สพร. / PRD
กรกฎาคม 2564

มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัลอยู่ระหว่างการจัดทำ
ห้ามใช้หรือยึดร่างนี้เป็นมาตรฐาน

มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัลฉบับสมบูรณ์จะมีประกาศโดย
สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

ร่าง

ข้อเสนอแนะสำหรับการจัดทำแนวปฏิบัติการบริหารจัดการข้อมูล

(RECOMMENDATION for WRITING DATA MANAGEMENT GUIDELINE)

สำหรับเวียนขอข้อคิดเห็นจากหน่วยงานต่าง ๆ ที่เกี่ยวข้อง

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ชั้น 17 อาคารบางกอกไทยทาวเวอร์ 108 ถนนรางน้ำ แขวงถนนพญาไท เขตราชเทวี กรุงเทพฯ 10400
หมายเลขโทรศัพท์: (+66) 0 2612 6000 โทรสาร: (+66) 0 2612 6011 (+66) 0 2612 6012

คำนำ

ด้วยพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 มาตรา 8 (4) การกำหนดนโยบายหรือกฎเกณฑ์การเข้าถึงและใช้ประโยชน์จากข้อมูลที่ชัดเจนและมีระบบบริหารจัดการ รวมทั้งมีมาตรการและหลักประกันในการคุ้มครองข้อมูลที่อยู่ในความครอบครองให้มีความมั่นคงปลอดภัยและมิให้ข้อมูลส่วนบุคคลถูกละเมิด และกฎเกณฑ์ข้อมูล และตามประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ ข้อ 4 (5) การจำแนกหมวดหมู่ของข้อมูล เพื่อกำหนดนโยบายข้อมูลหรือกฎเกณฑ์เกี่ยวกับผู้มีสิทธิเข้าถึงและใช้ประโยชน์จากข้อมูลต่าง ๆ ภายในหน่วยงาน สำหรับให้ผู้ซึ่งมีหน้าที่เกี่ยวข้องปฏิบัติตามนโยบายหรือกฎเกณฑ์ได้อย่างถูกต้อง และสอดคล้องตามกฎหมายที่เกี่ยวข้อง อันจะนำไปสู่การบริหารจัดการข้อมูลภาครัฐอย่างเป็นระบบ รวมทั้งสนับสนุนการจัดทำบัญชีข้อมูลหน่วยงานให้ได้มาตรฐานและเป็นไปในทิศทางเดียวกัน สอดคล้องตามกรอบธรรมาภิบาลข้อมูลภาครัฐ

ในการนี้ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ในฐานะที่มีหน้าที่อำนวยการและสนับสนุนการปฏิบัติงานตามที่คณะกรรมการพัฒนารัฐบาลดิจิทัลมอบหมาย และดำเนินการร่างมาตรฐาน ข้อกำหนด และหลักเกณฑ์ เสนอคณะกรรมการพัฒนารัฐบาลดิจิทัล จึงได้แต่งตั้งคณะกรรมการจัดทำร่างมาตรฐาน ข้อกำหนด และหลักเกณฑ์ ภายใต้พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 และแต่งตั้งคณะทำงานเทคนิคด้านมาตรฐานการจัดทำบัญชีข้อมูลภาครัฐ เพื่อจัดทำข้อเสนอแนะสำหรับการจัดทำแนวปฏิบัติการบริหารจัดการข้อมูล เพื่อเป็นคู่มือใช้งาน **เอกสารแม่แบบแนวปฏิบัติการบริหารจัดการข้อมูล (Data Management Guideline Template)** ให้หน่วยงานภาครัฐใช้เป็นตัวอย่างในการจัดทำแนวปฏิบัติการบริหารจัดการข้อมูลให้สอดคล้องตามนโยบายข้อมูล (Data Policy) ที่หน่วยงานประกาศ และใช้เป็นแนวทางให้ผู้มีส่วนได้ส่วนเสียเกี่ยวกับข้อมูลปฏิบัติตาม เพื่อให้ข้อมูลภายในหน่วยงานมีคุณภาพ และมีความมั่นคงปลอดภัย

เอกสารแม่แบบแนวปฏิบัติการบริหารจัดการข้อมูล ฉบับนี้จะประกอบด้วยหัวข้อและตัวอย่างเนื้อหาสาระที่เกี่ยวข้องกับการจัดทำแนวปฏิบัติการบริหารจัดการข้อมูลตามวงจรชีวิตของข้อมูล โดยแบ่งออกเป็น 6 หมวด ได้แก่ การสร้างข้อมูล การจัดเก็บข้อมูล (รวมการจัดเก็บถาวร) การประมวลผลข้อมูลและการใช้ข้อมูล การเปิดเผยข้อมูล การทำลายข้อมูล และการเชื่อมโยงและการแลกเปลี่ยนข้อมูล ในแต่ละหมวดจะระบุ วัตถุประสงค์ ผู้รับผิดชอบงาน อ้างอิง และข้อปฏิบัติ ซึ่งหน่วยงานสามารถกำหนดข้อปฏิบัติอื่น ๆ เพิ่มเติมให้สอดคล้องสภาพแวดล้อมและวัฒนธรรมองค์กร และจะต้องสอดคล้องกับกฎหมาย ระเบียบข้อบังคับ คำสั่ง หรือข้อกำหนดอื่น ๆ ที่เกี่ยวข้อง ทั้งนี้ แนวปฏิบัติการบริหารจัดการข้อมูลจะต้องผ่านการอนุมัติจากผู้บริหาร และจะต้องทำการเผยแพร่ในระบบประกาศบนอินทราเน็ตและจัดเก็บในระบบจัดเก็บเอกสารของหน่วยงานเพื่อให้เจ้าหน้าที่ทุกระดับของหน่วยงานได้รับทราบ และปฏิบัติตามแนวปฏิบัตินี้อย่างเคร่งครัด โดยแนวปฏิบัติที่จัดขึ้นนี้เมื่อเริ่มนำไปใช้ในระยะแรกสามารถทบทวนได้บ่อยครั้งเป็นรายไตรมาสเพื่อให้เหมาะสมกับบริบทการปฏิบัติงานจริง และจะต้องมีการทบทวนเป็นประจำอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ รวมถึงเมื่อมีข้อเสนอแนะจากคณะกรรมการธรรมาภิบาลข้อมูลหรือคณะทำงานที่เกี่ยวข้องเห็นสมควร

(ร่าง) ข้อเสนอแนะสำหรับการจัดทำแนวปฏิบัติการบริหารจัดการข้อมูล
(Recommendation for Writing Data Management Guideline)

ข้อเสนอแนะสำหรับการจัดทำแนวปฏิบัติการบริหารจัดการข้อมูลจัดทำขึ้น เพื่อเป็นคู่มือการใช้งานเอกสารแม่แบบแนวปฏิบัติการบริหารจัดการข้อมูล (Data Management Guideline Template) ซึ่งเป็นข้อเสนอแนะให้หน่วยงานภาครัฐนำ Template ไปใช้เป็นตัวอย่างในการจัดทำแนวปฏิบัติการบริหารจัดการข้อมูลของหน่วยงานให้สอดคล้องตามนโยบายด้านข้อมูลที่หน่วยงานจัดทำและประกาศใช้ และให้เหมาะสมกับบริบทของการทำงาน ระบบจัดเก็บข้อมูล (Legacy System) และระบบเทคโนโลยีสารสนเทศและเครื่องมือสำหรับการบริหารจัดการข้อมูลของหน่วยงาน รวมทั้งเป็นไปตามบทบัญญัติของกฎหมายและระเบียบที่เกี่ยวข้อง โดยข้อเสนอแนะฉบับนี้ จะแสดงคำอธิบายลักษณะของ Template คำแนะนำและเงื่อนไขในการใช้งาน Template ซึ่งเป็นเพียงแนวทางที่ใช้อธิบายเพื่อประกอบความเข้าใจในการจัดทำแนวปฏิบัติการบริหารจัดการข้อมูลของหน่วยงาน ส่วนการบังคับใช้เป็นไปตามพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 มาตรา 8 (4) และประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ ข้อ 4 (5) อันจะนำไปสู่การบริหารจัดการข้อมูลภาครัฐอย่างเป็นระบบ รวมทั้งสนับสนุนการจัดทำบัญชีข้อมูลหน่วยงานให้ได้มาตรฐานและเป็นไปในทิศทางเดียวกัน สอดคล้องตามกรอบธรรมาภิบาลข้อมูลภาครัฐ

เอกสารแม่แบบแนวปฏิบัติการบริหารจัดการข้อมูล (Data Management Guideline Template) มีรายละเอียดลักษณะของ Template และคำแนะนำและเงื่อนไขในการใช้งาน Template ดังนี้

1. ลักษณะของ Template

หัวข้อ	รายละเอียด
ชื่อ Template	แนวปฏิบัติการบริหารจัดการข้อมูล (Data Management Guideline)
ชื่อผู้อนุมัติ	หัวหน้าหน่วยงานของรัฐ หรือ ผู้ได้รับมอบอำนาจจากหัวหน้าหน่วยงานของรัฐ
ชื่อผู้ตรวจสอบ	คณะกรรมการธรรมาภิบาลข้อมูล หรือ ผู้บริหารข้อมูลระดับสูง (Chief Data Officer)
ชื่อผู้จัดทำ	กอง/สำนัก/ฝ่าย/ศูนย์ หรือ คณะทำงานธรรมาภิบาลข้อมูล
บทนำ	ระบุหลักการและขอบเขตของแนวปฏิบัติการบริหารจัดการข้อมูลว่าจัดทำโดยใคร มีผลบังคับใช้กับใคร ความรับผิดหากไม่ปฏิบัติตาม และจะต้องครอบคลุมระบบบริหารและกระบวนการจัดการข้อมูล หรือวงจรชีวิตของข้อมูลและองค์ประกอบในการบริหารจัดการข้อมูล รวมทั้งกำหนดหมวดหมู่และการจัดระดับชั้นของข้อมูล ผู้เกี่ยวข้อง คำนิยามสำคัญ การเผยแพร่และการทบทวน
แนวปฏิบัติการบริหารจัดการข้อมูล	ระบุแนวปฏิบัติการบริหารจัดการข้อมูลตามวงจรชีวิตข้อมูล โดยแบ่งออกเป็น 6 หมวด ได้แก่ การสร้างข้อมูล การจัดเก็บข้อมูล (รวมการจัดเก็บถาวร) การประมวลผลข้อมูลและการใช้ข้อมูล การเปิดเผยข้อมูล การทำลายข้อมูล และการเชื่อมโยงและการแลกเปลี่ยนข้อมูล ในแต่ละหมวดจะระบุ วัตถุประสงค์ ผู้รับผิดชอบงาน อ้างอิงและข้อปฏิบัติ และตารางแสดงความสัมพันธ์ระหว่างกระบวนการ/กิจกรรมและผู้มีส่วนได้ส่วนเสีย ซึ่งหน่วยงานสามารถกำหนดข้อปฏิบัติอื่น ๆ เพิ่มเติมให้สอดคล้องกับสภาพแวดล้อมและวัฒนธรรมองค์กร และจะต้องสอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง หรือข้อกำหนดอื่น ๆ ที่เกี่ยวข้อง

