



กรมพัฒนาพลังงานทดแทน
และอนุรักษ์พลังงาน
กระทรวงพลังงาน

คู่มือธรรมาภิบาลข้อมูล

ของกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน



สารบัญ

หน้า

บทสรุปผู้บริหาร (Executive Summary)	I
บทที่ 1 บทนำ	1
1.1 ความเป็นมา	1
1.2 วัตถุประสงค์	1
1.3 นโยบายข้อมูล	2
1.4 นิยามศัพท์ที่เกี่ยวข้องกับธรรมาภิบาลข้อมูล	3
บทที่ 2 แนวคิดธรรมาภิบาลข้อมูล	4
2.1 ธรรมาภิบาลข้อมูล (Data Governance)	4
2.1.1 นิยามของธรรมาภิบาลข้อมูล (Definition)	4
2.1.2 กฎเกณฑ์ในการกำกับดูแลข้อมูล (Rules)	4
2.1.3 องค์ประกอบหลักของธรรมาภิบาลข้อมูลที่ดี	5
2.2 ข้อมูล (Data)	6
2.2.1 ประเภทข้อมูล	7
2.2.2 ชุดข้อมูล	7
2.2.3 ฐานข้อมูล	8
2.3 การบริหารจัดการข้อมูล	8
2.3.1 ระบบบริหารและกระบวนการจัดการข้อมูล	9
2.3.2 องค์ประกอบในการบริหารจัดการข้อมูล	10
2.4 ความสัมพันธ์ระหว่างธรรมาภิบาลข้อมูลและการบริหารจัดการข้อมูล	14
บทที่ 3 กรอบธรรมาภิบาลข้อมูล ของ พพ.	16
3.1 โครงสร้างธรรมาภิบาลข้อมูลภาครัฐ (Data Governance Structure)	17
3.1.1 คณะกรรมการธรรมาภิบาลข้อมูล	18
3.1.2 ทีมบริการข้อมูล	20
3.1.3 ผู้มีส่วนได้ส่วนเสียกับข้อมูล	21
3.2 นิยามและกฎเกณฑ์ที่เกี่ยวข้องกับข้อมูล (Definition and Rules)	23
3.2.1 สภาพแวดล้อมของธรรมาภิบาลข้อมูล	23
3.2.2 นิยามข้อมูล	24
3.2.3 กฎเกณฑ์ของข้อมูล/นโยบายข้อมูล	24
3.3 กระบวนการกำกับดูแลข้อมูล (Data Governance Process)	29
3.3.1 กระบวนการจัดการข้อมูลและการคุ้มครองข้อมูล	29
3.3.2 กระบวนการกำกับดูแลข้อมูล	49
3.3.3 การจัดการกระบวนการธรรมาภิบาลข้อมูล	50

สารบัญ(ต่อ)

	หน้า
บทที่ 4 การวัดการดำเนินการและความสำเร็จของธรรมาภิบาลข้อมูลภาครัฐ	53
4.1 การประเมินความพร้อมของธรรมาภิบาลข้อมูลภาครัฐ	54
4.2 การประเมินคุณภาพข้อมูล	55
4.3 การประเมินความมั่นคงปลอดภัยของข้อมูล	56
ภาคผนวก คำอธิบายข้อมูลหรือเมทาดาตาสำหรับชุดข้อมูลภาครัฐ	60
บรรณานุกรม	80

บทสรุปผู้บริหาร (Executive Summary)

ธรรมาภิบาลข้อมูลภาครัฐ (Data Governance) คือ กระบวนการหรือโครงสร้างที่ใช้ในการกำหนดนโยบาย ข้อกำหนด และกระบวนการที่เกี่ยวข้องกับการบริหารจัดการข้อมูลที่เกี่ยวข้องกับหน่วยงานของรัฐ ธรรมาภิบาลข้อมูลภาครัฐมุ่งเน้นการบริหารจัดการข้อมูลให้มีความเป็นระเบียบ มีความน่าเชื่อถือ และเป็นไปตามหลักการทางกฎหมาย โดยรวมถึงการกำหนดนโยบาย กรอบแนวทาง และข้อกำหนดในการเก็บรวบรวม ใช้ ประมวลผล และเผยแพร่ข้อมูลภาครัฐ

ธรรมาภิบาลข้อมูลภาครัฐมีความสำคัญในการสร้างความโปร่งใส ความน่าเชื่อถือ และความเป็นธรรมในการใช้ข้อมูลภาครัฐ โดยหลักการของธรรมาภิบาลข้อมูลภาครัฐเน้นการบริหารจัดการข้อมูลให้มีความรับผิดชอบต่อประชาชน สร้างความไว้วางใจและความเชื่อมั่นให้กับประชาชน และสร้างการควบคุมและตรวจสอบการใช้ข้อมูลให้มีประสิทธิภาพและป้องกันการละเมิดความเป็นส่วนตัวของข้อมูล

พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 ได้กำหนดให้หน่วยงานของรัฐต้องมีการบริหารจัดการและบูรณาการข้อมูลการทำงานให้มีความสอดคล้องและเชื่อมโยงเข้าด้วยกันอย่างมั่นคงปลอดภัยและมีธรรมาภิบาล โดยได้จัดทำคู่มือธรรมาภิบาลข้อมูลภาครัฐในระดับหน่วยงาน เพื่อนำไปสู่การเปิดเผยเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐผ่านระบบดิจิทัล และเปลี่ยนผ่านในการเป็นหน่วยงานที่ขับเคลื่อนด้วยข้อมูลอย่างมีคุณภาพ รักษาความเป็นส่วนบุคคล และมีความมั่นคงปลอดภัยในส่วนหลักการและแนวทางในการดำเนินการด้านธรรมาภิบาลข้อมูลภาครัฐนั้นให้เป็นไปตามประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัลเรื่องธรรมาภิบาลข้อมูลภาครัฐ ประกาศ ณ วันที่ 12 มีนาคม พ.ศ. 2563

ในปัจจุบันกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน (พพ.) ได้ตระหนักและเล็งเห็นถึงความสำคัญดังกล่าว จึงได้มีการจัดทำคู่มือธรรมาภิบาลข้อมูล (Data Governance Manual) โดยมีวัตถุประสงค์เพื่อกำหนดมาตรการ/แนวทางการดำเนินงานด้านการกำกับดูแลข้อมูลของ พพ. ให้เป็นไปตามมาตรฐาน และสามารถนำข้อมูลของหน่วยงานไปใช้ได้อย่างถูกวิธี ครบถ้วน สมบูรณ์ และเป็นปัจจุบัน รวมทั้งช่วยรักษาความเป็นส่วนบุคคลและสามารถเชื่อมโยงข้อมูลกับหน่วยงานภายนอกได้อย่างเป็นระบบและมีความมั่นคงปลอดภัย โดยการจัดทำคู่มือธรรมาภิบาลข้อมูลนั้น ได้ศึกษาจากธรรมาภิบาลข้อมูลภาครัฐและมาตรฐานต่าง ๆ ด้านการกำกับดูแลข้อมูลของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) เพื่อประกอบการจัดทำคู่มือฉบับนี้

จากการศึกษาธรรมาภิบาลข้อมูลของ พพ. พบว่า การขับเคลื่อนกระบวนการธรรมาภิบาลข้อมูล ของ พพ. ประกอบด้วยกระบวนการที่สำคัญ 7 กระบวนการ ได้แก่ กำหนดเป้าหมาย (Develop a Value Statement) กำหนดทิศทางการดำเนินการ (Prepare a Roadmap) วางแผนงานและงบประมาณ (Plan and Fund) ออกแบบแผนดำเนินการ (Design the Program) ประกาศใช้อย่างเป็นทางการ (Deploy the Program) ดำเนินการธรรมาภิบาลข้อมูล (Govern the Data) และติดตามการดำเนินงาน/วัดผลการดำเนินงาน/รายงานผลการดำเนินงาน (Monitor, Measure, Report) โดยกระบวนการต่าง ๆ นั้นถูกขับเคลื่อนโดยบุคลากรในส่วนต่าง ๆ ภายใต้โครงสร้างธรรมาภิบาลข้อมูล ประกอบด้วย คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council) ทีมบริการข้อมูล (Data Steward Team) และผู้มีส่วนได้ส่วนเสียกับข้อมูล (Data Stakeholders) ซึ่งจะมีบทบาทหน้าที่ที่เกี่ยวข้องกับข้อมูลในลักษณะที่แตกต่างกันออกไป ทั้งในด้านของการกำหนดนโยบายการขับเคลื่อนกระบวนการกำกับดูแลข้อมูลการผลิตและการนำข้อมูลไปใช้ให้เกิดประโยชน์ต่อองค์กรภาครัฐอย่างสูงสุด รวมทั้งเป็นไปตามระเบียบ ข้อบังคับและนโยบายขององค์กรภาครัฐอย่างเคร่งครัด

บทที่ 1

บทนำ

เนื้อหาในบทนี้จะกล่าวถึง หลักการเหตุผล ความเป็นมา วัตถุประสงค์ และนโยบายข้อมูล รวมทั้ง นิยามศัพท์ที่เกี่ยวข้อง เพื่อให้ผู้ศึกษาทราบถึงรายละเอียดในเบื้องต้น และสร้างความเข้าใจในคำศัพท์เชิง เทคนิคต่าง ๆ เพื่อให้การศึกษาในบทถัดไปเกิดความเข้าใจได้โดยง่าย โดยประกอบด้วยผลการศึกษาต่าง ๆ ดังต่อไปนี้

1.1 ความเป็นมา

ปัจจุบันโลกได้ก้าวเข้าสู่ยุคดิจิทัล (Digital Era) อย่างเต็มรูปแบบ ซึ่งได้ก่อให้เกิดเทคโนโลยีสมัยใหม่ที่ได้ เข้ามาช่วยสนับสนุนการดำเนินงานในภาคส่วนต่าง ๆ เป็นจำนวนมาก ทั้งในด้านของเกษตรกรรม อุตสาหกรรม และการบริการต่าง ๆ รวมทั้งพฤติกรรมบุคคล ลูกค้า และผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับการดำเนินงานของ องค์กร โดยมีการนำเทคโนโลยีสมัยใหม่เข้ามาช่วยในการทำกิจกรรมต่าง ๆ มากขึ้น เช่น การสื่อสารผ่านสื่อ สังคมออนไลน์ การสั่งซื้อสินค้าออนไลน์ หรือการทำธุรกรรมออนไลน์ เป็นต้น โดยพฤติกรรมเหล่านี้มีแนวโน้ม ที่จะสูงขึ้นเรื่อย ๆ เพราะช่วยเอื้ออำนวยความสะดวก รวดเร็ว และประหยัดค่าใช้จ่าย ประกอบกับเทคโนโลยีมี การพัฒนาขึ้นอย่างต่อเนื่องเพื่อสนับสนุนและรองรับความต้องการของทุกภาคส่วน ซึ่งผลที่เกิดขึ้นดังกล่าว ทำให้ในปัจจุบันมีข้อมูลข่าวสารเกิดขึ้นเป็นจำนวนมาก ทั้งในรูปแบบมีโครงสร้าง กึ่งโครงสร้าง และไม่มี โครงสร้าง โดยในหลายองค์กรสามารถใช้ประโยชน์จากการเกิดขึ้นของข้อมูลจำนวนมาก มาช่วยสนับสนุนการ ดำเนินงานขององค์กรให้มีประสิทธิภาพมากขึ้น แต่บางหน่วยงานกลับขาดกลไกการตรวจสอบ และกำกับดูแล อย่างถูกต้อง ทำให้ส่งผลกระทบต่อการทำงานขององค์กรตามมาในภายหลัง

การกำกับดูแลข้อมูลหรือธรรมาภิบาลข้อมูล (Data Governance) จึงได้เข้ามามีบทบาทสำคัญในการ ส่งเสริมการใช้งานและบริหารจัดการข้อมูลอย่างเหมาะสม ทั้งในด้านการตัดสินใจ การกำหนดสิทธิ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน และการรักษาความมั่นคงปลอดภัยของข้อมูล ทำให้หลายหน่วยงาน จึงได้มีการกำหนดหลักเกณฑ์ เพื่อใช้เป็นแนวทางการดำเนินงานขององค์กรอย่างเหมาะสม เช่น ธรรมาภิบาล ข้อมูลภาครัฐของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) การกำกับดูแลข้อมูลบริหารจัดการข้อมูล ขนาดใหญ่ขององค์กรของสำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ และการกำกับดูแลข้อมูลของสถาบันการ กำกับดูแลข้อมูล (The Data Governance Institute)

ดังนั้น พพ. ได้ตระหนักและเล็งเห็นถึงความสำคัญดังกล่าว จึงได้มีการจัดทำคู่มือธรรมาภิบาลข้อมูล (Data Governance Manual) ขึ้น เพื่อใช้เป็นแนวทางปฏิบัติในการกำกับดูแลข้อมูลให้กับผู้บริหาร เจ้าหน้าที่ ตลอดจนผู้มีส่วนได้ส่วนเสียต่าง ๆ ที่เกี่ยวข้อง ให้สามารถมีวิธีการใช้ข้อมูลได้อย่างถูกต้อง เหมาะสม และ เกิดประโยชน์ในกระบวนการงานของ พพ. ต่อไป

1.2 วัตถุประสงค์

1.2.1 เพื่อดำเนินการจัดทำธรรมาภิบาลข้อมูลภาครัฐของกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน เป็นไปตามข้อกำหนดในพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562

1.2.2 เพื่อให้มีกรอบธรรมาภิบาลข้อมูลสำหรับช่วยในการวางแผนทางบริหารจัดการข้อมูลให้มีคุณภาพ มีความเป็นปัจจุบัน สอดคล้องกับความต้องการของผู้ประกอบการ ประชาชน และผู้มีส่วนได้ส่วนเสีย

1.2.3 เพื่อนำข้อมูลที่มีคุณภาพไปใช้ประโยชน์ได้อย่างถูกต้อง ครบถ้วนสมบูรณ์ และเป็นปัจจุบัน รวมทั้ง มีการจัดเก็บข้อมูลที่มีมาตรฐาน ช่วยรักษาความเป็นส่วนบุคคล และสามารถเชื่อมโยงข้อมูลกับหน่วยงาน ภายนอกได้อย่างเป็นระบบและมีความมั่นคงปลอดภัย

1.3 นโยบายข้อมูล

พพ. ได้กำหนดนโยบายธรรมาภิบาลข้อมูลเพื่อเป็นกลไกในการขับเคลื่อนงานด้านธรรมาภิบาลข้อมูล โดยแบ่งออกเป็น 2 ส่วน ได้แก่ การกำหนดนโยบายข้อมูลตามมาตรฐาน และหลักเกณฑ์การเปิดเผยข้อมูลเปิด ภาครัฐ ในรูปแบบข้อมูลดิจิทัลต่อสาธารณะของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) และมาตรฐาน ISO 27001 ดังนี้

1.3.1 การกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร เพื่อให้ภาครัฐทุกแห่ง มีแนวทางการดำเนินงานไปในทิศทางเดียวกัน โดยสาระสำคัญของการกำกับดูแลข้อมูลและการบริหารจัดการ ข้อมูลขนาดใหญ่ขององค์กร มีดังนี้

1.3.1.1 มีการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ของ องค์กรที่ครอบคลุมถึงกระบวนการกำกับดูแลข้อมูล โครงสร้างการกำกับดูแลข้อมูล นโยบายข้อมูล และการตรวจสอบ การวัดประสิทธิภาพกระบวนการและคุณภาพข้อมูล และการวัดความคุ้มค่าและการ ปรับปรุงอย่างต่อเนื่อง

1.3.1.2 กำหนดข้อมูลและสารสนเทศที่สำคัญขององค์กร

1.3.1.3 มีการกำหนดสิทธิ หน้าที่ และความรับผิดชอบของผู้มีส่วนได้ส่วนเสียในการบริหารจัดการ ข้อมูลทุกขั้นตอน เพื่อให้การได้มาและการนำไปใช้ข้อมูลของหน่วยงาน ได้ถูกต้องแม่นยำ ครบถ้วน เป็นปัจจุบัน และใช้งานง่าย

1.3.2 มาตรฐาน ISO 27001

ISO 27001 เป็นมาตรฐานสากลสำหรับระบบการจัดการความปลอดภัยของข้อมูล (Information Security Management Systems) ในด้านต่าง ๆ เช่น การป้องกันโปรแกรมไม่ประสงค์ดี การบริหารจัดการ ทรัพย์สินสารสนเทศ หรือเข้าพื้นที่โดยบุคคลภายนอก เป็นต้น โดยจะเห็นได้ว่าการจัดการความปลอดภัยของ ข้อมูลเป็นส่วนหนึ่งของการกำกับดูแลข้อมูล เพื่อให้ข้อมูลมีความปลอดภัยในการนำไปใช้งานไม่ขัดต่อระเบียบ ข้อบังคับ หรือส่งผลกระทบต่อเชิงลบใด ๆ ต่อ พพ. โดยมีตัวอย่างนโยบายที่เกี่ยวข้อง ดังนี้

1.3.2.1 นโยบายการเข้ารหัสข้อมูล

1.3.2.2 นโยบายการรักษาความมั่นคงปลอดภัยของการควบคุมการเข้าถึงระบบ

1.3.2.3 นโยบายความมั่นคงปลอดภัยของการสำรองข้อมูล

1.3.2.4 นโยบายการโอนถ่ายข้อมูลสารสนเทศ

1.4 นิยามศัพท์ที่เกี่ยวข้องกับธรรมาภิบาลข้อมูล

คู่มือธรรมาภิบาลข้อมูลฉบับนี้ ได้กำหนดนิยามศัพท์ไว้ดังต่อไปนี้

ตารางที่ 1.1 นิยามศัพท์คู่มือธรรมาภิบาลข้อมูลของ พพ.

คำศัพท์	คำนิยาม
การกำกับดูแลข้อมูล หรือธรรมาภิบาลข้อมูล (Data Governance)	การกำหนดแนวทางการดำเนินงานด้านข้อมูลของ พพ. ที่ครอบคลุมถึง สิทธิ หน้าที่ และความรับผิดชอบของผู้บริหาร เจ้าหน้าที่ และผู้มีส่วนได้ส่วนเสียต่าง ๆ เพื่อให้สามารถนำข้อมูลไปใช้งานได้อย่างถูกต้อง เหมาะสม และก่อให้เกิด ประโยชน์ต่อองค์กรได้อย่างสูงสุด
คำอธิบายชุดข้อมูลดิจิทัล หรือเมทาดาตา (Metadata)	ข้อมูลที่ใช้กำกับและอธิบายกลุ่มของข้อมูลอื่น ซึ่งจะช่วยให้ทราบรายละเอียด หรือลักษณะของข้อมูลดังกล่าวมากขึ้น โดยสามารถแบ่งออกเป็น 2 กลุ่ม ได้แก่ เมทาดาตาเชิงธุรกิจ (Business Metadata) และเมทาดาตาเชิงเทคนิค (Technical Metadata)
หมวดหมู่ของข้อมูล (Data Category)	หมวดหมู่ของข้อมูลสามารถแบ่งออกเป็น 5 หมวด ได้แก่ ข้อมูลสาธารณะ ข้อมูลใช้ภายใน ข้อมูลส่วนบุคคล ข้อมูลความลับของทางราชการ และข้อมูล ความมั่นคง
บัญชีข้อมูล (Data Catalog)	รายการชุดข้อมูลที่ พพ. ถือครองและบริหารจัดการ ประกอบด้วย ข้อมูลของ กลุ่มภารกิจการอนุรักษ์พลังงาน ข้อมูลของกลุ่มภารกิจการใช้พลังงาน ข้อมูล ของกลุ่มภารกิจการผลิตพลังงานทดแทน ข้อมูลของกลุ่มภารกิจรายชื่อโรงงาน/ อาคารควบคุม และข้อมูลของกลุ่มภารกิจบริหารและอำนวยการ
พจนานุกรมข้อมูล (Data Dictionary)	พจนานุกรมข้อมูลที่แสดงรายละเอียดตารางในฐานข้อมูล (Database) ซึ่งประกอบด้วย รีเลชัน (Relation Name) แอตทริบิวต์ (Attribute) ชื่อแทน (Aliases Name) รายละเอียดข้อมูล (Data Description) แอตทริบิวโดเมน (Attribute Domain) ฯลฯ ทำให้สามารถค้นหารายละเอียดที่ต้องการได้ สะดวกมากยิ่งขึ้น

บทที่ 2

แนวคิดธรรมาภิบาลข้อมูล

ในบทนี้ได้กล่าวถึงแนวคิด (Concept) ที่เกี่ยวข้องกับธรรมาภิบาลข้อมูล เพื่อให้ทราบถึงพื้นฐานของหลักการ (Principles) นิยาม (Definition) และความสัมพันธ์ระหว่างองค์ประกอบต่าง ๆ ที่เกี่ยวข้องกับการกำกับดูแลข้อมูล ซึ่งประโยชน์ของการศึกษาในส่วนนี้จะช่วยให้ พพ. มีกรอบในการกำกับดูแลข้อมูลที่ต้องปฏิบัติตามหลักการทางวิชาการ ที่ได้มีการศึกษาจากเอกสารทางวิชาการที่ได้รับการยอมรับจากทั้งในและต่างประเทศ โดยประกอบด้วยการศึกษาในประเด็นต่าง ๆ ได้แก่ ธรรมาภิบาลข้อมูล ข้อมูล และการบริหารจัดการข้อมูล ซึ่งสามารถอธิบายได้ ดังต่อไปนี้

2.1 ธรรมาภิบาลข้อมูล (Data Governance)

2.1.1 นิยามของธรรมาภิบาลข้อมูล (Definition)

การกำกับดูแลข้อมูลหรือธรรมาภิบาลข้อมูล (Data Governance) มีผู้เชี่ยวชาญจากหน่วยงานต่าง ๆ ให้คำนิยามไว้ดังนี้

- "กิจกรรมที่ประกอบด้วยการกำหนดอำนาจ การควบคุม และการตัดสินใจในการบริหารจัดการข้อมูล โดยข้อมูลถูกจัดให้เป็นหนึ่งในทรัพย์สินของหน่วยงาน" (Askham, N., 2016)
- "ระบบที่กำหนดถึงอำนาจการตัดสินใจ และหน้าที่ความรับผิดชอบต่อกระบวนการที่เกี่ยวข้องกับข้อมูล โดยที่มีแบบแผนที่ชัดเจนและได้รับการยอมรับ ซึ่งแบบแผนดังกล่าวต้องสามารถอธิบายได้ว่า ใครมีบทบาทในการทำอะไรกับข้อมูลชุดไหน เมื่อไร ใช้หลักการและวิธีการอย่างไรในการใช้ข้อมูล" (Thomas, 2009)
- "การกำหนดสิทธิและการควบคุม (การวางแผน การตรวจสอบ และการบังคับ) ในการบริหารจัดการข้อมูล" (Henderson et al., 2017)
- "การจัดการข้อมูลจากมุมมองที่เกี่ยวข้องกับข้อมูล ทำให้หน่วยงานตระหนักถึงการจัดทำมาตรฐานข้อมูลที่เป็นระบบและการบูรณาการข้อมูล ทั้งข้อมูลที่อยู่ในระบบข้อมูลที่สัมพันธ์กับการดำเนินงานของหน่วยงาน นโยบาย และกระบวนการปฏิบัติงานต่าง ๆ" (Kim, H. Y., & Cho, J. S., 2017)

จากนิยามข้างต้น จึงสามารถสรุปได้ว่า การกำกับดูแลข้อมูลหรือธรรมาภิบาลข้อมูล หมายถึง "การกำหนดสิทธิในการตัดสินใจและความรับผิดชอบ ในการส่งเสริมให้เกิดกระบวนการจัดทำ การใช้งาน และการบริหารจัดการข้อมูล รวมถึงกระบวนการที่กำหนดบทบาท นโยบาย และมาตรฐานที่ช่วยสนับสนุนให้การดำเนินงานเกี่ยวกับข้อมูลมีประสิทธิภาพมากยิ่งขึ้น ซึ่งส่งผลให้หน่วยงานสามารถบรรลุเป้าหมายได้"

2.1.2 กฎเกณฑ์ในการกำกับดูแลข้อมูล (Rules)

การกำหนดหลักเกณฑ์ในการกำกับดูแลข้อมูล จะใช้เป็นแนวทางในการดำเนินงานขององค์กรให้เป็นไปในทิศทางเดียวกัน โดยแนวทางการดำเนินงานด้านการกำกับดูแลข้อมูลขององค์กรจะต้องครอบคลุมถึงกระบวนการกำกับดูแลข้อมูล โครงสร้างการกำกับดูแลข้อมูล นโยบายข้อมูลและการตรวจสอบ การวัดประสิทธิภาพกระบวนการและคุณภาพข้อมูล โดยแนวทางการดำเนินงานดังกล่าว มีลักษณะเป็นระดับวุฒิภาวะ (Mutuality Level) ที่ช่วยยกระดับการดำเนินงานด้านการกำกับดูแลข้อมูลของภาครัฐให้สูงขึ้นตามลำดับ ดังนี้

ตารางที่ 2.1 ระดับการกำกับดูแลข้อมูล

ระดับที่	แนวทางการดำเนินงาน
ระดับที่ 1 ผู้เริ่มต้น (Beginner)	มีการดำเนินการด้านการกำกับดูแลข้อมูล
ระดับที่ 2 ปานกลาง (Intermediate)	- มีกระบวนการกำกับดูแลข้อมูลที่เป็นมาตรฐานส่วนงาน/บริการ - มีโครงสร้างการกำกับดูแลข้อมูล - มีการกำหนดผู้กำกับดูแลในแต่ละส่วนงาน/บริการ - มีนโยบายข้อมูลและการตรวจสอบบังคับใช้ในส่วนงาน/บริการ
ระดับที่ 3 เพียงพอ (Sufficient)	- มีกระบวนการกำกับดูแลข้อมูลที่เป็นมาตรฐานหน่วยงาน - มีโครงสร้างการกำกับดูแลข้อมูลที่ชัดเจน - มีส่วนงานกลางในการกำกับดูแลซึ่งประกอบไปด้วยบุคคลด้านธุรกิจ และเทคโนโลยีสารสนเทศ - มีนโยบายข้อมูลและการตรวจสอบบังคับใช้ทั้งหน่วยงาน - มีการวัดคุณภาพข้อมูล
ระดับที่ 4 ก้าวหน้า (Progressive)	- มีกระบวนการกำกับดูแลข้อมูลที่เป็นมาตรฐานหน่วยงาน - มีโครงสร้างการกำกับดูแลข้อมูลที่ชัดเจน - มีส่วนงานกลางในการกำกับดูแลข้อมูล - มีการวัดประสิทธิภาพกระบวนการและคุณภาพข้อมูล
ระดับที่ 5 ขั้นสูง (Advanced)	- มีกระบวนการกำกับดูแลข้อมูลที่เป็นมาตรฐานหน่วยงาน - มีโครงสร้างการกำกับดูแลข้อมูลที่ชัดเจน - มีส่วนงานกลางในการกำกับดูแล - มีการวัดประสิทธิภาพกระบวนการและคุณภาพข้อมูล - มีการวัดความคุ้มค่าและดำเนินการปรับปรุงกระบวนการอย่างต่อเนื่อง - มีการใช้ข้อมูลในรูปแบบที่หลากหลายจากแหล่งข้อมูลที่มีความแตกต่างกันนำมาใช้วิเคราะห์ร่วมกัน เพื่อปรับปรุงทิศทางการดำเนินธุรกิจ

ทั้งนี้ การดำเนินงานตามระดับวุฒิภาวะดังกล่าว จะต้องดำเนินการตามกิจกรรมต่าง ๆ ที่กำหนดไว้ในแต่ละระดับให้ครบถ้วน จึงจะสามารถผ่านเกณฑ์การประเมินในแต่ละระดับที่กำหนดไว้ จากนั้นจึงเข้าสู่การประเมินในระดับถัดไป ซึ่งภาครัฐจะไม่สามารถประเมินข้ามระดับได้

2.1.3 องค์ประกอบหลักของธรรมาภิบาลข้อมูลที่ดี

ธรรมาภิบาลข้อมูลเป็นการกำหนดสิทธิในการตัดสินใจและความรับผิดชอบในการส่งเสริมให้เกิดกระบวนการจัดทำ การใช้งาน และการบริหารจัดการข้อมูล รวมถึงกระบวนการที่กำหนดบทบาท นโยบาย และมาตรฐานที่ช่วยสนับสนุนให้การดำเนินงานเกี่ยวกับข้อมูลมีประสิทธิภาพมากยิ่งขึ้น ซึ่งส่งผลให้หน่วยงาน

สามารถบรรลุเป้าหมายได้ โดย Intragovernmental Group on Geographic Information (IGGI, 2005) ได้ให้องค์ประกอบหลักของธรรมาภิบาลข้อมูลที่ดี ประกอบด้วย

- 1) มีความมั่นคงปลอดภัยและรักษาความเป็นส่วนตัวส่วนบุคคลโดยมีมาตรการในการรักษาความมั่นคงปลอดภัย และความเป็นส่วนตัว ซึ่งช่วยป้องกันความเสียหายที่จะเกิดขึ้นกับข้อมูล และการละเมิดสิทธิส่วนบุคคล
- 2) มีมาตรการควบคุมและจัดการวงจรชีวิตของข้อมูลประกอบด้วย การประเมินธุรกิจ การกำหนดประเภทและแนวทางการแบ่งประเภทของชุดข้อมูล มีการตรวจสอบอย่างต่อเนื่อง ทั้งการเก็บข้อมูล และการทำลายข้อมูล
- 3) มีนโยบายการใช้ข้อมูลที่ชัดเจน โดยกำหนดนโยบายและกฎเกณฑ์ของข้อมูลเป็นกรอบสำหรับการบริหารจัดการและกำกับดูแลข้อมูล
- 4) มีการกำหนดบทบาทหน้าที่ของเจ้าของข้อมูลโดยกำหนดวิธีการที่ผู้ดูแลข้อมูลหรือเจ้าของข้อมูลสามารถจัดการเปลี่ยนแปลงหรือส่งผ่านข้อมูลให้ชัดเจน เพื่อไม่ให้เกิดปัญหาในกรณีที่ชุดข้อมูล หรือฐานข้อมูลบางแหล่งอาจจะมีผู้ดูแล ผู้ใช้งาน หรือเจ้าของข้อมูลหลายคนหรือหลายหน่วยงาน
- 5) ข้อมูลมีเมทาดาตา โดยเมทาดาตาจะช่วยให้ผู้ใช้งานเข้าใจว่า ข้อมูลชุดนี้คือข้อมูลที่เกี่ยวข้องกับอะไร สามารถนำไปใช้งานอย่างไร และมีข้อจำกัดอะไรบ้าง อีกทั้งยังควรจัดทำเมทาดาตาให้เป็นไปตามมาตรฐาน เพื่อช่วยอำนวยความสะดวกในการสืบค้นข้อมูล และใช้ประโยชน์ในการจัดทำบัญชีข้อมูลของหน่วยงาน
- 6) ข้อมูลมีคุณภาพ โดยมีมาตรการในการควบคุมคุณภาพของข้อมูลให้มีคุณภาพสูง ซึ่งจะสนับสนุนให้การดำเนินงานของหน่วยงานเป็นไปอย่างมีประสิทธิภาพและประสิทธิผล

2.2 ข้อมูล (Data)

ข้อมูล (Data) หมายถึง "ข้อเท็จจริงซึ่งใช้เป็นพื้นฐานสำหรับการอธิบายเหตุผล การสนทนา หรือการคำนวณ" (Australian Institute of Health and Welfare, 2014) ข้อมูลถือเป็นองค์ประกอบหลักในการขับเคลื่อนหน่วยงาน ซึ่งมีความสัมพันธ์กับกระบวนการปฏิบัติงานเทคโนโลยีสารสนเทศ สถานที่ รวมถึงบุคลากร

ข้อมูลจึงเปรียบเสมือนทรัพย์สินที่มีความสำคัญเช่นเดียวกับทรัพย์สินประเภทอื่น หน่วยงานจึงจำเป็นต้องมีมาตรการในการรักษาความมั่นคงปลอดภัยและคุณภาพของข้อมูล เช่น การรักษาความลับของข้อมูล (Confidentiality) การป้องกันไม่ให้เกิดเหตุการณ์ที่ทำให้ไม่สามารถใช้งานข้อมูลได้ (Loss of Availability) การรักษาความถูกต้องครบถ้วนของข้อมูล (Integrity) และการทำให้ข้อมูลเป็นปัจจุบันอยู่เสมอ (Timeliness) ทั้งนี้ เพื่อสนับสนุนการตัดสินใจทั้งในระดับปฏิบัติการและระดับยุทธศาสตร์ให้มีประสิทธิภาพมากยิ่งขึ้น



รูปที่ 2.1 ประเภทข้อมูล

2.2.1 ประเภทข้อมูล (Types of Data)

ข้อมูลถูกจัดแบ่งออกได้เป็น 3 ประเภท ดังนี้

1) ข้อมูลแบบมีโครงสร้าง (Structured Data)

ข้อมูลแบบมีโครงสร้างหรือข้อมูลเชิงโครงสร้างเป็นข้อมูลที่มีการจัดรูปแบบของข้อมูลที่ชัดเจน เป็นระเบียบอยู่ในรูปแบบเดียวกัน สามารถจัดเก็บในรูปแบบฐานข้อมูลเชิงสัมพันธ์ (Relational Database) ได้ ทำให้ง่ายต่อการนำมาวิเคราะห์หรือใช้ประโยชน์ในด้านต่าง ๆ ข้อมูลประเภทนี้ส่วนใหญ่จะมีลักษณะเป็น ตัวเลข หรือข้อความสั้น ๆ

ตารางที่ 2.2 ตัวอย่างข้อมูลแบบมีโครงสร้าง

ลำดับที่	ชื่อ	เลขที่ทะเบียน	ประเภท	จังหวัด
1				
2				

2) ข้อมูลกึ่งโครงสร้าง (Semi-Structured Data)

ข้อมูลกึ่งโครงสร้างเป็นข้อมูลที่ถูกจัดเก็บอย่างมีรูปแบบในระดับหนึ่ง สามารถค้นหา (Search) หรือติดตาม (Tag) ได้ ตัวอย่างของข้อมูลประเภทนี้ เช่น เว็บเพจ คำสำคัญในเพจ เป็นต้น

3) ข้อมูลแบบไม่มีโครงสร้าง (Unstructured Data)

ข้อมูลแบบไม่มีโครงสร้าง หรือข้อมูลไร้โครงสร้างเป็นข้อมูลที่มีรูปแบบหลากหลาย ไม่แน่นอน สามารถเป็นได้ทั้งข้อความ เสียง ภาพ และวิดีโอ ไม่สามารถจัดเก็บในรูปแบบฐานข้อมูลเชิงสัมพันธ์ (Relational Database) ได้ด้วยรูปแบบที่ไม่มีความชัดเจนเป็นมาตรฐานเดียวกัน ทำให้ก่อนการนำข้อมูล ประเภทนี้จึงต้องมีการตรวจสอบ กรั่นกรอง หรือทำความสะอาดข้อมูล (Data Cleansing) ก่อน

2.2.2 ชุดข้อมูล (Datasets)

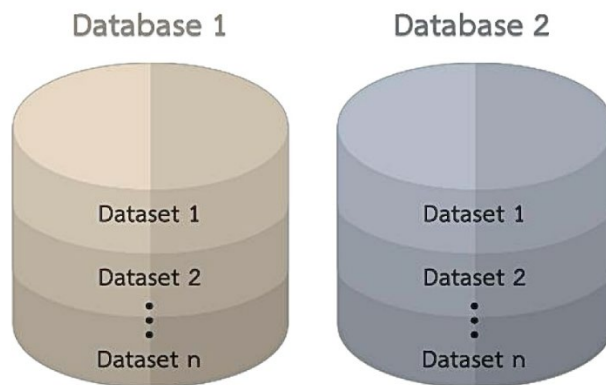
ชุดข้อมูล หมายถึง "ข้อมูลที่มีการรวบรวมไว้ โดยปกติอยู่ในรูปแบบของตารางข้อมูล" (Askham et al., 2013) ซึ่งการรวบรวมข้อมูลนี้มาจากหลายแหล่งและนำมาจัดเป็นชุดให้ถูกต้องตามลักษณะโครงสร้างข้อมูลที่กำหนดไว้ ตัวอย่างเช่น ตารางที่ 2.3 แสดงชุดข้อมูลพนักงานในรูปแบบตารางข้อมูลหรือข้อมูลที่มีโครงสร้าง (Structured Data) โดยมีทั้งหมด 3 แถว และ 5 ฟิลด์ (Data Field/Element/Attribute) ได้แก่ ชื่อ, นามสกุล, เพศ, อายุ และระดับการศึกษา

