



แนวปฏิบัติการบริหารจัดการข้อมูล
ของสำนักงานปรมาณูเพื่อสันติ

จัดทำโดย
คณะกรรมการธรรมาภิบาลข้อมูลของสำนักงานปรมาณูเพื่อสันติ

การอนุมัติเอกสาร

ชื่อเอกสาร			
แนวปฏิบัติการบริหารจัดการข้อมูล			ฉบับที่ 01 / เวอร์ชัน 01
การอนุมัติ	ชื่อ-สกุล	ตำแหน่ง	ลงนาม
ผู้อนุมัติ	นพ.รุ่งเรือง กิจผาติ	ประธานคณะกรรมการ ธรรมาภิบาลข้อมูล (CEO)	
ผู้ตรวจสอบ	นายชลกานต์ เอี่ยมสำอาง นางสาวปิยวรรณ ศรีกงพาน นายไกรสร วิหาร	กรรมการและผู้ช่วยเลขานุการ คณะกรรมการธรรมาภิบาลข้อมูล	
ผู้จัดทำ	คณะบริหารข้อมูล		
วันที่อนุมัติ 1 กรกฎาคม 2569		วันที่บังคับใช้ 1 กรกฎาคม 2569	

บันทึกประวัติการแก้ไขเอกสาร

ครั้งที่ แก้ไข	วันที่แก้ไข	รายการเปลี่ยนแปลง	ผู้จัดทำ

สารบัญ

แนวปฏิบัติการบริหารจัดการข้อมูล	1
สารบัญ	2
สารบัญตาราง	4
บทนำ	5
1.1 หลักการและขอบเขต	6
1.2 วงจรชีวิตของข้อมูล	8
1.3 หมวดยุทธศาสตร์และการจัดระดับชั้นของข้อมูล	9
1.4 ผู้เกี่ยวข้อง	11
1.5 คำนิยาม	13
1.6 การเผยแพร่และการทบทวน	20
ส่วนที่ 1 แนวปฏิบัติการบริหารจัดการข้อมูล	21
หมวด 1 การสร้างข้อมูล	22
หมวด 2 การจัดเก็บข้อมูล	26
หมวด 3 การประมวลผลข้อมูลและการใช้ข้อมูล	32
หมวด 4 การเปิดเผยข้อมูล	34
หมวด 5 กระบวนการจัดเก็บข้อมูลถาวร	38
หมวด 6 การทำลายข้อมูล	41
ส่วนที่ 2 แนวปฏิบัติในการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน	43
2.1 วัตถุประสงค์	44
2.2 ขอบปฏิบัติ	44

สารบัญ (ต่อ)

ส่วนที่ 3 แนวปฏิบัติในการจัดทำบัญชีข้อมูลของหน่วยงาน.....	46
3.1 วัตถุประสงค์.....	47
3.2 คำนิยาม	47
3.3 กฎหมายและแนวทางที่เกี่ยวข้อง	49
3.4 ข้อปฏิบัติ.....	50
ส่วนที่ 4 แนวปฏิบัติในการประเมินคุณภาพข้อมูล	52
4.1 วัตถุประสงค์.....	53
4.2 คำนิยาม	53
4.3 ข้อปฏิบัติ.....	54
4.3.1 การกำหนดหลักเกณฑ์คุณภาพข้อมูล (Data Quality Requirement)	55
4.3.2 การประเมินคุณภาพข้อมูล (Data Quality Assessment)	55
4.3.3 การปรับปรุงคุณภาพข้อมูล (Data Quality Improvement)	59
4.3.4 การควบคุมและติดตามให้ข้อมูลมีคุณภาพ (Monitoring and Control)	61
เอกสารอ้างอิง	63

สารบัญตาราง

ตารางที่ 1	ผู้มีส่วนได้ส่วนเสียในการสร้างข้อมูล	25
ตารางที่ 2	ผู้มีส่วนได้ส่วนเสียในการจัดเก็บข้อมูล	31
ตารางที่ 3	ผู้มีส่วนได้ส่วนเสียในการประมวลผลข้อมูลและการใช้ข้อมูล	33
ตารางที่ 4	ผู้มีส่วนได้ส่วนเสียในการเปิดเผยข้อมูล	37
ตารางที่ 5	ผู้มีส่วนได้ส่วนเสียในการจัดเก็บข้อมูลถาวร	40
ตารางที่ 6	ผู้มีส่วนได้ส่วนเสียในการทำลายข้อมูล	42

สารบัญรูป

รูปที่ 1	กระบวนการบริหารจัดการข้อมูลตลอดวงจรชีวิตของข้อมูล (Data Life Cycle) และองค์ประกอบที่เกี่ยวข้องกับการบริหารจัดการข้อมูล	7
รูปที่ 2	การจัดระดับชั้นความลับของข้อมูล	10
รูปที่ 3	ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับข้อมูลตามประกาศ	12

บทนำ

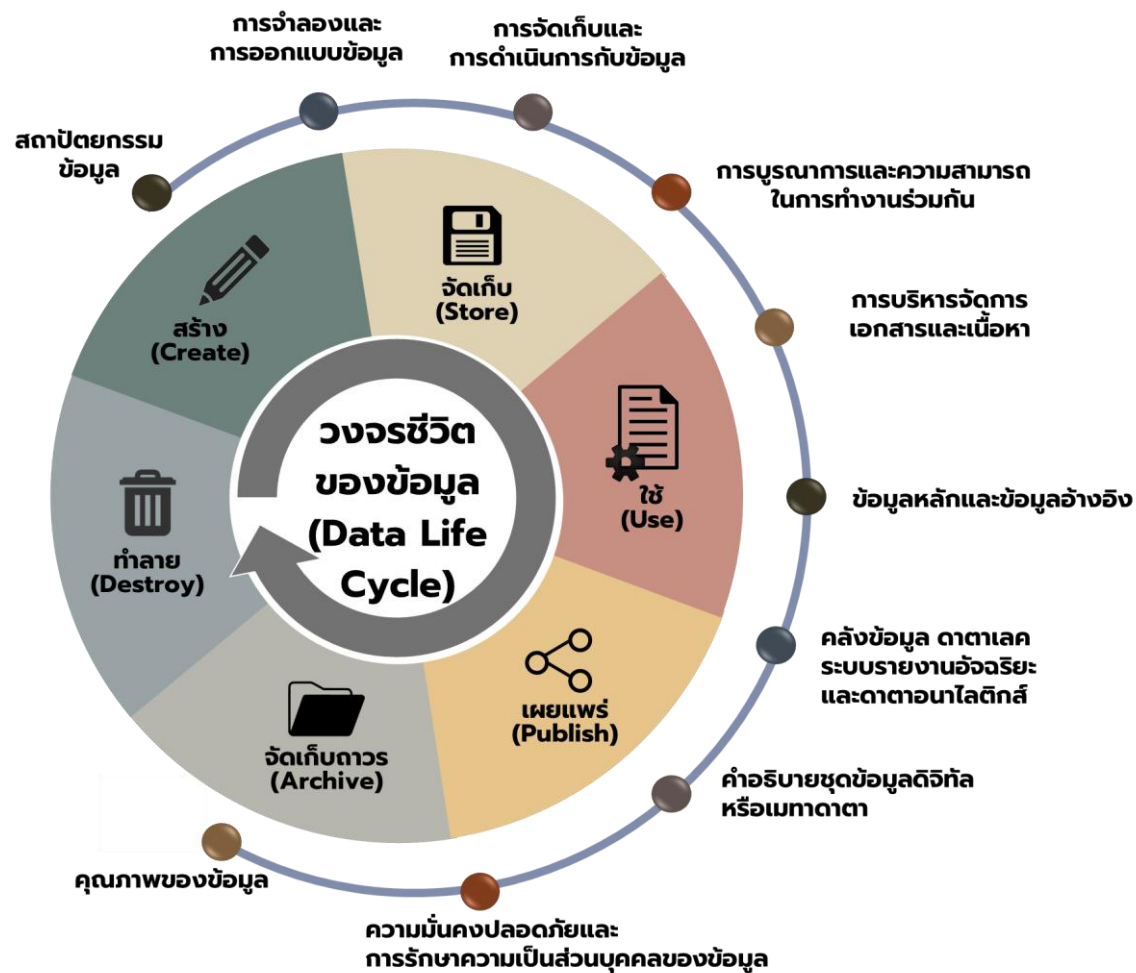
การบริหารจัดการข้อมูลอย่างมีประสิทธิภาพเป็นกลไกสำคัญในการขับเคลื่อนการดำเนินงานของสำนักงานปรมาณูเพื่อสันติ (ปส.) ในยุคดิจิทัล แนวปฏิบัติการบริหารจัดการข้อมูลฉบับนี้จัดทำขึ้นภายใต้กรอบธรรมาภิบาลข้อมูลภาครัฐ เพื่อกำหนดหลักเกณฑ์ ขอบเขต และแนวทางในการบริหารจัดการข้อมูลให้เป็นไปอย่างมีมาตรฐาน ถูกต้อง ครบถ้วน เป็นปัจจุบัน และมั่นคงปลอดภัย สอดคล้องกับกฎหมาย ระเบียบ และนโยบายที่เกี่ยวข้อง โดยมีผลบังคับใช้กับบุคลากรทุกระดับ รวมถึงหน่วยงานหรือบุคคลภายนอกที่เกี่ยวข้องกับการได้มา การเข้าถึง การใช้ การประมวลผล การเชื่อมโยง การแลกเปลี่ยน และการเปิดเผยข้อมูลของ ปส. ซึ่งผู้ที่เกี่ยวข้องต้องปฏิบัติตามแนวปฏิบัตินี้อย่างเคร่งครัด มิฉะนั้นอาจถูกดำเนินการตามกฎหมาย ระเบียบ หรือข้อบังคับที่เกี่ยวข้อง

แนวปฏิบัตินี้ครอบคลุมการบริหารจัดการข้อมูลตลอดวงจรชีวิตของข้อมูล (Data Life Cycle) ตั้งแต่การสร้าง การจัดเก็บ การประมวลผล การเปิดเผย การจัดเก็บถาวร จนถึงการทำลายข้อมูล รวมถึงการจำแนกหมวดหมู่ข้อมูลและการจัดระดับชั้นความลับของข้อมูล เพื่อควบคุมการเข้าถึงและการใช้ข้อมูลให้เหมาะสมกับระดับความสำคัญและความอ่อนไหวของข้อมูล ตลอดจนกำหนดบทบาท หน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องในการบริหารจัดการข้อมูลอย่างชัดเจน เช่น เจ้าของข้อมูล (Data Owner) ผู้สร้างข้อมูล (Data Creator) ผู้ดูแลระบบสารสนเทศ (System Administrator) บริกรข้อมูล (Data Steward) และผู้ใช้ข้อมูล (Data User) รวมถึงกำหนดค่านิยมสำคัญเพื่อให้เกิดความเข้าใจที่ตรงกัน ทั้งนี้ ปส. จะเผยแพร่แนวปฏิบัตินี้ให้ผู้ที่เกี่ยวข้องรับทราบผ่านช่องทางที่เหมาะสม และทบทวนหรือปรับปรุงอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ เพื่อให้สอดคล้องกับสถานการณ์ กฎหมาย และมาตรฐานที่เกี่ยวข้อง รวมทั้งเพื่อให้สามารถนำไปใช้ได้อย่างมีประสิทธิภาพและต่อเนื่อง

1.1 หลักการและขอบเขต

แนวปฏิบัติการบริหารจัดการข้อมูลฉบับนี้จัดทำขึ้นให้สอดคล้องกับนโยบายธรรมาภิบาลข้อมูล (Data Governance Policy) ที่ ปส. ประกาศใช้ ซึ่งเป็นหนึ่งในองค์ประกอบสำคัญตามกรอบธรรมาภิบาลข้อมูลภาครัฐ โดยจัดทำขึ้นภายใต้การกำกับดูแลของคณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council) ของ ปส. และมีผลบังคับใช้กับผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับข้อมูลของสำนักงาน ทั้งบุคลากรภายใน ปส. รวมถึงหน่วยงานหรือบุคคลภายนอกที่เกี่ยวข้องกับการได้มา การเข้าถึง การใช้ การประมวลผล การเชื่อมโยง การแลกเปลี่ยน และการเปิดเผยข้อมูลของสำนักงาน โดยผู้ที่มีหน้าที่และความรับผิดชอบด้านข้อมูลต้องสนับสนุนและปฏิบัติตามแนวปฏิบัตินี้อย่างเคร่งครัด ส่วนผู้ใช้งานหรือผู้เกี่ยวข้องอื่นที่ไม่มีหน้าที่โดยตรงในการบริหารจัดการข้อมูล ต้องให้ความร่วมมือในการดำเนินงานตามแนวปฏิบัติดังกล่าว ทั้งนี้ ผู้ที่ฝ่าฝืนหรือไม่ปฏิบัติตามอาจถูกดำเนินการตามกฎหมาย ระเบียบ ข้อบังคับ หรือมาตรการที่ ปส. กำหนด

แนวปฏิบัตินี้ครอบคลุมทั้งระบบการบริหารจัดการข้อมูล กระบวนการบริหารจัดการข้อมูลตลอดวงจรชีวิตของข้อมูล (Data Life Cycle) และองค์ประกอบที่เกี่ยวข้องกับการบริหารจัดการข้อมูล ดังแสดงในรูปต่อไปนี้



รูปที่ 1 กระบวนการบริหารจัดการข้อมูลตลอดวงจรชีวิตของข้อมูล (Data Life Cycle) และองค์ประกอบที่เกี่ยวข้องกับการบริหารจัดการข้อมูล¹

¹ ที่มา: สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน). มาตรฐานรัฐบาลดิจิทัล มรด. 6 : 2566 ว่าด้วยกรอบธรรมาภิบาลข้อมูลภาครัฐ ฉบับปรับปรุง: แนวปฏิบัติ (Data Governance Framework Revised: Guideline) Version 2.0. สำนักนายกรัฐมนตรี, 2566

1.2 วงจรชีวิตของข้อมูล

1.2.1 การสร้างข้อมูล (Create) เป็นการสร้างข้อมูลขึ้นมาใหม่ หรือปรับปรุงข้อมูลเดิม โดยวิธีการบันทึกเข้าไปด้วยบุคคลหรือบันทึกอัตโนมัติด้วยอุปกรณ์อิเล็กทรอนิกส์ เช่น อุปกรณ์ตรวจจับสัญญาณ (Sensor) รวมถึงการจัดหาข้อมูลจากแหล่งภายนอก เช่น การซื้อข้อมูลหรือการรับข้อมูลจากหน่วยงานอื่น เพื่อนำมาจัดเก็บและใช้ประโยชน์ต่อไป

1.2.2 การจัดเก็บข้อมูล (Store) เป็นการจัดเก็บข้อมูลที่เกิดจากกระบวนการสร้าง หรือข้อมูลที่ได้จากการเชื่อมโยงและ/หรือแลกเปลี่ยนกับหน่วยงานอื่น ไม่ว่าจะจัดเก็บลงแฟ้มข้อมูล (File) หรือระบบการจัดการฐานข้อมูล (Database Management System - DBMS) เพื่อให้เกิดความมีระเบียบง่ายต่อการใช้งาน ข้อมูลไม่สูญหายหรือถูกทำลาย และช่วยให้ผู้ใช้งานสามารถประมวลผลข้อมูลต่าง ๆ ตามความต้องการได้อย่างรวดเร็ว

1.2.3 การประมวลผลและการใช้ข้อมูล (Processing and Use) เป็นการนำข้อมูลที่จัดเก็บมาประมวลผล เช่น การถ่ายโอนข้อมูล การเปลี่ยนรูปแบบการจัดเก็บข้อมูล การวิเคราะห์ข้อมูล การจัดทำรายงาน เพื่อนำข้อมูลเหล่านั้นมาใช้งานให้เกิดประโยชน์ตามวัตถุประสงค์ รวมถึงการสำรอง (Backup) ข้อมูลโดยการคัดลอกข้อมูลที่ใช้งานอยู่ในปัจจุบัน เพื่อทำสำเนา เช่น ใช้โปรแกรมในการสำรองข้อมูล เป็นการหลีกเลี่ยงความเสียหายที่จะเกิดขึ้นหากข้อมูลเกิดการเสียหายหรือสูญหาย ซึ่งสามารถนำข้อมูลที่สำรองไว้ในสื่อบันทึกข้อมูลกลับมาใช้งานได้ทันที โดยการกู้คืน (Restore)

1.2.4 การเปิดเผยข้อมูล (Disclosure) เป็นการนำข้อมูลที่อยู่ในความครอบครองของ ปส. ไปเผยแพร่ผ่านช่องทางต่าง ๆ อย่างเหมาะสม เช่น การเปิดเผยข้อมูล (Open data) การแชร์ข้อมูล (Sharing) การกระจายข้อมูล (Dissemination) การควบคุมการเข้าถึง (Access Control) การแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน (Exchange) และการกำหนดเงื่อนไขในการนำข้อมูลไปใช้ (Condition) ทั้งนี้ ก่อนการเผยแพร่ข้อมูลต้องมีการตรวจสอบหมวดหมู่และระดับชั้นความลับของข้อมูล รวมถึงต้องได้รับอนุมัติจากเจ้าของข้อมูล ตามกระบวนการที่กำหนด

1.2.5 กระบวนการจัดเก็บข้อมูลถาวร (Archive) เป็นการย้ายข้อมูลที่มีช่วงอายุเกินช่วงใช้งานหรือไม่ได้ใช้งานแล้ว เพื่อเก็บรักษาถาวรโดยที่ข้อมูลนั้นไม่มีการลบ ปรับปรุง หรือแก้ไขอีก และสามารถนำกลับไปใช้งานได้ใหม่เมื่อต้องการ

1.2.6 การทำลายข้อมูล (Destroy) เป็นการทำลายข้อมูลที่มีการจัดเก็บถาวรเป็นระยะเวลานาน หรือเกินกว่าระยะเวลาที่กำหนด โดยการทำลายข้อมูลต้องอ้างอิงตารางระยะเวลาการเก็บรักษาข้อมูล (Retention Schedule) ของแต่ละชุดข้อมูล ทั้งนี้ การทำลายข้อมูลต้องดำเนินการตามมาตรการด้านความมั่นคงปลอดภัยและกฎหมายที่เกี่ยวข้อง พร้อมจัดเก็บบันทึกและหลักฐานการทำลายข้อมูลไว้เพื่อรองรับการตรวจสอบย้อนหลังได้

1.3 หมวดหมู่และการจัดระดับชั้นของข้อมูล

ข้อมูลของ ปส. สามารถแบ่งหมวดหมู่ตามกรอบธรรมาภิบาลข้อมูลและการใช้งานภายในหน่วยงาน ดังนี้

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

โดยมีการจัดระดับชั้นความลับของข้อมูล ดังนี้

1) ข้อมูลใช้ภายใน (Internal Use Only) ได้แก่ ข้อมูลสำหรับการดำเนินการภายในของ ปส. ซึ่งไม่อนุญาตให้นำไปใช้งานภายนอกก่อนได้รับอนุญาต เช่น นโยบาย มาตรฐาน และขั้นตอนการปฏิบัติงาน ประกาศ และบันทึกภายในของ ปส. เป็นต้น

2) ข้อมูลที่มีชั้นความลับ (Secret) แบ่งเป็น ข้อมูลลับที่สุด (Top Secret) ข้อมูลลับมาก (Secret) และข้อมูลลับ (Confidential)

3) ข้อมูลเปิดเผยได้ (Public) ได้แก่ ข้อมูลที่สามารถเปิดเผยให้แก่บุคคลทั่วไป เช่น ข้อมูลเผยแพร่บนเว็บไซต์ ข้อมูลจากการแถลงข่าว หรือรายงานประจำปีของ ปส.

