบข้อมูลสารสนเทศที่หน่วยงานกำหนด

3) คณะกรรมการธรรมาภิบาลข้อมูลภาครัฐ/คณะอนุกรรมการธรรมาภิบาลข้อมูลภาครัฐ/เจ้าของข้อมูล ผู้ดูแลข้อมูล ผู้สร้างข้อมูล ผู้บริหารจัดการฐานข้อมูล และผู้ใช้ข้อมูล ต้องปฏิบัติหน้าที่ที่ได้รับมอบหมายภายใต้นโยบายนี้

5. คำนิยาม

1) ข้อมูล (Data) หมายความว่า สิ่งที่สื่อความหมายให้รู้เรื่องราวข้อเท็จจริงหรือเรื่องอื่นใด ไม่ว่าการสื่อ ความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเอง หรือโดยผ่านวิธีการใด ๆ และไม่ว่าจะได้จัดทำไว้ในรูปของ เอกสารแฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ภาพถ่ายดาวเทียม ฟิล์ม การบันทึกภาพหรือ เสียง การบันทึกโดยเครื่องคอมพิวเตอร์ เครื่องมือตรวจวัด การสำรวจระยะไกล หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึก ไว้ปรากฏได้

2) ชุดข้อมูล (Data Set) หมายความว่า การนำข้อมูลจากหลายแหล่งมารวบรวม เพื่อจัดเป็นชุดให้ตรงตาม ลักษณะโครงสร้างของข้อมูล หรือจากการใช้ประโยชน์ของข้อมูล

3) บัญชีข้อมูล (Data Catalog) หมายความว่า เอกสารแสดงบรรดารายการของชุดข้อมูล ที่จำแนกแยกแยะโดยการจัดกลุ่มหรือจัดประเภทข้อมูลที่อยู่ในความครอบครองหรือควบคุมของหน่วยงาน

4) ธรรมาภิบาลข้อมูลภาครัฐ (Data Governance for Government) หมายความว่า การกำหนดสิทธิ หน้าที่ และความรับผิดชอบของผู้มีส่วนได้เสียในการบริหารจัดการข้อมูลทุกขั้นตอน เพื่อให้การได้มาและการนำไปใช้ ข้อมูลของหน่วยงานภาครัฐถูกต้อง ครบถ้วน เป็นปัจจุบัน รักษาความเป็นส่วนตัวและสามารถเชื่อมโยงกันได้อย่าง มีประสิทธิภาพและมั่นคงปลอดภัย

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

6) การจัดชั้นความลับของข้อมูล (Data Classification) หมายความว่า การกำหนดประเภทและข้อกำหนดของการจัดชั้นความลับของข้อมูล เพื่อกำหนดสิทธิในการเข้าถึงและสามารถนำข้อมูลไปใช้ได้อย่างเหมาะสม ซึ่งตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 กำหนดให้มีชั้นความลับเป็นชั้นลับ ชั้นลับมาก หรือชั้นลับที่สุด โดยคำนึงถึงการปฏิบัติหน้าที่ของหน่วยงานและประโยชน์แห่งรัฐประกอบกัน ดังนั้น ชั้นความลับของข้อมูล มักถูกกำหนดให้สอดคล้องกับผลกระทบต่อหน่วยงานและความมั่นคงของ ประเทศ อาทิ ชื่อเสียง ความต่อเนื่องของการดำเนินงาน การเงิน และทรัพยากรบุคคล

7) วงจรชีวิตของข้อมูล (Data Life Cycle) หมายความว่า ลำดับขั้นตอนของข้อมูลตั้งแต่เริ่มสร้างข้อมูล ไปจนถึงการทำลายข้อมูล ตามกรอบธรรมาภิบาลข้อมูลภาครัฐ

8) ข้อมูลหลักและข้อมูลอ้างอิง (Master and Reference Data) หมายความว่า การบริหารจัดการข้อมูล เพื่อให้ทั้งหน่วยงานสามารถเข้าถึงและใช้ข้อมูลร่วมกันได้ โดยข้อมูลถูกจัดเก็บไว้แหล่งเดียว มีการกำหนด มาตรฐานของข้อมูล เพื่อช่วยลดความซ้ำซ้อนของข้อมูลและทำให้ข้อมูลมีคุณภาพ ซึ่ง Master data เป็นข้อมูล ที่สร้างและถูกใช้งานอยู่ภายในหน่วยงาน มีโอกาสเปลี่ยนแปลงได้และมีรายละเอียดหรือจำนวนฟิลด์ข้อมูล ที่มาก เช่น ข้อมูลกลุ่มเป้าหมาย ข้อมูลครุภัณฑ์ ข้อมูลการให้บริการ ข้อมูลผู้ใช้บริการ และข้อมูลสถานที่ ในขณะที่ Reference data มีความเป็นสากลถูกสร้างและใช้งานโดยทั่วไป โดยหลากหลายองค์กร หรือ แม้กระทั่งใช้งานไปทั่วโลก เช่น รหัสไปรษณีย์ รหัสประเทศ หน่วยวัดระยะทาง

9) คุณภาพของข้อมูล (Data Quality) หมายความว่า ข้อมูลที่ดี ได้มาตรฐานตามที่กำหนดและตรง กับความต้องการของผู้ใช้กล่าวคือผลรวมของคุณลักษณะและคุณสมบัติของผลิตผลข้อมูลที่พึงประสงค์ทุก ประการของผลการปฏิบัติงานตามดัชนีตัวชี้วัดคุณภาพและองค์ประกอบที่กำหนดไว้

10) การประเมินคุณภาพข้อมูล (Data Quality Assessment) หมายความว่า กระบวนการประเมินผลโดยภาพรวมว่า เมื่อได้มีการบริหารจัดการและกำกับดูแลคุณภาพข้อมูลแล้วทำให้เกิดการ เปลี่ยนแปลงในเชิงคุณภาพอย่างไร ทั้งนี้การตรวจสอบและประเมินคุณภาพจะต้องทำอย่างเป็นระบบมีหลักเกณฑ์และแนวปฏิบัติที่ชัดเจนมีการประกาศให้ทราบล่วงหน้าและกระทำโดยผู้ประเมินคุณภาพข้อมูล

11) คณะกรรมการธรรมาภิบาลข้อมูลภาครัฐ สค. หมายความว่า กลุ่มบุคคลที่หน่วยงานจัดตั้งขึ้นให้มีหน้าที่ กำหนดนโยบาย กรอบแนวทาง มาตรฐาน ทิศทางการดำเนินงาน ตรวจสอบ การกำกับ

และประเมินผลเพื่อให้สอดคล้องกับประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ รวมถึงแต่งตั้งคณะอนุกรรมการหรือคณะทำงานดำเนินงานด้านธรรมาภิบาลข้อมูล

12) คณะอนุกรรมการธรรมาภิบาลข้อมูลภาครัฐ สค. หมายความว่า กลุ่มบุคคลที่คณะกรรมการธรรมาภิบาลข้อมูลภาครัฐ สค. แต่งตั้งขึ้นเพื่อดำเนินการ ดังนี้

(1) ยุทธศาสตร์และนโยบายข้อมูล (Data Policy) มีหน้าที่ กำหนดนโยบาย กรอบแนวทาง มาตรฐานข้อมูล และทิศทางการดำเนินงาน

(2) บริกรข้อมูล (Data Steward มีหน้าที่กำหนดมาตรฐาน กำกับดูแล ติดตาม และรายงานผลการดำเนินการธรรมาภิบาลข้อมูลบริการด้านข้อมูล ซึ่งประกอบ บริกรข้อมูลด้านธุรกิจ (Business Data Steward) ทำหน้าที่รับผิดชอบในการนิยามความต้องการด้านคุณภาพ รักษาความเป็นส่วนบุคคล และความมั่นคงปลอดภัย เพื่อให้ได้ข้อมูลที่ตรงตามความต้องการของผู้ใช้ข้อมูลที่อาจได้รับมาจากผู้ใช้ข้อมูล บริกรข้อมูลด้านเทคนิค (Technical Data Steward) มีหน้าที่สนับสนุนด้านเทคโนโลยีสารสนเทศแก่บริกรข้อมูลด้านธุรกิจ และบริกรข้อมูลด้านคุณภาพข้อมูล (Data Quality Steward) มีหน้าที่ดำเนินการในเรื่องคุณภาพข้อมูล

(3) บูรณาการแลกเปลี่ยน เชื่อมโยง ความมั่นคงปลอดภัยของข้อมูล (Data Privacy and Data Security) มีหน้าที่ประเมินความพร้อมของธรรมาภิบาลข้อมูลภาครัฐ คุณภาพข้อมูล ความมั่นคงปลอดภัย และการรักษาความเป็นส่วนบุคคล

13) ผู้มีส่วนได้เสียกับข้อมูล (Data Stakeholders) หมายความว่า ผู้มีส่วนได้ส่วนเสียกับข้อมูล ได้แก่ เจ้าของข้อมูล ทีมจัดการข้อมูล ผู้ใช้ข้อมูล และผู้สร้างข้อมูล มีหน้าที่ มีส่วนร่วมในการดำเนินงานด้านธรรมาภิบาลข้อมูลภาครัฐ แจ้งประเด็นปัญหาที่พบระหว่างการใช้ข้อมูลทั้งด้านคุณภาพ การรักษาความเป็นส่วนบุคคลและความมั่นคงปลอดภัยของข้อมูล รวมถึงให้ข้อคิดเห็น ข้อเสนอแนะ

14) เจ้าของข้อมูล (Data Owner) หมายความว่า ผู้ที่ได้รับมอบหมายในการปฏิบัติงานให้ รับผิดชอบข้อมูลที่ระบุไว้ ซึ่งรวมถึงผู้บังคับบัญชาของเจ้าของข้อมูลนั้นด้วย โดยทำหน้าที่กำกับดูแลตามธรรมาภิบาลข้อมูล และตามกฎ ระเบียบที่กำหนดไว้ (กรณีข้อมูลลับ) ตลอดวงจรชีวิตของข้อมูลนั้น ๆ รวมทั้งทำหน้าที่กำหนดสิทธิในการเข้าถึงข้อมูลและกำหนดชั้นความลับของข้อมูล

15) ผู้ดูแลข้อมูล หมายความว่า ผู้ที่มีข้อมูลหรือผู้ที่ได้รับการแต่งตั้งให้รับผิดชอบข้อมูลนั้น มีหน้าที่จัดการและกำกับดูแลข้อมูลให้มีคุณภาพเพื่อสร้างความมั่นใจให้กับผู้ใช้ข้อมูล รวมถึงป้องกันภัยคุกคาม สำรองข้อมูลและรักษาความปลอดภัยของข้อมูล

16) ผู้บริหารจัดการฐานข้อมูล (Database Administrator) หมายความว่า ผู้ที่ดูแลฐานข้อมูลและระบบจัดการฐานข้อมูล มีหน้าที่รับผิดชอบด้านความปลอดภัยของข้อมูล ประสานงาน และตรวจสอบการใช้งาน รวมทั้งจัดหา และดูแลรักษาอุปกรณ์ ทั้งทางด้านฮาร์ดแวร์ และซอฟต์แวร์

17) ผู้สร้างข้อมูล (Data Creators) หมายความว่า ผู้ที่ทำหน้าที่บันทึก แก้ไข ปรับปรุง หรือลบข้อมูลให้สอดคล้องกับโครงสร้างที่ถูกกำหนดไว้

18) ผู้ใช้ข้อมูล (Data Users) หมายความว่า บุคลากรในหน่วยงาน รวมถึงหน่วยงานภายนอกที่ได้รับอนุญาต (Authorized Users) ให้สามารถเข้ามาใช้ ข้อมูลของหน่วยงานตามสิทธิและหน้าที่ความรับผิดชอบ พร้อมทั้งรายงาน ประเด็นปัญหาที่พบระหว่างการใช้ข้อมูล

19) เจ้าของข้อมูลส่วนบุคคล (Data Subject) หมายความว่า บุคคลธรรมดาที่เป็นเจ้าของข้อมูลส่วนบุคคล

20) เจ้าของระบบงาน (System Owner) หมายความว่า ผู้ที่มีหน้าที่รับผิดชอบในการใช้งาน ดูแลและบำรุงรักษา หรือปรับปรุง ระบบงานที่ใช้ในหน่วยงาน

6. นโยบายการบริหารจัดการข้อมูล

6.1 ข้อกำหนดทั่วไป

1) การกำหนดบทบาท หน้าที่ และความรับผิดชอบของแต่ละบุคคลตามโครงสร้างธรรมาภิบาลข้อมูลภาครัฐ ต้องได้รับการมอบอำนาจและการอนุมัติจากผู้บริหาร พร้อมทั้งกำหนดหน่วยงานเจ้าของข้อมูล เพื่อทำหน้าที่ในการบริหารจัดการข้อมูลนั้นๆ