หัวข้อ	รายละเอียด
ภาคผนวก	ระบุเอกสารและแบบฟอร์มที่ใช้ในการบริหารจัดการข้อมูล อาทิ การเลือกภารกิจ/กระบวนงานของหน่วยงาน โดยใช้แบบฟอร์มรายชื่อชุดข้อมูลที่สัมพันธ์กับกระบวนการทำงานตามภารกิจของหน่วยงาน การจัดทำคำอธิบายชุดข้อมูล (Metadata) โดยใช้แบบฟอร์มคำอธิบายข้อมูล (Metadata) แบบฟอร์มคำอธิบายข้อมูลของทรัพยากร (Resource Metadata) ที่สอดคล้องตามมาตรฐานที่ สพร. และ สสช. กำหนด และแนวทางในการพิจารณาชุดข้อมูลที่มีคุณค่าสูง โดยใช้แบบฟอร์ม High Value Datasets Checklist

2. คำแนะนำและเงื่อนไขในการใช้งาน Template

2.1 ขอบเขตการใช้งาน

1) Template แนวปฏิบัติการบริหารจัดการข้อมูล เป็นเพียงตัวอย่างสำหรับการจัดทำแนวปฏิบัติการบริหารจัดการข้อมูลของหน่วยงานเท่านั้น

2) ควรจัดทำแนวปฏิบัติการบริหารจัดการข้อมูลให้สอดคล้องกับนโยบายการบริหารจัดการข้อมูลที่หน่วยงานจัดทำขึ้น

3) หน่วยงานภาครัฐสามารถปรับลดหรือเพิ่มเติมข้อกำหนดภายใต้ Template ให้สอดคล้องนโยบายและแนวทางการบริหารจัดการข้อมูล

2.2 หลักการกำหนดแนวปฏิบัติการบริหารจัดการข้อมูล

1) ควรกำหนดแนวปฏิบัติที่สามารถดำเนินการได้เหมาะสมกับบริบทของการทำงาน ระบบจัดเก็บข้อมูล (Legacy System) และระบบเทคโนโลยีสารสนเทศและเครื่องมือสำหรับการบริหารจัดการข้อมูลของหน่วยงาน รวมทั้งเป็นไปตามตามบทบัญญัติของกฎหมายและระเบียบที่เกี่ยวข้อง

2) การกำหนดบทบาทและความรับผิดชอบของผู้มีส่วนเกี่ยวข้อง หน่วยงานภาครัฐสามารถปรับเปลี่ยนให้สอดคล้องกับบทบาทและภารกิจของหน่วยงาน และเหมาะสมกับลักษณะ/วัตถุประสงค์ในการใช้งานข้อมูลของหน่วยงาน ทั้งนี้ ผู้มีส่วนเกี่ยวข้องในแต่ละคนอาจถูกกำหนดให้ทำหน้าที่ในหลายบทบาท

3) การจัดหมวดหมู่และระดับชั้นของข้อมูล ในที่นี้แนะนำให้แบ่งหมวดหมู่ออกเป็น 5 หมวดหมู่ตามกรอบธรรมาภิบาลข้อมูลและการใช้งานภายในหน่วยงาน และกำหนดให้มีการจัดระดับชั้นความลับของข้อมูลอย่างน้อย 3 ระดับ ได้แก่ ข้อมูลใช้ภายใน (Internal Use Only) ข้อมูลที่มีชั้นความลับ (Secret) ข้อมูลเปิดเผยได้ (Public) หน่วยงานภาครัฐสามารถจัดหมวดหมู่และการจัดระดับชั้นของข้อมูล ที่ปรับลดหรือแบ่งย่อยได้ตามความเหมาะสม อย่างไรก็ดี ควรมีการ Mapping ให้สอดคล้องหรือเข้ากับหมวดหมู่และระดับชั้นของข้อมูลที่แนะนำไว้ด้วย เพื่อให้สามารถจัดการและสามารถนำเข้าระบบบัญชีข้อมูลภาครัฐ (Governance Data Catalog หรือ GD Catalog) ได้อย่างมีประสิทธิภาพและเป็นระบบ

2.3 ข้อเสนอแนะเพิ่มเติม

1) ควรสร้างความตระหนักรู้และรับรู้ให้ผู้ปฏิบัติงานทุกระดับในองค์กร

2) ควรมีการจัดทำหลักสูตรอบรมด้านการจัดทำธรรมาภิบาลข้อมูล โดยกำหนดกลุ่มผู้เรียนตามบทบาทที่เกี่ยวข้องกับการใช้งานข้อมูลพร้อมเกณฑ์องค์ความรู้ขั้นต่ำที่ผู้เข้าอบรมจำเป็นต้องรู้ และมีการปรับปรุงหลักสูตรอย่างสม่ำเสมอให้สอดรับกับเทคโนโลยีและปฏิบัติจริงได้

3) ควรมีผู้เชี่ยวชาญหรือที่ปรึกษาให้การสนับสนุนระหว่างปฏิบัติงานจริงได้อย่างมีประสิทธิภาพ

เอกสารแม่แบบแนวปฏิบัติการบริหารจัดการข้อมูล

(Data Management Guideline Template)

พิมพ์ชื่อหน่วยงาน

จัดทำโดย

พิมพ์ชื่อกอง/สำนัก/ฝ่าย/ศูนย์ที่จัดทำแนวปฏิบัติการบริหารจัดการข้อมูล

การอนุมัติเอกสาร

ชื่อเอกสาร			
แนวปฏิบัติการบริหารจัดการข้อมูล			ฉบับที่ xx / เวอร์ชั่น xx
การอนุมัติ	**ชื่อ-สกุล**	**ตำแหน่ง**	**ลงนาม**
ผู้อนุมัติ			
ผู้ตรวจสอบ			
ผู้จัดทำ			
วันที่อนุมัติ		**วันที่บังคับใช้**	

บันทึกประวัติการแก้ไขเอกสาร

ครั้งที่แก้ไข	วันที่แก้ไข	รายการเปลี่ยนแปลง	ผู้จัดทำ

สารบัญ

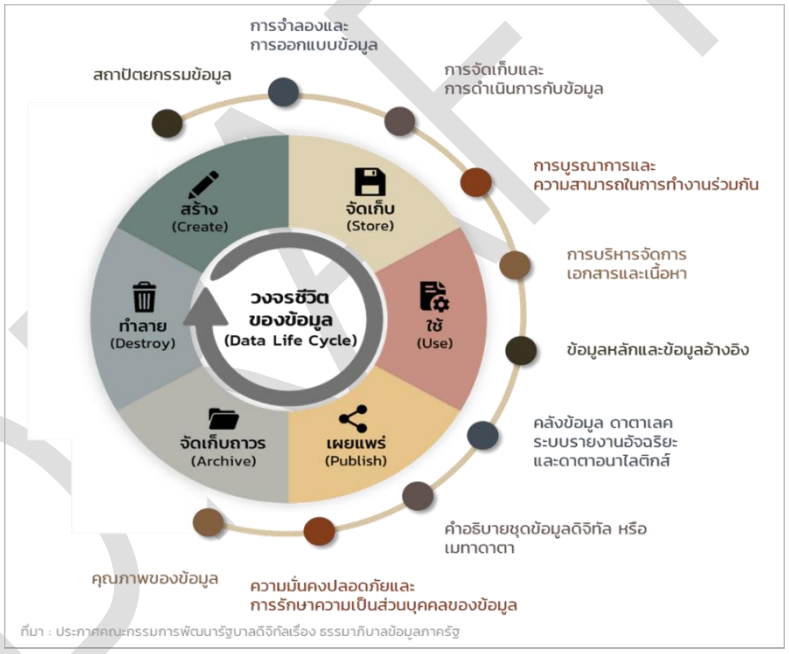
หน้า

บทนำ

ในส่วนนี้ระบุหลักการและขอบเขตของแนวปฏิบัติการบริหารจัดการข้อมูลว่าจัดทำโดยใคร มีผลบังคับใช้กับใคร ความรับผิดหากไม่ปฏิบัติตาม และจะต้องครอบคลุมระบบบริหารและกระบวนการจัดการข้อมูลหรือวงจรชีวิตของข้อมูลและองค์ประกอบในการบริหารจัดการข้อมูล รวมทั้งกำหนดหมวดหมู่และการจัดระดับชั้นของข้อมูล ผู้เกี่ยวข้อง คำนิยามสำคัญ และการเผยแพร่และการทบทวน

