

รรมาภิบาลข้อมูลภาครัฐ

Data Governance for Government

เวอร์ชัน 1.0

(มิถุนายน 2561)

ประธานกรรมการ

รองศาสตราจารย์วรากรณ์ สามโกเศศ

รองประธานกรรมการ

นายวรากรณ์ อาวุธ

คณะกรรมการ

นายสมเกียรติ ตั้งกิจวานิชย์

นางสาวกษิธิธ ภูมราดิ

ผู้ช่วยศาสตราจารย์ไพฑูริย์ ธรรมบุษดี

ผู้อำนวยการสำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

ผู้อำนวยการสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ

ผู้อำนวยการสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ผู้จัดการใหญ่บริษัท ข้อมูลเครดิตแห่งชาติ จำกัด

ผู้อำนวยการศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

ผู้อำนวยการสำนักบริหารการทะเบียน กรมการปกครอง

ผู้แทนสำนักงานสภาพัฒนาการเศรษฐกิจ

ผู้แทนสำนักงานคณะกรรมการกฤษฎีกา

เลขานุการคณะกรรมการ

นายวิบูลย์ ภัทรพิบูล (รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล)

บรรณาธิการบริหาร

นายสุพจน์ เขียวรุฒ

บรรณาธิการ

นายวิบูลย์ ภัทรพิบูล

นางสาวอุรชฎา เกตุพรหม

จัดทำ

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

ออกแบบและจัดพิมพ์

บริษัท ไอเดีย พรินต์ (2013) จำกัด

พิมพ์ครั้งที่ 1

ตุลาคม 2563

จำนวน

1,000 เล่ม

ISBN

978-616-8001-15-8



DGA

Digital Government Development Agency

ธรรมาภิบาลข้อมูลภาครัฐ

Data Governance for Government

เวอร์ชัน 1.0

(มิถุนายน 2561)

คณะกรรมการศึกษากระบวนการธรรมาภิบาล

และการเปิดเผยข้อมูลดิจิทัล เพื่อการบริหารราชแผ่นดิน

ประธานกรรมการ

รองศาสตราจารย์วรากรณ์ สามโกเศศ

รองประธานกรรมการ

นายวรรณวิทย์ อาชุนทร

คณะกรรมการ

นายสมเกียรติ ตั้งกิจวานิชย์

นางสาวกษิธิธ ภูกราตย์

ผู้ช่วยศาสตราจารย์ไพฑูริรัตน์ ธรรมบุษดี

ผู้อำนวยการสำนักงานคณะกรรมการรัฐธรรมนูญทางอิเล็กทรอนิกส์

ผู้อำนวยการสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ

ผู้อำนวยการสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ผู้จัดการใหญ่บริษัท ข้อมูลเครดิตแห่งชาติ จำกัด

ผู้อำนวยการศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

ผู้อำนวยการสำนักบริหารการทะเบียน กรมการปกครอง

ผู้แทนสำนักงานสภาความมั่นคงแห่งชาติ

ผู้แทนสำนักงานคณะกรรมการกฤษฎีกา

เลขาธิการคณะกรรมการ

นายวิบูลย์ ภัทรพิบูล (รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล)

สารบัญ

บทสรุปผู้บริหาร

1

(EXECUTIVE SUMMARY)

บทที่ 1

บทนำ (INTRODUCTION)

3

1.1 ความเป็นมา

5

1.2 วัตถุประสงค์

6

1.3 หน่วยงานภาครัฐที่นำไปใช้

7

1.4 ขอบเขตของเนื้อหาภายในธรรมาภิบาลข้อมูลภาครัฐ

8

บทที่ 2

แนวคิดธรรมาภิบาลข้อมูลภาครัฐ

9

(DATA GOVERNANCE FOR GOVERNMENT CONCEPT)

2.1 นิยามของธรรมาภิบาลข้อมูลภาครัฐ

11

2.2 ข้อมูล

14

2.2.1 ประเภทข้อมูล

15

2.2.2 ชุดข้อมูล

16

2.2.3 ฐานข้อมูล

17

2.3 การบริหารจัดการข้อมูล

18

2.3.1 ระบบบริหารและกระบวนการจัดการข้อมูล

20

หรือวงจรชีวิตของข้อมูล

2.3.2 องค์ประกอบในการบริหารจัดการข้อมูล

21

2.4 ความสัมพันธ์ระหว่างธรรมาภิบาลข้อมูลกับการบริหารจัดการข้อมูล

49

บทที่ 3

กรอบธรรมาภิบาลข้อมูลภาครัฐ	51
(DATA GOVERNANCE FRAMEWORK FOR GOVERNMENT)	
3.1 โครงสร้างธรรมาภิบาลข้อมูลภาครัฐ	53
3.1.1 โครงสร้างของบุคลากรที่รับผิดชอบในธรรมาภิบาลข้อมูลภาครัฐ	54
3.1.2 บทบาทและความรับผิดชอบ	59
3.2 กระบวนการธรรมาภิบาลข้อมูลภาครัฐ	61
3.2.1 กระบวนการธรรมาภิบาลข้อมูลภาครัฐ	63
3.2.2 แนวทางการจัดการกระบวนการธรรมาภิบาลข้อมูลภาครัฐ	65
3.3 สภาพแวดล้อมของธรรมาภิบาลข้อมูล	70
3.3.1 กฎหมาย ระเบียบ ข้อบังคับ แผนนโยบาย และแนวปฏิบัติที่เกี่ยวข้องกับธรรมาภิบาลข้อมูลภาครัฐ	71
3.3.2 หลักการของสภาพแวดล้อมและวัฒนธรรมของหน่วยงานที่เอื้อต่อการมีธรรมาภิบาลข้อมูลภาครัฐ	79
3.4 การนิยามข้อมูล	80
3.4.1 หมวดหมู่ของข้อมูล	81
3.4.2 คำอธิบายชุดข้อมูลดิจิทัล หรือเมทาดาตา	85
3.4.3 บัญชีข้อมูล	86
3.4.4 คลังเมทาดาตา หรือพจนานุกรมข้อมูล	86
3.5 กฎเกณฑ์ข้อมูล	87
3.5.1 นโยบายข้อมูล	88
3.5.2 มาตรฐานข้อมูล	94
3.6 การวัดการดำเนินการและความสำเร็จของธรรมาภิบาลข้อมูลภาครัฐ	95
3.6.1 การประเมินความพร้อมของธรรมาภิบาลข้อมูลภาครัฐ	96
3.6.2 การประเมินคุณภาพของข้อมูล	100
3.6.3 การประเมินความมั่นคงปลอดภัยของข้อมูล	105

ภาคผนวก

111

ภาคผนวก ก

แบบฟอร์มการจัดทำคำอธิบายชุดข้อมูลดิจิทัล หรือเมทาดาตา 113

ภาคผนวก ข

บทบาท และความรับผิดชอบของผู้มีส่วนได้เสียกับข้อมูล 116

ภาคผนวก ค

แนวนโยบายและแนวปฏิบัติในการเชื่อมโยงและแลกเปลี่ยนข้อมูล
ระหว่างหน่วยงาน 120

ภาคผนวก ง

แนวนโยบายและแนวปฏิบัติในการเปิดเผยข้อมูล และการขอใช้ข้อมูล 125

ภาคผนวก จ

แนวนโยบายและแนวปฏิบัติอื่น ๆ 130

ภาคผนวก ฉ

แนวคิดธรรมาภิบาลข้อมูลจากต่างประเทศ 133

แนวคิดของ Data Governance Institute 133

แนวคิดของ Data Management Association International 135

ภาคผนวก ช

กรณีศึกษาธรรมาภิบาลข้อมูลจากต่างประเทศ 138

กรณีศึกษาของประเทศออสเตรเลีย 138

กรณีศึกษาของประเทศเกาหลีใต้ 143

กรณีศึกษาของสภราชอาณาจักร 145

บรรณานุกรม

147



สารบัญตาราง

ตารางที่ 1	ตัวอย่างชุดข้อมูลพนักงาน	17
ตารางที่ 2	ตัวอย่างความสัมพันธ์ระหว่างข้อมูลกับแอปพลิเคชัน สำหรับงานบริหารจัดการพัสดุ	25
ตารางที่ 3	สรุปการบริหารจัดการสถาปัตยกรรมข้อมูล	26
ตารางที่ 4	สรุปการบริหารจัดการการจำลองและการออกแบบข้อมูล	31
ตารางที่ 5	สรุปการบริหารจัดการการจัดเก็บและการดำเนินการกับข้อมูล	32
ตารางที่ 6	สรุปการบริหารจัดการการบูรณาการ และความสามารถในการทำงานร่วมกัน	34
ตารางที่ 7	สรุปการบริหารจัดการเอกสารและเนื้อหา	35
ตารางที่ 8	สรุปการบริหารจัดการข้อมูลหลักและข้อมูลอ้างอิง	36
ตารางที่ 9	สรุปการบริหารจัดการคลังข้อมูล ดาตาเลค ระบบรายงานอัจฉริยะ และดาตาอานาไลติกส์	39
ตารางที่ 10	ตัวอย่างเมทาดาตาของข้อมูลครุภัณฑ์	41
ตารางที่ 11	สรุปการบริหารจัดการคำอธิบายชุดข้อมูลดิจิทัล หรือ เมทาดาตา	44
ตารางที่ 12	สรุปการบริหารจัดการความมั่นคงปลอดภัย และการรักษาความเป็นส่วนตัวของข้อมูล	46
ตารางที่ 13	สรุปการบริหารจัดการคุณภาพของข้อมูล	48
ตารางที่ 14	ความสัมพันธ์ระหว่างกระบวนการ ส่วนนำเข้า ส่วนนำออก และผู้มีส่วนได้เสียกับข้อมูล	65
ตารางที่ 15	ความสัมพันธ์ระหว่างกระบวนการ/กิจกรรม และผู้มีส่วนได้เสียกับข้อมูล	69
ตารางที่ 16	ระดับความพร้อมของธรรมาภิบาลข้อมูลภาครัฐ	98
ตารางที่ 17	ตัวอย่างการวัดคุณภาพข้อมูลที่เป็นโครงสร้างสำหรับ แต่ละชุดข้อมูล	102
ตารางที่ 18	ตัวอย่างการวัดความมั่นคงปลอดภัยของข้อมูล	106
ตารางที่ 19	แบบฟอร์มการจัดทำคำอธิบายชุดข้อมูลดิจิทัล หรือเมทาดาตา	113
ตารางที่ 20	บทบาท และความรับผิดชอบของผู้มีส่วนได้เสียกับข้อมูล	116

สารบัญรูปภาพ

รูปที่ 1	ประเภทของข้อมูล	15
รูปที่ 2	ความสัมพันธ์ระหว่างฐานข้อมูลกับชุดข้อมูล	17
รูปที่ 3	ระบบบริหารและกระบวนการจัดการข้อมูล หรือ วงจรชีวิตของข้อมูล และองค์ประกอบในการบริหาร จัดการข้อมูล	19
รูปที่ 4	ตัวอย่างความสัมพันธ์ระหว่างกลุ่มข้อมูลกับ กลุ่มกระบวนการปฏิบัติงาน	23
รูปที่ 5	ตัวอย่างแบบจำลองข้อมูลเชิงความคิด สำหรับงานบริหารจัดการพัสดุ	28
รูปที่ 6	ตัวอย่างแบบจำลองข้อมูลเชิงตรรกะ สำหรับงานบริหารจัดการพัสดุ	29
รูปที่ 7	ตัวอย่างแบบจำลองข้อมูลเชิงกายภาพ สำหรับงานบริหารจัดการพัสดุ	30
รูปที่ 8	ตัวอย่างความสัมพันธ์ระหว่างคลังข้อมูล ดาตาเลค ระบบรายงานอัจฉริยะ และดาตาอานาไลติกส์ สำหรับงานบริหารจัดการพัสดุ	38
รูปที่ 9	กรอบธรรมาภิบาลข้อมูลภาครัฐในระดับหน่วยงาน	53
รูปที่ 10	ตัวอย่างโครงสร้างธรรมาภิบาลข้อมูลภาครัฐภายในหน่วยงาน	55
รูปที่ 11	กระบวนการธรรมาภิบาลข้อมูลภาครัฐ	63
รูปที่ 12	ตัวอย่างแผนภาพการดำเนินการธรรมาภิบาลข้อมูลภาครัฐ	68
รูปที่ 13	กฎหมาย ระเบียบ ข้อบังคับ แนวนโยบาย และแนวปฏิบัติที่เกี่ยวข้องกับธรรมาภิบาลข้อมูลภาครัฐ	72
รูปที่ 14	หมวดหมู่ของข้อมูล	81
รูปที่ 15	ความสัมพันธ์ระหว่างบัญชีข้อมูล เมทาดาตา คลังเมทาดาตา พจนานุกรมข้อมูล และชุดข้อมูล	87
รูปที่ 16	นโยบายข้อมูล	89
รูปที่ 17	องค์ประกอบในการประเมินคุณภาพข้อมูล	100
รูปที่ 18	ความสัมพันธ์ระหว่างธรรมาภิบาลข้อมูลภาครัฐ และการแลกเปลี่ยนข้อมูล	121