ตารางที่ 2.3 ตัวอย่างชุดข้อมูลพนักงาน

ชื่อ	นามสกุล	เพศ	อายุ	ระดับการศึกษา
เฉลิมเดช	ประพันธ์โรจน์	ชาย	27	ปริญญาตรี
นัฐพงษ์	โกศล	ชาย	25	ปริญญาตรี
นพมาศ	ใจบุญ	หญิง	29	ปริญญาโท

2.2.3 ฐานข้อมูล (Database)

ฐานข้อมูล คือ "กลุ่มข้อมูลที่มีความสัมพันธ์กันได้ถูกรวบรวมเข้าไว้ด้วยกัน ซึ่งสนับสนุนกิจกรรมของหน่วยงาน" (Malinowski, E. & Zimanyi, E., 2009) หรือกล่าวได้ว่า แต่ละฐานข้อมูลจะประกอบไปด้วยหลายๆ ชุดข้อมูลที่มีความสัมพันธ์กันดังแสดงในรูปที่ 2.2



รูปที่ 2.2 ความสัมพันธ์ระหว่างฐานข้อมูลกับชุดข้อมูล

2.3 การบริหารจัดการข้อมูล

การบริหารจัดการข้อมูล หมายถึง "กระบวนการที่ใช้ในการวางแผน (Plan) ระบุ (Specify) เปิดใช้งาน (Enable) สร้าง (Create) รับ (Acquire) ดูแลรักษา (Maintain) ใช้ (Use) จัดเก็บถาวร (Archive) ดึงข้อมูล (Retrieve) ควบคุม (Control) และทำลายข้อมูล (Purge)" (Cupola et al., 2014) การบริหารจัดการข้อมูลเป็นสิ่งสำคัญสำหรับทุกหน่วยงาน ซึ่งแต่ละหน่วยงานต้องตระหนักว่าข้อมูลที่มีอยู่เป็นทรัพย์สินที่มีค่าและเกิดขึ้นจากข้อมูล

จำนวนมหาศาล ไม่ว่าจะเป็นข้อมูลที่รวบรวมมาจากระบบหรืออุปกรณ์ต่าง ๆ โดยอัตโนมัติ หรือข้อมูลที่เกิดจากการป้อนข้อมูลหรือโต้ตอบกับผู้ใช้ งาน จำเป็นต้องได้รับการบริหารจัดการอย่างถูกต้องเหมาะสม และสอดคล้องกับวัตถุประสงค์ของหน่วยงาน เพื่อให้การบริหารจัดการข้อมูลมีประสิทธิภาพ หน่วยงานต้องดำเนินการดังนี้

- 1) จัดเก็บ นำมาใช้งาน และประมวลผลข้อมูลตามที่หน่วยงานต้องการ
- 2) ควบคุม ตรวจสอบ และป้องกัน โดยใช้กระบวนการธรรมาภิบาลข้อมูลภาครัฐและความปลอดภัยของข้อมูล
- 3) จัดหมวดหมู่ และกำหนดมาตรฐานของข้อมูล โดยใช้การจำแนกข้อมูล และกำหนดกรอบการทำงานที่เป็นที่รู้จักแพร่หลาย
- 4) กำหนดข้อมูลให้อยู่ในรูปแบบที่เรียกใช้ได้อย่างมีประสิทธิภาพเพื่อให้สามารถนำข้อมูลกลับมาใช้ได้ใหม่ภายหลัง
- 5) ปรับปรุงข้อมูลให้เป็นปัจจุบัน และมีความถูกต้องสมบูรณ์อยู่เสมอ
- 6) ปกป้องข้อมูลจากการลักลอบใช้งานหรือแก้ไขโดยไม่ชอบ รวมถึงจากภัยธรรมชาติหรือความบกพร่องภายในระบบคอมพิวเตอร์

การบริหารจัดการข้อมูลต้องครอบคลุม และมีองค์ประกอบตามระบบบริหารและกระบวนการจัดการข้อมูล หรือวงจรชีวิตของข้อมูล ดังรูป 2.3



รูปที่ 2.3 ระบบบริหารและกระบวนการจัดการข้อมูล หรือวงจรชีวิตของข้อมูล และองค์ประกอบในการบริหารจัดการข้อมูล

2.3.1 ระบบบริหารและกระบวนการจัดการข้อมูล

ระบบบริหารและกระบวนการจัดการข้อมูล (Data Life Cycle) หรือวงจรชีวิตของข้อมูล คือ “ลำดับขั้นตอนของข้อมูลตั้งแต่เริ่มสร้างข้อมูลไปจนถึงการทำลายข้อมูล” ประกอบด้วย 6 ขั้นตอน ดังนี้ (ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล, 2563 12-13)

- 1) กระบวนการสร้างข้อมูล (Create) เป็นการสร้างข้อมูลขึ้นมาใหม่ โดยวิธีการบันทึกเข้าไปด้วยบุคคล หรือบันทึกอัตโนมัติด้วยอุปกรณ์อิเล็กทรอนิกส์ เช่น อุปกรณ์ตรวจจับสัญญาณ (Sensor) รวมถึงการซื้อข้อมูล หรือการรับข้อมูลจากหน่วยงานอื่น เพื่อนำมาจัดเก็บในภายหลัง
- 2) กระบวนการจัดเก็บข้อมูล (Store) เป็นการจัดเก็บข้อมูลที่เกิดจากกระบวนการสร้าง หรือข้อมูลที่ได้จากการแลกเปลี่ยนกับหน่วยงานอื่น เพื่อให้มีระเบียบ ง่ายต่อการใช้งาน ไม่สูญหาย หรือถูกทำลาย และให้ผู้ใช้สามารถประมวลผลข้อมูลต่าง ๆ ตามความต้องการได้อย่างรวดเร็ว ไม่ว่าจะจัดเก็บลงแฟ้มข้อมูล (File) หรือระบบการจัดการฐานข้อมูล (Database Management System - DBMS)
- 3) กระบวนการใช้ข้อมูล (Use) เป็นการนำข้อมูลที่จัดเก็บมาประมวลผล เช่น การถ่ายโอนข้อมูล การเปลี่ยนรูปแบบการจัดเก็บข้อมูล การวิเคราะห์ข้อมูล การจัดทำรายงาน เพื่อนำข้อมูลเหล่านั้นมาใช้งานให้เกิดประโยชน์ตามวัตถุประสงค์ รวมถึงการสำรอง (Backup) ข้อมูล โดยการคัดลอกข้อมูลที่ใช้ภายในปัจจุบันเพื่อทำสำเนา เช่น การใช้โปรแกรมในการสำรองข้อมูลเป็นการหลีกเลี่ยงความเสียหายที่จะเกิดขึ้น หากข้อมูลเกิดการเสียหายหรือสูญหาย ซึ่งสามารถนำข้อมูลที่สำรองไว้ในสื่อบันทึกข้อมูลกลับมาใช้งานได้ทันที โดยการกู้คืน (Restore)
- 4) กระบวนการเผยแพร่ข้อมูล (Publish) เป็นการแชร์ข้อมูล (Sharing) การกระจายข้อมูล (Dissemination) การควบคุมการเข้าถึง (Access Control) การแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน (Exchange) และการกำหนดเงื่อนไขในการนำข้อมูลไปใช้ (Condition)
- 5) กระบวนการจัดเก็บข้อมูลถาวร (Archive) เป็นการคัดลอกเอาข้อมูลที่มีช่วงอายุเกินช่วงใช้งาน หรือไม่ได้ใช้งานแล้ว เพื่อทำสำเนาสำหรับการเก็บรักษา โดยที่ข้อมูลนั้นไม่มีการลบ ปรับปรุง หรือแก้ไขอีก และสามารถนำกลับไปใช้งานได้ใหม่เมื่อต้องการ
- 6) กระบวนการทำลายข้อมูล (Destroy) เป็นการทำลายข้อมูล ซึ่งปกติจะเป็นการทำลายข้อมูลที่มีการจัดเก็บถาวรเป็นระยะเวลานานหรือเกินกว่าระยะเวลาที่กำหนด

2.3.2 องค์ประกอบในการบริหารจัดการข้อมูล (Data Management Component)

DAMA International (Henderson et al., 2017) ได้อธิบายถึงแนวคิดในการบริหารจัดการซึ่งประกอบด้วยองค์ประกอบในด้านต่าง ๆ ดังต่อไปนี้

2.3.2.1 สถาปัตยกรรมข้อมูล (Data Architecture)

เป็นส่วนหนึ่งของการพัฒนาสถาปัตยกรรมองค์กร (Enterprise Architecture) เป็นการอธิบายเกี่ยวกับกลุ่มของข้อมูลทั้งหมดที่มีในหน่วยงาน ความสัมพันธ์ระหว่างข้อมูลกับกระบวนการปฏิบัติงาน ความสัมพันธ์ระหว่างข้อมูลกับแอปพลิเคชัน สถาปัตยกรรมเทคโนโลยีข้อมูล สถาปัตยกรรมการบูรณาการข้อมูล สถาปัตยกรรมเมทาดาตา เป็นต้น สถาปัตยกรรมข้อมูลจะอยู่ในรูปแบบของแบบจำลองข้อมูลที่ทำให้มองเห็นภาพรวม ความเชื่อมโยง และการไหลของข้อมูลในระดับต่าง ๆ ทั้งหมดของหน่วยงาน ทั้งที่เป็นหน่วยงานต้นน้ำกลางน้ำ หรือปลายน้ำ สามารถอธิบายสถานะที่มีอยู่ในปัจจุบัน และกำหนดความต้องการสำหรับอนาคต เพื่อให้หน่วยงานเกิดความเข้าใจและเห็นเป็นภาพเดียวกัน ดังนั้นจึงเป็นพื้นฐานที่สำคัญในการวางแผนบริหารจัดการข้อมูล

2.3.2.2 การจำลองและการออกแบบข้อมูล (Data Modeling and Design)

เป็นวิธีการวิเคราะห์ความต้องการของผู้ใช้งาน รวมถึงการระบุข้อกำหนดและแก้ปัญหาต่าง ๆ ที่เกี่ยวข้อง โดยแบบจำลองข้อมูลจะแสดงในรูปแบบของไดอะแกรม (Diagram) ที่ออกแบบโครงสร้างของข้อมูล

เพื่อใช้ในการสื่อสารภายในหน่วยงานให้เข้าใจตรงกัน แบบจำลองข้อมูลนี้แสดงถึงความสัมพันธ์ระหว่างข้อมูลที่เกี่ยวข้องกัน พร้อมทั้งรายละเอียดของโครงสร้างข้อมูล โดยแบ่งออกเป็น 3 ระดับ ได้แก่

1. แบบจำลองข้อมูลเชิงความคิด (Conceptual Data Model)
2. แบบจำลองข้อมูลเชิงตรรกะ (Logical Data Model)
3. แบบจำลองข้อมูลเชิงกายภาพ (Physical Data Model)

ขั้นตอนในการสร้างแบบจำลองและการออกแบบข้อมูล เริ่มจากการวิเคราะห์ความต้องการของผู้ใช้เพื่อนำมากำหนดเป็นแบบจำลองข้อมูลเชิงความคิด ซึ่งเป็นขั้นตอนการกำหนดเค้าโครงในเบื้องต้นสามารถมองเห็นความสัมพันธ์ของข้อมูล แต่ยังไม่สามารถใช้งานได้จริงเพราะเป็นเพียงแนวคิดเท่านั้น หลังจากนั้นจะทำการออกแบบข้อมูลให้ชัดเจนมากขึ้นโดยกำหนดเป็นแบบจำลองข้อมูลเชิงตรรกะ ซึ่งให้รายละเอียดของข้อมูลมากขึ้น (เช่น ฟิลด์ข้อมูล) ขั้นตอนสุดท้ายคือ การกำหนดแบบจำลองข้อมูลเชิงกายภาพเพื่อให้สามารถใช้งานได้จริง ซึ่งต้องมีการกำหนดรายละเอียดของข้อมูลเพิ่มเติม เช่น รูปแบบของข้อมูล และขนาดของข้อมูล

2.3.2.3 แบบจำลองพัฒนาการ (Maturity Model) การบริหารจัดการข้อมูล

การพัฒนาแบบจำลองพัฒนาการ (Maturity Model) การบริหารจัดการข้อมูลอยู่บนพื้นฐาน และอ้างอิงจากนโยบายมาตรฐานและแนวปฏิบัติที่ดี (Best Practices) ตามมาตรฐานสากล และของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ดังต่อไปนี้

1) แบบจำลองพัฒนาการด้านการบริหารจัดการข้อมูลตามมาตรฐาน CCMI (CMMI Data Management Maturity Model)

สถาบันวิศวกรรมซอฟต์แวร์ (Software Engineering Institute SEI) ประเทศสหรัฐอเมริกา ได้กำหนดมาตรฐานการบูรณาการแบบจำลองพัฒนาการขีดความสามารถองค์กร (Capability Maturity Model Integration CMMI) ซึ่งครอบคลุมขีดความสามารถองค์กรในมิติต่าง ๆ รวมถึงการบริหารจัดการข้อมูล

2) แบบจำลองพัฒนาการด้านการบริหารจัดการข้อมูลของสมาคม DAMA International
สมาคม DAMA International ประเทศสหรัฐอเมริกา เป็นองค์กรอิสระที่รวบรวมผู้เชี่ยวชาญด้านข้อมูล เข้าด้วยกัน เพื่อส่งเสริมให้เกิดความรู้ ความเข้าใจ และสนับสนุนให้เกิดการพัฒนาแนวคิด และแนวปฏิบัติในการบริหารจัดการข้อมูล ได้กำหนดแบบจำลองพัฒนาการด้านการบริหารจัดการข้อมูล

3) การจัดเก็บและการดำเนินการกับข้อมูล (Data Storage and Operations)
การจัดเก็บและการดำเนินการกับข้อมูลเป็นการจัดเก็บข้อมูลที่มีโครงสร้างโดยจัดเก็บในรูปแบบของฐานข้อมูล ส่วนการดำเนินการกับข้อมูลจะเกี่ยวข้องตั้งแต่การวางแผนการใช้งานการสำรองข้อมูล (Backup) การกู้คืนข้อมูล (Restore) การจัดเก็บข้อมูลถาวร (Archive) กระบวนการที่เกี่ยวข้องกับข้อมูล (Create Read Update Delete – CRUD) ตลอดทั้งระบบบริหารและกระบวนการจัดการข้อมูล หรือวงจรชีวิตของข้อมูล การโอนย้ายข้อมูล (Migration) รวมถึงการปรับปรุงประสิทธิภาพของฐานข้อมูลให้พร้อมใช้งานได้ตลอดเวลา เพื่อรักษาความมั่นคงปลอดภัยและความถูกต้องของข้อมูล

4) การบูรณาการและความสามารถในการทำงานร่วมกัน (Data Integration and Interoperability)

การเชื่อมโยงข้อมูลเป็นการรวบรวมข้อมูลจากแหล่งข้อมูลต่าง ๆ ในรูปแบบที่สอดคล้องกันเข้ามารวมอยู่ในแหล่งข้อมูลเดียวกัน เพื่อนำไปใช้ในการจัดทำข้อมูลหลัก (Master Data) คลังข้อมูล (Data Warehouse) ทะเลสาบข้อมูล (Data Lake) รวมถึงการแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน ส่วนความสามารถในการทำงานร่วมกัน (Interoperability) จะมีการกำหนดมาตรฐานหรือข้อตกลงร่วมกันระหว่างหน่วยงานหรือระบบ โดยมีการอ้างอิงถึงคุณลักษณะของระบบต่าง ๆ ที่สามารถแลกเปลี่ยนข้อมูลกันหรือสื่อสารกันได้ เช่น มีการแลกเปลี่ยนข้อมูลในรูปแบบของ Application Programming Interfaces (API) ในการรวบรวมข้อมูลจากแหล่งต่าง ๆ เข้าด้วยกัน ทำให้การบูรณาการข้อมูลมีส่วนช่วยควบคุม และจัดการคุณภาพของข้อมูลให้ดียิ่งขึ้น

ขณะที่การแลกเปลี่ยนข้อมูลจะสนับสนุนให้เกิดประสิทธิภาพของการดำเนินงานระหว่างหน่วยงานหรือส่วนงาน เพราะทั้งหมดนี้มุ่งเน้นการแปลงข้อมูล (Transform) และรวมข้อมูลจากหน่วยงานหรือระบบต้นทางไปจนถึงหน่วยงานหรือระบบกลาง และจากหน่วยงานหรือระบบกลางไปยังหน่วยงาน หรือระบบปลายทาง เพื่อใช้ในการวิเคราะห์ข้อมูลต่อไป

5) การบริหารจัดการเอกสารและเนื้อหา (Document and Content Management)

การบริหารจัดการเอกสารและเนื้อหาเป็นการวางแผนการจัดการ การเข้าถึง การใช้งาน และการควบคุมกิจกรรมต่าง ๆ ที่เกี่ยวกับข้อมูลที่ไม่มีโครงสร้างหรือแบบกึ่งโครงสร้าง เช่น การจัดเก็บ การป้องกันความเสียหาย การเข้าถึงข้อมูล ทั้งที่เก็บอยู่ในรูปแบบกระดาษ และไฟล์อิเล็กทรอนิกส์ มีข้อความ รูปภาพ เสียง ภาพเคลื่อนไหว เป็นต้น การบริหารจัดการดังกล่าวมุ่งเน้นที่การรักษาความถูกต้องสมบูรณ์ และช่วยให้สามารถเข้าถึงเอกสารและข้อมูลที่ไม่มีโครงสร้างหรือแบบกึ่งโครงสร้างได้

6) ข้อมูลหลักและข้อมูลอ้างอิง (Master and Reference Data)

ข้อมูลหลักและข้อมูลอ้างอิงเป็นการบริหารจัดการข้อมูล เพื่อให้ทั้งหน่วยงานสามารถเข้าถึงและใช้ข้อมูลร่วมกันได้ โดยข้อมูลถูกจัดเก็บไว้แหล่งเดียว มีการกำหนดมาตรฐานของข้อมูล เพื่อช่วยลดความซ้ำซ้อนของข้อมูล ทำให้ข้อมูลมีคุณภาพ ความแตกต่างระหว่างข้อมูลหลัก (Master Data) กับข้อมูลอ้างอิง (Reference Data) กล่าวคือ ข้อมูลอ้างอิงจะเป็นข้อมูลที่เป็นสากล มีการกำหนดให้เป็นมาตรฐาน และใช้งานร่วมกัน มีการเปลี่ยนแปลงค่อนข้างน้อย เช่น รหัสไปรษณีย์ รหัสประเทศ หน่วยวัด ระยะทาง ขณะที่ข้อมูลหลักมีโอกาสเปลี่ยนแปลงได้มากกว่า มีรายละเอียดหรือจำนวนฟิลด์ข้อมูลที่มากกว่าและเป็นข้อมูลที่สร้างและใช้งานร่วมกันภายในขอบเขตการดำเนินงานตามภารกิจของหน่วยงาน เช่น ข้อมูลพนักงาน ข้อมูลผู้ประกอบการ ข้อมูลครุภัณฑ์ และข้อมูลสถานที่ เป็นต้น

7) คลังข้อมูล ทะเลสาบข้อมูล ดาตามาร์ท ระบบรายงานอัจฉริยะ และการวิเคราะห์ข้อมูล (Data Warehouse, Data Lake, Data Mart, Business Intelligence, and Data Analytics)

คลังข้อมูล (Data Warehouse) เป็นข้อมูลที่ได้จากการเชื่อมโยงข้อมูล (Data Integration) ซึ่งเกิดจากการรวบรวมข้อมูลจากแหล่งข้อมูลต่าง ๆ ที่มีหลากหลายรูปแบบมาเก็บในคลังข้อมูล โดยผ่านกระบวนการของ Extract Transform Load (ETL) ในรูปแบบข้อมูลที่มีโครงสร้าง และถูกจัดทำให้อยู่ในรูปแบบที่เหมาะสมสำหรับการนำไปวิเคราะห์ข้อมูล ทั้งในรูปแบบของรายงานอัจฉริยะ (Business Intelligence) และการวิเคราะห์ข้อมูล (Data Analytics)

ทะเลสาบข้อมูล (Data Lake) เป็นแหล่งสำหรับเก็บรวบรวมข้อมูลหลากหลายรูปแบบ ข้อมูลที่จัดเก็บเป็นข้อมูลที่มีโครงสร้าง ข้อมูลกึ่งโครงสร้าง และข้อมูลที่ไม่มีโครงสร้าง โดยข้อมูลถูกเก็บรักษาไว้ในรูปแบบที่เหมือนหรือใกล้เคียงกับรูปแบบที่ได้รับมาจากแหล่งข้อมูลต้นฉบับ และสามารถใช้เป็นที่ยืนยันข้อมูลต้นฉบับได้

ดาตามาร์ท (Data Mart) เป็นพื้นที่เก็บข้อมูลที่ตอบสนองความต้องการของหน่วยธุรกิจแบบเฉพาะเจาะจง เช่น ฝ่ายการเงิน ฝ่ายขายของบริษัท เป็นต้น

คลังข้อมูลและทะเลสาบข้อมูลจะเกิดจากการรวบรวมข้อมูลจากแหล่งข้อมูลต่าง ๆ ซึ่งแต่ละแหล่งอาจจะมีรูปแบบของข้อมูลที่แตกต่างกัน การรวบรวมข้อมูลใช้วิธีการบูรณาการข้อมูล โดยข้อมูลจากคลังข้อมูลสามารถรวมเข้าไปที่ทะเลสาบข้อมูลเพื่อใช้สำหรับการวิเคราะห์ข้อมูลที่ซับซ้อนมากยิ่งขึ้น ข้อมูลในคลังข้อมูลจะต้องถูกจัดกลุ่มออกเป็นดาตามาร์ท (Data Mart) โดยต้องสอดคล้องกับหน่วยงานที่จะนำไปใช้ เช่น ดาตามาร์ทของฝ่ายบุคคล ดาตามาร์ทของฝ่ายการตลาด ดาตามาร์ทของฝ่ายการเงิน หลังจากนั้นข้อมูลในดาตามาร์ทถูกนำไปใช้สำหรับการทำรายงานอัจฉริยะ (Business Intelligence) หรือการดำเนินงานที่จะเกิดขึ้นในอนาคตผ่านวิธีการวิเคราะห์ข้อมูล ในกรณีของทะเลสาบข้อมูลสามารถนำข้อมูลไปใช้สำหรับการทำรายงานอัจฉริยะและการวิเคราะห์ข้อมูลได้ทันที โดยไม่ต้องสร้างดาตามาร์ท

8) คำอธิบายชุดข้อมูลดิจิทัล (Metadata)

คำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตา เป็นข้อมูลที่ใช้อธิบายข้อมูลหลักหรือกลุ่มข้อมูลอื่น ๆ ที่เกี่ยวข้องทั้งกระบวนการเชิงธุรกิจและเชิงเทคโนโลยีสารสนเทศ กฎและข้อจำกัดของข้อมูล และโครงสร้างของข้อมูล เมทาดาตาช่วยให้หน่วยงานสามารถเข้าใจข้อมูล ระบบ และขั้นตอนการทำงานได้ดียิ่งขึ้น

การบริหารจัดการเมทาดาตา (Metadata Management) เริ่มตั้งแต่การเก็บรวบรวม การจัดกลุ่ม การดูแล และการควบคุมเมทาดาตา ทั้งนี้ ข้อมูลแต่ละชุดควรมีเมทาดาตา เพื่อให้ผู้ใช้งานทราบเกี่ยวกับชุดข้อมูล เช่น รายละเอียดชุดข้อมูล สิ่งที่เกี่ยวข้องกับชุดข้อมูล วัตถุประสงค์การนำไปใช้ไฟล์ข้อมูล

9) ความมั่นคงปลอดภัยและการรักษาความเป็นส่วนตัวของข้อมูล (Data Security and Privacy)

ความมั่นคงปลอดภัยของข้อมูลเป็นการป้องกันข้อมูลในบริบทของการรักษาความลับ ความถูกต้องของข้อมูล ความพร้อมใช้งานของข้อมูล ตามมาตรฐาน ISO/IEC 27001 โดยมีรายละเอียด ดังนี้

- การรักษาความลับ (Confidentiality) หมายถึง การรักษาข้อมูลตามสภาพของการจัดชั้นความลับ และมีการกำหนดสิทธิ์การเข้าถึงข้อมูล เนื่องจากข้อมูลในหน่วยงานอาจมีหลายประเภท ข้อมูลบางประเภทเป็นข้อมูลที่มีความสำคัญหรืออ่อนไหว จึงต้องมีการรักษาความลับเพื่อลดความเสี่ยงของการถูกคุกคาม และเป็นการป้องกันการรั่วไหลของข้อมูลโดยมิชอบ เช่น การส่งข้อมูลที่ปกปิดหรือเป็นความลับ ต้องมีวิธีการที่ทำให้ทราบได้ว่า บุคคลที่ต้องการส่งข้อมูลมาให้ หรือการที่ผู้ได้รับการอนุญาตให้เข้าถึงข้อมูลเท่านั้นที่สามารถอ่านข้อมูลได้

- ความถูกต้องของข้อมูล (Integrity) หมายถึง การคงสภาพของข้อมูล หรือการรักษาความถูกต้องสมบูรณ์ของข้อมูลให้มีความถูกต้องและน่าเชื่อถือ รวมถึงมีการปกป้องข้อมูลให้ปราศจากการถูกเปลี่ยนแปลงโดยผู้ไม่มีสิทธิ์ เช่น ข้อมูลที่จะจะต้องเป็นข้อมูลที่ถูกต้องอย่างแท้จริง ไม่มีการดัดแปลงหรือแก้ไขระหว่างทาง

- ความพร้อมใช้งานของข้อมูล (Availability) หมายถึง ข้อมูลต้องพร้อมสำหรับการใช้งานอยู่เสมอ รวมถึงมีการสำรองข้อมูลไว้เมื่อเกิดภัยพิบัติ หรือเหตุการณ์ที่ไม่คาดฝัน เช่น หากต้องการใช้ข้อมูล ผู้ใช้งานสามารถใช้อย่างปลอดภัยได้ทันที และใช้ได้อย่างต่อเนื่อง

ความมั่นคงปลอดภัยของข้อมูลต้องดำเนินการตั้งแต่การวางแผน การจัดทำ การปฏิบัติตาม และการบังคับใช้นโยบายและขั้นตอนด้านการรักษาความปลอดภัย เพื่อสนับสนุนด้านการพิสูจน์ตัวตน การกำหนดสิทธิ์ การเข้าถึงข้อมูล การตรวจสอบ และความพร้อมใช้ของข้อมูลอย่างเหมาะสม นอกจากนี้ต้องรักษาความเป็นส่วนตัวของข้อมูล (Data Privacy) ตั้งแต่การรวบรวม จัดเก็บ ใช้ เผยแพร่ หรือดำเนินการอื่นใดเกี่ยวกับข้อมูล โดยต้องระบุวัตถุประสงค์ให้ชัดเจน ห้ามเปิดเผยหรือแสดงข้อมูลในลักษณะอื่นที่ไม่สอดคล้องกับวัตถุประสงค์ เว้นแต่จะได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลหรือมีกฎหมายกำหนดให้กระทำได้

10) คุณภาพของข้อมูล (Data Quality)

คุณภาพของข้อมูลเป็นเครื่องมือในการวัดความน่าเชื่อถือและประสิทธิภาพของการนำข้อมูลไปใช้ ต้องมีการวางแผนการดำเนินการและการควบคุมกิจกรรมต่าง ๆ รวมถึงการปรับปรุง เพื่อให้ข้อมูลมีคุณภาพ เนื่องจากข้อมูลที่มีคุณภาพสูงทำให้การดำเนินงานของหน่วยงานเป็นไปอย่างมีประสิทธิภาพ การทำให้ข้อมูลมีคุณภาพ ประกอบด้วย การทำให้ข้อมูลมีความถูกต้อง (Accuracy) ข้อมูลมีความครบถ้วน (Completeness) ข้อมูลมีความตรงกัน (Consistency) ข้อมูลมีความเป็นปัจจุบัน (Timeliness) ข้อมูลตรงตามความต้องการของผู้ใช้ (Relevancy) และข้อมูลมีความพร้อมใช้ (Availability)

2.4 ความสัมพันธ์ระหว่างธรรมาภิบาลข้อมูลและการบริหารจัดการข้อมูล

จากผลการศึกษาที่เกี่ยวข้องกับการบริหารจัดการข้อมูลของสมาคมบริหารจัดการข้อมูลระหว่างประเทศ (Data Management Association International) จะเห็นว่าธรรมาภิบาลข้อมูล (Data Governance) เป็นส่วนที่สำคัญในการบริหารจัดการข้อมูล (Data Management) โดยธรรมาภิบาลข้อมูลจะมุ่งเน้นการจัดการควบคุม และดูแลข้อมูลให้นำไปใช้ในทางที่เหมาะสม เป็นไปตามระเบียบ ข้อบังคับ ข้อกำหนด และนโยบายขององค์กร เพื่อให้เกิดประโยชน์ต่อองค์กรอย่างสูงสุดและไม่ก่อให้เกิดความเสียหาย ทั้งทางตรงและทางอ้อมตามมาภายหลัง ส่วนการบริหารจัดการข้อมูลจะมุ่งเน้นในส่วนของกระบวนการทำงาน และนำเอากระบวนการด้านเทคโนโลยีสารสนเทศเข้ามาช่วยในการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับข้อมูล จากข้อความข้างต้นทำให้ทราบว่า ธรรมาภิบาลข้อมูลและการบริหารจัดการข้อมูลเป็นเรื่องที่เกี่ยวข้องกัน เนื่องจากปัจจุบันข้อมูลมีจำนวนเพิ่มขึ้นเป็นจำนวนมาก ทั้งภายในและภายนอกองค์กร ประกอบกับข้อมูลต่าง ๆ ล้วนมีความหลากหลาย ไม่คงเส้นคงวา และไม่ครบถ้วนสมบูรณ์ หากไม่มีการบริหารจัดการข้อมูลที่ถูกต้องและเป็นมาตรฐาน อาจส่งผลกระทบต่อองค์กรตามมาในภายหลังได้ ดังนั้น การบริหารจัดการข้อมูลจึงมีความสำคัญ และมักจะเกี่ยวข้องกับกระบวนการต่าง ๆ ได้แก่ การวางแผน การกำหนดสิทธิ การควบคุม การบังคับ การใช้ อำนาจในการตัดสินใจ และวิธีการใช้ข้อมูลที่เหมาะสม

การวางแผนถือเป็นกระบวนการบริหารจัดการข้อมูลอันดับแรกที่ต้องดำเนินการ ได้แก่ การกำหนดบทบาท หน้าที่ และความรับผิดชอบของผู้มีส่วนได้ส่วนเสีย นั่นคือ ธรรมาภิบาลข้อมูล

ธรรมาภิบาลข้อมูลมีพื้นฐานของแนวคิดมาจากทั้งในและต่างประเทศ ที่ต่างได้ให้ความสำคัญกับข้อมูล โดยเล็งเห็นว่า ปัจจุบันข้อมูลเป็นทรัพยากรสำคัญต่อการดำเนินงานขององค์กร ซึ่งมีข้อมูลอยู่เป็นจำนวนมาก อีกทั้งยังมีแนวโน้มเพิ่มสูงขึ้นอย่างต่อเนื่อง โดยแนวคิดดังกล่าวนอกจากจะมุ่งเน้นที่ข้อมูลเป็นสำคัญแล้ว ยังพิจารณารวมถึงการบริหารจัดการข้อมูลครอบคลุมถึงปัจจัยต่าง ๆ ที่เกี่ยวข้อง อาทิ การกำหนดบทบาทหน้าที่ของผู้รับผิดชอบ การปฏิบัติตามระเบียบและข้อบังคับในการนำข้อมูลไปใช้งาน และการควบคุมความมั่นคงปลอดภัยของข้อมูล ฯลฯ โดยปัจจัยดังกล่าว ล้วนมีความสัมพันธ์เกี่ยวเนื่องกันทั้งระบบ ดังนั้น การให้ความสำคัญกับการกำกับดูแลข้อมูลจึงต้องอาศัยความร่วมมือจากทั้งผู้บริหาร เจ้าหน้าที่ ตลอดจนผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับข้อมูล เพื่อให้การกำกับดูแลข้อมูลนั้นเป็นไปอย่างมีประสิทธิภาพมากยิ่งขึ้น

บทที่ 3

กรอบธรรมาภิบาลข้อมูลของ พพ.

พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 กำหนดให้หน่วยงานของรัฐจัดให้มีการบริหารงานภาครัฐและการจัดทำบริการสาธารณะเป็นไปด้วย ความสะดวก รวดเร็ว มีประสิทธิภาพ และตอบสนองต่อการให้บริการและการอำนวยความสะดวกแก่ประชาชน รวมทั้งกำหนดให้หน่วยงานของรัฐจัดให้มีการบริหารจัดการและการบูรณาการข้อมูลภาครัฐ และการทำงานให้มีความสอดคล้องกัน และเชื่อมโยงเข้าด้วยกันอย่างมั่นคงปลอดภัยและมีธรรมาภิบาล จึงจำเป็นต้องกำหนดให้มีธรรมาภิบาลข้อมูลภาครัฐ เพื่อเป็นหลักการและแนวทางในการดำเนินการให้เป็นไปตามพระราชบัญญัติฉบับนี้

ธรรมาภิบาลข้อมูลภาครัฐ (Data Governance) คือ กระบวนการหรือโครงสร้างที่ใช้ในการกำหนดนโยบาย ข้อกำหนด และกระบวนการที่เกี่ยวข้องกับการบริหารจัดการข้อมูลที่เกี่ยวข้องกับหน่วยงานของรัฐ ธรรมาภิบาลข้อมูลภาครัฐมุ่งเน้นการบริหารจัดการข้อมูลให้มีความเป็นระเบียบ มีความน่าเชื่อถือและเป็นไปตามหลักการทางกฎหมาย โดยรวมถึงการกำหนดนโยบาย กรอบแนวทาง และข้อกำหนดในการเก็บรวบรวม ใช้ ประมวลผล และเผยแพร่ข้อมูลภาครัฐ กรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน (พพ.) เป็นหน่วยงานของรัฐ จึงต้องปฏิบัติตามพระราชบัญญัตินี้ดังกล่าว พพ. จึงได้รวบรวมแนวคิดเกี่ยวกับธรรมาภิบาลข้อมูลจากหน่วยงานต่าง ๆ ไม่ว่าจะเป็นระบบบริหารและกระบวนการจัดการข้อมูล ตั้งแต่กระบวนการสร้างข้อมูลจนกระทั่งการทำลายข้อมูล เพื่อให้การบริหารจัดการข้อมูลเป็นไปอย่างถูกต้อง ปลอดภัยและเป็นตามข้อกำหนด ประกอบกับได้นำแนวคิดของ Data Management Association International (DAMA International) ที่เป็นองค์กรอิสระที่มีความเชี่ยวชาญด้านข้อมูลของประเทศสหรัฐอเมริกา และได้นำกรอบการกำกับดูแลข้อมูล (Data Governance Framework) ของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) มาประยุกต์ใช้ในการจัดทำกรอบธรรมาภิบาลข้อมูลของ พพ. ซึ่งประกอบด้วยองค์ประกอบ 3 ส่วนหลัก ได้แก่

- 1) โครงสร้างธรรมาภิบาลข้อมูลภาครัฐ (Data Governance Structure)
- 2) นิยามและกฎเกณฑ์ที่เกี่ยวข้องกับข้อมูล (Definition and Rules)
- 3) กระบวนการกำกับดูแลข้อมูล (Data Governance processes)

โดยกรอบการกำกับดูแลข้อมูลหรือกรอบธรรมาภิบาลข้อมูลของ พพ. ประกอบจากองค์ประกอบทั้ง 3 เข้าด้วยกัน ทั้งในด้านบุคคล นิยามและกฎเกณฑ์ที่เกี่ยวข้องกับข้อมูล และกระบวนการ อีกทั้งยังต้องดำเนินการด้านการวัดการดำเนินการและความสำเร็จของธรรมาภิบาลข้อมูล เพื่อให้ทราบถึงสถานการณ์ดำเนินการของ พพ. และทราบถึงปัญหาที่เกิดขึ้น เพื่อนำไปสู่การแก้ปัญหาอย่างเหมาะสม อันจะนำไปสู่การบรรลุเป้าหมายของการดำเนินงานตามที่ พพ. กำหนดไว้อย่างยั่งยืน



3.1 กรอบธรรมาภิบาลข้อมูลของ พพ.