หลักการและขอบเขต

แนวปฏิบัติการบริหารจัดการข้อมูล ได้กำหนดขึ้นให้สอดคล้องตามนโยบายข้อมูล (Data Policy) ที่หน่วยงานประกาศ ซึ่งเป็นหนึ่งในองค์ประกอบตามกรอบธรรมาภิบาลข้อมูลภาครัฐ จัดทำโดย ระบุกอง/สำนัก/ฝ่าย/ศูนย์ มีผลบังคับใช้กับผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับข้อมูลตามแนวปฏิบัติที่ ระบุชื่อหน่วยงานประกาศ ซึ่งมีหน้าที่โดยตรงที่จะต้องสนับสนุน ดำเนินการและปฏิบัติตามอย่างเคร่งครัด และผู้ใช้อื่นที่เกี่ยวข้องแต่ไม่มีหน้าที่ในการดูแลข้อมูลจะต้องให้ความร่วมมือในการดำเนินการตามแนวปฏิบัตินี้ ผู้ฝ่าฝืนมีความผิดและจะต้องได้รับการดำเนินการตามระเบียบของหน่วยงาน โดยแนวปฏิบัติจะต้องครอบคลุมระบบบริหารและกระบวนการจัดการข้อมูล หรือวงจรชีวิตของข้อมูลและองค์ประกอบในการบริหารจัดการข้อมูล ดังรูปต่อไปนี้



วงจรชีวิตของข้อมูล

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

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

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

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

5. กระบวนการจัดเก็บข้อมูลถาวร (Archive) เป็นการย้ายข้อมูลที่มีช่วงอายุเกินช่วงใช้งานหรือไม่ได้ใช้งานแล้ว เพื่อเก็บรักษาถาวรโดยที่ข้อมูลนั้นไม่มีการลบ ปรับปรุง หรือแก้ไขอีก และสามารถนำกลับไปใช้งานได้ใหม่เมื่อต้องการ

6. การทำลายข้อมูล (Destroy) เป็นการทำลายข้อมูลที่มีการจัดเก็บถาวรเป็นระยะเวลานานหรือเกินกว่าระยะเวลาที่กำหนด

7. การเชื่อมโยงและแลกเปลี่ยนข้อมูล (Linkage and Exchange) การเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงานทั้งภายในและภายนอกให้มีความมั่นคงปลอดภัยและข้อมูลมีคุณภาพ สามารถนำไปใช้ประโยชน์ได้อย่างมีประสิทธิภาพ

หมวดหมู่และการจัดระดับชั้นของข้อมูล

ข้อมูลของหน่วยงานสามารถแบ่งหมวดหมู่ตามกรอบธรรมาภิบาลข้อมูลและการใช้งานภายในหน่วยงาน ดังนี้

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

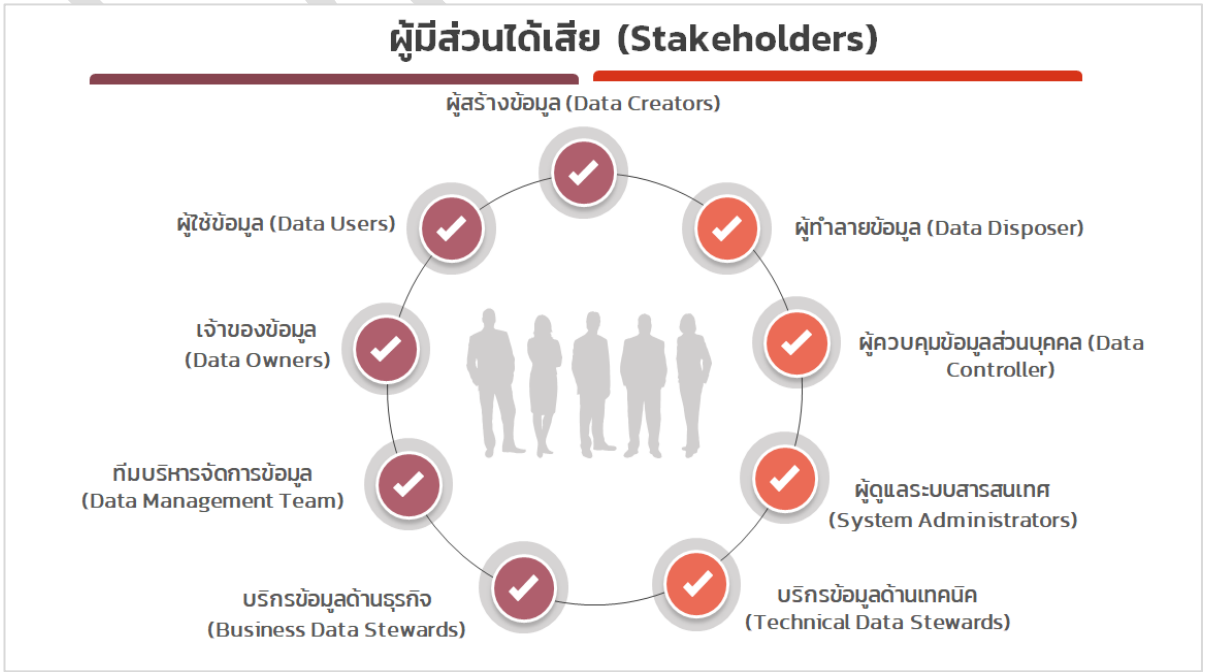
โดยมีการจัดระดับชั้นความลับของข้อมูล ดังนี้

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

ผู้เกี่ยวข้อง

ทั้งนี้แนวปฏิบัติเกี่ยวกับข้อมูลนี้บังคับใช้กับผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับข้อมูลตามประกาศแนวปฏิบัติการกำกับดูแลและบริหารจัดการข้อมูลของหน่วยงาน รวมถึงผู้เกี่ยวข้องอื่น ๆ ที่ไม่ได้ระบุไว้ในแนวปฏิบัติ ดังนี้

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



คำนิยาม

คำศัพท์	ความหมาย
สำนักงาน / กรม	ระบุชื่อหน่วยงาน
คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Committee)	ประกอบไปด้วย ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer) ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer) ผู้บริหารข้อมูลระดับสูง (Chief Data Officer) ผู้บริหารด้านการรักษาความปลอดภัยระดับสูง (Chief Security Officer) ผู้บริหารจากส่วนงานต่าง ๆ ทั้งจากฝ่ายบริหารและฝ่ายเทคโนโลยีสารสนเทศ รวมไปถึงหัวหน้าทีมบริกรข้อมูล (Lead Data Steward) คณะกรรมการธรรมาภิบาลข้อมูลมีอำนาจสูงสุดในธรรมาภิบาลข้อมูลภายในหน่วยงาน หรือ คณะกรรมการ/คณะทำงาน ซึ่งทำหน้าที่ตัดสินใจเชิงนโยบาย แก้ไขปัญหา และบริหารจัดการข้อมูลของหน่วยงาน ทั้งนี้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงอาจจะทำหน้าที่แทนผู้บริหารข้อมูลระดับสูง
หัวหน้าหน่วยงานของรัฐ	ระบุชื่อตำแหน่งผู้บริหารระดับสูง/ผู้อำนวยการของหน่วยงาน
ผู้บริหาร	ผู้บริหารที่เกี่ยวข้องกับการบริหารจัดการข้อมูล ตามคณะกรรมการ/คณะทำงานที่เกี่ยวข้อง
ข้าราชการ/เจ้าหน้าที่/พนักงาน	บุคคลผู้ที่หน่วยงานบรรจุและแต่งตั้งเป็นเจ้าหน้าที่ของหน่วยงาน
ลูกจ้าง	บุคคลผู้ที่หน่วยงานบรรจุและแต่งตั้งเป็นลูกจ้าง โดยมีสัญญาจ้างให้ปฏิบัติงานเป็นการชั่วคราวและมีกำหนดระยะเวลาและสิ้นสุดที่แน่นอน
ผู้บังคับบัญชา	ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของสำนักงาน
ผู้สร้างข้อมูล (Data Creators)	บุคลากรของทุก ระบุกอง/สำนัก/ฝ่าย/ศูนย์ ที่ทำหน้าที่บันทึก แก้ไข ปรับปรุง หรือลบข้อมูลให้สอดคล้องกับโครงสร้างที่ถูกกำหนดไว้
ผู้ใช้ข้อมูล (Data Users)	คณะกรรมการ ผู้อำนวยการ ข้าราชการ/เจ้าหน้าที่/พนักงาน ลูกจ้าง รวมถึงหน่วยงานภายนอกที่ได้รับอนุญาต (Authorized Users) ให้สามารถเข้ามาใช้ข้อมูลของหน่วยงานตามสิทธิและหน้าที่ความรับผิดชอบ พร้อมทั้งรายงานประเด็นปัญหาที่พบระหว่างการใช้ข้อมูล
สิทธิของผู้ใช้งานข้อมูล	สิทธิและหน้าที่ตามบทบาท (Role) ที่เกี่ยวข้องกับข้อมูลและระบบสารสนเทศของหน่วยงาน มีดังนี้ - สิทธิใช้งานทั่วไป หมายถึง คณะกรรมการ ผู้อำนวยการ ข้าราชการ/เจ้าหน้าที่/พนักงาน ลูกจ้าง ที่ใช้งานระบบสารสนเทศพื้นฐานของสำนักงาน ผู้ใช้งานข้อมูลต้องขออนุญาตจาก ผู้บังคับบัญชา โดยให้ใช้แบบฟอร์มเพื่อขออนุมัติตามที่หน่วยงานกำหนด - สิทธิจำเพาะ หมายถึง สิทธิเฉพาะตามหน้าที่ความรับผิดชอบที่เกี่ยวข้องกับการปฏิบัติงาน ผู้ใช้งานข้อมูลต้องได้รับสิทธิจากผู้บังคับบัญชา - สิทธิพิเศษ หมายถึง สิทธิที่ได้รับมอบหมายเพิ่มเติมจากผู้บังคับบัญชาเป็นกรณีพิเศษ ผู้ใช้งานต้องได้รับมอบหมายจากผู้บังคับบัญชาเป็นครั้งคราว