2) มีการจัดทำนโยบายการบริหารจัดการข้อมูลเป็นลายลักษณ์อักษร มีการอนุมัติเผยแพร่เพื่อประกาศใช้ และถือปฏิบัติ โดยให้มีผลบังคับใช้กับบุคลากรในหน่วยงาน ตลอดจนหน่วยงาน/บุคคลภายนอกที่เกี่ยวข้องกับการได้มาและการใช้ข้อมูลของหน่วยงาน พร้อมทั้งจัดทำแนวปฏิบัติและมาตรฐานที่เกี่ยวกับข้อมูลเพื่อสนับสนุนการปฏิบัติงานให้สอดคล้องตามนโยบายดังกล่าว

3) มีการกำหนดมาตรการ วิธีการ และแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของข้อมูลเพื่อป้องกันการละเมิด การเข้าถึง การสูญหาย การทำลาย หรือการเปลี่ยนแปลงข้อมูล โดยปราศจากอำนาจโดยมิชอบหรือโดยมิได้รับอนุญาต โดยให้เป็นไปตามนโยบายความมั่นคงปลอดภัยสารสนเทศของกรมกิจการสตรีและสถาบันครอบครัว

4) มีการกำหนดมาตรการ วิธีการ และแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลที่สอดคล้องกับกฎหมาย ระเบียบ และแนวปฏิบัติของหน่วยงาน โดยให้เป็นไปตามนโยบาย การคุ้มครองข้อมูลส่วนบุคคลของกรมกิจการสตรีและสถาบันครอบครัว และเป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

5) มีการตรวจสอบความมีอยู่และรายละเอียดของข้อมูลที่สำคัญ เช่น คำอธิบายข้อมูลหรือเมทาดาตา ชุดข้อมูล การจัดชั้นความลับข้อมูล และมีการรายงานผลให้แก่ผู้รับผิดชอบตามโครงสร้างธรรมาภิบาลข้อมูลภาครัฐ ตลอดจนมีการดำเนินการตามกระบวนการธรรมาภิบาลข้อมูลภาครัฐ

6) มีการตรวจสอบ ติดตาม และประเมินผลการปฏิบัติตามนโยบายการบริหารจัดการข้อมูลโดยผู้ตรวจประเมินที่คณะกรรมการธรรมาภิบาลข้อมูลของ กรมกิจการสตรีและสถาบันครอบครัว กำหนด พร้อมทั้งมีการกำหนดให้มีการทบทวนนโยบาย รวมถึง มาตรการ วิธีการ และแนวปฏิบัติต่าง ๆ เกี่ยวกับข้อมูลอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญตามความเหมาะสม

7) มีการตรวจสอบ ติดตาม และประเมินผลการดำเนินงานธรรมาภิบาลข้อมูลของหน่วยงานอย่างน้อยปีละ 1 ครั้ง ในเรื่อง (1) การประเมินความพร้อมธรรมาภิบาลข้อมูล (2) การประเมินคุณภาพข้อมูล โดยให้

เป็นไปตามประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่องมาตรฐานรัฐบาลดิจิทัลว่าด้วยหลักเกณฑ์การประเมินคุณภาพข้อมูลสำหรับหน่วยงานภาครัฐ และ (3) การประเมินความมั่นคงปลอดภัยของข้อมูลเป็นอย่างน้อย

8) จัดให้มีทรัพยากรด้านงบประมาณ ทรัพยากรบุคคล และเทคโนโลยีที่เพียงพอต่อการบริหารจัดการข้อมูล พร้อมทั้งสนับสนุนการฝึกอบรมธรรมาภิบาลข้อมูลภาครัฐและการบริหารจัดการข้อมูลให้ครอบคลุมทั้งวงจรชีวิตของข้อมูลแก่บุคลากรในหน่วยงาน อย่างน้อยปีละ 1 ครั้ง

9) ข้อกำหนดอื่น ๆ ตามที่หน่วยงานกำหนดเพิ่มเติม

6.2 <u>การจัดหมวดหมู่และชั้นความลับของข้อมูล</u>

1) กำหนดหมวดหมู่และประเภทชั้นความลับของข้อมูลที่ใช้กับข้อมูลทุกรูปแบบของหน่วยงาน ด้วยการประเมินผลกระทบของข้อมูลหน่วยงาน เพื่อระบุหมวดหมู่และประเภทชั้น ความลับของข้อมูล รวมทั้งกำหนดความปลอดภัยที่เหมาะสมสำหรับการสร้าง/จัดเก็บ การใช้ และการ เข้าถึงชุดข้อมูล และเพื่อใช้กับบุคลากรรวมถึงตัวแทนบุคคลที่สามที่ได้รับอนุญาตให้เข้าถึงข้อมูลในหน่วยงาน พร้อมทั้งกำหนด หน้าที่ให้บุคลากรในการจัดหมวดหมู่และชั้นความลับ เพื่อป้องกัน จัดการ และกำกับ ดูแลข้อมูลให้เหมาะสม

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

3) กำกับดูแลและติดตามอย่างต่อเนื่อง โดยตรวจสอบความปลอดภัยการใช้งานและรูปแบบการเข้าถึง ของระบบและข้อมูลทั้งผ่านกระบวนการอัตโนมัติหรือโดยบุคคล เพื่อระบุภัยคุกคามภายนอก การบำรุงรักษา การทำงานของระบบตามปกติ และติดตามการเปลี่ยนแปลงของสภาพแวดล้อมของระบบและข้อมูล

6.3 <u>การบริหารจัดการข้อมูลตามวงจรชีวิตของข้อมูล</u>

1) กำหนดนโยบาย แนวปฏิบัติ และสภาพแวดล้อมการบริหารจัดการข้อมูลตามวงจรชีวิตของข้อมูลที่เอื้อต่อการรักษาความมั่นคงปลอดภัย คุ้มครองความเป็นส่วนตัวของข้อมูล และเพื่อให้ได้ข้อมูลที่มี คุณภาพ

2) จัดทำแนวปฏิบัติการจัดการชุดข้อมูล รวมถึงการรักษาความปลอดภัยตามหมวดหมู่และประเภทชั้นความลับตามแนวทางที่เหมาะสม และปรับปรุงอย่างต่อเนื่องให้สอดคล้องกับสถานการณ์

3) จัดเก็บข้อมูลให้สอดคล้องกับแนวทางหรือมาตรฐานการจัดชั้นความลับของข้อมูลที่กำหนดไว้ โดย ข้อมูลต้องมีความถูกต้อง สมบูรณ์ และเป็นปัจจุบัน พร้อมทั้งกำหนดสิทธิและจัดหาระบบ/เครื่องมือที่ใช้ในการเข้าถึงข้อมูลเพื่อรักษาความมั่นคงปลอดภัยและคุณภาพข้อมูล และทำลายข้อมูลตามแนวปฏิบัติและกฎหมายที่เกี่ยวข้อง

4) จัดทำแนวปฏิบัติและมาตรฐานการประมวลผลและใช้ข้อมูล เพื่อผู้ใช้นำข้อมูลไปใช้อย่างถูกต้องตามวัตถุประสงค์ที่ต้องการเพื่อให้เกิดประโยชน์สูงสุด

5) ห้ามเปิดเผยข้อมูลที่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง นโยบาย และแนวปฏิบัติ ไม่ว่าข้อมูลจะ อยู่ในรูปแบบใดหรือสถานที่ใดก็ตาม และต้องได้รับการอนุญาตจากตัวแทนหน่วยงาน หรือเจ้าของ ข้อมูลก่อนการเปิดเผยข้อมูล รวมทั้งจัดให้มีช่องทางการเปิดเผยข้อมูลที่เข้าถึงและนำไปใช้ได้ง่าย โดยให้เป็นไปตามประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง มาตรฐานและหลักเกณฑ์การเปิดเผยข้อมูลเปิดภาครัฐ ในรูปแบบข้อมูลดิจิทัลต่อสาธารณะ

6) กระบวนการ เทคโนโลยี และมาตรฐานทางเทคนิคที่ใช้ในการแลกเปลี่ยนข้อมูล และจัดทำสัญญาอนุญาตหรือข้อตกลงในการแลกเปลี่ยนข้อมูลและการนำข้อมูลไปใช้ โดยให้เป็นไปตามประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง มาตรฐานและหลักเกณฑ์การเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัล ว่าด้วยเรื่อง กรอบแนวทางการพัฒนามาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ

7) จัดทำแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยด้านคุณภาพข้อมูลและด้านคุ้มครองความเป็นส่วนตัวของข้อมูล รวมถึงแนวปฏิบัติให้กับผู้ประสานงานหรือศูนย์ติดต่อ (Contact Center) และตรวจสอบให้แน่ใจว่าได้บริหารจัดการข้อมูลอย่างเหมาะสมตามแนวทางหรือแนวปฏิบัติที่กำหนดไว้

8) สร้างความรู้ความเข้าใจในการบริหารจัดการข้อมูลตามวงจรชีวิตของข้อมูล ให้แก่ผู้เกี่ยวข้องภายในหน่วยงาน

9) แนวทางอื่น ๆ ตามที่หน่วยงานกำหนดเพิ่มเติม

6.4 <u>คุณภาพข้อมูล</u>

1) มีการจัดการข้อมูลของ กรมกิจการสตรีและสถาบันครอบครัว ให้มีคุณภาพตามประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่องมาตรฐานรัฐบาลดิจิทัลว่าด้วยหลักเกณฑ์การประเมินคุณภาพข้อมูลสำหรับหน่วยงานภาครัฐ โดยผู้ดูแลข้อมูล มีหน้าที่จัดการและกำกับดูแลข้อมูลให้มีคุณภาพเพื่อสร้างความมั่นใจให้กับผู้ใช้ข้อมูล ในขณะที่ผู้ใช้ข้อมูล มีบทบาทในการให้ข้อเสนอแนะแก่ผู้ดูแลข้อมูลเพื่อการปรับปรุงคุณภาพให้ดียิ่งขึ้น

2) มีการจัดทำเกณฑ์คุณภาพข้อมูลที่สามารถวัดผลได้ พร้อมทั้งจัดทำแผนพัฒนาคุณภาพข้อมูลที่สามารถระบุตัวชี้วัดคุณภาพและแผนปฏิบัติการเพื่อจัดการคุณภาพข้อมูลได้อย่างมีประสิทธิภาพ โดยออกแบบการเก็บ รวบรวมข้อมูลเพื่อให้ได้ข้อมูลสำหรับประเมินคุณภาพตามเกณฑ์ดังกล่าวให้รวมอยู่ในระบบเทคโนโลยีสารสนเทศและกระบวนการทำงาน (Quality by design) เพื่อลดข้อผิดพลาดและปรับปรุงคุณภาพตั้งแต่จุดการป้อนข้อมูลหรือการสร้างข้อมูลไปจนถึงการประมวลผลข้อมูล โดยให้เป็นไปตามประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่องมาตรฐานรัฐบาลดิจิทัลว่าด้วยหลักเกณฑ์การประเมินคุณภาพข้อมูลสำหรับหน่วยงานภาครัฐ

3) มีการประเมินผลและจัดการคุณภาพข้อมูลอย่างสม่ำเสมอตลอดวงจรชีวิตของข้อมูล โดยเจ้าของข้อมูล และบริกรข้อมูล ต้องกำหนดกรอบคุณภาพข้อมูลที่เป็นไปตามประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่องมาตรฐานรัฐบาลดิจิทัลว่าด้วยหลักเกณฑ์การประเมินคุณภาพข้อมูลสำหรับหน่วยงานภาครัฐ

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

5) แนวทางอื่น ๆ ตามที่หน่วยงานกำหนดเพิ่มเติม

7. ข้อกฎหมายและเอกสารอ้างอิง

1. พระราชบัญญัติการฌาปนกิจสงเคราะห์ พ.ศ. 2545 และกฎ/ระเบียบที่เกี่ยวข้อง
2. พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562
3. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
4. พระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. 2540
5. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
6. พระราชบัญญัติคุ้มครองผู้ถูกกระทำด้วยความรุนแรงในครอบครัว พ.ศ. 2550 และกฎ/ระเบียบที่เกี่ยวข้อง
7. พระราชบัญญัติความเท่าเทียมระหว่างเพศ พ.ศ. 2558 และกฎ/ระเบียบที่เกี่ยวข้อง
8. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม
9. พระราชบัญญัติป้องกันและปราบปรามการค้าประเวณี พ.ศ. 2539 และกฎ/ระเบียบที่เกี่ยวข้อง
10. พระราชบัญญัติวิธีปฏิบัติราชการทางปกครอง พ.ศ. 2539 และที่แก้ไขเพิ่มเติม
11. พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544
12. ระเบียบกรมกิจการสตรีและสถาบันครอบครัวครอบครัวว่าด้วยการช่วยเหลือสตรีหรือครอบครัวที่ประสบปัญหาทางสังคม พ.ศ. 2560
13. ระเบียบกรมกิจการสตรีและสถาบันครอบครัวว่าด้วยเงินอุดหนุน พ.ศ. 2563 และที่แก้ไขเพิ่มเติม
14. ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม
15. ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ
16. ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง มาตรฐานและหลักเกณฑ์การเปิดเผยข้อมูลเปิดภาครัฐในรูปแบบข้อมูลดิจิทัลต่อสาธารณะ
17. ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง มาตรฐานและหลักเกณฑ์ การเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัลว่าด้วยเรื่อง กรอบแนวทางการพัฒนามาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ (มรด. 2-1:2565)
18. ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง มาตรฐานรัฐบาลดิจิทัลว่าด้วย แนวทางการจัดทำบัญชีข้อมูลภาครัฐ (มรด. 3-1:2565)
19. ประกาศกรมกิจการสตรีและสถาบันครอบครัว เรื่อง นโยบายความมั่นคงปลอดภัยสารสนเทศของกรมกิจการสตรีและสถาบันครอบครัว

20. ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่องมาตรฐานรัฐบาลดิจิทัลว่าด้วยข้อเสนอแนะสำหรับการจัดทำนโยบายและแนวปฏิบัติการบริหารจัดการข้อมูล (มรด. 4-1:2565)

21. ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่องมาตรฐานรัฐบาลดิจิทัลว่าด้วยหลักเกณฑ์การประเมินคุณภาพข้อมูลสำหรับหน่วยงานภาครัฐ (มรด. 5:2565)

22. แผนปฏิบัติการกรมกิจการสตรีและสถาบันครอบครัว พ.ศ. 2566 – 2570

23. แผนปฏิบัติการดิจิทัลกรมกิจการสตรีและสถาบันครอบครัว พ.ศ. 2566 – 2570

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

8. ประวัติการแก้ไขเอกสาร

1) ประกาศนี้เริ่มใช้เมื่อ 28 สิงหาคม 2566

9. ข้อมูลเพิ่มเติม

การกำหนดบทบาทและความรับผิดชอบของผู้มีส่วนเกี่ยวข้อง

บทบาท	ความรับผิดชอบ
คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Committee)	เป็นไปตามคำสั่งคณะกรรมการธรรมาภิบาลข้อมูลภาครัฐ กรมกิจการสตรีและสถาบันครอบครัว ที่ 1/2566 ลงวันที่ 3 พฤษภาคม 2566 • ประกอบไปด้วย ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer) ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer) ผู้บริหารจากส่วน งานต่าง ๆ ทั้งจากฝ่ายบริหารและฝ่ายเทคโนโลยีสารสนเทศ รวมไปถึงประธานคณะอนุกรรมการธรรมาภิบาลข้อมูลภาครัฐ หัวหน้าทีมบริกรข้อมูล (Lead Data Steward) • มีอำนาจสูงสุดในธรรมาภิบาลข้อมูลภายในหน่วยงาน ทำหน้าที่ตัดสินใจเชิง นโยบาย แก้ไขปัญหา และบริหารจัดการข้อมูลของหน่วยงาน ทั้งนี้ ผู้บริหาร เทคโนโลยีสารสนเทศระดับสูงอาจจะทำหน้าที่แทนผู้บริหารข้อมูลระดับสูง

คณะอนุกรรมการธรรมาภิบาลข้อมูลภาครัฐ สค.	เป็นไปตามคำสั่งคณะกรรมการธรรมาภิบาลข้อมูลภาครัฐ กรมกิจการสตรีและสถาบันครอบครัว ที่ 1/2566 ลงวันที่ 3 พฤษภาคม 2566 • จัดทำ ร่างนโยบายข้อมูล มาตรฐาน และแนวปฏิบัติต่าง ๆ ที่เกี่ยวข้องกับข้อมูล • ทำหน้าที่ให้บริการข้อมูลและให้บริการด้านข้อมูล (Data Stewards) • นิยามความต้องการด้านคุณภาพและความมั่นคงปลอดภัย • นิยามคำอธิบายชุดข้อมูลหรือเมทาดาตา (Metadata) • ตรวจสอบการปฏิบัติตามนโยบายข้อมูล ตรวจสอบคุณภาพ ตรวจสอบ ความมั่นคงปลอดภัยของข้อมูล วิเคราะห์ผลจากการตรวจสอบ •บูรณาการแลกเปลี่ยน เชื่อมโยง และความมั่นคงปลอดภัยของข้อมูล
เจ้าของข้อมูล (Data Owner)	• ตรวจสอบ ดูแล และรักษาคุณภาพของข้อมูล • ทบทวนและอนุมัติการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับข้อมูล เพิ่มมีการกำหนดสิทธิ์ชั้นความลับด้วย
ผู้สร้างข้อมูล (Data Creator)	• บันทึก แก้ไข ปรับปรุง หรือลบข้อมูลให้สอดคล้องกับโครงสร้างที่ถูกกำหนดไว้ • ทำงานร่วมกับบริกรข้อมูล เพื่อตรวจสอบและแก้ไขปัญหาด้านคุณภาพข้อมูล และความปลอดภัยของข้อมูล
ผู้บริหารจัดการฐานข้อมูล (Database Administrator)	• บริหารจัดการ และควบคุมเกี่ยวกับระบบฐานข้อมูลภายในหน่วยงาน • กำหนดนโยบาย มาตรการ และมาตรฐานของระบบฐานข้อมูล ทั้งหมด ภายในหน่วยงาน เช่น รายละเอียดและวิธีการจัดเก็บข้อมูล การใช้งานฐานข้อมูล การรักษาความปลอดภัยของข้อมูล การสำรองข้อมูล การกู้คืน ข้อมูล เป็นต้น

ผู้ใช้ข้อมูล (Data User)	• นำข้อมูลไปใช้งานทั้งในระดับปฏิบัติงานและระดับบริหาร • สนับสนุนการกำกับดูแลข้อมูล • รายงานประเด็นปัญหาที่พบระหว่างการใช้ข้อมูล ทั้งด้านคุณภาพ และ ความปลอดภัยของข้อมูล

ความสัมพันธ์ระหว่างกระบวนการ/กิจกรรมและผู้มีส่วนได้ส่วนเสีย

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

หมายเหตุ

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

แนวปฏิบัติการบริหารจัดการข้อมูล
กรมกิจการสตรีและสถาบันครอบครัว

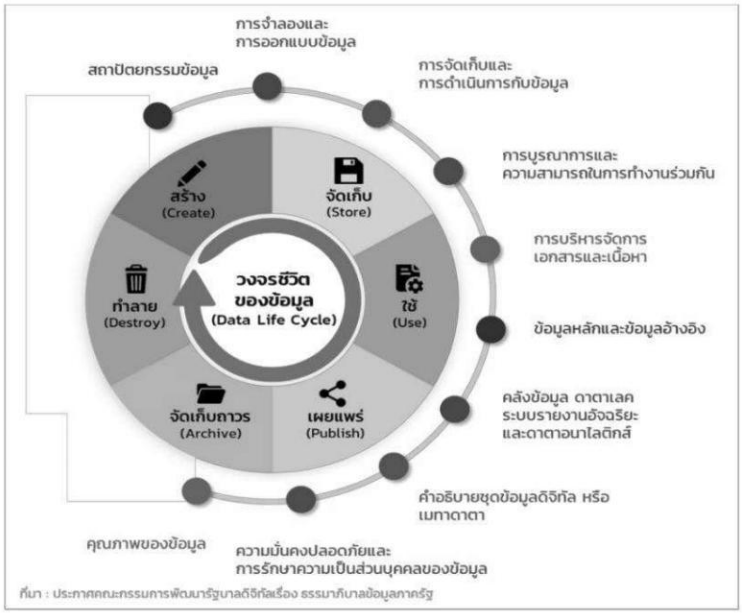
จัดทำโดย
คณะอนุกรรมการธรรมาภิบาลข้อมูลภาครัฐ
กรมกิจการสตรีและสถาบันครอบครัว

บทนำ

หลักการและขอบเขต

แนวปฏิบัติการบริหารจัดการข้อมูล ได้กำหนดขึ้นให้สอดคล้องตามนโยบายข้อมูล (Data Policy) ที่หน่วยงานประกาศ ซึ่งเป็นหนึ่งในองค์ประกอบตามกรอบธรรมาภิบาลข้อมูลภาครัฐ จัดทำโดยคณะอนุกรรมการธรรมาภิบาลข้อมูลภาครัฐ กรมกิจการสตรีและสถาบันครอบครัว มีผลบังคับใช้กับผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับข้อมูลตามแนวปฏิบัติที่ กรมกิจการสตรีและสถาบันครอบครัว (สค.) ประกาศ ซึ่งมีหน้าที่โดยตรงที่จะต้องสนับสนุน ดำเนินการและปฏิบัติตามอย่างเคร่งครัด และผู้ใช้อื่นที่เกี่ยวข้องแต่ไม่มีหน้าที่ในการดูแลข้อมูลจะต้องให้ความร่วมมือในการดำเนินการตามแนวปฏิบัตินี้ ผู้ฝ่าฝืนมีความผิดและจะต้องได้รับการดำเนินการตามระเบียบของหน่วยงาน โดยแนวปฏิบัติจะต้องครอบคลุมระบบบริหารและกระบวนการจัดการข้อมูล หรือวงจรชีวิตของข้อมูลและองค์ประกอบในการบริหารจัดการข้อมูลดังรูปต่อไปนี้

วงจรชีวิตของข้อมูล



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

2. การจัดเก็บข้อมูล (Store) เป็นการจัดเก็บข้อมูลที่เกิดจากกระบวนการสร้างหรือข้อมูลที่ได้จากการเชื่อมโยงและ/หรือแลกเปลี่ยนกับหน่วยงานอื่น ไม่ว่าจะจัดเก็บลงแฟ้มข้อมูล (File) หรือระบบการจัดการฐานข้อมูล (Database Management System - DBMS) 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

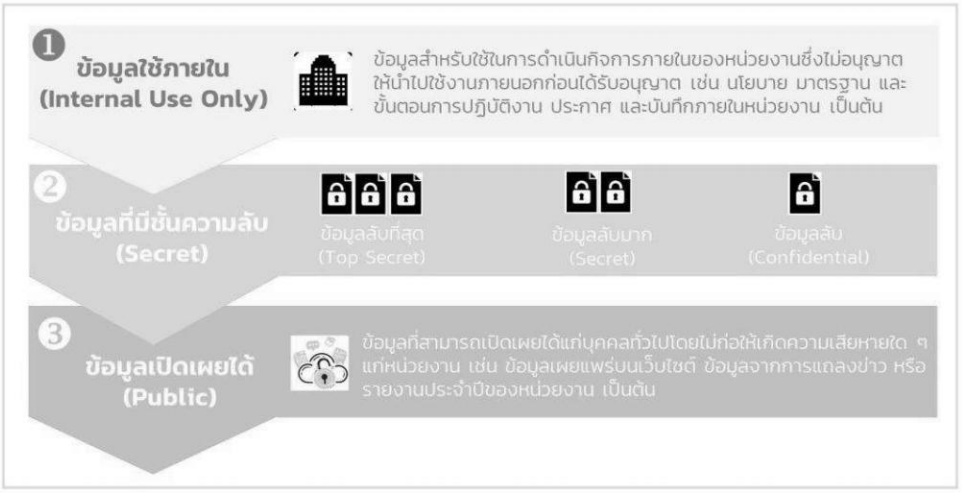
ข้อมูลของหน่วยงานสามารถแบ่งหมวดหมู่ตามกรอบธรรมาภิบาลข้อมูลและการใช้งานภายในหน่วยงาน ดังนี้

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

โดยมีการจัดระดับชั้นความลับของข้อมูล ดังนี้

- ข้อมูลใช้ภายใน (Internal Use Only) ได้แก่ ข้อมูลสำหรับใช้ในการดำเนินกิจการภายในของหน่วยงานซึ่งไม่อนุญาตให้นำไปใช้งานภายนอกก่อนได้รับอนุญาต เช่น นโยบาย มาตรฐานและขั้นตอนการปฏิบัติงาน 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)