บทสรุปผู้บริหาร

(EXECUTIVE SUMMARY)

ข้อมูลจัดเป็นทรัพย์สินที่สำคัญในการดำเนินงานของหน่วยงานภาครัฐ จึงได้ให้ความสำคัญกับการนำข้อมูลมาใช้สนับสนุนการขับเคลื่อนนโยบาย เศรษฐกิจและสังคมดิจิทัลให้กับทุกภาคส่วน แต่ในปัจจุบันหน่วยงานภาครัฐ ยังประสบกับปัญหาและอุปสรรคในการดำเนินงานในด้านต่าง ๆ ที่เกี่ยวข้องกับ ข้อมูล ซึ่งเป็นประเด็นปัญหาเชิงนโยบายและปฏิบัติ ทั้งในเรื่องความซ้ำซ้อน ของข้อมูล ความมั่นคงปลอดภัยของข้อมูล (เช่น การรักษาความลับ การเข้าถึง ข้อมูล การรักษาความเป็นส่วนบุคคล) คุณภาพของข้อมูล (เช่น ความถูกต้อง ความครบถ้วน ความเป็นปัจจุบัน) การเปิดเผยข้อมูล (เช่น หน่วยงานเจ้าของ ข้อมูลไม่อนุญาตให้เข้าถึงข้อมูล กระบวนการขอใช้ข้อมูลซับซ้อนและใช้เวลานาน ข้อมูลไม่อยู่ในรูปแบบที่ใช้งานต่อได้ง่าย) และยังไม่มีการนำข้อมูลไปใช้ประโยชน์ อย่างเป็นรูปธรรม ประเด็นปัญหาและอุปสรรคเหล่านี้อาจเป็นผลมาจากการ บริหารจัดการข้อมูลที่ไม่ครอบคลุมและไม่ชัดเจนของหน่วยงาน ดังนั้น จึงจำเป็นต้องให้หน่วยงานมีมาตรการและแนวปฏิบัติในธรรมาภิบาลข้อมูล และบริหารจัดการข้อมูลที่มีประสิทธิภาพและประสิทธิผล

จากการศึกษาเกี่ยวกับธรรมาภิบาลข้อมูลและการบริหารจัดการข้อมูล (Data Governance) พบว่า ธรรมาภิบาลข้อมูลภาครัฐถือเป็นหัวใจสำคัญ ในการบริหารจัดการข้อมูล (Data Management) กล่าวคือ ธรรมาภิบาลข้อมูลภาครัฐ เป็นกลไกในการกำหนดทิศทาง ควบคุม และทวนสอบการบริหารจัดการข้อมูล เพื่อให้หน่วยงานได้ดำเนินการบริหารจัดการข้อมูลตามนโยบาย กฎ ระเบียบ หรือข้อบังคับที่ได้กำหนดไว้ ธรรมาภิบาลข้อมูลภาครัฐที่ดีก่อให้เกิดการบริหาร จัดการข้อมูลที่ดี ส่งผลให้ข้อมูลมีความมั่นคงปลอดภัย มีคุณภาพ มีคุณค่า ทางเศรษฐกิจและสังคม และมีความคุ้มค่าต่อการดำเนินงาน

เพื่อให้การได้มาและการนำไปใช้ข้อมูลของหน่วยงานภาครัฐ ถูกต้องครบถ้วน เป็นปัจจุบัน มั่นคงปลอดภัย รักษาความเป็นส่วนตัวบุคคล และสามารถเชื่อมโยงกันได้ อย่างมีประสิทธิภาพและมั่นคงปลอดภัยได้จริง ธรรมาภิบาลข้อมูลภาครัฐ (Data Governance for Government) ในเอกสารฉบับนี้จึงถูกจัดทำขึ้น เพื่อกำหนดสิทธิ หน้าที่ และความรับผิดชอบของผู้มีส่วนได้เสียในการบริหารจัดการข้อมูล โดยประกอบด้วย สภาพแวดล้อมของธรรมาภิบาลข้อมูลภาครัฐ กฎเกณฑ์หรือนโยบายที่เกี่ยวข้องกับการดำเนินงานกับข้อมูล บทบาทและความรับผิดชอบในธรรมาภิบาลข้อมูลภาครัฐ กระบวนการธรรมาภิบาลข้อมูล ภาครัฐ และการวัดการดำเนินการและความสำเร็จของธรรมาภิบาล กล่าวคือ บุคคลที่ได้รับบทบาทในธรรมาภิบาลจะมีหน้าที่ในการกำหนดขอบเขต กฎเกณฑ์ และนโยบายข้อมูลที่ใช้ในกระบวนการธรรมาภิบาล เพื่อควบคุมและตรวจสอบ การดำเนินงานที่เกี่ยวข้องกับข้อมูล ตั้งแต่การสร้าง การจัดเก็บ การประมวลผล การใช้ การเผยแพร่ จนถึงการทำลาย โดยกฎเกณฑ์และนโยบายข้อมูล ต้องสอดคล้องกับสภาพแวดล้อมและวัฒนธรรมองค์กรของแต่ละหน่วยงาน การวัดผลการดำเนินการช่วยให้เห็นระดับการดำเนินการของธรรมาภิบาลข้อมูลภาครัฐ ซึ่งส่งผลต่อความสำเร็จของการดำเนินการหรือคุณภาพของข้อมูล

ธรรมาภิบาลข้อมูลภาครัฐจะเป็นแนวทางให้หน่วยงานภาครัฐ ทั้งส่วน ราชการ รัฐวิสาหกิจ องค์กรการมหาชน และหน่วยงานของรัฐรูปแบบใหม่ นำไปปรับใช้ให้เข้ากับลักษณะเฉพาะของแต่ละหน่วยงานเพื่อให้สามารถ ปรับตัวตามบริบทที่เปลี่ยนแปลงอย่างต่อเนื่อง

บทที่ 1 บทนำ

(INTRODUCTION)



1.1 ความเป็นมา

ข้อมูลจัดเป็นหนึ่งในทรัพย์สินที่สำคัญ และเป็นกลไกในการขับเคลื่อนการดำเนินงานของหน่วยงานเพื่อนำไปสู่เป้าหมายที่ได้กำหนดไว้อย่างไรก็ตามสถานการณ์ด้านการบริหารจัดการข้อมูลและการใช้ประโยชน์จากข้อมูลของ

หน่วยงานภาครัฐในปัจจุบันยังมีอุปสรรคในด้านต่าง ๆ ทั้งในด้านการจัดเก็บข้อมูล (เช่น ข้อมูลเดียวกันแต่จัดเก็บกระจายไปในหลายระบบ หลายส่วนงาน หลายรูปแบบ) ด้านการเปิดเผยข้อมูล (เช่น หน่วยงานเจ้าของข้อมูลไม่อนุญาตให้เข้าถึงข้อมูล กระบวนการขอใช้ข้อมูลซับซ้อนและใช้เวลานาน ข้อมูลไม่อยู่ในรูปแบบที่ใช้งานต่อได้ง่าย) ด้านความมั่นคงปลอดภัยของข้อมูล (เช่น การรักษาความลับ การเข้าถึงความเป็นส่วนตัว) และด้านคุณภาพของข้อมูล (เช่น ความถูกต้อง ความสมบูรณ์ ความต้องกัน ความเป็นปัจจุบัน ตรงตามความต้องการใช้งาน ความพร้อมใช้)

สาเหตุของปัญหานั้นมาจากการขาดการวางแผนในการบริหารจัดการข้อมูลทั้งระบบบริหารและกระบวนการจัดการข้อมูลหรือวงจรชีวิตของข้อมูล (สร้าง จัดเก็บ ประมวลผล นำไปใช้ เผยแพร่ และทำลาย) ขาดการบูรณาการข้อมูลอุปสรรคทางด้านกฎระเบียบ รวมถึงการบริหารจัดการที่ไม่ครอบคลุมประเภทของข้อมูล นั่นคือ ข้อมูลที่มีโครงสร้าง (เช่น ฐานข้อมูล) กึ่งโครงสร้าง (เช่น Extensible Markup Language - XML) ไม่มีโครงสร้าง (เช่น เสียง ภาพ ภาพเคลื่อนไหว)

ดังนั้นเพื่อให้การนำข้อมูลไปใช้ก่อให้เกิดประโยชน์อย่างเต็มที่ และมีประสิทธิภาพ จะต้องอาศัย ธรรมาภิบาลข้อมูลภาครัฐ (Data Governance for Government) ที่เอื้อให้หน่วยงานภาครัฐต่าง ๆ สามารถนำไปใช้ธรรมาภิบาล และบริหารจัดการข้อมูลของหน่วยงานภาครัฐทุกชั้นตอนอย่างเป็นระบบและมีความชัดเจนมากยิ่งขึ้น

1.2 วัตถุประสงค์

การจัดทำธรรมาภิบาลข้อมูลภาครัฐ เพื่อให้หน่วยงานภาครัฐสามารถนำไปผลักดัน และดำเนินการในธรรมาภิบาลข้อมูลภาครัฐ รวมถึงติดตามการบริหารจัดการข้อมูลให้มีความโปร่งใส ตรวจสอบได้ ส่งผลต่อคุณภาพความมั่นคงปลอดภัย และบูรณาการข้อมูลได้อย่างครบถ้วน ถูกต้อง และข้อมูลเป็นปัจจุบัน

1.3 หน่วยงานภาครัฐที่นำไปใช้

ธรรมาภิบาลข้อมูลภาครัฐนี้ครอบคลุมถึงธรรมาภิบาลข้อมูลและการบริหารจัดการข้อมูลภายในหน่วยงานภาครัฐทั้ง 4 ประเภท คือ ส่วนราชการ รัฐวิสาหกิจ องค์การมหาชน และหน่วยงานของรัฐรูปแบบใหม่ ดังนี้

1) ส่วนราชการ หมายถึง หน่วยงานที่รับผิดชอบการให้บริการสาธารณะทางปกครอง ซึ่งเป็นภารกิจหลักของรัฐให้บริการเป็นการทั่วไปและไม่มุ่งกำไร และมีความสัมพันธ์กับรัฐ

2) รัฐวิสาหกิจ หมายถึง หน่วยงานที่รับผิดชอบบริการสาธารณะทางอุตสาหกรรมและพาณิชย์กรรม มีวัตถุประสงค์เพื่อการแสวงหารายได้ ต้องสามารถเลี้ยงตัวเองจากการดำเนินงานเชิงพาณิชย์ แต่สามารถรับเงินงบประมาณสนับสนุนเป็นครั้งคราวหรือบางส่วนในบางกรณี

3) องค์การมหาชน หมายถึง หน่วยงานที่รับผิดชอบบริการสาธารณะทางสังคมและวัฒนธรรม ไม่มีวัตถุประสงค์ในการแสวงหากำไร เป็นนิติบุคคล และมีความสัมพันธ์กับรัฐ ซึ่งประกอบด้วย รัฐจัดตั้ง ได้รับเงินอุดหนุนจากรัฐ หรือสามารถเลี้ยงตัวเองได้ และรัฐมีอำนาจบริหารจัดการ

4) หน่วยงานของรัฐรูปแบบใหม่ หมายถึง

- องค์การของรัฐที่เป็นอิสระ (Independent Administrative Organization) ซึ่งเป็นหน่วยงานรูปแบบใหม่ที่จัดตั้งขึ้นเพื่อทำหน้าที่ในการควบคุมกำกับดูแลกิจกรรมของรัฐ ตามนโยบายสำคัญที่ต้องการความเป็นกลางอย่างเคร่งครัด

- กองทุนที่เป็นนิติบุคคล ซึ่งเป็นเครื่องมือทางเศรษฐกิจของรัฐ หมายถึง นิติบุคคลที่จัดตั้งขึ้นโดยตราเป็นพระราชบัญญัติ เนื่องจากต้องการอำนาจรัฐในการบังคับฝ่ายเดียวต่อภาคเอกชน หรือประชาชน ในการสมทบเงินเข้ากองทุน

ธรรมาภิบาลข้อมูลภาครัฐในพระราชบัญญัติการบริหารงาน และการให้บริการภาครัฐผ่านระบบดิจิทัล ได้กำหนดหน่วยงานของรัฐ หมายความว่า ราชการส่วนกลาง ราชการส่วนภูมิภาค ราชการส่วนท้องถิ่น รัฐวิสาหกิจ องค์การมหาชน รัฐสภา ศาล (ครอบคลุมเพียงหน่วยงานของศาล ในส่วนที่ไม่เกี่ยวกับการพิจารณาอาชญากรรม) องค์การอิสระตามรัฐธรรมนูญ องค์การอัยการ สถาบันอุดมศึกษาของรัฐ และหน่วยงานอิสระของรัฐ