คำศัพท์	ความหมาย
เจ้าของข้อมูล (Data Owner)	ผู้ที่ได้รับมอบหมายในปฏิบัติงานให้รับผิดชอบข้อมูลที่ระบุไว้ ซึ่งรวมถึงผู้บังคับบัญชาของเจ้าของข้อมูลนั้นด้วย โดยทำหน้าที่กำกับดูแลตามธรรมาภิบาลข้อมูลตลอดวงจรชีวิตของข้อมูลนั้นๆ รวมทั้งทำหน้าที่กำหนดสิทธิในการเข้าถึงข้อมูลและจัดชั้นความลับของข้อมูล
เจ้าของข้อมูลส่วนบุคคล (Data Subject)	บุคคลธรรมดาที่ข้อมูลส่วนบุคคลเกี่ยวกับบุคคลนั้นระบุถึง
เจ้าของระบบงาน (System Owner)	ผู้ที่มีหน้าที่รับผิดชอบในการใช้งาน ดูแลและบำรุงรักษา หรือปรับปรุงระบบงานที่ใช้ในหน่วยงาน
ทีมบริหารจัดการข้อมูล (Data Management Team)	กลุ่มบุคคลภายในฝ่ายเทคโนโลยีสารสนเทศของหน่วยงานที่ทำหน้าที่รับผิดชอบดูแลรักษาข้อมูลในระบบสารสนเทศของหน่วยงาน และสนับสนุนกิจกรรมของธรรมาภิบาลข้อมูลภาครัฐ เช่น ช่วยเหลือในการนิยามเมทาดาตา ร่างนโยบายข้อมูลและมาตรฐานข้อมูล และกำหนดสิทธิการเข้าถึงข้อมูลโดย DBA เป็นต้น
บริกรข้อมูลด้านธุรกิจ (Business Data Stewards)	บุคลากรระดับหัวหน้ากลุ่ม/ส่วนงานจากทุก ระบุกอง/สำนัก/ฝ่าย/ศูนย์ ที่ได้รับมอบหมายให้ทำหน้าที่กำหนดนิยามความต้องการด้านคุณภาพและความมั่นคงปลอดภัยซึ่งอาจจะได้รับมาจากผู้ใช้ข้อมูล (Data Users) หรือผู้มีส่วนได้เสียอื่น ๆ นิยามคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตาโดยการสนับสนุนจากผู้ใช้ข้อมูล ร่างนโยบายข้อมูลด้วยการช่วยเหลือจากทีมบริหารจัดการข้อมูล (Data Management Team) ตรวจสอบการปฏิบัติตามนโยบายข้อมูล ตรวจสอบคุณภาพ ตรวจสอบความมั่นคงปลอดภัยของข้อมูล วิเคราะห์ผลจากการตรวจสอบ แล้วรายงานผลลัพธ์ไปยังคณะกรรมการธรรมาภิบาลข้อมูลและผู้ที่เกี่ยวข้องอื่น ๆ ให้ทราบ
บริกรข้อมูลด้านเทคนิค (Technical Data Stewards)	บุคลากรจากทุก ระบุกอง/สำนัก/ฝ่าย/ศูนย์ ที่ทำหน้าที่ให้การสนับสนุนด้านเทคโนโลยีสารสนเทศแก่บริกรข้อมูลด้านธุรกิจ เช่น นิยามเมทาดาตาเชิงเทคนิคซึ่งอาจจะได้รับการช่วยเหลือจากทีมบริหารจัดการข้อมูล ให้ข้อเสนอแนะเชิงเทคนิคในการร่างนโยบายข้อมูล ตรวจสอบคุณภาพข้อมูล ความมั่นคงปลอดภัยของข้อมูล และการปฏิบัติตามนโยบายข้อมูลในเชิงเทคนิค
ผู้ดูแลระบบสารสนเทศ (System Administrators)	บุคลากรของทุก ระบุกอง/สำนัก/ฝ่าย/ศูนย์ ที่มีหน้าที่ดูแลรับผิดชอบระบบสารสนเทศของหน่วยงาน
ผู้ดูแลระบบแม่ข่าย (Server Administrators)	บุคลากรที่มีหน้าที่ดูแลรับผิดชอบระบบแม่ข่ายของหน่วยงาน
ผู้จัดการโครงการ (Project Managers)	บุคลากรจากทุก ระบุกอง/สำนัก/ฝ่าย/ศูนย์ ของหน่วยงานหลักที่ได้รับมอบหมายบริหารจัดการโครงการตามแผนดำเนินงาน
ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)	บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจ เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
ผู้ทำลายข้อมูล (Data Destroyers)	บุคลากรที่ได้รับการกำหนดสิทธิจากเจ้าของข้อมูลให้มีสิทธิในการทำลายข้อมูล

คำศัพท์	ความหมาย
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 และอื่นๆ
ระบบสารสนเทศ (Information System)	ระบบงานที่นำเทคโนโลยีมาช่วยในการสร้างสารสนเทศที่สามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งประกอบด้วยเทคโนโลยีคอมพิวเตอร์และเทคโนโลยีการสื่อสารโทรคมนาคม ได้แก่ ระบบคอมพิวเตอร์ (Computer System) ระบบเครือข่าย (Network System) ซอฟต์แวร์ (Software) ข้อมูล (Data) และสารสนเทศ (Information) เป็นต้น
อินทราเน็ต (Intranet)	เป็นระบบเครือข่ายที่สามารถเข้าถึงได้โดยผู้ใช้งานภายในสำนักงานเท่านั้น โดยมีจุดประสงค์เพื่อการติดต่อสื่อสาร แลกเปลี่ยนข้อมูลและสารสนเทศภายในสำนักงาน
การเข้าถึงและควบคุมการใช้งานข้อมูล	การเข้าถึงและการใช้งานข้อมูลทั้งทางอิเล็กทรอนิกส์หรือกายภาพ รวมทั้งการอนุญาต การกำหนดสิทธิในเข้าถึงและใช้งานข้อมูล การปรับปรุงข้อมูล การเพิกถอนหรือการยกเลิกสิทธิการเข้าถึงข้อมูล
การเข้าถึงและควบคุมการใช้งานระบบสารสนเทศ	การเข้าถึงและการใช้งานระบบสารสนเทศ รวมทั้งการตรวจสอบ การอนุมัติ การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ และการเพิกถอนหรือการยกเลิกสิทธิการเข้าถึงเครือข่ายหรือระบบสารสนเทศ
ทรัพย์สิน (Asset)	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. 2562)
ข้อมูลความมั่นคง (National Security Data)	ข้อมูลเกี่ยวกับความมั่นคงของรัฐ ที่ทำให้เกิดความสงบเรียบร้อย การมีเสถียรภาพความเป็นปึกแผ่น ปลอดภัยจากภัยคุกคาม เป็นต้น
ข้อมูลความลับทางราชการ (Confidential Government Data)	ข้อมูลที่อยู่ในความครอบครองหรือควบคุมดูแลของหน่วยงานของรัฐที่มีคำสั่งไม่ให้มีการเปิดเผย และมีการกำหนดชั้นความลับของข้อมูล
ข้อมูลลับ (Confidential)	ข้อมูลข่าวสารซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์ของรัฐซึ่งผู้ที่สามารถเข้าถึงได้ต้องเป็นบุคคลที่มีสิทธิเท่านั้นและห้ามเผยแพร่ต่อบุคคลภายนอกเว้นแต่จะได้รับอนุมัติเป็นลายลักษณ์อักษรโดย ระบุผู้บริหารระดับหัวหน้ากลุ่ม/ส่วนงานเจ้าของข้อมูล ขึ้นไปโดยต้องมีการลงนามในเอกสารข้อตกลงการไม่เปิดเผยข้อมูล (Non-Disclosure Agreement) เว้นแต่การเผยแพร่ดังกล่าวเป็นไปตามอำนาจที่กฎหมายให้การรับรอง
ข้อมูลลับมาก (Secret)	ข้อมูลข่าวสารซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรงซึ่งผู้ที่สามารถเข้าถึงได้ต้องเป็นบุคคลที่มีสิทธิเท่านั้นและห้ามเผยแพร่ต่อบุคคลภายนอก เว้นแต่จะได้รับอนุมัติเป็นลายลักษณ์อักษรโดย ระบุผู้บริหารระดับผู้ช่วยผู้อำนวยการ กอง/สำนัก/ฝ่าย/ศูนย์ที่เป็นเจ้าของข้อมูลขึ้นไปโดยต้องมีการลงนามในเอกสารข้อตกลงการไม่เปิดเผยข้อมูล (Non-Disclosure Agreement) เว้นแต่การเผยแพร่ดังกล่าวเป็นไปตามอำนาจที่กฎหมายให้การรับรอง
ข้อมูลลับที่สุด (Top Secret)	ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรงที่สุดซึ่งผู้ที่สามารถเข้าถึงได้ต้องเป็นบุคคลที่มีสิทธิเท่านั้นและห้ามเผยแพร่ต่อบุคคลภายนอกเว้นแต่จะได้รับอนุมัติเป็นลายลักษณ์อักษรโดย ระบุผู้บริหารระดับรอง/ผู้ช่วยผู้อำนวยการสำนักงาน/รองปลัด/รองอธิบดี ขึ้นไปโดยต้องมีการลงนามในเอกสารข้อตกลงการไม่เปิดเผยข้อมูล (Non-Disclosure Agreement) เว้นแต่การเผยแพร่ดังกล่าวเป็นไปตามอำนาจที่กฎหมายให้การรับรอง
ข้อมูลใช้ภายใน (Internal Use Only)	ข้อมูลสำหรับใช้ในการดำเนินกิจการภายในของหน่วยงานซึ่งไม่อนุญาตให้นำไปใช้งานภายนอกก่อนได้รับอนุญาต เช่น นโยบาย มาตรฐาน และขั้นตอนการปฏิบัติงาน ประกาศ และบันทึกภายในหน่วยงาน เป็นต้น

การเผยแพร่และการทบทวน

แนวปฏิบัติเกี่ยวกับข้อมูลนี้จะต้องทำการเผยแพร่โดยการประกาศเวียนในระบบอินทราเน็ตและจดหมายอิเล็กทรอนิกส์เพื่อให้เจ้าหน้าที่ทุกระดับในหน่วยงาน ได้รับทราบ และถือปฏิบัติตามแนวปฏิบัตินี้อย่างเคร่งครัด โดยแนวปฏิบัติที่จัดขึ้นนี้เมื่อเริ่มนำไปใช้ในระยะแรกสามารถทบทวนได้บ่อยครั้งเป็นรายไตรมาสเพื่อให้เหมาะสมกับบริบทการปฏิบัติงานจริง และจะต้องมีการทบทวนเป็นประจำอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ รวมถึงเมื่อมีข้อเสนอแนะคณะกรรมการธรรมาภิบาลข้อมูลเห็นสมควร