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

คำนิยาม

คำศัพท์	ความหมาย
กรม	กรมกิจการสตรีและสถาบันครอบครัว
คณะกรรมการธรรมาภิบาลข้อมูลภาครัฐ สค. (Data Governance Council)	ประกอบด้วย ผู้บริหารข้อมูลระดับสูง (Chief Data Officer) ผู้เชี่ยวชาญเฉพาะด้าน ผู้อำนวยการ สำนัก/กอง และหัวหน้าหน่วยขึ้นตรงต่าง ๆ รวมไปถึงผู้อำนวยการกลุ่มกฎหมาย และกลุ่มเทคโนโลยีสารสนเทศ คณะกรรมการธรรมาภิบาลข้อมูลมีอำนาจสูงสุดในธรรมาภิบาลข้อมูลภายในหน่วยงาน หรือ คณะกรรมการ/คณะทำงาน ซึ่งทำหน้าที่ตัดสินใจเชิงนโยบาย แก้ไขปัญหา และบริหารจัดการข้อมูลของหน่วยงาน
คณะอนุกรรมการธรรมาภิบาลข้อมูลภาครัฐ สค.	ประกอบด้วย ผู้เชี่ยวชาญเฉพาะด้าน ผู้อำนวยการกองยุทธศาสตร์และแผนงาน ผู้อำนวยการกลุ่มมาตรการและกลไกของกองต่าง ๆ และผู้แทนกอง/สำนัก/หน่วยขึ้นตรง รวมทั้งผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศ และผู้อำนวยการกลุ่มนโยบายและยุทธศาสตร์ โดยทำหน้าที่จัดทำยุทธศาสตร์และนโยบายข้อมูล (Data Policy) บริหารจัดการข้อมูล (Data Management) บริกรข้อมูลด้านธุรกิจ (Business Data Stewards) บริกรข้อมูลด้านเทคนิค (Technical Data Stewards) บริกรข้อมูลด้านคุณภาพ (Data Quality Stewards) รวมทั้งบูรณาการแลกเปลี่ยนเชื่อมโยงความมั่นคงปลอดภัยข้อมูล
หัวหน้าหน่วยงานของรัฐ	อธิบดีกรมกิจการสตรีและสถาบันครอบครัว
ผู้บริหาร	ผู้บริหารที่เกี่ยวข้องกับการบริหารจัดการข้อมูล ตามคณะกรรมการ/คณะอนุกรรมการ/คณะทำงานที่เกี่ยวข้อง
ข้าราชการ/ลูกจ้างประจำ/พนักงานราชการ	บุคคลผู้ที่หน่วยงานบรรจุและแต่งตั้งเป็นเจ้าหน้าที่ของหน่วยงาน
ลูกจ้าง	บุคคลผู้ที่หน่วยงานจ้างให้ปฏิบัติงานเป็นการชั่วคราวโดยมีสัญญาจ้างที่กำหนดระยะเวลาจ้างและสิ้นสุดที่แน่นอน
ผู้บังคับบัญชา	ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของหน่วยงาน
ผู้สร้างข้อมูล (Data Creators)	บุคลากร (ข้าราชการ/ ลูกจ้างประจำ/ พนักงานราชการ/ ลูกจ้าง) ของทุกกอง/สำนัก/กลุ่มขึ้นตรง ที่ทำหน้าที่บันทึก แก้ไข ปรับปรุง หรือลบข้อมูลให้สอดคล้องกับโครงสร้างที่ถูกกำหนดไว้
ผู้ใช้ข้อมูล (Data Users)	คณะกรรมการ คณะอนุกรรมการ ผู้อำนวยการ ข้าราชการ/ลูกจ้างประจำ/พนักงานราชการ/ ลูกจ้าง รวมถึงหน่วยงานภายนอกที่ได้รับอนุญาต (Authorized Users) ให้สามารถเข้ามาใช้ข้อมูลของหน่วยงานตามสิทธิและหน้าที่ความรับผิดชอบ พร้อมทั้งรายงานประเด็นปัญหาที่พบระหว่างการใช้ข้อมูล

คำศัพท์	ความหมาย
สิทธิของผู้ใช้งานข้อมูล	สิทธิและหน้าที่ตามบทบาท (Role) ที่เกี่ยวข้องกับข้อมูลและระบบสารสนเทศของหน่วยงาน มีดังนี้ - สิทธิใช้งานทั่วไป หมายถึง คณะกรรมการ ผู้อำนวยการ ข้าราชการ/เจ้าหน้าที่/พนักงาน ลูกจ้าง ที่ใช้งานระบบสารสนเทศพื้นฐานของสำนักงาน ผู้ใช้งานข้อมูลต้องขออนุญาตจากผู้บังคับบัญชา โดยให้ใช้แบบฟอร์มเพื่อขออนุมัติตามที่หน่วยงานกำหนด - สิทธิจำเพาะ หมายถึง สิทธิเฉพาะตามหน้าที่ความรับผิดชอบที่เกี่ยวข้องกับการปฏิบัติงาน ผู้ใช้งานข้อมูลต้องได้รับสิทธิจากผู้บังคับบัญชา - สิทธิพิเศษ หมายถึง สิทธิที่ได้รับมอบหมายเพิ่มเติมจากผู้บังคับบัญชาเป็นกรณีพิเศษ ผู้ใช้งานต้องได้รับมอบหมายจากผู้บังคับบัญชาเป็นครั้งคราว
เจ้าของข้อมูล (Data Owner)	ผู้ที่ได้รับมอบหมายในการปฏิบัติงานให้รับผิดชอบข้อมูลที่ระบุไว้ ซึ่งรวมถึงผู้บังคับบัญชาของเจ้าของข้อมูลนั้นด้วย โดยทำหน้าที่กำกับดูแลตามธรรมาภิบาลข้อมูลตลอดวงจรชีวิตของข้อมูลนั้น ๆ รวมทั้งทำหน้าที่กำหนดสิทธิในการเข้าถึงข้อมูลและจัดชั้นความลับของข้อมูล
เจ้าของข้อมูลส่วนบุคคล (Data Subject)	บุคคลธรรมดาที่เป็นเจ้าของข้อมูลส่วนบุคคลเกี่ยวกับบุคคลนั้นระบุถึง
เจ้าของระบบงาน (System Owner)	ผู้ที่มีหน้าที่รับผิดชอบในการใช้งาน ดูแลและบำรุงรักษา หรือปรับปรุงระบบงานที่ใช้ในหน่วยงาน
ทีมบริหารจัดการข้อมูล (Data Management Team)	คณะอนุกรรมการธรรมาภิบาลข้อมูลภาครัฐ หรือกลุ่มบุคคลที่ทำหน้าที่รับผิดชอบดูแลรักษาข้อมูลในระบบสารสนเทศของหน่วยงาน และสนับสนุนกิจกรรมของธรรมาภิบาลข้อมูลภาครัฐ เช่น ช่วยเหลือในการนิยามเมทาดาตา (Metadata) ร่างนโยบายข้อมูลและมาตรฐานข้อมูล และกำหนดสิทธิการเข้าถึงข้อมูลโดย DBA เป็นต้น
บริกรข้อมูลด้านธุรกิจ (Business Data Stewards)	คณะอนุกรรมการธรรมาภิบาลข้อมูลภาครัฐ หรือบุคลากรระดับหัวหน้ากลุ่ม/ส่วนงานจาก สำนัก/กอง/หน่วยขึ้นตรง ที่ได้รับมอบหมายให้ทำหน้าที่ - กำหนดนิยามความต้องการด้านคุณภาพและความมั่นคงปลอดภัยซึ่งอาจจะได้รับมาจากผู้ใช้ข้อมูล (Data Users) หรือผู้มีส่วนได้เสียอื่น ๆ - นิยามคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตาโดยการสนับสนุนจากผู้ใช้ข้อมูล - ร่างนโยบายข้อมูลด้วยการช่วยเหลือจากทีมบริหารจัดการข้อมูล (Data Management Team) - ตรวจสอบการปฏิบัติตามนโยบายข้อมูล ตรวจสอบคุณภาพ ตรวจสอบความมั่นคงปลอดภัยของข้อมูล วิเคราะห์ผลจากการตรวจสอบ แล้วรายงานผลลัพธ์ไปยังคณะกรรมการธรรมาภิบาลข้อมูลและผู้ที่เกี่ยวข้องอื่น ๆ ให้ทราบ
บริกรข้อมูลด้านเทคนิค (Technical Data Stewards)	คณะอนุกรรมการธรรมาภิบาลข้อมูลภาครัฐ บุคลากรกลุ่มเทคโนโลยีสารสนเทศ หรือบุคลากรจาก สำนัก/กอง/หน่วยขึ้นตรง ที่ทำหน้าที่ให้การสนับสนุนด้านเทคโนโลยีสารสนเทศแก่บริกรข้อมูลด้านธุรกิจ เช่น นิยามเมทาดาตาเชิงเทคนิคซึ่งอาจจะได้รับการช่วยเหลือจากทีมบริหารจัดการข้อมูล

คำศัพท์	ความหมาย
	ให้ข้อเสนอแนะเชิงเทคนิคในการร่างนโยบายข้อมูล ตรวจสอบคุณภาพข้อมูล ความมั่นคงปลอดภัยของข้อมูล และการปฏิบัติตามนโยบายข้อมูลในเชิงเทคนิค
ผู้ดูแลระบบสารสนเทศ (System Administrators)	บุคลากรของ สำนัก/กอง/หน่วยขึ้นตรง ที่มีหน้าที่ดูแลรับผิดชอบระบบสารสนเทศของหน่วยงาน
ผู้ดูแลระบบแม่ข่าย (Server Administrators)	บุคลากรที่มีหน้าที่ดูแลรับผิดชอบระบบแม่ข่ายของหน่วยงาน
ผู้จัดการโครงการ (Project Managers)	ผู้อำนวยการ สำนัก/กอง/หน่วยขึ้นตรง ที่ได้รับมอบหมายบริหารจัดการโครงการตามแผนดำเนินงาน
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
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)	เป็นระบบเครือข่ายที่สามารถเข้าถึงได้โดยผู้ใช้งานภายในหน่วยงานเท่านั้น โดยมีจุดประสงค์เพื่อการติดต่อสื่อสาร แลกเปลี่ยนข้อมูลและสารสนเทศของหน่วยงาน

คำศัพท์	ความหมาย
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
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)	ข้อมูลที่อยู่ในความครอบครองหรือควบคุมดูแลของหน่วยงานของรัฐที่มีคำสั่งไม่ให้มีการเปิดเผย และมีการกำหนดชั้นความลับของข้อมูล
ข้อมูลลับ (Confidential)	ข้อมูลข่าวสารซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์ของรัฐซึ่งผู้ที่สามารถเข้าถึงได้ต้องเป็นบุคคลที่มีสิทธิเท่านั้นและห้ามเผยแพร่ต่อบุคคลภายนอกเว้นแต่จะได้รับอนุมัติเป็นลายลักษณ์อักษรโดย รองอธิบดี/อธิบดี ขึ้นไปโดยต้องมีการลงนามในเอกสารข้อตกลงการไม่เปิดเผยข้อมูล (Non-Disclosure Agreement) เว้นแต่การเผยแพร่ดังกล่าวเป็นไปตามอำนาจที่กฎหมายให้การรับรอง
ข้อมูลลับมาก (Secret)	ข้อมูลข่าวสารซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรงซึ่งผู้ที่สามารถเข้าถึงได้ต้องเป็นบุคคลที่มีสิทธิเท่านั้นและห้ามเผยแพร่ต่อบุคคลภายนอก เว้นแต่จะได้รับอนุมัติเป็นลายลักษณ์อักษรโดย รองอธิบดี/อธิบดี ที่เป็นเจ้าของข้อมูลขึ้นไปโดยต้องมีการลงนามในเอกสารข้อตกลงการไม่เปิดเผยข้อมูล (Non-Disclosure Agreement) เว้นแต่การเผยแพร่ดังกล่าวเป็นไปตามอำนาจที่กฎหมายให้การรับรอง

คำศัพท์	ความหมาย
ข้อมูลลับที่สุด (Top Secret)	ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรงที่สุดซึ่งผู้ที่สามารถเข้าถึงได้ต้องเป็นบุคคลที่มีสิทธิเท่านั้นและห้ามเผยแพร่ต่อบุคคลภายนอกเว้นแต่จะได้รับอนุมัติเป็นลายลักษณ์อักษรโดย อธิบดี ต้องมีการลงนามในเอกสารข้อตกลงการไม่เปิดเผยข้อมูล (Non-Disclosure Agreement) เว้นแต่การเผยแพร่ดังกล่าวเป็นไปตามอำนาจที่กฎหมายให้การรับรอง
ข้อมูลใช้ภายใน (Internal Use Only)	ข้อมูลสำหรับใช้ในการดำเนินกิจการภายในของหน่วยงานซึ่งไม่อนุญาตให้นำไปใช้งานภายนอกก่อนได้รับอนุญาต เช่น นโยบาย มาตรฐาน และขั้นตอนการปฏิบัติงาน ประกาศ และบันทึกภายในหน่วยงาน เป็นต้น

การเผยแพร่และการทบทวน

แนวปฏิบัติเกี่ยวกับข้อมูลนี้จะต้องทำการเผยแพร่โดยการประกาศเวียนในระบบอินทราเน็ต เว็บไซต์ของหน่วยงาน และจดหมายอิเล็กทรอนิกส์เพื่อให้บุคลากรทุกคนของหน่วยงาน ได้รับทราบ และถือปฏิบัติตามแนวปฏิบัตินี้อย่างเคร่งครัด โดยแนวปฏิบัติที่จัดขึ้นนี้สามารถทบทวนได้เพื่อให้เหมาะสมกับบริบทการปฏิบัติงานจริง อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ รวมถึงเมื่อมีข้อเสนอแนะจากคณะกรรมการธรรมาภิบาลข้อมูลภาครัฐ

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. พระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537 ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัติลิขสิทธิ์ (ฉบับที่ 2) พ.ศ. 2558
2. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560
3. พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562
4. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553
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
8. ข้อปฏิบัติอื่น ๆ ตามที่หน่วยงานกำหนดเพิ่มเติม