1.4 ขอบเขตของเนื้อหาภายในธรรมาภิบาลข้อมูลภาครัฐ

ขอบเขตของธรรมาภิบาลข้อมูลภาครัฐในเอกสารฉบับนี้ ประกอบด้วย บทที่ 2 อธิบายถึงแนวคิดธรรมาภิบาลข้อมูลภาครัฐ ประกอบด้วย นิยามของธรรมาภิบาลข้อมูลภาครัฐ ความหมายและประเภทข้อมูล การบริหารจัดการข้อมูล ความสัมพันธ์ระหว่างธรรมาภิบาลข้อมูลภาครัฐกับการบริหารจัดการข้อมูล บทที่ 3 กล่าวถึงกรอบธรรมาภิบาลข้อมูลภาครัฐ ประกอบด้วย โครงสร้างของธรรมาภิบาลข้อมูลภาครัฐ กระบวนการธรรมาภิบาลข้อมูลภาครัฐ สภาพแวดล้อมของธรรมาภิบาลข้อมูลภาครัฐ การนิยามข้อมูล กฎเกณฑ์ข้อมูล และการวัดการดำเนินการ และความสำเร็จของธรรมาภิบาลข้อมูลภาครัฐ

บทที่ 2

แนวคิดธรรมาภิบาล
ข้อมูลภาครัฐ
(DATA GOVERNANCE
FOR GOVERNMENT CONCEPT)



2.1 นิยามของธรรมาภิบาลข้อมูลภาครัฐ

(Data Governance for Government Definition)

ธรรมาภิบาลข้อมูลภาครัฐ (Data Governance for Government) ได้มีผู้เชี่ยวชาญจากหน่วยงานต่าง ๆ ให้คำนิยามไว้ ดังนี้

“กิจกรรมที่ประกอบด้วยการกำหนดอำนาจการควบคุมและการตัดสินใจในการบริหารจัดการข้อมูล โดยที่ข้อมูลถูกจัดให้เป็นหนึ่งในทรัพย์สินของหน่วยงาน”

(Askham, N., 2016)

“ระบบที่กำหนดถึงอำนาจการตัดสินใจและหน้าที่ความรับผิดชอบต่อกระบวนการที่เกี่ยวข้องกับข้อมูล โดยมีแบบแผนที่ชัดเจนและได้รับการยอมรับ ซึ่งแบบแผนดังกล่าวต้องสามารถอธิบายได้ว่า ใครมีบทบาทในการทำอะไรกับข้อมูลชุดไหน เมื่อไร ใช้หลักการและวิธีการอย่างไรในการใช้ข้อมูล”

(Thomas, 2009)

“การกำหนดสิทธิและการควบคุม
(การวางแผน การตรวจสอบ และการบังคับ)
ในการบริหารจัดการข้อมูล”

(Henderson et al., 2017)

“การจัดการข้อมูล จากมุมมองที่เกี่ยวข้องกับข้อมูล
ทำให้หน่วยงานตระหนักถึงการจัดทำมาตรฐานข้อมูลที่เป็นระบบ
และการบูรณาการข้อมูล ทั้งข้อมูลที่อยู่ในระบบ
ข้อมูลที่สัมพันธ์กับการดำเนินงานของหน่วยงาน นโยบาย
และกระบวนการปฏิบัติงานต่าง ๆ”

(Kim, H. Y., & Cho, J. S., 2017)

จากนิยามต่าง ๆ ข้างต้น จึงได้ข้อสรุปว่า ธรรมาภิบาลข้อมูลภาครัฐ (Data Governance for Government) คือ “การกำหนดสิทธิในการตัดสินใจ และความรับผิดชอบ ในการส่งเสริมให้เกิดกระบวนการจัดทำ การใช้งาน และการบริหารจัดการข้อมูล รวมถึงกระบวนการที่กำหนดบทบาท นโยบาย และมาตรฐาน ที่ช่วยสนับสนุนให้การดำเนินงานเกี่ยวกับข้อมูลมีประสิทธิภาพ มากยิ่งขึ้น ซึ่งส่งผลให้หน่วยงานสามารถบรรลุเป้าหมายได้”

ในมุมมองของภาครัฐ ธรรมาภิบาลข้อมูลภาครัฐ (Data Governance for Government) หมายถึง “การกำหนดสิทธิ หน้าที่ และความรับผิดชอบของ ผู้มีส่วนได้เสียในการบริหารจัดการข้อมูลทุกขั้นตอน เพื่อให้การได้มา และการนำไปใช้ข้อมูลของหน่วยงานภาครัฐถูกต้อง ครบถ้วน เป็นปัจจุบัน รักษาความเป็นส่วนบุคคล และสามารถเชื่อมโยงกันได้อย่างมีประสิทธิภาพและ มั่นคงปลอดภัย โดยใช้ข้อมูลเป็นหลักในการขับเคลื่อนประเทศ เช่น การใช้ข้อมูลในการวิเคราะห์การตัดสินใจเชิงนโยบายและการบริหารราชการ แผ่นดิน การเพิ่มประสิทธิภาพในการบริการประชาชน การเสริมสร้างและผลักดันธุรกิจที่เกิดจากการใช้นวัตกรรมข้อมูล” ทั้งนี้ Intra-governmental Group on Geographic Information (IGGI, 2005) ให้องค์ประกอบหลักของ ธรรมาภิบาลข้อมูลภาครัฐที่ดี ประกอบไปด้วย

- 1) มีความมั่นคงปลอดภัยและรักษาความเป็นส่วนตัวบุคคล โดยมีมาตรการในการรักษาความมั่นคงปลอดภัยและความเป็นส่วนตัวบุคคล ซึ่งช่วยป้องกันความเสียหายที่จะเกิดขึ้นกับข้อมูลและการละเมิดสิทธิส่วนบุคคล
- 2) มีมาตรการควบคุมและจัดการระบบบริหารและกระบวนการจัดการข้อมูลหรือวงจรชีวิตของข้อมูล ซึ่งประกอบด้วย การประเมินธุรกิจ การกำหนดประเภทและแนวทางการแบ่งประเภทของชุดข้อมูล มีการตรวจสอบอย่างต่อเนื่อง ทั้งการเก็บข้อมูลและการทำลายข้อมูล
- 3) มีนโยบายการใช้ข้อมูลที่ชัดเจน โดยกำหนดนโยบายและกฎเกณฑ์ของข้อมูลสำหรับธรรมาภิบาลข้อมูลและการบริหารจัดการข้อมูล
- 4) มีการกำหนดบทบาทหน้าที่ของเจ้าของข้อมูล โดยกำหนดวิธีการที่ผู้ดูแลข้อมูลหรือเจ้าของข้อมูลสามารถจัดการ เปลี่ยนแปลง หรือส่งผ่านข้อมูลให้ชัดเจน เพื่อไม่ให้เกิดปัญหาในกรณีที่ชุดข้อมูลหรือฐานข้อมูลบางแหล่งอาจจะมีผู้ดูแล ผู้ใช้งาน หรือเจ้าของข้อมูลหลายคนหรือหลายหน่วยงาน
- 5) ข้อมูลมีเมทาดาตา โดยเมทาดาตาจะช่วยให้ผู้ใช้งานเข้าใจว่าข้อมูลชุดนี้คือข้อมูลที่เกี่ยวข้องกับอะไร สามารถนำไปใช้งานอย่างไร และมีข้อจำกัดอะไร โดยมีมาตรฐานของเมทาดาตาที่เหมาะสมกับการใช้งาน
- 6) ข้อมูลมีคุณภาพ โดยมีมาตรการในการควบคุมคุณภาพของข้อมูล ให้มีคุณภาพสูง ซึ่งจะสนับสนุนให้การดำเนินงานของหน่วยงานเป็นไปอย่างมีประสิทธิภาพและประสิทธิผล

ดังนั้น สรุปได้ว่า

“ธรรมาภิบาลข้อมูลภาครัฐ หมายความว่า การกำหนดสิทธิหน้าที่ และความรับผิดชอบของผู้มีส่วนได้เสียในการบริหารจัดการข้อมูลภาครัฐทุกขั้นตอน เพื่อให้การได้มาและการนำข้อมูลของหน่วยงานของรัฐไปใช้อย่างถูกต้องครบถ้วน เป็นปัจจุบัน รักษาความเป็นส่วนบุคคล และสามารถเชื่อมโยงแลกเปลี่ยน และบูรณาการระหว่างกันได้ อย่างมีประสิทธิภาพและมั่นคงปลอดภัย โดยใช้ข้อมูลเป็นหลักในการบริหารงานภาครัฐและการบริการสาธารณะ”

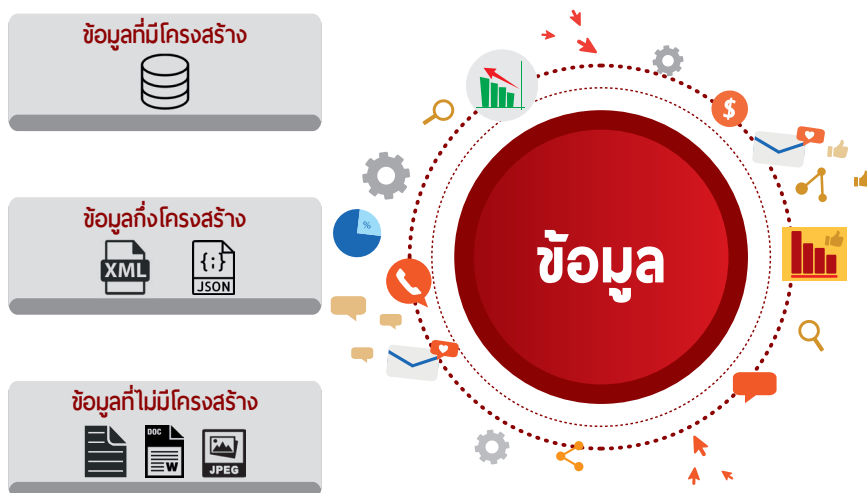
2.2 ข้อมูล (Data)

ข้อมูล คือ “ข้อเท็จจริงซึ่งใช้เป็นพื้นฐานสำหรับการอธิบายเหตุผล การสนทนา หรือการคำนวณ” (Australian Institute of Health and Welfare, 2014) ข้อมูลจัดเป็นองค์ประกอบหลักในการขับเคลื่อนหน่วยงานซึ่งมีความสัมพันธ์กับกระบวนการปฏิบัติงาน เทคโนโลยีสารสนเทศ สถานที่ รวมถึงบุคลากร

ข้อมูลจึงเปรียบเสมือนทรัพย์สินที่มีความสำคัญเช่นเดียวกับทรัพย์สินประเภทอื่น ดังนั้นหน่วยงานจึงจำเป็นต้องมีมาตรการในการรักษาความมั่นคงปลอดภัย และคุณภาพของข้อมูล เช่น การรักษาความลับของข้อมูล (Confidentiality) การป้องกันไม่ให้เกิดเหตุการณ์ที่ทำให้ไม่สามารถใช้งานข้อมูลได้ (Loss of Availability) การรักษาความถูกต้องครบถ้วนของข้อมูล (Integrity) การทำให้ข้อมูลเป็นปัจจุบันอยู่เสมอ (Timeliness) ทั้งนี้เพื่อตอบสนองต่อการตัดสินใจทั้งในระดับปฏิบัติการและระดับยุทธศาสตร์ได้อย่างมีประสิทธิภาพมากยิ่งขึ้น

2.2.1 ประเภทข้อมูล (Types of Data)

ข้อมูลถูกจัดแบ่งออกได้เป็น 3 ประเภท ดังนี้



รูปที่ 1 ประเภทของข้อมูล

1) **ข้อมูลที่มีโครงสร้าง (Structured Data)** เป็นข้อมูลที่มีการนิยามโครงสร้างของข้อมูลไว้ โดยนิยามความหมายและคุณสมบัติของแต่ละฟิลด์ข้อมูล โครงสร้างมีชั้นเดียวทำให้ง่ายต่อการค้นหา เช่น ตารางข้อมูลในฐานข้อมูล Comma-Separated Values – CSV ดังแสดงในตารางที่ 1

2) **ข้อมูลกึ่งโครงสร้าง (Semi-structured Data)** เป็นข้อมูลที่มีการนิยามโครงสร้างของข้อมูลไว้ แต่โครงสร้างเป็นแบบลำดับชั้น (Hierarchy) เช่น Extensible Markup Language - XML JavaScript Object Notation - JSON

3) **ข้อมูลที่ไม่มีโครงสร้าง (Unstructured Data)** เป็นข้อมูลที่ไม่ได้มีการนิยามโครงสร้างของข้อมูลไว้ มักจะอยู่ในรูปแบบ เช่น ข้อความ รูปภาพ เสียง วิดีทัศน์

2.2.2 ชุดข้อมูล (Datasets)

ชุดข้อมูล คือ “ข้อมูลที่มีการรวบรวมไว้ โดยปกติอยู่ในรูปแบบของตารางข้อมูล” (Askham et al., 2013) ซึ่งการรวบรวมข้อมูลนี้มาจากหลายแหล่ง และนำข้อมูลมาจัดเป็นชุดให้ถูกต้องตามลักษณะโครงสร้างข้อมูลที่กำหนดไว้ ดังตารางที่ 1 แสดงตัวอย่างชุดข้อมูลพนักงานในรูปแบบตารางข้อมูลหรือข้อมูลที่มีโครงสร้าง (Structured Data) มีทั้งหมด 3 แถว 5 ฟิลด์ (Data Field/Element/Attribute) ได้แก่ ชื่อ นามสกุล เพศ อายุ และระดับการศึกษา