3.1 โครงสร้างธรรมาภิบาลข้อมูลภาครัฐ (Data Governance Structure)

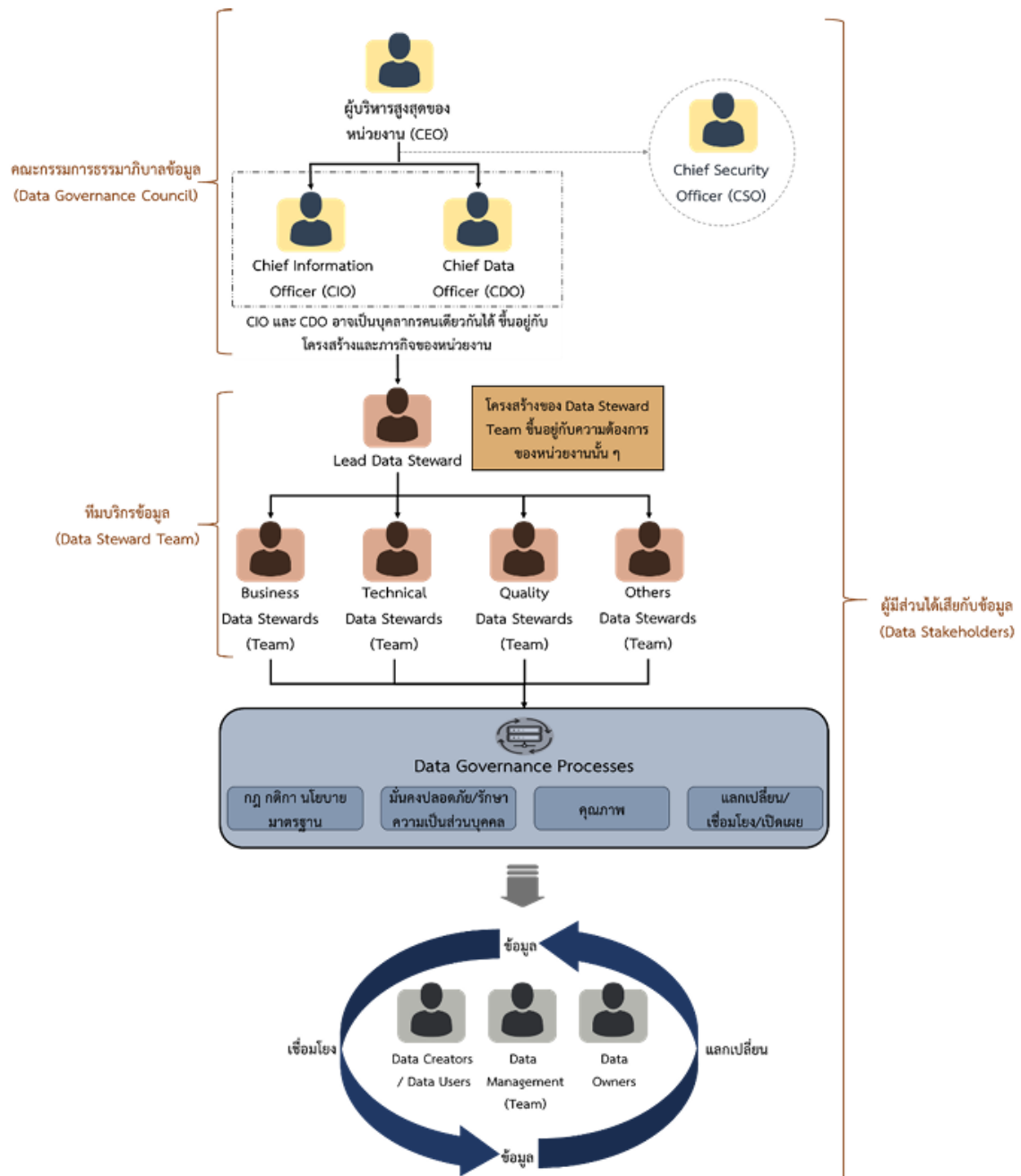
การกำหนดโครงสร้างธรรมาภิบาลข้อมูลภาครัฐ เพื่อแสดงลำดับชั้นของกลุ่มบุคคลที่เกี่ยวข้องกับธรรมาภิบาลข้อมูลภาครัฐ และสิทธิในการสั่งการตามลำดับชั้น ทั้งนี้ จำนวนบุคลากรและลำดับชั้นให้พิจารณาตามความเหมาะสมของแต่ละหน่วยงานของรัฐ หน่วยงานของรัฐสามารถจัดตั้งส่วนงานธรรมาภิบาลข้อมูลในรูปแบบที่แตกต่างกัน ได้ 3 รูปแบบดังนี้

- 1) รูปแบบทีมเสมือน (Virtual Team) ที่คัดเลือกมาจากส่วนงานต่าง ๆ
- 2) รูปแบบที่มีส่วนงานรับผิดชอบชัดเจน ซึ่งอาจจัดตั้งใหม่หรือกำหนดหน้าที่ให้กับส่วนงานที่มีหน้าที่คล้ายกับโครงสร้าง

- 3) รูปแบบผสม ซึ่งจะแยกหน้าที่ให้ชัดเจนระหว่างส่วนงานที่รับผิดชอบหลักกับทีมเสมือน

โครงสร้างธรรมาภิบาลข้อมูลภาครัฐ ซึ่งแบ่งออกเป็น 3 ส่วน ได้แก่

- 1) คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council)
- 2) ทีมบริกรข้อมูล (Data Steward Team)
- 3) ผู้มีส่วนได้ส่วนเสียกับข้อมูล (Data Stakeholders)



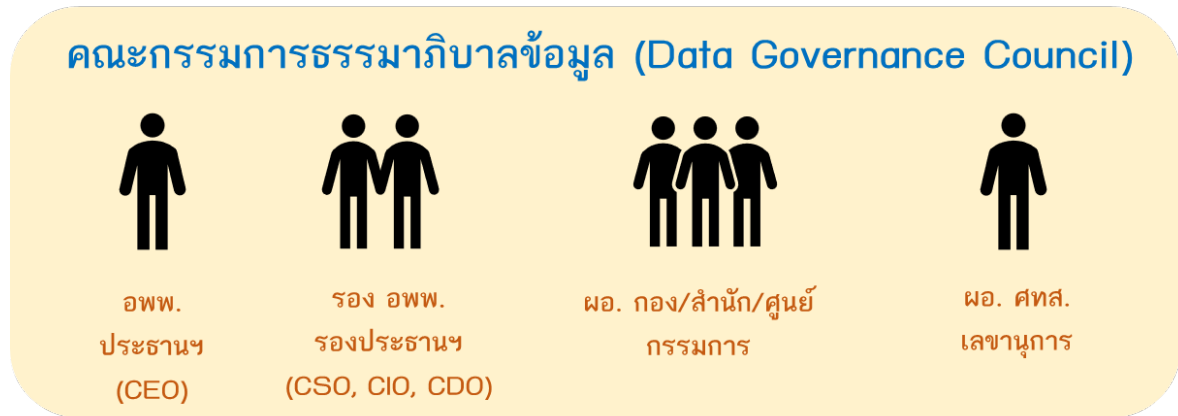
รูปที่ 3.2 แสดงตัวอย่างโครงสร้างธรรมาภิบาลข้อมูลภาครัฐ

โครงสร้างธรรมาภิบาลข้อมูลของ พพ. และการกำหนดบทบาทและหน้าที่ความรับผิดชอบตามตำแหน่งต่าง ๆ ได้ใช้โครงสร้างธรรมาภิบาลข้อมูลภาครัฐ ดังรูปที่ 3.2 มาปรับใช้ให้ในการดำเนินการ ดังนี้

3.1.1 คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council)

คณะกรรมการธรรมาภิบาลข้อมูลประกอบด้วยผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer : CEO) ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO) ผู้บริหารข้อมูลระดับสูง (Chief Data Officer : CDO) ผู้บริหารด้านการรักษาความปลอดภัยระดับสูง (Chief

Security Officer : CSO) และผู้นำหรือผู้รับผิดชอบในแต่ละส่วนงานหลักขององค์กร (Key Business Unit Head) ได้แก่ ด้านบริหาร ด้านอำนวยการ ด้านปฏิบัติการ



รูปที่ 3.3 แสดงคณะกรรมการธรรมาภิบาลข้อมูลของ พพ.

ตารางที่ 3.1 ตำแหน่งและบทบาทหน้าที่ของคณะกรรมการกำกับดูแลข้อมูล

คณะกรรมการกำกับดูแลข้อมูล	บทบาทหน้าที่
(1) ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer : CEO) (อธิบดีกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน)	ตัดสินใจเชิงนโยบาย แก้ไขปัญหา และบริหารจัดการภายในคณะกรรมการกำกับดูแลข้อมูล
(2) ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO) หรือผู้บริหารข้อมูลระดับสูง (Chief Data Officer : CDO) (รองอธิบดีหรือผู้ที่ได้รับการแต่งตั้งจากผู้บริหารระดับสูงสุดของหน่วยงาน)	- วิเคราะห์ข้อมูลของหน่วยงานเพื่อสร้างและส่งมอบเทคโนโลยีเครื่องมือ แนวทาง และวิธีการในการทำให้ข้อมูลของหน่วยงานมีคุณค่า และเกิดประโยชน์สูงสุดต่อองค์กร เพื่อขยายผลต่อไปให้เกิดผลสัมฤทธิ์ ในการส่งเสริมให้องค์กรใช้ข้อมูลได้อย่างถูกต้องและมีประสิทธิภาพ - วิเคราะห์ข้อมูลร่วมกับผู้บริหารส่วนอื่น ๆ เพื่อจัดทำยุทธศาสตร์และดำเนินการกำกับดูแลข้อมูลให้มีคุณภาพ และการควบคุมอื่น ๆ เพื่อรักษาความสมบูรณ์ของข้อมูลองค์กร

คณะกรรมการกำกับดูแลข้อมูล	บทบาทหน้าที่
(3) ผู้บริหารด้านการรักษาความปลอดภัยระดับสูง (Chief Security Officer : CSO) (รองอธิบดีหรือผู้ที่ได้รับการแต่งตั้งจากผู้บริหารระดับสูงสุดของหน่วยงาน)	- บริหารข้อมูลให้มีความปลอดภัย และเพียงพอสำหรับการทำงาน - ทำให้เกิดการเชื่อมต่อระหว่างหน่วยงานภาครัฐ รวมทั้งปรับปรุงความมั่นคงทางกายภาพ และความปลอดภัยด้านเทคโนโลยีให้มากขึ้น - ทำงานร่วมกับผู้บริหารอื่น ๆ ในการตัดสินใจเกี่ยวกับลำดับความสำคัญของความต้องการด้านความปลอดภัย - กำหนดเป้าหมายและวัตถุประสงค์ของการป้องกันหน่วยงาน เพื่อให้สอดคล้องกับแผนกลยุทธ์ของหน่วยงาน - ดูแลเครือข่ายของคณะกรรมการ ผู้บริหาร และเจ้าหน้าที่รักษาความปลอดภัย - ทำงานร่วมกับหน่วยงานด้านความมั่นคง และหน่วยงานรักษาความปลอดภัยอื่น ๆ
(4) ผู้รับผิดชอบในแต่ละส่วนงานหลักขององค์กร (Key Business Unit Head) (หัวหน้าส่วนราชการระดับกอง/สำนัก/ศูนย์ หรือผู้ที่ได้รับมอบหมาย)	- ให้คำแนะนำ ข้อเสนอแนะ และวิพากษ์ประเด็นต่าง ๆ ที่เกี่ยวข้องกับการบริหารจัดการข้อมูลในส่วนงานที่ตนเองรับผิดชอบและส่วนงานอื่น ๆ ที่เกี่ยวข้อง - ร่วมกำหนดนโยบายธรรมาภิบาลข้อมูล - สื่อสารไปยังทีมงานภายใต้ส่วนงานที่ตนรับผิดชอบ เพื่อให้บุคลากรอื่น ๆ ในองค์กร ได้รับทราบถึงนโยบายและแนวปฏิบัติของธรรมาภิบาลข้อมูล

3.1.2 ทีมบริการข้อมูล (Data Steward Team)

ทีมบริการข้อมูลทำหน้าที่ในการให้ข้อมูลและให้ความรู้ต่าง ๆ ที่เกี่ยวข้องกับการบริหารงานดิจิทัล การกำกับมาตรฐานงานด้านดิจิทัล และโครงสร้างพื้นฐานของงานดิจิทัลในด้านต่าง ๆ อันจะสนับสนุนให้เกิดการกำกับดูแลข้อมูลที่ดีอย่างเป็นระบบ อย่างไรก็ตามทีมบริการข้อมูลไม่ได้มีการกำหนดโครงสร้างของทีมงานอย่างชัดเจน โดยสามารถปรับเปลี่ยนตามความต้องการหรือบริบทองค์กรนั้น ๆ เป็นสำคัญ ทั้งนี้เมื่อพิจารณาจากโครงสร้างองค์กรของ พพ. ในปัจจุบัน สามารถนำมากำหนดเป็นทีมบริการข้อมูลได้ ดังนี้



รูปที่ 3.4 แสดงทีมบริการข้อมูลของ พพ.

ตารางที่ 3.2 ตำแหน่งและบทบาทหน้าที่ของทีมบริการข้อมูล

ทีมบริการข้อมูล	บทบาทหน้าที่
(1) หัวหน้าบริการข้อมูล (Lead Data Steward) (ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือผู้ที่ได้รับการแต่งตั้งจากผู้บริหารระดับสูงสุดของหน่วยงาน และควรเป็นเลขานุการของคณะกรรมการธรรมาภิบาลข้อมูล)	ควบคุมและสั่งการภายในทีมบริการข้อมูล
(2) บริการข้อมูลด้านธุรกิจ (Business Data Stewards) (บุคลากรกอง/สำนัก/ศูนย์) (3) บริการข้อมูลด้านคุณภาพข้อมูล (Data Quality Stewards) (บุคลากรกอง/สำนัก/ศูนย์) (4) บริการข้อมูลด้านเทคนิค (Technical Data Stewards) (4.1) บริการข้อมูลด้านการกำกับมาตรฐานงานดิจิทัลสารสนเทศ (หัวหน้ากลุ่มพัฒนาระบบสารสนเทศ และหัวหน้ากลุ่มเทคโนโลยีสารสนเทศ) (4.2) บริการข้อมูลด้านวิเคราะห์ข้อมูลและพัฒนาระบบดิจิทัล (หัวหน้ากลุ่มพัฒนาระบบสารสนเทศ) (4.3) บริการข้อมูลด้านโครงสร้างพื้นฐานดิจิทัล (หัวหน้ากลุ่มเทคโนโลยีสารสนเทศ)	- กำหนดมาตรฐาน แผนงาน และการให้บริการ รวมถึงแนวทางในการใช้โครงข่ายพื้นฐานเพื่อสนับสนุนเทคโนโลยีสารสนเทศขององค์กร - ควบคุม กำกับ ตรวจสอบ และติดตามการปฏิบัติตามนโยบายข้อมูล ตรวจสอบคุณภาพ ตรวจสอบความมั่นคงปลอดภัยของข้อมูล วิเคราะห์ผลจากการตรวจสอบ - ให้ข้อเสนอแนะมาตรฐาน วิเคราะห์ข้อมูล และเชิงเทคนิคและการนำไปประยุกต์ใช้บริหารข้อมูลสารสนเทศ และการปฏิบัติตามนโยบายข้อมูลงานระบบสารสนเทศ - ให้คำปรึกษาและแนะนำหรือ ฝึกอบรม การใช้คอมพิวเตอร์และการใช้โปรแกรมพัฒนาบุคลากรภาครัฐด้านเทคโนโลยีสารสนเทศและการสื่อสาร - พัฒนาระบบเครือข่าย รวมทั้งเฝ้าระวัง ป้องกัน และแก้ไขภัยคุกคามที่อาจเกิดขึ้น จากระบบงานเทคโนโลยีสารสนเทศ - ประสานงานและสนับสนุนด้านเทคโนโลยีสารสนเทศ โดยดำเนินการบริหารโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศขององค์กรทั้งที่เป็นศูนย์กลางหรือที่ใช้ร่วมกัน - สำรวจ เก็บรวบรวมข้อมูล ติดตามความเคลื่อนไหวของสถานการณ์ และแนวโน้มการพัฒนาด้านดิจิทัล - บำรุงรักษาโครงสร้างพื้นฐานสารสนเทศให้พร้อมใช้งานตลอดเวลา แก้ไข และช่วยเหลือผู้ใช้งานระบบสารสนเทศในองค์กร - รายงานผลลัพธ์การตรวจสอบไปยังคณะกรรมการธรรมาภิบาลข้อมูล และผู้ที่เกี่ยวข้องอื่น ๆ ให้ทราบ

3.1.3 ผู้มีส่วนได้ส่วนเสียกับข้อมูล (Data Stakeholders)

ผู้มีส่วนได้ส่วนเสียกับข้อมูล ทำหน้าที่ให้การสนับสนุนการกำกับดูแลข้อมูลขององค์กรต่อทีมบริการข้อมูล และคณะกรรมการกำกับดูแลข้อมูล ประกอบไปด้วย เจ้าของข้อมูล (Data Owners) ทีมบริหารจัดการ

ข้อมูล (Data Management Team) ผู้สร้างข้อมูล (Data Creators) และผู้ใช้ข้อมูล (Data Users) โดยผู้มีส่วนได้ส่วนเสียกับข้อมูลกลุ่มนี้ มีบทบาทหน้าที่ดังนี้

ตารางที่ 3.3 ตำแหน่งและบทบาทหน้าที่ของผู้มีส่วนได้ส่วนเสียกับข้อมูล

ผู้มีส่วนได้ส่วนเสียกับข้อมูล	บทบาทหน้าที่
(1) เจ้าของข้อมูล (Data Owners) (หัวหน้าส่วนราชการระดับกอง/สำนัก/ศูนย์ กลุ่ม หรือผู้ที่ได้รับมอบหมาย)	ตรวจสอบดูแลข้อมูลโดยตรง เพื่อสร้างความมั่นใจได้ว่าการบริหารจัดการข้อมูลมีความสอดคล้องกับนโยบาย มาตรฐาน กฎระเบียบหรือกฎหมาย โดยเจ้าของข้อมูลจะทำการทบทวนและอนุมัติการดำเนินการต่าง ๆ ที่เกี่ยวข้องข้อมูล
(2) ทีมบริหารจัดการข้อมูล (Data Management Team)	มีหน้าที่หลักในการบริหารจัดการข้อมูลให้สอดคล้องกับการบริหารจัดการข้อมูล และดูแลรักษาข้อมูลในระบบสารสนเทศของหน่วยงาน และสนับสนุนกิจกรรมของธรรมาภิบาลข้อมูลภาครัฐ
(2.1) สถาปนิกข้อมูล (Data Architects)	ทำหน้าที่ออกแบบและจัดทำสถาปัตยกรรมข้อมูล (Data Architecture) จำลองและการออกแบบข้อมูล (Data Modeling and Design) และกำหนดโครงสร้าง (infrastructure) สำหรับจัดการกับข้อมูล
(2.2) นักจัดการฐานข้อมูล (Database Administrators)	ทำหน้าที่จัดเก็บ และการดำเนินการกับข้อมูล (Data Storage and Operations) รวมถึงการดูแล บำรุงรักษา ปรับปรุงประสิทธิภาพการทำงาน และวางแผนการจัดเก็บข้อมูล
(2.3) นักวิเคราะห์ข้อมูล (Data Analysts)	ทำหน้าที่นำข้อมูลมาวิเคราะห์ หรือแก้ปัญหาจากสิ่งที่ไม่ปกติโดยใช้ประสบการณ์และหลักสถิติ รวมถึงใช้โมเดลหรือเครื่องมือในการทำรายงาน เพื่อสรุปข้อมูลสำหรับการตัดสินใจ
(2.4) นักวิทยาการข้อมูล (Data Scientists)	ทำหน้าที่นำข้อมูลจากหลาย ๆ แหล่ง และแปลงข้อมูล เพื่อหารูปแบบและความสัมพันธ์ของข้อมูล รวมถึงสร้างแบบจำลอง และดำเนินการกับข้อมูลด้วยวิธีการต่าง ๆ เช่น Machine Learning หรือเขียนโปรแกรม เพื่อทำนายมุมมองหรือการคาดการณ์ในอนาคต
(3) ผู้สร้างข้อมูล (Data Creators) (ข้าราชการ พนักงานราชการ ลูกจ้าง คณะ บุคคลหรือผู้ซึ่งมีอำนาจหน้าที่ปฏิบัติงานให้แก่ กรมพัฒนาพลังงานทดแทนและอนุรักษ์ พลังงาน ทำหน้าที่ในการนำเข้าข้อมูลหรือ กรอกข้อมูล)	ทำหน้าที่ในการบันทึก แก้ไข ปรับปรุง หรือลบข้อมูลให้สอดคล้องกับโครงสร้างที่ถูกกำหนดไว้ นอกจากนี้ยังมีหน้าที่ ในการทำงานร่วมกับบริการข้อมูล เพื่อตรวจสอบและแก้ไขปัญหาด้านคุณภาพข้อมูลและความมั่นคงปลอดภัย

ผู้มีส่วนได้ส่วนเสียกับข้อมูล	บทบาทหน้าที่
(4) ผู้ใช้ข้อมูล (Data Users) (ผู้บริหารและข้าราชการ พ.พ. ผู้ใช้บริการของ พ.พ. และผู้มีส่วนได้ส่วนเสียอื่น ๆ ที่เกี่ยวข้องกับ พ.พ.)	ทำหน้าที่ในการนำข้อมูลไปใช้งานทั้งในระดับบริหารและระดับปฏิบัติงาน และสนับสนุนการกำกับดูแลข้อมูลภาครัฐโดยการให้ความต้องการในการใช้ข้อมูล พร้อมทั้งรายงานประเด็นปัญหาที่พบระหว่างการใช้อข้อมูล ทั้งด้านคุณภาพและความปลอดภัยของข้อมูลไปยังบริการข้อมูล

3.2 นิยามและกฎเกณฑ์ที่เกี่ยวข้องกับข้อมูล (Definition and Rules)

3.2.1 สภาพแวดล้อมของธรรมาภิบาลข้อมูล (Data Governance Environment)

ปัจจุบันกฎหมายที่เกี่ยวข้องกับข้อมูล ข่าวสาร หรือสิทธิส่วนบุคคลในประเทศไทยมีประเด็นที่อาจส่งผลกระทบต่อหลักแนวคิดธรรมาภิบาลข้อมูลภาครัฐ ซึ่งหากหน่วยงานในประเทศไทยต้องการสร้างหรือปรับปรุงระบบภายในให้มีธรรมาภิบาลข้อมูลภาครัฐ จะต้องพิจารณาประเด็นที่เกี่ยวข้องกับกฎหมาย ดังนี้

3.2.1.1 การเปิดเผยข้อมูล

การเปิดเผยข้อมูลเป็นสิ่งจำเป็นต่อการดำเนินงานของหน่วยงานรัฐ เพื่อแสดงความโปร่งใสในการดำเนินงานและความสามารถในการตรวจสอบได้จากภาคเอกชนและประชาชน รวมไปถึงการสนับสนุนให้ ภาคเอกชนและประชาชนนำข้อมูลที่เปิดเผยไปสร้างนวัตกรรมผลิตภัณฑ์และบริการ เพื่อยกระดับการพัฒนาประเทศ โดยประเทศไทยมีกฎหมายที่เกี่ยวข้องกับการเปิดเผยข้อมูล เช่น รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560 (มาตราที่ 59) พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 และพระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. 2540 เป็นต้น

3.2.1.2 การเชื่อมโยงและแลกเปลี่ยนข้อมูล

การเชื่อมโยงและแลกเปลี่ยนข้อมูลเป็นสิ่งสำคัญต่อการบูรณาการในการดำเนินงานระหว่าง หน่วยงานภาครัฐ ซึ่งเป็นประโยชน์ต่อหน่วยงานภาครัฐและประชาชนในการขอใช้บริการจากภาครัฐ โดยมี กฎหมายที่เกี่ยวข้องกับการเชื่อมโยงและแลกเปลี่ยนข้อมูล เช่น พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562

3.2.1.3 การคุ้มครองข้อมูลส่วนบุคคล

การคุ้มครองข้อมูลส่วนบุคคลเป็นสิ่งสำคัญที่ภาครัฐต้องดำเนินการ โดยปัจจุบันมีการนำระบบสารสนเทศและการสื่อสารมาประยุกต์ใช้ประกอบการทำธุรกรรมทางอิเล็กทรอนิกส์อย่างแพร่หลาย ซึ่งหน่วยงานภาครัฐอาจจะมีการเก็บ รวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคลของ ผู้ใช้บริการในรูปของข้อมูลอิเล็กทรอนิกส์ เพื่อเป็นการป้องกันการละเมิดข้อมูลส่วนบุคคล ซึ่งเป็นสิทธิขั้นพื้นฐานของประชาชนที่ต้องได้รับการคุ้มครอง ดังนั้นการคุ้มครองข้อมูลส่วนบุคคลจำเป็นที่จะต้องนำมาวิเคราะห์เพื่อให้เกิดธรรมาภิบาลข้อมูลภาครัฐที่ดี โดยมีกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล เช่น พระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. 2540 และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นต้น

3.2.1.4 การรักษาความลับของทางราชการ

การรักษาความลับทางราชการเป็นสิ่งที่จำเป็นต่อการดำเนินงานของหน่วยงานภาครัฐ ซึ่งเป็นการป้องกันความเสียหายที่จะเกิดขึ้นต่อภาครัฐ ทั้งในด้านความมั่นคงของรัฐ และผลประโยชน์ของชาติ ตลอดจนความสามารถในการพัฒนาประเทศและภาพลักษณ์ โดยมีกฎหมายที่เกี่ยวข้องกับการรักษา

ความลับของทางราชการ เช่น พระราชบัญญัติข่าวกรองแห่งชาติ พ.ศ. 2562 และระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม เป็นต้น

นอกจากการพิจารณากฎหมาย ระเบียบ และข้อบังคับข้างต้นแล้ว หน่วยงานควรจะต้องพิจารณา กฎหมาย ระเบียบ นโยบาย หรือพระราชบัญญัติอื่นที่เกี่ยวข้องกับเรื่องธรรมาภิบาลข้อมูลภาครัฐอีกด้วย เช่น พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 เพื่อให้การได้มาและการนำไปใช้ข้อมูลของ หน่วยงานภาครัฐถูกต้อง ครบถ้วน เป็นปัจจุบัน มั่นคงปลอดภัย รักษาความเป็นส่วนตัว และสามารถ เชื่อมโยงกันได้อย่างมีประสิทธิภาพและมั่นคงปลอดภัยได้จริง

3.2.2 นิยามข้อมูล (Data Definition)

การนิยามข้อมูลต้องมีความถูกต้องและชัดเจน เพื่อสร้างความเข้าใจที่ตรงกันระหว่างผู้ที่เกี่ยวข้อง ทั้งนี้ การจัดหมวดหมู่ของข้อมูล ทำให้มองเห็นถึงภาพรวมของข้อมูล โดยข้อมูลแบ่งออกได้เป็น 5 หมวดหมู่ ดังนี้

1) ข้อมูลสาธารณะ (Public Data) คือ ข้อมูลที่สามารถเปิดเผยได้ สามารถนำไปใช้ได้อย่างอิสระ ไม่ว่าจะเป็นข้อมูลข่าวสาร ข้อมูลส่วนบุคคล ข้อมูลอิเล็กทรอนิกส์ เป็นต้น

2) ข้อมูลใช้ภายใน (Internal Use Only) คือ ข้อมูลสำหรับใช้ในการดำเนินการภายในของ หน่วยงาน ไม่อนุญาตให้นำไปใช้งานภายนอกก่อนได้รับอนุญาตจากเจ้าของข้อมูล เช่น ร่างนโยบาย ร่างมาตรฐาน และขั้นตอนการปฏิบัติงาน ประกาศ และบันทึกภายในหน่วยงานที่อยู่ระหว่างการขออนุมัติ เป็นต้น

3) ข้อมูลส่วนบุคคล (Personal Data) คือ ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม

4) ข้อมูลความลับทางราชการ (Classified Information) คือ ข้อมูลข่าวสารตามมาตรา 14 หรือ มาตรา 15 แห่งพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ที่มีคำสั่งไม่ให้เปิดเผยและอยู่ในความ ครอบครอง หรือควบคุมดูแลของหน่วยงานของรัฐ ไม่ว่าจะเป็นเรื่องที่เกี่ยวกับการดำเนินงานของรัฐ หรือ ที่เกี่ยวกับเอกชน ซึ่งมีการกำหนดให้มีชั้นความลับเป็น ชั้นลับ ชั้นลับมาก หรือชั้นลับที่สุด ตามระเบียบว่าด้วย การรักษาความลับของทางราชการ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม โดยคำนึงถึงการปฏิบัติหน้าที่ของ หน่วยงานของรัฐและประโยชน์แห่งรัฐประกอบกัน

5) ข้อมูลความมั่นคง (National Security Information) คือ ข้อมูลภายใต้กรอบความมั่นคง แห่งชาติ หรือภาวะที่ประเทศปลอดจากภัยคุกคามต่อเอกราช อธิปไตยบูรณภาพแห่งอาณาเขต สถาบัน ศาสนา สถาบันพระมหากษัตริย์ ความปลอดภัยของประชาชน การดำรงชีวิต โดยปกติสุขของประชาชน หรือที่กระทบต่อ ผลประโยชน์แห่งชาติหรือการปกครองระบอบประชาธิปไตย อันมีพระมหากษัตริย์ทรงเป็นประมุข รวมทั้งความ พร้อมของประเทศที่จะเผชิญสถานการณ์ต่าง ๆ อันเกิดจากภัยคุกคามทุกรูปแบบ และครอบคลุม ด้านความ มั่นคงปลอดภัยของประเทศ (National Security) ในมิติเศรษฐกิจ อาหาร สุขภาพ สิ่งแวดล้อมและ สิทธิมนุษยชน ส่วนบุคคล ชุมชน การเมือง และการต่างประเทศ ที่สอดคล้องตามเป้าหมายของนโยบายและ แผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ

3.2.3 กฎเกณฑ์ของข้อมูล/นโยบายข้อมูล (Data Rules/Data Policies)

3.2.3.1 การกำหนดทิศทางการดำเนินการและแนวนโยบายที่เกี่ยวข้องกับธรรมาภิบาลข้อมูล

ปัจจุบันกฎหมายที่เกี่ยวข้องกับข้อมูล ข่าวสาร หรือสิทธิส่วนบุคคลในประเทศไทยมี ประเด็นที่อาจส่งผลกระทบต่อหลักแนวคิดธรรมาภิบาลข้อมูลภาครัฐ ซึ่งหากหน่วยงานในประเทศไทยต้องการ

สร้างหรือปรับปรุงระบบภายในให้มีธรรมาภิบาลข้อมูลภาครัฐจะต้องพิจารณาประเด็นหลัก ๆ ที่เกี่ยวข้องกั กฎหมาย ดังนี้

1) การกำหนดภารกิจ (Mission) และวิสัยทัศน์ (Vision) ในธรรมาภิบาลข้อมูลจะต้อง มีกำหนดเป็นภารกิจที่ชัดเจน เพื่อให้มีทิศทางการดำเนินการธรรมาภิบาลข้อมูล โดยควรมุ่งเน้นการตอบสนอง และแก้ไขปัญหาที่อาจเกิดขึ้นได้ทันเวลา และสามารถให้บริการข้อมูลแก่ผู้ที่เกี่ยวข้องได้อย่างทันท่วงที ทั้งนี้ จะต้องสอดคล้องกับวิสัยทัศน์ขององค์กร คือ แผนพลังงานแห่งชาติ (สำนักงานนโยบายและแผนพลังงาน, 2564) และภารกิจหลักที่มีอยู่ในทุกด้านตามที่กำหนดไว้รวมถึงจะต้องมีการทบทวนนโยบายและบริบทของ สภาพแวดล้อมข้อมูลเทคโนโลยีดิจิทัลในปัจจุบันและอนาคต มาประกอบรวมกันทุกส่วนแล้วกำหนดเป็นภารกิจ ด้านธรรมาภิบาลข้อมูลของ พพ.