แนวปฏิบัติการบริหารจัดการข้อมูล

ในส่วนนี้ระบุแนวปฏิบัติการบริหารจัดการข้อมูลตามวงจรชีวิตข้อมูล โดยแบ่งออกเป็น 6 หมวด ได้แก่ การสร้างข้อมูล การจัดเก็บข้อมูล การประมวลผลข้อมูลและการใช้ข้อมูล การเชื่อมโยงและการแลกเปลี่ยนข้อมูล การเปิดเผยข้อมูล และการทำลายข้อมูล ในแต่ละหมวดจะระบุ วัตถุประสงค์ ผู้รับผิดชอบงาน อ้างอิง และข้อปฏิบัติ และตารางแสดงความสัมพันธ์ระหว่างกระบวนการ/กิจกรรมและผู้มีส่วนได้ส่วนเสีย ซึ่งหน่วยงานสามารถกำหนดข้อปฏิบัติอื่น ๆ เพิ่มเติมให้สอดคล้องกับสภาพแวดล้อมและวัฒนธรรมองค์กร และจะต้องสอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง หรือข้อกำหนดอื่น ๆ ที่เกี่ยวข้อง

หมวด 1 การสร้างข้อมูล

วัตถุประสงค์

กำหนดแนวปฏิบัติสำหรับผู้ที่เกี่ยวข้องในการสร้างข้อมูลให้มีคุณภาพ มีความมั่นคงปลอดภัย และเป็นประโยชน์ต่อผู้ใช้ข้อมูล

ผู้รับผิดชอบงาน

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

อ้างอิง

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

ข้อปฏิบัติ

1. เจ้าของข้อมูล *(ไม่ว่า เจ้าของข้อมูล จะอยู่ภายใน กอง/สำนัก/ฝ่าย/ศูนย์ เดียว หรือ มากกว่าหลาย กอง /สำนัก/ฝ่าย/ศูนย์ ต้องมีการกำหนดชัดเจน ถึงอำนาจหน้าที่และขั้นตอนการทำงานร่วมกัน)*
   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) และเผยแพร่เป็น

ข้อมูลเปิดของหน่วยงานต่อสาธารณะตามกฎหมายว่าด้วยข้อมูลข่าวสารของราชการในรูปแบบข้อมูลดิจิทัล

4. ห้ามมิให้ผู้สร้างข้อมูลนำข้อมูลที่มีลักษณะดังต่อไปนี้เข้าสู่ระบบคอมพิวเตอร์ที่ขัดต่อกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์
   - ข้อมูลที่บิดเบือน หรือปลอมไม่ว่าทั้งหมดหรือบางส่วน
   - ข้อมูลอันเป็นเท็จ ที่น่าจะเกิดความเสียหายต่อการรักษาความมั่นคงปลอดภัย ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจ หรือ โครงสร้างพื้นฐาน หรือ ก่อให้เกิดความตื่นตระหนก
   - ข้อมูลอันเป็นความผิดเกี่ยวกับความมั่นคง หรือ ความผิดเกี่ยวกับการก่อการร้าย
   - ข้อมูลที่มีลักษณะอันลามก และอาจเข้าถึงได้
   - ข้อมูลที่ปรากฏภาพของผู้อื่น และเป็นภาพที่สร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ ทำให้ผู้อื่นเสียชื่อเสียง ถูกดูหมิ่นถูกเกลียดชัง หรือ ได้รับความอับอาย

5. ห้ามมิให้ผู้สร้างข้อมูล ทำการสร้าง/ทำซ้ำต่อข้อมูลที่ขัดต่อกฎหมายว่าด้วยลิขสิทธิหรือทรัพย์สินทางปัญญาของผู้อื่น เว้นแต่จะเป็นไปตามอำนาจที่กฎหมายรับรอง
6. กำหนดให้ผู้สร้างข้อมูลสร้างข้อมูลที่มาจากแหล่งข้อมูลที่เชื่อถือได้เท่านั้น
7. กำหนดให้เจ้าของข้อมูลตรวจสอบความถูกต้องของข้อมูลที่ถูกสร้างขึ้น
8. ข้อปฏิบัติอื่น ๆ ตามที่หน่วยงานกำหนดเพิ่มเติม

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

ตารางที่ 1 *ตัวอย่างผู้มีส่วนได้ส่วนเสียในการสร้างข้อมูล*

หมายเหตุ

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

หมวด 2 การจัดเก็บข้อมูล

วัตถุประสงค์

กำหนดแนวปฏิบัติสำหรับผู้ที่เกี่ยวข้องในการจัดเก็บข้อมูล ให้มีคุณภาพ เข้าถึงและใช้งานได้อย่างมั่นคงปลอดภัย

ผู้รับผิดชอบงาน

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

อ้างอิง

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

ข้อปฏิบัติ

1. กำหนดให้เจ้าของข้อมูลจะต้องกำหนดระยะเวลาในการจัดเก็บข้อมูลที่ชัดเจน
2. กำหนดให้ทีมบริหารจัดการข้อมูล และผู้ดูแลระบบสารสนเทศทำการย้ายข้อมูลที่มีการจัดเก็บเกินระยะเวลาที่กำหนดแล้วเพื่อจัดเก็บเป็นข้อมูลถาวร

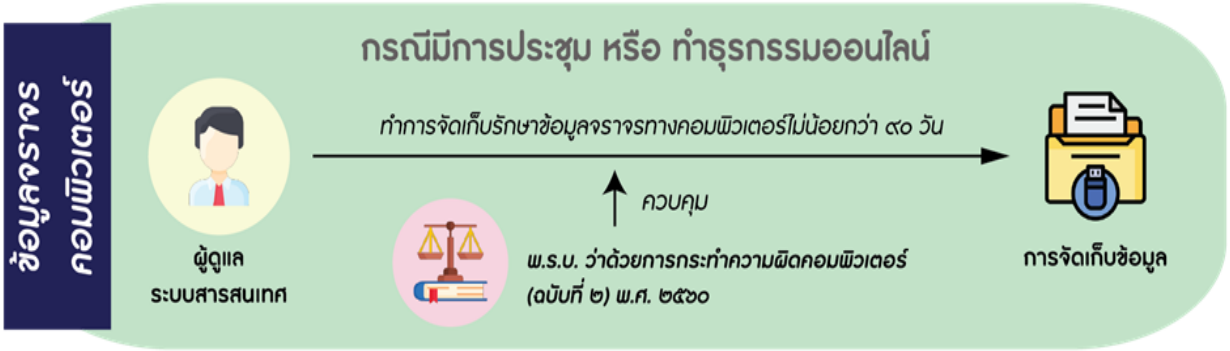
3. กำหนดให้การจัดเก็บชุดข้อมูลจะต้องมีคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตา หากไม่มีหรือไม่ครบถ้วน ทีมบริหารจัดการข้อมูลจะต้องแจ้งผู้รับผิดชอบ ได้แก่ เจ้าของข้อมูล บริกรข้อมูลด้านเทคนิค และบริกรข้อมูลด้านธุรกิจ โดยทีมบริหารจัดการข้อมูลร่วมกันจัดทำและปรับปรุงให้เป็นปัจจุบัน
4. ผู้มีส่วนได้ส่วนเสียเกี่ยวข้องกับข้อมูล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

6. ในการจัดเก็บข้อมูลส่วนบุคคล**ให้เก็บรวบรวมได้เท่าที่จำเป็น** ภายใต้อำนาจหน้าที่และวัตถุประสงค์อันชอบด้วยกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล และ**ไม่เก็บรวบรวมข้อมูลส่วนบุคคล** ดังต่อไปนี้ เว้นแต่ได้รับการยินยอมจากเจ้าของข้อมูลส่วนบุคคล หรือพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล หรือกฎหมายอื่นบัญญัติให้กระทำได้
   - เชื้อชาติ
   - เผ่าพันธุ์
   - ความคิดเห็นทางการเมือง
   - ความเชื่อในลัทธิ ศาสนาหรือปรัชญา
   - พฤติกรรมทางเพศ
   - ประวัติอาชญากรรม

- ข้อมูลสุขภาพ ความพิการ หรือข้อมูลสุขภาพจิต
- ข้อมูลสหภาพแรงงาน
- ข้อมูลพันธุกรรม
- ข้อมูลชีวภาพ
- ข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลในทำนองเดียวกันตามที่หน่วยงานกำหนด

7. กำหนดให้มีการยกเลิกการจัดเก็บข้อมูลส่วนบุคคลกรณีเจ้าของข้อมูลส่วนบุคคลถอนความยินยอมตามที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลกำหนด

8. ในกรณีที่มีการประชุมหรือธุรกรรมออนไลน์ กำหนดให้มีการจัดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่า 90 วัน นับแต่วันที่ข้อมูลเข้าสู่ระบบคอมพิวเตอร์ โดยจัดเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการนับแต่เริ่มใช้บริการให้สอดคล้องตามกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์และในการจัดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ให้สอดคล้องตามกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ ผู้ให้บริการจะต้องใช้วิธีการที่มั่นคงปลอดภัยอย่างน้อย ดังนี้
   - เก็บลงในสื่อที่รักษาความครบถ้วนถูกต้องแท้จริง (Integrity) และระบุตัวตน (Identification) ที่เข้าถึงสื่อได้
   - มีการรักษาความลับของข้อมูล และกำหนดชั้นความลับในการเข้าถึงและจัดเก็บข้อมูล เพื่อรักษาความน่าเชื่อถือของข้อมูล และไม่อนุญาตให้ผู้ดูแลระบบแก้ไขข้อมูลที่จัดเก็บไว้ได้
   - การจัดเก็บข้อมูลระบุรายละเอียดผู้ใช้บริการเป็นรายบุคคลได้ (Identification and Authentication) เช่น Proxy Server NAT และอื่น ๆ