ตารางที่ 1 ตัวอย่างชุดข้อมูลพนักงาน

ชื่อ	นามสกุล	เพศ	อายุ	ระดับการศึกษา
วิชัย	ใจดี	ชาย	26	ปริญญาตรี
พิเชษฐ์	วิเศษศิลป์	ชาย	28	ปริญญาโท
วิมลมาส	วงศ์สกุล	หญิง	25	ปริญญาตรี

2.2.3 ฐานข้อมูล (Database)

ฐานข้อมูล คือ “กลุ่มข้อมูล ที่มีความสัมพันธ์กันได้ถูกรวบรวมเข้าไว้ด้วยกัน ซึ่งสนับสนุนกิจกรรมของหน่วยงาน” (Malinowski, E. & Zimanyi, E., 2009) หรือกล่าวได้ว่า แต่ละฐานข้อมูลจะประกอบไปด้วยหลาย ๆ ชุดข้อมูลที่มีความสัมพันธ์กันดังแสดงในรูปที่ 2



รูปที่ 2 ความสัมพันธ์ระหว่างฐานข้อมูลกับชุดข้อมูล

2.3 การบริหารจัดการข้อมูล (Data Management)

การบริหารจัดการข้อมูล คือ “คำจำกัดความที่อธิบายถึงกระบวนการที่ใช้ในการวางแผน (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 ซึ่งแต่ละหน่วยงานต้องตระหนักว่าข้อมูลที่มีอยู่เป็นทรัพย์สินที่มีค่า และจากการเกิดขึ้นของข้อมูลที่มีปริมาณมหาศาล ไม่ว่าจะเป็นข้อมูลที่รวบรวมมาโดยอัตโนมัติจากระบบหรืออุปกรณ์ต่าง ๆ หรือข้อมูลที่เกิดขึ้นจากการป้อนข้อมูลหรือโต้ตอบกับผู้ใช้งาน เพื่อให้หน่วยงานสามารถนำข้อมูลเหล่านี้ไปประมวลผลหรือใช้ในการตัดสินใจได้อย่างแม่นยำ จึงต้องได้รับการบริหารจัดการอย่างถูกต้อง เหมาะสม และสอดคล้องกับวัตถุประสงค์ในการบริหารจัดการข้อมูลของหน่วยงาน เช่น

- 1) เพื่อการจัดเก็บ นำมาใช้งาน และประมวลผลข้อมูลตามที่หน่วยงานต้องการ
- 2) เพื่อควบคุม ตรวจสอบ และป้องกัน โดยใช้กระบวนการธรรมาภิบาลข้อมูลภาครัฐและความปลอดภัยของข้อมูล
- 3) เพื่อจัดหมวดหมู่ และกำหนดมาตรฐานของข้อมูล โดยใช้การจำแนกข้อมูล และกำหนดกรอบการทำงานที่เป็นที่รู้จักแพร่หลาย

- 4) เพื่อให้สามารถนำข้อมูลกลับมาใช้ได้ใหม่ภายหลัง โดยกำหนดข้อมูลให้อยู่ในรูปแบบที่เรียกใช้ได้อย่างมีประสิทธิภาพ
- 5) เพื่อการปรับปรุงข้อมูลให้เป็นปัจจุบัน และมีความถูกต้องสมบูรณ์อยู่เสมอ
- 6) เพื่อการปกป้องข้อมูลจากการลักลอบใช้งานหรือแก้ไขโดยมิชอบ รวมถึงจากเหตุการณ์ที่อาจเกิดจากภัยธรรมชาติหรือความบกพร่องภายในระบบคอมพิวเตอร์

ซึ่งในการบริหารจัดการข้อมูลนั้น มีองค์ประกอบในการบริหารจัดการตลอดทั้งระบบบริหารและกระบวนการจัดการข้อมูล หรือวงจรชีวิตของข้อมูล ดังรูปที่ 3



รูปที่ 3 ระบบบริหารและกระบวนการจัดการข้อมูล
หรือวงจรชีวิตของข้อมูล และองค์ประกอบในการบริหารจัดการข้อมูล

2.3.1 ระบบบริหารและกระบวนการจัดการข้อมูล หรือวงจรชีวิตของข้อมูล (Data Life Cycle)

ระบบบริหารและกระบวนการจัดการข้อมูล หรือวงจรชีวิตของข้อมูล คือ “ลำดับขั้นตอนของข้อมูลตั้งแต่เริ่มสร้างข้อมูลไปจนถึงการทำลายข้อมูล” ประกอบด้วย 6 ขั้นตอน ดังนี้

1) **กระบวนการสร้างข้อมูล (Create)** เป็นการสร้างข้อมูลขึ้นมาใหม่ โดยวิธีการบันทึกเข้าไปด้วยบุคคลหรือบันทึกอัตโนมัติด้วยอุปกรณ์อิเล็กทรอนิกส์ 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 โดยการคัดลอกข้อมูลที่ใช้งานอยู่ในปัจจุบัน เพื่อทำสำเนา เช่น ใช้โปรแกรมในการสำรองข้อมูล เป็นการหลีกเลี่ยงความเสียหายที่จะเกิดขึ้นหากข้อมูลเกิดการเสียหายหรือสูญหาย ซึ่งสามารถนำข้อมูลที่สำรองไว้ในสื่อบันทึกข้อมูลกลับมาใช้งานได้ทันที โดยการกู้คืน (Restore)

4) กระบวนการเผยแพร่ข้อมูล (Publish) เป็นการแชร์ข้อมูล (Sharing) การกระจายข้อมูล (Dissemination) การควบคุมการเข้าถึง (Access Control) การแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน (Exchange) และการกำหนดเงื่อนไขในการนำข้อมูลไปใช้ (Condition)

5) กระบวนการจัดเก็บข้อมูลถาวร (Archive) เป็นการคัดลอกเอาข้อมูลที่มีช่วงอายุเกินช่วงใช้งานหรือไม่ได้ใช้งานแล้ว เพื่อทำสำเนาสำหรับการเก็บรักษา โดยที่ข้อมูลนั้นไม่มีการลบ ปรับปรุง หรือแก้ไขอีก และสามารถนำกลับไปใช้งานได้ใหม่เมื่อต้องการ

6) กระบวนการทำลายข้อมูล (Destroy) เป็นการทำลายข้อมูลซึ่งปกติจะเป็นการทำลายข้อมูลที่มีการจัดเก็บถาวรเป็นระยะเวลานานหรือเกินกว่าระยะเวลาที่กำหนด

2.3.2 องค์ประกอบในการบริหารจัดการข้อมูล (Data Management Component)

จากการศึกษาแนวคิดของ DAMA International (Henderson et al., 2017) ในการบริหารจัดการข้อมูล ได้กำหนดองค์ประกอบในการบริหารจัดการข้อมูล ดังนี้

2.3.2.1 สถาปัตยกรรมข้อมูล (Data Architecture)

สถาปัตยกรรมข้อมูล (Data Architecture) เป็นส่วนหนึ่งของการพัฒนาสถาปัตยกรรมองค์กร (Enterprise Architecture) เป็นการอธิบายเกี่ยวกับกลุ่มของข้อมูลทั้งหมดที่มีในหน่วยงาน ความสัมพันธ์ระหว่างข้อมูลกับกระบวนการปฏิบัติงาน ความสัมพันธ์ระหว่างข้อมูลกับแอปพลิเคชัน

สถาปัตยกรรมเทคโนโลยีข้อมูล สถาปัตยกรรมการบูรณาการข้อมูล สถาปัตยกรรมเมทาดาตา เป็นต้น สถาปัตยกรรมข้อมูลจะอยู่ในรูปแบบของแบบจำลองข้อมูลที่มองเห็นภาพรวม ความเชื่อมโยง และการไหลของข้อมูลในระดับต่าง ๆ ทั้งหมดของหน่วยงาน ทั้งที่เป็นหน่วยงานต้นน้ำ กลางน้ำ หรือปลายน้ำ สามารถอธิบายสถานะที่มีอยู่ในปัจจุบัน และกำหนดความต้องการสำหรับอนาคต เพื่อให้หน่วยงานเกิดความเข้าใจและเห็นเป็นภาพเดียวกัน ดังนั้น จึงเป็นพื้นฐานที่สำคัญในการวางแผนบริหารจัดการข้อมูล

1. กลุ่มกระบวนการด้านยุทธศาสตร์

- | | |
|--|--------------------------------|
| D1 : นโยบายรัฐบาลอิเล็กทรอนิกส์ภาครัฐ | D6 : ข้อมูลการตลาด |
| D2 : ยุทธศาสตร์และกลยุทธ์ฯ ด้านธุรกิจ | D7 : ข้อมูลการพัฒนาองค์กร |
| D3 : ยุทธศาสตร์และกลยุทธ์ฯ ด้านดิจิทัล | D8 : ข้อมูลสถาปัตยกรรมองค์กร |
| D4 : ตัวชี้วัด ด้านธุรกิจ | D9 : ข้อมูลงบประมาณ |
| D5 : ตัวชี้วัด ด้านดิจิทัล | D10 : ข้อมูลข้อตกลงความร่วมมือ |

2. กลุ่มกระบวนการออกแบบและพัฒนา

- | | |
|--|---|
| D11 : ข้อมูลวิจัยผลิตภัณฑ์/บริการ | D17 : ข้อมูลบริหารโครงการพัฒนา |
| D12 : ข้อมูลการวิเคราะห์และการออกแบบ | D18 : ข้อมูลการปรับปรุงผลิตภัณฑ์/บริการ |
| D13 : ข้อมูลต้นแบบผลิตภัณฑ์/บริการ | D19 : ข้อมูลการเปลี่ยนแปลง |
| D14 : ข้อมูลผลิตภัณฑ์/บริการ | D20 : ข้อมูลการติดตั้ง |
| D15 : ข้อมูลผลิตภัณฑ์ที่พัฒนาขึ้น | D21 : ข้อมูลการประชาสัมพันธ์ |
| D16 : ข้อมูลการพัฒนาและการทำงานผลิตภัณฑ์ | |

3. กลุ่มกระบวนการให้บริการ

- | | |
|------------------------------|--|
| D22 : ข้อมูลลูกค้า | D26 : ข้อมูลการติดตาม ควบคุม และการบำรุงรักษา |
| D23 : ข้อมูลบริหารโครงการขาย | D27 : แผนการบริหารความต่อเนื่อง และกู้คืนภัยพิบัติ |
| D24 : ข้อมูลการขาย | D28 : ข้อมูลเหตุการณ์/ปัญหา และแนวทางการแก้ไข |
| D25 : ข้อมูลโครงสร้างพื้นฐาน | |

4. กลุ่มกระบวนการสนับสนุน

- | | |
|--------------------------------------|----------------------------------|
| D29 : ข้อมูลโครงสร้างองค์กร | D37 : กฎระเบียบ ข้อบังคับ |
| D30 : ข้อมูลพนักงาน | D38 : สัญญา |
| D31 : ข้อมูลการจัดซื้อจัดจ้าง | D39 : ข้อมูลร้องทุกข์ |
| D32 : ข้อมูลพัสดุ | D40 : ทรัพย์สินทางปัญญา |
| D33 : ข้อมูลโครงสร้างพื้นฐานสำนักงาน | D41 : ข้อมูลการนัดหมายผู้บริหาร |
| D34 : ข้อมูลงานสารบรรณ | D42 : ข้อมูลภาวะ/รายงานการประชุม |
| D35 : ข้อมูลทางบัญชี | D43 : ข้อมูลองค์ความรู้ |
| D36 : ข้อมูลมาตรฐานสากลและกระบวนการ | |

5. กลุ่มกระบวนการวัดและประเมินผล

- | | |
|--------------------------------------|---|
| D44 : ข้อมูลความเสี่ยง | D48 : ข้อมูลความสอดคล้อง กฎระเบียบสำนักงาน
กับกฎหมาย |
| D45 : ข้อมูลการควบคุมภายใน | |
| D46 : ข้อมูลการตรวจสอบภายใน | D49 : ความพึงพอใจต่อบริการ |
| D47 : ข้อมูลการปฏิบัติตามมาตรฐานสากล | D50 : ผลการประเมินการให้บริการ |