ซึ่งทุกชุดข้อมูลและเอกสารต้องติดป้ายกำกับหมวดหมู่และชั้นความลับ (Data Classification Label) ทั้งในระบบดิจิทัลและเอกสารกระดาษ เพื่อให้การควบคุมการเข้าถึงเป็นไปอย่างถูกต้อง

1 ข้อมูลใช้ภายใน
(Internal Use Only)



ข้อมูลสำหรับการใช้ในการดำเนินงานภายในของหน่วยงานซึ่งไม่อนุญาตให้นำไปใช้งานภายนอกก่อนได้รับอนุญาต เช่น นโยบาย มาตรฐาน และ ขั้นตอนการปฏิบัติงาน ประกาศ และบันทึกภายในหน่วยงาน เป็นต้น

2 ข้อมูลที่มีชั้นความลับ
(Secret)



ข้อมูลลับที่สุด
(Top Secret)



ข้อมูลลับมาก
(Secret)



ข้อมูลลับ
(Confidential)

3 ข้อมูลเปิดเผยได้
(Public)



ข้อมูลที่สามารถเปิดเผยได้แก่บุคคลทั่วไปโดยไม่ก่อให้เกิดความเสียหายใด ๆ แก่หน่วยงาน เช่น ข้อมูลเผยแพร่บนเว็บไซต์ ข้อมูลจากการแถลงข่าว หรือ รายงานประจำปีของหน่วยงาน เป็นต้น

รูปที่ 2 การจัดระดับชั้นความลับของข้อมูล²

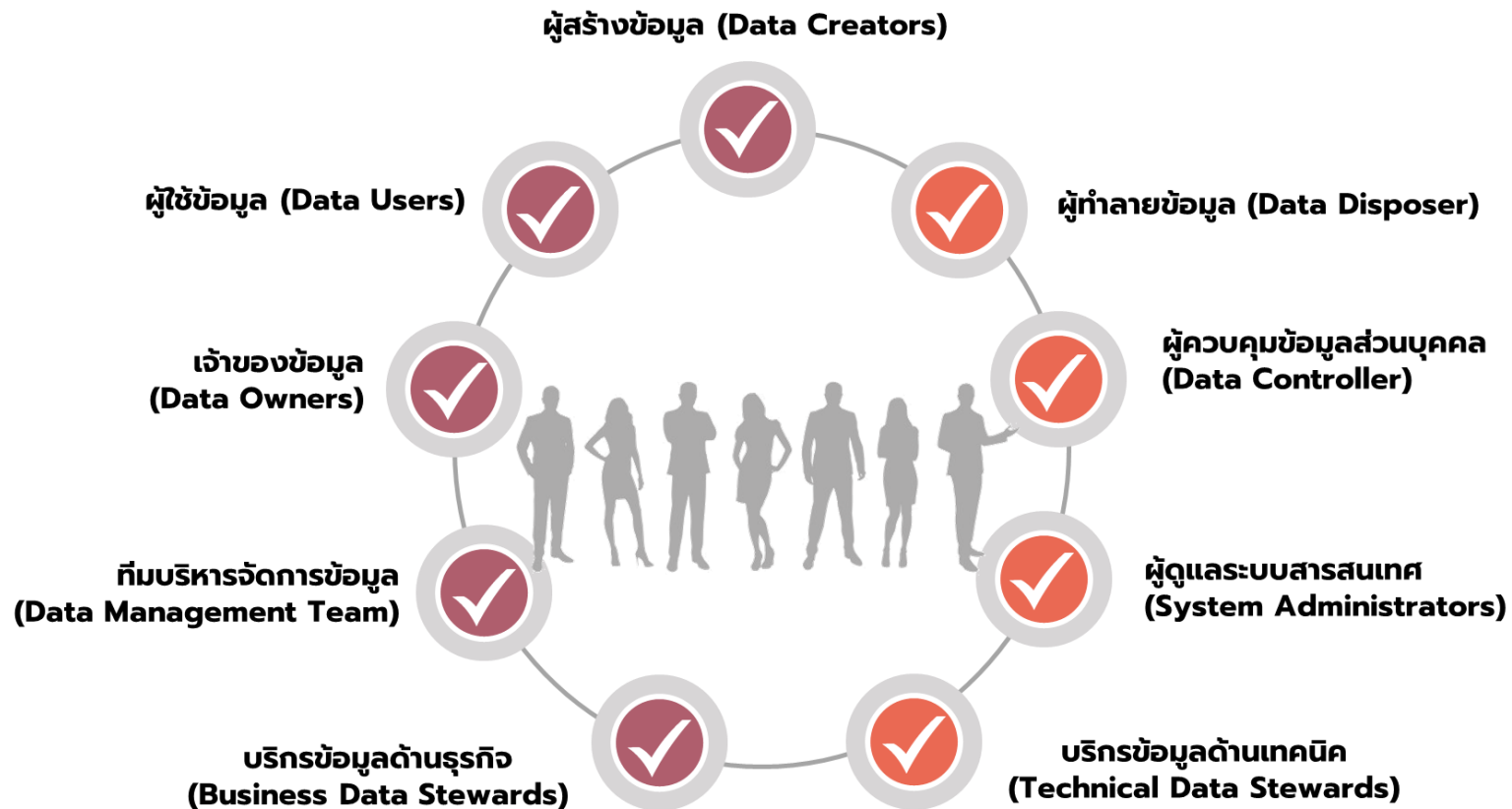
² ที่มา : เอกสารแม่แบบแนวปฏิบัติการบริหารจัดการข้อมูล (Data Management Guideline Template) ตาม มาตรฐานรัฐบาลดิจิทัล มรด. 4-2 : 2565 ว่าด้วยข้อเสนอแนะสำหรับการจัดทำแนวปฏิบัติการบริหารจัดการข้อมูล (Recommendation for Writing Data Management Guideline) Version 1.0, สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน), สำนักนายกรัฐมนตรี

1.4 ผู้เกี่ยวข้อง

ทั้งนี้แนวปฏิบัติเกี่ยวกับข้อมูลนี้บังคับใช้กับผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับข้อมูลตามประกาศแนวปฏิบัติการบริหารจัดการข้อมูลของ ปส. (Data Management) รวมถึงผู้เกี่ยวข้องอื่น ๆ ที่ไม่ได้ระบุไว้ในแนวปฏิบัติ ดังนี้

- 1) ผู้สร้างข้อมูล (Data Creators)
- 2) ผู้ใช้ข้อมูล (Data Users)
- 3) เจ้าของข้อมูล (Data Owners)
- 4) ทีมบริหารจัดการข้อมูล (Data Management Team)
- 5) บริกรข้อมูลด้านธุรกิจ (Business Data Stewards)
- 6) บริกรข้อมูลด้านเทคนิค (Technical Data Stewards)
- 7) ผู้ดูแลระบบสารสนเทศ (System Administrators)
- 8) ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)
- 9) ผู้ทำลายข้อมูล (Data Disposer)

ผู้มีส่วนได้เสีย (Stakeholders)



รูปที่ 3 ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับข้อมูลตามประกาศ³

³ ที่มา : เอกสารแม่แบบแนวปฏิบัติการบริหารจัดการข้อมูล (Data Management Guideline Template) ตาม มาตรฐานรัฐบาลดิจิทัล มรด. 4-2 : 2565 ว่าด้วยข้อเสนอแนะสำหรับการจัดทำแนวปฏิบัติการบริหารจัดการข้อมูล (Recommendation for Writing Data Management Guideline) Version 1.0, สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน), สำนักนายกรัฐมนตรี

1.5 คำนิยาม

คำศัพท์	ความหมาย
สำนักงาน	สำนักงานปรมาณูเพื่อสันติ (ปส.)
คณะกรรมการบริหารจัดการ ธรรมาภิบาลข้อมูล (Data Governance Council)	ประกอบไปด้วย - ผู้บริหารระดับสูงสุดของ ปส. (Chief Executive Officer : CEO) - ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO) - ผู้บริหารข้อมูลระดับสูง (Chief Data Officer : CDO) - หัวหน้าหน่วยงานเทคโนโลยีสารสนเทศ (ททส.) และผู้ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Chief Information Security Officer : CISO) - ผู้บริหารจากส่วนงานต่าง ๆ ทั้งจากสายงานบริหารและสายงานเทคโนโลยีสารสนเทศ รวมไปถึงหัวหน้าทีมบริการข้อมูล (Lead Data Steward Team) - คณะกรรมการธรรมาภิบาลข้อมูลมีอำนาจสูงสุดในธรรมาภิบาลข้อมูลภายในสำนักงานปรมาณูเพื่อสันติ หรือคณะกรรมการ/คณะทำงาน ซึ่งทำหน้าที่ตัดสินใจเชิงนโยบาย แก้ไขปัญหา และบริหารจัดการข้อมูลของ ปส. หมายเหตุ : เพื่อให้การกำกับดูแลข้อมูลเป็นไปตามหลักธรรมาภิบาลข้อมูล ควรกำหนดให้มีผู้บริหารข้อมูลระดับสูง (Chief Data Officer : CDO) โดยเฉพาะเพื่อรับผิดชอบด้านการบริหารจัดการข้อมูลของหน่วยงาน อย่างไรก็ตาม ในกรณีที่หน่วยงานมีข้อจำกัดด้านบุคลากร ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO) อาจได้รับมอบหมายให้ปฏิบัติหน้าที่เป็น CDO ได้ ทั้งนี้ แนวปฏิบัติที่เหมาะสมควรมีผู้รับผิดชอบแยกบทบาทระหว่าง CIO และ CDO เพื่อให้เกิดประสิทธิภาพในการกำกับดูแลด้านเทคโนโลยีสารสนเทศ และการบริหารจัดการข้อมูลอย่างเหมาะสม
หัวหน้าหน่วยงานของรัฐ	เลขาธิการสำนักงานปรมาณูเพื่อสันติ
ผู้บริหาร	ผู้บริหารที่เกี่ยวข้องกับการบริหารจัดการข้อมูล ตามคณะกรรมการ/คณะทำงานที่เกี่ยวข้อง
ข้าราชการ/พนักงาน ราชการ/ลูกจ้างประจำ	บุคคลผู้ที่ได้รับการบรรจุ และแต่งตั้งเป็นเจ้าหน้าที่ของ ปส.
ลูกจ้าง	บุคคลที่มีสัญญาจ้างให้ปฏิบัติงานเป็นการชั่วคราว และมีกำหนดระยะเวลา และสิ้นสุดที่แน่นอนแต่ไม่เกินปีงบประมาณ ซึ่งเป็นเจ้าหน้าที่ของ ปส.
ผู้บังคับบัญชา	ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของ ปส.
ผู้สร้างข้อมูล (Data Creators)	บุคลากรของทุกกอง/ศูนย์/กลุ่ม ที่ทำหน้าที่บันทึก แก้ไข ปรับปรุง หรือลบข้อมูลให้สอดคล้องกับโครงสร้างที่ถูกกำหนดไว้

คำศัพท์	ความหมาย
ผู้ใช้ข้อมูล (Data Users)	คณะกรรมการ ผู้อำนวยการ ข้าราชการ/เจ้าหน้าที่/พนักงาน ลูกจ้าง รวมถึงหน่วยงานภายนอกที่ได้รับอนุญาต (Authorized Users) ให้สามารถเข้ามาใช้ข้อมูลของ ปส. ตามสิทธิ์และหน้าที่ความรับผิดชอบ พร้อมทั้งรายงานประเด็นปัญหาที่พบระหว่างการใช้อข้อมูล
สิทธิ์ของผู้ใช้งานข้อมูล	สิทธิ์และหน้าที่ตามบทบาท (Role) ที่เกี่ยวข้องกับข้อมูลและระบบสารสนเทศของ ปส. มีดังนี้ ▪ สิทธิ์ใช้งานทั่วไป หมายถึง คณะกรรมการ ผู้อำนวยการ ข้าราชการ/เจ้าหน้าที่/พนักงาน ลูกจ้าง ที่ใช้งานระบบสารสนเทศพื้นฐานของ ปส. ผู้ใช้งานข้อมูลต้องขออนุญาตจากผู้บังคับบัญชา โดยให้ใช้แบบฟอร์มเพื่อขออนุมัติตามที่ ปส. กำหนด ▪ สิทธิ์จำเพาะ หมายถึง สิทธิ์เฉพาะตามหน้าที่ความรับผิดชอบที่เกี่ยวข้องกับการปฏิบัติงาน ผู้ใช้งานข้อมูลต้องได้รับสิทธิ์จากผู้บังคับบัญชา ▪ สิทธิ์พิเศษ หมายถึง สิทธิ์ที่ได้รับมอบหมายเพิ่มเติมจากผู้บังคับบัญชาเป็นกรณีพิเศษ ผู้ใช้งานต้องได้รับมอบหมายจากผู้บังคับบัญชาเป็นครั้งคราว
เจ้าของข้อมูล (Data Owner)	ผู้ที่ได้รับมอบหมายในการปฏิบัติงานให้รับผิดชอบข้อมูลที่ระบุไว้ ซึ่งรวมถึงผู้บังคับบัญชาของเจ้าของข้อมูลนั้นด้วย โดยทำหน้าที่กำกับดูแลตามธรรมชาติของข้อมูลตลอดวงจรชีวิตของข้อมูลนั้น ๆ รวมทั้งทำหน้าที่กำหนดสิทธิ์ในการเข้าถึงข้อมูลและจัดชั้นความลับของข้อมูล
เจ้าของข้อมูลส่วนบุคคล (Data Subject)	บุคคลผู้เป็นเจ้าของข้อมูลส่วนบุคคลหรือผู้มีสิทธิ์โดยชอบตามกฎหมาย ซึ่งในนโยบายนี้ หมายถึง บุคคลธรรมดาซึ่งเป็นเจ้าของข้อมูลส่วนบุคคลที่ ปส. เก็บรวบรวม ใช้ หรือเปิดเผย
เจ้าของระบบงาน (System Owner)	ผู้ที่มีหน้าที่รับผิดชอบในการใช้งาน ดูแลและบำรุงรักษา หรือปรับปรุงระบบงานที่ใช้ใน ปส.
ทีมบริหารจัดการข้อมูล (Data Management Team)	กลุ่มบุคลากรภายในระดับกอง/ศูนย์/กลุ่ม ที่รับผิดชอบดูแลและบริหารจัดการระบบสารสนเทศหลักของหน่วยงาน โดยมีเจ้าหน้าที่กลุ่มเทคโนโลยีสารสนเทศ (IT) ทำหน้าที่ให้คำปรึกษาและสนับสนุนการดำเนินงาน ร่วมกับหน่วยงานเจ้าของข้อมูลของ ปส. ในการดูแลรักษาข้อมูลในระบบสารสนเทศ และสนับสนุนการดำเนินงานด้านธรรมาภิบาลข้อมูลภาครัฐ เช่น การจัดทำนิยามคำอธิบายข้อมูล (Metadata) การจัดทำนโยบายและมาตรฐานข้อมูล รวมถึง การกำหนดสิทธิ์การเข้าถึงข้อมูล โดยมีผู้ดูแลฐานข้อมูล (Database Administrator: DBA) เป็นผู้รับผิดชอบในส่วนที่เกี่ยวข้อง

คำศัพท์	ความหมาย
หัวหน้าคณะทำงานบริการข้อมูล (Lead Data Steward Team)	บุคลากรที่ทำหน้าที่ในการกำกับดูแลและสนับสนุนการดำเนินงานของคณะทำงานบริการข้อมูล (Lead Data Steward Team) ให้เป็นไปตามกรอบธรรมาภิบาลข้อมูลภาครัฐ
บริการข้อมูลด้านธุรกิจ (Business Data Stewards Team)	บุคลากรที่ได้รับมอบหมายให้ทำหน้าที่กำหนดนิยามความต้องการด้านคุณภาพและความมั่นคงปลอดภัยซึ่งอาจจะได้รับมาจากผู้ใช้ข้อมูล (Data Users) หรือผู้มีส่วนได้เสียอื่น ๆ มีหน้าที่ ดังนี้ 1) จัดทำ (ร่าง) ธรรมาภิบาลข้อมูลภาครัฐของ ปส. ร่วมกับคณะบริการข้อมูลด้านอื่น ๆ โดยกำหนดนโยบายข้อมูล จำแนกหมวดหมู่ข้อมูล มาตรการควบคุมและพัฒนาคุณภาพข้อมูลเพื่อให้ข้อมูลมีความถูกต้อง ครบถ้วน เป็นปัจจุบัน มั่นคงปลอดภัย และไม่ละเมิดความเป็นส่วนตัว รวมทั้งสามารถเชื่อมโยงข้อมูล แลกเปลี่ยน บูรณาการ และใช้ประโยชน์ได้อย่างมีประสิทธิภาพ 2) กำหนดความต้องการด้านคุณภาพข้อมูลและความมั่นคงปลอดภัยจากผู้ใช้อข้อมูลหรือผู้มีส่วนได้ส่วนเสียกับข้อมูลร่วมกับคณะบริการข้อมูลด้านอื่น ๆ 3) กำหนดนิยามพร้อมจัดทำคำอธิบายชุดข้อมูลดิจิทัล (Metadata) และบัญชีข้อมูลให้ครบถ้วนตามความจำเป็นในการใช้งานและตรงความต้องการของผู้มีส่วนได้ส่วนเสียกับข้อมูล ร่วมกับคณะบริการข้อมูลด้านเทคนิค 4) ดำเนินงานให้สอดคล้องกับนโยบาย เป้าประสงค์ ความต้องการของผู้มีส่วนได้ส่วนเสียกับข้อมูล รวมทั้งติดตามการดำเนินงานตามแผนที่กำหนดเพื่อตรวจสอบการปฏิบัติตามนโยบายข้อมูล 5) ทบทวนและปรับปรุงกระบวนการ เพื่อนำมาปรับปรุงกระบวนการทำงาน 6) รายงานผลลัพธ์ไปยังคณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council) ของ ปส. 7) ปฏิบัติงานอื่น ๆ ตามที่ได้รับมอบหมายจากคณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council) ของ ปส.
บริการข้อมูลด้านเทคนิค (Technical Data Stewards Team)	บุคลากรที่ทำหน้าที่ให้การสนับสนุนด้านเทคโนโลยีสารสนเทศแก่บริการข้อมูลด้านธุรกิจ มีหน้าที่ ดังนี้ 1) จัดทำ (ร่าง) ธรรมาภิบาลข้อมูลภาครัฐของ ปส. ร่วมกับคณะบริการข้อมูลด้านอื่น ๆ โดยกำหนดนโยบายข้อมูล จำแนกหมวดหมู่ข้อมูล มาตรการควบคุมและพัฒนาคุณภาพข้อมูลเพื่อให้ข้อมูลมีความถูกต้อง ครบถ้วน เป็นปัจจุบัน มั่นคงปลอดภัย และไม่ละเมิดความเป็นส่วนตัว รวมทั้งสามารถเชื่อมโยงข้อมูล แลกเปลี่ยน บูรณาการ และใช้ประโยชน์ได้อย่างมีประสิทธิภาพ

คำศัพท์	ความหมาย
	2) กำหนดความต้องการด้านคุณภาพข้อมูลและความมั่นคงปลอดภัยจากผู้ใช้ข้อมูลหรือผู้มีส่วนได้ส่วนเสียกับข้อมูลร่วมกับคณะบริการข้อมูลด้านอื่น ๆ 3) กำหนดนิยามพร้อมจัดทำคำอธิบายชุดข้อมูลดิจิทัล (Metadata) และบัญชีข้อมูลให้ครบถ้วนตามความจำเป็นในการใช้งานและตรงความต้องการของผู้มีส่วนได้ส่วนเสียกับข้อมูล ร่วมกับคณะบริการข้อมูลด้านธุรกิจ 4) ให้การสนับสนุนด้านเทคโนโลยีสารสนเทศแก่คณะบริการข้อมูลด้านอื่น ๆ ในการจัดทำรวมทั้งให้ข้อเสนอแนะเชิงเทคนิคที่สอดคล้องกับนโยบายและเป้าประสงค์ความต้องการของผู้มีส่วนได้ส่วนเสียกับข้อมูล 5) กำหนดรายละเอียดที่เกี่ยวข้องกับการออกแบบระบบเทคโนโลยีสารสนเทศและอื่น ๆ ที่เกี่ยวข้อง 6) สนับสนุนการดำเนินงานด้านเทคโนโลยีสารสนเทศ 7) ปฏิบัติงานอื่น ๆ ตามที่ได้รับมอบหมายจากคณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council) ของ ปส.
บริการข้อมูลด้านคุณภาพ (Quality Data Stewards Team)	บุคลากรที่ทำหน้าที่ดำเนินการในเรื่องคุณภาพข้อมูล เช่น กำหนดนโยบายข้อมูลด้านคุณภาพ การตรวจวัดคุณภาพข้อมูล และการวิเคราะห์คุณภาพข้อมูล มีหน้าที่ ดังนี้ 1) จัดทำ (ร่าง) ธรรมาภิบาลข้อมูลภาครัฐของ ปส. เพื่อสันติร่วมกับคณะบริการข้อมูลด้านอื่น ๆ โดยกำหนดนโยบายข้อมูล จำแนกหมวดหมู่ข้อมูล มาตรการควบคุมและพัฒนาคุณภาพข้อมูลเพื่อให้ข้อมูลมีความถูกต้อง ครบถ้วน เป็นปัจจุบัน มั่นคงปลอดภัย และไม่ละเมิดความเป็นส่วนตัว รวมทั้งสามารถเชื่อมโยงข้อมูล แลกเปลี่ยน บูรณาการ และใช้ประโยชน์ได้อย่างมีประสิทธิภาพ 2) กำหนดความต้องการด้านคุณภาพข้อมูลและความมั่นคงปลอดภัยจากผู้ใช้ข้อมูลหรือผู้มีส่วนได้ส่วนเสียกับข้อมูล ร่วมกับคณะบริการข้อมูลด้านอื่น ๆ 3) วิเคราะห์ความพร้อมของธรรมาภิบาลข้อมูลภาครัฐของ ปส. ความต้องการด้านคุณภาพ การรักษาความเป็นส่วนตัวและความมั่นคงปลอดภัย ให้เหมาะสมกับสถานการณ์ปัจจุบัน 4) ตรวจสอบ วิเคราะห์ และวัดผลการดำเนินงาน 5) รายงานผลลัพธ์ไปยังคณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council) ของ ปส. 6) ปฏิบัติงานอื่น ๆ ตามที่ได้รับมอบหมายจากคณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council) ของ ปส.