กิจกรรม	ผู้มีส่วนได้ส่วนเสีย				
	เจ้าของข้อมูล	ผู้สร้างข้อมูล	ทีมบริหารจัดการข้อมูล	บริกรข้อมูล	ผู้ดูแลระบบสารสนเทศ
1. กำหนดผู้มีสิทธิในการสร้างข้อมูล และกำหนดหมวดหมู่และชั้นความลับ	R	I	I	C	S
2. กำหนดสิทธิในการสร้างข้อมูลในระบบให้แก่ผู้สร้างข้อมูล	S	I	I	I	R
3. สร้างข้อมูลที่ไม่ขัดต่อกฎหมายและจากแหล่งข้อมูลที่เชื่อถือได้เท่านั้น	C	R	I	C	S
4. จัดทำคำอธิบายชุดข้อมูลดิจิทัล	R	S	S	R	S
5. ประเมินคุณค่าของชุดข้อมูลดิจิทัล	R	I	I	R	I
6. ตรวจสอบความถูกต้องของข้อมูล	R	I	I	R	I

ตารางที่: 1 ผู้มีส่วนได้ส่วนเสียในการสร้างข้อมูล

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)

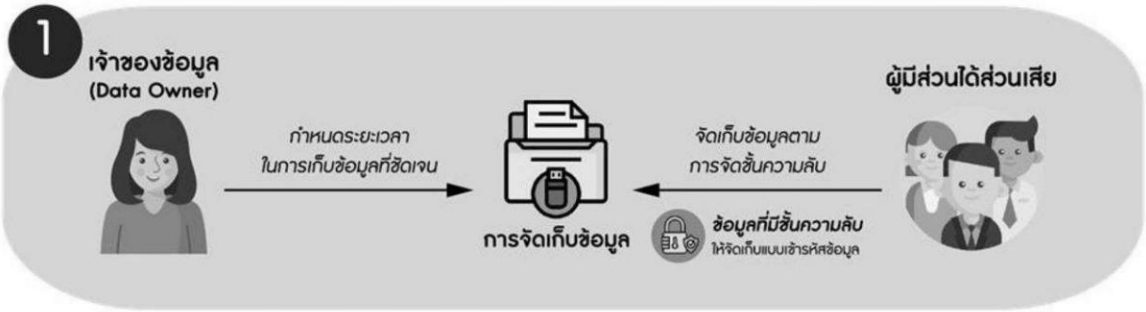
อ้างอิง

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

ข้อปฏิบัติ

1. กำหนดให้เจ้าของข้อมูลจะต้องกำหนดระยะเวลาในการจัดเก็บข้อมูลที่ชัดเจน
2. กำหนดให้ทีมบริหารจัดการข้อมูล และผู้ดูแลระบบสารสนเทศทำการย้ายข้อมูลที่มีการจัดเก็บเกินระยะเวลาที่กำหนดแล้วเพื่อจัดเก็บเป็นข้อมูลถาวร
3. กำหนดให้การจัดเก็บชุดข้อมูลจะต้องมีคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตา หากไม่มีหรือไม่ครบถ้วน ทีมบริหารจัดการข้อมูลจะต้องแจ้งผู้รับผิดชอบ ได้แก่ เจ้าของข้อมูล บริกรข้อมูลด้านเทคนิคและบริกรข้อมูลด้านธุรกิจ 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 เพื่อเป็นการป้องกันไม่ให้ผู้ไม่มีสิทธิในการเข้าถึงข้อมูลเข้าถึงข้อมูลได้

5. กำหนดให้มีวิธีปฏิบัติการกู้คืนข้อมูลที่จัดเก็บถาวร สำหรับข้อมูลที่มีความสำคัญมากต่อการดำเนินงานของหน่วยงาน เพื่อสอบทานความถูกต้อง ครบถ้วน ความพร้อมใช้งาน คุณภาพข้อมูล
6. ในการจัดเก็บข้อมูลส่วนบุคคล**ให้เก็บรวบรวมได้เท่าที่จำเป็น** ภายใต้อำนาจหน้าที่และวัตถุประสงค์



อันชอบด้วยกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล 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 รวมทั้งกรณีที่มีการเคลื่อนย้าย

อุปกรณ์ที่จัดเก็บข้อมูล เพื่อป้องกันมิให้มีการเข้าถึงโดยมิได้รับอนุญาต หรือลักลอบนำข้อมูลไปใช้ที่ก่อให้เกิดความเสียหายต่อหน่วยงาน

10. กำหนดมาตรการรักษาความปลอดภัยของข้อมูลที่จัดเก็บถาวร เพื่อป้องกันข้อมูลไม่ให้มีการลบ ปรับปรุง แก้ไขได้ รวมทั้งป้องกันมิให้ข้อมูลที่จัดเก็บถาวรรั่วไหลไปยังบุคคลที่ไม่ได้รับอนุญาต
11. กำหนดให้มีมาตรการรักษาความปลอดภัยของการถ่ายโอนข้อมูลกับหน่วยงานภายนอกที่ผ่านช่องทางการสื่อสารทุกชนิด โดยต้องสอดคล้องตามนโยบายความมั่นคงปลอดภัยสารสนเทศ
12. ห้ามมิให้จัดเก็บข้อมูลส่วนตัวหรือข้อมูลที่ไม่เกี่ยวข้องกับการดำเนินงานของหน่วยงาน สำหรับการจัดเก็บข้อมูลถาวรบนเครื่องแม่ข่ายที่หน่วยงานจัดสรรไว้
13. กำหนดให้มีการทบทวนเกี่ยวกับช่วงระยะเวลาการจัดเก็บข้อมูล มาตรการ และวิธีปฏิบัติที่เกี่ยวข้องกับการจัดเก็บข้อมูลถาวร อย่างน้อยปีละ 1 ครั้ง
14. ข้อปฏิบัติอื่น ๆ ตามที่หน่วยงานกำหนดเพิ่มเติม

กิจกรรม	**ผู้มีส่วนได้ส่วนเสีย**					
	เจ้าของข้อมูล	ผู้ดูแลระบบสารสนเทศ	ผู้สร้างข้อมูล	ผู้ใช้ข้อมูล	บริกรข้อมูล	ทีมบริหารจัดการข้อมูล
1. กำหนดระยะเวลาในการจัดเก็บข้อมูล	R	S	S	I	I	S
2. ย้ายข้อมูลที่มีการจัดเก็บเกินระยะเวลาที่กำหนด	I	R	I	I	I	R
3. จัดทำคำอธิบายชุดข้อมูลดิจิทัลและปรับปรุงให้เป็นปัจจุบัน	R	S	S	I	R	R
4. จัดเก็บข้อมูลตามการจัดชั้นความลับของหน่วยงาน	R	S	R	I	C	S
5. จัดเก็บข้อมูลส่วนบุคคลเท่าที่จำเป็น	R	R/S	S	R	C	S
6. ยกเลิกการจัดเก็บข้อมูลส่วนบุคคลกรณีเจ้าของข้อมูลส่วนบุคคลถอนความยินยอม	R	R	I	R	I	I
7. จัดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์	I	R	I	I	I	I

ตารางที่: 2 ผู้มีส่วนได้ส่วนเสียในการจัดเก็บข้อมูล

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. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
3. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553

ข้อปฏิบัติ

1. เจ้าของข้อมูลจะต้องกำหนดผู้มีสิทธิเข้าถึงเพื่อประมวลผลและใช้ข้อมูลตามชั้นความลับ ดังนี้
   - ข้อมูลเปิดเผยได้ ไม่กำหนดสิทธิการเข้าถึงเพื่อประมวลผลและใช้งานข้อมูล
   - ข้อมูลที่มีชั้นความลับ กำหนดให้ผู้ใช้งานที่ได้รับสิทธิเข้าถึงและใช้ข้อมูลตามอำนาจหน้าที่เท่านั้น
   - ข้อมูลใช้ภายใน กำหนดให้บุคลากรของหน่วยงานเท่านั้นที่มีสิทธิเข้าถึงเพื่อประมวลผลและใช้งานข้อมูลได้
2. ผู้ดูแลระบบสารสนเทศจะต้องกำหนดสิทธิในการเข้าถึงข้อมูลในระบบเพื่อประมวลผลและใช้ข้อมูลของผู้ใช้งานตามที่เจ้าของข้อมูลกำหนด
3. เจ้าของข้อมูลจะต้องทบทวนสิทธิการเข้าถึงเพื่อประมวลผลและใช้ข้อมูลของผู้ใช้งานอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ เช่น การลาออก เปลี่ยนตำแหน่ง โอนย้าย สิ้นสุดการจ้าง การปรับโครงสร้าง หรือเมื่อมีการปรับปรุงระบบสารสนเทศ
4. ผู้ที่มีสิทธิเข้าใช้งานข้อมูลที่มีชั้นความลับตามที่กำหนดโดยเจ้าของข้อมูลจะต้องใช้ข้อมูลอย่างระมัดระวัง โดยคำนึงถึงความปลอดภัยและต้องไม่ใช้งานข้อมูลที่มีชั้นความลับในพื้นที่สาธารณะ

5. ผู้ใช้ข้อมูลจะประมวลผลข้อมูลหรือใช้ข้อมูลส่วนบุคคลเท่าที่จำเป็นภายใต้อำนาจหน้าที่และวัตถุประสงค์อันชอบด้วยกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล หรือตามคำสั่งที่ได้รับจากหน่วยงานเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคล
6. หน่วยงานต้องยกเลิกการประมวลผลข้อมูลหรือการใช้ข้อมูลส่วนบุคคล กรณีที่เจ้าของข้อมูลส่วนบุคคลถอนความยินยอมตามที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลกำหนด

7. ผู้ใช้ข้อมูลจะต้องไม่ใช้ข้อมูลในเครือข่ายของหน่วยงานเพื่อประโยชน์ในเชิงธุรกิจเป็นการส่วนตัว หรือเพื่อเข้าสู่เว็บไซต์ที่ไม่เหมาะสมหรือใช้ข้อมูลอันก่อให้เกิดความเสียหายต่อหน่วยงาน
8. ข้อปฏิบัติอื่น ๆ ตามที่หน่วยงานกำหนดเพิ่มเติม

กิจกรรม	ผู้มีส่วนได้ส่วนเสีย		
	เจ้าของข้อมูล	ผู้ใช้ข้อมูล	ผู้ดูแลระบบสารสนเทศ
1. กำหนดสิทธิในการประมวลผลและใช้งานข้อมูลตามชั้นความลับ	R	I	I
2. กำหนดสิทธิในการประมวลผลและเข้าใช้งานข้อมูลในระบบ	C	I	R
3. ไม่ใช้ข้อมูลในเครือข่ายของหน่วยงานเพื่อประโยชน์ในเชิงธุรกิจเป็นการส่วนตัว	C	R	S
4. ประมวลผลข้อมูลหรือใช้ข้อมูลส่วนบุคคลเท่าที่จำเป็น	C	R	S
5. ยกเลิกการประมวลผลข้อมูลหรือการใช้ข้อมูลส่วนบุคคล กรณีที่เจ้าของข้อมูลส่วนบุคคลถอนความยินยอม	C	R	S

ตารางที่: 3 ผู้มีส่วนได้ส่วนเสียในการประมวลผลและใช้ข้อมูล

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

หมวด 4 การเปิดเผยข้อมูล

วัตถุประสงค์

กำหนดแนวปฏิบัติการเปิดเผยข้อมูลต่อสาธารณะโดยอิงจากกฎหมาย กฎเกณฑ์และแนวปฏิบัติที่เกี่ยวข้อง ทั้งนี้ข้อมูลที่เปิดเผยควรเป็นประโยชน์ สามารถนำไปประมวลผลและใช้ต่อยอดในการพัฒนาในรูปแบบต่าง ๆ ได้

ผู้รับผิดชอบงาน

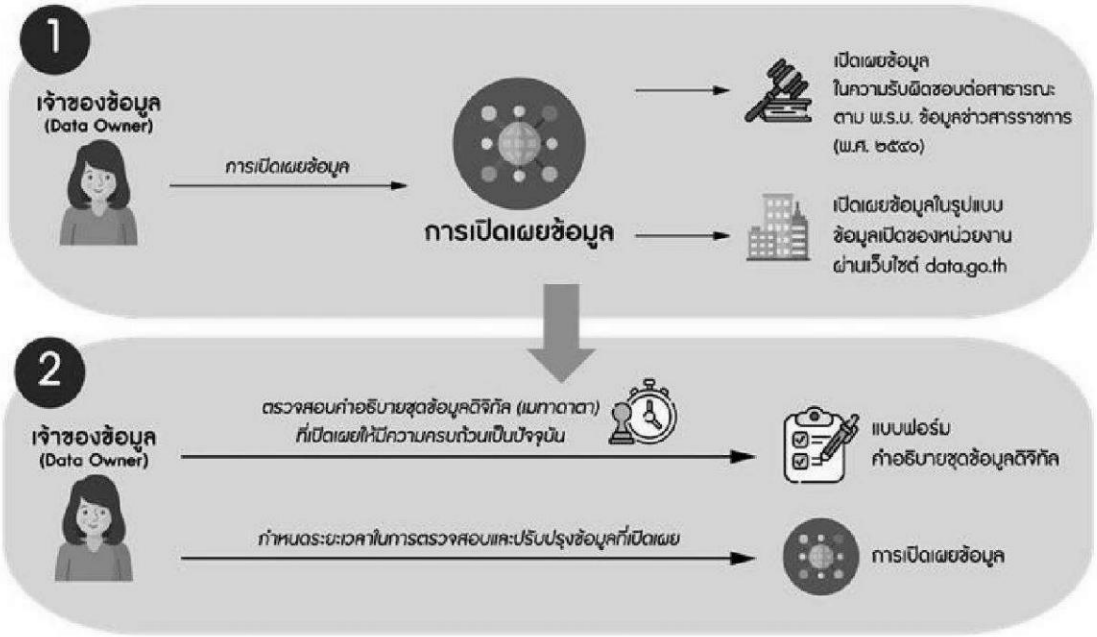
1. เจ้าของข้อมูล (Data Owners)
2. ผู้ใช้ข้อมูล (Data Users)
3. บริกรข้อมูล (Data Stewards)
4. ทีมบริหารจัดการข้อมูล (Data Management Team)