2) การกำหนดเป้าหมาย (Goal) การวัดการดำเนินการ (Metrics) การวัดความสำเร็จ (Success Measure) และการจัดหางบประมาณ (Funding) การดำเนินการธรรมาภิบาลข้อมูลจะต้องมีการ ระบุเป้าหมายและระบุแนวทางการวัดความสำเร็จของการดำเนินการรวมถึงจะต้องมีการวางแผนด้าน งบประมาณที่ต้องใช้ในการดำเนินการ เพื่อให้มีความพร้อมในการดำเนินการและให้เกิดความสำเร็จด้านธรร มาภิบาลข้อมูล

3) การกำหนดสิทธิในการตัดสินใจ (Decision Rights) การดำเนินการธรรมาภิบาลข้อมูล ตามกระบวนการธรรมาภิบาลข้อมูลมีผู้ที่เกี่ยวข้องในกระบวนการหลายส่วนงาน ตามที่ระบุไว้ในโครงสร้าง ธรรมาภิบาลข้อมูล เพื่อให้การดำเนินการเป็นมีความคล่องตัวในธรรมาภิบาลข้อมูล จะต้องกำหนดโครงสร้าง สิทธิในการตัดสินใจ โดยพิจารณาจากระดับความสำคัญของข้อมูล หรือกิจกรรมที่อยู่ในกระบวนการธรรมาภิบาลข้อมูล ประกอบกับโครงสร้างองค์กร รวมถึงอำนาจหน้าที่ผู้บริหารที่เกี่ยวข้องกับธรรมาภิบาลข้อมูล โดยในการ ออกแบบโครงสร้างการตัดสินใจควรคำนึงถึงความถูกต้อง รวดเร็วและตรวจสอบได้

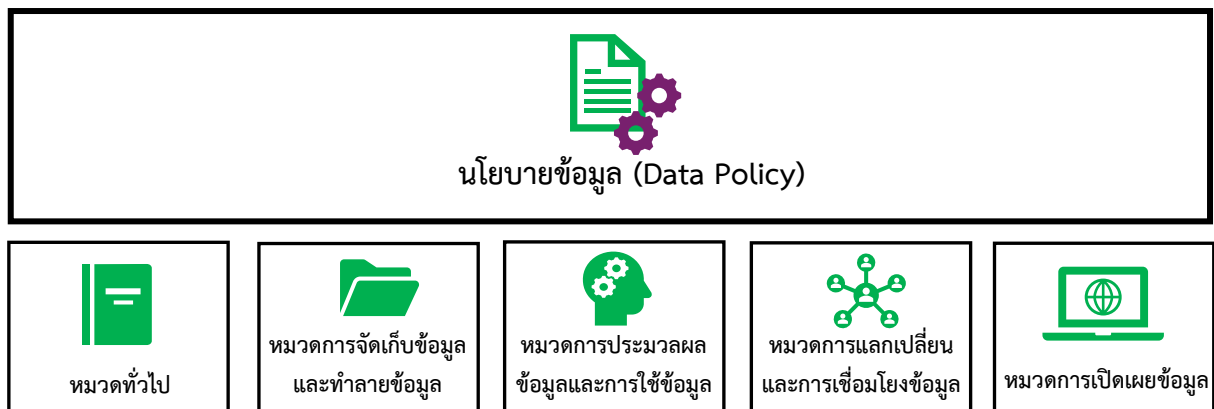
4) การกำหนดความรับผิดชอบต่อความสำเร็จ (Accountabilities) การกำหนดภาระ ความผิดชอบตามโครงสร้างการธรรมาภิบาลข้อมูล (People and Organizational Bodies) จะต้องระบุ บทบาท (Roles) หน้าที่ (Responsibilities) และความรับผิดชอบต่อความสำเร็จ (Accountabilities) ของ บุคลากรในโครงสร้างให้ชัดเจน และสอดคล้องกับโครงสร้างหลักในการดำเนินงานของ พพ. เพื่อให้มี ผู้รับผิดชอบในกิจกรรมในกระบวนการธรรมาภิบาลข้อมูลที่ชัดเจนและครบถ้วน

5) การกำหนดกลไกการควบคุมความเสี่ยง (Controls) เพื่อกำหนดขั้นตอน กระบวนการ หรือกลไกการควบคุมธรรมาภิบาลข้อมูล เพื่อให้มั่นใจว่าเป็นไปตามนโยบาย กฎ ระเบียบของ ธรรมาภิบาลข้อมูลโดยมีรูปแบบการควบคุม ประกอบด้วย การควบคุมแบบป้องกัน (Preventive Control) การควบคุมแบบตรวจสอบ (Detective Control) และการควบคุมแบบแก้ไข (Corrective Control) รวมถึง การกำหนดวิธีการควบคุมโดยใช้บุคคล หรือเทคโนโลยีเข้ามาช่วยในการควบคุม

3.2.3.2 กฎเกณฑ์ข้อมูล (Data Rules)

ธรรมาภิบาลข้อมูลจะต้องมีการมีการกำหนดความถูกต้องและชัดเจนของข้อมูล เพื่อให้เกิด ความเข้าใจที่ตรงกันระหว่างผู้ที่เกี่ยวข้อง รวมถึงต้องมีการพิจารณาถึงกฎเกณฑ์ที่เกี่ยวข้องกับข้อมูล ทั้งในส่วน ที่เป็นกฎหมาย นโยบาย และมาตรฐานของข้อมูลจะต้องมีความสอดคล้องกับธรรมาภิบาลข้อมูล เพื่อให้มี แนวทางในการดำเนินการ โดยทั่วไปการกำหนดกฎเกณฑ์ข้อมูลจะจัดทำเป็นนโยบายข้อมูล (Data Policies) และการจัดทำมาตรฐานข้อมูล (Data Standards) โดยมีรายละเอียด ดังนี้

1) นโยบายข้อมูล (Data Policies) การกำหนดนโยบายข้อมูลจัดเป็นหนึ่งในพื้นฐานของธรรมาภิบาลข้อมูลภาครัฐ ดังนั้นเพื่อให้ธรรมาภิบาลข้อมูลภาครัฐมีประสิทธิภาพ จึงต้องมีการกำหนดนโยบายที่ระบุอย่างชัดเจน สอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง หรือข้อกำหนดอื่น ๆ ที่เกี่ยวข้อง โดยผ่านการอนุมัติจากผู้บริหารมีการเผยแพร่และสื่อสารให้กับเจ้าหน้าที่และผู้ที่เกี่ยวข้อง ทั้งภายในและภายนอกหน่วยงาน รวมถึงควรมีการทบทวนนโยบายอย่างสม่ำเสมอ เพื่อให้นโยบายข้อมูลได้ถูกนำมาปฏิบัติอย่างมีประสิทธิภาพและต่อเนื่อง โดยนโยบายข้อมูลควรครอบคลุมระบบบริหารและกระบวนการจัดการข้อมูลหรือวงจรชีวิตของข้อมูล ซึ่งจะต้องประกอบไปด้วยนโยบายต่าง ๆ หรือหมวดนโยบายตามกรอบนโยบายข้อมูล (Data Policy Framework)



ก. หมวดทั่วไป (General Domain) เพื่อกำหนดนโยบายทั่วไปที่เกี่ยวข้องกับข้อมูล เช่น โครงสร้างที่เกี่ยวข้องหน้าที่ความรับผิดชอบ โดยมีรายละเอียด ดังนี้

- กำหนดบทบาทและความรับผิดชอบที่ประกอบกันเป็นโครงสร้างธรรมาภิบาลข้อมูล โดยต้องได้รับการมอบอำนาจและการอนุมัติจากผู้บริหาร
- กำหนดกลุ่มบุคคลหรือบุคคลภายในหน่วยงานเพื่อเป็นเจ้าของข้อมูลในการบริหารจัดการข้อมูลของหน่วยงานเพราะหน่วยงานถือเป็นเจ้าของข้อมูลทุกประเภทที่เกิดจากการดำเนินงานภายในหน่วยงานนั้น ๆ
- กำหนดขอบเขตข้อมูลทีนโยบายข้อมูลครอบคลุม เช่น ข้อมูลที่มีโครงสร้าง (ฐานข้อมูลและ CSV) ข้อมูลกึ่งโครงสร้าง (XML และ JSON) ข้อมูลที่ไม่มีโครงสร้าง (เอกสาร เสียงภาพ และ ภาพเคลื่อนไหว)
- กำหนดนโยบายมาตรการการรักษาความปลอดภัยของข้อมูล เพื่อป้องกันการเข้าถึง การสูญหาย การทำลาย หรือการเปลี่ยนแปลงข้อมูลโดยไม่ได้รับการอนุญาต
- นำระบบเทคโนโลยีสารสนเทศหรือระบบอัตโนมัติมาใช้ในการจัดทำเมตาดาตา
- ตรวจสอบความสอดคล้องกันระหว่างนโยบายข้อมูลกับการดำเนินการใด ๆ ของผู้มีส่วนได้ส่วนเสียอย่างน้อยปีละ 1 ครั้ง
- ทบทวนนโยบายข้อมูลอย่างน้อยปีละ 1 ครั้ง และให้ดำเนินการปรับปรุงอย่างต่อเนื่อง หากพบว่านโยบายข้อมูลยังไม่มีประสิทธิภาพเพียงพอ

- สื่อสารและเผยแพร่นโยบายข้อมูลให้กับผู้ที่เกี่ยวข้องทั้งภายในหน่วยงานและภายนอกหน่วยงาน

- สนับสนุนให้มีการฝึกอบรมเพื่อสร้างความตระหนักถึงธรรมาภิบาลข้อมูล และการบริหารจัดการข้อมูล โดยให้ครอบคลุมทุกระบวนการของการบริหารจัดการและระบบบริหารและกระบวนการจัดการข้อมูล (วงจรชีวิตของข้อมูล)

ข. หมวดการจัดเก็บข้อมูลและทำลายข้อมูล (Data Storage and Destruction Domain) เพื่อกำหนดนโยบายในการจัดเก็บข้อมูลและทำลายข้อมูลอย่างมีคุณภาพมีการรักษาความปลอดภัยของข้อมูล โดยมีรายละเอียด ดังนี้

- กำหนดสภาพแวดล้อมของการจัดเก็บข้อมูลที่เอื้อต่อการรักษาความมั่นคงปลอดภัยและคุณภาพของข้อมูล

- กำหนดชั้นความลับของข้อมูลและจัดเก็บให้สอดคล้องกับแนวทางหรือ มาตรฐานการจัดชั้นความลับของข้อมูล (Data Classification Guideline/Standard) ที่กำหนดไว้เพื่อให้ข้อมูลมีความมั่นคงปลอดภัยและรักษาคุณภาพของข้อมูล

- กำหนดสิทธิ์การเข้าถึงข้อมูลและเครื่องมือที่ใช้ในการเข้าถึงข้อมูล

- จัดเก็บข้อมูลให้สอดคล้องกับความต้องการและวัตถุประสงค์ในการดำเนินงาน โดยข้อมูลจะต้องมีความถูกต้อง สมบูรณ์และเป็นปัจจุบันอยู่เสมอ ทั้งนี้ ควรจัดทำเมทาดาตาสำหรับชุดข้อมูลที่มีการจัดเก็บ

- ในกรณีที่มีการร้องขอให้ทำลายข้อมูลส่วนบุคคลจากเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลหรือหน่วยงานที่จัดเก็บต้องดำเนินการทำลายให้เร็วที่สุด ทั้งนี้ต้องไม่ขัดต่อข้อตกลงระหว่างเจ้าของข้อมูลส่วนบุคคลกับผู้ควบคุมข้อมูลส่วนบุคคล หรือไม่ขัดต่อข้อกำหนดใด ๆ

- กำหนดแนวทางในการทำลายข้อมูล เมื่อข้อมูลนั้นไม่มีการใช้งานหรือมีการเก็บข้อมูลไว้นานเกินกว่าระยะเวลาที่กำหนด แต่ควรมีการเก็บรักษาเมทาดาตาของข้อมูลที่ทำลายไว้เพื่อใช้ สำหรับการตรวจสอบภายหลัง

- สร้างความรู้ความเข้าใจในการจัดเก็บและทำลายข้อมูลแก่ผู้ที่เกี่ยวข้องทั้งภายในหน่วยงานและภายนอกหน่วยงาน

ค. หมวดการประมวลผลข้อมูลและการใช้ข้อมูล (Data Processing and Use Domain) เพื่อกำหนดนโยบายในการประมวลผลข้อมูลและการใช้ข้อมูลให้ได้ข้อมูลที่มีประสิทธิภาพ ถูกต้องตรงตามวัตถุประสงค์ของการใช้ข้อมูลให้เกิดประโยชน์ โดยมีรายละเอียดดังนี้

- กำหนดแนวปฏิบัติและมาตรฐานของการประมวลผลข้อมูลและทำการสื่อสารให้แก่ผู้ที่เกี่ยวข้องรับทราบ

- การดำเนินการประมวลผลข้อมูลที่เป็นความลับ เช่น ข้อมูลส่วนบุคคล ให้เป็นไปตามขอบเขต เงื่อนไข หรือวัตถุประสงค์ในการยินยอมให้ดำเนินการกับข้อมูลส่วนบุคคล

- จัดทำเมทาดาตาสำหรับข้อมูลที่จัดเก็บอยู่ในคลังข้อมูล (Data Warehouse)

- ต้องมีการบันทึกประวัติการประมวลผลและการใช้ข้อมูล (Log File) เพื่อให้สามารถตรวจสอบย้อนกลับได้

ง. หมวดการแลกเปลี่ยนและการเชื่อมโยงข้อมูล (Data Exchange and Integration Domain) เพื่อกำหนดนโยบายในการแลกเปลี่ยนข้อมูลระหว่างหน่วยงานให้มีความมั่นคงปลอดภัยและข้อมูลมีคุณภาพ สามารถนำไปใช้ประโยชน์ได้อย่างมีประสิทธิภาพ โดยมีรายละเอียด ดังนี้

- กำหนดแนวปฏิบัติในการจัดการเรื่องความมั่นคงปลอดภัยคุณภาพข้อมูลและ
ผู้ประสานงานหรือศูนย์ติดต่อ (Contact Center)

- กำหนดกระบวนการในการแลกเปลี่ยนข้อมูลให้ชัดเจนเริ่มตั้งแต่ขั้นตอนการ
เตรียมการ ขั้นตอนเริ่มดำเนินการ ขั้นตอนระหว่างดำเนินการ และขั้นตอนสิ้นสุดการดำเนินการ

- กำหนดเมทาดาตาของชุดข้อมูลที่ต้องการแลกเปลี่ยนที่จำเป็นให้ครบถ้วน
- ทำสัญญาอนุญาตหรือข้อตกลงในการแลกเปลี่ยนข้อมูลและการนำข้อมูลไปใช้
- กำหนดเทคโนโลยีและมาตรฐานทางเทคนิคที่ใช้ในการแลกเปลี่ยนข้อมูล
- บันทึกรายละเอียดและจัดเก็บข้อมูลการดำเนินงานที่เกิดขึ้นในแต่ละครั้งที่มีการ
แลกเปลี่ยนข้อมูล (Log File) ระหว่างหน่วยงานเพื่อให้สามารถตรวจสอบย้อนกลับได้

- สามารถตรวจสอบได้ว่าการแลกเปลี่ยนข้อมูลได้ดำเนินการอย่างเหมาะสม หรือ
เป็นไปตามแนวทางปฏิบัติกระบวนการแลกเปลี่ยน และมาตรฐานตามที่กำหนด

จ. หมวดการเปิดเผยข้อมูล (Data Disclosure Domain) เพื่อกำหนดนโยบายในการ
เปิดเผยข้อมูล เพื่อให้สามารถเปิดเผยข้อมูลได้อย่างถูกต้องตรงตามวัตถุประสงค์ของการให้นำข้อมูลไปใช้ประโยชน์
โดยมีรายละเอียด ดังนี้

- ห้ามเปิดเผยข้อมูลที่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง นโยบาย แนวปฏิบัติ
ไม่ว่าข้อมูลจะอยู่ในรูปแบบใดหรือสถานที่ใดก็ตาม

- ต้องได้รับการอนุญาตจากตัวแทนหน่วยงานหรือเจ้าของข้อมูลก่อนการเปิดเผยข้อมูล
- ควรมีการระบุช่องทางการเปิดเผยข้อมูลที่เข้าถึงและนำไปใช้ได้ง่าย
- ควรมีการเปิดเผยเมทาดาตาควบคู่ไปกับข้อมูลที่เปิดเผย
- สามารถตรวจสอบได้ว่าการเปิดเผยข้อมูลได้ถูกดำเนินการอย่างเหมาะสมหรือเป็นไป
ตามแนวทางที่ได้กำหนดไว้ เพื่อให้ได้ข้อมูลที่มีคุณภาพและเป็นการรักษาคุณภาพของข้อมูล

2) มาตรฐานข้อมูล (Data Standards) มาตรฐานข้อมูลอ้างอิงมาตรฐานที่เกี่ยวข้องกับการ
บริหารจัดการข้อมูลและการใช้ข้อมูล ซึ่งเป็นกลไกอย่างหนึ่งในธรรมาภิบาลข้อมูลมีวัตถุประสงค์เพื่อสร้าง
ความเข้าใจที่ตรงกัน และลดความหลากหลายของวิธีการปฏิบัติ เช่น มาตรฐานเมทาดาตา (Metadata
Standard) มาตรฐานชุดข้อมูล (Datasets Standard) มาตรฐานการจัดชั้นความลับของข้อมูล (Data
Classification Standard) โดยมีรายละเอียดในแต่ละมาตรฐาน ดังนี้

ก. มาตรฐานเมทาดาตา (Metadata Standard) คือ การกำหนดรูปแบบและข้อกำหนด
ของเมทาดาตา โดยระบุรายละเอียด แหล่งข้อมูล และคำอธิบายรายละเอียดเกี่ยวกับข้อมูล ซึ่งจะช่วยให้ผู้ใช้ข้อมูล
ทราบว่าข้อมูลมาจากแหล่งใด มีรูปแบบอย่างไร เพื่อให้สามารถเข้าใจได้ถูกต้องตรงกันตลอดทั้งหน่วยงาน
ISO/IEC 11179 และ Dublin Core Metadata Initiative (DCMI) ได้กำหนดมาตรฐานเมทาดาตาสำหรับ
อธิบายชุดข้อมูล เช่น ชื่อ ข้อมูล ชื่อเจ้าของข้อมูล คำอธิบายข้อมูล ขอบเขตการจัดเก็บ รูปแบบข้อมูล ภาษา สิทธิ
การเข้าถึง ทั้งนี้ มาตรฐานเมทาดาต้ามักจะอ้างอิงถึงทั้งเมทาดาตาเชิงธุรกิจและเมทาดาตาเชิงเทคนิค แต่มักจะไม่
รวมองค์ประกอบของฟิลด์ข้อมูล ซึ่งเป็นคุณลักษณะเฉพาะของแต่ละชุดข้อมูล

ข. มาตรฐานชุดข้อมูล (Datasets Standard) คือ การกำหนดรูปแบบและข้อกำหนด
ของข้อมูลที่มีการใช้ร่วมกันจากหลาย ๆ ส่วนงานหรือหน่วยงาน เพื่อลดความซ้ำซ้อนของข้อมูล ลดความยุ่งยาก
ในการบริหารจัดการ และสนับสนุนให้ข้อมูลมีคุณภาพ ซึ่งส่วนงานหรือหน่วยงานต้องร่วมกันกำหนดเมทาดาตาขึ้นมา

เพื่ออธิบายคุณลักษณะของชุดข้อมูลที่ใช้ร่วมกัน แล้วดำเนินการบูรณาการข้อมูลที่กระจายอยู่ตามส่วนงานหรือหน่วยงานต่าง ๆ เข้าด้วยกัน มาตรฐานชุดข้อมูลมักจะอธิบายถึงองค์ประกอบของฟิลด์ข้อมูล เช่น ชื่อฟิลด์ข้อมูล ประเภทข้อมูล (เช่น ตัวเลข ตัวหนังสือ วันที่) ช่วงค่าของข้อมูล และการอนุญาตให้ฟิลด์ข้อมูลเป็นค่าว่าง

3) มาตรฐานการจัดชั้นความลับของข้อมูล (Data Classification Standard) คือ การกำหนดรูปแบบ และข้อกำหนดของการจัดชั้นความลับของข้อมูล เพื่อป้องกันการเข้าถึงและสามารถนำข้อมูลไปใช้ได้เหมาะสม ชั้นความลับของข้อมูลมักถูกกำหนดให้สอดคล้องกับผลกระทบต่อหน่วยงานและความมั่นคงของประเทศ ตัวอย่างชั้นความลับ ได้แก่ ลับที่สุด ลับมาก ลับ และเปิดเผยได้ ตัวอย่างประเภทของผลกระทบ

(1) ด้านความมั่นคงและผลประโยชน์ของชาติ เช่น เปิดเผยแล้วจะกระทบต่อความสัมพันธ์ระหว่างประเทศ หรือมีผลกระทบต่อภาพรวมของเศรษฐกิจ รวมทั้งอาจกระทบต่อความสงบเรียบร้อยภายในประเทศ

(2) ด้านภาพลักษณ์และความเชื่อมั่น ความโปร่งใสในการบริหารจัดการองค์กร สูญเสียภาพลักษณ์ที่ดี รวมทั้งทำให้ระดับความเชื่อมั่นในการบริหารจัดการองค์กรลดต่ำลง

(3) ด้านความต่อเนื่องของการดำเนินการ เช่น ข้อมูลระบบเครือข่ายถูกเปิดเผยทำให้ระบบเครือข่ายหรือระบบอินเทอร์เน็ตถูกโจมตี ส่งผลให้การดำเนินงานของหน่วยงานหยุดชะงักหรือล่าช้า

(4) ด้านการเงิน เช่น ค่าเสียหายหรือค่าใช้จ่ายที่จะเกิดขึ้น หากข้อมูลมีการถูกเปิดเผย

(5) ด้านทรัพยากรบุคคล เช่น ข้อมูลเงินเดือนถูกเปิดเผย ส่งผลให้บุคลากรต้องลาออก

3.3 กระบวนการกำกับดูแลข้อมูล (Data governance processes)

3.3.1 กระบวนการจัดการข้อมูลและการคุ้มครองข้อมูล

หลังจากการจัดตั้งคณะกรรมการธรรมาภิบาลข้อมูลภาครัฐ และทีมบริการข้อมูล รวมถึงทราบบทบาทหน้าที่ความรับผิดชอบของผู้มีส่วนได้ส่วนเสียกับข้อมูลในข้างต้นแล้ว สิ่งที่ต้องดำเนินการถัดไปคือ การบริหารจัดการข้อมูลตามวงจรชีวิตของข้อมูลในบทที่ 2 โดยแบ่งออกเป็น 6 ขั้นตอน ได้แก่ การสร้าง การจัดเก็บ การประมวลผลหรือใช้ การเผยแพร่ การจัดเก็บ และการทำลาย

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ได้รวบรวมข้อมูลและวิเคราะห์เพื่อกำหนดกระบวนการจัดการข้อมูลและการคุ้มครองข้อมูลให้เป็นไปตามมาตรา 8 ของพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 โดยมีรายละเอียดดังนี้

1) การสร้างข้อมูล

การสร้างข้อมูลเป็นขั้นตอนแรกของวงจรชีวิตข้อมูล เป็นการสร้างข้อมูลขึ้นมาใหม่ หรือปรับปรุงข้อมูลขึ้นใหม่ โดยวิธีการบันทึกเข้าไปด้วยบุคคล หรือบันทึกอัตโนมัติด้วยอุปกรณ์อิเล็กทรอนิกส์ หรือการรับข้อมูลจากหน่วยงานอื่นที่กรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงานเป็นผู้ดูแลข้อมูล มีวัตถุประสงค์เพื่อกำหนดแนวปฏิบัติ สำหรับผู้ที่เกี่ยวข้องในการสร้างข้อมูลให้มีคุณภาพ มีความมั่นคงปลอดภัยและเป็นประโยชน์ต่อผู้ใช้ข้อมูล โดยมีแนวทางการปฏิบัติงานของผู้มีส่วนได้ส่วนเสียกับข้อมูล และกิจกรรมที่ต้องดำเนินการดังตารางที่ 3.4 และ 3.5 ตามลำดับ โดยมีแผนภาพประกอบแนวปฏิบัติแสดงดังรูปที่ 3.5

ตารางที่ 3.4 แนวทางการปฏิบัติงานของผู้มีส่วนได้ส่วนเสียกับการสร้างข้อมูล

ผู้มีส่วนได้ส่วนเสีย	แนวปฏิบัติ
ผู้สร้างข้อมูล (Data Creators) เจ้าของข้อมูล (Data Owners) บริการข้อมูล (Data Stewards) ผู้ดูแลระบบสารสนเทศ (System Administrators)	1. เจ้าของข้อมูล/บริการข้อมูลเป็นผู้กำหนดผู้มีสิทธิ์ในการสร้างข้อมูล และจะต้องทบทวนสิทธิ์นั้น อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ ได้แก่ การลาออก เปลี่ยนตำแหน่ง โอนย้าย สิ้นสุดการจ้างการปรับ โครงสร้าง หรือเมื่อมีการปรับปรุงระบบสารสนเทศ เป็นต้น 2. เจ้าของข้อมูล/ทีมบริการข้อมูลเป็นผู้กำหนดชั้นความลับของข้อมูลของข้อมูลที่ถูกสร้างขึ้นตามการจำแนกชั้นความลับของข้อมูลของคู่มือฉบับนี้ 3. กำหนดให้มีวิธีปฏิบัติการจำแนกชั้นความลับของข้อมูลสำหรับชุดข้อมูลที่ ถูกสร้างขึ้น 4. ผู้ดูแลระบบสารสนเทศจะต้องกำหนดสิทธิในการสร้างข้อมูลให้แก่ผู้สร้างข้อมูลตามที่เจ้าของข้อมูลกำหนด 5. เจ้าของข้อมูลและทีมบริการข้อมูลร่วมจัดทำคำอธิบายชุดข้อมูล (Metadata) เมื่อมีการสร้างชุดข้อมูล (Datasets) ตามมาตรฐานขั้นต่ำคำอธิบาย ชุดข้อมูลที่ สพร. กำหนด และกำหนดให้ทำการประเมินคุณค่าของชุดข้อมูลตามแบบฟอร์ม ประเมินคุณค่าชุดข้อมูลที่ สพร. หรือตามที่คู่มือฉบับนี้กำหนด และเผยแพร่เป็นข้อมูลเปิดของหน่วยงานต่อสาธารณะตามกฎหมายว่าด้วยข้อมูล ข่าวสารของ ราชการในรูปแบบข้อมูลดิจิทัล และ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล 6. ห้ามมิให้ผู้สร้างข้อมูลนำข้อมูลที่มีลักษณะดังต่อไปนี้เข้าสู่ระบบคอมพิวเตอร์ ที่ขัดต่อกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ - ข้อมูลที่บิดเบือน หรือปลอมไม่ว่าทั้งหมดหรือบางส่วน - ข้อมูลอันเป็นเท็จที่นำจะเกิดความเสียหายต่อการรักษาความมั่นคง ปลอดภัย ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจ หรือโครงสร้างพื้นฐาน หรือก่อให้เกิดความตื่นตระหนก - ข้อมูลอันเป็นความผิดเกี่ยวกับความมั่นคง หรือความผิดเกี่ยวกับการก่อการร้าย - ข้อมูลที่มีลักษณะอันลามก - ข้อมูลที่ปรากฏภาพของผู้อื่น และเป็นภาพที่สร้างขึ้น ตัดต่อ เดิม หรือ ดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ ทำให้ผู้อื่นเสียชื่อเสียง ถูกดูหมิ่นถูกเกลียดชัง หรือได้รับความอับอาย 7. ห้ามมิให้ผู้สร้างข้อมูล ทำการสร้าง/ทำซ้ำต่อข้อมูลที่ขัดต่อกฎหมายว่า ด้วยลิขสิทธิ์ หรือทรัพย์สินทางปัญญาของผู้อื่นเว้นแต่จะเป็นไปตามอำนาจที่ กฎหมายรับรอง 8. กำหนดให้ผู้สร้างข้อมูลสร้างข้อมูลที่มาจากแหล่งข้อมูลที่เชื่อถือได้เท่านั้น 9. กำหนดให้เจ้าของข้อมูลตรวจสอบความถูกต้องของข้อมูลที่ถูกสร้างขึ้น 10. กำหนดให้มีวิธีปฏิบัติเกี่ยวกับสร้างข้อมูลให้มีความปลอดภัย และเป็น ประโยชน์ต่อผู้ใช้ข้อมูล

ตารางที่ 3.5 แสดงกิจกรรมที่ต้องดำเนินการของผู้มีส่วนได้ส่วนเสียกับการสร้างข้อมูล

กิจกรรม	ผู้มีส่วนได้ส่วนเสีย			
	ผู้สร้างข้อมูล	เจ้าของข้อมูล	บริการข้อมูล	ผู้ดูแลระบบสารสนเทศ
กำหนดผู้มีสิทธิ์ในการสร้างข้อมูล		/		
กำหนดสิทธิ์ในการสร้างข้อมูลให้แก่ผู้สร้างข้อมูล				/
สร้างข้อมูลที่ไม่ขัดต่อกฎหมายและจากแหล่งข้อมูล ที่เชื่อถือได้เท่านั้น	/			
กำหนดชั้นความลับข้อมูลของข้อมูลที่ถูกสร้างขึ้น		/		
จัดทำคำอธิบายชุดข้อมูล		/	/	
ประเมินคุณค่าของชุดข้อมูล		/		
ตรวจสอบความถูกต้องของข้อมูล		/		

1



2



3



4



รูปที่ 3.5 แผนภาพแนวปฏิบัติการสร้างข้อมูล

2) การจัดเก็บข้อมูล

การจัดเก็บข้อมูลที่เกิดจากกระบวนการสร้างหรือข้อมูลที่ได้จากการเชื่อมโยงและ/หรือ แลกเปลี่ยนกับหน่วยงานอื่น ไม่ว่าจะจัดเก็บลงไฟล์ข้อมูล (File) เพื่อให้เกิดความมีระเบียบง่ายต่อการใช้งาน ข้อมูลไม่สูญหายหรือถูกทำลาย และช่วยให้ผู้ใช้งานสามารถประมวลผลข้อมูลได้อย่างรวดเร็ว มีวัตถุประสงค์ เพื่อกำหนดแนวปฏิบัติสำหรับผู้ที่เกี่ยวข้องในการจัดเก็บข้อมูล ให้มีคุณภาพ เข้าถึงและใช้งานได้อย่างมั่นคง ปลอดภัย อย่างไรก็ตามจากการเก็บและวิเคราะห์ข้อมูลของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร พบว่า กรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงานยังมีข้อมูลที่ยังอยู่ในรูปเอกสาร แฟ้มข้อมูล และไฟล์ข้อมูล ดังนั้นเพื่อให้มั่นใจว่า กรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงานได้มีจัดเก็บข้อมูลอย่างถูกต้องเป็นไปตามกฎหมาย ระเบียบของทางราชการ แนวปฏิบัติการจัดเก็บ ข้อมูลนี้จึงรวมไปถึงข้อมูลที่เป็นเอกสาร และการดูแลอุปกรณ์ที่เกี่ยวข้องด้วย โดยมีแนวทางการปฏิบัติงานของผู้มีส่วนได้ส่วนเสียกับข้อมูล และกิจกรรมที่ต้อง ดำเนินการดังตารางที่ 3.6 และ 3.7 ตามลำดับ โดยมีแผนภาพประกอบแนวปฏิบัติแสดงดังรูปที่ 3.6

ตารางที่ 3.6 แนวทางการปฏิบัติงานของผู้มีส่วนได้ส่วนเสียกับข้อมูล ด้านการจัดเก็บข้อมูล

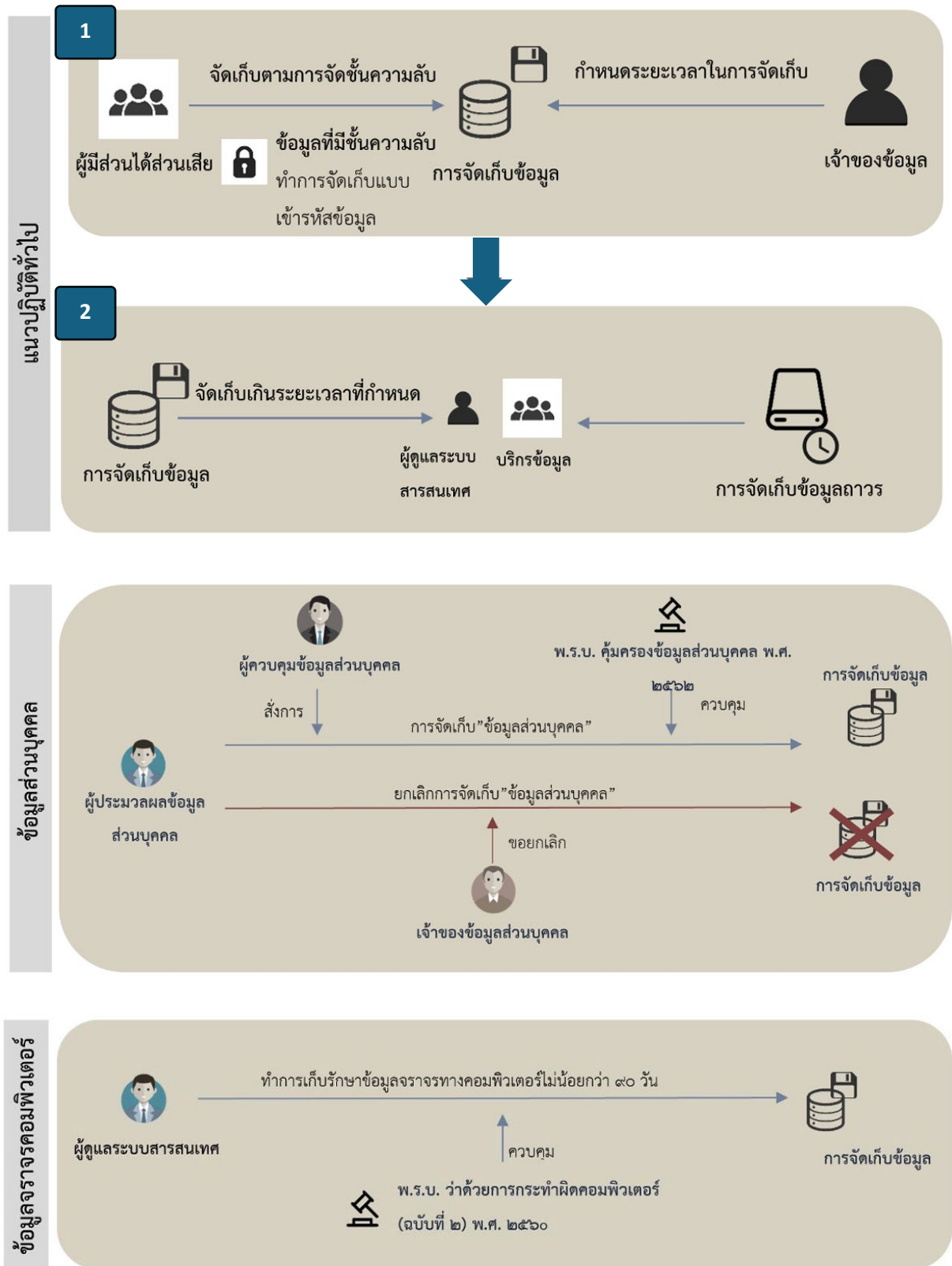
ผู้มีส่วนได้ส่วนเสีย	แนวปฏิบัติ
เจ้าของข้อมูล (Data Owners) ผู้สร้างข้อมูล (Data Creators) ผู้ใช้ข้อมูล (Data Users) บริกรข้อมูล (Data Stewards) ผู้ดูแลระบบสารสนเทศ (System Administrators)	- กำหนดให้การจัดเก็บชุดข้อมูลจะต้องมีคำอธิบายชุดข้อมูลหรือเมทาดาตา หากไม่มีหรือไม่ครบถ้วน ทีมบริหารจัดการข้อมูลจะต้องแจ้งผู้รับผิดชอบ ได้แก่ เจ้าของข้อมูล และบริกรข้อมูล ร่วมกันจัดทำและปรับปรุงให้เป็นปัจจุบัน - กำหนดให้เจ้าของข้อมูลจะต้องกำหนดระยะเวลาในการจัดเก็บข้อมูลที่ชัดเจน - กำหนดให้บริกรข้อมูลและผู้ดูแลระบบสารสนเทศทำการย้ายข้อมูลที่มีการจัดเก็บเกินระยะเวลาที่กำหนดแล้ว เพื่อจัดเก็บเป็นข้อมูลถาวร - ผู้มีส่วนได้ส่วนเสียเกี่ยวกับข้อมูล ทั้งเจ้าของข้อมูล ผู้สร้างข้อมูล ผู้ใช้ข้อมูล และบริกรข้อมูลจะต้องจัดเก็บข้อมูลตามการจัดชั้นความลับของกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน - กำหนดให้ผู้มีส่วนได้ส่วนเสียเกี่ยวกับข้อมูล ทั้งเจ้าของข้อมูล ผู้สร้างข้อมูล ผู้ใช้ข้อมูล และบริกรข้อมูล จัดเก็บข้อมูลที่มีชั้นความลับโดยทำการเข้ารหัสข้อมูล เพื่อป้องกันการเข้าถึงหรือแก้ไขข้อมูลโดยไม่ได้รับอนุญาต ทั้งนี้การเข้ารหัสข้อมูลให้ปฏิบัติตามวิธีการเข้ารหัสข้อมูลแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงานสำหรับกรณีที่ในตารางฐานข้อมูลเดียวกันมีฟิลด์ข้อมูลที่มีชั้นความลับและไม่มีชั้นความลับอยู่ร่วมกัน ให้ทำการเข้ารหัสข้อมูลเฉพาะฟิลด์ข้อมูลที่มีชั้นความลับเท่านั้น สำหรับกรณีข้อมูลที่จัดเก็บในรูปแบบเอกสาร ให้มีการจัดเก็บดังนี้ - เก็บในสถานที่เหมาะสม สามารถปิดล็อกได้เมื่อไม่ใช้งาน - เก็บแยกออกจากอุปกรณ์ประมวลผลต่าง ๆ เช่น เครื่องพิมพ์ เครื่องถ่ายเอกสาร เป็นต้น โดยทันที เพื่อเป็นการป้องกันไม่ให้ผู้ไม่มีสิทธิ์ในการ

ผู้มีส่วนได้ส่วนเสีย	แนวปฏิบัติ
	เข้าถึงข้อมูลได้ 6. กำหนดให้มีการจัดเก็บข้อมูลส่วนบุคคล โดยให้เก็บรวบรวมได้เท่าที่จำเป็น ภายใต้อำนาจหน้าที่และวัตถุประสงค์อันชอบด้วยกฎหมายว่าด้วยการคุ้มครอง ข้อมูลส่วนบุคคล และไม่เก็บรวบรวมข้อมูลส่วนบุคคล ดังต่อไปนี้ เว้นแต่ได้รับการยินยอมจากเจ้าของข้อมูล - เชื้อชาติ - เผ่าพันธุ์ - ความคิดเห็นทางการเมือง - ความเชื่อในลัทธิ ศาสนาหรือปรัชญา - พฤติกรรมทางเพศ - ประวัติอาชญากรรม - ข้อมูลสุขภาพ ความพิการ หรือข้อมูลสุขภาพจิต - ข้อมูลสหภาพแรงงาน - ข้อมูลพันธุกรรม - ข้อมูลชีวภาพ - ข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลในทำนองเดียวกันตามที่ หน่วยงานกำหนด 7. กำหนดให้การยกเลิกการจัดเก็บข้อมูล กรณีเจ้าของข้อมูลถอนความยินยอม ตามที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลกำหนด 8. กำหนดให้มีการจัดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่า 90 วัน นับแต่วันที่ข้อมูลเข้าสู่ระบบคอมพิวเตอร์ โดยจัดเก็บรักษาข้อมูล ของผู้ใช้บริการเท่าที่จำเป็น เพื่อให้สามารถระบุตัวผู้ใช้บริการนับแต่เริ่มใช้ บริการให้สอดคล้องตามกฎหมายว่าด้วยการกระทำความผิดทาง คอมพิวเตอร์ 9. กำหนดให้มีการจัดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ให้สอดคล้องตาม กฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ ผู้ให้บริการจะต้องใช้ วิธีการที่มั่นคงปลอดภัยอย่างน้อย ดังนี้ - เก็บในสื่อ (Media) ที่สามารถรักษาความครบถ้วน ถูกต้องแท้จริง (Integrity) และระบุตัวตน (Identification) ที่เข้าถึงสื่อดังกล่าวได้ - มีระบบการเก็บรักษาความลับของข้อมูลที่จัดเก็บ และกำหนดชั้น ความลับในการเข้าถึงข้อมูลดังกล่าว เพื่อรักษาความน่าเชื่อถือของ ข้อมูล และไม่อนุญาตให้ผู้ดูแลระบบแม่ข่ายแก้ไขข้อมูลที่จัดเก็บไว้ได้ - การจัดเก็บข้อมูลต้องสามารถระบุรายละเอียดผู้ใช้งานเป็นรายบุคคลได้ 10. กำหนดให้มีมาตรการรักษาความปลอดภัยในการจัดเก็บข้อมูล รวมทั้ง กรณีที่มีการเคลื่อนย้ายอุปกรณ์ที่จัดเก็บข้อมูล เพื่อป้องกันมิให้มีการเข้าถึง