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

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

ตารางที่ 2 ตัวอย่างผู้มีส่วนได้ส่วนเสียในการจัดเก็บข้อมูล

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

หมวด 3 การประมวลผลข้อมูลและการใช้ข้อมูล

วัตถุประสงค์

กำหนดแนวปฏิบัติในการประมวลผลข้อมูลและการใช้ข้อมูลที่มีประสิทธิภาพถูกต้อง ตรงตามวัตถุประสงค์ เพื่อให้เกิดประโยชน์สูงสุด

ผู้รับผิดชอบงาน

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

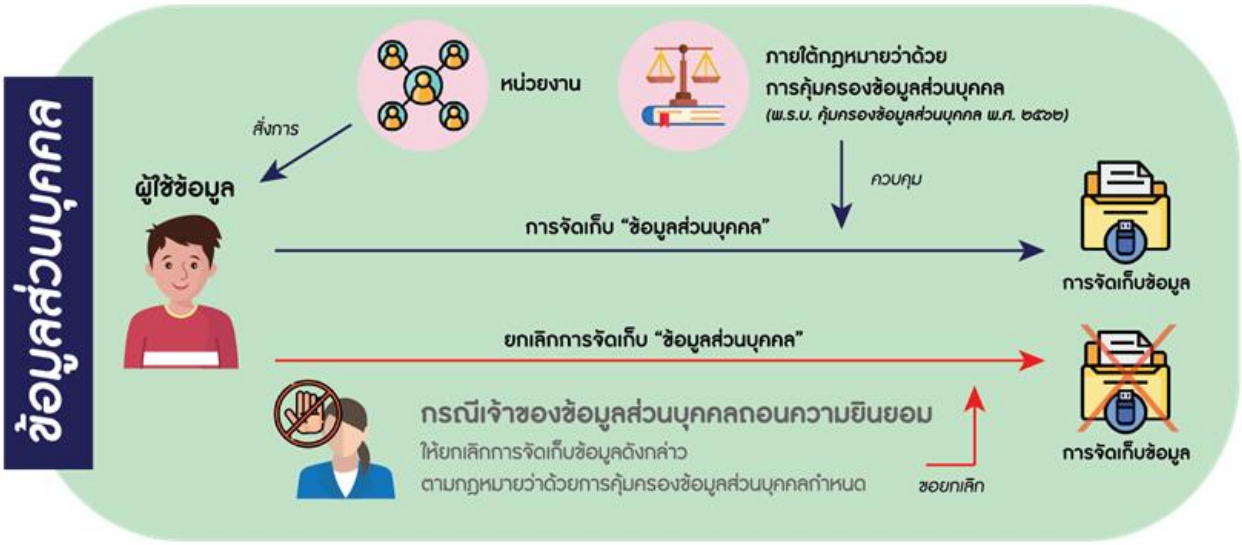
อ้างอิง

1. พระราชบัญญัติข้อมูลข่าวสารราชการ พ.ศ. 2540
2. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553
3. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ข้อปฏิบัติ

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

5. ผู้ใช้ข้อมูลจะประมวลผลข้อมูลหรือใช้ข้อมูลส่วนบุคคลเท่าที่จำเป็นภายใต้อำนาจหน้าที่และวัตถุประสงค์อันชอบด้วยกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล หรือตามคำสั่งที่ได้รับจากหน่วยงานเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคล
6. หน่วยงานต้องยกเลิกการประมวลผลข้อมูลหรือการใช้ข้อมูลส่วนบุคคล กรณีที่เจ้าของข้อมูลส่วนบุคคลถอนความยินยอมตามที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลกำหนด



7. ผู้ใช้ข้อมูลจะต้องไม่ใช้ข้อมูลในเครือข่ายของหน่วยงานเพื่อประโยชน์ในเชิงธุรกิจเป็นการส่วนตัวหรือเพื่อเข้าสู่เว็บไซต์ที่ไม่เหมาะสมหรือใช้ข้อมูลอันก่อให้เกิดความเสียหายต่อหน่วยงาน
8. ข้อปฏิบัติอื่นๆ ตามที่หน่วยงานกำหนดเพิ่มเติม

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

ตารางที่ 3 ตัวอย่างผู้มีส่วนได้ส่วนเสียในการประมวลผลและใช้ข้อมูล

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

หมวด 4 การเปิดเผยข้อมูล

วัตถุประสงค์

กำหนดแนวปฏิบัติการเปิดเผยข้อมูลต่อสาธารณะโดยอิงจากกฎหมาย กฎเกณฑ์และแนวปฏิบัติที่เกี่ยวข้อง ทั้งนี้ข้อมูลที่เปิดเผยควรเป็นประโยชน์ สามารถนำไปประมวลผลและใช้ต่อยอดในการพัฒนาในรูปแบบต่าง ๆ ได้

ผู้รับผิดชอบงาน

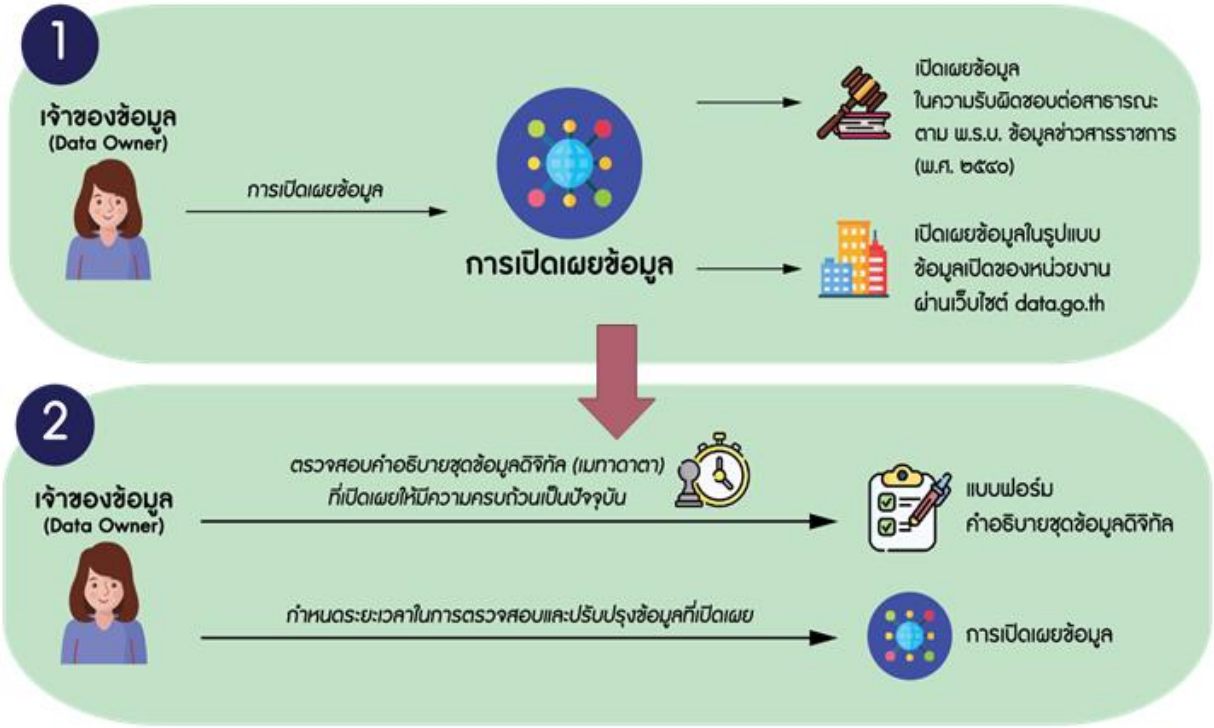
1. เจ้าของข้อมูล (Data Owners)
2. ผู้ใช้ข้อมูล (Data Users)
3. บริกรข้อมูล (Data Stewards)
4. ทีมบริหารจัดการข้อมูล (Data Management Team)

อ้างอิง

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

ข้อปฏิบัติ

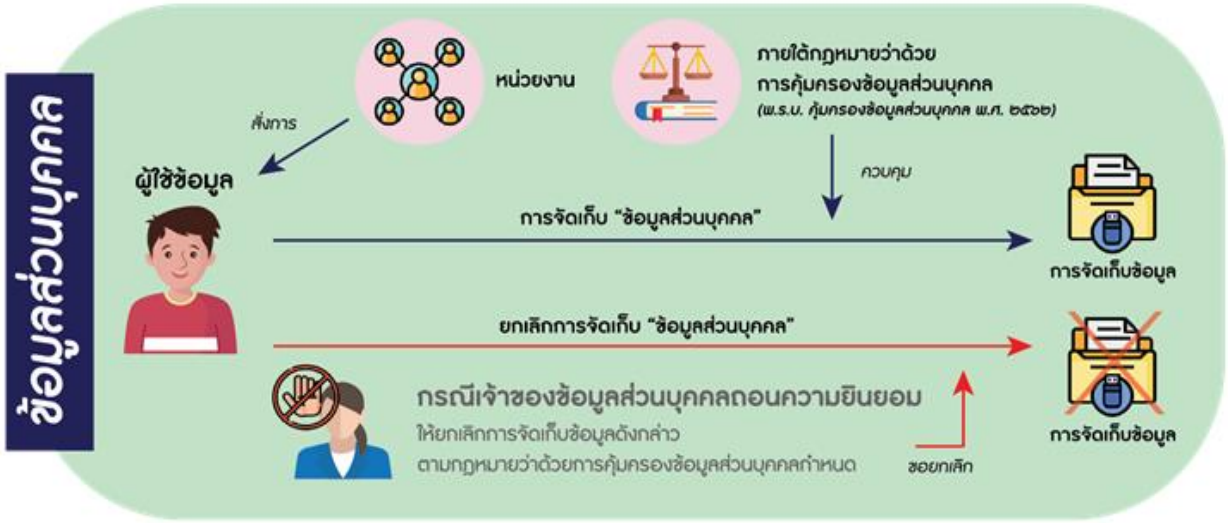
1. เจ้าของข้อมูลจะต้องเปิดเผยข้อมูลในความรับผิดชอบต่อสาธารณะตามกฎหมายว่าด้วยข้อมูลข่าวสารของราชการ และมาตรฐานและหลักเกณฑ์การเปิดเผยข้อมูลเปิดภาครัฐในรูปแบบข้อมูลดิจิทัลต่อสาธารณะ