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. เจ้าของข้อมูลทำการเปิดเผยข้อมูลในความรับผิดชอบในรูปแบบข้อมูลเปิดของหน่วยงาน โดยดำเนินการดังนี้
   - กำหนดลักษณะของข้อมูลที่เผยแพร่กำหนดให้อยู่ในรูปแบบที่เครื่องสามารถประมวลผลได้
   - กำหนดให้มีคำอธิบายข้อมูลหรือเมทาดาตาสำหรับข้อมูลที่ต้องเปิดเผย
   - ข้อมูลที่เผยแพร่จะต้องมีการบันทึกเวลา (Timestamps) ที่ช่วยให้ผู้ใช้งานสามารถระบุได้ว่าข้อมูลนั้นเป็นปัจจุบัน
   - ข้อมูลที่เผยแพร่ต้องมาจากแหล่งที่เก็บข้อมูลโดยตรง ด้วยระดับความละเอียดสูงโดยไม่มีการปรับแต่งหรือเป็นข้อมูลรูปแบบสรุป (Summary data)
   - ชุดข้อมูลและรายการชุดข้อมูลที่เผยแพร่จะต้องมีการจัดรูปแบบที่กำหนดเป็นมาตรฐานและกำหนดภายใต้หมวดหมู่เดียวกัน 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
10. ข้อปฏิบัติอื่น ๆ ตามที่หน่วยงานกำหนดเพิ่มเติม

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

ตารางที่: 4 ผู้มีส่วนได้ส่วนเสียในการเปิดเผยข้อมูล

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

หมวด 5 การทำลายข้อมูล

วัตถุประสงค์

กำหนดแนวปฏิบัติการทำลายข้อมูล และการพิจารณาอนุมัติทำลายโดยเจ้าของข้อมูลเพื่อเป็นการรักษาความมั่นคงปลอดภัยของข้อมูล

ผู้รับผิดชอบงาน

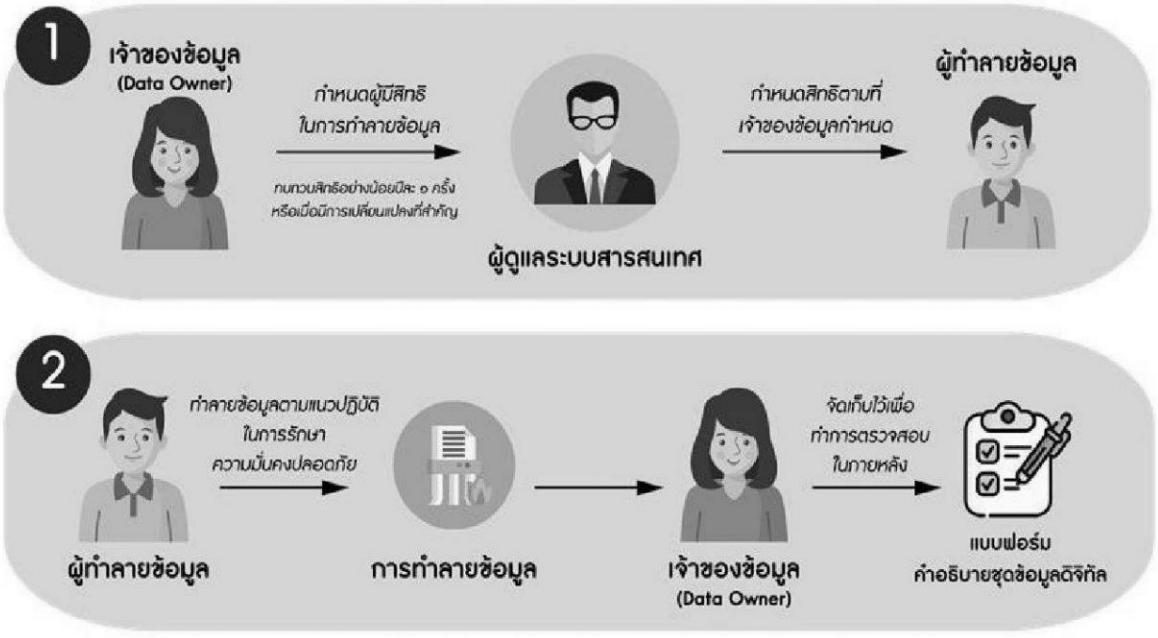
1. เจ้าของข้อมูล (Data Owners)
2. ผู้ทำลายข้อมูล (Data Disposer)
3. ผู้ดูแลระบบสารสนเทศ (Systems Administrators)

อ้างอิง

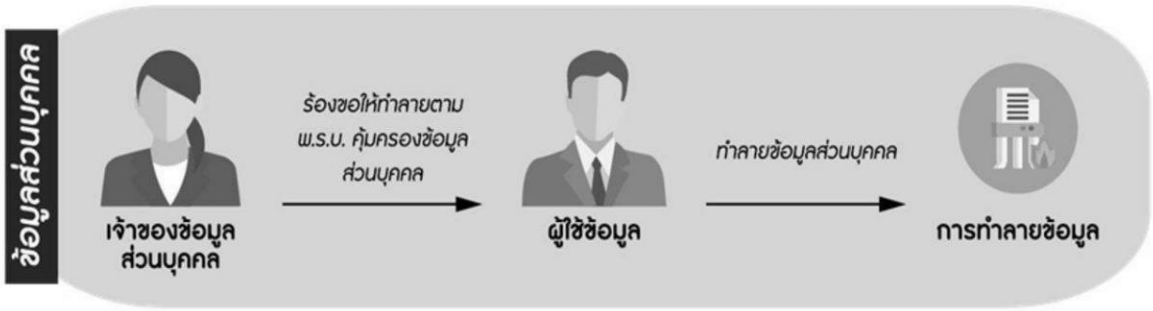
1. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
2. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553

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



7. ข้อปฏิบัติอื่น ๆ ตามที่หน่วยงานกำหนดเพิ่มเติม

กิจกรรม	ผู้มีส่วนได้ส่วนเสีย			
	เจ้าของข้อมูล	ผู้ดูแลระบบสารสนเทศ	ผู้ทำลายข้อมูล	ผู้ใช้ข้อมูล
1. กำหนดผู้มีสิทธิในการทำลายข้อมูล	R	R	I	I
2. ทำลายข้อมูลตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน	C	S	R	I
3. จัดเก็บคำอธิบายข้อมูลที่ทำลายสำหรับตรวจสอบในภายหลัง	R	S	R	I
4. จัดเก็บบันทึกรายละเอียดการทำลายข้อมูล	I	S	R	I
5. ทำลายข้อมูลส่วนบุคคลเมื่อเจ้าของข้อมูลส่วนบุคคลร้องขอตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562	C	S	I	R

ตารางที่: 5 ผู้มีส่วนได้ส่วนเสียในการทำลายข้อมูล

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

หมวด 6 การเชื่อมโยงและการแลกเปลี่ยนข้อมูล

วัตถุประสงค์

เพื่อกำหนดแนวปฏิบัติและมาตรฐานด้านเทคนิคในการเชื่อมโยงและการแลกเปลี่ยนข้อมูลดิจิทัล ทั้งภายในหน่วยงานและระหว่างหน่วยงาน อย่างมีประสิทธิภาพและก่อให้เกิดประโยชน์ต่อภาคประชาชน ภาครัฐ และภาคเอกชน

ผู้รับผิดชอบงาน

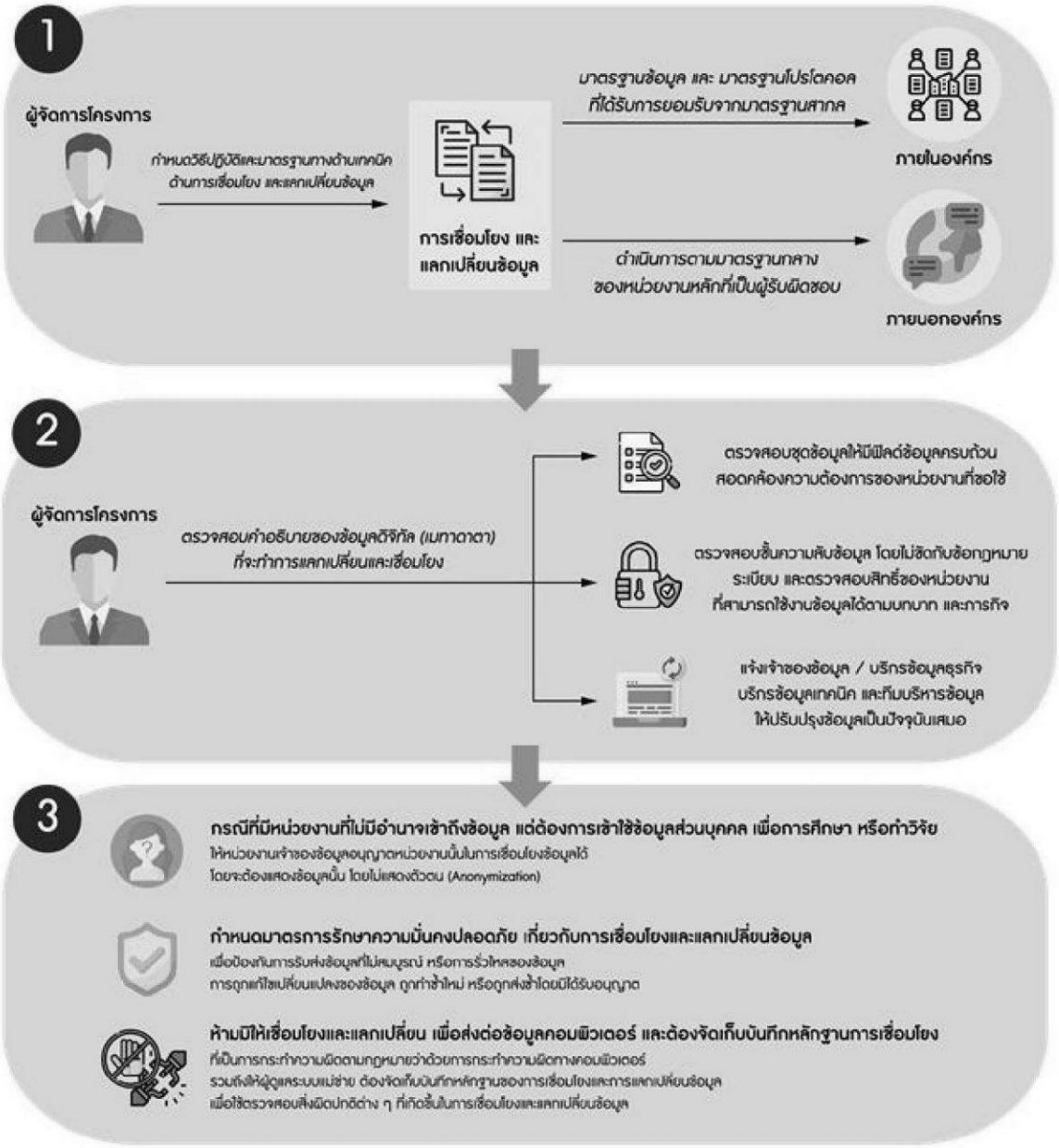
1. ผู้จัดการโครงการ (Project Managers)
2. ผู้ดูแลระบบแม่ข่าย (Server Administrators)
3. เจ้าของข้อมูล (Data Owners)
4. บริกรข้อมูล (Data Stewards)
5. ทีมบริหารจัดการข้อมูล (Data Management Team)

อ้างอิง

1. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560
2. พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562
3. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
4. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553

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
7. ข้อปฏิบัติอื่น ๆ ตามที่หน่วยงานกำหนดเพิ่มเติม