รูปที่ 4 ตัวอย่างความสัมพันธ์ระหว่างกลุ่มข้อมูลกับกลุ่มกระบวนการปฏิบัติงาน

จากรูปที่ 4 ตัวอย่างความสัมพันธ์ระหว่างกลุ่มข้อมูลกับกลุ่มกระบวนการปฏิบัติงาน ซึ่งชี้ให้เห็นถึงภาพรวมของข้อมูลทั้งหมดที่มีการดำเนินการในแต่ละกลุ่มกระบวนการปฏิบัติงาน กอง หรือ ส่วนงานภายในหน่วยงานความสัมพันธ์นี้สามารถใช้เป็นจุดเริ่มต้นในการจัดลำดับความสำคัญของข้อมูล กำหนดขอบเขต กำหนดอัตรากำลังคน และจัดสรรงบประมาณสำหรับธรรมาภิบาลข้อมูล และการบริหารจัดการข้อมูล จากตารางที่ 2 แสดงความสัมพันธ์ระหว่างข้อมูลกับแอปพลิเคชันในงานบริหารจัดการพัสดุ ซึ่งชี้ให้เห็นว่าข้อมูลเดียวกันอาจจะมีการใช้งานหรือเก็บซ้ำซ้อนกันในหลาย ๆ แอปพลิเคชัน

ดังนั้นความสัมพันธ์ระหว่างข้อมูลกับแอปพลิเคชันสามารถสนับสนุนการบูรณาการข้อมูล (Data Integration) ได้จากการที่ข้อมูลกระจายอยู่ตามแอปพลิเคชันต่าง ๆ ตัวอย่างสถาปัตยกรรมการบูรณาการข้อมูล ดังแสดงในรูปที่ 8 ซึ่งแสดงความสัมพันธ์ระหว่างคลังข้อมูล ดาตาเลค ระบบรายงาน อัจฉริยะ และดาตาอานาไลติกส์

ตารางที่ 2 ตัวอย่างความสัมพันธ์ระหว่างข้อมูลกับแอปพลิเคชันสำหรับการจัดการพัสดุ

ข้อมูล / แอปพลิเคชัน		แอปพลิเคชัน								
D32 : ข้อมูลพัสดุ	ข้อมูลครุภัณฑ์	×	×	×	×	×	×	×	×	×
	ข้อมูลการตรวจสอบพัสดุ									
	ข้อมูลบาร์โค้ด									
	ข้อมูลสถานะพัสดุ	×								
	ข้อมูลการโอนคืน									
	ข้อมูลการจำหน่าย									
	ข้อมูลตราสินค้า	×								
	ข้อมูลการรับประกัน	×								
	ข้อมูลการซ่อมบำรุง									
	ข้อมูลพนักงาน	×								
D31 : ข้อมูลการจัดซื้อจัดจ้าง	ข้อมูลใบสั่งซื้อ (PO)									

ตารางที่ 3 สรุปการบริหารจัดการสถาปัตยกรรมข้อมูล

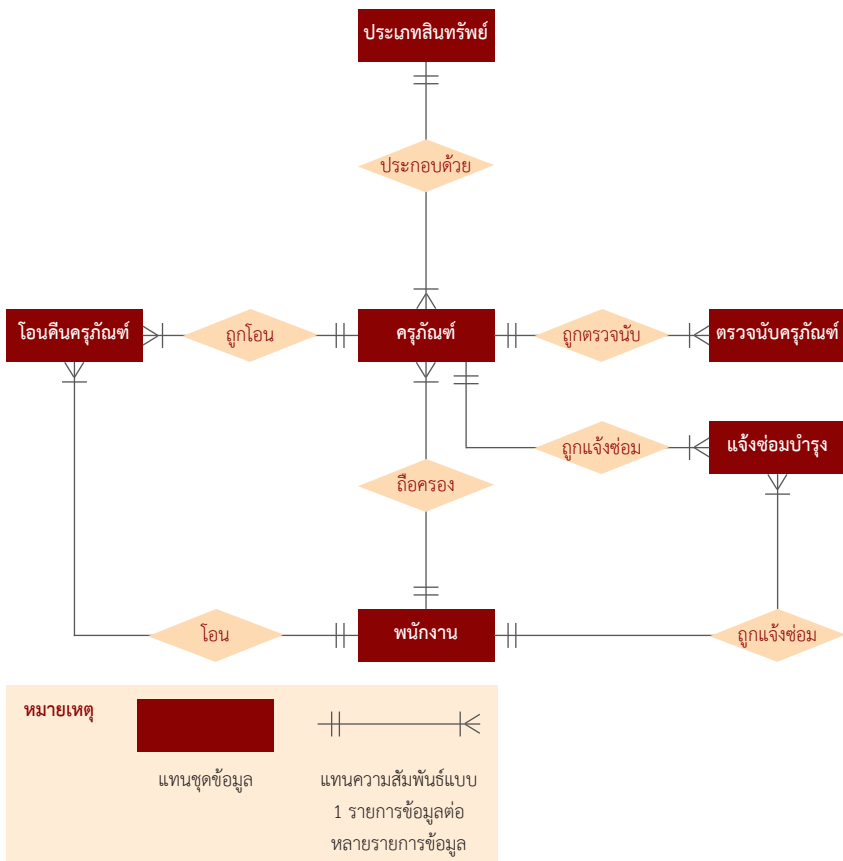
การบริหารจัดการสถาปัตยกรรมข้อมูล	
วิธีดำเนินการ	- ทำความเข้าใจกับความต้องการข้อมูลของหน่วยงาน - ประเมินสถานะและข้อกำหนดของสถาปัตยกรรมข้อมูลในปัจจุบัน - ออกแบบ พัฒนา และปรับปรุงแบบจำลองข้อมูลของหน่วยงาน - สร้างความสอดคล้องของข้อมูลของหน่วยงานกับส่วนงานอื่น ๆ ที่เกี่ยวข้อง เช่น กระบวนการธุรกิจ แอปพลิเคชัน - ออกแบบ พัฒนา และปรับปรุงสถาปัตยกรรมข้อมูล
สิ่งที่นำเข้า	- สถาปัตยกรรมองค์กร (Enterprise Architecture) - มาตรฐานและเป้าหมายที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ
เครื่องมือที่ใช้	- เครื่องมือจัดทำแบบจำลองข้อมูล (Data Modeling Tool) สำหรับจัดทำแบบจำลองข้อมูลระดับหน่วยงาน - เครื่องมือบริหารจัดการแบบจำลอง (Model Management Tool) สำหรับจัดเก็บแบบจำลองข้อมูลและควบคุมการเปลี่ยนแปลงของแบบจำลองข้อมูล
ผลที่ได้รับ	- แบบจำลองข้อมูลระดับหน่วยงาน (Enterprise Data Model) - ความสัมพันธ์ระหว่างข้อมูลกับส่วนงาน ข้อมูลกับกระบวนการปฏิบัติงาน และข้อมูลกับแอปพลิเคชัน เป็นต้น - สถาปัตยกรรมเทคโนโลยีข้อมูล (Data Technology Architecture)
ผู้ที่เกี่ยวข้อง	สถาปนิกข้อมูล (Data Architect)

2.3.2.2 การจำลองและการออกแบบข้อมูล

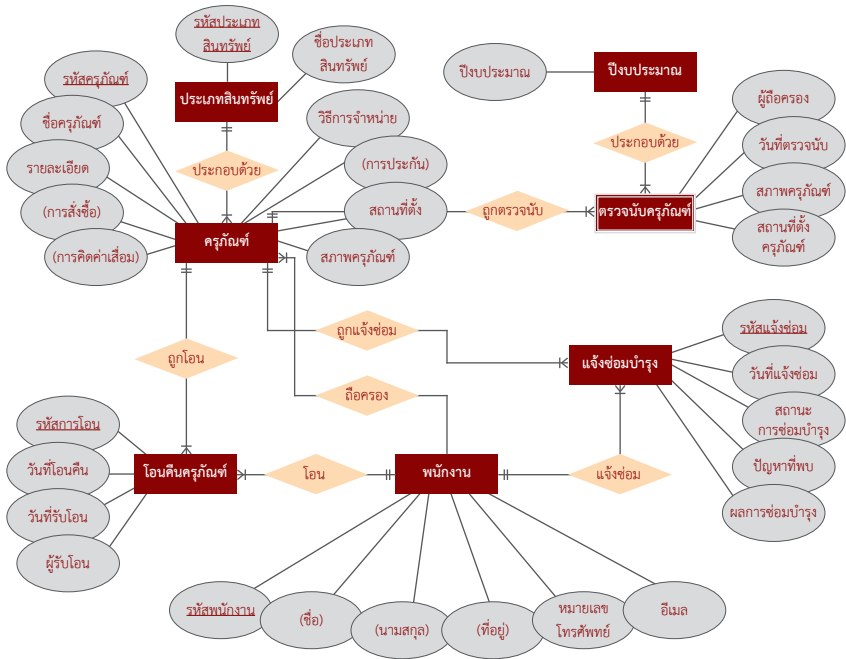
(Data Modeling and Design)

การจำลองและการออกแบบข้อมูล (Data Modeling and Design) เป็นวิธีการวิเคราะห์ความต้องการของผู้ใช้งาน รวมถึงระบุข้อกำหนดและการแก้ปัญหาต่าง ๆ ที่เกี่ยวข้อง แบบจำลองข้อมูลแสดงในรูปแบบของไดอะแกรม (Diagram) ที่มีการออกแบบลักษณะโครงสร้างของข้อมูล เพื่อใช้ในการสื่อสารภายในหน่วยงานให้เข้าใจตรงกัน แบบจำลองข้อมูลจะแสดงถึงความสัมพันธ์ระหว่างข้อมูลที่เกี่ยวข้องกันพร้อมทั้งรายละเอียดของโครงสร้างของข้อมูล โดยแบ่งออกเป็น 3 ระดับ ได้แก่ (1) แบบจำลองข้อมูลเชิงความคิด (Conceptual Data Model) (2) แบบจำลองข้อมูลเชิงตรรกะ (Logical Data Model) และ (3) แบบจำลองข้อมูลเชิงกายภาพ (Physical Data Model)

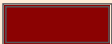
ขั้นตอนในการสร้างแบบจำลองและการออกแบบข้อมูล เริ่มตั้งแต่การวิเคราะห์ความต้องการของผู้ใช้ เพื่อกำหนดเป็นแบบจำลองข้อมูลเชิงความคิดของข้อมูลขึ้นมา เป็นขั้นตอนของการกำหนดเค้าโครงในระดับเบื้องต้น สามารถมองเห็นถึงความสัมพันธ์ของข้อมูล แต่ยังไม่สามารถนำไปใช้งานได้จริง เพราะเป็นเพียงแนวคิดเท่านั้น หลังจากนั้นทำการออกแบบข้อมูลให้มีความชัดเจนมากขึ้นโดยกำหนดเป็นแบบจำลองข้อมูลเชิงตรรกะ ซึ่งเป็นการให้รายละเอียดของข้อมูลที่มากขึ้น (เช่น ฟิลด์ข้อมูล) ขั้นตอนสุดท้ายจึงกำหนดแบบจำลองข้อมูลเชิงกายภาพ เพื่อให้สามารถใช้งานได้จริง โดยกำหนดรายละเอียดของข้อมูลเพิ่มเติม เช่น รูปแบบของข้อมูล ขนาดของข้อมูล



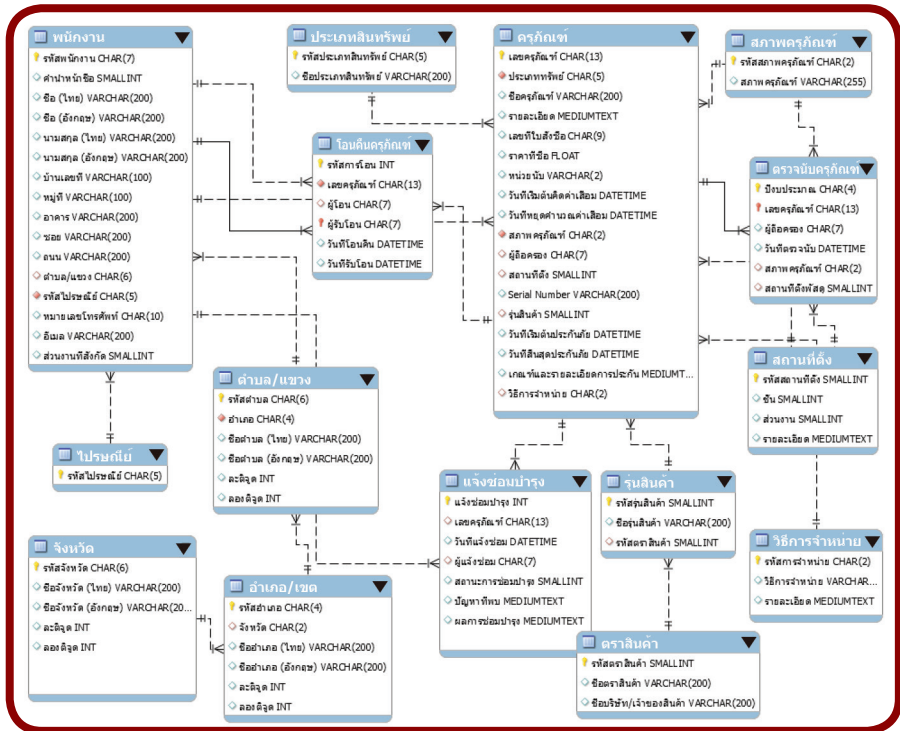
รูปที่ 5 ตัวอย่างแบบจำลองข้อมูลเชิงความคิด (Conceptual Data Model) สำหรับงานบริหารจัดการพัสดุ