2. เจ้าของข้อมูลทำการเปิดเผยข้อมูลในความรับผิดชอบในรูปแบบข้อมูลเปิดของหน่วยงานโดยดำเนินการดังนี้
   - กำหนดลักษณะของข้อมูลที่เผยแพร่กำหนดให้อยู่ในรูปแบบที่เครื่องสามารถประมวลผลได้
   - กำหนดให้มีคำอธิบายข้อมูลหรือเมทาดาตาสำหรับข้อมูลที่ต้องเปิดเผย
   - ข้อมูลที่เผยแพร่จะต้องมีการบันทึกเวลา (Timestamps) ที่ช่วยให้ผู้ใช้งานสามารถระบุได้ว่าข้อมูลนั้นเป็นปัจจุบัน
   - ข้อมูลที่เผยแพร่ต้องมาจากแหล่งที่เก็บข้อมูลโดยตรง ด้วยระดับความละเอียดสูงโดยไม่มีการปรับแต่งหรือเป็นข้อมูลรูปแบบสรุป (Summary data)
   - ชุดข้อมูลและรายการชุดข้อมูลที่เผยแพร่จะต้องมีการจัดรูปแบบที่กำหนดเป็นมาตรฐาน และกำหนดภายใต้หมวดหมู่เดียวกัน เพื่อให้ผู้ใช้ข้อมูลสามารถค้นหาและเข้าถึงข้อมูลได้ง่าย
3. กำหนดให้เงื่อนไขและข้อกำหนดของข้อมูลที่นำมาเปิดเผยภายในเครือข่ายของหน่วยงาน ข้อมูลที่เผยแพร่ต้องไม่ขัดต่อกฎหมายว่าด้วยทรัพย์สินทางปัญญา เว้นแต่การเปิดเผยข้อมูลจะเป็นไปตามอำนาจที่กฎหมายรับรอง
4. สนับสนุนการจัดทำบัญชีข้อมูลหน่วยงานและการลงทะเบียนบัญชีข้อมูลภาครัฐ โดยบริหารจัดการข้อมูลสำคัญ จัดทำบัญชีข้อมูลของหน่วยงาน และทำการลงทะเบียนบัญชีข้อมูลของหน่วยงานและชุดข้อมูลสำคัญ เข้าสู่ระบบบัญชีข้อมูลภาครัฐ (Government Data Catalog หรือ GD Catalog) เพื่อการเปิดเผยข้อมูลภาครัฐที่เป็นระบบ และมีเอกภาพ สามารถสืบค้นชุดข้อมูล คำอธิบายชุดข้อมูล รวมไปถึงแหล่งต้นทางของชุดข้อมูลภาครัฐที่สำคัญ สนับสนุนการใช้ประโยชน์ข้อมูลภาครัฐร่วมกัน
5. สนับสนุนการเผยแพร่ข้อมูลผ่านช่องทางที่ง่ายต่อการเข้าถึงข้อมูล และสนับสนุนการเปิดเผยข้อมูลในรูปแบบดิจิทัลต่อสาธารณะที่ศูนย์กลางข้อมูลเปิดภาครัฐ (Government Open Data) ผ่านเว็บไซต์ data.go.th โดย

- กำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัยในการเปิดเผยข้อมูลที่กำหนดลำดับชั้นข้อมูลตั้งแต่ลับขึ้นไป อย่างเพียงพอและมีประสิทธิภาพ
- มีการตรวจสอบข้อมูลที่เผยแพร่จากหน่วยงานทั้งภายในและภายนอกหน่วยงาน เพื่อให้มั่นใจว่าหน่วยงานได้มีข้อมูลที่เผยแพร่ที่มีคุณค่า
- การเผยแพร่ข้อมูล ต้องมีการตรวจสอบรูปแบบข้อมูลที่เผยแพร่ให้สอดคล้องกับมาตรฐานที่หน่วยงานกำหนด
- หากการเปิดเผยนั้นเป็นการเปิดเผยบนช่องทางที่ดูแลรับผิดชอบโดยหน่วยงานอื่นที่ให้ปฏิบัติตามเอกสาร คู่มือ การนำข้อมูลขึ้นเผยแพร่ของหน่วยงานนั้น
- หากการเปิดเผยข้อมูลไม่ครบถ้วน หรือไม่เป็นปัจจุบัน ให้แจ้งเจ้าของข้อมูล บริกรข้อมูลธุรกิจ บริกรข้อมูลเทคนิค และทีมบริหารจัดการข้อมูลทำการจัดทำ/ปรับปรุงให้เป็นปัจจุบัน

6. กำหนดให้เปิดเผยข้อมูลส่วนบุคคลตามข้อกำหนดของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือตามคำสั่งที่ได้รับจากหน่วยงานเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติในกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล



7. เจ้าของข้อมูลห้ามเปิดเผยข้อมูลความมั่นคงและข้อมูลความลับทางราชการที่อยู่ในความครอบครองของหน่วยงานรวมทั้งห้ามเปิดเผยข้อมูลที่เป็นการกระทำความผิดตามกฎหมาย นโยบาย และแนวปฏิบัติอันทำให้เกิดความเสียหายต่อหน่วยงาน
8. กำหนดให้เจ้าของข้อมูลคัดเลือกข้อมูลที่จะเปิดเผยในรูปแบบข้อมูลเปิดจากลำดับชั้นความสำคัญของชุดข้อมูลที่มีคุณค่าสูง (High Value Dataset)
9. กำหนดให้เจ้าของข้อมูลต้องกำหนกรอบระยะเวลาในการตรวจสอบและปรับปรุงข้อมูลที่เปิดเผยเพื่อให้ข้อมูลถูกต้อง และเป็นปัจจุบัน
10. ข้อปฏิบัติอื่นๆ ตามที่หน่วยงานกำหนดเพิ่มเติม

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

ตารางที่ 4 *ตัวอย่างผู้มีส่วนได้ส่วนเสียในการเปิดเผยข้อมูล*

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

หมวด 5 การทำลายข้อมูล

วัตถุประสงค์

กำหนดแนวปฏิบัติการทำลายข้อมูล และการพิจารณาอนุมัติทำลายโดยเจ้าของข้อมูลเพื่อเป็นการรักษาความมั่นคงปลอดภัยของข้อมูล

ผู้รับผิดชอบงาน

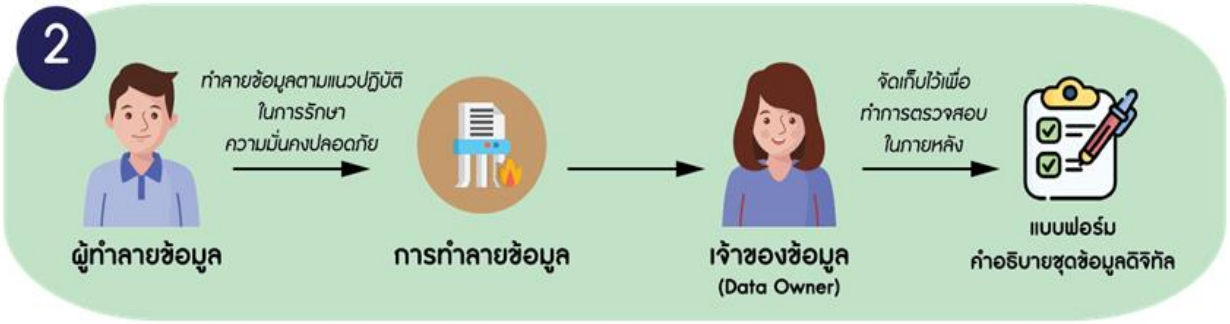
1. เจ้าของข้อมูล (Data Owners)
2. ผู้ทำลายข้อมูล (Data Destroyers)
3. ผู้ดูแลระบบสารสนเทศ (Systems Administrators)

อ้างอิง

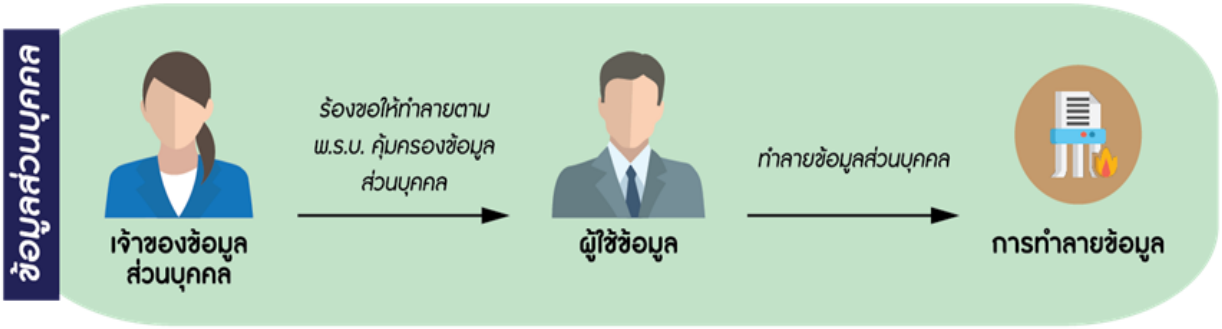
1. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553
2. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ข้อปฏิบัติ

1. เจ้าของข้อมูลเป็นผู้กำหนดผู้มีสิทธิในการทำลายข้อมูล และจะต้องทบทวนสิทธินั้น อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ เช่น การลาออก เปลี่ยนตำแหน่ง โอนย้าย สิ้นสุดการจ้าง การปรับโครงสร้าง หรือเมื่อมีการปรับปรุงระบบสารสนเทศ เป็นต้น
2. ผู้ดูแลระบบสารสนเทศจะต้องกำหนดสิทธิในการทำลายข้อมูลในระบบให้แก่ผู้ทำลายข้อมูลตามที่เจ้าของข้อมูลกำหนด
3. ผู้ทำลายข้อมูลต้องทำลายข้อมูลตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน
4. กำหนดให้เจ้าของข้อมูลต้องจัดเก็บคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตาที่ทำลายสำหรับตรวจสอบในภายหลัง
5. กำหนดให้ผู้ทำลายข้อมูลจัดเก็บบันทึกรายละเอียดการทำลายข้อมูลไว้ในทะเบียนควบคุมและบันทึกการทำลายข้อมูล โดยให้เก็บรักษาไว้เป็นหลักฐานไม่น้อยกว่า 1 ปี