คำศัพท์	ความหมาย
ผู้ดูแลระบบสารสนเทศ (System Administrators)	บุคลากรภายในกอง/ศูนย์/กลุ่ม ที่ทำหน้าที่ดูแลและรับผิดชอบระบบสารสนเทศหลักของหน่วยงานในฐานะหน่วยงานเจ้าของระบบ โดยมีเจ้าหน้าที่กลุ่มเทคโนโลยีสารสนเทศ (IT) ทำหน้าที่ให้คำปรึกษาและสนับสนุนด้านเทคนิคเพื่อให้ระบบสามารถดำเนินงานได้อย่างมีประสิทธิภาพ มีเสถียรภาพ และสอดคล้องตามมาตรฐานที่กำหนด
ผู้ดูแลระบบแม่ข่าย (Server Administrators)	บุคลากรของกลุ่มเทคโนโลยีสารสนเทศ (IT) ที่มีหน้าที่ดูแล บริหารจัดการ และควบคุมการทำงานของระบบแม่ข่าย (Server) ของ ปส. เพื่อให้ระบบมีความพร้อมใช้งาน มีเสถียรภาพ และมีความมั่นคงปลอดภัย
ผู้จัดการโครงการ (Project Managers)	บุคลากรจากทุกกอง/ศูนย์/กลุ่ม ของหน่วยงานหลักที่ได้รับมอบหมายบริหารจัดการโครงการตามแผนดำเนินงาน
ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)	บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
ผู้ทำลายข้อมูล (Data Disposer)	บุคลากรที่ได้รับการกำหนดสิทธิ์จากเจ้าของข้อมูลให้มีสิทธิ์ในการทำลายข้อมูล
ข้อมูล (Data)	สิ่งที่สื่อความหมายให้รู้เรื่องราวข้อเท็จจริงหรือเรื่องอื่นใด ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั่นเอง 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)	การนำข้อมูลจากหลายแหล่งมารวบรวม เพื่อจัดเป็นชุดให้ตรงตามลักษณะโครงสร้างของข้อมูล หรือจากการใช้ประโยชน์ของข้อมูล
สารสนเทศ (Information)	ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบข้อมูล ซึ่งอาจอยู่ในรูปของตัวเลข ข้อความหรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้งานสามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ
ระบบสารสนเทศ (Information System)	ระบบงานที่นำเทคโนโลยีมาช่วยในการสร้างสารสนเทศที่สามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนา และควบคุมการติดต่อสื่อสาร ซึ่งประกอบด้วยเทคโนโลยีคอมพิวเตอร์และเทคโนโลยีการสื่อสารโทรคมนาคม เช่น ระบบคอมพิวเตอร์

คำศัพท์	ความหมาย
	(Computer System) ระบบเครือข่าย (Network System) ซอฟต์แวร์ (Software) ข้อมูล (Data) และสารสนเทศ (Information) เป็นต้น
อินทราเน็ต (Intranet)	เป็นระบบเครือข่ายที่สามารถเข้าถึงได้โดยผู้ใช้งานภายในสำนักงานเท่านั้น โดยมีจุดประสงค์เพื่อการติดต่อสื่อสาร แลกเปลี่ยนข้อมูลและสารสนเทศภายในสำนักงาน
การเข้าถึงและควบคุมการใช้งานข้อมูล	การเข้าถึงและการใช้งานข้อมูลทั้งทางอิเล็กทรอนิกส์หรือกายภาพ รวมทั้งการอนุญาต การกำหนดสิทธิ์ในการเข้าถึงและใช้งานข้อมูล การปรับปรุงข้อมูล การเพิกถอนหรือการยกเลิกสิทธิ์การเข้าถึงข้อมูล
การเข้าถึงและควบคุมการใช้งานระบบสารสนเทศ	การเข้าถึงและการใช้งานระบบสารสนเทศ รวมทั้งการตรวจสอบ การอนุมัติ การกำหนดสิทธิ์หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ และการเพิกถอนหรือการยกเลิกสิทธิ์การเข้าถึงเครือข่ายหรือระบบสารสนเทศ
ทรัพย์สิน (Asset)	สิ่งที่มีคุณค่าหรือมูลค่าต่อสำนักงานและเป็นทรัพย์สินที่เกี่ยวข้องกับการประมวลผลสารสนเทศที่สำนักงานเป็นเจ้าของ เช่า ว่าจ้าง พัฒนา หรือจัดซื้อ โดยแบ่งแยกออกเป็นประเภทต่าง ๆ ได้แก่ สารสนเทศ (Information) ซอฟต์แวร์ (Software) ทรัพย์สินที่มีรูปร่าง (Physical Asset) บริการสาธารณูปโภคพื้นฐาน (Service) และบุคลากร (People)
ข้อมูลของหน่วยงาน	ข้อมูลที่อยู่ในความครอบครองหรือควบคุมดูแลของสำนักงาน
ข้อมูลสาธารณะ (Public Data)	ข้อมูลที่สามารถเปิดเผยได้ สามารถนำไปใช้ได้อย่างอิสระ ไม่ว่าจะเป็นข้อมูลข่าวสาร ข้อมูลอิเล็กทรอนิกส์ เป็นต้น
ข้อมูลส่วนบุคคล (Personal Data)	ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ (พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562)
ข้อมูลความมั่นคง (National Security Data)	ข้อมูลเกี่ยวกับความมั่นคงของรัฐ ที่ทำให้เกิดความสงบเรียบร้อย การมีเสถียรภาพ ความเป็นปึกแผ่น ปลอดภัยจากภัยคุกคาม เป็นต้น
ข้อมูลความลับทางราชการ (Confidential Government Data)	ข้อมูลที่อยู่ในความครอบครองหรือควบคุมดูแลของสำนักงานที่มีคำสั่งไม่ให้มีการเปิดเผย และมีการกำหนดชั้นความลับของข้อมูล
ข้อมูลลับ (Confidential)	ข้อมูลข่าวสารซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์ของรัฐซึ่งผู้ที่สามารถเข้าถึงได้ต้องเป็นบุคคลที่มีสิทธิ์เท่านั้น และห้ามเผยแพร่ต่อบุคคลภายนอกเว้นแต่จะได้รับอนุมัติเป็นลายลักษณ์อักษร

คำศัพท์	ความหมาย
	โดยผู้บริหารระดับหัวหน้ากลุ่มงานที่เป็นเจ้าของข้อมูลขึ้นไป ⁴ โดยต้องมีการลงนามในเอกสารข้อตกลงการไม่เปิดเผยข้อมูล (Non-Disclosure Agreement) เว้นแต่การเผยแพร่ดังกล่าวเป็นไปตามอำนาจที่กฎหมายให้การรับรอง
ข้อมูลลับมาก (Secret)	ข้อมูลข่าวสารซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรงซึ่งผู้ที่สามารถเข้าถึงได้ต้องเป็นบุคคลที่มีสิทธิ์เท่านั้นและห้ามเผยแพร่ต่อบุคคลภายนอก เว้นแต่จะได้รับอนุมัติเป็นลายลักษณ์อักษรโดยผู้บริหารระดับผู้ช่วยผู้อำนวยการระดับกอง/สำนัก/ศูนย์ ที่เป็นเจ้าของข้อมูลขึ้นไป ⁵ โดยต้องมีการลงนามในเอกสารข้อตกลงการไม่เปิดเผยข้อมูล (Non-Disclosure Agreement) เว้นแต่การเผยแพร่ดังกล่าวเป็นไปตามอำนาจที่กฎหมายให้การรับรอง
ข้อมูลลับที่สุด (Top Secret)	ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรงที่สุดซึ่งผู้ที่สามารถเข้าถึงได้ต้องเป็นบุคคลที่มีสิทธิ์เท่านั้นและห้ามเผยแพร่ต่อบุคคลภายนอกเว้นแต่จะได้รับอนุมัติเป็นลายลักษณ์อักษรโดยผู้บริหารระดับเลขาธิการ/รองเลขาธิการขึ้นไป ⁶ โดยต้องมีการลงนามในเอกสารข้อตกลงการไม่เปิดเผยข้อมูล (Non-Disclosure Agreement) เว้นแต่การเผยแพร่ดังกล่าวเป็นไปตามอำนาจที่กฎหมายให้การรับรอง
ข้อมูลใช้ภายใน (Internal Use Only)	ข้อมูลสำหรับใช้ในการดำเนินการภายใน ปรส. ซึ่งไม่อนุญาตให้นำไปใช้งานภายนอกก่อนได้รับอนุญาต เช่น นโยบาย มาตรฐานและขั้นตอนการปฏิบัติงาน ประกาศ และบันทึกภายในหน่วยงาน เป็นต้น

⁴ ที่มา : เอกสารแม่แบบแนวปฏิบัติการบริหารจัดการข้อมูล (Data Management Guideline Template) ตาม มาตรฐานรัฐบาลดิจิทัล มรด. 4-2 : 2565 ว่าด้วยข้อเสนอแนะสำหรับการจัดทำแนวปฏิบัติการบริหารจัดการข้อมูล (Recommendation for Writing Data Management Guideline) Version 1.0, สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน), สำนักนายกรัฐมนตรี

⁵ ที่มา : เอกสารแม่แบบแนวปฏิบัติการบริหารจัดการข้อมูล (Data Management Guideline Template) ตาม มาตรฐานรัฐบาลดิจิทัล มรด. 4-2 : 2565 ว่าด้วยข้อเสนอแนะสำหรับการจัดทำแนวปฏิบัติการบริหารจัดการข้อมูล (Recommendation for Writing Data Management Guideline) Version 1.0, สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน), สำนักนายกรัฐมนตรี

⁶ ที่มา : เอกสารแม่แบบแนวปฏิบัติการบริหารจัดการข้อมูล (Data Management Guideline Template) ตาม มาตรฐานรัฐบาลดิจิทัล มรด. 4-2 : 2565 ว่าด้วยข้อเสนอแนะสำหรับการจัดทำแนวปฏิบัติการบริหารจัดการข้อมูล (Recommendation for Writing Data Management Guideline) Version 1.0, สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน), สำนักนายกรัฐมนตรี

1.6 การเผยแพร่และการทบทวน

แนวปฏิบัติเกี่ยวกับข้อมูลฉบับนี้ จะได้รับการเผยแพร่ผ่านการประกาศในศูนย์ข้อมูลข่าวสารอิเล็กทรอนิกส์ของราชการ ปส. และการแจ้งเวียนผ่านระบบสารบรรณอิเล็กทรอนิกส์ รวมถึงการประชาสัมพันธ์ผ่านเว็บไซต์ของหน่วยงานและไปรษณีย์อิเล็กทรอนิกส์ (Email) เพื่อให้เจ้าหน้าที่ทุกระดับของ ปส. รับทราบและถือปฏิบัติอย่างเคร่งครัด

ทั้งนี้ จะมีการทบทวนแนวปฏิบัติดังกล่าวเป็นประจำอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ และ/หรือเมื่อได้รับข้อเสนอแนะจากคณะกรรมการธรรมาภิบาลข้อมูลว่ามีความจำเป็นต้องปรับปรุงแก้ไข



ส่วนที่ 1

แนวปฏิบัติการบริหารจัดการข้อมูล

แนวปฏิบัติการบริหารจัดการข้อมูล

แนวปฏิบัติการบริหารจัดการข้อมูลฉบับนี้กำหนดกรอบการดำเนินงานตามวงจรชีวิตของข้อมูล (Data Life Cycle) โดยแบ่งออกเป็น 6 หมวด ได้แก่ การสร้างข้อมูล การจัดเก็บข้อมูล การประมวลผลและการใช้ข้อมูล การเปิดเผยข้อมูล การจัดเก็บข้อมูลถาวร และการทำลายข้อมูล ซึ่งในแต่ละหมวดได้กำหนดวัตถุประสงค์ ผู้รับผิดชอบ เอกสารอ้างอิง และข้อปฏิบัติไว้อย่างชัดเจน พร้อมทั้งจัดทำตารางแสดงความสัมพันธ์ระหว่างกระบวนการหรือกิจกรรมกับผู้มีส่วนได้ส่วนเสีย เพื่อให้การบริหารจัดการข้อมูลเป็นไปอย่างเป็นระบบ มีประสิทธิภาพ และสามารถตรวจสอบย้อนหลังได้ ทั้งนี้ หน่วยงานสามารถกำหนดแนวปฏิบัติหรือมาตรการเพิ่มเติมให้เหมาะสมกับบริบทการดำเนินงานและวัฒนธรรมองค์กรได้ โดยต้องไม่ขัดต่อกฎหมายระเบียบ ข้อบังคับ คำสั่ง นโยบาย และข้อกำหนดที่เกี่ยวข้องอย่างเคร่งครัด

หมวด 1 การสร้างข้อมูล

วัตถุประสงค์

กำหนดแนวปฏิบัติสำหรับผู้ที่เกี่ยวข้องในการสร้างข้อมูลให้มีคุณภาพ มีความมั่นคงปลอดภัย และเป็นประโยชน์ต่อผู้ใช้ข้อมูล

ผู้รับผิดชอบงาน

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

อ้างอิง

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

ข้อปฏิบัติ

1) เจ้าของข้อมูล โดยดำเนินการ ดังนี้

1.1) กำหนดผู้มีสิทธิ์ในการสร้างข้อมูล และจะต้องทบทวนสิทธิ์นั้น อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ เช่น การลาออก เปลี่ยนตำแหน่ง โอนย้าย สิ้นสุดการจ้าง การปรับโครงสร้าง หรือเมื่อมีการปรับปรุงระบบสารสนเทศ เป็นต้น

1.2) กำหนดหมวดหมู่และชั้นความลับของข้อมูลตามมาตรฐานของ ปส.

1.3) รับผิดชอบในการตรวจสอบความถูกต้อง ครบถ้วน เป็นปัจจุบันของข้อมูลที่ถูกสร้างขึ้น และดำเนินการแก้ไขหากพบข้อผิดพลาด เพื่อให้มั่นใจว่าข้อมูลมีคุณภาพและสามารถนำไปใช้งานได้ถูกต้อง

1.4) กำหนดมาตรฐานในการจัดเก็บข้อมูลที่สร้างขึ้นให้เหมาะสมกับประเภท หมวดหมู่ และระดับชั้นความลับของข้อมูล เพื่อให้ข้อมูลสามารถจัดเก็บ สืบค้น เข้าถึง และนำไปใช้งานได้ถูกต้อง มั่นคง ปลอดภัย และมีประสิทธิภาพ

2) ผู้ดูแลระบบสารสนเทศ โดยดำเนินการ ดังนี้

2.1) กำหนดสิทธิ์ในการสร้างข้อมูลในระบบให้แก่ผู้สร้างข้อมูลตามที่เจ้าของข้อมูลกำหนด

2.2) ควบคุมและตรวจสอบการให้สิทธิ์การเข้าถึงข้อมูลให้เป็นไปตามแนวนโยบายความมั่นคง ปลอดภัยด้านสารสนเทศสำนักงานปรมาณูเพื่อสันติ

3) เจ้าของข้อมูล บริกรข้อมูลด้านธุรกิจ บริกรข้อมูลด้านเทคนิค และทีมบริหารจัดการข้อมูล ร่วมกันจัดทำคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตา (Metadata) เมื่อมีการสร้างชุดข้อมูล (Datasets) โดยต้องเป็นไปตามมาตรฐานที่สำนักงานพัฒนารัฐบาลดิจิทัล (สพร.) กำหนด และต้องทำการประเมินคุณค่าของชุดข้อมูลดิจิทัลตามแบบฟอร์มประเมินที่ สพร. หรือ ปส. กำหนด เพื่อพิจารณาคัดเลือกเป็นชุดข้อมูลคุณค่าสูง (High Value Dataset) และเผยแพร่เป็นข้อมูลเปิดของหน่วยงานต่อสาธารณะ ตามกฎหมายว่าด้วยข้อมูลข่าวสารของราชการในรูปแบบข้อมูลดิจิทัล

4) การจัดทำบัญชีรายการ มีแนวทางดำเนินการ ดังนี้

4.1) เจ้าของข้อมูล ต้องกำหนดรายการชุดข้อมูล โดยมีหลักเกณฑ์ที่ชัดเจนในการพิจารณา ระดับความสำคัญของชุดข้อมูลที่เป็นต่อการวางแผน การปฏิบัติงาน และการให้บริการของหน่วยงาน เช่น ข้อมูลที่ใช้ในการจัดทำนโยบาย ยุทธศาสตร์ และตัวชี้วัดของ ปส. ข้อมูลที่ใช้ในการจัดทำรายงานตามภารกิจ ข้อมูลเพื่อการให้บริการประชาชน และข้อมูลที่ใช้ในการเชื่อมโยงหรือแลกเปลี่ยนระหว่างหน่วยงาน

4.2) เจ้าของข้อมูลต้องจัดทำคำอธิบายชุดข้อมูล (Metadata) โดยอ้างอิงตามแนวปฏิบัติการจัดทำคำอธิบายชุดข้อมูลของ ปส. เพื่อให้ข้อมูลมีความชัดเจน ถูกต้อง และสามารถนำไปใช้ประโยชน์ได้อย่างมีประสิทธิภาพ

4.3) บริกรข้อมูล (Data Steward) ของ ปส. ต้องรวบรวมรายการชุดข้อมูลและคำอธิบายชุดข้อมูล จัดทำเป็นบัญชีรายการข้อมูล (Data Catalog) และเผยแพร่ในรูปแบบที่สะดวกต่อการสืบค้นและใช้งาน ทั้งนี้ ต้องมีการปรับปรุงข้อมูลและคำอธิบายชุดข้อมูลให้เป็นปัจจุบันอย่างสม่ำเสมอ ตามความเหมาะสมและการเปลี่ยนแปลงของหน่วยงาน