ผู้มีส่วนได้ส่วนเสีย	แนวปฏิบัติ
	โดยมิได้รับอนุญาต หรือลักลอบนำข้อมูลไปใช้ที่ก่อให้เกิดความเสียหายต่อหน่วยงาน - กำหนดมาตรการรักษาความปลอดภัยของข้อมูลที่จัดเก็บถาวร เพื่อป้องกันข้อมูลไม่ให้เกิดการลบ ปรับปรุง แก้ไขได้ รวมทั้งป้องกันมิให้ข้อมูลที่จัดเก็บถาวรรั่วไหลไปยังบุคคลที่ไม่ได้รับอนุญาต - กำหนดให้มีมาตรการรักษาความปลอดภัยของการถ่ายโอนข้อมูลกับหน่วยงานภายนอกที่ผ่านช่องทางการสื่อสารทุกชนิด โดยต้องสอดคล้องตามนโยบายความมั่นคงปลอดภัยสารสนเทศ - ห้ามมิให้จัดเก็บข้อมูลส่วนตัวหรือข้อมูลที่ไม่เกี่ยวข้องกับการดำเนินงานของหน่วยงานสำหรับการจัดเก็บข้อมูลถาวรบนเครื่องแม่ข่ายที่หน่วยงานจัดสรรไว้

ตารางที่ 3.7 แสดงกิจกรรมที่ต้องดำเนินการของผู้มีส่วนได้ส่วนเสียในการจัดเก็บข้อมูล

กิจกรรม	ผู้มีส่วนได้ส่วนเสีย				
	ผู้สร้างข้อมูล	เจ้าของข้อมูล	บริการข้อมูล	ผู้ดูแลระบบสารสนเทศ	ผู้ใช้ข้อมูล
กำหนดระยะเวลาในการจัดเก็บข้อมูล		/			
จัดเก็บข้อมูลตามการจัดชั้นความลับ	/	/	/		/
จัดเก็บข้อมูลที่มีชั้นความลับโดยทำการเข้ารหัสข้อมูล	/	/	/		/
จัดเก็บข้อมูลส่วนบุคคลเท่าที่จำเป็น				/	
ยกเลิกการจัดเก็บข้อมูลกรณีเจ้าของข้อมูลส่วนบุคคลถอนความยินยอม				/	
จัดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์				/	
ทำการย้ายข้อมูลที่มีการจัดเก็บเกินระยะเวลาที่กำหนดเพื่อจัดเก็บเป็นข้อมูลถาวร				/	



รูปที่ 3.6 แผนภาพแนวปฏิบัติการการจัดเก็บข้อมูล แต่ละประเภท

3) การประมวลผลหรือใช้

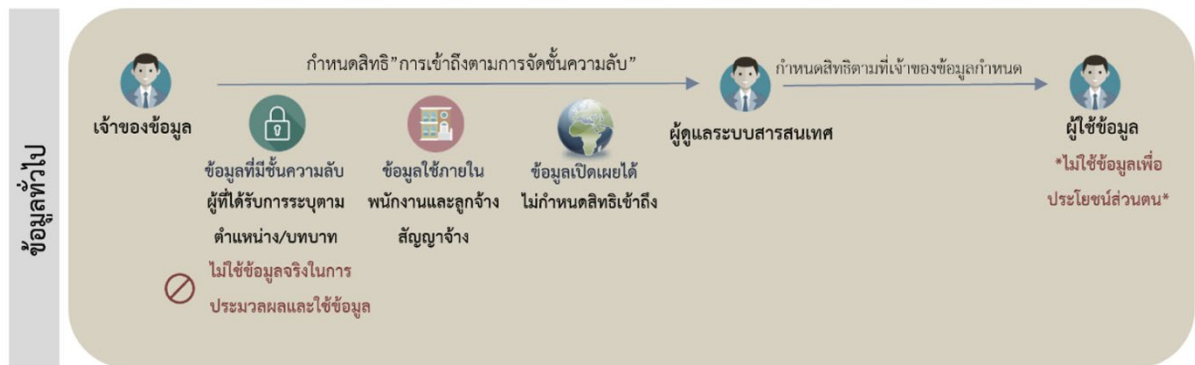
การประมวลผลหรือการใช้ข้อมูลเป็นการนำข้อมูลที่จัดเก็บมาประมวลผล ได้แก่ การถ่ายโอนข้อมูล การเปลี่ยนรูปแบบการ จัดเก็บข้อมูล การวิเคราะห์ข้อมูล การจัดทำรายงาน มีวัตถุประสงค์เพื่อนำข้อมูลที่ผ่านกระบวนการจัดเก็บข้อมูลมาใช้งาน ให้เกิดประโยชน์เพิ่มมูลค่าให้กับกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน เพื่อสนับสนุนการตัดสินใจด้านนโยบายและแผน และเป็นการกำหนดแนวปฏิบัติที่ตรงกันทั้งองค์กรในการประมวลผลข้อมูลและการใช้ข้อมูลที่มีประสิทธิภาพถูกต้องตรงตามวัตถุประสงค์ ไม่ผิดกฎหมายระเบียบและกฎเกณฑ์ที่จะนำมาซึ่งความเสียหายต่อทั้งตัวผู้ปฏิบัติงานและกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน โดยมีแนวทางการปฏิบัติงานของผู้มีส่วนได้ส่วนเสียกับข้อมูล และกิจกรรมที่ต้องดำเนินการดังตารางที่ 3.8 และ 3.9 ตามลำดับ โดยมีแผนภาพประกอบแนวปฏิบัติแสดงดังรูปที่ 3.7

ตารางที่ 3.8 แนวทางการปฏิบัติงานของผู้มีส่วนได้ส่วนเสียกับข้อมูลของการประมวลผลหรือการใช้ข้อมูล

ผู้มีส่วนได้ส่วนเสีย	แนวปฏิบัติ
เจ้าของข้อมูล (Data Owners) ผู้ใช้ข้อมูล (Data Users) บริกรข้อมูล (Data Stewards) ผู้ดูแลระบบสารสนเทศ (System Administrators)	1. เจ้าของข้อมูลจะต้องกำหนดผู้มีสิทธิ์เข้าถึงเพื่อประมวลผลและใช้ข้อมูลตามชั้นความลับ ดังนี้ - ข้อมูลที่มีชั้นความลับ กำหนดให้ผู้ใช้งานที่ได้รับสิทธิ์ตามตำแหน่ง/บทบาทเท่านั้น ทั้งนี้ผู้ใช้งานที่ได้รับสิทธิ์จะต้องไม่ใช่ข้อมูลจริงในการใช้งาน และประมวลผล - ข้อมูลใช้ภายใน กำหนดให้ผู้บริหาร เจ้าหน้าที่ และลูกจ้างเท่านั้น ที่มีสิทธิ์ เข้าถึงเพื่อประมวลผลและใช้งานข้อมูลได้ ทั้งนี้ต้องปกป้องข้อมูลจากการเข้าถึงโดยบุคคลภายนอก - ข้อมูลเปิดเผยได้ไม่กำหนดสิทธิ์การเข้าถึงเพื่อประมวลผลและใช้งานข้อมูล 2. เจ้าของข้อมูลจะต้องทบทวนสิทธิ์การเข้าถึงเพื่อประมวลผลและใช้ข้อมูลของผู้ใช้งาน อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ ได้แก่ การลาออก เปลี่ยนตำแหน่ง โอนย้าย สิ้นสุดการจ้าง การปรับโครงสร้าง หรือเมื่อมีการปรับปรุงระบบสารสนเทศ 3. ผู้ดูแลระบบสารสนเทศจะต้องกำหนดสิทธิ์ในการเข้าถึงเพื่อประมวลผลและใช้ข้อมูลผู้ใช้งานตามที่เจ้าของข้อมูลกำหนด 4. ผู้ที่มีสิทธิ์เข้าใช้งานข้อมูลที่มีชั้นความลับตามที่กำหนดโดยเจ้าของข้อมูล จะต้องใช้ข้อมูลอย่างระมัดระวัง โดยคำนึงถึงความปลอดภัยและต้องไม่ใช้งานข้อมูลที่มีชั้นความลับในพื้นที่สาธารณะ 5. ผู้ใช้ข้อมูลจะต้องไม่ใช่ข้อมูลในเครือข่ายของหน่วยงาน เพื่อประโยชน์ในเชิงธุรกิจเป็นการส่วนตัวหรือเพื่อเข้าสู่เว็บไซต์ที่ไม่เหมาะสมหรือใช้ข้อมูลอัน ก่อให้เกิดความเสียหายต่อกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน

ตารางที่ 3.9 แสดงกิจกรรมที่ต้องดำเนินการของผู้มีส่วนได้ส่วนเสียกับการประมวลผลหรือการใช้ข้อมูล

กิจกรรม	ผู้มีส่วนได้ส่วนเสีย			
	เจ้าของข้อมูล	บริการข้อมูล	ผู้ดูแลระบบสารสนเทศ	ผู้ใช้ข้อมูล
กำหนดผู้มีสิทธิ์ประมวลผลและเข้าใช้งานข้อมูลตามชั้นความลับ	/	/	/	
กำหนดสิทธิ์ในการประมวลผลและเข้าใช้งานข้อมูลให้แก่ผู้ใช้ข้อมูล			/	
ไม่ใช้ข้อมูลที่เป็นทรัพย์สินของกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน เพื่อประโยชน์ในเชิงธุรกิจเป็นการส่วนตัว				/



รูปที่ 3.7 แผนภาพแนวปฏิบัติการการประมวลผลหรือการใช้ข้อมูล

4) การเผยแพร่ข้อมูล

การเผยแพร่เป็นการนำข้อมูลที่อยู่ในความครอบครองของกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน เผยแพร่ตามช่องทางต่าง ๆ อย่างเหมาะสม อาทิ การเปิดเผยข้อมูล (Open data) การแชร์ข้อมูล (Sharing) การกระจายข้อมูล (Dissemination) การควบคุมการเข้าถึง (Access Control) การแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน (Exchange) และการกำหนดเงื่อนไขในการนำข้อมูลไปใช้ (Condition) ซึ่งในที่นี้จะขอกล่าวถึงแนวปฏิบัติการเปิดเผยแพร่ และการแลกเปลี่ยนข้อมูล เนื่องจากเป็นขั้นตอนที่มีการใช้งานเป็นจำนวนมากในปัจจุบัน

4.1) การเปิดเผยข้อมูล มีวัตถุประสงค์เพื่อกำหนดแนวปฏิบัติการเปิดเผยข้อมูลต่อสาธารณะโดยอิงจากกฎหมาย กฎเกณฑ์และแนวปฏิบัติที่เกี่ยวข้อง ทั้งนี้ ข้อมูลที่เปิดเผยควรเป็นประโยชน์สามารถนำไปประมวลผลและใช้ต่อยอดในการพัฒนาในรูปแบบต่าง ๆ ได้ ซึ่งมีแนวทางการปฏิบัติงานของผู้มีส่วนได้ส่วนเสียกับข้อมูล และกิจกรรมที่ต้องดำเนินการดังตารางที่ 3.10 และ 3.11 ตามลำดับ โดยมีแผนภาพประกอบแนวปฏิบัติแสดงดังรูปที่ 3.8

ตารางที่ 3.10 แนวทางการปฏิบัติงานของผู้มีส่วนได้ส่วนเสียกับข้อมูลของการเผยแพร่ข้อมูล

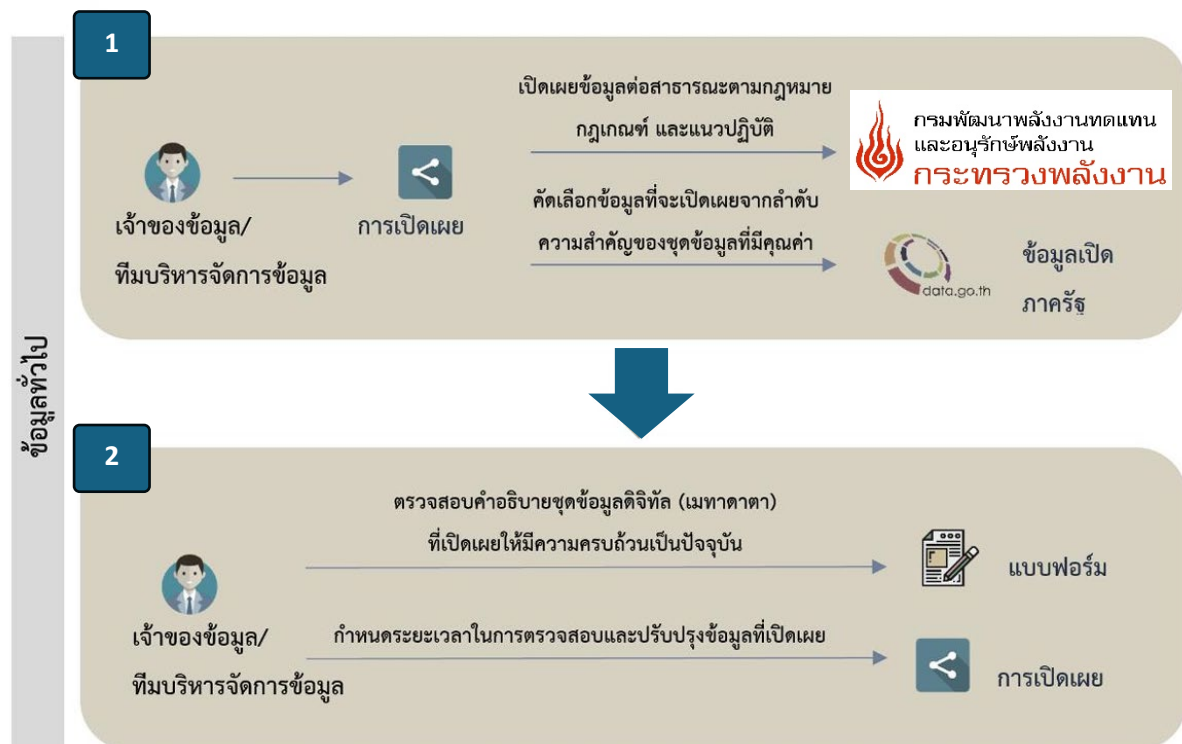
ผู้มีส่วนได้ส่วนเสีย	แนวปฏิบัติ
เจ้าของข้อมูล (Data Owners) ทีมบริหารจัดการข้อมูล (Data Management Team) ผู้ดูแลระบบสารสนเทศ (System Administrators)	1. เจ้าของข้อมูล/ทีมบริหารจัดการข้อมูลจะต้องเปิดเผยข้อมูลในความรับผิดชอบต่อสาธารณะตามกฎหมายว่าด้วยข้อมูลข่าวสารของราชการ และแนวปฏิบัติการเปิดเผยข้อมูลอย่างเคร่งครัด 2. เจ้าของข้อมูล/ทีมบริหารจัดการข้อมูลห้ามเปิดเผยข้อมูลความมั่นคง และข้อมูลความลับทางราชการที่อยู่ในความครอบครองของกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน 3. กำหนดให้เจ้าของข้อมูล/ทีมบริหารจัดการข้อมูลที่จะทำการเปิดเผยข้อมูลในความรับผิดชอบในรูปแบบข้อมูลเปิดของกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน โดยดำเนินการ ดังนี้ - กำหนดลักษณะของข้อมูลที่เผยแพร่กำหนดให้อยู่ในรูปแบบที่เครื่องสามารถประมวลผลได้ - กำหนดให้มีคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตา สำหรับข้อมูลที่ต้องเปิดเผย - ข้อมูลที่เผยแพร่จะต้องมีการบันทึกเวลา (Timestamps) ที่ช่วยให้ผู้ใช้งานสามารถระบุได้ว่าข้อมูลนั้นเป็นปัจจุบัน - ข้อมูลที่เผยแพร่ต้องมาจากแหล่งที่เก็บข้อมูลโดยตรง ด้วยระดับความละเอียดสูง โดยไม่มีการปรับแต่งหรือเป็นข้อมูลรูปแบบสรุป (Summary data) - ชุดข้อมูลและรายการชุดข้อมูลที่เผยแพร่จะต้องมีการจัดรูปแบบที่กำหนดเป็นมาตรฐาน และกำหนดภายใต้หมวดหมู่เดียวกันเพื่อให้ผู้ใช้ข้อมูลสามารถค้นหาและเข้าถึงข้อมูลได้ง่าย 4. เงื่อนไขและข้อกำหนดของข้อมูลที่จะนำมาเปิดเผยภายในเครือข่ายของกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงานข้อมูลที่เผยแพร่ต้องไม่ขัดต่อกฎหมายว่าด้วยทรัพย์สินทางปัญญา เว้นแต่การเปิดเผยข้อมูลจะเป็นไปตามอำนาจที่กฎหมายรับรอง โดยกำหนดให้ทีมบริหารจัดการข้อมูลเป็นผู้ดำเนินการตรวจสอบ 5. ให้ทีมบริหารจัดการข้อมูล/ผู้ดูแลระบบสารสนเทศสนับสนุนการเผยแพร่ข้อมูลผ่านช่องทางที่ง่ายต่อการเข้าถึงข้อมูล และต้องเปิดเผยข้อมูลในรูปแบบดิจิทัลต่อสาธารณะที่ศูนย์กลางข้อมูลเปิดภาครัฐ (Government Open Data) ผ่านเว็บไซต์ data.go.th โดย - กำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัยในการเปิดเผยข้อมูลที่กำหนดลำดับชั้นข้อมูลตั้งแต่ลับขึ้นไป อย่างเพียงพอและมีประสิทธิภาพ - มีการตรวจสอบข้อมูลที่เผยแพร่จากหน่วยงานทั้งภายในและภายนอกหน่วยงาน เพื่อให้มั่นใจว่าหน่วยงานได้มีข้อมูลที่เผยแพร่ที่มีคุณค่า

ผู้มีส่วนได้ส่วนเสีย	แนวปฏิบัติ
	- การเผยแพร่ข้อมูลต้องมีการตรวจสอบรูปแบบข้อมูลที่เผยแพร่ให้สอดคล้องกับมาตรฐานที่หน่วยงานกำหนด - หากการเปิดเผยนั้นเป็นการเปิดเผยบนช่องทางที่ดูแลรับผิดชอบโดยหน่วยงานอื่นที่ให้ปฏิบัติตามเอกสาร คู่มือ การนำข้อมูลขึ้นเผยแพร่ของหน่วยงานนั้น - หากการเปิดเผยข้อมูลไม่ครบถ้วนหรือไม่เป็นปัจจุบัน ให้แจ้งเจ้าของข้อมูล และบริการข้อมูลหากการจัดทำ/ปรับปรุงให้เป็นปัจจุบัน 6. กำหนดให้เปิดเผยข้อมูลส่วนบุคคลตามข้อกำหนดของ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล หรือตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลที่แต่งตั้งโดยหน่วยงานเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัติ 7. เจ้าของข้อมูลห้ามเปิดเผยข้อมูลความมั่นคง และข้อมูลความลับทางราชการที่อยู่ในความครอบครองของหน่วยงาน รวมทั้งห้ามเปิดเผยข้อมูลที่เป็นการกระทำความผิดตามกฎหมาย นโยบาย และแนวปฏิบัติอื่นทำให้เกิดความเสียหายต่อหน่วยงาน 8. กำหนดให้เจ้าของข้อมูลคัดเลือกข้อมูลที่จะเปิดเผยในรูปแบบข้อมูลเปิดจากลำดับชั้นความสำคัญของชุดข้อมูล 9. กำหนดให้เจ้าของข้อมูลต้องกำหนดรอบระยะเวลาในการตรวจสอบและปรับปรุงข้อมูลที่เปิดเผยเพื่อให้ข้อมูลถูกต้องและเป็นปัจจุบัน

ตารางที่ 3.11 แสดงกิจกรรมที่ต้องดำเนินการของผู้มีส่วนได้ส่วนเสียของการเผยแพร่ข้อมูล

กิจกรรม	ผู้มีส่วนได้ส่วนเสีย		
	เจ้าของข้อมูล	ผู้ดูแลระบบสารสนเทศ	ทีมบริหารจัดการข้อมูล
เปิดเผยข้อมูลกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน ในความรับผิดชอบต่อสาธารณะตามกฎหมายที่กำหนดไว้และลงบันทึกเวลา		/	/
คัดเลือกข้อมูลที่จะเปิดเผยในรูปแบบข้อมูลเปิดจากลำดับชั้นความสำคัญของข้อมูล	/		/
ตรวจสอบคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตาของชุดข้อมูลที่จะทำการเปิดเผยให้มีความครบถ้วนเป็นปัจจุบัน	/		/

กิจกรรม	ผู้มีส่วนได้ส่วนเสีย		
	เจ้าของข้อมูล	ผู้ดูแลระบบสารสนเทศ	ทีมบริหารจัดการข้อมูล
กำหนดกรอบระยะเวลาในการตรวจสอบและปรับปรุงข้อมูลที่เปิดเผย	/		/



รูปที่ 3.8 แผนภาพแนวปฏิบัติการเผยแพร่ข้อมูล

4.2) การแลกเปลี่ยนข้อมูล เป็นการนำข้อมูลที่จัดเก็บหรือที่ได้จากการประมวลผลมาเชื่อมโยงและแลกเปลี่ยนระหว่างหน่วยงานทั้งภายในและภายนอกได้อย่างมีประสิทธิภาพ มีวัตถุประสงค์เพื่อกำหนดแนวปฏิบัติและมาตรฐานด้านเทคนิคในการเชื่อมโยง และการแลกเปลี่ยนข้อมูลดิจิทัลทั้งระหว่างระบบสารสนเทศของหน่วยงานภายในกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน และระหว่างระบบสารสนเทศของกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงานกับหน่วยงานภายนอกอย่างมีประสิทธิภาพ และก่อให้เกิดประโยชน์ต่อภาคประชาชน ภาครัฐ และภาคเอกชน โดยมีแนวทางการปฏิบัติงานของผู้มีส่วนได้ส่วนเสียกับข้อมูล และกิจกรรมที่ต้องดำเนินการ ดังตารางที่ 3.12 และ 3.13 ตามลำดับ โดยมีแผนภาพประกอบแนวปฏิบัติแสดงดังรูปที่ 3.9

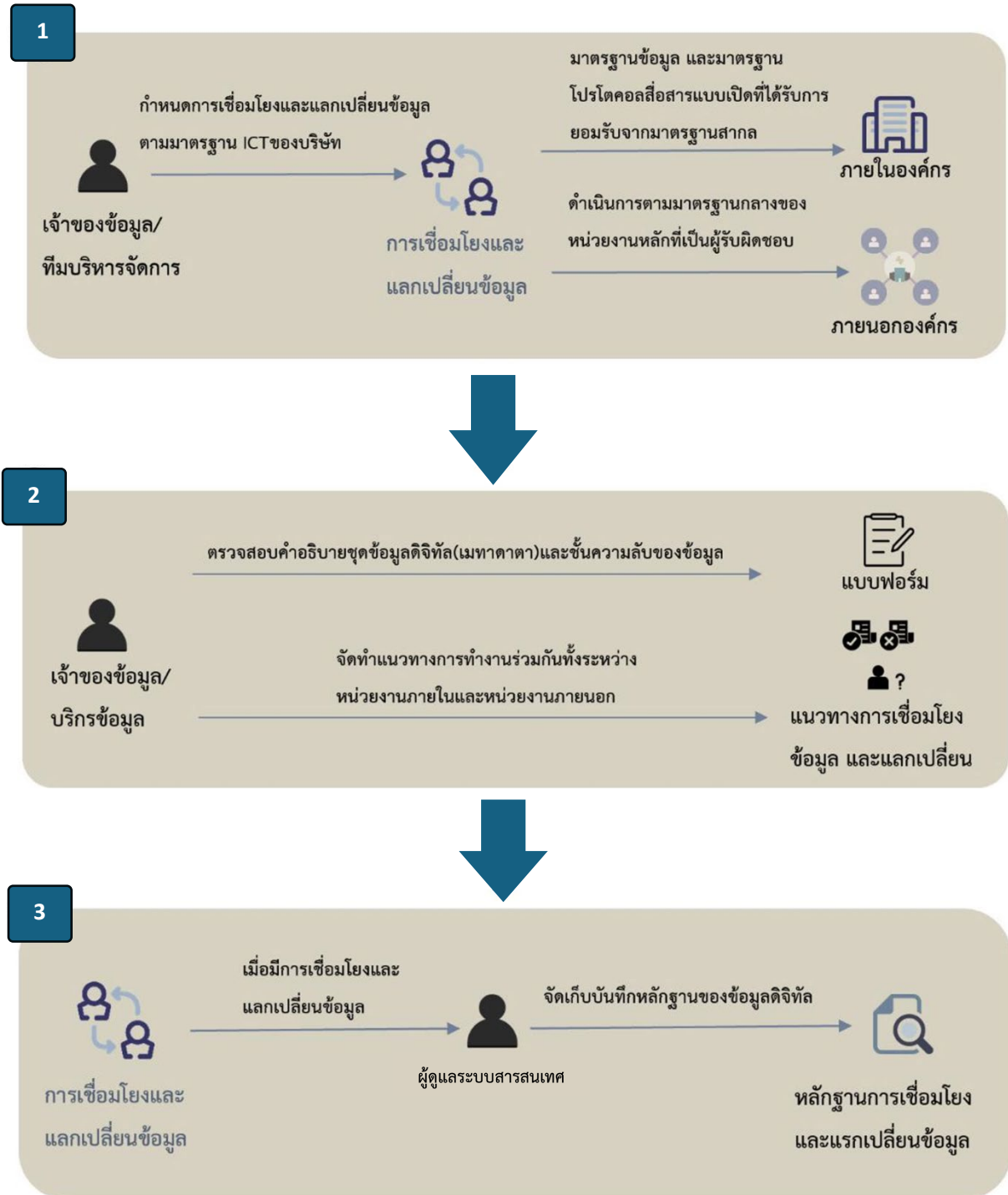
ตารางที่ 3.12 แนวทางการปฏิบัติงานของผู้มีส่วนได้ส่วนเสียกับการแลกเปลี่ยนข้อมูล

ผู้มีส่วนได้ส่วนเสีย	แนวปฏิบัติ
เจ้าของข้อมูล (Data Owners) ทีมบริหารจัดการข้อมูล (Data Management Team) ผู้ดูแลระบบสารสนเทศ (System Administrators) บริการข้อมูล (Data Stewards)	- กำหนดให้เจ้าของข้อมูล หรือทีมบริหารจัดการข้อมูลตามที่ได้รับมอบหมาย ตรวจสอบชั้นความลับของข้อมูลว่า อยู่ในชั้นความลับที่สามารถเปิดเผยได้หรือไม่ หมายถึงต้องไม่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ ความมั่นคงของ ประเทศ ความลับ ทางราชการ และความเป็นส่วนบุคคล พร้อมทั้ง ตรวจสอบสิทธิ์ของหน่วยงานที่สามารถนำข้อมูลไปใช้ได้ตามบทบาทและ ภารกิจตามกฎหมายของหน่วยงาน - หากสามารถให้เชื่อมโยงแลกเปลี่ยนได้ กำหนดให้เจ้าของข้อมูล หรือบริการ ข้อมูลตามที่ได้รับมอบหมาย ดำเนินการตรวจสอบคำอธิบายชุดข้อมูล ดิจิทัลหรือเมทาเดตาของข้อมูลที่จะทำการเชื่อมโยงและแลกเปลี่ยนให้ ครบถ้วน ดังนี้ - ตรวจสอบเมทาเดตาของชุดข้อมูลดิจิทัลที่จัดเก็บให้มีฟิลด์ข้อมูลครบถ้วน สอดคล้องกับความต้องการของหน่วยงานที่ขอใช้ หากไม่ครบถ้วนหรือไม่ เป็นปัจจุบันให้แจ้งเจ้าของข้อมูลและบริการข้อมูลทำการจัดทำหรือ ปรับปรุงให้เป็นปัจจุบัน ทั้งนี้ ควรจัดทำเพิ่มเติมตามความเหมาะสม ซึ่งต้องไม่กระทบกับระบบสารสนเทศ ระบบฐานข้อมูลการทำงานปกติ ของกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน - กำหนดให้เจ้าของข้อมูล หรือทีมบริหารจัดการข้อมูลจัดทำแนวทางการ ทำงานร่วมกันในการเชื่อมโยงแลกเปลี่ยนข้อมูลทั้งระหว่างหน่วยงาน ภายใน และหน่วยงานภายนอก โดยมีองค์ประกอบอย่างน้อย ดังต่อไปนี้ - วัตถุประสงค์ในการนำข้อมูลไปใช้งาน - ขอบเขตการนำข้อมูลไปใช้งาน - ช่วงเวลาและความถี่ในการเข้าถึงข้อมูลและการนำข้อมูลไปใช้ - ระดับการให้บริการ (Service Level Agreement-SLA) - ฟิลด์ข้อมูลที่สามารถเข้าถึง - รายการข้อมูลที่สามารถเข้าถึง ในกรณีขอข้อมูลส่วนบุคคลเป็นรายคน ต้องจัดทำหนังสือแสดงความยินยอม (Consent Letter) เพื่อรับการ ยินยอมจากเจ้าของข้อมูล ยกเว้นหน่วยงานที่ขอใช้ข้อมูลมีอำนาจตาม กฎหมายโดยชอบธรรม - กำหนดรายละเอียดหลักฐานของการเชื่อมโยงและการแลกเปลี่ยนข้อมูล ดิจิทัล - กำหนดวิธียืนยันตัวตนในการเชื่อมโยงและแลกเปลี่ยนข้อมูล - กำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัยเกี่ยวกับการเชื่อมโยงและ แลกเปลี่ยนข้อมูลดิจิทัลเพื่อป้องกันมิให้มีการรับส่งข้อมูลที่ไม่สมบูรณ์ หรือ ส่งข้อมูลไปผิดที่ หรือมีการรั่วไหลของข้อมูล หรือข้อมูลถูกแก้ไข เปลี่ยนแปลงถูกทำซ้ำใหม่ ถูกส่งซ้ำโดยมิได้รับอนุญาต

ผู้มีส่วนได้ส่วนเสีย	แนวปฏิบัติ
	5. ห้ามมิให้เชื่อมโยงและแลกเปลี่ยนเพื่อส่งต่อข้อมูลคอมพิวเตอร์ที่เป็นการกระทำความผิดตามกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ 6. กำหนดให้ผู้ระบบสารสนเทศต้องจัดเก็บบันทึกหลักฐานของการเชื่อมโยงและการแลกเปลี่ยนข้อมูลดิจิทัล เพื่อใช้ตรวจสอบสิ่งผิดปกติต่างๆที่เกิดขึ้นในการเชื่อมโยงและแลกเปลี่ยนข้อมูล 7. กำหนดให้มีวิธีปฏิบัติหรือระเบียบในการดำเนินการเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัลระหว่างหน่วยงานของรัฐแห่งอื่นที่ได้จัดทำหรือรวบรวมข้อมูลดิจิทัลไว้เป็นข้อมูลหลักไม่ว่าทั้งหมดหรือบางส่วน โดยกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงานไม่ต้องจัดทำข้อมูลดังกล่าวขึ้นใหม่ทั้งหมด

ตารางที่ 3.13 แสดงกิจกรรมที่ต้องดำเนินการของผู้มีส่วนได้ส่วนเสียกับการแลกเปลี่ยนข้อมูล

กิจกรรม	ผู้มีส่วนได้ส่วนเสีย			
	เจ้าของข้อมูล	บริการข้อมูล	ผู้ดูแลระบบสารสนเทศ	ทีมบริหารจัดการข้อมูล
ตรวจสอบชั้นความลับของข้อมูลว่าอยู่ในชั้นความลับที่สามารถเปิดเผยได้หรือไม่	/			/
กำหนดการเชื่อมโยงและแลกเปลี่ยนข้อมูลตามมาตรฐานเทคโนโลยีสารสนเทศและการสื่อสารของกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน	/	/		/
ตรวจสอบคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตา	/	/	/	
จัดทำแนวทางการทำงานร่วมกันทั้งระหว่างหน่วยงานภายในและหน่วยงานภายนอก ในการเชื่อมโยงและแลกเปลี่ยนข้อมูล	/	/	/	
จัดเก็บบันทึกหลักฐานของการเชื่อมโยง และการแลกเปลี่ยนข้อมูลดิจิทัล			/	/



รูปที่ 3.9 แผนภาพแนวปฏิบัติการแลกเปลี่ยนข้อมูล

5) การจัดเก็บ

การจัดเก็บข้อมูลเป็นการคัดลอกเอาข้อมูลที่มีช่วงอายุเกินระยะเวลาใช้งานหรือไม่ได้ใช้งานแล้วตามนโยบายข้อมูลมาเก็บรักษาไว้ โดยไม่มีการลบ ปรับปรุง หรือแก้ไขข้อมูลเพิ่มเติม และสามารถนำข้อมูลกลับไปใช้งานได้ใหม่เมื่อต้องการ กิจกรรมนี้เกิดขึ้นเมื่อข้อมูลถูกใช้ไปในช่วงระยะเวลาที่เหมาะสมตามกำหนด หรือไม่ได้ใช้งานแล้ว จึงนำเข้าสู่กระบวนการจัดเก็บถาวร ซึ่งข้อมูลดังกล่าวยังคงต้องได้รับการควบคุม

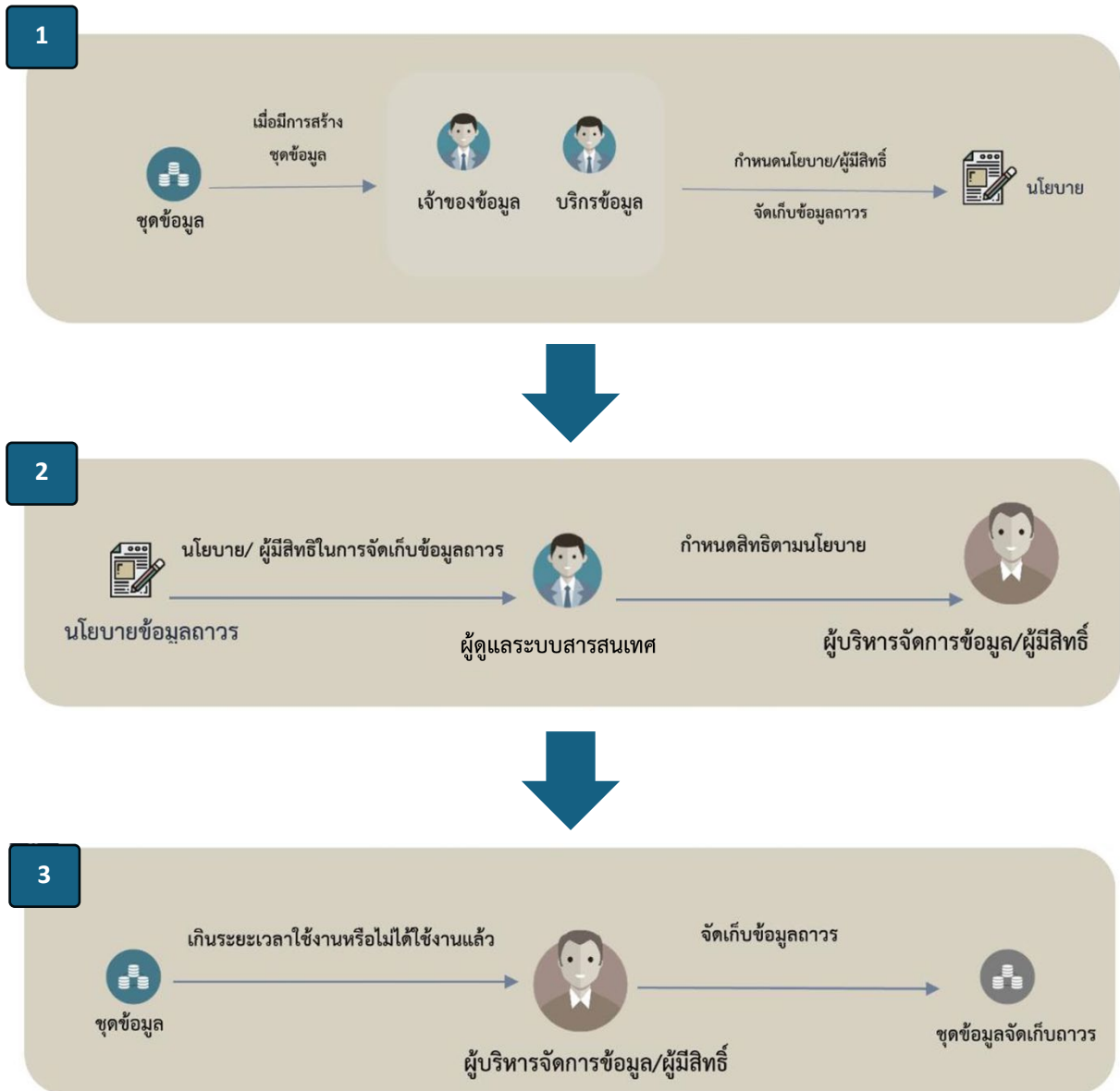
และดูแลความปลอดภัยในการเข้าถึงข้อมูลเช่นเดียวกับข้อมูลที่ถูกใช้งานปัจจุบัน เพียงแต่ข้อมูลถาวรอาจถูกโยกย้ายไปเก็บในฐานข้อมูลอื่นเพื่อจัดเก็บระยะยาวตามระยะเวลาที่กำหนด ซึ่งมีแนวทางการปฏิบัติงานของผู้มีส่วนได้ส่วนเสียกับข้อมูล และกิจกรรมที่ต้องดำเนินการดังตารางที่ 3.14 และ 3.15 ตามลำดับ โดยมีแผนภาพประกอบแนวปฏิบัติแสดงดังรูปที่ 3.10