กิจกรรม	**ผู้มีส่วนได้ส่วนเสีย**				
	ผู้จัดการโครงการ	ผู้ดูแลระบบแม่ข่าย	เจ้าของข้อมูล	บริกรข้อมูล	ทีมบริหารจัดการข้อมูล
1. กำหนดวิธีปฏิบัติและมาตรฐานทางด้านเทคนิคที่จำเป็นในการเชื่อมโยงและแลกเปลี่ยนข้อมูลของโครงการ	R	S	I	I	I
2. ตรวจสอบคำอธิบายชุดข้อมูลดิจิทัล และชั้นความลับของข้อมูล	R	R	C	C	S
3. จัดทำแนวทางการทำงานร่วมกันทั้งระหว่างหน่วยงานภายในและหน่วยงานภายนอกในการเชื่อมโยงและแลกเปลี่ยนข้อมูล	R	S	S	S	S
4. จัดเก็บบันทึกหลักฐานของการเชื่อมโยงและการแลกเปลี่ยนข้อมูลดิจิทัล	I	R	I	I	I

ตารางที่: 6 ผู้มีส่วนได้ส่วนเสียในการเชื่อมโยงและแลกเปลี่ยนข้อมูล

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

ภาคผนวก

ชุดข้อมูลฌาปนกิจสงเคราะห์

1) ข้อมูลฌาปนกิจสงเคราะห์

No.	รายการ	คำอธิบาย
1	ประเภทข้อมูล	ข้อมูลระเบียน
2	ชื่อชุดข้อมูล	การฌาปนกิจสงเคราะห์
3	องค์กร	กรมกิจการสตรีและสถาบันครอบครัว
4	ชื่อผู้คิดต่อ	กลุ่มเสริมสร้างหลักประกันความมั่นคงของครอบครัว
5	อีเมล์ผู้ติดต่อ	familychapa2545@gmail.com
6	คำสำคัญ	ฌาปนกิจสงเคราะห์, ฌาปนกิจ, สมาคม
7	รายละเอียด	ข้อมูลกิจการฌาปนกิจสงเคราะห์
8	วัตถุประสงค์	กฎหมายที่เกี่ยวข้อง - พระราชบัญญัติการฌาปนกิจสงเคราะห์ พ.ศ. 2545
9	9.1 หน่วยความถี่ของการปรับปรุงข้อมูล	
	9.2 ค่าความถี่ของการปรับปรุงข้อมูล	
10	ขอบเขตเชิงภูมิศาสตร์หรือเชิงพื้นที่	ตำบล
11	แหล่งที่มา	ระบบฐานข้อมูลด้านการฌาปนกิจสงเคราะห์
12	รูปแบบการเก็บข้อมูล	Database
13	หมวดหมู่ข้อมูลตามธรรมาภิบาลข้อมูลภาครัฐ	ข้อมูลส่วนบุคคล
14	สัญญาอนุญาตให้ใช้ข้อมูล	License not specified
15	เงื่อนไขในการเข้าถึงข้อมูล	

2) รายงานข้อมูลด้านฌาปนกิจสงเคราะห์

No.	รายการ	คำอธิบาย
1	ประเภทข้อมูล	ข้อมูลหลากหลาย
2	ชื่อชุดข้อมูล	รายงานข้อมูลด้านฌาปนกิจสงเคราะห์
3	องค์กร	กรมกิจการสตรีและสถาบันครอบครัว
4	ชื่อผู้คิดต่อ	กลุ่มเสริมสร้างหลักประกันความมั่นคงของครอบครัว
5	อีเมล์ผู้ติดต่อ	familychapa2545@gmail.com
6	คำสำคัญ	ฌาปนกิจสงเคราะห์, ฌาปนกิจ, สมาคม
7	รายละเอียด	ข้อมูลกิจการฌาปนกิจสงเคราะห์
8	วัตถุประสงค์	กฎหมายที่เกี่ยวข้อง - พระราชบัญญัติการฌาปนกิจสงเคราะห์ พ.ศ. 2545
9	9.1 หน่วยความถี่ของการปรับปรุงข้อมูล	ปี
	9.2 ค่าความถี่ของการปรับปรุงข้อมูล	1
10	ขอบเขตเชิงภูมิศาสตร์หรือเชิงพื้นที่	ตำบล
11	แหล่งที่มา	ระบบฐานข้อมูลด้านการฌาปนกิจสงเคราะห์
12	รูปแบบการเก็บข้อมูล	Database, PDF, EXCEL
13	หมวดหมู่ข้อมูลตามธรรมาภิบาลข้อมูลภาครัฐ	ข้อมูลสาธารณะ
14	สัญญาอนุญาตให้ใช้ข้อมูล	License not specified

ชุดข้อมูลการช่วยเหลือกรณีการถูกเลือกปฏิบัติโดยไม่เป็นธรรมระหว่างเพศ และเงินชดเชยและเยียวยาผู้เสียหายจากการเลือกปฏิบัติโดยไม่เป็นธรรมระหว่างเพศ

1) การช่วยเหลือกรณีการถูกเลือกปฏิบัติโดยไม่เป็นธรรมระหว่างเพศและเงินชดเชยและเยียวยาผู้เสียหายจากการเลือกปฏิบัติโดยไม่เป็นธรรมระหว่างเพศ

No.	รายการ	คำอธิบาย
1	ประเภทข้อมูล	ข้อมูลประเภทอื่น ๆ
2	ชื่อชุดข้อมูล	การช่วยเหลือกรณีการถูกเลือกปฏิบัติโดยไม่เป็นธรรมระหว่างเพศและเงินชดเชยและเยียวยาผู้เสียหายจากการเลือกปฏิบัติโดยไม่เป็นธรรมระหว่างเพศ
3	องค์กร	กรมกิจการสตรีและสถาบันครอบครัว
4	ชื่อผู้คิดต่อ	กลุ่มคณะกรรมการวินิจฉัยการเลือกปฏิบัติโดยไม่เป็นธรรมระหว่างเพศ
5	อีเมล์ผู้ติดต่อ	gidentity3@gmail.com
6	คำสำคัญ	เลือกปฏิบัติโดยไม่เป็นธรรมระหว่างเพศ, การชดเชย, เยียวยา, ความเท่าเทียม, ถูกเลือกปฏิบัติ
7	รายละเอียด	การช่วยเหลือกรณีการถูกเลือกปฏิบัติโดยไม่เป็นธรรมระหว่างเพศและเงินชดเชยและเยียวยาผู้เสียหายจากการเลือกปฏิบัติโดยไม่เป็นธรรมระหว่างเพศ
8	วัตถุประสงค์	กฎหมายที่เกี่ยวข้อง - พระราชบัญญัติความเท่าเทียมระหว่างเพศ พ.ศ. 2558
9	9.1 หน่วยความถี่ของการปรับปรุงข้อมูล	
	9.2 ค่าความถี่ของการปรับปรุงข้อมูล	
10	ขอบเขตเชิงภูมิศาสตร์หรือเชิงพื้นที่	ตำบล
11	แหล่งที่มา	กลุ่มคณะกรรมการวินิจฉัยการเลือกปฏิบัติโดยไม่เป็นธรรมระหว่างเพศ กองส่งเสริมความเสมอภาคระหว่างเพศ
12	รูปแบบการเก็บข้อมูล	Image, PDF, XLS
13	หมวดหมู่ข้อมูลตามธรรมาภิบาลข้อมูลภาครัฐ	ข้อมูลส่วนบุคคล
14	สัญญาอนุญาตให้ใช้ข้อมูล	License not specified
15	เงื่อนไขในการเข้าถึงข้อมูล	มี - อ่านได้อย่างเดียว : อธิบดี สค. รองอธิบดี สค. ที่ได้รับมอบหมาย และพนักงานเจ้าหน้าที่ - อ่านได้และแก้ไข : คณะกรรมการ วลพ. คณะอนุกรรมการ วลพ. และบุคลากรในกลุ่มงาน วลพ. - อ่านได้เฉพาะเอกสารที่ตนเองสร้างขึ้น : ผู้ร้อง และผู้ถูกร้อง

2) สถานการณ์การช่วยเหลือกรณีการถูกเลือกปฏิบัติโดยไม่เป็นธรรมระหว่างเพศและเงินชดเชยและเยียวยาผู้เสียหายจากการเลือกปฏิบัติโดยไม่เป็นธรรมระหว่างเพศ

No.	รายการ	คำอธิบาย
1	ประเภทข้อมูล	ข้อมูลหลากหลายประเภท
2	ชื่อชุดข้อมูล	สถานการณ์การช่วยเหลือกรณีการถูกเลือกปฏิบัติโดยไม่เป็นธรรมระหว่างเพศและเงินชดเชยและเยียวยาผู้เสียหายจากการเลือกปฏิบัติโดยไม่เป็นธรรมระหว่างเพศ
3	องค์กร	กรมกิจการสตรีและสถาบันครอบครัว
4	ชื่อผู้คิดต่อ	กลุ่มคณะกรรมการวินิจฉัยการเลือกปฏิบัติโดยไม่เป็นธรรมระหว่างเพศ
5	อีเมล์ผู้ติดต่อ	gidentity3@gmail.com
6	คำสำคัญ	เลือกปฏิบัติโดยไม่เป็นธรรมระหว่างเพศ, การชดเชย, เยียวยา, ความเท่าเทียม, ถูกเลือกปฏิบัติ
7	รายละเอียด	สถานการณ์การช่วยเหลือกรณีการถูกเลือกปฏิบัติโดยไม่เป็นธรรมระหว่างเพศและเงินชดเชยและเยียวยาผู้เสียหายจากการเลือกปฏิบัติโดยไม่เป็นธรรมระหว่างเพศ
8	วัตถุประสงค์	กฎหมายที่เกี่ยวข้อง - พระราชบัญญัติความเท่าเทียมระหว่างเพศ พ.ศ. 2558
9	9.1 หน่วยความถี่ของการปรับปรุงข้อมูล	ปี
	9.2 ค่าความถี่ของการปรับปรุงข้อมูล	1
10	ขอบเขตเชิงภูมิศาสตร์หรือเชิงพื้นที่	จังหวัด
11	แหล่งที่มา	กลุ่มคณะกรรมการวินิจฉัยการเลือกปฏิบัติโดยไม่เป็นธรรมระหว่างเพศ กองส่งเสริมความเท่าเทียมระหว่างเพศ
12	รูปแบบการเก็บข้อมูล	PDF, XLS
13	หมวดหมู่ข้อมูลตามธรรมาภิบาลข้อมูลภาครัฐ	ข้อมูลสาธารณะ
14	สัญญาอนุญาตให้ใช้ข้อมูล	License not specified

ชุดข้อมูลการให้คำปรึกษาแนะนำและให้ความช่วยเหลือแม่เลี้ยงเดี่ยวและครอบครัว

1) การจัดสวัสดิการแม่เลี้ยงเดี่ยวและครอบครัว

No.	รายการ	คำอธิบาย
1	ประเภทข้อมูล	ข้อมูลระเบียน
2	ชื่อชุดข้อมูล	จัดสวัสดิการแม่เลี้ยงเดี่ยวและครอบครัว
3	องค์กร	กรมกิจการสตรีและสถาบันครอบครัว
4	ชื่อผู้คิดต่อ	กองคุ้มครองและพัฒนาอาชีพ
5	อีเมล์ผู้ติดต่อ	singlemom@dwf.org
6	คำสำคัญ	singlemom, single parents, welfare for singlemom, single, parents, welfare, แม่เลี้ยงเดี่ยว ครอบครัวเลี้ยงเดี่ยว, สวัสดิการครอบครัวเลี้ยงเดี่ยว
7	รายละเอียด	การจัดบริการเพื่อพัมนาคุณภาพชีวิตแม่เลี้ยงเดี่ยวและครอบครัวรายกรณี
8	วัตถุประสงค์	พันธกิจหน่วยงาน
9	9.1 หน่วยความถี่ของการปรับปรุงข้อมูล	เดือน
	9.2 ค่าความถี่ของการปรับปรุงข้อมูล	1
10	ขอบเขตเชิงภูมิศาสตร์หรือเชิงพื้นที่	จังหวัด
11	แหล่งที่มา	ศูนย์บริการแม่เลี้ยงเดี่ยวและครอบครัว
12	รูปแบบการเก็บข้อมูล	XLS
13	หมวดหมู่ข้อมูลตามธรรมาภิบาลข้อมูลภาครัฐ	ข้อมูลส่วนบุคคล
14	สัญญาอนุญาตให้ใช้ข้อมูล	License not specified
15	เงื่อนไขในการเข้าถึงข้อมูล	