5) ห้ามมิให้ผู้สร้างข้อมูลนำข้อมูลที่มีลักษณะดังต่อไปนี้เข้าสู่ระบบคอมพิวเตอร์ที่ขัดต่อกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์

5.1) ข้อมูลที่บิดเบือน หรือปลอมไม่ว่าทั้งหมดหรือบางส่วน

5.2) ข้อมูลอันเป็นเท็จ ที่น่าจะเกิดความเสียหายต่อการรักษาความมั่นคงปลอดภัย ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจ หรือ โครงสร้างพื้นฐาน หรือ ก่อให้เกิดความตื่นตระหนก

5.3) ข้อมูลอันเป็นความผิดเกี่ยวกับความมั่นคง หรือ ความผิดเกี่ยวกับการก่อการร้าย

5.4) ข้อมูลที่มีลักษณะอันลามก และคนทั่วไปอาจเข้าถึงได้

5.5) ข้อมูลที่ปรากฏภาพของผู้อื่น และเป็นภาพที่สร้างขึ้น ตัดต่อ เดิม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ ทำให้ผู้อื่นเสียชื่อเสียง ถูกดูหมิ่นถูกเกลียดชัง หรือ ได้รับความอับอาย

6) ห้ามมิให้ผู้สร้างข้อมูล ทำการสร้าง/ทำซ้ำต่อข้อมูลที่ขัดต่อกฎหมายว่าด้วยลิขสิทธิ์หรือทรัพย์สินทางปัญญาของผู้อื่น เว้นแต่จะเป็นไปตามอำนาจที่กฎหมายรับรอง

7) กำหนดให้ผู้สร้างข้อมูลสร้างข้อมูลที่มาจากแหล่งข้อมูลที่เชื่อถือได้เท่านั้น

8) หากข้อมูลที่ได้รับจากบุคคลภายนอกหรือหน่วยงานอื่น ปส. ต้องจัดให้มีหลักฐาน แหล่งที่มา หรือการอ้างอิงที่ชัดเจน เพื่อให้สามารถตรวจสอบได้ และสร้างความเชื่อมั่นในความถูกต้องและความน่าเชื่อถือของข้อมูล

9) กรณีที่เป็นข้อมูลส่วนบุคคล ผู้สร้างหรือผู้รวบรวมข้อมูลต้องปฏิบัติตามนโยบายการคุ้มครองข้อมูลส่วนบุคคลของ ปส. และกฎหมายที่เกี่ยวข้อง

10) การเก็บรวบรวมข้อมูลส่วนบุคคลต้องเป็นไปตามหลักการที่ชอบด้วยกฎหมาย โดยมีวัตถุประสงค์ที่ชัดเจน และได้รับความยินยอมจากเจ้าของข้อมูล

11) กำหนดให้มีการตรวจสอบความถูกต้องของรูปแบบข้อมูลในระดับขั้นต่ำ (Validation) ตั้งแต่ต้นทาง เช่น รูปแบบวันที่ รหัสข้อมูล หน่วยวัด และการจัดการค่าที่ขาดหาย (Missing Data) เพื่อป้องกันและลดความเสี่ยงด้านคุณภาพข้อมูล

ตารางที่ 1 ผู้มีส่วนได้ส่วนเสียในการสร้างข้อมูล

กิจกรรม	ผู้มีส่วนได้ส่วนเสีย				
	ผู้สร้างข้อมูล	ทีมบริหารจัดการข้อมูล	เจ้าของข้อมูล	บริการข้อมูล	ผู้ดูแลระบบสารสนเทศ
กำหนดผู้มีสิทธิ์ในการสร้างข้อมูล และกำหนดหมวดหมู่และชั้นความลับ	I	I	R	C	S
กำหนดสิทธิ์ในการสร้างข้อมูลในระบบ ให้แก่ผู้สร้างข้อมูล	I	I	S	I	R
สร้างข้อมูลที่ไม่ขัดต่อกฎหมาย และจากแหล่งข้อมูลที่เชื่อถือได้เท่านั้น	R	I	C	C	S
จัดทำคำอธิบายชุดข้อมูลดิจิทัล	S	S	R	R	S
ประเมินคุณค่าของชุดข้อมูลดิจิทัล	I	I	R	R	I
ตรวจสอบความถูกต้องของข้อมูล	I	I	R	R	I

หมายเหตุ

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

หมวด 2 การจัดเก็บข้อมูล

วัตถุประสงค์

กำหนดแนวปฏิบัติสำหรับผู้ที่เกี่ยวข้องในการจัดเก็บข้อมูล ให้มีคุณภาพ เข้าถึงและใช้งานได้อย่างมั่นคงปลอดภัย

ผู้รับผิดชอบงาน

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

อ้างอิง

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

ข้อปฏิบัติ

- 1) เจ้าของข้อมูลต้องกำหนดระยะเวลาในการจัดเก็บข้อมูลของแต่ละประเภทข้อมูลให้ชัดเจน
- 2) ทีมบริหารจัดการข้อมูลและผู้ดูแลระบบสารสนเทศ โดยดำเนินการ ดังนี้
 - 2.1) ดำเนินการคัดแยกและย้ายข้อมูลที่มีอายุการจัดเก็บครบกำหนด ไปจัดเก็บเป็นข้อมูลถาวร (Archive) ตามหลักเกณฑ์ที่กำหนด
 - 2.2) พิจารณาและกำหนดวิธีการจัดเก็บข้อมูลให้เหมาะสมกับประเภท ลักษณะ และระดับความสำคัญของข้อมูล พร้อมทั้งดำเนินการจัดเก็บข้อมูลให้เป็นไปตามมาตรฐานที่กำหนด
 - 2.3) ดำเนินการทำลายข้อมูลเมื่อพ้นระยะเวลาการจัดเก็บ ตามหลักเกณฑ์ วิธีการ และมาตรการด้านความมั่นคงปลอดภัยที่กำหนด

3) กำหนดให้การจัดเก็บชุดข้อมูลจะต้องมีคำอธิบายชุดข้อมูล (Metadata) ดิจิทัลหรือเมทาดาทาที่ครบถ้วนและเป็นปัจจุบัน หากข้อมูลยังไม่มีหรือไม่ครบถ้วน บริการข้อมูลด้านธุรกิจและคุณภาพข้อมูลจะต้องแจ้งผู้รับผิดชอบ ได้แก่ เจ้าของข้อมูล โดยทีมบริหารจัดการข้อมูลร่วมกันจัดทำและปรับปรุงให้เป็นปัจจุบัน

4) ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับข้อมูล ได้แก่ เจ้าของข้อมูล ผู้สร้างข้อมูล ผู้ใช้ข้อมูล และทีมบริหารจัดการข้อมูล ต้องดำเนินการตรวจสอบความถูกต้อง ครบถ้วน และความสอดคล้องของข้อมูลก่อนการจัดเก็บและก่อนการนำข้อมูลไปใช้งานทุกครั้ง รวมทั้งต้องจัดเก็บข้อมูลให้เป็นไปตามการจำแนกหมวดหมู่ และระดับชั้นความลับของข้อมูลที่ ปส. กำหนด โดยต้องมีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เช่น การเข้ารหัสข้อมูล (Encryption) การกำหนดสิทธิ์การเข้าถึง (Access Control) เพื่อป้องกันการเข้าถึง การใช้ หรือการแก้ไขข้อมูลโดยไม่ได้รับอนุญาต ทั้งนี้ การดำเนินการดังกล่าวต้องเป็นไปตามแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศของ ปส. และในกรณีที่มีการนำข้อมูลลับไปใช้งาน ต้องปฏิบัติตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 และที่แก้ไขเพิ่มเติมอย่างเคร่งครัด โดยห้ามมิให้มีการเปิดเผย แบ่งปัน หรือส่งต่อข้อมูลลับแก่บุคคลที่ไม่มีสิทธิ์หรือไม่ได้รับอนุญาต และต้องใช้ความระมัดระวังในการใช้งาน การกระจาย หรือการแจกจ่ายข้อมูลลับ โดยจำกัดเฉพาะผู้ที่ได้รับสิทธิ์หรือได้รับอนุญาตเท่านั้น

4.1) ในกรณีที่ในตารางฐานข้อมูลเดียวกันมีฟิลด์ข้อมูลที่มีชั้นความลับและไม่มีชั้นความลับอยู่ร่วมกันให้ทำการเข้ารหัสข้อมูลเฉพาะฟิลด์ข้อมูลที่มีชั้นความลับเท่านั้น

4.2) ในกรณีข้อมูลที่จัดเก็บในรูปแบบเอกสารให้มีการจัดเก็บ ดังนี้

- เก็บในสถานที่เหมาะสม สามารถปิดล็อกได้เมื่อไม่ใช้งาน
- เก็บแยกออกจากอุปกรณ์ประมวลผลต่าง ๆ เช่น เครื่องพิมพ์ เครื่องถ่ายเอกสาร เป็นต้น โดยทันที เพื่อเป็นการป้องกันไม่ให้ผู้ไม่มีสิทธิ์ในการเข้าถึงข้อมูล เข้าถึงข้อมูลได้

ทั้งนี้ การจัดเก็บข้อมูลให้หมายความรวมถึงข้อมูลทั้งที่มีโครงสร้าง (Structured Data) และไม่มีโครงสร้าง (Unstructured Data) โดยมาตรการในการจัดเก็บข้อมูลอย่างน้อยต้องดำเนินการ ดังนี้

1) ต้องจัดเก็บข้อมูลตามหมวดหมู่ที่กำหนด โดย ปส. ได้กำหนดหมวดหมู่ข้อมูลไว้ ดังนี้

ลำดับ	หมวดหมู่ข้อมูล	ความหมาย
1	ข้อมูลสาธารณะ (Public Data)	ข้อมูลที่สามารถเปิดเผยได้และสามารถนำไปใช้ได้โดยอิสระ เช่น ข้อมูลข่าวสารทั่วไป ข้อมูลอิเล็กทรอนิกส์ หรือข้อมูลอื่นที่ไม่อยู่ภายใต้ข้อจำกัดทางกฎหมายหรือความลับ
2	ข้อมูลใช้ภายใน (Internal Use Only)	ข้อมูลสำหรับการดำเนินงานภายในหน่วยงาน ซึ่งยังไม่อนุญาตให้นำไปเผยแพร่ภายนอก เว้นแต่จะได้รับอนุญาตจากเจ้าของข้อมูล เช่น ร่างนโยบาย ร่างมาตรฐาน ขั้นตอนการปฏิบัติงาน ประกาศ หรือบันทึกภายใน ที่อยู่ระหว่างการพิจารณาอนุมัติ
3	ข้อมูลส่วนบุคคล (Personal Data)	ข้อมูลเกี่ยวกับบุคคลซึ่งสามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม ทั้งนี้ การดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลต้องเป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมตามที่กฎหมายกำหนด)
4	ข้อมูลความลับทางราชการ (Classified Information)	ข้อมูลข่าวสารของราชการตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ที่มีคำสั่งไม่ให้เปิดเผย และอยู่ในความครอบครองหรือควบคุมดูแลของหน่วยงานของรัฐ โดยกำหนดระดับชั้นความลับเป็นชั้นลับ ชั้นลับมาก หรือชั้นลับที่สุด
5	ข้อมูลความมั่นคง (National Security Information)	ข้อมูลที่เกี่ยวข้องกับความมั่นคงแห่งชาติ หรืออาจกระทบต่อ เอกราช อธิปไตย บูรณภาพแห่งอาณาเขต ศาสนา สถาบันพระมหากษัตริย์ ความปลอดภัยของประชาชน หรือผลประโยชน์ของประเทศ รวมถึงข้อมูลที่เกี่ยวข้องกับมิติความมั่นคงด้านเศรษฐกิจ อาหาร สุขภาพ สิ่งแวดล้อม สังคม การเมือง การต่างประเทศ และสิทธิมนุษยชน ทั้งนี้ ให้เป็นไปตามนโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ

2) การจัดเก็บข้อมูลตามระดับชั้นความลับของข้อมูล โดย ปส. ได้กำหนดระดับชั้นความลับของข้อมูลไว้ 3 ระดับ ตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม ดังนี้

ระดับชั้นข้อมูล	ความหมาย
ลับ	ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือบางส่วน อาจก่อให้เกิดความเสียหายต่อประโยชน์ของรัฐ
ลับมาก	ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือบางส่วน อาจก่อให้เกิดความเสียหายอย่างร้ายแรงต่อประโยชน์ของรัฐ
ลับที่สุด	ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือบางส่วน อาจก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุดต่อประโยชน์ของรัฐ

5) กำหนดให้มีมาตรการสำรองข้อมูล (Backup) และวิธีปฏิบัติการกู้คืนข้อมูลที่จัดเก็บถาวร (Archive) สำหรับข้อมูลที่มีความสำคัญมากต่อการดำเนินงานของหน่วยงาน เพื่อสอบทานความถูกต้อง ครบถ้วน ความพร้อมใช้งาน คุณภาพข้อมูล

6) ให้มีการทดสอบการกู้คืนข้อมูล (Restore Test) สำหรับข้อมูลสำคัญอย่างน้อยปีละ 1 ครั้ง และจัดเก็บรายงานผลการทดสอบเป็นหลักฐาน

7) ในการจัดเก็บข้อมูลส่วนบุคคลให้เก็บรวบรวมได้เท่าที่จำเป็น ภายใต้อำนาจหน้าที่และวัตถุประสงค์อันชอบด้วยกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล และ**ไม่เก็บรวบรวมข้อมูลส่วนบุคคล** ดังต่อไปนี้ เว้นแต่ได้รับการยินยอมจากเจ้าของข้อมูลส่วนบุคคล หรือพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือกฎหมายอื่นบัญญัติให้กระทำได้

- 7.1) เชื้อชาติ
- 7.2) เผ่าพันธุ์
- 7.3) ความคิดเห็นทางการเมือง
- 7.4) ความเชื่อในลัทธิ ศาสนาหรือปรัชญา
- 7.5) พฤติกรรมทางเพศ
- 7.6) ประวัติอาชญากรรม
- 7.7) ข้อมูลสุขภาพ ความพิการ หรือข้อมูลสุขภาพจิต
- 7.8) ข้อมูลสหภาพแรงงาน
- 7.9) ข้อมูลพันธุกรรม
- 7.10) ข้อมูลชีวภาพ
- 7.11) ข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลในทำนองเดียวกันตามที่สำนักงานกำหนด

8) กำหนดให้มีการยกเลิกการจัดเก็บข้อมูลส่วนบุคคล กรณีเจ้าของข้อมูลส่วนบุคคลถอนความยินยอมตามที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลกำหนด

9) ในกรณีที่มีการประชุมหรือธุรกรรมออนไลน์ กำหนดให้มีการจัดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่า 90 วัน นับแต่วันที่ข้อมูลเข้าสู่ระบบคอมพิวเตอร์ โดยจัดเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการนับแต่เริ่มใช้บริการให้สอดคล้องตามกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์และในการจัดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ให้สอดคล้องตามกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ ผู้ให้บริการจะต้องใช้วิธีการที่มั่นคงปลอดภัยอย่างน้อย ดังนี้

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

10) กำหนดให้มีมาตรการรักษาความปลอดภัยในการจัดเก็บข้อมูล รวมทั้งกรณีที่มีการเคลื่อนย้ายอุปกรณ์ที่จัดเก็บข้อมูล เพื่อป้องกันมิให้มีการเข้าถึงโดยมิได้รับอนุญาต หรือลักลอบนำข้อมูลไปใช้ที่ก่อให้เกิดความเสียหายต่อหน่วยงาน

11) กำหนดมาตรการรักษาความปลอดภัยของข้อมูลที่จัดเก็บถาวร เพื่อป้องกันข้อมูลไม่ให้มีการลบปรับปรุง แก้ไขได้ รวมทั้งป้องกันมิให้ข้อมูลที่จัดเก็บถาวรรั่วไหลไปยังบุคคลที่ไม่ได้รับอนุญาต

12) กำหนดให้มีมาตรการรักษาความปลอดภัยของการถ่ายโอนข้อมูลกับหน่วยงานภายนอก ที่ผ่านช่องทางการสื่อสารทุกชนิด โดยต้องสอดคล้องตามนโยบายความมั่นคงปลอดภัยสารสนเทศ

13) ห้ามมิให้จัดเก็บข้อมูลส่วนตัวหรือข้อมูลที่ไม่เกี่ยวข้องกับการดำเนินงานของสำนักงานบนเครื่องแม่ข่ายที่สำนักงานจัดสรรไว้

14) กำหนดให้มีการทบทวนเกี่ยวกับช่วงระยะเวลาการจัดเก็บข้อมูล มาตรการ และวิธีปฏิบัติที่เกี่ยวข้องกับการจัดเก็บข้อมูลถาวร อย่างน้อยปีละ 1 ครั้ง

ตารางที่ 2 ผู้มีส่วนได้ส่วนเสียในการจัดเก็บข้อมูล

กิจกรรม	ผู้มีส่วนได้ส่วนเสีย					
	เจ้าของข้อมูล	ผู้ดูแลระบบสารสนเทศ	ผู้สร้างข้อมูล	ผู้ใช้ข้อมูล	บริการข้อมูล	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

หมายเหตุ

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

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) เจ้าของข้อมูลจะต้องกำหนดผู้มีสิทธิ์เข้าถึงเพื่อประมวลผลและใช้ข้อมูลตามชั้นความลับ ดังนี้
 - 1.1) ข้อมูลเปิดเผยได้ ไม่กำหนดสิทธิ์การเข้าถึงเพื่อประมวลผลและใช้งานข้อมูล
 - 1.2) ข้อมูลที่มีชั้นความลับ กำหนดให้ผู้ใช้งานที่ได้รับสิทธิ์เข้าถึงและใช้ข้อมูลตามอำนาจหน้าที่เท่านั้น
 - 1.3) ข้อมูลใช้ภายใน กำหนดให้บุคลากรของหน่วยงานเท่านั้นที่มีสิทธิ์เข้าถึงเพื่อประมวลผลและใช้งานข้อมูลได้
- 2) ผู้ใช้ข้อมูลที่ไม่ใช่เจ้าของข้อมูล ต้องขออนุญาตใช้ข้อมูลจากเจ้าของข้อมูลตามกระบวนการที่กำหนด และปฏิบัติตามข้อกำหนดของหน่วยงานเจ้าของข้อมูลอย่างเคร่งครัด โดยการเข้าถึง การประมวลผล และการใช้ข้อมูลต้องได้รับอนุญาตก่อนดำเนินการ รวมทั้งต้องมีการบันทึกการเข้าถึง การประมวลผล และการใช้ข้อมูล (Audit Log) เพื่อให้สามารถตรวจสอบย้อนหลังได้ ทั้งนี้ การนำข้อมูลที่มีชั้นความลับหรือข้อมูลส่วนบุคคลไปประมวลผลและใช้ข้อมูล ต้องเป็นไปตามวัตถุประสงค์และเงื่อนไขที่ได้รับความยินยอมหรือที่กฎหมายกำหนดไว้เท่านั้น
- 3) ผู้ดูแลระบบสารสนเทศจะต้องกำหนดสิทธิ์ในการเข้าถึงข้อมูลในระบบเพื่อประมวลผลและใช้ข้อมูลของผู้ใช้งานตามที่เจ้าของข้อมูลกำหนด
- 4) เจ้าของข้อมูลจะต้องทบทวนสิทธิ์การเข้าถึงเพื่อประมวลผลและใช้ข้อมูลของผู้ใช้งานอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ เช่น การลาออก เปลี่ยนตำแหน่ง โอนย้าย สิ้นสุดการจ้าง การปรับโครงสร้าง หรือเมื่อมีการปรับปรุงระบบสารสนเทศ

5) ผู้ที่มีสิทธิ์เข้าใช้งานข้อมูลที่มีชั้นความลับตามที่กำหนดโดยเจ้าของข้อมูลจะต้องใช้ข้อมูลอย่างระมัดระวัง โดยคำนึงถึงความปลอดภัยและต้องไม่ใช้งานข้อมูลที่มีชั้นความลับในพื้นที่สาธารณะ

6) ผู้ใช้ข้อมูลต้องประมวลผลและใช้ข้อมูล โดยเฉพาะข้อมูลส่วนบุคคล เท่าที่จำเป็นภายใต้อำนาจหน้าที่และวัตถุประสงค์ที่ชอบด้วยกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล หรือเป็นไปตามคำสั่งของ ปส. ทั้งนี้ คำสั่งดังกล่าวต้องไม่ขัดต่อกฎหมาย โดยผู้ใช้ข้อมูลต้องรับผิดชอบต่อการประมวลผลและการใช้ข้อมูลให้เป็นไปตามกฎหมายและข้อกำหนดที่เกี่ยวข้อง

7) หน่วยงานต้องยกเลิกการประมวลผลข้อมูลหรือการใช้ข้อมูลส่วนบุคคล กรณีที่เจ้าของข้อมูลส่วนบุคคลถอนความยินยอมตามที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลกำหนด

8) ผู้ใช้ข้อมูลจะต้องไม่ใช้ข้อมูลในเครือข่ายของหน่วยงานเพื่อประโยชน์ในเชิงธุรกิจเป็นการส่วนตัว หรือเพื่อเข้าสู่เว็บไซต์ที่ไม่เหมาะสมหรือใช้ข้อมูลอันก่อให้เกิดความเสียหายต่อ ปส.