หมายเหตุ

	แทนชุดข้อมูล
	แทนชุดข้อมูลที่อาศัยฟีดของชุดข้อมูลอื่นเป็นคีย์หลัก
	แทนฟีดข้อมูลทั่วไป
	แทนฟีดข้อมูลที่เป็นคีย์หลัก
	แทนฟีดข้อมูลที่มีฟีดข้อมูลย่อย
	แทนความสัมพันธ์ แบบ 1 รายการข้อมูลต่อหลายรายการข้อมูล

รูปที่ 6 ตัวอย่างแบบจำลองข้อมูลเชิงตรรกะ (Logical Data Model)
สำหรับงานบริหารจัดการพัสดุ



รูปที่ 7 ตัวอย่างแบบจำลองข้อมูลเชิงกายภาพ (Physical Data Model) สำหรับงานบริหารจัดการพัสดุ

จากรูปที่ 5 แสดงตัวอย่างแบบจำลองข้อมูลเชิงความคิดสำหรับงานบริหารจัดการพัสดุ ซึ่งแสดงให้เห็นว่า ประเภทสิทธิประโยชน์หนึ่งประเภท ประกอบด้วย ครัวเรือนหลายรายการ พนักงานหนึ่งราย ถือครองครัวเรือนที่ได้หลายรายการ และแจ้งซ่อมได้หลายครั้ง ครัวเรือนหนึ่งรายการ สามารถโอน ตรวจสอบ และแจ้งซ่อมได้หลายครั้ง สำหรับฟิลด์ข้อมูลของแต่ละชุดข้อมูลแสดงในแบบจำลองเชิงตรรกะตามรูปที่ 6 ทั้งนี้รายละเอียดด้านเทคนิคอธิบายไว้ในรูปที่ 7 ประกอบด้วย คีย์หลัก ประเภทข้อมูล และความกว้างของฟิลด์ข้อมูล

ตารางที่ 4 สรุปการบริหารจัดการการจำลองและการออกแบบข้อมูล

การบริหารจัดการการจำลองและการออกแบบข้อมูล	
วิธีดำเนินการ	- วิเคราะห์ความต้องการข้อมูลของหน่วยงาน - ออกแบบและพัฒนาแบบจำลองของข้อมูล รวมถึงฐานข้อมูล
สิ่งที่นำเข้า	- สถาปัตยกรรมองค์กร (Enterprise Architecture) - มาตรฐานและเป้าหมายที่เกี่ยวกับเทคโนโลยีสารสนเทศ
เครื่องมือที่ใช้	- เครื่องมือจัดทำแบบจำลองข้อมูล (Data Modeling Tool) - เครื่องมือบริหารจัดการแบบจำลอง (Model Management Tool) - ระบบการจัดการฐานข้อมูล (Database Management System - DBMS) สำหรับออกแบบ แบบจำลองข้อมูลเชิงกายภาพ
ผลที่ได้รับ	- ความต้องการของข้อมูล (Data Requirement) และข้อกำหนดทางธุรกิจ (Business Rules) - แบบจำลองข้อมูลเชิงแนวคิด (Conceptual Data Models) - แบบจำลองข้อมูลเชิงตรรกะ (Logical Data Models) - แบบจำลองข้อมูลเชิงกายภาพ (Physical Data Models)
ผู้เกี่ยวข้อง	- สถาปนิกข้อมูล (Data Architect) - นักวิทยาการข้อมูล (Data Scientist) - นักวิเคราะห์ข้อมูล (Data Analyst) - นักวิเคราะห์ธุรกิจ (Business Analyst) - นักออกแบบจำลองข้อมูล (Data Modeler)

2.3.2.3 การจัดเก็บและการดำเนินการกับข้อมูล (Data Storage and Operations)

การจัดเก็บและการดำเนินการกับข้อมูล (Data Storage and Operations) เป็นการจัดเก็บข้อมูลที่มีโครงสร้าง โดยจัดเก็บในรูปแบบของฐานข้อมูล ส่วนการดำเนินการกับข้อมูลจะเกี่ยวข้องตั้งแต่การวางแผน การใช้งาน การสำรองข้อมูล (Backup) การกู้คืนข้อมูล (Restore) การจัดเก็บข้อมูลถาวร (Archive) กระบวนการที่เกี่ยวข้องกับข้อมูล (Create Read Update Delete - CRUD) ตลอดทั้งระบบบริหารและกระบวนการจัดการข้อมูล หรือวงจรชีวิตของข้อมูล การโอนย้ายข้อมูล (Migration) รวมถึงการปรับปรุงประสิทธิภาพของฐานข้อมูลให้พร้อมใช้งานได้ตลอดเวลา เพื่อรักษาความมั่นคงปลอดภัย และความถูกต้องของข้อมูล

ตารางที่ 5 สรุปการบริหารจัดการการจัดเก็บและการดำเนินการกับข้อมูล

การบริหารจัดการการจัดเก็บและการดำเนินการกับข้อมูล	
วิธีดำเนินการ	- สนับสนุนในส่วนของฐานข้อมูล เช่น การจัดเก็บ การสำรอง การกู้คืน การปรับปรุงประสิทธิภาพของระบบการจัดการฐานข้อมูล - จัดการในส่วนและเทคโนโลยีด้านข้อมูล เช่น ศึกษาความต้องการของเทคโนโลยีด้านข้อมูล
สิ่งที่นำเข้า	- ข้อกำหนดและเงื่อนไขการให้บริการ (Service Level Agreement) - สถาปัตยกรรมข้อมูล (Data Architecture) - ข้อเสนอแนะในการโอนย้ายข้อมูล (Migration)

ตารางที่ 5 สรุปการบริหารจัดการการจัดเก็บและการดำเนินการกับข้อมูล (ต่อ)

การบริหารจัดการการจัดเก็บและการดำเนินการกับข้อมูล	
เครื่องมือที่ใช้	- ระบบการจัดการฐานข้อมูล (Database Management System - DBMS) - เครื่องมือบริหารจัดการฐานข้อมูล (Database Administration Tool)
ผลที่ได้รับ	- แผนการสำรองและข้อมูลได้รับการสำรอง - แผนการกู้คืนข้อมูลและข้อมูลได้รับการกู้คืน - แผนความต่อเนื่องทางธุรกิจ (Business Continuity Plans)
ผู้เกี่ยวข้อง	- ผู้บริหารจัดการฐานข้อมูล (Database Administrator - DBA) - วิศวกรข้อมูล (Data Engineer)

2.3.2.4 การบูรณาการและความสามารถในการทำงานร่วมกัน (Data Integration and Interoperability)

การเชื่อมโยงข้อมูล (Data Integration) เป็นการรวบรวมข้อมูลจากแหล่งข้อมูลต่าง ๆ ในรูปแบบที่สอดคล้องกันเข้ามารวมอยู่ในแหล่งข้อมูลเดียวกัน เพื่อนำไปใช้ในการจัดทำข้อมูลหลัก (Master Data) คลังข้อมูล (Data Warehouse) ดาตาเลค (Data Lake) รวมถึงการแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน รูปที่ 8 แสดงความสัมพันธ์ระหว่างการบูรณาการข้อมูล คลังข้อมูล และดาตาเลค ส่วนความสามารถในการทำงานร่วมกัน (Interoperability) จะมีการกำหนดมาตรฐานหรือข้อตกลงร่วมกันระหว่างหน่วยงานหรือระบบโดยมีการอ้างอิงถึงคุณลักษณะของระบบต่าง ๆ ที่สามารถแลกเปลี่ยนข้อมูลกันหรือสื่อสารกันได้ เช่น มีการแลกเปลี่ยนข้อมูลในรูปแบบของ Application Programming Interfaces - API

ในการรวบรวมข้อมูลจากแหล่งต่าง ๆ เข้าด้วยกัน ทำให้การบูรณาการข้อมูล มีส่วนช่วยควบคุมและจัดการคุณภาพของข้อมูลให้ดียิ่งขึ้น ขณะที่การแลกเปลี่ยนข้อมูลจะสนับสนุนให้เกิดประสิทธิภาพของการดำเนินงานระหว่างหน่วยงานหรือส่วนงาน เพราะทั้งหมดนี้มุ่งเน้นการแปลงข้อมูล (Transform) และรวมข้อมูลจากหน่วยงานหรือระบบต้นทางไปจนถึงหน่วยงานหรือระบบกลาง และจากหน่วยงานหรือระบบกลางไปยังหน่วยงานหรือระบบปลายทาง เพื่อใช้ในการวิเคราะห์ข้อมูลต่อไป

ตารางที่ 6 สรุปการบริหารจัดการการบูรณาการและความสามารถในการทำงานร่วมกัน

การบริหารจัดการการบูรณาการและความสามารถในการทำงานร่วมกัน	
วิธีดำเนินการ	- กำหนดมาตรฐานและแบบจำลองอ้างอิงของการทำงานร่วมกัน - พัฒนาแผนการดำเนินงานการบูรณาการและการทำงานร่วมกัน
สิ่งที่นำเข้า	หลักเกณฑ์การแลกเปลี่ยนและเชื่อมโยงผ่านระบบและเครือข่ายสารสนเทศและการสื่อสาร
เครื่องมือที่ใช้	- เครื่องมือจัดทำแบบจำลองข้อมูล (Data Modeling Tool) - Enterprise Service Bus (ESB) คือ ตัวกลางที่ทำให้ผู้ต้องการเรียกใช้งานบริการ (Services) ต่าง ๆ จากระบบสามารถเรียกผ่าน ESB ได้
ผลที่ได้รับ	- รายละเอียดของสิ่งที่เกี่ยวข้อง เช่น ฐานข้อมูล API - แนวปฏิบัติในการแลกเปลี่ยนข้อมูล - ข้อตกลงในการเข้าถึงข้อมูลและแลกเปลี่ยนข้อมูล
ผู้เกี่ยวข้อง	วิศวกรข้อมูล (Data Engineer)

2.3.2.5 การบริหารจัดการเอกสารและเนื้อหา
(Document and Content Management)

การบริหารจัดการเอกสารและเนื้อหา (Document and Content Management) เป็นการวางแผน การจัดการ การเข้าถึง การใช้งาน และการควบคุมกิจกรรมต่าง ๆ ที่เกี่ยวกับข้อมูลที่ไม่มีโครงสร้างหรือแบบกึ่งโครงสร้าง เช่น การจัดเก็บ การป้องกันความเสียหาย การเข้าถึงข้อมูล ทั้งที่เก็บอยู่ในรูปแบบกระดาษ และไฟล์อิเล็กทรอนิกส์ มีความ รูปภาพ เสียง ภาพเคลื่อนไหว เป็นต้น การบริหารจัดการดังกล่าวมุ่งเน้นที่การรักษาความถูกต้องสมบูรณ์ และช่วยให้สามารถเข้าถึงเอกสารและข้อมูลที่ไม่มีโครงสร้างหรือแบบกึ่งโครงสร้างได้

ตารางที่ 7 สรุปการบริหารจัดการเอกสารและเนื้อหา

การบริหารจัดการเอกสารและเนื้อหา	
วิธีดำเนินการ	- พัฒนาระบบจัดการเอกสาร เพื่อการจัดเก็บ การเข้าถึง และการควบคุมความปลอดภัย - จัดทำนโยบายการจัดทำเนื้อหา (Content Handling Policies)
สิ่งที่นำเข้า	- ข้อมูลที่เป็นสื่อสังคมออนไลน์ (Social Media) - เอกสารที่เป็นกระดาษ
เครื่องมือที่ใช้	- เครื่องมือบริหารจัดการเอกสาร (Document Management Tool) - เครื่องมือจัดการเนื้อหา (Content Management Tool)
ผลที่ได้รับ	เอกสารหรือรายงาน
ผู้เกี่ยวข้อง	พนักงานหรือเจ้าหน้าที่

2.3.2.6 ข้อมูลหลักและข้อมูลอ้างอิง

(Master and Reference Data)

ข้อมูลหลักและข้อมูลอ้างอิง (Master and Reference Data) เป็นการบริหารจัดการข้อมูลเพื่อให้ทั้งหน่วยงานสามารถเข้าถึง และใช้ข้อมูลร่วมกันได้ โดยข้อมูลถูกจัดเก็บไว้แหล่งเดียว มีการกำหนดมาตรฐานของข้อมูล เพื่อช่วยลดความซ้ำซ้อนของข้อมูล ทำให้ข้อมูลมีคุณภาพ ความแตกต่างระหว่างข้อมูลหลัก (Master Data) กับข้อมูลอ้างอิง (Reference Data) กล่าวคือ ข้อมูลอ้างอิง จะเป็นข้อมูลที่เป็นสากล มีการกำหนดให้เป็นมาตรฐาน และใช้งานร่วมกัน มีการเปลี่ยนแปลงค่อนข้างน้อย เช่น รหัสไปรษณีย์ รหัสประเทศ หน่วยวัดระยะทาง ขณะที่ข้อมูลหลักมีโอกาสเปลี่ยนแปลงได้มากกว่า มีรายละเอียดหรือจำนวนฟิลด์ข้อมูลที่มากกว่า และเป็นข้อมูลที่สร้างและใช้งานร่วมกันภายในขอบเขตการดำเนินงานตามภารกิจของหน่วยงาน เช่น ข้อมูลพนักงาน ข้อมูลลูกค้า ข้อมูลผู้ขาย ข้อมูลสินค้า ข้อมูลครุภัณฑ์ ข้อมูลสถานที่