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



7. ข้อปฏิบัติอื่นๆ ตามที่หน่วยงานกำหนดเพิ่มเติม

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

ตารางที่ 5 *ตัวอย่างผู้มีส่วนได้ส่วนเสียในการทำลายข้อมูล*

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

หมวด 6 การเชื่อมโยงและการแลกเปลี่ยนข้อมูล

วัตถุประสงค์

เพื่อกำหนดแนวปฏิบัติและมาตรฐานด้านเทคนิคในการเชื่อมโยงและการแลกเปลี่ยนข้อมูลดิจิทัล ทั้งภายในหน่วยงานและระหว่างหน่วยงาน อย่างมีประสิทธิภาพและก่อให้เกิดประโยชน์ต่อภาคประชาชน ภาครัฐ และภาคเอกชน

ผู้รับผิดชอบงาน

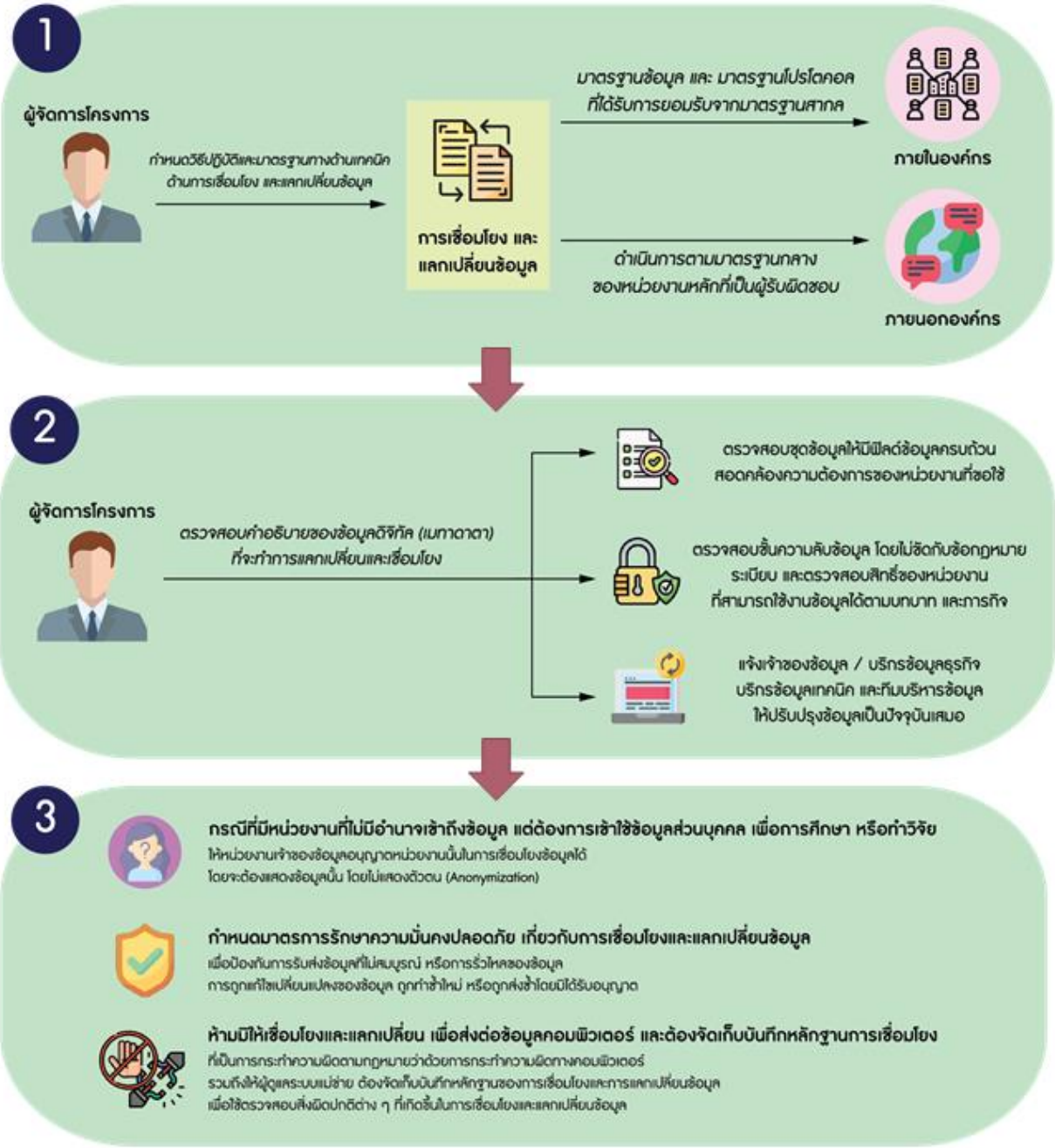
1. ผู้จัดการโครงการ (Project Managers)
2. ผู้ดูแลระบบแม่ข่าย (Server Administrators)
3. เจ้าของข้อมูล (Data Owners)
4. บริกรข้อมูล (Data Stewards)
5. ทีมบริหารจัดการข้อมูล (Data Management Team)

อ้างอิง

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

ข้อปฏิบัติ

1. กำหนดให้ผู้จัดการโครงการกำหนดวิธีปฏิบัติและมาตรฐานทางด้านเทคนิคที่จำเป็นต้องใช้เกี่ยวกับการเชื่อมโยงและแลกเปลี่ยนข้อมูลของโครงการในความรับผิดชอบ ดังนี้
   - การเชื่อมโยงและแลกเปลี่ยนข้อมูลภายในหน่วยงาน กำหนดให้ใช้รูปแบบที่เป็นมาตรฐานเปิด (Open Format) ทั้งในส่วนมาตรฐานข้อมูล เช่น XML และ JSON เป็นต้น มาตรฐานโปรโตคอลสื่อสาร เช่น SOAP REST หรืออื่น ๆ ที่ได้รับการยอมรับจากมาตรฐานสากล
   - การเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน ให้ดำเนินการตามมาตรฐานกลางของหน่วยงานหลักที่เป็นผู้รับผิดชอบ
2. กำหนดให้ผู้จัดการโครงการตรวจสอบคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตาที่จะทำการเชื่อมโยงและแลกเปลี่ยนให้ครบถ้วน ดังนี้
   - ตรวจสอบเมทาดาตาของชุดข้อมูลดิจิทัลที่จัดเก็บให้มีฟิลด์ข้อมูลครบถ้วนสอดคล้องกับความต้องการของหน่วยงานที่ขอใช้ หากไม่ครบถ้วนต้องจัดทำเพิ่มเติมตามความต้องการของหน่วยงานที่ขอใช้
   - ตรวจสอบชั้นความลับของข้อมูลว่าอยู่ในชั้นความลับที่สามารถเปิดเผยได้หรือไม่ นั่นคือ ต้องไม่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ ความมั่นคงของประเทศ ความลับทางราชการ และความเป็นส่วนตัว พร้อมทั้งตรวจสอบสิทธิของหน่วยงานที่สามารถนำข้อมูลไปใช้ได้ตามบทบาทและภารกิจตามกฎหมายของหน่วยงานนั้น ๆ
   - หากไม่ครบถ้วน หรือไม่เป็นปัจจุบัน ให้แจ้งเจ้าของข้อมูล บริกรข้อมูลธุรกิจ บริกรข้อมูลเทคนิค และทีมบริหารจัดการข้อมูลทำการจัดทำ/ปรับปรุงให้เป็นปัจจุบัน



3. ในกรณีที่มีหน่วยงานอื่นที่ไม่มีอำนาจในการเข้าถึงข้อมูลส่วนบุคคลแต่ต้องการใช้ข้อมูลส่วนบุคคลในการครอบครองของหน่วยงาน เพื่อทำการศึกษาหรือวิจัย ซึ่งเป็นข้อยกเว้นตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ให้หน่วยงานเจ้าของข้อมูลอนุญาตหน่วยงานนั้นในการเชื่อมโยงข้อมูลได้ โดยจะต้องแสดงข้อมูลนั้นด้วยวิธีไม่แสดงตัวตน (Anonymization)
4. กำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัยเกี่ยวกับการเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัล เพื่อป้องกันมิให้มีการรับส่งข้อมูลที่ไม่สมบูรณ์ หรือส่งข้อมูลไปผิดที่หรือมีการรั่วไหลของข้อมูล หรือข้อมูลถูกแก้ไขเปลี่ยนแปลง ถูกทำซ้ำใหม่ ถูกส่งซ้ำโดยมิได้รับอนุญาต
5. ห้ามมิให้เชื่อมโยงและแลกเปลี่ยนเพื่อส่งต่อข้อมูลคอมพิวเตอร์ที่เป็นการกระทำความผิดตามกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์
6. กำหนดให้ผู้ดูระบบแม่ข่ายต้องจัดเก็บบันทึกหลักฐานของการเชื่อมโยงและการแลกเปลี่ยนข้อมูลดิจิทัล เพื่อใช้ตรวจสอบสิ่งผิดปกติต่าง ๆ ที่เกิดขึ้นในการเชื่อมโยงและแลกเปลี่ยนข้อมูล
7. ข้อปฏิบัติอื่นๆ ตามที่หน่วยงานกำหนดเพิ่มเติม

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

ตารางที่ 6 *ตัวอย่างผู้มีส่วนได้ส่วนเสียในการเชื่อมโยงและแลกเปลี่ยนข้อมูล*

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

ภาคผนวก

การเลือกภารกิจ/กระบวนงานของหน่วยงาน

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

การจัดทำคำอธิบายชุดข้อมูล (Metadata)

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

แนวทางในการพิจารณาชุดข้อมูลที่มีคุณค่าสูง

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