ตารางที่ 3 ผู้มีส่วนได้ส่วนเสียในการประมวลผลข้อมูลและการใช้ข้อมูล

กิจกรรม	ผู้มีส่วนได้ส่วนเสีย		
	เจ้าของข้อมูล	ผู้ใช้ข้อมูล	ผู้ดูแลระบบสารสนเทศ
กำหนดสิทธิ์ในการประมวลผลและใช้งานข้อมูลตามชั้นความลับ	R	I	I
กำหนดสิทธิ์ในการประมวลผลและเข้าใช้งานข้อมูลในระบบ	C	I	R
ไม่ใช้ข้อมูลในเครือข่ายของหน่วยงานเพื่อประโยชน์ในเชิงธุรกิจเป็นการส่วนตัว	C	R	S
ประมวลผลข้อมูลหรือใช้ข้อมูลส่วนบุคคลเท่าที่จำเป็น	C	R	S
ยกเลิกการประมวลผลข้อมูลหรือการใช้ข้อมูลส่วนบุคคล กรณีที่เจ้าของข้อมูลส่วนบุคคลถอนความยินยอม	C	R	S

หมายเหตุ

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

หมวด 4 การเปิดเผยข้อมูล

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) เจ้าของข้อมูลหรือบริกรข้อมูล คัดเลือกและจัดเตรียมชุดข้อมูลที่จะเผยแพร่ โดยดำเนินการ ดังนี้
 - 2.1) พิจารณาคัดเลือกข้อมูลที่สามารถเปิดเผยได้ โดยต้องเป็นข้อมูลสาธารณะที่ไม่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ นโยบาย และข้อกำหนดด้านความมั่นคงปลอดภัยหรือการคุ้มครองข้อมูลส่วนบุคคล
 - 2.2) กำหนดหมวดหมู่ ประเภทข้อมูล ระดับการเปิดเผย และช่องทางการเผยแพร่ข้อมูลให้เหมาะสม เช่น เว็บไซต์ของ ปส. หรือระบบข้อมูลเปิดของหน่วยงาน
 - 2.3) จัดทำคำอธิบายชุดข้อมูล (Metadata) ให้ครบถ้วนและเพียงพอต่อการทำความเข้าใจและนำข้อมูลไปใช้ โดยอย่างน้อยต้องประกอบด้วย ชื่อชุดข้อมูล คำอธิบายข้อมูล คำสำคัญ วันที่ปรับปรุง

ข้อมูลล่าสุด ชื่อหน่วยงานเจ้าของข้อมูล และรายละเอียดฟิลด์ข้อมูล ทั้งนี้ ต้องตรวจสอบความครบถ้วน ถูกต้อง และความสอดคล้องของฟิลด์ข้อมูลให้ตรงตามวัตถุประสงค์และความต้องการของผู้ใช้ข้อมูล

2.4) จัดรูปแบบข้อมูลให้อยู่ในรูปแบบมาตรฐานที่เครื่องสามารถประมวลผลได้ และกำหนดรูปแบบชุดข้อมูลให้อยู่ภายใต้มาตรฐานเดียวกัน เพื่อให้สามารถสืบค้น เชื่อมโยง และใช้งานข้อมูลได้อย่างมีประสิทธิภาพ

2.5) ข้อมูลที่เผยแพร่ต้องมาจากแหล่งข้อมูลต้นทางโดยตรง มีความถูกต้อง ครบถ้วน และเหมาะสมต่อการใช้งาน โดยหลีกเลี่ยงการปรับแต่งข้อมูลที่อาจส่งผลกระทบต่อความน่าเชื่อถือของข้อมูล

2.6) ข้อมูลที่เผยแพร่ต้องระบุวันและเวลาปรับปรุงข้อมูลล่าสุด (Timestamp) เพื่อให้ผู้ใช้งานสามารถตรวจสอบความเป็นปัจจุบันของข้อมูลได้

3) การจัดเตรียมข้อมูลให้อยู่ในรูปแบบที่เหมาะสมต่อการใช้งาน ให้ดำเนินการ ดังนี้

3.1) ความพร้อมของข้อมูลในการส่งต่อหรือเปิดเผย

3.1.1) ต้องมีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลที่เหมาะสม เพื่อป้องกันการสูญหาย การเข้าถึง การใช้ การเปลี่ยนแปลง แก้ไข หรือการเปิดเผยข้อมูลโดยมิชอบ

3.1.2) กรณีมีการเปิดเผยหรือส่งต่อข้อมูลส่วนบุคคลให้แก่บุคคลหรือหน่วยงานอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล ต้องมีมาตรการป้องกันมิให้มีการนำข้อมูลไปใช้หรือเปิดเผยโดยมิชอบ

3.1.3) ต้องมีระบบหรือกลไกในการลบ ทำลาย หรือทำให้ข้อมูลส่วนบุคคลไม่สามารถระบุตัวบุคคลได้ เมื่อพ้นระยะเวลาการเก็บรักษา หรือเมื่อข้อมูลไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวม หรือเมื่อมีคำขอจากเจ้าของข้อมูลตามที่กฎหมายกำหนด

3.2) การเชื่อมโยงข้อมูล ต้องจัดให้มีการเชื่อมโยงข้อมูลที่จัดเก็บไว้อย่างเป็นระบบ เพื่อให้สามารถเข้าถึง ตรวจสอบ หรือเปิดเผยข้อมูลแก่ผู้ที่เกี่ยวข้องได้อย่างเหมาะสมและมีประสิทธิภาพ

4) กำหนดให้เงื่อนไขและข้อกำหนดของข้อมูลที่นำมาเปิดเผยภายในเครือข่ายของหน่วยงาน ข้อมูลที่เผยแพร่ต้องไม่ขัดต่อกฎหมายว่าด้วยทรัพย์สินทางปัญญา เว้นแต่การเปิดเผยข้อมูลจะเป็นไปตามอำนาจที่กฎหมายรับรอง

5) สนับสนุนการจัดทำบัญชีข้อมูลหน่วยงานและการลงทะเบียนบัญชีข้อมูลภาครัฐ โดยบริหารจัดการข้อมูลสำคัญ จัดทำบัญชีข้อมูลของหน่วยงาน และทำการลงทะเบียนบัญชีข้อมูลของหน่วยงาน และชุดข้อมูลสำคัญ เข้าสู่ระบบบัญชีข้อมูลภาครัฐ (Government Data Catalog หรือ GD Catalog) เพื่อการเปิดเผยข้อมูลภาครัฐที่เป็นระบบ และมีเอกภาพ สามารถสืบค้นชุดข้อมูล คำอธิบายชุดข้อมูล รวมไปถึงแหล่งต้นทางของชุดข้อมูลภาครัฐที่สำคัญ สนับสนุนการใช้ประโยชน์ข้อมูลภาครัฐร่วมกัน

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

6.1) กำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัยในการเปิดเผยข้อมูลที่กำหนดลำดับชั้นข้อมูลตั้งแต่กลับขึ้นไป อย่างเพียงพอและมีประสิทธิภาพ

6.2) มีการตรวจสอบข้อมูลที่เผยแพร่จากหน่วยงานทั้งภายในและภายนอกหน่วยงาน เพื่อให้มั่นใจว่าข้อมูลมีความถูกต้อง ครบถ้วน เหมาะสม และเป็นปัจจุบันก่อนการเผยแพร่

6.3) การเผยแพร่ข้อมูล ต้องมีการตรวจสอบรูปแบบข้อมูลที่เผยแพร่ให้สอดคล้องกับมาตรฐานที่หน่วยงานกำหนด

6.4) หากการเปิดเผยนั้นเป็นการเปิดเผยบนช่องทางที่ถูกละเมิดโดยหน่วยงานอื่นที่ให้ปฏิบัติตามเอกสาร คู่มือ การนำข้อมูลขึ้นเผยแพร่ของหน่วยงานนั้น

6.5) หากการเปิดเผยข้อมูลไม่ครบถ้วน หรือไม่ปัจจุบัน ให้แจ้งเจ้าของข้อมูล บริกรข้อมูล ด้านธุรกิจและคุณภาพ และทีมบริหารจัดการข้อมูลทำการจัดทำ/ปรับปรุงให้เป็นปัจจุบัน

6.6) ต้องจัดให้มีการบันทึกประวัติการเปิดเผยหรือการเข้าถึงข้อมูล (Log) เพื่อรองรับการตรวจสอบย้อนหลัง และให้เป็นไปตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์และกฎหมายที่เกี่ยวข้อง

7) การเปิดเผยหรือให้เข้าถึงข้อมูลส่วนบุคคลต้องดำเนินการตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และกฎหมายที่เกี่ยวข้อง โดยกรณีที่เป็นข้อมูลส่วนบุคคลรายบุคคล หน่วยงานที่ขอใช้ข้อมูลต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลก่อน เว้นแต่เป็นกรณีที่กฎหมายกำหนดให้สามารถดำเนินการได้ ทั้งนี้ หน่วยงานผู้ถือครองข้อมูลต้องแจ้งผลการให้ความยินยอมแก่หน่วยงานที่เกี่ยวข้อง และอาจกำหนดขอบเขตการเข้าถึงข้อมูลเฉพาะบางส่วนตามวัตถุประสงค์ที่ได้รับความยินยอม พร้อมทั้งต้องมีมาตรการปกปิดหรือทำให้ไม่สามารถระบุตัวบุคคลได้ เพื่อป้องกันการเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ

8) เจ้าของข้อมูลห้ามเปิดเผยข้อมูลความมั่นคง ข้อมูลลับทางราชการ หรือข้อมูลอื่นใดที่อาจก่อให้เกิดความเสียหายต่อหน่วยงานหรือกระทบต่อความมั่นคงปลอดภัยของสำนักงาน รวมถึงห้ามเปิดเผยข้อมูลที่เป็นการกระทำความผิดตามกฎหมาย นโยบาย และแนวปฏิบัติที่เกี่ยวข้อง

9) กำหนดให้เจ้าของข้อมูลคัดเลือกข้อมูลที่จะเปิดเผยในรูปแบบข้อมูลเปิดจากลำดับชั้นความสำคัญของชุดข้อมูลที่มีคุณค่าสูง (High Value Dataset)

10) กำหนดให้เจ้าของข้อมูลต้องกำหนดรอบระยะเวลาในการตรวจสอบและปรับปรุงข้อมูลที่เปิดเผยเพื่อให้ข้อมูลถูกต้อง และเป็นปัจจุบัน

ตารางที่ 4 ผู้มีส่วนได้ส่วนเสียในการเปิดเผยข้อมูล

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

หมายเหตุ

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

หมวด 5 กระบวนการจัดเก็บข้อมูลถาวร

วัตถุประสงค์

กำหนดแนวปฏิบัติการจัดเก็บข้อมูลถาวร ให้เป็นไปอย่างมีระบบ มีความมั่นคงปลอดภัย สามารถตรวจสอบและเรียกใช้ข้อมูลได้อย่างมีประสิทธิภาพ

ผู้รับผิดชอบงาน

- 1) เจ้าของข้อมูล (Data Owners)
- 2) ทีมบริหารจัดการข้อมูล (Data Management Team)
- 3) ผู้ดูแลระบบสารสนเทศ (Systems Administrators)
- 4) บริกรข้อมูล (Data Stewards)

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) พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540
- 6) ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม

ข้อปฏิบัติ

- 1) เจ้าของข้อมูลต้องกำหนดหลักเกณฑ์ ระยะเวลา วิธีการ และระบบที่ใช้ในการจัดเก็บข้อมูลถาวร ให้เหมาะสมกับประเภท ลักษณะ ความสำคัญ และระดับชั้นความลับของข้อมูล รวมทั้งสอดคล้องกับกฎหมาย ระเบียบ และความจำเป็นในการใช้งานของหน่วยงาน
- 2) ทีมบริหารจัดการข้อมูลร่วมกับผู้ดูแลระบบสารสนเทศ ต้องดำเนินการคัดแยก ย้าย และจัดเก็บข้อมูลที่พ้นระยะเวลาการใช้งานปกติไปจัดเก็บเป็นข้อมูลถาวร (Archive) ตามหลักเกณฑ์และระยะเวลาที่กำหนด โดยประสานความร่วมมือกับหน่วยงานที่เกี่ยวข้องอย่างเหมาะสม
- 3) การจัดเก็บข้อมูลถาวรต้องมีคำอธิบายชุดข้อมูล (Metadata) ที่ครบถ้วน ถูกต้อง และเป็นปัจจุบัน เพื่อรองรับการสืบค้น การตรวจสอบย้อนหลัง และการนำข้อมูลกลับมาใช้งานได้อย่างมีประสิทธิภาพ

4) ศึกษาและวิเคราะห์ลักษณะของข้อมูลก่อนดำเนินการจัดเก็บข้อมูลถาวร โดยเลือกใช้เครื่องมือเทคโนโลยี วิธีการ และกระบวนการที่เป็นมาตรฐาน เพื่อให้ข้อมูลมีความคงทน มั่นคงปลอดภัย และสามารถเข้าถึงหรือเรียกใช้งานได้อย่างต่อเนื่องในระยะยาว

5) กำหนดและใช้มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลถาวรอย่างเหมาะสม เช่น การเข้ารหัสข้อมูล (Encryption) การกำหนดสิทธิ์การเข้าถึงข้อมูล (Access Control) การป้องกันการแก้ไขข้อมูลโดยไม่ได้รับอนุญาต และการจัดเก็บบันทึกการใช้งาน (Log) เพื่อรองรับการตรวจสอบย้อนหลัง

6) กำหนดสิทธิ์การเข้าถึงและการใช้งานข้อมูลถาวรเฉพาะผู้ที่ได้รับอนุญาต และสอดคล้องกับระดับชั้นความลับของข้อมูล รวมทั้งต้องมีการทบทวนสิทธิ์การเข้าถึงอย่างเหมาะสมและสม่ำเสมอ

7) ต้องจัดให้มีระบบสำรองข้อมูล (Backup) และแนวทางการกู้คืนข้อมูลถาวร เพื่อรองรับกรณีเกิดเหตุฉุกเฉินหรือเหตุการณ์ที่อาจส่งผลกระทบต่อความพร้อมใช้งานของข้อมูล

8) ต้องมีการทดสอบการกู้คืนข้อมูล (Restore Test) สำหรับข้อมูลถาวรที่มีความสำคัญอย่างน้อยปีละ 1 ครั้ง และจัดเก็บผลการทดสอบไว้เป็นหลักฐานเพื่อใช้ในการตรวจสอบและประเมินประสิทธิภาพของกระบวนการกู้คืนข้อมูล

9) หน่วยงานที่เกี่ยวข้องต้องส่งเสริมและสร้างความรู้ความเข้าใจด้านการจัดเก็บข้อมูลถาวร การรักษาความมั่นคงปลอดภัยของข้อมูล และแนวปฏิบัติที่เกี่ยวข้องแก่ผู้ปฏิบัติงานและผู้มีส่วนเกี่ยวข้องอย่างสม่ำเสมอ เพื่อให้สามารถปฏิบัติงานได้อย่างถูกต้องและมีประสิทธิภาพ

10) ต้องมีการทบทวนความเหมาะสมของข้อมูลถาวร ระยะเวลาการจัดเก็บ มาตรการรักษาความมั่นคงปลอดภัย วิธีปฏิบัติ และระบบที่เกี่ยวข้องอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญด้านกฎหมาย เทคโนโลยี ระบบสารสนเทศ หรือบริบทการดำเนินงานของหน่วยงาน

ตารางที่ 5 ผู้มีส่วนได้ส่วนเสียในการจัดเก็บข้อมูลถาวร

กิจกรรม	ผู้มีส่วนได้ส่วนเสีย			
	เจ้าของข้อมูล	ผู้ดูแลระบบสารสนเทศ	บริการข้อมูล	ทีมบริหารจัดการข้อมูล
กำหนดหลักเกณฑ์ ระยะเวลา และระดับชั้นความลับในการจัดเก็บข้อมูลถาวร	R	S	S	S
คัดแยก ย้าย และจัดเก็บข้อมูลเข้าสู่ระบบจัดเก็บข้อมูลถาวร	I	R	S	R
จัดทำและปรับปรุงคำอธิบายชุดข้อมูลดิจิทัล (Metadata) ให้เป็นปัจจุบัน	R	S	R	R
กำหนดมาตรฐาน วิธีการ และมาตรการรักษาความมั่นคงปลอดภัยในการจัดเก็บข้อมูลถาวร	S	R	S	R
กำหนดสิทธิ์ ควบคุมการเข้าถึง และจัดเก็บบันทึกการใช้งานข้อมูลถาวร (Log)	R	R	I	S
สำรองข้อมูล ทดสอบการกู้คืนข้อมูล และจัดทำแนวทางการกู้คืนข้อมูลถาวร	I	R	I	R
ทบทวนความเหมาะสมของข้อมูลถาวร ระยะเวลาการจัดเก็บ และสื่อสารแนวปฏิบัติที่เกี่ยวข้อง	R	S	S	R

หมายเหตุ

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

หมวด 6 การทำลายข้อมูล

วัตถุประสงค์

กำหนดแนวปฏิบัติการทำลายข้อมูล และการพิจารณาอนุมัติทำลายโดยเจ้าของข้อมูลเพื่อเป็นการรักษาความมั่นคงปลอดภัยของข้อมูล

ผู้รับผิดชอบงาน

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

อ้างอิง

- 1) ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553
- 2) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ข้อปฏิบัติ

- 1) เจ้าของข้อมูลกำหนดขั้นตอน วิธีการ และแนวปฏิบัติในการทำลายข้อมูลอย่างชัดเจน โดยประสานความร่วมมือกับหน่วยงานที่เกี่ยวข้อง และให้สอดคล้องกับกฎหมาย ระเบียบ และแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศของ ปส.
- 2) เจ้าของข้อมูลเป็นผู้กำหนดสิทธิ์ของผู้มีอำนาจในการทำลายข้อมูล และต้องมีการทบทวนสิทธิ์ดังกล่าวอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ เช่น การลาออก เปลี่ยนตำแหน่ง โอนย้าย สิ้นสุดการจ้าง การปรับโครงสร้าง หรือเมื่อมีการปรับปรุงระบบสารสนเทศ เป็นต้น ทั้งนี้ ผู้ดูแลระบบสารสนเทศต้องกำหนดสิทธิ์ในระบบให้สอดคล้องตามที่กำหนด และจัดให้มีการบันทึกประวัติการดำเนินการทุกครั้ง
- 3) ผู้ดูแลระบบสารสนเทศจะต้องกำหนดสิทธิ์ในการทำลายข้อมูลในระบบให้แก่ผู้ทำลายข้อมูลตามที่เจ้าของข้อมูลกำหนด
- 4) ทีมบริหารจัดการข้อมูลและผู้ดูแลระบบสารสนเทศต้องดำเนินการทำลายข้อมูลเมื่อพ้นระยะเวลาการจัดเก็บ ตามหลักเกณฑ์ วิธีการ และมาตรการด้านความมั่นคงปลอดภัยที่กำหนด โดยผู้ปฏิบัติต้องดำเนินการให้เป็นไปตามแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศของ ปส. อย่างเคร่งครัด
- 5) กำหนดให้มีการจัดเก็บรายละเอียดและหลักฐานการทำลายข้อมูลไว้ในทะเบียนควบคุม รวมถึงบันทึกการทำลายข้อมูล (Log) เพื่อให้สามารถตรวจสอบย้อนหลังได้ โดยเก็บรักษาไว้นานอย่างน้อย 1 ปี และให้เจ้าของข้อมูลจัดเก็บคำอธิบายชุดข้อมูล (Metadata) ของข้อมูลที่ถูกทำลายเพื่อใช้ในการอ้างอิง