ตารางที่ 8 สรุปการบริหารจัดการข้อมูลหลักและข้อมูลอ้างอิง

การบริหารจัดการหลักและข้อมูลอ้างอิง	
วิธีดำเนินการ	- ทำความเข้าใจเกี่ยวกับความต้องการข้อมูลทั้งข้อมูลหลักและข้อมูลอ้างอิง - กำหนดแหล่งที่มา (Source) ของข้อมูลหลักและข้อมูลอ้างอิง - ดำเนินการจัดทำข้อมูลหลักและข้อมูลอ้างอิง
สิ่งที่นำเข้า	อภิธานศัพท์ข้อมูล (Data Glossary)

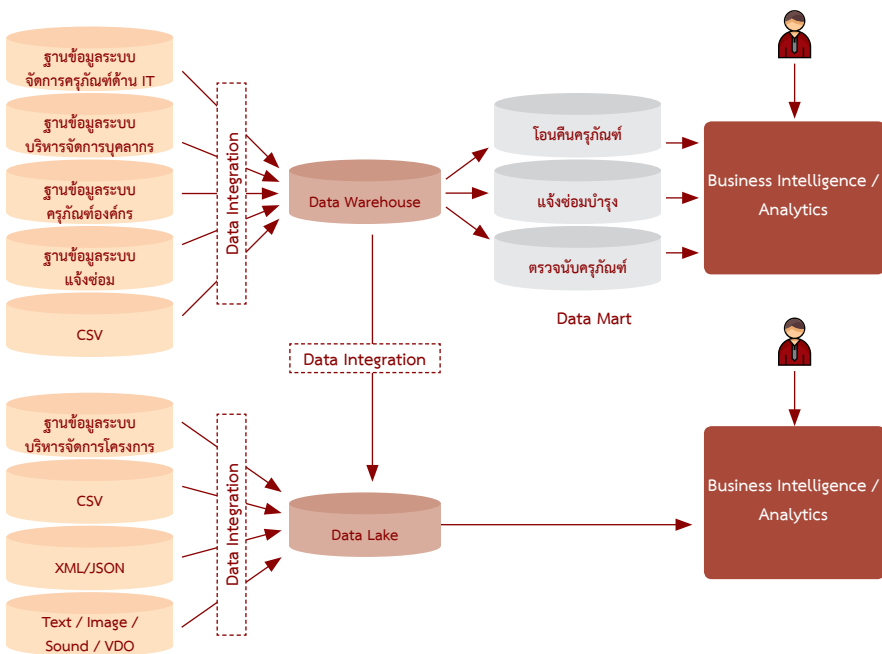
ตารางที่ 8 สรุปการบริหารจัดการข้อมูลหลักและข้อมูลอ้างอิง (ต่อ)

การบริหารจัดการหลักและข้อมูลอ้างอิง	
เครื่องมือที่ใช้	- เครื่องมือบริหารจัดการข้อมูลหลัก (Master Data Management Tools) - เครื่องมือบริหารจัดการข้อมูลอ้างอิง (Reference Data Management Tools) - เครื่องมือจัดทำแบบจำลองข้อมูล (Data Modeling Tools) - เครื่องมือสำหรับบูรณาการข้อมูล (Data Integration Tools)
ผลที่ได้รับ	ข้อมูลหลักและข้อมูลอ้างอิง
ผู้เกี่ยวข้อง	- สถาปนิกข้อมูล (Data Architect) - นักวิทยาการข้อมูล (Data Scientist) - วิศวกรข้อมูล (Data Engineer) - นักออกแบบจำลองข้อมูล (Data Modeler)

2.3.2.7 คลังข้อมูล ดาตาเลค ระบบรายงานอัจฉริยะ และดาตาอานาไลติกส์ (Data Warehouse, Data Lake, Business Intelligence, and Data Analytics)

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

ดาตาเลค (Data Lake) เป็นแหล่งสำหรับเก็บรวบรวมข้อมูลที่มีหลากหลายรูปแบบ ข้อมูลที่จัดเก็บเป็นข้อมูลที่มีโครงสร้าง ข้อมูลกึ่งโครงสร้าง และข้อมูลที่ไม่มีโครงสร้าง โดยข้อมูลถูกเก็บรักษาไว้ในรูปแบบที่เหมือนหรือใกล้เคียงกับรูปแบบที่ได้รับมาจากแหล่งข้อมูลต้นฉบับ และสามารถใช้เป็นทีสำรองข้อมูลต้นฉบับได้



รูปที่ 8 ตัวอย่างความสัมพันธ์ระหว่างคลังข้อมูล ดาตาเลค ระบบรายงานอัจฉริยะ และดาตาอานาไลติกส์สำหรับงานบริหารจัดการพัสดุ

จากรูปที่ 8 คลังข้อมูลและดาตาเลคจะเกิดจากการรวบรวมข้อมูลจากแหล่งข้อมูลต่าง ๆ ซึ่งแต่ละแหล่งอาจจะมีรูปแบบของข้อมูลที่แตกต่างกัน การรวบรวมข้อมูลใช้วิธีการบูรณาการข้อมูล (ดูที่หัวข้อ 2.3.2.4) โดยข้อมูลจากคลังข้อมูลสามารถรวมเข้าไปที่ดาตาเลคเพื่อใช้สำหรับการวิเคราะห์ข้อมูลที่ซับซ้อนมากยิ่งขึ้น ข้อมูลในคลังข้อมูลจะต้องถูกจัดกลุ่มออกเป็นดาตามาร์ท (Data Mart) โดยต้องสอดคล้องกับหน่วยงานที่จะนำไปใช้ เช่น ดาตามาร์ทของฝ่ายบุคคล ดาตามาร์ทของฝ่ายการตลาด ดาตามาร์ทของฝ่ายการเงิน หลังจากนั้นข้อมูลในดาตามาร์ทถูกนำไปใช้สำหรับการทำรายงานอัจฉริยะ (Business Intelligence) หรือการทำนายสิ่งที่จะเกิดขึ้นในอนาคตผ่านวิธีการของดาตาอานาไลติกส์ ในกรณีของดาตาเลคสามารถนำข้อมูลไปใช้สำหรับทำรายงานอัจฉริยะและดาตาอานาไลติกส์ได้ทันทีโดยไม่ต้องสร้างดาตามาร์ท หลังจากข้อมูลต่าง ๆ ถูกทำการวิเคราะห์หรือออกเป็นรายงานอัจฉริยะ และผลการทำนายแล้ว จะถูกนำไปใช้ เพื่อสนับสนุนการตัดสินใจของหน่วยงานทั้งในระดับปฏิบัติการและระดับบริหารต่อไป

ตารางที่ 9 สรุปการบริหารจัดการคลังข้อมูล ดาตาเลค ระบบรายงานอัจฉริยะ และดาตาอานาไลติกส์

การบริหารจัดการคลังข้อมูล ดาตาเลค ระบบรายงานอัจฉริยะ และดาตาอานาไลติกส์	
วิธีดำเนินการ	- จัดเตรียมข้อมูลจากหลาย ๆ แหล่งมารวมกันในคลังข้อมูล - ประมวลผลข้อมูลสำหรับการวิเคราะห์
สิ่งที่นำเข้า	- ความต้องการทางธุรกิจ (Business Requirement) - ข้อมูลหลักและข้อมูลอ้างอิง

ตารางที่ 9 สรุปการบริหารจัดการคลังข้อมูล ดาตาเลค ระบบรายงานอัจฉริยะ และดาตาอานาไลติกส์ (ต่อ)

การบริหารจัดการคลังข้อมูล ดาตาเลค ระบบรายงานอัจฉริยะ และดาตาอานาไลติกส์	
เครื่องมือที่ใช้	• เครื่องมือสำหรับบูรณาการข้อมูล (Data Integration Tools) • เครื่องมือบริหารจัดการเก็บข้อมูล (Data Storage Tools) • เครื่องมือสำหรับจัดทำรายงานอัจฉริยะ (Business Intelligence Tools) • เครื่องมือวิเคราะห์ทางสถิติ (Statistics Tools) • การเรียนรู้ของเครื่องและปัญญาประดิษฐ์ (Machine Learning and Artificial Intelligence)
ผลที่ได้รับ	• รายงาน และ Dashboard • ผลการดำเนินงาน
ผู้เกี่ยวข้อง	• สถาปนิกข้อมูล (Data Architect) • นักวิทยาการข้อมูล (Data Scientist) • วิศวกรข้อมูล (Data Engineer) • นักวิเคราะห์ข้อมูล (Data Analyst)

2.3.2.8 คำอธิบายชุดข้อมูลดิจิทัล หรือเมทาดาตา (Metadata)

คำอธิบายชุดข้อมูลดิจิทัล หรือเมทาดาตา (Metadata) เป็นข้อมูลที่ใช้อธิบายข้อมูลหลักหรือกลุ่มข้อมูลอื่น ๆ ที่เกี่ยวข้องทั้งกระบวนการเชิงธุรกิจและเชิงเทคโนโลยีสารสนเทศ กฎและข้อจำกัดของข้อมูล และโครงสร้างของข้อมูล เมทาดาตาช่วยให้หน่วยงานสามารถเข้าใจข้อมูลระบบ และขั้นตอนการทำงานได้ดียิ่งขึ้น โดยการบริหารจัดการเมทาดาตา (Metadata Management) เริ่มตั้งแต่ การเก็บรวบรวม การจัดกลุ่ม การดูแล และการควบคุมเมทาดาตา

ทั้งนี้ข้อมูลแต่ละชุดควรมีเมทาดาตา เพื่อให้ผู้ใช้งานทราบเกี่ยวกับชุดข้อมูล เช่น รายละเอียดชุดข้อมูล สิ่งที่เกี่ยวข้องกับชุดข้อมูล วัตถุประสงค์การนำไปใช้ ฟิลด์ข้อมูล

ตารางที่ 10 ตัวอย่างเมทาดาตาของข้อมูลครุภัณฑ์

ชื่อข้อมูล	ข้อมูลครุภัณฑ์			
คำอธิบายอย่างย่อ	อ้างถึงครุภัณฑ์ที่หน่วยงานถือครองทั้งจากการซื้อมาหรือรับมารวมถึงพัสดุประเภทวัสดุควบคุม			
เจ้าของข้อมูล	ส่วนจัดซื้อและพัสดุ			
Attribute	Description	Type	Allowed Null	Key
เลขครุภัณฑ์	รูปแบบเลขครุภัณฑ์ : xx-xxxx-xxx-xxxx รูปแบบเลขวัสดุควบคุม : ED-xx-xxxx-xxx-xxxx (ในกรณีเป็นวัสดุควบคุมขณะแสดงรหัสวัสดุควบคุมให้นำ “ED” ไว้ข้าง xx-xxxx-xxx-xxxx)	CHAR(13)	N	PK
ประเภทสินทรัพย์	อ้างอิง : รหัสประเภทสินทรัพย์	CHAR(5)	N	FK
ชื่อครุภัณฑ์		VARCHAR(200)	N	
รายละเอียด		MEDIUMTEXT	Y	

ตารางที่ 10 ตัวอย่างเมตาเดตาของข้อมูลครุภัณฑ์ (ต่อ)

ชื่อข้อมูล	ข้อมูลครุภัณฑ์			
คำอธิบายอย่างย่อ	อ้างอิงครุภัณฑ์ที่หน่วยงานถือครองทั้งจากการซื้อมาหรือรับมารวมถึงพัสดุประเภทวัสดุควบคุม			
เจ้าของข้อมูล	ส่วนจัดซื้อและพัสดุ			
Attribute	Description	Type	Allowed Null	Key
เลขที่ใบสั่งซื้อ	รูปแบบ : DGA/XX/XXXX คำอธิบาย : XX อ้างอิงปีงบประมาณ และ XXXX อ้างอิง Running Number ตัวอย่าง : DGA/59/0001	CHAR(9)	N	
ราคาที่ซื้อ		FLOAT	N	
หน่วยนับ	อ้างอิง : รหัสหน่วยนับ	VARCHAR(2)	N	FK
วันที่เริ่มต้น คิดค่าเสื่อม	รูปแบบ : YYYY-MM-DD คำอธิบาย : ปี ค.ศ.-เดือน-วัน ตัวอย่าง : 2016-04-15	DATETIME	N	
วันที่หยุดคำนวณ ค่าเสื่อม	รูปแบบ : YYYY-MM-DD คำอธิบาย : ปี ค.ศ.-เดือน-วัน ตัวอย่าง : 2016-04-15	DATETIME	N	
สภาพครุภัณฑ์	อ้างอิง : รหัสสภาพครุภัณฑ์	CHAR(2)	N	FK
ผู้ถือครอง	อ้างอิง : รหัสพนักงาน	CHAR(7)	N	FK
สถานที่ตั้งพัสดุ	อ้างอิง : รหัสสถานที่ตั้ง	SMALLINT	N	FK