2) สรุปผลการจัดสวัสดิการแม่เลี้ยงเดี่ยวและครอบครัว

No.	รายการ	คำอธิบาย
1	ประเภทข้อมูล	ข้อมูลหลากหลายประเภท
2	ชื่อชุดข้อมูล	สรุปผลจัดสวัสดิการแม่เลี้ยงเดี่ยวและครอบครัว
3	องค์กร	กรมกิจการสตรีและสถาบันครอบครัว
4	ชื่อผู้คิดต่อ	กองคุ้มครองและพัฒนาอาชีพ
5	อีเมล์ผู้ติดต่อ	singlemom@dwf.org
6	คำสำคัญ	singlemom, single parents, welfare for singlemom, single, parents, welfare, แม่เลี้ยงเดี่ยว ครอบครัวเลี้ยงเดี่ยว, สวัสดิการครอบครัวเลี้ยงเดี่ยว
7	รายละเอียด	ข้อมูลการจัดบริการแก่แม่เลี้ยงเดี่ยวและครอบครัว
8	วัตถุประสงค์	พันธกิจหน่วยงาน
9	9.1 หน่วยความถี่ของการปรับปรุงข้อมูล	เดือน
	9.2 ค่าความถี่ของการปรับปรุงข้อมูล	1
10	ขอบเขตเชิงภูมิศาสตร์หรือเชิงพื้นที่	จังหวัด
11	แหล่งที่มา	ศูนย์บริการแม่เลี้ยงเดี่ยวและครอบครัว
12	รูปแบบการเก็บข้อมูล	XLS, PDF
13	หมวดหมู่ข้อมูลตามธรรมาภิบาลข้อมูลภาครัฐ	ข้อมูลสาธารณะ
14	สัญญาอนุญาตให้ใช้ข้อมูล	License not specified

ชุดข้อมูลการให้ความช่วยเหลือหญิงไทยในต่างประเทศ

1) เครือข่ายอาสาสมัครให้คำปรึกษาแก่หญิงไทยที่แต่งงานกับชาวต่างชาติ

No.	รายการ	คำอธิบาย
1	ประเภทข้อมูล	ข้อมูลระเบียน
2	ชื่อชุดข้อมูล	เครือข่ายอาสาสมัครให้คำปรึกษาแก่หญิงไทยที่แต่งงานกับชาวต่างชาติ
3	องค์กร	กรมกิจการสตรีและสถาบันครอบครัว
4	ชื่อผู้คิดต่อ	กลุ่มส่งเสริมความร่วมมือระหว่างประเทศ
5	อีเมล์ผู้ติดต่อ	yingthai@dwf.org
6	คำสำคัญ	woman, Yingthai, married,marry a foreigner คำปรึกษาแก่หญิงไทย,แต่งงานกับชาวต่างชาติ ,จิตอาสา, อาสาสมัคร,volunteer,foreign widow,ภรรยาคนต่างชาติ,foreigner's wife,ช่วยหญิงไทย,help yingthai, บริการเพื่อหญิงไทย,service for Thai Women,ล่ามอาสา,volunteer interpreter
7	รายละเอียด	ข้อมูลเครือข่ายอาสาสมัครให้คำปรึกษาแก่หญิงไทยที่แต่งงานกับชาวต่างชาติ
8	วัตถุประสงค์	พันธกิจหน่วยงาน
9	9.1 หน่วยความถี่ของการปรับปรุงข้อมูล	ครึ่งปี
	9.2 ค่าความถี่ของการปรับปรุงข้อมูล	1
10	ขอบเขตเชิงภูมิศาสตร์หรือเชิงพื้นที่	ทวีป/กลุ่มประเทศในทวีป
11	แหล่งที่มา	กลุ่มส่งเสริมความร่วมมือระหว่างประเทศ กองยุทธศาสตร์และแผนงาน
12	รูปแบบการเก็บข้อมูล	XLS
13	หมวดหมู่ข้อมูลตามธรรมาภิบาลข้อมูลภาครัฐ	ข้อมูลส่วนบุคคล
14	สัญญาอนุญาตให้ใช้ข้อมูล	License not specified
15	เงื่อนไขในการเข้าถึงข้อมูล	

2) ศูนย์ช่วยเหลือหญิงไทยในต่างประเทศ

No.	รายการ	คำอธิบาย
1	ประเภทข้อมูล	ข้อมูลสถิติ
2	ชื่อชุดข้อมูล	ศูนย์ช่วยเหลือหญิงไทยในต่างประเทศ
3	องค์กร	กรมกิจการสตรีและสถาบันครอบครัว
4	ชื่อผู้คิดต่อ	กลุ่มส่งเสริมความร่วมมือระหว่างประเทศ
5	อีเมล์ผู้ติดต่อ	yingthai@dwf.org
6	คำสำคัญ	woman, Yingthai, married,marry a foreigner คำปรึกษาแก่หญิงไทย,แต่งงานกับชาวต่างชาติ ,จิตอาสา, อาสาสมัคร,volunteer,foreign widow,ภรรยาคนต่างชาติ,foreigner's wife,ช่วยหญิงไทย,help yingthai, บริการเพื่อหญิงไทย,service for Thai Women,ล่ามอาสา,volunteer interpreter
7	รายละเอียด	ข้อมูลศูนย์ช่วยเหลือหญิงไทยในต่างประเทศ
8	วัตถุประสงค์	พันธกิจหน่วยงาน
9	9.1 หน่วยความถี่ของการปรับปรุงข้อมูล	ปี
	9.2 ค่าความถี่ของการปรับปรุงข้อมูล	1
10	ขอบเขตเชิงภูมิศาสตร์หรือเชิงพื้นที่	ทวีป/กลุ่มประเทศในทวีป
11	แหล่งที่มา	กลุ่มส่งเสริมความร่วมมือระหว่างประเทศ กองยุทธศาสตร์และแผนงาน
12	รูปแบบการเก็บข้อมูล	XLS
13	หมวดหมู่ข้อมูลตามธรรมาภิบาลข้อมูลภาครัฐ	ข้อมูลสาธารณะ
14	สัญญาอนุญาตให้ใช้ข้อมูล	License not specified

ชุดข้อมูลความรุนแรงในครอบครัว

1) ข้อมูลความรุนแรงต่อเด็ก สตรี และบุคคลในครอบครัว

No.	รายการ	คำอธิบาย
1	ประเภทข้อมูล	ข้อมูลระเบียน
2	ชื่อชุดข้อมูล	ความรุนแรงต่อเด็ก สตรี และบุคคลในครอบครัว
3	องค์กร	กรมกิจการสตรีและสถาบันครอบครัว
4	ชื่อผู้คิดต่อ	ศูนย์ปฏิบัติการกรมกิจการสตรีและสถาบันครอบครัว
5	อีเมล์ผู้ติดต่อ	dwf_sorporkor@hotmail.com
6	คำสำคัญ	ความรุนแรง, ความรุนแรงในครอบครัว
7	รายละเอียด	ข้อมูลการรับแจ้งเหตุ และการให้ความช่วยเหลือเกี่ยวกับความรุนแรงในครอบครัว
8	วัตถุประสงค์	พันธกิจของหน่วยงาน
9	9.1 หน่วยความถี่ของการปรับปรุงข้อมูล	อื่น ๆ - ความถี่ในการรับแจ้งเหตุขึ้นอยู่กับการรับเรื่องและการบันทึกรายงานของเจ้าหน้าที่
	9.2 ค่าความถี่ของการปรับปรุงข้อมูล	
10	ขอบเขตเชิงภูมิศาสตร์หรือเชิงพื้นที่	จังหวัด
11	แหล่งที่มา	ฐานข้อมูลความรุนแรงในครอบครัว (กรมกิจการสตรีและสถาบันครอบครัว)
12	รูปแบบการเก็บข้อมูล	Database
13	หมวดหมู่ข้อมูลตามธรรมาภิบาลข้อมูลภาครัฐ	ข้อมูลส่วนบุคคล
14	สัญญาอนุญาตให้ใช้ข้อมูล	License not specified
15	เงื่อนไขในการเข้าถึงข้อมูล	

2) ข้อมูลสถานการณ์ด้านความรุนแรงในครอบครัว

No.	รายการ	คำอธิบาย
1	ประเภทข้อมูล	ข้อมูลสถิติ
2	ชื่อชุดข้อมูล	สถานการณ์ด้านความรุนแรงในครอบครัว
3	องค์กร	กรมกิจการสตรีและสถาบันครอบครัว
4	ชื่อผู้คิดต่อ	ศูนย์ปฏิบัติการกรมกิจการสตรีและสถาบันครอบครัว
5	อีเมล์ผู้ติดต่อ	dwf_sorporkor@hotmail.com
6	คำสำคัญ	ความรุนแรง, ความรุนแรงในครอบครัว
7	รายละเอียด	รายงานสถานการณ์ด้านความรุนแรงในครอบครัว
8	วัตถุประสงค์	พันธกิจของหน่วยงาน
9	9.1 หน่วยความถี่ของการปรับปรุงข้อมูล	ปี
	9.2 ค่าความถี่ของการปรับปรุงข้อมูล	1
10	ขอบเขตเชิงภูมิศาสตร์หรือเชิงพื้นที่	จังหวัด
11	แหล่งที่มา	ฐานข้อมูลความรุนแรงในครอบครัว (กรมกิจการสตรีและสถาบันครอบครัว)
12	รูปแบบการเก็บข้อมูล	Database
13	หมวดหมู่ข้อมูลตามธรรมาภิบาลข้อมูลภาครัฐ	ข้อมูลสาธารณะ
14	สัญญาอนุญาตให้ใช้ข้อมูล	License not specified

ชุดข้อมูลการจัดการเรื่องร้องเรียน

1) การจัดการเรื่องร้องเรียน ร้องทุกข์ ข้อคิดเห็นและข้อเสนอแนะ และข้อร้องเรียนการทุจริต

No.	รายการ	คำอธิบาย
1	ประเภทข้อมูล	ข้อมูลหลากหลายประเภท
2	ชื่อชุดข้อมูล	การจัดการเรื่องร้องเรียน
3	องค์กร	กรมกิจการสตรีและสถาบันครอบครัว
4	ชื่อผู้คิดต่อ	ศูนย์ส่งเสริมจริยธรรมและต่อต้านการทุจริต (ศจท.)
5	อีเมล์ผู้ติดต่อ	dwf0518@gmai.com
6	คำสำคัญ	ร้องเรียน, ร้องทุกข์
7	รายละเอียด	การจัดการเรื่องร้องเรียนร้องทุกข์ ข้อคิดเห็นและข้อเสนอแนะ และข้อร้องเรียนการทุจริต รวมทั้งรายงานผลการสอบข้อเท็จจริง
8	วัตถุประสงค์	เพื่อการให้บริการประชาชน
9	9.1 หน่วยความถี่ของการปรับปรุงข้อมูล	
	9.2 ค่าความถี่ของการปรับปรุงข้อมูล	
10	ขอบเขตเชิงภูมิศาสตร์หรือเชิงพื้นที่	
11	แหล่งที่มา	ช่องทางรับเรื่องร้องเรียน เช่น เว็บไซต์ หน่วยงานที่เกี่ยวข้อง
12	รูปแบบการเก็บข้อมูล	Database
13	หมวดหมู่ข้อมูลตามธรรมาภิบาลข้อมูลภาครัฐ	ข้อมูลส่วนบุคคล, ข้อมูลความลับทางราชการ
14	สัญญาอนุญาตให้ใช้ข้อมูล	License not specified
15	เงื่อนไขในการเข้าถึงข้อมูล	มี - เข้าถึงได้เฉพาะเจ้าหน้าที่ ศจท. ที่ได้รับมอบหมาย - หน่วยงานที่เกี่ยวข้องกับเรื่องที่ร้องเรียน

2) สรุปรายงานเรื่องร้องเรียน ร้องทุกข์ ข้อคิดเห็นและข้อเสนอแนะ และข้อร้องเรียนการทุจริต

No.	รายการ	คำอธิบาย
1	ประเภทข้อมูล	ข้อมูลสถิติ
2	ชื่อชุดข้อมูล	สรุปรายงานเรื่องร้องเรียน ร้องทุกข์ ข้อคิดเห็นและข้อเสนอแนะ และข้อร้องเรียนการทุจริต
3	องค์กร	กรมกิจการสตรีและสถาบันครอบครัว
4	ชื่อผู้คิดต่อ	ศูนย์ส่งเสริมจริยธรรมและต่อต้านการทุจริต (ศจท.)
5	อีเมล์ผู้ติดต่อ	dwf0518@gmai.com
6	คำสำคัญ	ร้องเรียน, ร้องทุกข์
7	รายละเอียด	สถิติการร้องเรียนร้องทุกข์ ข้อคิดเห็นและข้อเสนอแนะ และข้อร้องเรียนการทุจริต รวมทั้งรายงานผลการสอบข้อเท็จจริง
8	วัตถุประสงค์	เพื่อการให้บริการประชาชน
9	9.1 หน่วยความถี่ของการปรับปรุงข้อมูล	เดือน
	9.2 ค่าความถี่ของการปรับปรุงข้อมูล	1
10	ขอบเขตเชิงภูมิศาสตร์หรือเชิงพื้นที่	ไม่มี
11	แหล่งที่มา	ช่องทางรับเรื่องร้องเรียน เช่น เว็บไซต์ หน่วยงานที่เกี่ยวข้อง
12	รูปแบบการเก็บข้อมูล	Text, PDF
13	หมวดหมู่ข้อมูลตามธรรมาภิบาลข้อมูลภาครัฐ	ข้อมูลสารณะ
14	สัญญาอนุญาตให้ใช้ข้อมูล	License not specified