6) การทำลายข้อมูลส่วนบุคคลต้องเป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 รวมถึงกรณีที่เจ้าของข้อมูลส่วนบุคคลร้องขอให้ลบหรือทำลายข้อมูล ต้องดำเนินการภายในขอบเขตและเงื่อนไขที่กฎหมายกำหนด

7) หน่วยงานที่เกี่ยวข้องต้องดำเนินการสร้างความรู้ ความเข้าใจ และสื่อสารแนวปฏิบัติในการทำลายข้อมูลแก่ผู้ปฏิบัติงานและผู้เกี่ยวข้องอย่างสม่ำเสมอ ผ่านการอบรม การประชุม การประชาสัมพันธ์ หรือช่องทางการสื่อสารที่เหมาะสม เพื่อให้เกิดความตระหนักและสามารถปฏิบัติตามแนวทางการทำลายข้อมูลได้อย่างถูกต้อง สอดคล้องกับกฎหมาย ระเบียบ และนโยบายที่เกี่ยวข้อง

ตารางที่ 6 ผู้มีส่วนได้ส่วนเสียในการทำลายข้อมูล

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

หมายเหตุ

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



ส่วนที่ 2

แนวปฏิบัติในการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน

แนวปฏิบัติในการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน

2.1 วัตถุประสงค์

เพื่อกำหนดแนวปฏิบัติ มาตรฐาน และมาตรการด้านเทคนิคในการเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัล ทั้งภายในสำนักงานปรมาณูเพื่อสันติ (ปส.) และระหว่างหน่วยงาน ให้เป็นไปอย่างถูกต้อง ครบถ้วน ปลอดภัย มีประสิทธิภาพ และสามารถนำข้อมูลไปใช้ประโยชน์ร่วมกันได้อย่างเหมาะสม ทั้งต่อภาครัฐ ภาคเอกชน และภาคประชาชน โดยการดำเนินการเชื่อมโยงและแลกเปลี่ยนข้อมูลต้องสอดคล้องกับกฎหมาย ระเบียบ หลักเกณฑ์ นโยบาย และมาตรฐานที่เกี่ยวข้อง รวมถึงข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศ และการคุ้มครองข้อมูลส่วนบุคคลของ ปส.

2.2 ข้อปฏิบัติ

1) กำหนดให้ผู้จัดการโครงการหรือหน่วยงานที่เกี่ยวข้องกำหนดวิธีปฏิบัติ มาตรฐานข้อมูล และมาตรฐานทางเทคนิคที่ใช้ในการเชื่อมโยงและแลกเปลี่ยนข้อมูลให้เป็นไปตามมาตรฐานสากล และมาตรฐานกลางภาครัฐ เช่น รูปแบบข้อมูลแบบเปิด (Open Format) มาตรฐานการรับส่งข้อมูล และมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อให้สามารถเชื่อมโยงและใช้งานข้อมูลร่วมกันได้อย่างมีประสิทธิภาพ ปลอดภัย และเป็นมาตรฐานเดียวกัน

2) การเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่าง ปส.กับหน่วยงานภายนอก ต้องได้รับอนุญาตตาม กระบวนการที่สำนักงานกำหนด และต้องมีการกำหนดแนวทางหรือข้อตกลงในการบริหารจัดการข้อมูลร่วมกัน อย่างชัดเจน เช่น บันทึกข้อตกลงความร่วมมือ (Memorandum of Understanding : MOU) สัญญารักษา ความลับ (Non-Disclosure Agreement : NDA) หรือข้อตกลงอื่นที่เกี่ยวข้องกับการเชื่อมโยง การแลกเปลี่ยน และการนำข้อมูลไปใช้

3) กำหนดให้ตรวจสอบคำอธิบายชุดข้อมูล (Metadata) และรายละเอียดข้อมูลก่อนดำเนินการ เชื่อมโยงหรือแลกเปลี่ยนข้อมูล โดยต้องตรวจสอบให้ข้อมูลมีความครบถ้วน ถูกต้อง เป็นปัจจุบัน และ สอดคล้องกับวัตถุประสงค์การใช้งาน รวมถึงตรวจสอบสิทธิในการเข้าถึงและระดับชั้นความลับของข้อมูล ให้เป็นไปตามกฎหมาย ระเบียบ และข้อกำหนดที่เกี่ยวข้อง

4) กรณีการเชื่อมโยงหรือแลกเปลี่ยนข้อมูลผ่านระบบอิเล็กทรอนิกส์อย่างต่อเนื่องหรือเป็นประจำ ต้องได้รับการอนุมัติตามกระบวนการที่สำนักงานกำหนด และให้มีการกำหนดชุดข้อมูล วิธีการเชื่อมโยง ผู้รับผิดชอบ และมาตรการรักษาความมั่นคงปลอดภัยอย่างชัดเจน

5) กรณีการเชื่อมโยงหรือแลกเปลี่ยนข้อมูลเป็นครั้งคราว หรือผ่านช่องทางอื่นที่มีในระบบเชื่อมโยงอัตโนมัติ ให้ดำเนินการตามขั้นตอนและสิทธิ์การอนุมัติที่กำหนด โดยกรณีที่มีการแลกเปลี่ยนข้อมูลผ่าน API หรือช่องทางอิเล็กทรอนิกส์ ต้องใช้มาตรการด้านความมั่นคงปลอดภัยที่เหมาะสม เช่น การเข้ารหัสข้อมูล การยืนยันตัวตน และการกำหนดสิทธิ์การเข้าถึงตามหลัก Least Privilege

6) การเชื่อมโยงและแลกเปลี่ยนข้อมูลต้องมีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล และข้อมูลส่วนบุคคลให้เป็นไปตามกฎหมาย ระเบียบ นโยบายความมั่นคงปลอดภัยสารสนเทศ และนโยบายการคุ้มครองข้อมูลส่วนบุคคลของ ปส. เพื่อป้องกันการเข้าถึง การใช้ การเปิดเผย การแก้ไข หรือการรั่วไหลของข้อมูลโดยมิชอบ

7) ทุกการเชื่อมโยงและแลกเปลี่ยนข้อมูลต้องจัดให้มีการบันทึกประวัติการเข้าถึง การรับส่ง และการใช้งานข้อมูล (Audit Trail หรือ Log) เพื่อรองรับการตรวจสอบย้อนหลัง รวมทั้งต้องมีการตรวจสอบและเฝ้าระวังความมั่นคงปลอดภัยของระบบและช่องทางเชื่อมโยงข้อมูลอย่างสม่ำเสมอ

8) กำหนดให้มีมาตรการป้องกันการสูญหายหรือการรั่วไหลของข้อมูล (Data Loss Prevention: DLP) รวมถึงมาตรการป้องกันการรับส่งข้อมูลที่ไม่สมบูรณ์ การส่งข้อมูลผิดพลาดทาง หรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

9) กรณีเป็นข้อมูลส่วนบุคคลหรือข้อมูลอ่อนไหว การเชื่อมโยงและแลกเปลี่ยนข้อมูลต้องดำเนินการภายใต้นโยบายการคุ้มครองข้อมูลส่วนบุคคลของสำนักงานปรมาณูเพื่อสันติ และในกรณีที่กฎหมายกำหนดให้ต้องได้รับความยินยอม ต้องดำเนินการให้เป็นไปตามเงื่อนไขและวัตถุประสงค์ที่ได้รับความยินยอมจากเจ้าของข้อมูล

10) กรณีที่มีการใช้ข้อมูลเพื่อการศึกษา วิจัย หรือประโยชน์สาธารณะตามที่กฎหมายกำหนด และมีการเปิดเผยข้อมูลส่วนบุคคล ให้ดำเนินการปกปิดตัวตนหรือทำข้อมูลให้อยู่ในรูปแบบที่ไม่สามารถระบุตัวบุคคลได้ (Anonymization) ก่อนการเชื่อมโยงหรือแลกเปลี่ยนข้อมูล

11) ห้ามมิให้มีการเชื่อมโยงหรือแลกเปลี่ยนข้อมูลที่เป็นการกระทำความผิดตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ หรือข้อมูลที่ขัดต่อกฎหมาย ระเบียบ นโยบาย และข้อกำหนดของสำนักงาน

12) กำหนดให้มีการทบทวนมาตรการ วิธีปฏิบัติ เทคโนโลยี และมาตรฐานที่เกี่ยวข้องกับการเชื่อมโยงและแลกเปลี่ยนข้อมูลอย่างสม่ำเสมอ เพื่อให้สอดคล้องกับกฎหมาย มาตรฐานด้านเทคโนโลยี และความเสี่ยด้านความมั่นคงปลอดภัยที่เปลี่ยนแปลงไป



ส่วนที่ 3

แนวปฏิบัติในการจัดทำบัญชีข้อมูลของหน่วยงาน

แนวปฏิบัติในการจัดทำบัญชีข้อมูลของหน่วยงาน

3.1 วัตถุประสงค์

เพื่อกำหนดแนวทางในการจัดทำและบริหารจัดการบัญชีข้อมูลของสำนักงานปรมาณูเพื่อสันติ (ปส.) (Data Catalog) ให้เป็นระบบและมีมาตรฐานเดียวกัน สามารถใช้ในการสืบค้น เข้าถึง แลกเปลี่ยน และใช้ประโยชน์ข้อมูลได้อย่างมีประสิทธิภาพ รวมทั้งสนับสนุนการจัดทำและเชื่อมโยงบัญชีข้อมูลภาครัฐ (Government Data Catalog : GD Catalog) ให้สอดคล้องกับกรอบธรรมาภิบาลข้อมูลภาครัฐ กฎหมาย และมาตรฐานที่เกี่ยวข้อง เพื่อส่งเสริมการบูรณาการและการใช้ประโยชน์ข้อมูลร่วมกันระหว่างหน่วยงานภาครัฐ อันจะนำไปสู่การพัฒนาการให้บริการภาครัฐ การตัดสินใจเชิงนโยบาย และการสร้างคุณค่าจากข้อมูลอย่างเป็นรูปธรรมและยั่งยืน

3.2 คำนิยาม

บัญชีข้อมูล (Data Catalog) หมายความว่า เอกสารแสดงบรรดารายการของชุดข้อมูลที่จำแนกแยกแยะโดยการจัดกลุ่มหรือจัดประเภทข้อมูลที่อยู่ในความครอบครองหรือควบคุมของหน่วยงาน

ระบบบัญชีข้อมูล หมายความว่า ระบบโปรแกรมประยุกต์ที่ทำหน้าที่บริหารจัดการบัญชีข้อมูลของหน่วยงาน เช่น การจัดการชุดข้อมูล การจัดการคำอธิบายข้อมูล การค้นหาข้อมูล การเชื่อมต่อ Application Program Interface (API)

บัญชีข้อมูลภาครัฐ (Government Data Catalog) หมายความว่า เอกสารแสดงบรรดารายการของชุดข้อมูลที่รวบรวมจากบัญชีข้อมูลของหน่วยงานภาครัฐ

ระบบบัญชีข้อมูลภาครัฐ (GD Catalog) หมายความว่า ระบบงานที่ทำหน้าที่บริหารจัดการบัญชีข้อมูลภาครัฐมารวบรวมและจัดหมวดหมู่ รวมถึงระบบนามานุกรม (Directory Services) ที่ให้บริการสืบค้นบัญชีรายการข้อมูลภาครัฐ

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

ชุดข้อมูล (Dataset) หมายความว่า การนำข้อมูลจากหลายแหล่งมารวบรวม เพื่อจัดเป็นชุดให้ตรงตามลักษณะโครงสร้างของข้อมูล หรือจากการใช้ประโยชน์ของข้อมูล

ข้อมูลเปิดภาครัฐ (Open Data) หมายความว่า ข้อมูลที่หน่วยงานของรัฐต้องเปิดเผยต่อสาธารณะ ตามกฎหมายว่าด้วยข้อมูลข่าวสารของราชการและกฎหมายอื่นในรูปแบบข้อมูลดิจิทัล ที่สามารถเข้าถึงและใช้ได้อย่างเสรี ไม่จำกัดแพลตฟอร์ม ไม่เสียค่าใช้จ่าย เผยแพร่ทำซ้ำ หรือใช้ประโยชน์ได้โดยไม่จำกัด วัตถุประสงค์

คำอธิบายชุดข้อมูลดิจิทัล หรือเมทาดาตา (Metadata) หมายความว่า ข้อมูลที่ใช้อธิบายข้อมูลหลัก หรือกลุ่มข้อมูลอื่น ๆ ที่เกี่ยวข้องทั้งกระบวนการเชิงธุรกิจ (ในที่นี้หมายถึง กระบวนการทำงานตามภารกิจ ของหน่วยงาน) และเชิงเทคโนโลยีสารสนเทศ กฎและข้อจำกัดของข้อมูล และโครงสร้างของข้อมูล เมทาดาตา ช่วยให้หน่วยงานสามารถเข้าใจข้อมูล ระบบ และขั้นตอนการทำงานได้ดียิ่งขึ้น โดยการบริหารจัดการเมทาดาตา (Metadata Management) เริ่มตั้งแต่ การเก็บรวบรวม การจัดกลุ่ม การดูแล และการควบคุมเมทาดาตา ทั้งนี้ข้อมูลแต่ละชุดควรมีเมทาดาตา เพื่อให้ผู้ใช้งานทราบเกี่ยวกับ ชุดข้อมูล เช่น รายละเอียดชุดข้อมูล สิ่งที่เกี่ยวข้องกับชุดข้อมูล วัตถุประสงค์การนำไปใช้ ไฟล์ข้อมูล

มาตรฐานเมทาดาตา (Metadata Standard) หมายความว่า การกำหนดรูปแบบและข้อกำหนด ของเมทาดาตาเพื่อให้สามารถเข้าใจได้ถูกต้องตรงกันตลอดทั้งหน่วยงาน ISO/IEC 11179 และ Dublin Core Metadata Initiative (DCMI) ได้กำหนดมาตรฐานเมทาดาตาสำหรับอธิบายชุดข้อมูล เช่น ชื่อข้อมูล ชื่อเจ้าของข้อมูล คำอธิบายข้อมูล ขอบเขตการจัดเก็บ รูปแบบข้อมูล ภาษา สิทธิการเข้าถึง ทั้งนี้มาตรฐาน เมทาดาตามักจะอ้างอิงถึงทั้งเมทาดาตาเชิงธุรกิจ (Business Metadata) และเมทาดาตาเชิงเทคนิค (Technical Metadata) แต่มักจะไม่รวมองค์ประกอบของไฟล์ข้อมูล ซึ่งเป็นคุณลักษณะ เฉพาะของแต่ละชุดข้อมูล

ศูนย์กลางข้อมูลเปิดภาครัฐ (Open Government Data) หมายความว่า ศูนย์กลางในการเข้าถึง ข้อมูลเปิดภาครัฐของประเทศที่ให้ประชาชนสามารถเข้าถึงข้อมูลภาครัฐได้สะดวก รวดเร็ว ตลอดเวลา โดยข้อมูลที่เผยแพร่อยู่ในรูปแบบไฟล์ที่สามารถแสดงตัวอย่างข้อมูล (Preview) การแสดงข้อมูลด้วยภาพ (Visualization) และ Application Program Interface (API) แบบอัตโนมัติให้กับชุดข้อมูลที่เผยแพร่ได้ รวมทั้ง ยังสามารถจัดการชุดข้อมูลและเมทาดาตาของข้อมูลได้

ศูนย์แลกเปลี่ยนข้อมูลกลาง (Government Data Exchange Center) หมายความว่า ศูนย์กลาง ในการแลกเปลี่ยนข้อมูลและเอกสารทะเบียนดิจิทัลระหว่างหน่วยงานภาครัฐ เพื่ออำนวยความสะดวก แก่ประชาชนและภาคเอกชนเมื่อใช้บริการจากภาครัฐ ช่วยให้หน่วยงานภาครัฐสามารถแลกเปลี่ยนเชื่อมโยง ข้อมูลในรูปแบบดิจิทัล

ข้อมูลแบ่งปัน (Shared data) หมายความว่า ข้อมูลอ่อนไหวที่ได้รับการจัดระดับชั้นข้อมูล ยกเว้น ในระดับชั้นลับที่สุด ซึ่งสามารถแบ่งปันและแลกเปลี่ยนกันได้ระหว่างหน่วยงาน โดยจำเป็นต้องมีการกำหนด สิทธิในการเข้าถึงและใช้งาน รวมถึงการคุ้มครองข้อมูลให้มีความมั่นคงปลอดภัย

เจ้าของข้อมูล (Data Owner) หมายความว่า บุคคล/คณะบุคคลที่ทำหน้าที่รับผิดชอบดูแลข้อมูลโดยตรง สร้างความมั่นใจได้ว่าการบริหารจัดการข้อมูลสอดคล้องกับนโยบายมาตรฐาน กฎระเบียบ หรือกฎหมาย โดยเจ้าของข้อมูลทำการทบทวนและอนุมัติการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับข้อมูล เช่น การเปลี่ยนแปลงเมทาดาตา และเกณฑ์การทำข้อมูลให้ถูกต้องสมบูรณ์ (Data Cleansing) นอกจากนี้ยังมีหน้าที่ใน การให้สิทธิ์ในการเข้าถึงข้อมูลและการจัดระดับชั้นข้อมูล เจ้าของข้อมูลส่วนใหญ่อยู่ในตำแหน่งบริหาร เช่น ผู้อำนวยการฝ่ายหรือหัวหน้าส่วนงานบุคคลเป็นเจ้าของข้อมูลบุคคล ผู้อำนวยการฝ่ายหรือหัวหน้าส่วนงาน การเงินเป็นเจ้าของข้อมูลการเงิน

เจ้าหน้าที่ผู้รับผิดชอบดูแลข้อมูล (Data Agents) หมายความว่า บุคคล/คณะบุคคลที่มีหน้าที่จัดเก็บข้อมูลให้มั่นคงปลอดภัย รวมทั้งทบทวน หรือเสนออนุมัติการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับข้อมูล และรายงานบันทึกกิจกรรมการ ประมวลผลข้อมูล