ตารางที่ 3.14 แนวทางการปฏิบัติงานของผู้มีส่วนได้ส่วนเสียกับข้อมูลของการจัดเก็บข้อมูล

ผู้มีส่วนได้ส่วนเสีย	แนวปฏิบัติ
เจ้าของข้อมูล (Data Owners) ทีมบริหารจัดการข้อมูล (Data Management Team) ผู้ดูแลระบบสารสนเทศ (System Administrators) บริกรข้อมูล (Data Stewards)	- กำหนดระยะเวลาหรือเงื่อนไขให้กับชุดข้อมูลที่ถูกสร้างขึ้น รวมถึงกำหนดผู้มีสิทธิ์ในการจัดเก็บข้อมูลถาวร และจะต้องทบทวนสิทธิ์นั้นอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ ได้แก่ การลาออก เปลี่ยนตำแหน่ง โอนย้ายสิ้นสุดการจ้าง การปรับโครงสร้าง หรือเมื่อมีการปรับปรุงระบบสารสนเทศ เป็นต้น - ผู้ดูแลระบบสารสนเทศจะต้องกำหนดสิทธิ์ในการจัดเก็บข้อมูลถาวรให้แก่ทีมบริหารจัดการข้อมูลตามที่เจ้าของข้อมูล หรือตามนโยบายข้อมูลกำหนด - ทีมบริหารจัดการข้อมูล/ผู้มีสิทธิ์ ต้องจัดเก็บข้อมูลถาวร ตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน - ให้เจ้าของข้อมูลต้องตรวจสอบชุดข้อมูลที่ถูกจัดเก็บแบบถาวร อย่างน้อยปีละ 1 ครั้ง

ตารางที่ 3.15 แสดงกิจกรรมที่ต้องดำเนินการของผู้มีส่วนได้ส่วนเสียของการจัดเก็บข้อมูล

กิจกรรม	ผู้มีส่วนได้ส่วนเสีย			
	เจ้าของข้อมูล	ผู้ดูแลระบบสารสนเทศ	ทีมบริหารจัดการข้อมูล	บริกร ข้อมูล
กำหนดนโยบายในการจัดเก็บข้อมูลถาวร	/			/
กำหนดผู้มีสิทธิ์ในการจัดเก็บข้อมูลถาวร	/			/
กำหนดสิทธิ์ในการจัดเก็บข้อมูลถาวรให้แก่ผู้มีสิทธิ์		/		
จัดเก็บข้อมูลถาวรตามนโยบายในการจัดเก็บข้อมูลถาวรและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน			/	
ตรวจสอบชุดข้อมูลที่ถูกจัดเก็บแบบถาวร อย่างน้อยปีละ 1 ครั้ง	/			



รูปที่ 3.10 แผนภาพแนวปฏิบัติการจัดเก็บข้อมูล

7) การทำลาย

การทำลายเป็นการทำลายข้อมูลที่มีการจัดเก็บถาวรเป็นระยะเวลานานหรือเกินกว่าระยะเวลาที่กำหนด หรือเมื่อข้อมูลที่กรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงานไม่ได้ใช้งานหรือไม่ต้องดูแลรับผิดชอบแล้ว โดยมีวัตถุประสงค์เพื่อให้มั่นใจได้ว่าข้อมูลดังกล่าวจะไม่ถูกนำกลับไปใช้อีก อีกทั้งยังเป็นการกำหนดแนวปฏิบัติการทำลายข้อมูล และการพิจารณาอนุมัติทำลายโดยเจ้าของข้อมูล เพื่อรักษาความมั่นคงปลอดภัยของข้อมูล ซึ่งมีแนวทางการปฏิบัติงานของผู้มีส่วนได้ส่วนเสียกับข้อมูล และกิจกรรมที่ต้องดำเนินการดังตารางที่ 3.16 และ 3.17 ตามลำดับ โดยมีแผนภาพประกอบแนวปฏิบัติแสดงดังรูปที่ 3.11

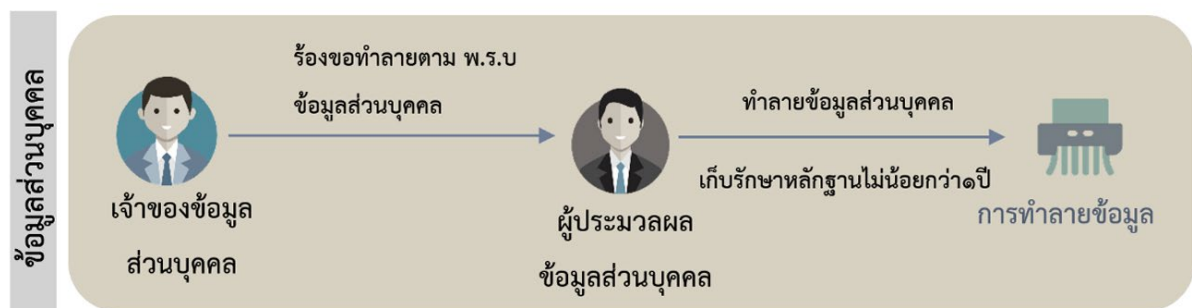
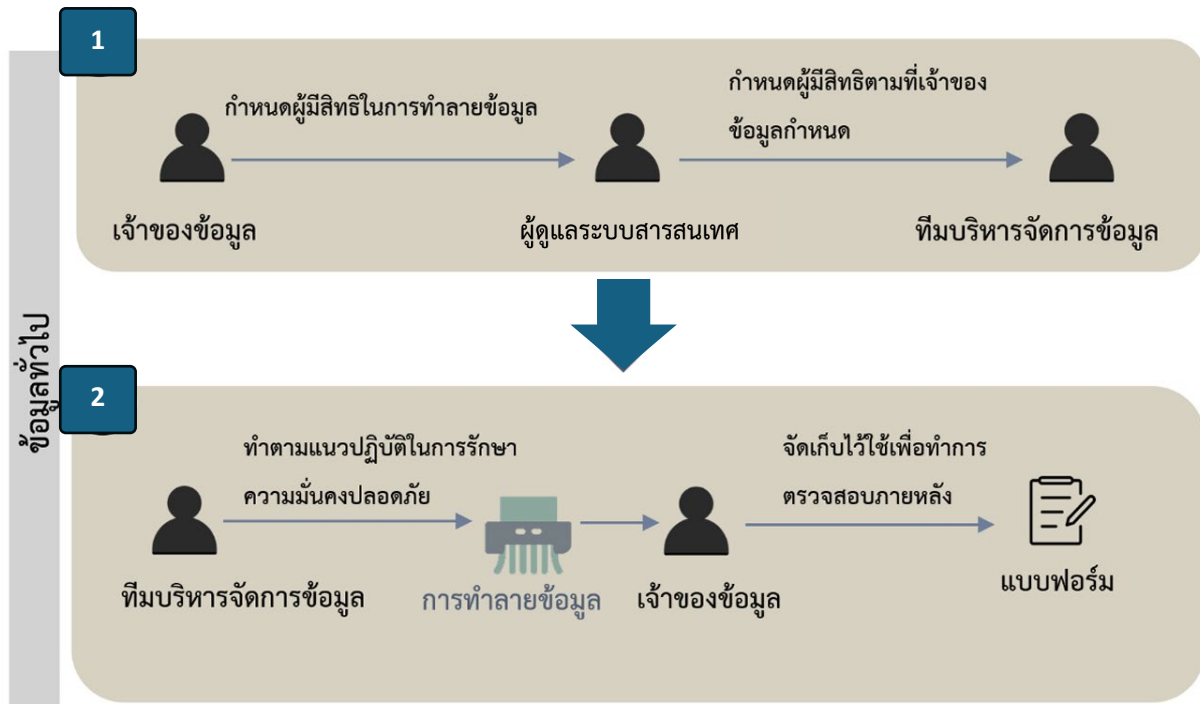
ตารางที่ 3.16 แนวทางการปฏิบัติงานของผู้มีส่วนได้ส่วนเสียกับข้อมูลของการทำลายข้อมูล

ผู้มีส่วนได้ส่วนเสีย	แนวปฏิบัติ
เจ้าของข้อมูล (Data Owners) ทีมบริหารจัดการข้อมูล (Data Management Team) ผู้ดูแลระบบสารสนเทศ (System Administrators)	1. เจ้าของข้อมูลเป็นผู้กำหนดผู้มีสิทธิในการทำลายข้อมูล และจะต้องทบทวนสิทธินั้นอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ ได้แก่ การลาออก เปลี่ยนตำแหน่ง โอนย้ายสิ้นสุดการจ้าง การปรับโครงสร้าง หรือเมื่อมีการปรับปรุงระบบสารสนเทศ เป็นต้น 2. ผู้ดูแลระบบสารสนเทศจะต้องกำหนดสิทธิในการทำลายข้อมูลให้แก่ทีมบริหารจัดการข้อมูลตามที่เจ้าของข้อมูลกำหนด 3. ทีมบริหารจัดการข้อมูลต้องทำลายข้อมูลตามแนวปฏิบัติในการรักษา ความมั่นคงปลอดภัยด้านสารสนเทศของกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน 4. กำหนดให้เจ้าของข้อมูลต้องจัดเก็บคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตาที่ทำลายสำหรับตรวจสอบในภายหลัง 5. กำหนดให้ทีมบริหารจัดการข้อมูลจัดเก็บบันทึกรายละเอียดการทำลายข้อมูลไว้ในทะเบียนควบคุมและบันทึกการทำลายข้อมูล โดยให้เก็บรักษาไว้เป็นหลักฐานไม่น้อยกว่า 1 ปี 6. กำหนดให้ผู้ประมวลผลข้อมูลส่วนบุคคลทำลายข้อมูลส่วนบุคคลเมื่อเจ้าของข้อมูลส่วนบุคคลร้องขอตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล

ตารางที่ 3.17 แสดงกิจกรรมที่ต้องดำเนินการของผู้มีส่วนได้ส่วนเสียของการทำลายข้อมูล

กิจกรรม	ผู้มีส่วนได้ส่วนเสีย		
	เจ้าของข้อมูล	ผู้ดูแลระบบสารสนเทศ	ทีมบริหารจัดการข้อมูล
กำหนดผู้มีสิทธิในการทำลายข้อมูล	/		
กำหนดสิทธิในการทำลายข้อมูลให้แก่ผู้ทำลายข้อมูล		/	
ทำลายข้อมูลตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน			/
จัดเก็บคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตาที่ทำลายสำหรับตรวจสอบในภายหลัง	/		
จัดเก็บบันทึกรายละเอียดการทำลายข้อมูลไว้ในทะเบียนควบคุมและบันทึกการทำลายข้อมูล โดยให้เก็บรักษาไว้เป็นหลักฐานไม่น้อยกว่า 1 ปี			/

กิจกรรม	ผู้มีส่วนได้ส่วนเสีย		
	เจ้าของข้อมูล	ผู้ดูแลระบบสารสนเทศ	ทีมบริหารจัดการข้อมูล
ทำลายข้อมูลส่วนบุคคลเมื่อเจ้าของข้อมูลส่วนบุคคลร้องขอตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล			/



รูปที่ 3.11 แผนภาพแนวปฏิบัติการทำลายข้อมูล

3.3.2 กระบวนการกำกับดูแลข้อมูล (Data Governance Process)

การกำหนดกระบวนการกำกับดูแลข้อมูล เป็นการกำหนดขั้นตอนที่ใช้ในการดำเนินการธรรมาภิบาลข้อมูลของ พพ. เพื่อให้เป็นไปตามกฎหมาย กฎระเบียบ ข้อบังคับ แนวนโยบายที่เกี่ยวข้องกับการธรรมาภิบาลข้อมูล โดยเริ่มตั้งแต่ระดับการวางแผนไปจนถึงระดับการปรับปรุงอย่างต่อเนื่อง เพื่อให้ข้อมูลของ พพ. มีคุณภาพ มีความปลอดภัย สร้างมูลค่า และสามารถเพิ่มศักยภาพในการดำเนินงานทั้งในส่วนของการเปิดเผยข้อมูล การเชื่อมโยงข้อมูล และแลกเปลี่ยนและการสร้างประโยชน์จากข้อมูลสำหรับการดำเนินงานตามภารกิจของ พพ. ซึ่งกระบวนการธรรมาภิบาลข้อมูลของ พพ. ประกอบด้วยกระบวนการที่สำคัญ 7 กระบวนการ ดังนี้

3.3.2.1 กำหนดเป้าหมาย (Develop a Value Statement) เป็นการกำหนดผลลัพธ์ที่คาดหวังว่าจะได้รับจากการดำเนินงานธรรมาภิบาลข้อมูล โดยเป้าหมายธรรมาภิบาลข้อมูลของ พพ. ได้แก่ ข้อมูลของ พพ. มีความถูกต้อง ครบถ้วน เป็นปัจจุบัน มีความมั่นคงปลอดภัย ไม่ละเมิดระเบียบข้อบังคับต่าง ๆ รวมทั้งสามารถเชื่อมโยงและบูรณาการข้อมูลจากทั้งภายในองค์กรและภายนอกองค์กร ได้อย่างมีประสิทธิภาพสามารถนำไปสู่การพัฒนาองค์กรให้เกิดประโยชน์ได้อย่างสูงสุด

3.3.2.2 กำหนดทิศทางการดำเนินการ (Prepare a Roadmap) เป็นการกำหนดวิธีการดำเนินการธรรมาภิบาลข้อมูลและบริหารจัดการข้อมูล โดยพิจารณาถึงความพร้อมขององค์กรเพื่อให้สามารถขับเคลื่อนไปสู่การบรรลุเป้าหมายที่กำหนดไว้

3.3.2.3 วางแผนงานและงบประมาณ (Plan and Fund) เป็นการกำหนดรายละเอียดของขอบเขตการดำเนินงานและงบประมาณที่จะต้องใช้ในการดำเนินการ

3.3.2.4 ออกแบบแผนดำเนินการ (Design the Program) เป็นการกำหนดรายละเอียดของแผนการดำเนินงาน ประกอบด้วย

- 1) กลยุทธ์
- 2) โครงการ/กิจกรรม
- 3) วัตถุประสงค์การดำเนินงาน
- 4) หน่วยงานผู้รับผิดชอบ
- 5) วิธีการประเมินผลการดำเนินงาน
- 6) ผลผลิตและผลลัพธ์ที่ได้จากการดำเนินงาน
- 7) ระยะเวลาการดำเนินงาน

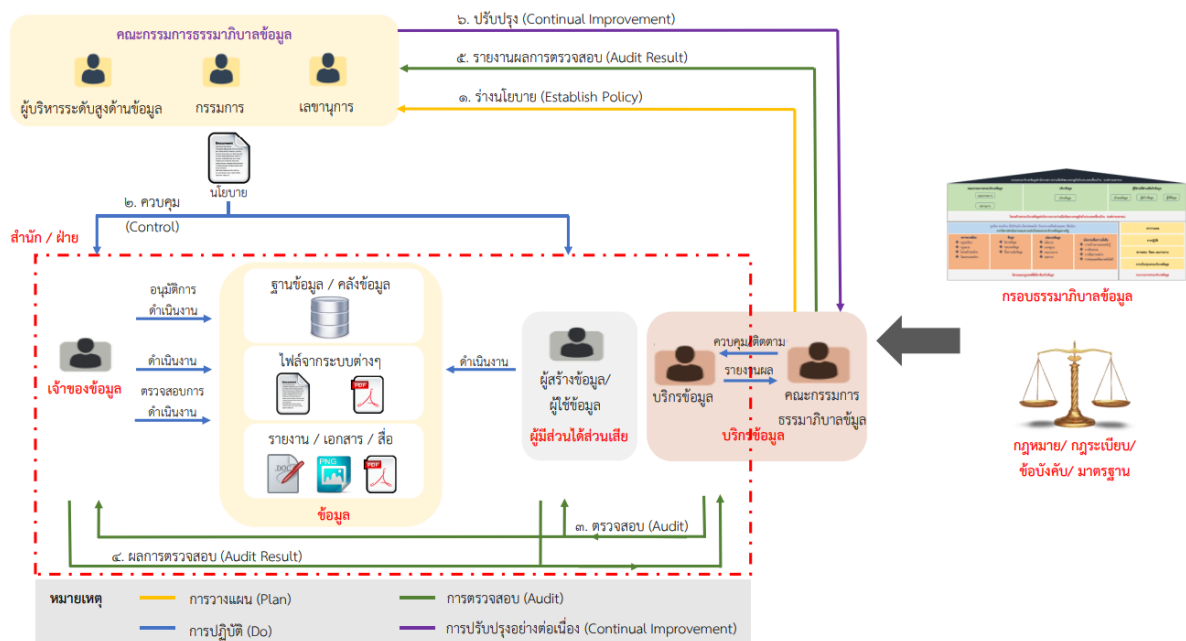
3.3.2.5 ประกาศใช้อย่างเป็นทางการ (Deploy the Program) เป็นการสื่อสารให้บุคลากรภายในองค์กร ได้รับรู้ ตระหนัก และเข้าใจถึงเป้าหมาย นโยบาย แนวทางการดำเนินงานธรรมาภิบาลข้อมูลของ พพ. อันจะนำไปสู่การปฏิบัติตนอย่างเหมาะสมกับบทบาทหน้าที่ของแต่ละบุคคล โดยวิธีการประกาศนั้นจะผ่านช่องทางการสื่อสารที่หลากหลาย เพื่อให้สามารถเข้าถึงบุคลากรได้ทุกกลุ่ม ได้แก่ การติดประกาศตามจุดต่างๆ ขององค์กร เว็บไซต์ ระบบ Web Portal หนังสือเวียนองค์กร และการสื่อสารในที่ประชุม

3.3.2.6 ดำเนินการธรรมาภิบาลข้อมูล (Govern the Data) เป็นการปฏิบัติตามแผนการดำเนินงานที่ได้ออกแบบไว้ของบุคคลที่เกี่ยวข้องกับกระบวนการธรรมาภิบาลข้อมูล ตามที่ระบุไว้ในโครงสร้างธรรมาภิบาลข้อมูล โดยในระหว่างการทำงาน จะกำหนดให้มีการประชุมคณะกรรมการฯ เป็นระยะเพื่อติดตามผลการดำเนินงาน หากพบประเด็นปัญหาที่เกิดขึ้นจะสามารถแก้ไขได้อย่างทันท่วงที

3.3.2.7 ติดตามการดำเนินงาน/วัดผลการดำเนินงาน/รายงานผลการดำเนินงาน (Monitor, Measure, Report) เป็นการติดตามการดำเนินงาน และตรวจสอบโดยบริการข้อมูลจะดำเนินการตรวจสอบ

ความ สอดคล้องกันระหว่างกฎระเบียบ นโยบาย และมาตรฐานที่กำหนดกับการปฏิบัติงานของบุคคลที่เกี่ยวข้องกับการบริหารจัดการข้อมูลและผู้ที่เกี่ยวข้องอื่น ๆ พร้อมทั้งทำการวัดผลด้านคุณภาพข้อมูล หลังจาก นั้นรายงานผลความสอดคล้อง คุณภาพข้อมูล ความมั่นคงปลอดภัย และความเสี่ยงที่เกี่ยวข้องกับข้อมูลไปยัง คณะกรรมการธรรมาภิบาลข้อมูลและผู้ที่เกี่ยวข้อง เพื่อให้ทราบถึงผลการดำเนินงานและประเด็นปัญหาที่พบ ทั้งนี้การกำหนดตัวชี้วัดวัดผลการดำเนินงานจะขึ้นอยู่กับการออกแบบแผนการดำเนินในแต่ละกิจกรรม โดย สามารถยกตัวอย่างตัวชี้วัดที่ช่วยสะท้อนผลการดำเนินงานธรรมาภิบาลข้อมูลได้ ดังนี้

- 1) จำนวนผู้ที่ทำผิดกฎ ระเบียบ หรือข้อบังคับต่างๆ ที่เกี่ยวข้อง กับข้อมูล ที่ พพ. กำหนด
- 2) จำนวนหน่วยงานภายนอกที่มีการบูรณาการข้อมูลร่วมกันกับ พพ.
- 3) จำนวนข้อมูลที่ได้รับการตรวจสอบความถูกต้องสมบูรณ์
 - ฯ) พพ. สามารถยกระดับประสิทธิภาพการดำเนินงานมากขึ้น จากการนำข้อมูลมาช่วยสนับสนุนการดำเนินงาน



รูปที่ 3.12 ขั้นตอนการดำเนินงานธรรมาภิบาลข้อมูลของ พพ.

กระบวนการกำกับดูแลข้อมูลจะต้องดำเนินการอย่างต่อเนื่อง ตามระบบบริหารและกระบวนการจัดการข้อมูลหรือวงจรชีวิตของข้อมูล เนื่องจากบริบทของการบริหารจัดการ กฎหมาย กฎระเบียบ รวมถึงความต้องการของผู้มีส่วนได้ส่วนเสียมีการเปลี่ยนแปลงตลอดเวลา ตลอดจนรายงานผลจากการติดตามและตรวจสอบการดำเนินการธรรมาภิบาลข้อมูลที่เกิดขึ้น ทำให้ต้องมีการทบทวนและปรับปรุงอย่างต่อเนื่อง (Continual Improvement) ดังรูปที่ 3.12

3.3.3 การจัดการกระบวนการธรรมาภิบาลข้อมูล

เพื่อให้เกิดความเข้าใจในแนวทางการจัดการกระบวนการธรรมาภิบาลข้อมูลของ พพ. และเห็นความสัมพันธ์ระหว่างกระบวนการธรรมาภิบาลข้อมูล เครื่องมือ หรือเอกสารที่ใช้ในการธรรมาภิบาลข้อมูล ผลลัพธ์ที่ได้และผู้ที่เกี่ยวข้องหรือผู้มีส่วนได้ส่วนเสีย ดังแสดงในตารางที่ 3.18 และความสัมพันธ์ระหว่างกระบวนการ/กิจกรรมและผู้มีส่วนได้ส่วนเสียกับข้อมูล ดังแสดงในตารางที่ 3.19

ตารางที่ 3.18 ความสัมพันธ์ระหว่างระดับของกระบวนการ ส่วนนำเข้า ส่วนนำออก และผู้มีส่วนได้ส่วนเสียกับกระบวนการ

ระดับของ กระบวนการ	กระบวนการ	ส่วนนำเข้า	ส่วนนำออก	ผู้มีส่วนได้ส่วนเสีย
การวางแผน	1) กำหนดเป้าหมาย 2) กำหนดทิศทางการดำเนินการ 3) วางแผนงานและงบประมาณ 4) ออกแบบแผนดำเนินการ 5) ประกาศใช้อย่างเป็นทางการ	1) นโยบาย กฎ ระเบียบ ข้อบังคับและกฎหมายที่เกี่ยวข้องกับข้อมูล 2) รายการชุดข้อมูล 3) รายการประเด็นปัญหาจากรายงานผลการตรวจสอบความสอดคล้องของการดำเนินงานต่อนโยบายข้อมูล รายงานคุณภาพข้อมูล รายงานความมั่นคงปลอดภัยต่อข้อมูล รายงานความเสี่ยงต่อข้อมูล	แผนดำเนินการ (กิจกรรม บุคลากร งบประมาณ และระยะเวลาในการดำเนินการ)	1) คณะกรรมการธรรมาภิบาลข้อมูล 2) บริกรข้อมูลด้านธุรกิจ 3) บริกรข้อมูลด้านเทคนิค 4) บริกรข้อมูลด้านคุณภาพ
การปฏิบัติ	ดำเนินการธรรมาภิบาลข้อมูล	1) นโยบาย กฎ ระเบียบ ข้อบังคับและกฎหมายที่เกี่ยวข้องกับข้อมูล 2) แผนดำเนินการ (กิจกรรม บุคลากร งบประมาณและระยะเวลาในการดำเนินการ)	1) รายงานความก้าวหน้าในการปฏิบัติงาน 2) ผลการปฏิบัติงาน 3) ประเด็นปัญหาที่พบระหว่างปฏิบัติงาน	1) ผู้บริหารงาน 2) บริกรข้อมูลด้านธุรกิจ 3) บริกรข้อมูลด้านเทคนิค 4) บริกรข้อมูลด้านคุณภาพ 5) ผู้ปฏิบัติงานที่เกี่ยวข้อง
การตรวจสอบ	ติดตามการดำเนินงาน/วัดผลการดำเนินงาน/ รายงานผลการดำเนินงาน	1) นโยบาย กฎ ระเบียบ ข้อบังคับและกฎหมายที่เกี่ยวข้องกับข้อมูล 2) เกณฑ์การประเมินความพร้อมของธรรมาภิบาลข้อมูล ระดับคุณภาพข้อมูล	1) รายงานผลการตรวจสอบความสอดคล้องของการดำเนินงานต่อนโยบายข้อมูล 2) รายงานคุณภาพข้อมูล 3) รายงานความมั่นคงปลอดภัยต่อข้อมูล 4) รายงานความเสี่ยงต่อข้อมูล	1) บริกรข้อมูลด้านธุรกิจ 2) บริกรข้อมูลด้านเทคนิค 3) บริกรข้อมูลด้านคุณภาพ
ปรับปรุง ธรรมาภิบาล	การปรับปรุงอย่างต่อเนื่อง	1) นโยบาย กฎ ระเบียบ ข้อบังคับและกฎหมายที่เกี่ยวข้องกับข้อมูล 2) โครงสร้างธรรมาภิบาลข้อมูล 3) เกณฑ์การประเมินความพร้อมของธรรมาภิบาลข้อมูล และระดับคุณภาพข้อมูล 4) รายงานผลการตรวจสอบความสอดคล้องของการดำเนินงานต่อนโยบาย ข้อมูล รายงานความมั่นคงปลอดภัย ต่อข้อมูล และรายงานความเสี่ยงต่อข้อมูล 5) รายการความต้องการจากผู้บริหารและผู้มีส่วนได้ส่วนเสีย	1) กระบวนการ ธรรมาภิบาลข้อมูล 2) นโยบาย กฎ ระเบียบ ข้อบังคับ และกฎหมาย ที่เกี่ยวข้องกับข้อมูล 3) เกณฑ์การประเมินความพร้อมของธรรมาภิบาลข้อมูล และระดับคุณภาพข้อมูล 4) โครงสร้างธรรมาภิบาลข้อมูล	1) คณะกรรมการธรรมาภิบาลข้อมูล 2) บริกรข้อมูลด้านธุรกิจ 3) บริกรข้อมูลด้านเทคนิค 4) บริกรข้อมูลด้านคุณภาพ

จากตารางข้างต้นจะเห็นได้ว่า แนวทางการจัดการกระบวนการธรรมาภิบาลข้อมูลของ พพ. จะประกอบด้วยกระบวนการต่าง ๆ ซึ่งภายใต้ในแต่ละกระบวนการจะมีผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับกระบวนการ โดยมีบทบาทหน้าที่และความรับผิดชอบที่แตกต่างกันไปประกอบด้วย ผู้ที่มีหน้าที่ในการดูแลรับผิดชอบในแต่ละกิจกรรม (R) ผู้ที่มีหน้าที่ในการกำหนดแนวทางหรือเป้าหมายของกิจกรรม (A) ผู้ที่มีหน้าที่ในการให้คำปรึกษา (C) และผู้ที่ต้องรับรู้ข้อมูลกระบวนการ/กิจกรรมต่าง ๆ ที่กำลังดำเนินงาน โดยสามารถสรุปได้ ดังนี้

ตารางที่ 3.19 ความสัมพันธ์ระหว่างกระบวนการ/กิจกรรม และผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับกระบวนการ

กระบวนการ/กิจกรรม	ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับกระบวนการ				
	คณะกรรมการ ธรรมาภิบาล ข้อมูล	ทีมบริการ ข้อมูล	เจ้าของ ข้อมูล	ทีมบริหาร จัดการ ข้อมูล	ผู้สร้าง และใช้งาน ข้อมูล
กำหนดและปรับปรุงนโยบาย และ มาตรฐานข้อมูล	A	R	R	R	R
ตรวจสอบการปฏิบัติตามนโยบาย ข้อมูล	A	R	R	R	R
การประเมินความพร้อมของ ธรรมาภิบาลข้อมูล	C,I	A	R	R	R
ประเมินความมั่นคงปลอดภัย และ คุณภาพข้อมูล	C,I	C,I	I	A	I
รายงานผลการตรวจสอบความ มั่นคงปลอดภัย และคุณภาพข้อมูล	C	A	I	R	I
กำหนดสิทธิในการเข้าถึงข้อมูล	A	R	I	R	I

หมายเหตุ

Responsible หมายถึง ผู้ที่มีหน้าที่ในการดูแลรับผิดชอบให้แต่ละกิจกรรมประสบความสำเร็จ

Accountable หมายถึง ผู้ที่มีหน้าที่ในการกำหนดแนวทางหรือเป้าหมายของกิจกรรม รวมทั้งกำหนดหน้าที่ความรับผิดชอบในกระบวนการปฏิบัติงาน

Consulted หมายถึง ผู้ที่มีหน้าที่ในการให้คำปรึกษา ให้ความรู้ หรือคำแนะนำต่าง ๆ

Informed หมายถึง บุคคลที่เกี่ยวข้องกับกระบวนการ และจะต้องรับรู้ถึงข้อมูลในกระบวนการนั้น ๆ

บทที่ 4

การวัดการดำเนินการและความสำเร็จของธรรมาภิบาลข้อมูลภาครัฐ (Data Governance Metrics and Success Measures)

การวัดการดำเนินการธรรมาภิบาลข้อมูลภาครัฐเป็นการประเมินความพร้อมของธรรมาภิบาลข้อมูลแสดงถึงสถานะปัจจุบันของหน่วยงานในด้านความพร้อมและความก้าวหน้าในการดำเนินการธรรมาภิบาลข้อมูลภาครัฐ ผลของการดำเนินการนี้จะสะท้อนถึงความสำเร็จของธรรมาภิบาลข้อมูลภาครัฐ ซึ่งประกอบด้วยคุณภาพของข้อมูล ความมั่นคงปลอดภัยของข้อมูล และการวัดความคุ้มค่าและการปรับปรุงอย่างต่อเนื่อง ระดับความพร้อมที่สูงควรสะท้อนถึงความสำเร็จที่สูง อย่างไรก็ตามระดับความพร้อมกับความสำเร็จอาจไม่สอดคล้องกัน ซึ่งอาจเกิดจากสาเหตุอื่นหรือเกณฑ์การประเมินความพร้อมยังไม่มีประสิทธิภาพเพียงพอ ดังนั้น หน่วยงานควรค้นหาสาเหตุที่แน่ชัดและดำเนินการแก้ไขเกณฑ์การประเมินความพร้อมเพื่อให้สอดคล้องกับลักษณะเฉพาะของหน่วยงาน แนวทางการประเมินความพร้อมของธรรมาภิบาลข้อมูลภาครัฐ การประเมินคุณภาพของข้อมูล และการประเมินความมั่นคงปลอดภัยของข้อมูล มีรายละเอียดดังนี้

4.1 การประเมินความพร้อมของธรรมาภิบาลข้อมูลภาครัฐ (Data Governance Readiness Assessment)

การประเมินความพร้อมของธรรมาภิบาลข้อมูลภาครัฐจะช่วยให้ทราบถึงสิ่งที่ได้ดำเนินการแล้ว และสิ่งที่ควรดำเนินการต่อไปเพื่อปรับปรุงการดำเนินงานให้เกิดประสิทธิภาพสูงสุด ระดับความพร้อมของธรรมาภิบาลข้อมูลภาครัฐถูกใช้เป็นเครื่องมือในการประเมินความพร้อม ซึ่งประกอบด้วย 5 ระดับดังนี้

ระดับ 0 : None หมายถึง ไม่มีธรรมาภิบาลข้อมูลภาครัฐหรือมีแต่ไม่ได้ดำเนินการอย่างเป็นทางการ โดยมี การดำเนินงานบางส่วนแต่ไม่มีการประกาศให้ทราบอย่างเป็นทางการ

ระดับ 1 : Initial หมายถึง ไม่มีการกำหนดมาตรฐานของกระบวนการ กระบวนการถูกกำหนดขึ้นมาเฉพาะกิจทำให้แต่ละโครงการหรือบริการมีรูปแบบกระบวนการที่แตกต่างกัน และอำนาจในการจัดการ และธรรมาภิบาลข้อมูลส่วนใหญ่ถูกดำเนินการโดยฝ่ายเทคโนโลยีสารสนเทศ ทำให้การทำงานร่วมกันระหว่าง ฝ่ายธุรกิจและฝ่ายเทคโนโลยีสารสนเทศไม่สอดคล้องกัน

ระดับ 2 : Managed หมายถึง เริ่มมีการกำหนดมาตรฐานของกระบวนการเฉพาะแต่ละส่วนงานหรือ บริการและมีการกำหนดบุคคลที่เกี่ยวข้องกับการกำกับติดตาม เช่น บริกรข้อมูลและเจ้าของข้อมูล

ระดับ 3 : Standardized หมายถึง กระบวนการถูกกำหนดเป็นมาตรฐานของหน่วยงานมีการกำหนด ส่วนงานกลางในการกำกับและติดตามข้อมูล ซึ่งมาจากบุคคลด้านธุรกิจและเทคโนโลยีสารสนเทศ มีการบังคับ ใช้นโยบายข้อมูลครอบคลุมทั้งหน่วยงาน และมีการติดตาม วิเคราะห์ และรายงานคุณภาพข้อมูลหรือความ มั่นคงปลอดภัย

ระดับ 4 : Advanced หมายถึง กระบวนการถูกกำหนดเป็นมาตรฐานของหน่วยงาน มีการกำหนดส่วน งานกลางในการกำกับและติดตามข้อมูล ซึ่งมาจากบุคคลด้านธุรกิจและเทคโนโลยีสารสนเทศมีการบังคับใช้ นโยบายข้อมูลครอบคลุมทั้งหน่วยงาน และมีการติดตาม วิเคราะห์และรายงานคุณภาพข้อมูลและความ มั่นคงปลอดภัย

ระดับ 5 : Optimized หมายถึง มีการดำเนินการสอดคล้องกับระดับ 4 โดยมีการวิเคราะห์สาเหตุของ ปัญหา (Root Cause) ซึ่งรวมถึงความไม่สอดคล้องในการปฏิบัติงานกับนโยบายข้อมูลคุณภาพข้อมูลที่ต่ำ และ

ความไม่คุ้มค่าในการบริหารจัดการข้อมูล พร้อมทั้งดำเนินการปรับปรุงกระบวนการ กฎเกณฑ์และนโยบายข้อมูล หรือโครงสร้างธรรมาภิบาลข้อมูลภาครัฐ เพื่อแก้ไขปัญหาที่พบจากผลการวิเคราะห์ และให้สอดคล้องกับความต้องการของผู้ที่เกี่ยวข้องและวัตถุประสงค์ที่เปลี่ยนไปของหน่วยงาน

4.2 การประเมินคุณภาพข้อมูล (Data Quality Assessment)

การประเมินคุณภาพของข้อมูลเป็นการตรวจสอบผลลัพธ์หรือความสำเร็จจากธรรมาภิบาลข้อมูลภาครัฐ โดยองค์ประกอบในการประเมินคุณภาพ ประกอบด้วย



รูปที่ 4.1 องค์ประกอบในการประเมินคุณภาพของข้อมูล

4.2.1 ความถูกต้อง (Accuracy)

ความถูกต้องของข้อมูลเป็นหนึ่งในคุณสมบัติที่สำคัญในการประเมินคุณภาพของข้อมูล เพราะถึงแม้ว่าหน่วยงานจะดำเนินการเก็บรวบรวมข้อมูลไว้มากเพียงใด แต่หากข้อมูลที่ถูกจัดเก็บต่าง ๆ เหล่านั้นไม่มีความถูกต้องย่อมส่งผลกระทบต่อการใช้งานที่ผิดพลาด โดยเฉพาะอย่างยิ่งการตัดสินใจเชิงนโยบายที่ต้องอาศัยข้อมูลสำคัญประกอบการพิจารณาตัดสินใจเพื่อการขับเคลื่อนองค์กร ดังนั้น ในกระบวนการบริหารจัดการข้อมูล ขั้นตอนการทำความสะอาดข้อมูล (Data Cleansing) จึงเป็นขั้นตอนที่ใช้เวลามากที่สุด เพื่อให้ข้อมูลที่ได้มีความถูกต้องสมบูรณ์สูงสุด

4.2.2 ความครบถ้วน (Completeness)

การพิจารณาตัดสินใจเพื่อดำเนินการใด ๆ ขององค์กร จำเป็นต้องอาศัยข้อมูลที่หลากหลาย เพื่อให้ได้มาซึ่งการตัดสินใจที่ดีที่สุดหรือเกิดประโยชน์ต่อองค์กรอย่างสูงสุด หรือการตัดสินใจแม้มีความสัมพันธ์เกี่ยวข้องกับหลาย ๆ ภาคส่วน ตัวอย่าง การบริการข้อมูลด้านพลังงานทดแทนและอนุรักษ์พลังงานของ พพ. ผู้บริหารมีความจำเป็นต้องทราบปัจจัยต่าง ๆ ที่ส่งผล เช่น ความต้องการของผู้ใช้บริการข้อมูล และการพัฒนาข้อมูลเดิมที่มีอยู่ เป็นต้น จากตัวอย่างดังกล่าว หากผู้บริหารไม่ทราบความต้องการของผู้ใช้บริการข้อมูล ก็อาจส่งผลให้การพัฒนาข้อมูลใหม่เพื่อนำไปใช้นั้น ไม่สอดคล้องกับความต้องการของผู้ใช้บริการ อาจทำให้ข้อมูลใหม่ไม่เป็นที่ต้องการของผู้ใช้บริการ เป็นต้น

4.2.3 ความคงเส้นคงวา (Consistency)

ความคงเส้นคงวา หรือความสอดคล้องกัน หมายถึง การได้รับข้อมูลชุดเดียวกันจากแหล่งข้อมูลต่าง ๆ ที่แตกต่างกัน จะต้องมีความเหมือนกันเพื่อมิให้เกิดความสับสนในการนำไปใช้งาน จนอาจนำไปสู่การนำข้อมูลไปใช้งานที่ผิดพลาดได้ เช่น ข้อมูลการผลิตไฟฟ้าจากพลังงานน้ำที่มาจากกองพัฒนาพลังงานทดแทน และศูนย์เทคโนโลยีสารสนเทศและการสื่อสารต้องมีข้อมูลที่ตรงกัน เป็นต้น

4.2.4 ความเป็นปัจจุบัน (Timeliness)

การวิเคราะห์พิจารณาตัดสินใจเพื่อดำเนินการ จำเป็นต้องใช้ข้อมูลที่ทันสมัย เพื่อให้ทราบถึงสถานะปัจจุบันที่กำลังเกิดขึ้น อย่างไรก็ตามข้อมูลที่ไม่มีปัจจุบันก็ยังมีประโยชน์ในการช่วยให้ผู้บริหารทราบถึงแนวโน้ม (Trend) ที่อาจจะเกิดขึ้นในอนาคตได้

4.2.5 ความสอดคล้องตรงกับความต้องการของผู้ใช้งาน (Relevancy)

วัตถุประสงค์หลักของการเก็บรวบรวมข้อมูล เพื่อให้ผู้บริหารและปฏิบัติงานสามารถนำข้อมูลไปใช้ประโยชน์ในกิจกรรมต่าง ๆ ขององค์กร ดังนั้นการเก็บรวบรวมข้อมูลจึงมีความจำเป็นต้องรับรู้และเข้าใจความต้องการของผู้ใช้งาน เพื่อให้ข้อมูลที่มีอยู่สามารถนำไปใช้พัฒนาองค์กรได้อย่างแท้จริง อย่างไรก็ตามในหลาย ๆ องค์กรมีการเก็บข้อมูลต่าง ๆ อยู่เป็นจำนวนมาก แต่ไม่สามารถนำไปใช้ประโยชน์ได้ สาเหตุส่วนหนึ่งเป็นเพราะขาดเป้าหมายในการเก็บรวบรวมข้อมูลที่ชัดเจน และไม่ทราบความต้องการของผู้ใช้งานที่แท้จริง ทำให้สิ้นเปลืองทรัพยากรขององค์กรอย่างไม่เกิดประโยชน์ ดังนั้นก่อนการเก็บรวบรวมข้อมูล นอกจากจะมีการวางแผนที่ดีแล้ว จำเป็นต้องมีการศึกษาความต้องการในการนำข้อมูลไปใช้งานของส่วนงานต่าง ๆ อย่างเป็นระบบ เพื่อที่จะนำความต้องการที่ได้รับเข้าสู่กระบวนการเก็บรวบรวมข้อมูลต่อไป

4.2.6 ความพร้อมใช้ (Availability)

ข้อมูลที่ดีควรมีความพร้อมสำหรับการนำไปใช้งานอยู่เสมอ คือ สามารถดึงข้อมูลไปใช้งานได้ทุกที่ทุกเวลาผ่านอุปกรณ์ต่าง ๆ ที่หลากหลายเพื่ออำนวยความสะดวกให้กับผู้ใช้งาน

4.3 การประเมินความมั่นคงปลอดภัยของข้อมูล

พพ. ได้กำหนดการประเมินความมั่นคงปลอดภัยของข้อมูลโดยมีแนวทางดังต่อไปนี้

4.3.1 กำหนดกรอบในการประเมินความมั่นคงปลอดภัยของข้อมูล โดยในการประเมินความมั่นคงปลอดภัยของข้อมูล จะต้องอยู่ในกรอบของกฎหมาย และข้อกำหนดของหน่วยงานกำกับดูแล ดังต่อไปนี้

1) กฎหมาย อาทิ

- (1) พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2562
- (2) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560
- (3) พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540
- (4) พระราชบัญญัติระบบการชำระเงิน พ.ศ. 2560
- (5) พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
- (6) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

2) ข้อกำหนดหลักเกณฑ์การบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Management) ขององค์กรไว้ดังนี้

- (1) การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT Asset Management)
- (2) การรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศ (Data and Information Security)

- (3) การควบคุมการเข้าถึง (Access Control)
- (4) การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environmental Security)
- (5) การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร (Communications Security)
- (6) การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT Operations Security)
- (7) การจัดหาและการพัฒนาระบบเทคโนโลยีสารสนเทศ (System Acquisition and Development)
- (8) การบริหารจัดการเหตุการณ์ผิดปกติและปัญหาด้านเทคโนโลยีสารสนเทศ (IT Incident and Problem Management)
- (9) การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan)
- (10) การบริหารจัดการผู้ให้บริการภายนอก (Third Party Management)

4.3.2 จัดทำนโยบายด้านความมั่นคงปลอดภัยของข้อมูลตามมาตรฐาน ISO 27001 ได้แก่ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Policy) โดยแบ่งออกเป็น 2 ส่วน ได้แก่ สำหรับผู้ใช้งานและสำหรับผู้ดูแลระบบ ดังนี้

- 2.1 หมวดที่ 1 นโยบายด้านความมั่นคงปลอดภัยสารสนเทศสำหรับผู้ใช้งาน มีดังต่อไปนี้
 - (1) นโยบายการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Security)
 - (2) นโยบายการรักษาความมั่นคงปลอดภัยของการควบคุมการเข้าถึงระบบ (Access Control Policy)
 - (3) นโยบายการรักษาความมั่นคงปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Network and Server Policy)
 - (4) นโยบายการรักษาความมั่นคงปลอดภัยของเครือข่ายไร้สาย (Wireless Policy) (5) นโยบายการรักษาความมั่นคงปลอดภัยของไฟร์วอลล์ (Firewall Policy)
 - (6) นโยบายการรักษาความมั่นคงปลอดภัยของจดหมายอิเล็กทรอนิกส์ (E-mail Policy)
 - (7) นโยบายการรักษาความมั่นคงปลอดภัยของอินเทอร์เน็ต (Internet Security Policy)
 - (8) นโยบายบริหารจัดการทรัพย์สินสารสนเทศ (Asset Management Policy)
- 2.2 หมวดที่ 2 นโยบายด้านความมั่นคงปลอดภัยสารสนเทศสำหรับผู้ดูแลระบบ มีดังต่อไปนี้
 - (1) นโยบายการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Security)
 - (2) นโยบายการรักษาความมั่นคงปลอดภัยของการควบคุมการเข้าถึงระบบ (Access Control Policy)
 - (3) นโยบายการรักษาความมั่นคงปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Network and Server Policy)
 - (4) นโยบายการรักษาความมั่นคงปลอดภัยของเครือข่ายไร้สาย (Wireless Policy)
 - (5) นโยบายการรักษาความมั่นคงปลอดภัยของไฟร์วอลล์ (Firewall Policy)
 - (6) นโยบายความมั่นคงปลอดภัยของการตรวจจับการบุกรุก (Intrusion Detection System / Intrusion Prevention System Policy IDS/IPS Policy)

(7) นโยบายการบริหารจัดการความต่อเนื่องของระบบสารสนเทศ (Information Security Aspects of Business Continuity Management Policy)

(8) นโยบายความมั่นคงปลอดภัยด้านบุคลากร (Human Security Policy)

(9) นโยบายการบริหารจัดการโครงการด้านเทคโนโลยีสารสนเทศ (Project Management Policy)

(10) นโยบายบริหารจัดการทรัพย์สินสารสนเทศ (Asset Management Policy)

(11) นโยบายการถ่ายโอนสารสนเทศ (Information Transfer Policy)

(12) นโยบายการพัฒนาระบบอย่างมั่นคงปลอดภัย (Secure development Policy)

(13) นโยบายความมั่นคงปลอดภัยด้านบริการที่ได้รับจากผู้ให้บริการ (Supplier Relationships Policy)

(14) นโยบายการปฏิบัติตามกฎหมาย มาตรฐาน และ ข้อบังคับ (Compliance Policy)

(15) เอกสารสนับสนุน (Supporting Document)

4.3.3 มีการจัดชั้นความลับของข้อมูล (Data Classification) ที่สอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ ที่เกี่ยวข้อง เพื่อป้องกันผลกระทบที่อาจจะเกิดขึ้นจากการนำข้อมูลไปใช้อย่างไม่ถูกต้อง รวมทั้งการดัดแปลง แก้ไข หรือแต่งเติมข้อมูลต่าง ๆ โดยไม่ได้รับอนุญาต โดย พพ. ได้มีการกำหนดชั้นความลับของข้อมูลไว้ดังนี้

1) ข้อมูลส่วนบุคคล แบ่งระดับชั้นความลับได้เป็น 3 ประเภท ได้แก่

ลำดับ	ระดับชั้นข้อมูล	เงื่อนไขการเข้าถึงข้อมูล
1	ลับ (Confidential)	ผ่านการอนุมัติจากผู้บริหารระดับผู้อำนวยการกอง/สำนัก/ศูนย์ ขึ้นไป
2	ลับมาก (Secret)	ผ่านการอนุมัติจากผู้บริหารระดับรองอธิบดี ขึ้นไป
3	ลับที่สุด (Top secret)	ผ่านการอนุมัติจากผู้บริหารระดับอธิบดี ขึ้นไป

2) ข้อมูลทั่วไป แบ่งระดับชั้นความลับได้เป็น 5 ประเภท ได้แก่

ลำดับ	ระดับชั้นข้อมูล	เงื่อนไขการเข้าถึงข้อมูล
1	เปิดเผย (Open)	ไม่มีการจำกัดการเข้าถึงข้อมูล
2	เผยแพร่ภายในองค์กร (Private)	เฉพาะบุคคลภายในองค์กร
3	ลับ (Confidential)	ผ่านการอนุมัติจากผู้บริหารระดับผู้อำนวยการกอง/สำนัก/ศูนย์ ขึ้นไป
4	ลับมาก (Secret)	ผ่านการอนุมัติจากผู้บริหารระดับรองอธิบดี ขึ้นไป
5	ลับที่สุด (Top secret)	ผ่านการอนุมัติจากผู้บริหารระดับอธิบดี ขึ้นไป

Data Class. Level Data Category	เปิดเผย (Open)	เผยแพร่ภายในองค์กร (Private)	ลับ (Confidential / sensitive)	ลับมาก (Secret / Medium Sensitive)	ลับที่สุด (Top secret / Highly Sensitive)
ข้อมูลสาธารณะ	- พ.ร.บ. ข้อมูลข่าวสารของ ทางราชการ 2540 (มาตรา 7 และมาตรา 9) - มาตรฐานและหลักเกณฑ์ การเปิดเผยข้อมูลภาครัฐ				
ข้อมูลใช้ภายใน		ISO 27001: 2013			
ข้อมูลส่วนบุคคล		พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล 2562 (มาตรา 24 - มาตรา 27)	พ.ร.บ. ข้อมูลข่าวสารของทางราชการ 2540 (มาตรา 9 และมาตรา 15 ที่เปิดเผยได้)		
ข้อมูลข่าวสารลับ			ระเบียบว่าด้วยการรักษาความลับของทางราชการ 2544		พ.ร.บ. ข้อมูลข่าวสาร ของทางราชการ 2540 (มาตรา 14 - มาตรา 15 อาจมีคำสั่งไม่ให้เปิดเผย)
ข้อมูลความมั่นคง			นโยบายและแผนระดับชาติ ว่าด้วยความมั่นคงแห่งชาติ (พ.ศ. 2562-2565)		

รูปที่ 4.2 การจัดหมวดหมู่และระดับชั้นความลับของข้อมูลภาครัฐ

4.3.4 กำหนดมาตรการควบคุมและป้องกันการเข้าถึงข้อมูล (Data Protection) โดยคำนึงถึงการจัดชั้นความลับของข้อมูลเป็นสำคัญ ดังนี้

- 1) กำหนดประเภทของข้อมูลและสารสนเทศ
- 2) พิจารณาประเภทของข้อมูลหรือสารสนเทศตามระดับต่าง ๆ ตามที่ได้กำหนด
- 3) ดำเนินการร้องขอความยินยอมในการจัดเก็บข้อมูลส่วนบุคคลจากเจ้าของข้อมูล
- 4) กำหนดชั้นความลับของข้อมูลและสารสนเทศตามระดับชั้นของข้อมูลและสารสนเทศ

โดยเป็นไปตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544

- 5) จัดทำป้ายบ่งชี้ระดับชั้นความลับของข้อมูลและสารสนเทศตามประเภทชั้นความลับที่กำหนด
- 6) เมื่อเจ้าของข้อมูลกำหนดชั้นความลับของข้อมูลและสารสนเทศแล้ว ให้ผู้ควบคุมเอกสาร (Document Controller) และผู้ใช้งานต้องดำเนินการจัดการข้อมูลและสารสนเทศตามชั้นความลับที่ได้กำหนด ยกเว้นข้อมูลที่เปิดเผยได้ที่ไม่จำเป็นต้องมีการควบคุมการจัดการข้อมูลและสารสนเทศ แต่การเปิดเผยหรือเผยแพร่ข้อมูลและสารสนเทศในระดับชั้นความลับ “ข้อมูลที่เปิดเผยได้” ต้องได้รับการตรวจสอบความถูกต้องของข้อมูลและสารสนเทศ รวมถึงต้องได้รับอนุญาตให้เปิดเผยหรือเผยแพร่จากผู้ที่มีส่วนเกี่ยวข้องก่อน

การวัดการดำเนินงานและการกำกับดูแลข้อมูลของ พพ. เป็นส่วนหนึ่งของขั้นตอนที่สำคัญในกระบวนการกำกับดูแลข้อมูล เพื่อให้ผู้บริหารและผู้รับผิดชอบส่วนงานที่เกี่ยวข้องทราบถึงผลสะท้อนจากการดำเนินงานในตลอดระยะเวลาที่ผ่านมาสามารถนำผลต่างๆ เหล่านั้นมาปรับปรุงประสิทธิภาพในการดำเนินงานให้ดียิ่งขึ้นในอนาคต ทั้งในด้านของบุคลากร (People) กระบวนการ (Process) การบริหารจัดการ (Management) และเทคโนโลยี (Technology) ซึ่งล้วนแต่มีการเปลี่ยนแปลงอยู่เสมอ การวัดหรือการประเมินผลเป็นปะจําจึงช่วยให้องค์กรสามารถดำเนินการแก้ไขปัญหาต่าง ๆ ที่เกิดขึ้นได้ทันต่อสถานการณ์ในปัจจุบัน อีกทั้งยังช่วยลดความเสี่ยงจากการดำเนินงานที่ผิดพลาดลงได้

ภาคผนวก

คำอธิบายข้อมูลหรือเมทาดาทาสำหรับชุดข้อมูลภาครัฐ (Metadata Standard)

คำอธิบายข้อมูล(Metadata) สำหรับชุดข้อมูลภาครัฐ หมายถึง ข้อมูลที่ใช้อธิบายชุดข้อมูล โดยระบุรายละเอียดแหล่งข้อมูลและคำอธิบายรายละเอียดเกี่ยวกับข้อมูล ซึ่งจะช่วยให้ผู้ใช้ข้อมูลทราบว่าข้อมูลมาจากแหล่งใด มีรูปแบบอย่างไร ช่วยอำนวยความสะดวกในการสืบค้นข้อมูลและใช้ประโยชน์ในการจัดทำบัญชีข้อมูล (Data Catalog) ของหน่วยงานและของประเทศ เพื่อสนับสนุนให้เกิดการเปิดเผย เชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ หน่วยงานของรัฐจะต้องจัดทำและระบุรายละเอียดคำอธิบายข้อมูลหรือเมทาดาทาจำนวน 14 รายการบังคับสำหรับ 1 ชุดข้อมูล โดยได้กำหนดชื่อทางเทคนิคอ้างอิงตามระบบ CKAN ซึ่งหน่วยงานของรัฐสามารถนำไปปรับใช้กับการจัดทำ คำอธิบายข้อมูลของชุดข้อมูล 14 รายการ

1. คำอธิบายชุดข้อมูลส่วนหลัก (Mandatory Metadata) เป็นรายละเอียดคำอธิบายชุดข้อมูล ส่วนหลักที่ทุกชุดข้อมูลจำเป็นต้องมี โดย 1 ชุดข้อมูล ประกอบด้วยคำอธิบายข้อมูลจำนวน 14 รายการ ได้แก่ ประเภทข้อมูล ชื่อชุดข้อมูล องค์กร ชื่อผู้ติดต่อ อีเมลผู้ติดต่อ คำสำคัญ รายละเอียด วัตถุประสงค์ ความถี่ของการปรับปรุงข้อมูล ขอบเขตเชิงภูมิศาสตร์หรือเชิงพื้นที่ แหล่งที่มา รูปแบบในการเก็บข้อมูล หมวดหมู่ข้อมูล ตามธรรมาภิบาลข้อมูลภาครัฐ และสัญญาอนุญาตให้ใช้ข้อมูล

2. คำอธิบายชุดข้อมูลทางเลือก (Optional Metadata) เป็นส่วนของรายละเอียดคำอธิบายชุด ข้อมูลเพิ่มเติมที่ช่วยให้รายละเอียดของคำอธิบายชุดข้อมูลมีความสมบูรณ์มากยิ่งขึ้น

3. พจนานุกรมข้อมูล (Data Dictionary) เป็นส่วนหนึ่งของเมทาดาทาที่มีหน้าที่อธิบายข้อมูล ภายในชุดข้อมูลอย่างละเอียดเป็นรายตัวแปร (Attribute) เพื่อสนับสนุนให้ผู้ที่ต้องการใช้ข้อมูลสามารถเข้าใจ ชุดข้อมูลในระดับตัวแปรมีประโยชน์ในการตัดสินใจว่าชุดข้อมูลนั้นมีข้อมูลตามที่ผู้ต้องการใช้กำลังค้นหอยู่หรือไม่ โดยมีส่วนที่บังคับต้องทำการอธิบายข้อมูลรายตัวแปร 3 รายการ ได้แก่ ชื่อตัวแปรข้อมูล ชนิดของตัวแปรข้อมูล และคำอธิบายตัวแปรข้อมูล

คำอธิบายชุดข้อมูลส่วนหลัก (Mandatory Metadata) 14 รายการบังคับ

- 1 ประเภทข้อมูล (5 ทางเลือก)
 - ข้อมูลระเบียบ
 - ข้อมูลสถิติ
 - ข้อมูลภูมิสารสนเทศเชิงพื้นที่
 - ข้อมูลหลากหลายประเภท
 - ข้อมูลประเภทอื่น ๆ
- 2 ชื่อชุดข้อมูล
- 3 องค์กร
- 4 ชื่อผู้ติดต่อ
- 5 อีเมลผู้ติดต่อ
- 6 คำสำคัญ
- 7 รายละเอียด
- 8 วัตถุประสงค์ (14 ทางเลือก)
- 9.1 หน่วยงานที่ของการปรับปรุงข้อมูล (13 ทางเลือก)
- 9.2 ค่าความถี่ของการปรับปรุงข้อมูล
- 10 ขอบเขตเชิงภูมิศาสตร์หรือเชิงพื้นที่ (14 ทางเลือก)
- 11 แหล่งที่มา
- 12 รูปแบบการเก็บข้อมูล (16 ทางเลือก)
- 13 หมวดหมู่ข้อมูลตามรรมมาภิบาลข้อมูลภาครัฐ (4 ทางเลือก)
- 14 สัญญาอนุญาตให้ใช้ข้อมูล (7 ทางเลือก)

คำอธิบายชุดข้อมูล ส่วนที่เป็นทางเลือก (Optional Metadata)

ข้อมูล ระเบียบ	ข้อมูล หลากหลาย ประเภท	ข้อมูล ประเภท อื่น ๆ	ข้อมูลสถิติ	ข้อมูลภูมิสารสนเทศเชิงพื้นที่
15 เจือจางในการเข้าถึงข้อมูล			15 เจือจางในการเข้าถึงข้อมูล	15 เจือจางในการเข้าถึงข้อมูล
16 วันที่เริ่มต้นสร้าง			16 ปีข้อมูลเริ่มต้นจัดทำ	16 ชุดข้อมูลภูมิศาสตร์ (13 ทางเลือก)
17 วันที่ปรับปรุงข้อมูลล่าสุด			17 ปีข้อมูลล่าสุดที่เผยแพร่	17 มาตราส่วน (6 ทางเลือก)
18 URL			18 วันที่กำหนดเผยแพร่ข้อมูล	18.1 ค่าพิกัดรอบพื้นที่ด้านทิศตะวันตก
19 ผู้สนับสนุนหรือผู้ร่วมดำเนินการ (7 ทางเลือก)			19 วันที่ปรับปรุงข้อมูลล่าสุด	18.2 ค่าพิกัดรอบพื้นที่ด้านทิศตะวันออก
20 หน่วยงานที่ย่อยที่สุดของการจัดเก็บข้อมูล (13 ทางเลือก)			20 การจัดจำแนก (14 ทางเลือก)	18.3 ค่าพิกัดรอบพื้นที่ด้านทิศเหนือ
21 ภาษาที่ใช้ (14 ทางเลือก)			21 หน่วยวัด	18.4 ค่าพิกัดรอบพื้นที่ด้านทิศใต้
22 ชุดข้อมูลที่มีคุณค่าสูง			22 หน่วยตัวคูณ (15 ทางเลือก)	19 ความถูกต้องของตำแหน่ง
23 ข้อมูลอ้างอิง			23 วิธีการคำนวณ	20 เวลาอ้างอิง
			24 มาตรฐานการจัดทำข้อมูล	21 วันที่ปรับปรุงข้อมูลล่าสุด
			25 URL	22 วันที่กำหนดเผยแพร่ข้อมูล
			26 ภาษาที่ใช้	23 วันที่เผยแพร่ข้อมูล
			27 สถิติทางการ	24 URL
				25 ภาษาที่ใช้

ที่มา: https://gdhelppage.gdcatalog.go.th/data/0_03/files/Metadata_All_Edit_65.pdf

คำอธิบายรายละเอียดตัวเลือก

สำหรับรายการคำอธิบายข้อมูลส่วนหลัก (Mandatory Metadata) สำหรับชุดข้อมูลภาครัฐ

รายการที่ 1 ประเภทข้อมูล (data_type)

Code List	รายการตัวเลือกเพื่อแสดงผล	คำอธิบาย	หมายเหตุ
1	ข้อมูลระเบียบ	ข้อมูลระเบียบ (Record) ที่จากระบบฐานข้อมูลทะเบียนหรือจากการบริหารงานขององค์กร และที่ได้จากการสำมะโน/สำรวจด้วยตัวอย่าง รวมทั้ง Transaction Data ตัวอย่างเช่น จดทะเบียนธุรกิจ และ รายการจดทะเบียนสรรพสามิต เป็นต้น	อ้างอิงจาก World Bank แบ่งประเภทข้อมูลของบัญชีข้อมูลออกเป็น Time Series, Microdata และ Geospatial (https://datacatalog.worldbank.org/) เพิ่มเติมจากมาตรฐาน Dublin core เพื่อการจัดเก็บและใช้ประโยชน์ตามประเภทข้อมูล
2	ข้อมูลสถิติ	ข้อความหรือตัวเลขที่แสดงผลที่ประมวลจากข้อมูลที่เก็บรวบรวมได้	
3	ข้อมูลภูมิสารสนเทศเชิงพื้นที่	ข้อมูลหรือสารสนเทศที่มีความสัมพันธ์กับตำแหน่งในพื้นที่ เช่น แผนที่ ภาพถ่ายทางอากาศ และภาพถ่ายทาง	
4	ข้อมูลหลากหลายประเภท	ชุดข้อมูลที่รวบรวมมาจากข้อมูลหลากหลายประเภทมาจัดเป็นชุดข้อมูลตามความต้องการใช้งาน เช่น ชุดข้อมูลที่ประกอบด้วยข้อมูลทะเบียน ข้อมูล สถิติ ข้อมูลภาพ เป็นต้น	
9	ข้อมูลประเภทอื่น ๆ ระบุ...	ข้อมูลนอกเหนือจาก 4 ประเภทข้างต้น	

รายการที่ 3 องค์กร (data_owner)

Code List	รายการตัวเลือก เพื่อแสดงผล	คำอธิบาย	หมายเหตุ
01	สำนักงานรัฐมนตรี	ส่วนราชการ	อ้างอิงจากรหัสองค์กรภาครัฐ กรมบัญชีกลาง
0101	สำนักงานปลัดสำนักนายกรัฐมนตรี	ส่วนราชการ	
0102	กรมประชาสัมพันธ์	ส่วนราชการ	
0103	สำนักงานคณะกรรมการคุ้มครองผู้บริโภค	ส่วนราชการ	
02	กระทรวงกลาโหม	ส่วนราชการ	
0201	สำนักงานปลัดกระทรวงกลาโหม	ส่วนราชการ	
0202	กรมราชองครักษ์	ส่วนราชการ	
0203	กองบัญชาการทหารสูงสุด	ส่วนราชการ	
03	กระทรวงการคลัง	ส่วนราชการ	
0302	สำนักงานปลัดกระทรวงการคลัง	ส่วนราชการ	
0303	กรมธนารักษ์	ส่วนราชการ	
0304	กรมบัญชีกลาง	ส่วนราชการ	
S306	บริษัท ท่าอากาศยานไทย จำกัด (มหาชน)	รัฐวิสาหกิจ	
S307	บริษัท การบินไทย จำกัด (มหาชน)	รัฐวิสาหกิจ	
S318	บริษัท อสมท จำกัด (มหาชน)	รัฐวิสาหกิจ	
S507	บริษัท ปตท. จำกัด (มหาชน)	รัฐวิสาหกิจ	
S508	บริษัท ปตท.สำรวจและผลิตปิโตรเลียม จำกัด (มหาชน)	รัฐวิสาหกิจ	
S509	บริษัท บางจากปิโตรเลียม จำกัด (มหาชน)	รัฐวิสาหกิจ	
S702	ธนาคารกรุงไทย	รัฐวิสาหกิจ	
S306	บริษัท ท่าอากาศยานไทย จำกัด (มหาชน)	รัฐวิสาหกิจ	
8126	กองทุนบำเหน็จบำนาญข้าราชการ (กบข.)	องค์กรของรัฐที่ จัดตั้งโดยกฎหมาย เฉพาะ	
0811	สำนักงานการบินพลเรือนแห่งประเทศไทย	องค์กรอิสระ ตามรัฐธรรมนูญ	

หมายเหตุ ตัวอย่างรหัสองค์กรภาครัฐ กรมบัญชีกลาง

รายการที่ 8 วัตถุประสงค์ (objective)

Code List	รายการตัวเลือก เพื่อแสดงผล	คำอธิบาย	หมายเหตุ
01	ยุทธศาสตร์ชาติ	ยุทธศาสตร์ชาติตามกฎหมายว่าด้วยการจัดทำยุทธศาสตร์ชาติ ซึ่งเป็นเป้าหมายการพัฒนาประเทศอย่างยั่งยืนตามหลักธรรมาภิบาลเพื่อใช้เป็นกรอบในการจัดทำแผนต่าง ๆ ให้สอดคล้องและบูรณาการกันเพื่อให้เกิดเป็นพลังผลักดันร่วมกันไปสู่เป้าหมายดังกล่าว (รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560 หมวด 6 แนวนโยบายแห่งรัฐ มาตรา 65) (แผนระดับที่ 1)	- ตอบได้มากกว่า 1 ข้อ ให้สามารถระบุคำอธิบายรายละเอียดของแต่ละตัวเลือกได้ - อ้างอิงจากระดับของแผนสำนักงานสภาพัฒนาการเศรษฐกิจและสังคมแห่งชาติ - เพิ่มเติมจากมาตรฐาน
02	แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ	แผนสำหรับถ่ายทอดยุทธศาสตร์ชาติสู่กรอบและแนวทางในการพัฒนาประเทศในแต่ละช่วงระยะเวลา 5 ปี (แผนระดับที่ 2)	Dublin core เพื่อให้เห็นถึงวัตถุประสงค์ที่เฉพาะเจาะจงและประโยชน์ต่อการติดตาม
03	แผนความมั่นคงแห่งชาติ	นโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ” ตามกฎหมายว่าด้วยความมั่นคงแห่งชาติ ซึ่งเป็นนโยบายและแผนหลักของชาติที่เป็นกรอบหรือทิศทางในการดำเนินการป้องกัน แจ่งเตือน แก้ไขหรือระงับยับยั้งภัยคุกคามเพื่อธำรงไว้ซึ่งความมั่นคงแห่งชาติ ปี (แผนระดับที่ 2)	ประเมินผลการดำเนินงานของตามแผนระดับต่าง ๆ ของประเทศ เชื่อมโยงกับระบบติดตามและประเมินผลแห่งชาติ (eMENSER) ซึ่งเป็นหน้าที่ขององค์กรของรัฐทุก
04	แผนแม่บทภายใต้ยุทธศาสตร์ชาติ	แผนแม่บทเพื่อบรรลุเป้าหมายตามที่กำหนดไว้ในยุทธศาสตร์ชาติ (พระราชบัญญัติการจัดทำยุทธศาสตร์ชาติ พ.ศ. 2560 มาตรา 3 ปี (แผนระดับที่ 2)	หน่วยในการรายงานผลการดำเนินการตามยุทธศาสตร์ชาติ
05	แผนปฏิรูปประเทศ	แผนและขั้นตอนการดำเนินการปฏิรูปประเทศ ตามพระราชบัญญัติ แผนและขั้นตอนการดำเนินการปฏิรูปประเทศ พ.ศ. 2560 ปี (แผนระดับที่ 2)	- เพิ่มเติมในส่วนของคุณข้อมูลเพื่อการให้บริการประชาชน
06	แผนระดับที่ 3 (มติ ครม. 4 ธ.ค. 2560)	แผนที่จัดทำขึ้นเพื่อสนับสนุนการดำเนินงานของแผนระดับที่ 1 และแผนระดับที่ 2 ให้บรรลุเป้าหมายที่กำหนดไว้ หรือจัดทำขึ้นตามที่กฎหมายกำหนด หรือจัดทำขึ้นตามพันธกรณีหรืออนุสัญญาระหว่างประเทศ เช่น แผนปฏิบัติราชการของส่วนราชการ แผนปฏิบัติการด้านต่าง ๆ เพื่อถ่ายทอดเป้าหมายและตัวชี้วัดรวมถึงแนวทางการพัฒนาสู่การดำเนินงานขององค์กรอย่างเป็นระบบ	

รายการที่ 8 วัตถุประสงค์ (objective) (ต่อ)

Code List	รายการตัวเลือกเพื่อแสดงผล	คำอธิบาย	หมายเหตุ
07	นโยบายรัฐบาล/ข้อสั่งการนายกรัฐมนตรี		
08	มติคณะรัฐมนตรี	ผลการตัดสินใจร่วมกันของคณะรัฐมนตรีในการบริหารราชการแผ่นดินเรื่องต่าง ๆ ตามที่กำหนดไว้ในรัฐธรรมนูญ กฎหมาย และนโยบายของ คณะรัฐมนตรี เช่น มติคณะรัฐมนตรีเกี่ยวกับการ อนุมัติร่างกฎหมาย การอนุมัติงบประมาณ การ แต่งตั้งโยกย้ายข้าราชการ การกำหนดระเบียบและ แบบแผนในการปฏิบัติราชการ	
09	เพื่อให้การให้บริการประชาชน	ตาม พรบ. การอำนวยความสะดวกในการพิจารณาอนุญาตของทางราชการ ที่กำหนดให้องค์กรของรัฐ กำหนดกระบวนการขั้นตอนและเวลาในการพิจารณาอนุญาตให้มีความชัดเจน ซึ่งจะเป็นการอำนวยความสะดวกแก่ประชาชน	
10	กฎหมายที่เกี่ยวข้อง		
11	พันธกิจองค์กร		
12	ดัชนี/ตัวชี้วัดระดับนานาชาติ	ข้อมูลสำคัญที่แสดงสถานการณ์และแนวโน้มการพัฒนาของประเทศไทยโดยเปรียบเทียบกับประเทศอื่น ๆ	
98	ไม่ทราบ		
99	อื่น ๆ	วัตถุประสงค์อื่น ๆ ซึ่งมีได้จัดประเภทไว้ในที่อื่น	

รายการที่ 9.1 หน่วยความถี่ของการปรับปรุง (update_frequency_unit)

Code List	รายการตัวเลือก เพื่อแสดงผล	คำอธิบาย	หมายเหตุ
A	ปี	-	- อ้างอิงจาก SDMX Cross-Domain Code Lists (https://sdmx.org/?page_id=3215) เนื่องจาก Dublin Core ไม่มีมาตรฐานสำหรับรายการตัวเลือกของหน่วยความถี่ นอกจากนี้ได้มีการนิยามรหัสเพิ่มเติมเพื่อสนับสนุนการใช้งานจริง - กรณีที่ชุดข้อมูลมาจากหลายแหล่ง และมีความถี่ของการปรับปรุงแตกต่างกันให้เลือกความถี่การปรับปรุงข้อมูลที่บ่อยที่สุด
S	ครึ่งปี	-	
Q	ไตรมาส	-	
M	เดือน	-	
W	สัปดาห์	-	
D	วัน	-	
B	วันทำการ	-	
H	ชั่วโมง	-	
N	นาที	-	
R	ตามเวลาจริง	-	
O	ไม่มีการปรับปรุงหลังจากการจัดเก็บข้อมูล	-	
X	อื่น ๆ ระบุ...	-	
U	ไม่ทราบ	-	

รายการที่ 10 ขอบเขตเชิงภูมิศาสตร์หรือเชิงพื้นที่ (geo_coverage)

Code List	รายการตัวเลือกเพื่อแสดงผล	คำอธิบาย	หมายเหตุ
00	ไม่มี		- ในระดับสากลอ้างอิงตาม Geographic Scope of Activity ของ UN Data Catalog Metadata http://undatacatalog.org/g/metadata - ในระดับประเทศอ้างอิงตามการแบ่งเขตการปกครองของกระทรวงมหาดไทย และสำนักงานสถิติแห่งชาติ
01	โลก		
02	ทวีป/กลุ่มประเทศในทวีป	ทวีป ได้แก่ แอฟริกา อเมริกา เอเชีย ยุโรป โอเชียเนีย และกลุ่มประเทศภายใต้ทวีปดังกล่าว	
03	กลุ่มประเทศทางเศรษฐกิจ	กลุ่มตามระดับการพัฒนาทางเศรษฐกิจ ได้แก่ กลุ่มประเทศที่พัฒนาแล้ว กลุ่มประเทศที่พัฒนาแล้วกำลังพัฒนา กลุ่มประเทศที่มีระดับการพัฒนาน้อยที่สุด กลุ่มประเทศที่ไม่มีอาณาเขตติดทะเล (Landlocked developing countries) กลุ่มประเทศกำลังพัฒนาที่เป็นหมู่เกาะ (Small island developing states) รวมถึงการจัดกลุ่มประเทศในมิติอื่น ๆ เช่น OECD, ASEAN+3, OPEC ฯลฯ	
04	ประเทศ		
05	ภาค		
06	จังหวัด		
07	อำเภอ		
08	ตำบล		
09	หมู่บ้าน		
10	เทศบาล/อบต.	องค์การปกครองส่วนท้องถิ่น	
11	พิกัด	ค่าของตัวเลขที่ใช้อธิบายตำแหน่งของจุดบนระนาบหรือปริภูมิ ตัวอย่างเช่น ระดับความสูงจากน้ำทะเล ก็เป็นพิกัดอย่างหนึ่งที่อธิบายตำแหน่งของจุดเหนือระดับพื้นผิวโลก โดยกำหนดพิกัดละติจูด เป็นทศนิยม 6 หลัก	
99	อื่น ๆ ระบุ...	ขอบเขตเชิงภูมิศาสตร์หรือเชิงพื้นที่ซึ่งมิได้จัดประเภทไว้ในที่อื่น เช่น กลุ่มจังหวัด เขตปกครองพิเศษ เขตพัฒนาการท่องเที่ยว เขตส่งเสริมพิเศษ เขตสาธารณสุข เขตพื้นที่การศึกษา เป็นต้น	
98	ไม่ทราบ		