3.3 กฎหมายและแนวทางที่เกี่ยวข้อง

1. พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 มาตรา 7 และ มาตรา 8 ธรรมนูญข้อมูลภาครัฐ
2. มติคณะรัฐมนตรีเมื่อวันที่ 7 พฤษภาคม 2562 เรื่อง แนวทางการใช้ประโยชน์จากข้อมูลขนาดใหญ่ (Big Data) ให้หน่วยงานภาครัฐร่วมมือกับกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม โดยสำนักงานสถิติแห่งชาติ ในการจัดทำรายการข้อมูลภาครัฐ (Government Data Catalog) และระบบนามานุกรม (Directory Services) ตามที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเสนอ
3. มติคณะรัฐมนตรีวันที่ 22 ตุลาคม 2562 เรื่อง ขอเสนอมาตรฐานสถิติเพื่อให้คณะรัฐมนตรีเห็นชอบ คณะรัฐมนตรีมีมติเห็นชอบตามที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเสนอ ให้ส่วนราชการ รัฐวิสาหกิจ องค์กรปกครองส่วนท้องถิ่น และหน่วยงานของรัฐจัดส่งข้อมูลการใช้มาตรฐานสถิติ รวมถึงรายละเอียดของ ข้อมูล (Metadata) ตามมาตรฐานที่สำนักงานสถิติแห่งชาติ กำหนดทั้งข้อมูลระดับย่อย (Microdata) และ ข้อมูลสถิติ เพื่อให้ สำนักงานสถิติแห่งชาติ รวบรวมเป็นข้อมูลในการจัดทำศูนย์กลางรายการข้อมูลภาครัฐ (National Data Catalogue and Directory Services) และเพื่อให้สามารถติดตามและประเมินสถานการณ์ การ พัฒนาสถิติของประเทศให้มีคุณภาพตามหลักการพื้นฐานสถิติทางการและสอดคล้องตามมาตรฐานสากล สามารถนำมาใช้สนับสนุนการตัดสินใจของผู้บริหารและการใช้ประโยชน์จากข้อมูลร่วมกันได้อย่างคุ้มค่า
4. ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัลเรื่อง ธรรมนูญข้อมูลภาครัฐ ข้อ 4 (6) ธรรมนูญข้อมูล ภาครัฐในระดับหน่วยงาน การจัดทำคำอธิบายชุดข้อมูลดิจิทัลของภาครัฐและบัญชีข้อมูล ให้มีความถูกต้อง ครบถ้วน และเป็นปัจจุบัน

3.4 ข้อปฏิบัติ

1. กำหนดให้เจ้าของข้อมูลหรือหน่วยงานผู้ครอบครองข้อมูล มีหน้าที่กำหนดผู้รับผิดชอบในการบริหารจัดการข้อมูลและการจัดทำบัญชีข้อมูลของหน่วยงาน รวมทั้งกำกับดูแลและรับรองความถูกต้อง ครบถ้วน และความเป็นปัจจุบันของข้อมูลในความรับผิดชอบ

2. ผู้รับผิดชอบด้านข้อมูลต้องจัดทำคำอธิบายชุดข้อมูล (Metadata) สำหรับใช้ในการจัดทำบัญชีข้อมูลของหน่วยงาน โดยอย่างน้อยต้องครอบคลุมรายละเอียด ดังต่อไปนี้

2.1) ความสัมพันธ์และการเชื่อมโยงระหว่างชุดข้อมูล

2.2) ประเภทและชนิดของข้อมูล (Reference/Master Data Definition) แบ่งออกเป็น ดังนี้

(1) ข้อมูลอ้างอิง (Reference Data) ซึ่งเป็นข้อมูลที่มีโครงสร้างคงที่ เปลี่ยนแปลงไม่บ่อย และใช้เป็นข้อมูลอ้างอิงร่วมกันภายในหน่วยงานหรือระหว่างหน่วยงาน

(2) ข้อมูลหลัก (Master Data) ซึ่งเป็นข้อมูลสำคัญที่ใช้ในการดำเนินงานหลักของหน่วยงาน และอาจมีการเปลี่ยนแปลงหรือปรับปรุงอย่างต่อเนื่อง

2.3) ขอบเขตการดำเนินงานหรือภารกิจที่เกี่ยวข้องกับชุดข้อมูล

2.4) ชุดข้อมูลที่มีความเกี่ยวข้องหรือเชื่อมโยงกัน

2.5) กระบวนการหลัก กระบวนการย่อย และภารกิจที่เกี่ยวข้องกับข้อมูล

2.6) การระบุชุดข้อมูลที่มีอยู่ในปัจจุบันและชุดข้อมูลที่ต้องดำเนินการพัฒนาเพิ่มเติม

2.7) รูปแบบและวิธีการจัดเก็บข้อมูล

2.8) สถานะและความพร้อมใช้งานของชุดข้อมูล

2.9) แนวทางการเชื่อมโยงและแลกเปลี่ยนข้อมูลทั้งภายในและภายนอกหน่วยงาน

3. กำหนดให้ผู้รับผิดชอบด้านข้อมูลจัดทำพจนานุกรมข้อมูล (Data Dictionary) ในระดับโครงสร้างข้อมูลและฟิลด์ข้อมูล เพื่ออธิบายรายละเอียด มาตรฐาน และคุณลักษณะของข้อมูลสำหรับการใช้งานและการเชื่อมโยงข้อมูลร่วมกัน โดยอย่างน้อยต้องประกอบด้วย

3.1) รหัสคำอธิบายชุดข้อมูลหรือเลขที่เมทาดาตา (Metadata ID)

3.2) ชื่อชุดข้อมูล (Dataset Name)

3.3) รหัสข้อมูลหรือรหัสชุดข้อมูล (Data ID)

3.4) ชื่อตารางข้อมูล (Table Name)

3.5) ชื่อฟิลด์ข้อมูล (Field Name)

3.6) คำอธิบายข้อมูลหรือคำอธิบายฟิลด์ (Description)

3.7) ระดับชั้นความลับของข้อมูล (Classification)

3.8) ประเภทข้อมูล (Data Type)

3.9) ขนาดข้อมูล (Data Size)

3.10) คุณลักษณะของข้อมูล (Characteristic Type)

3.11) แหล่งที่มาของข้อมูล (Data Source)

3.12) รูปแบบข้อมูล (Data Format)

3.13) เงื่อนไขหรือข้อกำหนดในการใช้งานข้อมูล (Condition)

4. กำหนดให้ชุดข้อมูล คำอธิบายชุดข้อมูล และพจนานุกรมข้อมูลของหน่วยงาน มีความถูกต้อง ครบถ้วน สอดคล้องกัน และเป็นมาตรฐานเดียวกัน รวมทั้งสามารถสืบค้นหรือใช้งานได้อย่างมีประสิทธิภาพ

5. กำหนดให้มีการทบทวน ปรับปรุง และตรวจสอบบัญชีข้อมูล คำอธิบายชุดข้อมูล และพจนานุกรม ข้อมูลอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญเกี่ยวกับข้อมูล ระบบงาน หรือภารกิจของ หน่วยงาน เพื่อให้ข้อมูลมีความถูกต้องและเป็นปัจจุบันอยู่เสมอ

6. กำหนดให้มีการจัดทำบัญชีข้อมูลและคำอธิบายชุดข้อมูลต้องสอดคล้องกับมาตรฐานบัญชีข้อมูล ภาครัฐ (Government Data Catalog : GD Catalog) และมาตรฐานหรือหลักเกณฑ์ที่หน่วยงานภาครัฐ กำหนด

7. กำหนดให้มีการจัดชั้นความลับและกำหนดสิทธิ์การเข้าถึงข้อมูลในบัญชีข้อมูลให้เหมาะสมกับ ความอ่อนไหวของข้อมูล รวมทั้งสอดคล้องกับกฎหมาย ระเบียบ แผนนโยบายความมั่นคงปลอดภัย ด้านสารสนเทศ และนโยบายการคุ้มครองข้อมูลส่วนบุคคลสำนักงานปรมาณเพื่อสันติ

8. กำหนดให้มีการเผยแพร่บัญชีข้อมูลของหน่วยงานในรูปแบบดิจิทัลที่สามารถสืบค้น เข้าถึง และ นำไปใช้ประโยชน์ได้ โดยต้องไม่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ หรือแผนนโยบายความมั่นคงปลอดภัย ด้านสารสนเทศ และนโยบายการคุ้มครองข้อมูลส่วนบุคคลสำนักงานปรมาณเพื่อสันติ

9. สนับสนุนให้มีการเชื่อมโยงบัญชีข้อมูลของหน่วยงานเข้าสู่ระบบบัญชีข้อมูลภาครัฐ (Government Data Catalog : GD Catalog) เพื่อส่งเสริมการบูรณาการและการใช้ประโยชน์ข้อมูลร่วมกันระหว่างหน่วยงาน ภาครัฐอย่างเป็นระบบและมีประสิทธิภาพ

10. กำหนดให้การตั้งชื่อชุดข้อมูล ตารางข้อมูล ฟิลด์ข้อมูล และรหัสข้อมูล เป็นไปตามมาตรฐาน การตั้งชื่อข้อมูลของหน่วยงาน เพื่อให้สามารถสืบค้น เชื่อมโยง แลกเปลี่ยน และใช้งานข้อมูลร่วมกันได้ อย่างมีประสิทธิภาพและเป็นมาตรฐานเดียวกัน



ส่วนที่ 4

แนวปฏิบัติในการประเมินคุณภาพข้อมูล

แนวปฏิบัติในการประเมินคุณภาพข้อมูล

4.1 วัตถุประสงค์

เพื่อกำหนดหลักเกณฑ์ แนวทาง และกระบวนการบริหารจัดการคุณภาพข้อมูลของสำนักงานปรมาณูเพื่อสันติ (ปส.) ให้เป็นมาตรฐานเดียวกัน สำหรับใช้เป็นกรอบในการประเมิน ตรวจสอบ ควบคุม และปรับปรุงคุณภาพข้อมูลของหน่วยงาน เพื่อให้ข้อมูลมีความถูกต้อง ครบถ้วน เชื่อถือได้ เป็นปัจจุบัน และพร้อมใช้งานสามารถนำไปใช้ประโยชน์ในการดำเนินงาน การวิเคราะห์ การบูรณาการข้อมูล และการตัดสินใจเชิงนโยบายได้อย่างมีประสิทธิภาพและเหมาะสม รวมทั้งสนับสนุนการดำเนินงานตามหลักธรรมาภิบาลข้อมูลภาครัฐเพิ่มประสิทธิภาพการปฏิบัติงานและการให้บริการภาครัฐ ตลอดจนสร้างความเชื่อมั่นให้แก่ผู้ใช้ข้อมูลและรองรับการเชื่อมโยงและใช้ประโยชน์ข้อมูลร่วมกันระหว่างหน่วยงานภาครัฐอย่างเป็นระบบและมีประสิทธิภาพ

4.2 คำนิยาม

คุณภาพข้อมูล (Data Quality) หมายความว่า ข้อมูลที่ดี ได้มาตรฐานตามที่กำหนด และตรงกับความต้องการของผู้ใช้ กล่าวคือผลรวมของคุณลักษณะและคุณสมบัติของผลิตผลข้อมูลที่พึงประสงค์ทุกประการของผลการปฏิบัติงานตามดัชนีตัวชี้วัดคุณภาพและองค์ประกอบที่กำหนดไว้

การประเมินคุณภาพข้อมูล (Data Quality Assessment) หมายความว่า กระบวนการประเมินผลโดยภาพรวมว่า เมื่อได้มีการบริหารจัดการและกำกับดูแลคุณภาพข้อมูลแล้วทำให้เกิดการเปลี่ยนแปลงในเชิงคุณภาพอย่างไร ทั้งนี้การตรวจสอบและประเมินคุณภาพจะต้องทำอย่างเป็นระบบ มีหลักเกณฑ์และแนวปฏิบัติที่ชัดเจนมีการประกาศให้ทราบล่วงหน้าและกระทำโดยผู้ประเมินคุณภาพข้อมูล

ความถูกต้อง และสมบูรณ์ (Accuracy and Completeness) หมายความว่า ข้อมูลมีความถูกต้องแม่นยำสูง มีความครบถ้วนสมบูรณ์ของข้อมูลที่เก็บรวบรวมมา และมีการตรวจสอบความถูกต้องระหว่างข้อมูลในส่วนต่าง ๆ ในทุกขั้นตอน เพื่อให้ข้อมูลถูกต้องเชื่อถือได้และให้ผลลัพธ์ตรงตามความต้องการผู้ใช้ (ข้อมูลครบถ้วน ข้อมูลไม่ขาดหาย กว้างพอและลึกพอสำหรับการใช้งาน)

ความสอดคล้องกัน (Consistency) หมายความว่า ข้อมูลมีความสอดคล้องกันของ แนวคิด คำนิยาม วิธีการ รหัส และการนำเสนอที่ทำให้ข้อมูลจากต่างแหล่ง ต่างเวลา สามารถเปรียบเทียบข้ามช่วงเวลาและบูรณาการข้อมูลเพื่อใช้ประโยชน์ร่วมกันได้

ความเป็นปัจจุบัน (Timeliness) หมายความว่า ข้อมูลเป็นปัจจุบันทันสมัยเพียงพอต่อการใช้งานและพร้อมใช้งานตามที่กำหนดและในกรอบเวลาที่กำหนดไว้ หรือมีข้อมูลทันต่อการใช้งานทุกครั้งตามที่ใช้ต้องการ

ตรงตามความต้องการของผู้ใช้ (Relevancy) หมายความว่า ข้อมูลสามารถนำไปใช้ได้กับงานที่ทำอยู่ เป็นข้อมูลที่ผู้ใช้งานต้องการ หรือเป็นข้อมูลที่จำเป็นต้องทราบ มีมุมมองและความละเอียดเพียงพอต่อการนำไปใช้งาน

ความพร้อมใช้ (Availability) หมายความว่า ข้อมูลเข้าถึงได้ง่าย หรือมีข้อมูลนั้นอยู่ สามารถใช้งานได้จริง และสามารถใช้งานได้ตลอดเวลา

ผู้ประเมินคุณภาพข้อมูล (Data Assessment Team) หมายความว่า คณะบุคคล/ทีมงานที่กำหนดขึ้นเพื่อทำหน้าที่การประเมินคุณภาพข้อมูลขององค์กร ในที่นี้อาจเป็นทีมบริกรข้อมูล (Data Stewards Team) หรือฝ่ายตรวจสอบภายใน หรือผู้ไม่มีส่วนได้ส่วนเสียกับการดำเนินงานเพื่อให้ไม่เกิดผลประโยชน์ทับซ้อน

เจ้าของข้อมูล (Data Owner) หมายความว่า ผู้ที่ได้รับมอบหมายในการปฏิบัติงานให้รับผิดชอบข้อมูลที่ระบุไว้ ซึ่งรวมถึงผู้บังคับบัญชาของเจ้าของข้อมูลนั้นด้วย โดยทำหน้าที่กำกับดูแลตาม ธรรมชาติของข้อมูล และตามกฎหมาย ระเบียบที่กำหนดไว้ (กรณีข้อมูลลับ) ตลอดจนวงจรชีวิตของข้อมูลนั้น ๆ รวมทั้งทำหน้าที่กำหนดสิทธิ์ในการเข้าถึงข้อมูลและกำหนดชั้นความลับของข้อมูล

4.3 ข้อปฏิบัติ

กำหนดให้ ปส. ดำเนินการบริหารจัดการคุณภาพข้อมูล (Data Quality Management) เพื่อให้ข้อมูลที่ใช้ในการสนับสนุนการดำเนินงาน การกำหนดนโยบาย การตัดสินใจ การให้บริการ และการบูรณาการข้อมูล ร่วมกับหน่วยงานภายนอก มีความถูกต้อง ครบถ้วน เชื่อถือได้ เป็นปัจจุบัน และสามารถนำไปใช้ประโยชน์ได้อย่างมีประสิทธิภาพ สอดคล้องกับภารกิจของหน่วยงาน รวมถึงกฎหมาย ระเบียบ และมาตรฐานที่เกี่ยวข้อง

ทั้งนี้ การบริหารจัดการคุณภาพข้อมูล (Data Quality Management) ให้ครอบคลุมการกำกับดูแล ตรวจสอบ ปรับปรุง และควบคุมคุณภาพข้อมูล เพื่อให้ข้อมูลมีความพร้อมสำหรับการใช้งาน การแลกเปลี่ยน การเชื่อมโยง และการวิเคราะห์ข้อมูล ตลอดจนสนับสนุนการดำเนินงานตามหลักธรรมาภิบาลข้อมูลภาครัฐ (Data Governance) โดยกำหนดกรอบการบริหารจัดการคุณภาพข้อมูลของสำนักงานให้เป็นมาตรฐานเดียวกัน ครอบคลุมกระบวนการสำคัญ 4 ขั้นตอน ได้แก่

1. การกำหนดหลักเกณฑ์คุณภาพข้อมูล
2. การประเมินคุณภาพข้อมูล
3. การปรับปรุงคุณภาพข้อมูล
4. การควบคุม ติดตาม และทบทวนคุณภาพข้อมูลอย่างต่อเนื่อง

4.3.1 การกำหนดหลักเกณฑ์คุณภาพข้อมูล (Data Quality Requirement)

การกำหนดหลักเกณฑ์คุณภาพข้อมูล (Data Quality Requirement) ต้องดำเนินการกำหนดหลักเกณฑ์คุณภาพข้อมูลอย่างน้อย ดังนี้

4.3.1.1 การกำหนดองค์ประกอบข้อมูลที่สำคัญ (Critical Data Elements : CDE)

เจ้าของข้อมูล บริกรข้อมูล และผู้ใช้ข้อมูล ต้องร่วมกันกำหนดองค์ประกอบข้อมูลที่สำคัญ (Critical Data Elements : CDE) ของแต่ละชุดข้อมูล โดยพิจารณาจากความสำคัญของข้อมูล ต่อภารกิจ การดำเนินงาน และผลกระทบที่อาจเกิดขึ้น เช่น

- (1) ข้อมูลหลัก (Master Data)
- (2) มูลค่าทางการเงิน (Financial Value)
- (3) ผลกระทบต่อผู้ใช้บริการ (Impact on Customers)
- (4) ผลกระทบต่อองค์กร (Business Impact Analysis)
- (5) ข้อกำหนดด้านกฎหมาย ระเบียบ หรือข้อบังคับที่เกี่ยวข้อง (Regulatory Requirements)

ทั้งนี้ บริกรข้อมูลและผู้เชี่ยวชาญเฉพาะทาง ต้องร่วมกันกำหนดกฎเกณฑ์ทางธุรกิจ (Business Rules) และเงื่อนไขด้านคุณภาพข้อมูล เพื่ออธิบายลักษณะและมาตรฐานคุณภาพของข้อมูล ให้สามารถนำข้อมูลไปใช้ได้อย่างถูกต้อง เหมาะสม และสอดคล้องกับวัตถุประสงค์ในการใช้งาน

4.3.1.2 การกำหนดระดับคุณภาพข้อมูล (Data Quality Threshold)

เจ้าของข้อมูลต้องกำหนดระดับคุณภาพข้อมูล (Data Quality Threshold) สำหรับชุดข้อมูลแต่ละประเภท เพื่อใช้เป็นเกณฑ์ในการประเมินและควบคุมคุณภาพข้อมูล โดยพิจารณาให้สอดคล้องกับลักษณะ ความสำคัญ และวัตถุประสงค์ของการใช้งานข้อมูล รวมถึงความเสี่ยงและผลกระทบที่อาจเกิดขึ้นจากข้อมูลที่ไม่มีคุณภาพ

4.3.2 การประเมินคุณภาพข้อมูล (Data Quality Assessment)

4.3.2.1 การประเมินคุณภาพข้อมูลตามหลักเกณฑ์คุณภาพข้อมูล

ให้ดำเนินการประเมินคุณภาพข้อมูลโดยใช้วิธีการทำโปรไฟล์ข้อมูล (Data Profiling) สำหรับชุดข้อมูลที่เป็นองค์ประกอบข้อมูลที่สำคัญ (Critical Data Elements : CDE) และเปรียบเทียบผลกับระดับคุณภาพข้อมูลที่กำหนดไว้ โดยบริกรข้อมูล ผู้เชี่ยวชาญเฉพาะทาง และผู้ใช้ข้อมูล ต้องร่วมกันกำหนดเป้าหมายของการประเมินคุณภาพข้อมูล เพื่อศึกษารายละเอียดของข้อมูล วิเคราะห์ปัญหาคุณภาพข้อมูล และจัดทำแผนการปรับปรุงคุณภาพข้อมูลอย่างเหมาะสม

ทั้งนี้ การประเมินคุณภาพข้อมูลอาจเริ่มต้นจากชุดข้อมูลขนาดเล็ก พิลด์ข้อมูลเฉพาะหรือประเด็นปัญหาคุณภาพข้อมูลที่สำคัญ เพื่อทดสอบแนวทาง วิธีการ และกระบวนการปรับปรุงคุณภาพข้อมูลก่อนขยายผลไปยังชุดข้อมูลอื่น โดยการทำให้โปรไฟล์ข้อมูล (Data Profiling) ให้ดำเนินการอย่างน้อย ดังนี้