รายการที่ 12 รูปแบบการเก็บข้อมูล (data_format)

Code List	รายการตัวเลือกเพื่อแสดงผล	คำอธิบาย	หมายเหตุ
01	Database	-	มาตรฐานรูปแบบการจัดเก็บข้อมูลโดย Dublin Core (DCMI Metadata Terms) ไม่ได้กำหนดตัวเลือกสำหรับรูปแบบการเก็บข้อมูล (Format) ที่ชัดเจน คณะผู้จัดทำจึงกำหนดตัวเลือกเหล่านี้ขึ้นโดยอ้างอิงจากรูปแบบไฟล์ที่ใช้กันอย่างแพร่หลายในปัจจุบัน และประยุกต์ใช้บางรายการจากประเภทของ MIME (Internet Media Types) ที่ Dublin Core แนะนำเป็นแนวทาง ทั้งนี้ สามารถเลือกกรอกได้มากกว่า 1 ตัวเลือก
02	CSV	-	
03	XML	-	
04	Image	-	
05	Video	-	
06	Audio	-	
07	Text	-	
08	JSON	-	
09	HTML	-	
10	XLS	-	
11	PDF	-	
12	RDF	-	
13	NoSQL	-	
14	Vector	เช่น Shapefile SVG GML	
15	Raster	เช่น GeoTiff JPEG2000	
99	อื่น ๆ ระบุ	-	

รายการที่ 13 หมวดหมู่ข้อมูลตามธรรมาภิบาลข้อมูลภาครัฐ (data_category)

Code List	รายการตัวเลือกเพื่อแสดงผล	คำอธิบาย	หมายเหตุ
1	ข้อมูลสาธารณะ	ข้อมูลที่สามารถเปิดเผยได้ สามารถนำไปใช้ได้อย่างอิสระ ไม่ว่าจะเป็นข้อมูลข่าวสาร ข้อมูลส่วนบุคคล ข้อมูลอิเล็กทรอนิกส์ เป็นต้น	อ้างอิงประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ กรณีที่ชุดข้อมูลประกอบด้วยข้อมูลมากกว่า 1 ประเภท ให้เลือกหมวดหมู่ธรรมาภิบาลข้อมูลภาครัฐที่ต้องให้ความคุ้มครองสูงสุด
2	ข้อมูลส่วนบุคคล	ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรม โดยเฉพาะ (พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562)	
3	ข้อมูลความมั่นคง	ข้อมูลเกี่ยวกับความมั่นคงของรัฐ ที่ทำให้เกิดความสงบเรียบร้อย การมีเสถียรภาพ ความเป็นปึกแผ่น ปลอดภัยจากภัยคุกคาม เป็นต้น	
4	ข้อมูลความลับทางราชการ	ข้อมูลที่อยู่ในความครอบครองหรือควบคุมดูแลขององค์กรของรัฐที่มีคำสั่งไม่ให้มีการเปิดเผย และมีการกำหนดชั้นความลับของข้อมูล	
5	ข้อมูลใช้ภายใน	ข้อมูลสำหรับใช้ในการดำเนินงานภายในของหน่วยงานซึ่งไม่อนุญาตให้นำไปใช้งานภายนอกก่อนได้รับอนุญาตจากเจ้าของข้อมูล เช่น ร่างนโยบาย ร่างมาตรฐาน และขั้นตอนการปฏิบัติงาน ประกาศ และบันทึกภายในหน่วยงานที่อยู่ระหว่างการขออนุมัติ เป็นต้น	อยู่ระหว่างการกำหนด Code List ของหน่วยงานที่เกี่ยวข้อง

รายการที่ 14 สัญญาอนุญาตให้ใช้ข้อมูล (right_of_usage)

Code List ¹	รายการตัวเลือกเพื่อแสดงผล	คำอธิบาย	หมายเหตุ
	G0	อนุญาตให้ผู้อื่นสามารถนำผลงานไปใช้ ทำซ้ำ แจกจ่าย หรือดัดแปลงงานนั้นได้ โดยไม่มีข้อจำกัด	Open Data Common
	G1	อนุญาตให้ผู้อื่นสามารถนำผลงานไปใช้ ทำซ้ำ แจกจ่าย หรือดัดแปลงงานนั้นได้ แต่ต้องให้เครดิตที่มาของเจ้าของผลงาน	Creative Commons Attribution
	G2	อนุญาตให้ผู้อื่นสามารถนำผลงานไปใช้ ทำซ้ำ แจกจ่าย หรือดัดแปลงงานนั้นได้ แต่ต้องให้เครดิตที่มาของเจ้าของผลงาน และต้องไม่ใช่เพื่อการค้า	Creative Commons Attribution- NonCommercial
	G3.1	อนุญาตให้ผู้อื่นสามารถนำผลงานไปใช้ ทำซ้ำ แจกจ่าย หรือดัดแปลงงานนั้นได้ แต่ต้องให้เครดิตที่มาของเจ้าของผลงาน และจะต้องกำกับด้วยสัญญาอนุญาตเงื่อนไขเดียวกันกับต้นฉบับ	Creative Commons Attribution- ShareAlike
	G3.2	อนุญาตให้ผู้อื่นสามารถนำผลงานไปใช้ ทำซ้ำ แจกจ่าย หรือดัดแปลงงานนั้นได้ แต่ต้องไม่ใช่เพื่อการค้าและจะต้องกำกับด้วยสัญญาอนุญาตเงื่อนไขเดียวกันกับต้นฉบับ	Creative Commons Attribution- NonCommercialShareAlike
	G4.1	อนุญาตให้ผู้อื่นสามารถนำผลงานไปทำซ้ำ แจกจ่าย โดยห้ามแก้ไขหรือดัดแปลงผลงานนั้น แต่ต้องให้เครดิตที่มาของเจ้าของผลงาน และต้องไม่ใช่เพื่อการค้า	Creative Commons Attribution- NonCommercialNoDerivs
	G5	สัญญาอนุญาตให้ใช้ข้อมูลอื่น ๆ โดยเงื่อนไขเป็นไปตามที่เจ้าของข้อมูลกำหนด และผู้ใช้ข้อมูลสามารถขอใช้ข้อมูลได้เป็นรายกรณี	Others License
	G4.2	อนุญาตให้ผู้อื่นสามารถนำผลงานไปทำซ้ำ แจกจ่าย โดยห้ามแก้ไขหรือดัดแปลงผลงานนั้น และต้องให้เครดิตที่มาของเจ้าของผลงาน	Creative Commons Attribution- NoDerivs

¹ อยู่ระหว่างการกำหนด Code List ของหน่วยงานที่เกี่ยวข้อง

คำอธิบายรายละเอียดตัวเลือก
สำหรับรายการคำอธิบายข้อมูลส่วนที่เป็นทางเลือก (Optional Metadata)
สำหรับชุดข้อมูลภาครัฐ: ประเภทข้อมูลระเบียบ

รายการที่ 15 ระดับชั้นข้อมูล (data_classification)

Code List	รายการตัวเลือกเพื่อแสดงผล	คำอธิบาย	หมายเหตุ
	เปิดเผย	ข้อมูลที่สามารถเปิดเผยได้ สามารถนำไปใช้ได้อย่างอิสระ ไม่ว่าจะเป็นข้อมูลข่าวสาร ข้อมูลส่วนบุคคล ข้อมูลอิเล็กทรอนิกส์ เป็นต้น	อยู่ระหว่างการกำหนด Code List ของหน่วยงานที่เกี่ยวข้อง
	ชั้นเผยแพร่ภายในองค์กร	ข้อมูลอ่อนไหวที่มีการใช้และเผยแพร่ภายในองค์กร หรือไม่ได้เผยแพร่โดยอิสระ โดยทั่วไปจะเกี่ยวข้องกับข้อมูลที่มีลักษณะเป็นส่วนตัว (Private) ไม่ว่าจะเป็นข้อมูลบุคคล หรือองค์กร และแม้ว่าการสูญเสียหรือการเปิดเผยข้อมูล อาจไม่ส่งผลให้เกิดผลกระทบที่สำคัญ แต่ก็ไม่พึงประสงค์ที่เปิดเผยโดยไม่ได้รับอนุญาต ซึ่งการเปิดเผย ข้อมูลนี้แก่บุคคลที่ไม่ได้รับอนุญาต อาจขัดต่อกฎหมาย และระเบียบข้อบังคับขององค์กร	อยู่ระหว่างการกำหนด Code List ของหน่วยงานที่เกี่ยวข้อง
	ลับ	ความลับที่มีความสำคัญที่สุดเกี่ยวกับบุคคลข้อมูล ข่าวสารวัตถุ สถานที่ และทรัพย์สินมีค่าของแผ่นดินซึ่งหากความลับดังกล่าวทั้งหมด หรือเพียงบางส่วนรั่วไหล ไปถึงบุคคลผู้ไม่มีหน้าที่ได้ทราบจะทำให้เกิดความเสียหายต่อความมั่นคงและผลประโยชน์แห่งรัฐ ซึ่งผู้ที่เข้าถึงได้ต้องเป็นผู้มีสิทธิเท่านั้น และห้ามเผยแพร่ต่อบุคคลภายนอกเว้นแต่จะได้รับอนุมัติเป็นลายลักษณ์อักษรโดยผู้บริหารระดับต้น หรือ หัวหน้ากลุ่ม/เทียบเท่า ที่เป็นเจ้าของข้อมูลขึ้นไป โดยต้องมีการลงนามใน เอกสารข้อตกลงการไม่เปิดเผยข้อมูล (Non-Disclosure Agreement) เว้นแต่การเผยแพร่ดังกล่าวเป็นไปตาม อำนาจที่กฎหมายให้การรับรอง	อยู่ระหว่างการกำหนด Code List ของหน่วยงานที่เกี่ยวข้อง
	ลับมาก	ความลับที่มีความสำคัญที่สุดเกี่ยวกับบุคคลข้อมูล ข่าวสารวัตถุ สถานที่ และทรัพย์สินมีค่าของแผ่นดิน ซึ่งหากความลับดังกล่าวทั้งหมดหรือเพียงบางส่วนรั่วไหล ไปถึงบุคคลผู้ไม่มีหน้าที่ได้ทราบ จะทำให้เกิดความเสียหายต่อความมั่นคงและผลประโยชน์แห่งรัฐอย่างร้ายแรง ซึ่งผู้ที่สามารถเข้าถึงได้ต้องเป็นบุคคลที่มีสิทธิเท่านั้น และห้ามเผยแพร่ต่อบุคคลภายนอก เว้นแต่จะได้รับอนุมัติเป็นลายลักษณ์อักษรโดยผู้บริหาร ระดับกลาง หรือ ผู้อำนวยการ/เทียบเท่าเป็นเจ้าของข้อมูลขึ้นไปโดยต้องมีการลงนามในเอกสารข้อตกลงการไม่เปิดเผยข้อมูล (Non-Disclosure Agreement) เว้นแต่การเผยแพร่ดังกล่าวเป็นไปตามอำนาจที่กฎหมายให้การรับรอง	อยู่ระหว่างการกำหนด Code List ของหน่วยงานที่เกี่ยวข้อง

รายการที่ 15 เงื่อนไขการเข้าถึงข้อมูล

Code List	รายการตัวเลือกเพื่อแสดงผล	คำอธิบาย	หมายเหตุ
	ไม่มีการจำกัดการเข้าถึงข้อมูล	ข้อมูลระดับชั้นเปิดเผย	อยู่ระหว่างการ กำหนด Code List ของหน่วยงานที่เกี่ยวข้อง
	เฉพาะบุคคลภายในหน่วยงาน	ข้อมูลระดับชั้นเผยแพร่ภายในองค์กร จำกัดการเข้าถึงข้อมูลเฉพาะบุคคลภายในหน่วยงาน	อยู่ระหว่างการ กำหนด Code List ของหน่วยงานที่เกี่ยวข้อง
	ต้องได้รับอนุมัติจากผู้บริหารระดับผู้ช่วยผู้อำนวยการขึ้นไป	ข้อมูลระดับชั้นลับ การเข้าถึงต้องผ่านการอนุมัติจากผู้บริหารระดับผู้ช่วยผู้อำนวยการขึ้นไป	อยู่ระหว่างการ กำหนด Code List ของหน่วยงานที่เกี่ยวข้อง
	ต้องได้รับอนุมัติจากผู้บริหารระดับรองผู้อำนวยการขึ้นไป	ข้อมูลระดับชั้นลับมาก การเข้าถึงต้องผ่านการอนุมัติจากผู้บริหารระดับรองผู้อำนวยการขึ้นไป	อยู่ระหว่างการ กำหนด Code List ของหน่วยงานที่เกี่ยวข้อง

รายการที่ 19 ผู้สนับสนุนหรือผู้ร่วมดำเนินการ (data_support)

Code List	รายการตัวเลือกเพื่อแสดงผล	คำอธิบาย	หมายเหตุ
0	ไม่มี		เลือกรายการตัวเลือกพร้อมระบุชื่อองค์กร/องค์กร/ผู้ให้การสนับสนุนหรือร่วมดำเนินการ ทั้งนี้สามารถเลือกกรอกได้มากกว่า 1 ตัวเลือก
1	องค์กรของรัฐ	ส่วนราชการ รัฐวิสาหกิจ องค์กรมหาชน และองค์กรของรัฐรูปแบบใหม่ (ไม่รวมสถาบันการศึกษา)	
2	องค์กรเอกชน	องค์กรเอกชน (ไม่รวมสถาบันการศึกษา)	
3	องค์กร/องค์กรระหว่างประเทศ		
4	มูลนิธิ/สมาคม		
5	สถาบันการศึกษา		
9	อื่น ๆ		

รายการที่ 20 หน่วยที่ย่อยที่สุดของการจัดเก็บข้อมูล (data_collect)

Code List	รายการตัวเลือกเพื่อแสดงผล	คำอธิบาย	หมายเหตุ
00	ไม่มี		รายการที่ 1-5 อ้างอิงหน่วยวิเคราะห์ทางสถิติของสำนักงานสถิติแห่งชาติ
01	บุคคล		
02	ครัวเรือน/ครอบครัว		
03	บ้าน/ที่อยู่อาศัย		
04	บริษัท/ห้างร้าน/สถานประกอบการ		
05	อาคาร/สิ่งปลูกสร้าง		
06	พื้นที่การเกษตร ประมง ป่าไม้		
07	สัตว์และพันธุ์พืช		
08	ขอบเขตเชิงภูมิศาสตร์หรือเชิงพื้นที่		
09	แหล่งน้ำ เช่น แม่น้ำ อ่างเก็บน้ำ		
10	เส้นทางการเดินทาง เช่น ถนน ทางรถไฟ		
98	ไม่ทราบ		
99	อื่น ๆ ระบุ		

รายการที่ 21 ภาษาที่ใช้ (data_language)

Code List	รายการตัวเลือกเพื่อแสดงผล	คำอธิบาย	หมายเหตุ
01	ไทย		- ตอบได้มากกว่า 1 ข้อ - อ้างอิงจากภาษาที่ใช้มากในประเทศไทย https:// th.wikipedia.org/wiki/ภาษาที่ใช้ในประเทศไทย
02	อังกฤษ		
03	จีน		
04	มลายู		
05	พม่า		
06	ลาว		
07	เขมร		
08	ญี่ปุ่น		
09	เกาหลี		
10	ฝรั่งเศส		
11	เยอรมัน		
12	อารบิก		
98	ไม่ทราบ		
99	อื่น ๆ ระบุ		

คำอธิบายรายละเอียดตัวเลือก
สำหรับรายการคำอธิบายข้อมูลส่วนที่เป็นทางเลือก (Optional Metadata)
สำหรับชุดข้อมูลภาครัฐ: ประเภทข้อมูลสถิติ

รายการที่ 20 การจัดจำแนก (disaggregation)

Code List	รายการตัวเลือกเพื่อแสดงผล	คำอธิบาย	หมายเหตุ
00	ไม่มี		- สามารถตอบได้มากกว่า 1 คำตอบ - อ้างอิงจากการรวบรวมการจัดจำแนกที่ใช้มากในการจัดทำสถิติทางการสำนักงานสถิติแห่งชาติ
01	เพศ		
02	อายุ/กลุ่มอายุ		
03	สถานภาพสมรส		
04	ศาสนา		
05	ระดับการศึกษา		
06	อาชีพ		
07	สถานภาพการทำงาน		
08	อุตสาหกรรม/ประเภทกิจการ		
09	รายได้		
10	ขอบเขตเชิงภูมิศาสตร์หรือเชิงพื้นที่		
11	ผลิตภัณฑ์		
98	ไม่ทราบ		
99	อื่น ๆ ระบุ	ข้อมูลจัดจำแนกด้วยมิติอื่น ๆ ซึ่งมีได้จัดประเภทไว้ในที่อื่น โดยสามารถระบุได้มากกว่า 1 การจัดจำแนกโดยใช้เครื่องหมาย “,” คั่นระหว่างการจัด จำแนก เช่น ประเภทค่าใช้จ่าย, ประเภทสวัสดิการ	

รายการที่ 22 หน่วยตัวคูณ (unit_of_multiplier)

Code List	รายการตัวเลือก เพื่อแสดงผล	คำอธิบาย	หมายเหตุ
00	หน่วย	Units หรือ 10^0	อ้างอิงตาม Code list for concept "Unit Multiplier" as written in SDMX crossdomain code list. Version 1.1
01	สิบ	Tens หรือ 10^1	
02	ร้อย	Hundreds หรือ 10^2	
03	พัน	Thousands หรือ 10^3	
04	หมื่น	Tens of thousands หรือ 10^4	
05	แสน	Hundreds of thousands หรือ 10^5	
06	ล้าน	Millions หรือ 10^6	
07	สิบล้าน	Tens of Millions หรือ 10^7	
08	ร้อยล้าน	Hundreds of Millions หรือ 10^8	
09	พันล้าน	Billions หรือ 10^9	
10	หมื่นล้าน	Tens of Billions หรือ 10^{10}	
11	แสนล้าน	Hundreds of Billions หรือ 10^{11}	
12	ล้านล้าน	Trillions หรือ 10^{12}	
98	ไม่ทราบ	-	
99	อื่น ๆ ระบุ	ข้อมูลจัดจำแนกด้วยมิติอื่น ๆ ซึ่งมีได้จัดประเภทไว้ในที่อื่น โดยสามารถระบุได้มากกว่า 1 การจัดจำแนกโดยใช้ เครื่องหมาย “,”” คั่นระหว่างการจัด จำแนก เช่น ประเภทค่าใช้จ่าย, ประเภทสวัสดิการที่ได้รับ	

คำอธิบายรายละเอียดตัวเลือก
สำหรับรายการคำอธิบายข้อมูลส่วนที่เป็นทางเลือก (Optional Metadata)
สำหรับชุดข้อมูลภาครัฐ: ประเภทข้อมูลภูมิศาสตร์สารสนเทศ

รายการที่ 16 ชุดข้อมูลภูมิศาสตร์ (geographic_data_set)

Code list	รายการตัวเลือกเพื่อแสดงผล	คำอธิบาย	หมายเหตุ
01	ชั้นข้อมูลแปลงที่ดิน	ข้อมูลที่แสดงพื้นที่บนพื้นผิวโลกที่มีการถือครองโดย ภาครัฐและเอกชน	อ้างอิงจาก Fundamental Geographic Data Set http://www.ngis.go.th/home/wp-content/uploads/2019/03/FundamentalGeographicDataSet_FGDS.pdf
02	ชั้นข้อมูลขอบเขตการปกครอง	ข้อมูลที่ประกอบด้วยรูปลักษณ์ทางภูมิศาสตร์ 4 รายการ ได้แก่ หมุดหลักเขตการปกครอง เส้นเขตการปกครอง พื้นที่การปกครอง และจุดแทนพื้นที่การปกครอง	
03	ชั้นข้อมูลเส้นทางคมนาคม	ชั้นข้อมูลที่เป็นสื่อกลางสำหรับการแลกเปลี่ยนและการใช้ประโยชน์ร่วมกันในงานด้านการคมนาคม ประกอบด้วย รูปลักษณ์ทางภูมิศาสตร์ 12 รายการ ได้แก่ ขอบถนน จุดคมนาคม ถนน สะพาน อุโมงค์และทางลอด จุดกลับรถ จุดทางแยก/จุดตัด เส้นทางรถไฟ จุดสนใจ เส้นทาง เดินเรือ และข้อมูลอาณัติสัญญาณ	
04	ชั้นข้อมูลชุมชน/อาคาร	ชั้นข้อมูลที่ใช้จัดเก็บข้อมูลที่เกี่ยวข้องกับพื้นที่ที่มีการก่อสร้างโดยมนุษย์ ในรูปของโรงเรือน ร้าน หรือรูปแบบอื่นสำหรับการใช้สอย และมักมีคนอยู่เสมอ ประกอบด้วย รูปลักษณ์ทางภูมิศาสตร์ 4 รายการ คือ อาคาร สิ่งปลูกสร้าง สถานที่อ้างอิง และเขตชุมชน	
05	ชั้นข้อมูลป่าไม้	ชั้นข้อมูลป่าไม้ประกอบด้วย (1) พื้นที่ป่าไม้ตามกฎหมาย (Legal forest area) ที่จัดเก็บในรูปพื้นที่รูปปิด (polygon) เพื่อแสดงขอบเขตพื้นที่ป่าไม้ตามกฎหมายที่ถูกประกาศจัดตั้งขึ้นภายใต้กฎหมายเฉพาะ ได้แก่ อุทยานแห่งชาติ เขตรักษาพันธุ์สัตว์ป่า และป่าสงวนแห่งชาติ และ (2) พื้นที่ป่าไม้ตามสภาพ (Existing Forest area) ที่จัดเก็บในรูปพื้นที่รูปปิดสำหรับแสดงขอบเขตการปกคลุมของป่าไม้ที่เกิดขึ้นเองในธรรมชาติหรือโดยมนุษย์สร้างขึ้น ซึ่งได้จากการวิเคราะห์และแปลตีความข้อมูลภาพถ่ายจากดาวเทียม ภาพถ่ายทางอากาศ หรือการสำรวจข้อมูลภาคสนาม	

รายการที่ 16 ชุดข้อมูลภูมิศาสตร์ (geographic_data_set) (ต่อ)

Code list	รายการตัวเลือกเพื่อแสดงผล	คำอธิบาย	หมายเหตุ
06	ชั้นข้อมูลการใช้ประโยชน์ที่ดิน	ข้อมูลที่แสดงลักษณะของพื้นที่ที่มนุษย์เข้าไปครอบครองแล้วมีการจัดการเปลี่ยนแปลงพื้นที่ หรือมีการทำกิจกรรมต่าง ๆ เพื่อสนองความต้องการของมนุษย์ เช่น การใช้พื้นที่เป็นพื้นที่เกษตรกรรม พื้นที่กักเก็บน้ำ ใช้เป็นที่ตั้งบ้านเรือนที่อยู่อาศัย หรือเป็นที่ตั้งเขตอุตสาหกรรม	
07	ชั้นข้อมูลแหล่งน้ำ	ข้อมูลที่แสดงบริเวณที่มีการสะสมของน้ำบนพื้นผิวโลก แบ่งได้สองประเภทตามการกำเนิดคือ แหล่งน้ำธรรมชาติ เช่น แม่น้ำ หนอง บึง และน้ำบาดาล เป็นต้น และแหล่งน้ำที่มนุษย์สร้างขึ้น เช่น อ่างเก็บน้ำ บ่อน้ำในไร่นา บ่อน้ำบาดาลและคลองชลประทาน เป็นต้น นอกจากนี้ยังสามารถแบ่งตามการเคลื่อนที่ของน้ำ เช่น แม่น้ำและคลอง กล่าวถึงแหล่งน้ำที่มีการไหลจากที่หนึ่งไปอีกที่หนึ่ง ในขณะที่ทะเลสาบ น้ำจะไม่มีการไหลไปแหล่งอื่น แหล่งน้ำที่มีการสัญจรจะถูกเรียกว่าเส้นทางน้ำ ชั้นข้อมูลแหล่งน้ำประกอบด้วยสัญลักษณ์ทางภูมิศาสตร์ 3 กลุ่ม คือ 1.แหล่งน้ำธรรมชาติ 2.สิ่งก่อสร้างในลำน้ำ 3.แหล่งน้ำที่มนุษย์สร้างขึ้น	
08	ชั้นข้อมูลอุทกศาสตร์	ชั้นข้อมูลอุทกศาสตร์เป็นการนำข้อมูลที่อยู่ในทะเลและบนบกบางส่วนทั้งในส่วนที่มนุษย์สร้างขึ้น เช่น ท่าเรือ หรือประการและเกิดขึ้นเองตามธรรมชาติ เช่น แนวโซดหิน สันดอน เป็นต้น มีวัตถุประสงค์ในการจัดทำ เพื่อความปลอดภัยในการเดินเรือเพื่อสนับสนุนการพัฒนาประเทศในด้านการคมนาคมทางทะเล	
09	ชั้นข้อมูลมหุดหลักฐานแผนที่	ข้อมูลที่แสดงมหุดที่จัดสร้างขึ้นอย่างมั่นคง แข็งแรง และมีการรังวัดค่าพิกัดตำแหน่งที่มีความถูกต้องสูงชั้นข้อมูลมหุดหลักฐานแผนที่ประกอบด้วยสัญลักษณ์ทางภูมิศาสตร์ (geographic feature) 4 รายการ ได้แก่ มหุดหลักฐาน ทางราบ มหุดหลักฐานทางตั้ง มหุดหลักฐานสามมิติ และ จุดบังคับภาพถ่าย โดยมีข้อมูลลักษณะประจำที่สำคัญคือ รหัสหมายเลขประจำมหุดฯ คำอธิบายและภาพแผนที่ที่ตั้ง ของมหุด ค่าพิกัดของมหุดฯ องค์การที่รับผิดชอบ ระดับ ความถูกต้องของค่าพิกัดมหุดฯ และระดับชั้นงานของการสำรวจรังวัดมหุดฯ นั้น	

รายการที่ 16 ชุดข้อมูลภูมิศาสตร์ (geographic_data_set) (ต่อ)

Code list	รายการตัวเลือกเพื่อแสดงผล	คำอธิบาย	หมายเหตุ
10	ชั้นข้อมูลความสูงภูมิประเทศเชิงตัวเลข	ข้อมูลที่ใช้แสดงลักษณะความสูงภูมิประเทศเชิงเลขในพื้นที่แห่งหนึ่งโดยการบันทึกค่าระดับของกลุ่มของจุดที่มีระยะห่างระหว่างจุดคงที่ ครอบคลุมพื้นที่นั้น ๆ ลงในแฟ้มข้อมูลคอมพิวเตอร์	
11	ชั้นข้อมูลภาพแผนที่ภูมิประเทศ	ข้อมูลภาพ (image) ของแผนที่ภูมิประเทศมาตราส่วนหลักของประเทศไทย ที่มีแหล่งข้อมูลนำเข้าที่ได้มาตรฐานและครบถ้วนในรายละเอียดของแผนที่ภูมิประเทศ	
12	ชั้นข้อมูลแผนที่ภาพถ่ายทางอากาศ	ภาพราสเตอร์ของภาพถ่ายทางอากาศที่ผ่านการกระบวนการตัดแก้ (rectified) ผลกระทบจากการถ่ายภาพเอียง (tilted) และความสูงของภูมิประเทศ (relief displacement) โดยอ้างอิงกับระบบพิกัดโลกเรียบร้อยแล้ว ซึ่งในที่นี้จะหมายถึงแผนที่ภาพถ่ายทางอากาศมาตราส่วน 1:4,000 1:10,000 1:25,000 1:50,000 1:250,000	
13	ชั้นข้อมูลภาพวาดดาวเทียมตัดแก้	ภาพราสเตอร์ของข้อมูลภาพถ่ายจากดาวเทียมที่ผ่านการกระบวนการตัดแก้ทางด้านตำแหน่ง (geometric rectification) แล้ว	

รายการที่ 17 มาตราส่วนของชุดข้อมูล (equivalent_scale)

Code List	รายการตัวเลือกเพื่อแสดงผล	คำอธิบาย	หมายเหตุ
01	1:4,000		อ้างอิงจาก Fundamental Geographic Data Set
02	1:10,000		
03	1:25,000		
04	1:50,000		
05	1:250,000		
99	อื่น ๆ ระบุ.....		

สัญญาอนุญาตให้ใช้ข้อมูล

สัญญาอนุญาตให้ใช้ข้อมูลเป็นข้อตกลงแนวทางการใช้ข้อมูลระหว่างหน่วยงานผู้เป็นเจ้าของข้อมูลและผู้ใช้ข้อมูลเพื่อลดระยะเวลาในการจัดทำบันทึกข้อตกลงของภาครัฐ (MOU) และอำนวยความสะดวกให้เกิดการเปิดเผย/แบ่งปันข้อมูลที่สะดวกมากขึ้นโดยสัญญาอนุญาตให้ใช้ข้อมูลสามารถแบ่งได้เป็น 6 ประเภท (G0 – G5) ดังนี้

สัญญาอนุญาตให้ใช้ข้อมูล		คำอธิบายสัญญาของสัญญาอนุญาตให้ใช้ข้อมูล	ข้อเสนอแนะ
G0	Open Data Common	อนุญาตให้ผู้อื่นสามารถนำผลงานไปใช้ ทำซ้ำ แจกจ่าย หรือดัดแปลงงานนั้นได้ โดยไม่มีข้อจำกัด	ควรใช้กับหมวดหมู่ข้อมูลสาธารณะและไม่มีเงื่อนไขในการเข้าถึงข้อมูล
G1	Creative Commons Attribution	อนุญาตให้ผู้อื่นสามารถนำผลงานไปใช้ ทำซ้ำ แจกจ่าย หรือดัดแปลงงานนั้นได้ แต่ต้องให้เครดิตที่มาของเจ้าของผลงาน	ควรใช้กับหมวดหมู่ข้อมูลสาธารณะ
G2	Creative Commons Attribution-NonCommercial	อนุญาตให้ผู้อื่นสามารถนำผลงานไปใช้ ทำซ้ำ แจกจ่าย หรือดัดแปลงงานนั้นได้ แต่ต้องให้เครดิตที่มาของเจ้าของผลงาน และต้องไม่ใช่เพื่อการค้า	ควรใช้กับหมวดหมู่ข้อมูลสาธารณะ และมีระดับขั้นข้อมูลใช้ภายในเป็นต้นไป
G3.1	Creative Commons Attribution-ShareAlike	อนุญาตให้ผู้อื่นสามารถนำผลงานไปใช้ ทำซ้ำ แจกจ่าย หรือดัดแปลงงานนั้นได้ แต่ต้องให้เครดิตที่มาของเจ้าของผลงาน และจะต้องกำกับด้วยสัญญาอนุญาตเงื่อนไขเดียวกันกับต้นฉบับ	ควรใช้กับหมวดหมู่ข้อมูลสาธารณะ และมีระดับขั้นข้อมูลใช้ภายในเป็นต้นไป
G3.2	Creative Commons Attribution-NonCommercialShareAlike	อนุญาตให้ผู้อื่นสามารถนำผลงานไปใช้ ทำซ้ำ แจกจ่าย หรือดัดแปลงงานนั้นได้ แต่ต้องไม่ใช่เพื่อการค้าและจะต้องกำกับด้วยสัญญาอนุญาตเงื่อนไขเดียวกันกับต้นฉบับ	
G4.1	Creative Commons Attribution-NoDerivs	อนุญาตให้ผู้อื่นสามารถนำผลงานไปทำซ้ำ แจกจ่าย โดยห้ามแก้ไขหรือดัดแปลงผลงานนั้น และต้องให้เครดิต ที่มาของเจ้าของผลงาน	ควรใช้กับชุดข้อมูลที่มีเงื่อนไขในการเข้าถึงข้อมูล และมีระดับขั้นข้อมูลใช้ภายในเป็นต้นไป
G4.2	Creative Commons Attribution-NonCommercialNoDerivs	อนุญาตให้ผู้อื่นสามารถนำผลงานไปทำซ้ำ แจกจ่าย โดยห้ามแก้ไขหรือดัดแปลงผลงานนั้น แต่ต้องให้เครดิตที่มาของเจ้าของผลงานและต้องไม่ใช่เพื่อการค้า	
G5	Others License	สัญญาอนุญาตให้ใช้ข้อมูลอื่น ๆ โดยเงื่อนไขเป็นไปตามที่เจ้าของข้อมูลกำหนดและผู้ใช้ข้อมูลสามารถขอใช้ข้อมูลได้เป็นรายกรณี	ควรใช้กับชุดข้อมูลที่มีเงื่อนไขในการเข้าถึงข้อมูล และมีระดับขั้นข้อมูลเป็นขั้นลับ

บรรณานุกรม

- “ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ พ.ศ. 2563” (2563, 31 มีนาคม). ราชกิจจานุเบกษา. เล่ม 137 ตอนพิเศษ 74 ง. หน้า 47-48.
- “ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง มาตรฐานรัฐบาลดิจิทัลว่าด้วยกรอบธรรมาภิบาลข้อมูลภาครัฐ ฉบับปรับปรุง: แนวปฏิบัติ พ.ศ. 2566” (2566, 24 กรกฎาคม). ราชกิจจานุเบกษา. เล่ม 140 ตอนพิเศษ 207 ง. หน้า 28-31.
- “พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550” (2550, 18 มิถุนายน). ราชกิจจานุเบกษา. เล่ม 124 ตอนที่ 27 ก. หน้า 4-13.
- “พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562” (2562, 27 พฤษภาคม). ราชกิจจานุเบกษา. เล่ม 136 ตอนที่ 69 ก. หน้า 52-95.
- “พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562” (2562, 27 พฤษภาคม). ราชกิจจานุเบกษา. เล่ม 136 ตอนที่ 69 ก. หน้า 20-51.
- “พระราชบัญญัติระบบการชำระเงิน พ.ศ. 2560” (2560, 18 ตุลาคม). ราชกิจจานุเบกษา. เล่ม 134 ตอนที่ 110 ก. หน้า 1-16.
- “พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2562” (2562, 22 พฤษภาคม). ราชกิจจานุเบกษา. เล่ม 136 ตอนที่ 67 ก. หน้า 203-207.
- “พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540” (2540, 2 กันยายน). ราชกิจจานุเบกษา. เล่ม 114 ตอนที่ 105 ก. หน้า 1-16.
- สำนักงานนโยบายและแผนพลังงาน. (2564). แผนพลังงานแห่งชาติ พ.ศ. 2608-2564. กรุงเทพฯ: สำนักงานนโยบายและแผนพลังงาน.
- Askham, N. (2016). Squaring the circle: Using a data governance framework to support data quality. Experian Information Solutions, Inc.
- Askham, N., Cook, D., Doyle, M., Fereday, H., Gibson, M., Landbeck, U., Lee, R., Maynard, C., Palmer, G., & Schwarzenbach, J. (2013). THE SIX PRIMARY DIMENSIONS FOR DATA QUALITY ASSESSMENT: Defining Data Quality Dimensions. em360tech. [Online] 2013.
- Australian Institute of Health and Welfare. (2014). Data Governance Framework. Retrieved from <https://www.aihw.gov.au/getmedia/0d59ee71-9abe-4806-8e87-ce9de81974d3/AIHW-data-governance-framework.pdf.aspx>
- Cupola, P., Earley, S., & Henderson, D. (2014). DAMA-DMBOK2 Framework.
- Henderson, D., Earley, S., Sebastian-Coleman, L., Sykora, E., & Smith, E. (2017). DAMA guide to the data management body of knowledge (2nd ed.). Technics Publications.

บรรณานุกรม(ต่อ)

- International Organization for Standardization. (2013). ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements. Geneva: ISO.
- Intra-governmental Group on Geographic Information (IGGI). (2005). The principles of good data management. The Office of the Deputy Prime Minister.
- Kim, H. Y., & Cho, J. S. (2017, June). Data Governance Framework for Big Data Implementation with a Case of Korea. In Big Data (BigData Congress), 2017 IEEE International Congress on (pp. 384-391). IEEE.
- Malinowski, E., & Zimányi, E. (2009). Advanced Data Warehouse Design. Springer Berlin Heidelberg.
- Thomas, G. (2009). How to use the DGI data governance framework to configure your program. Data Governance Institute, 17.



กรมพัฒนาพลังงานทดแทน และอนุรักษ์พลังงาน กระทรวงพลังงาน