- (1) กำหนดเป้าหมายของการประเมินคุณภาพข้อมูล
- (2) ระบุชุดข้อมูลหรือพิลด์ข้อมูลที่จะทำการประเมิน โดยมุ่งเน้นข้อมูลที่มีความสำคัญหรือมีความเสี่ยงสูง
- (3) ระบุวัตถุประสงค์การใช้งานข้อมูลและกลุ่มผู้ใช้ข้อมูล
- (4) ประเมินความเสี่ยงและผลกระทบที่อาจเกิดขึ้นจากปัญหาคุณภาพข้อมูลต่อกระบวนการดำเนินงานขององค์กร
- (5) ตรวจสอบข้อมูลตามกฎเกณฑ์และเงื่อนไขด้านคุณภาพข้อมูลที่กำหนด
- (6) จัดทำรายงานผลการตรวจสอบ พร้อมระบุประเภทและลักษณะของปัญหาคุณภาพข้อมูลที่พบ
- (7) วิเคราะห์เชิงลึกเพื่อหาสาเหตุที่แท้จริงของปัญหา รวมถึงประเมินปริมาณ ความรุนแรง และผลกระทบทางธุรกิจ (Business Impact) เพื่อจัดลำดับความสำคัญของปัญหา
- (8) ประชุมร่วมกับบริการข้อมูล ผู้เชี่ยวชาญเฉพาะด้าน และผู้ใช้ข้อมูล เพื่อยืนยันผลการประเมิน และลำดับความสำคัญของปัญหา
- (9) จัดทำแผนการดำเนินงานเพื่อปรับปรุงคุณภาพข้อมูล โดยอย่างน้อยต้องครอบคลุม
 - การแก้ไขปัญหาที่ต้นเหตุ
 - การควบคุมและปรับปรุงกระบวนการทำงานเพื่อป้องกันการเกิดปัญหาซ้ำ
 - การติดตาม ควบคุม และรายงานผลการปรับปรุงคุณภาพข้อมูลอย่างต่อเนื่อง
- (10) การประเมินคุณภาพข้อมูลต้องพิจารณาตามมิติคุณภาพข้อมูล (Data Quality Dimension) ซึ่งเป็นคุณลักษณะสำคัญที่ใช้วัดและประเมินคุณภาพของข้อมูล เพื่อให้สามารถตรวจสอบ วิเคราะห์ และนำข้อมูลไปใช้ประโยชน์ได้อย่างมีประสิทธิภาพ โดยกำหนดมิติคุณภาพข้อมูลที่สำคัญ จำนวน 5 มิติ ได้แก่

- 1) ความถูกต้อง (Accuracy)
- 2) ความสอดคล้องกัน (Consistency)
- 3) ตรงตามความต้องการของผู้ใช้ (Relevancy)
- 4) ความเป็นปัจจุบัน (Timeliness)
- 5) ความพร้อมใช้งาน (Availability)

ทั้งนี้ ให้กำหนดรายละเอียดตัวชี้วัด (Indicators) และเกณฑ์การประเมินสำหรับแต่ละมิติ คุณภาพข้อมูลให้เหมาะสมกับลักษณะและวัตถุประสงค์ของการใช้งานข้อมูลของ ปส. เพื่อให้ข้อมูลมีคุณภาพ เชื่อถือได้ และสามารถรองรับการดำเนินงาน การวิเคราะห์ และการตัดสินใจได้อย่างมีประสิทธิภาพและเกิด ประโยชน์สูงสุดต่อองค์กรและภาคส่วนที่เกี่ยวข้อง ดังต่อไปนี้

ลำดับ	มิติคุณภาพข้อมูล	รายละเอียด	รายการตัวชี้วัด
1	ความถูกต้องและสมบูรณ์ (Accuracy and Completeness)	ประเมินเรื่องความถูกต้องแม่นยำ แหล่งข้อมูลที่น่าเชื่อถือ และมี กระบวนการตรวจสอบ	1) มีแหล่งข้อมูลที่น่าเชื่อถือ 2) มีกระบวนการหรือเครื่องมือ ตรวจสอบ จุดผิดพลาด ของข้อมูล 3) มีการตรวจสอบความครบถ้วน ของข้อมูล 4) มีวิธีเก็บข้อมูลมีความเป็นกลาง น่าเชื่อถือ และไม่สร้างข้อมูลที่ มีอคติ 5) มีการระบุค่านิยามและลักษณะ ข้อมูลที่ต้องการ
2	ความสอดคล้องกัน (Consistency)	ประเมินเรื่องรูปแบบของข้อมูล ความสอดคล้องกัน และมาตรฐาน ในการจัดทำข้อมูลของหน่วยงาน	1) มีการเก็บข้อมูลภายใต้ มาตรฐานข้อมูลเดียวกันหรือ มาตรฐานข้อมูลที่สอดคล้องกัน ทำให้สามารถใช้ประโยชน์ ข้อมูลร่วมกันได้ 2) มีการตรวจสอบรูปแบบข้อมูล ภายในชุดข้อมูลเดียวกัน 3) ข้อมูลมีความเชื่อมโยง และไม่ขัดแย้งกัน 4) มีการใช้กฎ วิธีการตรวจวัด ที่สอดคล้องกันทั้งหน่วยงาน รวมถึงหน่วยงานภายนอก 5) มีการกำหนดบทบาทและ ผู้รับผิดชอบข้อมูล

ลำดับ	มิติคุณภาพข้อมูล	รายละเอียด	รายการตัวชี้วัด
3	ตรงตามความต้องการ ของผู้ใช้ (Relevancy)	ประเมินว่าเป็นข้อมูลที่ใช้ต้องการ หรือเป็นข้อมูลที่จำเป็นต้องทราบ มีความละเอียดเพียงพอต่อ การนำไปใช้งาน	1) ข้อมูลตรงตามความต้องการ และวัตถุประสงค์ของ การใช้งาน 2) มีผลประเมินความพึงพอใจ ของผู้ใช้ และมีการปรับปรุง คุณภาพให้ตรงตาม ความต้องการของผู้ใช้
4	ความเป็นปัจจุบัน (Timeliness)	ประเมินเรื่องการเผยแพร่ข้อมูล การปรับปรุงข้อมูล และแผนเรื่องระยะเวลา	1) ข้อมูลมีการเผยแพร่ ส่งต่อ ตรงเวลา 2) ข้อมูลมีความเป็นปัจจุบัน 3) ข้อมูลมีการเผยแพร่ข้อมูล ในเวลาที่เหมาะสม 4) มีการจัดทำปฏิทินเผยแพร่ ข้อมูล
5	ความพร้อมใช้ (Availability)	ประเมินความพร้อมใช้ของข้อมูล รวมไปถึงช่องทางในการขอ หรือใช้ข้อมูล	1) ข้อมูลถูกจัดในรูปแบบที่พร้อม นำไปใช้งาน และเหมาะสมกับ ผู้ใช้งาน 2) มีการเผยแพร่ข้อมูล ที่เหมาะสมและสามารถ เข้าถึงได้ โดยผู้ใช้สามารถ เข้าถึงข้อมูลได้สะดวก ตามสิทธิ์ที่เหมาะสม 3) ข้อมูลสามารถอ่านด้วย โปรแกรมคอมพิวเตอร์ได้ 4) มีคำอธิบายข้อมูลที่ชัดเจน 5) มีคำอธิบายขั้นตอนการขอ ข้อมูลที่ไม่เผยแพร่

4.3.3 การปรับปรุงคุณภาพข้อมูล (Data Quality Improvement)

ต้องดำเนินการปรับปรุงคุณภาพข้อมูลอย่างน้อย ดังนี้

4.3.3.1 การปรับปรุงข้อมูลที่ไม่ผ่านเกณฑ์การประเมินคุณภาพ

ต้องมีกระบวนการปรับปรุงชุดข้อมูลที่ไม่ผ่านเกณฑ์การประเมินคุณภาพ พร้อมจัดลำดับความสำคัญของปัญหาโดยพิจารณาจากผลกระทบทางธุรกิจ ความเสี่ยง และความสำคัญของข้อมูลต่อภารกิจของหน่วยงาน ทั้งนี้ แนวทางการดำเนินการ มีดังต่อไปนี้

- (1) ระบุและจัดลำดับความสำคัญของปัญหาคุณภาพข้อมูลที่ต้องได้รับการปรับปรุง
- (2) จัดทำโปรไฟล์ข้อมูล (Data Profiling) สำหรับชุดข้อมูล เพื่อวิเคราะห์และทำความเข้าใจปัญหาคุณภาพข้อมูลที่เกิดขึ้น
- (3) สัมภาษณ์หรือรับฟังความคิดเห็นจากผู้มีส่วนได้ส่วนเสียเกี่ยวกับปัญหาคุณภาพข้อมูล
- (4) วิเคราะห์ผลกระทบของปัญหาคุณภาพข้อมูลต่อการดำเนินงานขององค์กร

4.3.3.2 การกำหนดเป้าหมายการปรับปรุงคุณภาพข้อมูล

ต้องกำหนดเป้าหมายและแนวทางการปรับปรุงคุณภาพข้อมูล โดยคำนึงถึงความเร็วในการแก้ไขปัญหา ความคุ้มค่าในการดำเนินงาน และผลตอบแทนจากการลงทุน (Return on Investment : ROI) รวมถึงผลกระทบในระยะสั้นและระยะยาว ทั้งนี้ ปัจจัยที่ใช้ประกอบการพิจารณา มีดังต่อไปนี้

- (1) การจัดลำดับความสำคัญของข้อมูลที่ได้รับผลกระทบ
- (2) ปริมาณข้อมูลที่ได้รับผลกระทบ
- (3) อายุหรือระยะเวลาของข้อมูล
- (4) จำนวนและประเภทของกระบวนการทางธุรกิจที่ได้รับผลกระทบ
- (5) จำนวนผู้ได้รับผลกระทบ เช่น ผู้ให้บริการ ผู้รับบริการ หรือบุคลากรของหน่วยงาน
- (6) ความเสี่ยงที่เกี่ยวข้องกับปัญหาคุณภาพข้อมูล
- (7) ค่าใช้จ่ายในการแก้ไขสาเหตุที่แท้จริงของปัญหา
- (8) ค่าใช้จ่ายหรือผลกระทบที่อาจเกิดขึ้นหากไม่มีการแก้ไขปัญหา

4.3.3.3 การวิเคราะห์หาสาเหตุที่แท้จริงของปัญหา (Root Cause Analysis)

ต้องวิเคราะห์หาสาเหตุที่แท้จริงของปัญหาคุณภาพข้อมูล เพื่อป้องกันไม่ให้เกิดปัญหาซ้ำในอนาคต โดยอาจใช้เครื่องมือวิเคราะห์ เช่น แผนภาพก้างปลา (Fishbone Diagram) หรือวิธีการอื่นที่เหมาะสม ทั้งนี้ ขั้นตอนการดำเนินการอย่างน้อยต้องประกอบด้วย ดังต่อไปนี้

- (1) กำหนดประเด็นปัญหาที่ต้องการวิเคราะห์
- (2) ระบุปัจจัยที่อาจก่อให้เกิดปัญหา เช่น ด้านกระบวนการ (Processes) วัสดุหรือข้อมูล (Materials) เครื่องมือหรือระบบงาน (Machines) และวิธีการปฏิบัติงาน (Methods)
- (3) ระดมความคิดเห็นเพื่อวิเคราะห์สาเหตุของปัญหาในแต่ละปัจจัย
- (4) วิเคราะห์และระบุสาเหตุหลักของปัญหา
- (5) จัดลำดับความสำคัญของสาเหตุที่ต้องดำเนินการแก้ไข
- (6) กำหนดแนวทางหรือมาตรการปรับปรุงที่เหมาะสมเพื่อแก้ไขและป้องกันปัญหา

4.3.3.4 การควบคุมและติดตามการปรับปรุงคุณภาพข้อมูล

ต้องกำหนดกระบวนการควบคุม ติดตาม และตรวจสอบการปรับปรุงคุณภาพข้อมูลอย่างเหมาะสม ครอบคลุมทั้งมาตรการเชิงป้องกันและมาตรการแก้ไข รวมถึงต้องจัดเก็บหลักฐานหรือบันทึกข้อมูลก่อนและหลังการแก้ไข เพื่อป้องกันการแก้ไขข้อมูลโดยไม่ได้รับอนุญาตและรองรับการตรวจสอบย้อนหลัง ทั้งนี้ องค์ประกอบอย่างน้อยต้องประกอบด้วย ดังต่อไปนี้

- (1) มาตรการเชิงป้องกัน (Preventive Actions) เพื่อป้องกันไม่ให้เกิดข้อมูลที่มีคุณภาพต่ำ
- (2) มาตรการเชิงแก้ไข (Corrective Actions) เพื่อแก้ไขปัญหาคุณภาพข้อมูลที่เกิดขึ้น และป้องกันไม่ให้เกิดซ้ำในอนาคต โดยทั่วไปดำเนินการได้ 3 วิธี ดังนี้

วิธีการ	รายละเอียด
การแก้ไขอัตโนมัติ (Automated Correction)	เป็นการแก้ไขข้อมูลด้วยกระบวนการอัตโนมัติตามมาตรฐานและกฎเกณฑ์ที่กำหนดไว้ เช่น การกำหนดรูปแบบมาตรฐานของข้อมูล การตรวจสอบความถูกต้องตามมาตรฐาน และการปรับแก้ข้อมูลให้เป็นไปตามมาตรฐานโดยอัตโนมัติ รวมถึงการอ้างอิงข้อมูลจากตารางอ้างอิง (Reference Table) หรือข้อกำหนดทางธุรกิจที่เกี่ยวข้อง เช่น การแก้ไขรูปแบบที่อยู่อัตโนมัติให้เป็นไปตามมาตรฐานที่กำหนด
การแก้ไขกึ่งอัตโนมัติ (Manually-Directed Correction)	เป็นการใช้เครื่องมืออัตโนมัติช่วยในการตรวจสอบหรือแก้ไขข้อมูล โดยต้องมีผู้ปฏิบัติงานตรวจสอบและยืนยันความถูกต้องก่อนดำเนินการแก้ไข รวมถึงต้องได้รับการทบทวนหรือรับรองผลการแก้ไขจากบริการข้อมูลหรือผู้รับผิดชอบข้อมูลที่เกี่ยวข้อง
การแก้ไขด้วยตนเอง (Manual Correction)	เป็นการแก้ไขข้อมูลโดยผู้ปฏิบัติงานในกรณีที่ไม่สามารถดำเนินการด้วยวิธีอัตโนมัติได้ โดยต้องดำเนินการภายใต้กระบวนการควบคุม ตรวจสอบ และอนุมัติที่เหมาะสม เพื่อให้การแก้ไขข้อมูลมีความถูกต้อง โปร่งใส และสามารถตรวจสอบย้อนหลังได้

4.3.4 การควบคุมและติดตามให้ข้อมูลมีคุณภาพ (Monitoring and Control)

ต้องดำเนินการควบคุม ติดตาม และทบทวนคุณภาพข้อมูลอย่างต่อเนื่อง อย่างน้อยดังนี้

4.3.4.1 การติดตามและตรวจสอบคุณภาพข้อมูลอย่างต่อเนื่อง

ต้องมีการติดตาม ประเมิน และปรับปรุงผลการประเมินคุณภาพข้อมูลอย่างต่อเนื่อง เพื่อให้สามารถตรวจสอบและเฝ้าระวังคุณภาพของชุดข้อมูลได้อย่างทันท่วงที ทั้งนี้ การตรวจสอบการปฏิบัติตามกฎเกณฑ์คุณภาพข้อมูลอาจดำเนินการโดยระบบอัตโนมัติ ทั้งในระหว่างการประมวลผลข้อมูล (In-Stream Processing) หรือภายหลังการประมวลผลแบบกลุ่มตามรอบระยะเวลาที่กำหนด (Batch Processing)

4.3.4.2 การแจ้งเตือนเมื่อพบปัญหาคุณภาพข้อมูล

ต้องจัดให้มีกระบวนการหรือเครื่องมือสำหรับแจ้งเตือนไปยังเจ้าของข้อมูลหรือผู้รับผิดชอบที่เกี่ยวข้อง เมื่อพบว่าชุดข้อมูลมีคุณภาพต่ำกว่าระดับคุณภาพข้อมูล (Data Quality Threshold) ที่กำหนด เพื่อให้สามารถดำเนินการแก้ไขได้อย่างเหมาะสมและทันท่วงที

4.3.4.3 การสอบทานคุณภาพข้อมูล

ต้องมีการสอบทานและตรวจสอบคุณภาพข้อมูลให้เป็นไปตามหลักเกณฑ์มาตรฐานและข้อกำหนดด้านคุณภาพข้อมูลที่กำหนดไว้อย่างสม่ำเสมอ เพื่อรักษาคุณภาพและความน่าเชื่อถือของข้อมูลอย่างต่อเนื่อง

4.3.4.4 การรายงานผลการติดตามคุณภาพข้อมูล

ต้องจัดทำรายงานผลการติดตามและประเมินคุณภาพข้อมูล รวมถึงสรุปความคืบหน้าของการแก้ไขและปรับปรุงชุดข้อมูลที่ไม่ผ่านเกณฑ์การประเมิน ตลอดจนรายงานประเด็นปัญหา ความเสี่ยง ภาพรวมของปัญหา และสาเหตุที่ส่งผลให้ข้อมูลไม่มีคุณภาพ เพื่อรายงานต่อคณะกรรมการธรรมาภิบาลข้อมูล หรือผู้บริหารที่เกี่ยวข้องอย่างสม่ำเสมอ โดยรายงานควรครอบคลุมอย่างน้อย ดังนี้

- (1) ผลการวัดคุณภาพข้อมูล (Data Quality Scorecard) เพื่อแสดงภาพรวมคะแนนและผลการประเมินคุณภาพข้อมูล
- (2) แนวโน้มคุณภาพข้อมูล เพื่อแสดงการเปลี่ยนแปลงและแนวโน้มของคุณภาพข้อมูลว่ามีการพัฒนาหรือมีความเสี่ยงลดลงหรือเพิ่มขึ้น
- (3) สถานะการจัดการและแก้ไขปัญหาคุณภาพข้อมูล รวมถึงผลการดำเนินการแก้ไข
- (4) ความสอดคล้องของการดำเนินงานกับนโยบายและแนวปฏิบัติด้านการบริหารจัดการข้อมูล
- (5) ผลลัพธ์หรือผลกระทบเชิงบวกจากการดำเนินโครงการหรือกิจกรรมปรับปรุงคุณภาพข้อมูล

เอกสารอ้างอิง

1. สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน). มาตรฐานรัฐบาลดิจิทัล มรด. 6 : 2566 ว่าด้วยกรอบธรรมาภิบาลข้อมูลภาครัฐ ฉบับปรับปรุง: แนวปฏิบัติ (Data Governance Framework Revised: Guideline) Version 2.0. สำนักนายกรัฐมนตรี, 2566
2. เอกสารแม่แบบแนวปฏิบัติการบริหารจัดการข้อมูล (Data Management Guideline Template) ตามมาตรฐานรัฐบาลดิจิทัล มรด. 4-2 : 2565 ว่าด้วยข้อเสนอแนะสำหรับการจัดทำแนวปฏิบัติการบริหารจัดการข้อมูล (Recommendation for Writing Data Management Guideline) Version 1.0, สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน), สำนักนายกรัฐมนตรี
3. สำนักงานปรมาณูเพื่อสันติ. (ม.ป.ป.). แนวนโยบายความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานปรมาณูเพื่อสันติ. กรุงเทพมหานคร: สำนักงานปรมาณูเพื่อสันติ
4. สำนักงานปรมาณูเพื่อสันติ. (2568). นโยบายการคุ้มครองข้อมูลส่วนบุคคลของสำนักงานปรมาณูเพื่อสันติ. กรุงเทพมหานคร: สำนักงานปรมาณูเพื่อสันติ