ตารางที่ 10 ตัวอย่างเมทาดาทาของข้อมูลครุภัณฑ์ (ต่อ)

ชื่อข้อมูล	ข้อมูลครุภัณฑ์			
คำอธิบายอย่างย่อ	อ้างอิงครุภัณฑ์ที่หน่วยงานถือครองทั้งจากการซื้อหรือรับมารวมถึงพัสดุประเภทวัสดุควบคุม			
เจ้าของข้อมูล	ส่วนจัดซื้อและพัสดุ			
Attribute	Description	Type	Allowed Null	Key
รหัสรุ่นสินค้า		VARCHAR(200)	N	
รุ่นสินค้า	อ้างอิง : รหัสรุ่นสินค้า	SMALLINT	N	FK
วันที่เริ่มต้นประกัน	รูปแบบ : YYYY-MM-DD คำอธิบาย : ปี ค.ศ.-เดือน-วัน ตัวอย่าง : 2016-04-15	DATETIME	Y	
วันที่สิ้นสุดประกัน	รูปแบบ : YYYY-MM-DD คำอธิบาย : ปี ค.ศ.-เดือน-วัน ตัวอย่าง : 2016-04-15	DATETIME	Y	
เกณฑ์และรายละเอียดการประกัน	เกณฑ์ รายละเอียดการประกัน และบริษัทที่ให้การประกัน	MEDIUMTEXT	Y	
วิธีการจำหน่ายพัสดุ	อ้างอิง : รหัสวิธีการจำหน่ายพัสดุ	CHAR(2)	N	

ตารางที่ 11 สรุปการบริหารจัดการคำอธิบายชุดข้อมูลดิจิทัล หรือ เมทาดาตา

การบริหารจัดการคำอธิบายชุดข้อมูลดิจิทัล หรือเมทาดาตา	
วิธีดำเนินการ	- ทำความเข้าใจเกี่ยวกับความต้องการในการจัดทำคำอธิบายชุดข้อมูลดิจิทัล หรือเมทาดาตา - กำหนดมาตรฐานของคำอธิบายชุดข้อมูลดิจิทัล หรือเมทาดาตา
สิ่งที่นำเข้า	คู่มือแนวปฏิบัติมาตรฐานการบริหารจัดการคำอธิบายชุดข้อมูลดิจิทัล หรือเมทาดาตา เช่น พจนานุกรมข้อมูล (Data Dictionary) การตั้งชื่อข้อมูล (Data Naming)
เครื่องมือที่ใช้	- เครื่องมือบริหารจัดการบัญชีข้อมูล (Data Catalog Management Tools) - เครื่องมือบริหารจัดการคำอธิบายชุดข้อมูลดิจิทัล หรือ เมทาดาตา (Metadata Repository Management Tools)
ผลที่ได้รับ	เมทาดาตาที่มีคุณภาพ มีความสอดคล้อง และความมั่นคงปลอดภัย
ผู้เกี่ยวข้อง	- บริกรข้อมูล (Data Stewards) - นักวิเคราะห์ข้อมูล (Data Analyst)

2.3.2.9 ความมั่นคงปลอดภัยและการรักษาความเป็นส่วนตัวของข้อมูล (Data Security and Privacy)

ความมั่นคงปลอดภัยของข้อมูล (Data Security) หมายถึง การป้องกันข้อมูลในบริบทของการรักษาความลับ ความถูกต้องของข้อมูล ความพร้อมใช้งานของข้อมูล จากข้อมูลของมาตรฐาน ISO/IEC27001 โดยมีรายละเอียด ดังนี้

- การรักษาความลับ (Confidentiality) หมายถึง การรักษาข้อมูลตามสภาพของการจัดชั้นความลับ และมีการกำหนดสิทธิ์การเข้าถึงข้อมูลนั้น เนื่องจากข้อมูลในหน่วยงานอาจมีหลายประเภท ข้อมูลบางประเภทเป็นข้อมูลที่มีความสำคัญ หรืออ่อนไหว จึงต้องมีการรักษาความลับเพื่อลดความเสี่ยงของการถูกคุกคาม และเป็นการป้องกันการรั่วไหลของข้อมูลโดยมิชอบ เช่น การส่งข้อมูลที่ปกปิดหรือเป็นความลับต้องมีวิธีการที่ทำให้ทราบได้ว่าบุคคลที่ต้องการส่งข้อมูลมาให้ หรือการที่ผู้ได้รับการอนุญาตให้เข้าถึงข้อมูลเท่านั้นที่สามารถอ่านข้อมูลได้

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

- ความพร้อมใช้งานของข้อมูล (Availability) หมายถึง การพร้อมในการใช้งานอยู่เสมอ กล่าวคือ ข้อมูลต้องพร้อมสำหรับการใช้งานได้เสมอ รวมถึงมีการสำรองข้อมูลไว้เมื่อเกิดภัยพิบัติหรือเหตุการณ์ที่ไม่คาดฝัน เช่น หากต้องการใช้ข้อมูล ผู้ใช้งานสามารถใช้ข้อมูลได้ทันที และใช้ได้อย่างต่อเนื่อง

โดยความมั่นคงปลอดภัยของข้อมูลต้องดำเนินการตั้งแต่การวางแผน การจัดทำ การปฏิบัติตาม และการบังคับใช้นโยบายและขั้นตอนด้านการรักษาความปลอดภัย เพื่อสนับสนุนในด้านที่เกี่ยวข้องกับการพิสูจน์ตัวตน การกำหนดสิทธิ์ การเข้าถึงข้อมูล การตรวจสอบ และความพร้อมใช้ของข้อมูลอย่างเหมาะสม

นอกจากนี้ ต้องมีการรักษาความเป็นส่วนบุคคลของข้อมูล (Data Privacy) ตั้งแต่การรวบรวม จัดเก็บ ใช้ เผยแพร่ หรือดำเนินการอื่นใดเกี่ยวกับข้อมูล โดยจะต้องมีการระบุวัตถุประสงค์เป็นหลักฐานให้ชัดเจน ห้ามมิให้มีการเปิดเผย หรือแสดง หรือทำให้ปรากฏในลักษณะอื่นใดที่ไม่สอดคล้องกับวัตถุประสงค์ เว้นแต่จะได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลนั้น ๆ หรือมีกฎหมายกำหนดให้สามารถกระทำสิ่งนั้นได้

ตารางที่ 12 สรุปการบริหารจัดการความมั่นคงปลอดภัยและการรักษาความเป็นส่วนตัวของข้อมูล

การบริหารจัดการความมั่นคงปลอดภัยและการรักษาความเป็นส่วนตัวของข้อมูล	
วิธีดำเนินการ	- กำหนดนโยบายและมาตรฐานด้านความปลอดภัยของข้อมูล - บริหารจัดการเกี่ยวกับข้อมูลตั้งแต่วิธีการจัดเก็บ การประมวลผล การเข้าถึงข้อมูล การนำไปใช้ การเปิดเผย และการทำลาย
สิ่งที่นำเข้า	- มาตรฐาน แนวปฏิบัติ และนโยบายที่เกี่ยวกับความปลอดภัยของข้อมูล - มาตรฐาน แนวปฏิบัติ และนโยบายที่เกี่ยวกับการรักษาความเป็นส่วนตัวของข้อมูล - มาตรฐานและหลักเกณฑ์การพิสูจน์และยืนยันตัวตนทางดิจิทัล
เครื่องมือที่ใช้	- ระบบการจัดการฐานข้อมูล (Database Management System - DBMS) - เทคโนโลยีจัดการข้อมูลเพื่อแสดงตัวตน (Identity Management Technology) - ระบบจัดการการเปลี่ยนแปลง (Change Control System) - หนังสือให้ความยินยอม (Letter of Consent)

ตารางที่ 12 สรุปการบริหารจัดการความมั่นคงปลอดภัยและการรักษาความเป็นส่วนตัวของข้อมูล (ต่อ)

การบริหารจัดการความมั่นคงปลอดภัย และการรักษาความเป็นส่วนตัวของข้อมูล	
ผลที่ได้รับ	- นโยบายด้านการรักษาความปลอดภัยและการรักษาความเป็นส่วนตัวของข้อมูล (Data Security and Privacy Policy) - มาตรฐานการจัดชั้นความลับของข้อมูล (Data Classification Standard)
ผู้เกี่ยวข้อง	- ผู้บริหารจัดการฐานข้อมูล (Database Administrator) - บริกรข้อมูล (Data Stewards) - ผู้ตรวจสอบภายใน (Internal Auditor)

2.3.2.10 คุณภาพของข้อมูล (Data Quality)

คุณภาพของข้อมูล (Data Quality) เป็นเครื่องมือในการวัดความน่าเชื่อถือและประสิทธิภาพของการนำข้อมูลไปใช้ ต้องมีการวางแผนการดำเนินการและการควบคุมกิจกรรมต่าง ๆ รวมถึงการปรับปรุง เพื่อให้ข้อมูลมีคุณภาพ เนื่องจากข้อมูลที่มีคุณภาพสูงทำให้การดำเนินงานของหน่วยงานเป็นไปอย่างมีประสิทธิภาพ การทำให้ข้อมูลมีคุณภาพ ประกอบด้วย การทำให้ข้อมูลมีความถูกต้อง (Accuracy) ข้อมูลมีความครบถ้วน (Completeness) ข้อมูลมีความตongกัน (Consistency) ข้อมูลมีความเป็นปัจจุบัน (Timeliness) ข้อมูลตรงตามความต้องการของผู้ใช้ (Relevancy) และข้อมูลมีความพร้อมใช้ (Availability) ดังแสดงรายละเอียดเพิ่มเติมในบทที่ 3.6.2 การประเมินคุณภาพของข้อมูล (Data Quality Assessment)

ตารางที่ 13 สรุปการบริหารจัดการคุณภาพของข้อมูล

การบริหารจัดการคุณภาพของข้อมูล	
วิธีดำเนินการ	- กำหนดข้อมูลที่ต้องมีคุณภาพ - พัฒนาและส่งเสริมการให้ความสำคัญกับคุณภาพของข้อมูล (Awareness) - กำหนดขอบเขตของ การประเมิน (Assessment) คุณภาพของข้อมูล - กำหนดและระบุลำดับความสำคัญ (Prioritize) ของการปรับปรุงข้อมูลให้มีคุณภาพ
สิ่งที่นำเข้า	- มาตรฐาน แนวปฏิบัติ และนโยบายที่เกี่ยวกับการทำให้ข้อมูลมีคุณภาพ เช่น การจัดทำโปรไฟล์ข้อมูล (Data Profiling) ดาตาคลีนซิง (Data Cleansing) - เมทาดาทาทั้งด้านธุรกิจและเทคโนโลยีสารสนเทศ
เครื่องมือที่ใช้	- เครื่องมือในการทำดาตาคลีนซิง (Data Cleansing Tools) - เครื่องมือวิเคราะห์ทางสถิติ (Statistical Analysis Tools)
ผลที่ได้รับ	- รายงานการรับรองคุณภาพของข้อมูล (Data Quality Certification Reports) - ข้อตกลงระดับคุณภาพของข้อมูล (Data Quality Service Level Agreements)
ผู้เกี่ยวข้อง	- นักวิเคราะห์ข้อมูล (Data Analyst) - บริกรข้อมูล (Data Stewards)

ทั้งนี้ระดับคุณภาพของข้อมูลในมุมมองของข้อมูลขนาดใหญ่ (Big Data) หรือวิทยาการข้อมูล (Data Science) มีความแตกต่างกับระดับคุณภาพข้อมูลทั่วไป เช่น ความพร้อมใช้ของผลการวิเคราะห์ที่ได้รับจากข้อมูลขนาดใหญ่ (Timely) ความเชื่อมั่นในผลการวิเคราะห์ (Reliable) ข้อมูลขนาดใหญ่มีความสัมพันธ์กับวัตถุประสงค์ของการวิเคราะห์หรือสิ่งที่ต้องการทำนาย (Meaningful) และความสามารถในการผลักดันผลการวิเคราะห์ถูกนำไปใช้ในสถานการณ์จริง (Sufficient) (Kim, H. Y., & Cho, J. S., 2017)

2.4 ความสัมพันธ์ระหว่างธรรมาภิบาลข้อมูลกับการบริหารจัดการข้อมูล

จากผลการศึกษาที่เกี่ยวข้องการบริหารจัดการข้อมูลของสมาคมบริหารจัดการข้อมูลระหว่างประเทศ (Data Management Association International) จะเห็นว่า ธรรมาภิบาลข้อมูล (Data Governance) เป็นส่วนที่สำคัญในการบริหารจัดการข้อมูล (Data Management) เป็นกลไกในการกำหนดทิศทางควบคุม และทวนสอบการบริหารจัดการข้อมูล เพื่อให้มั่นใจได้ว่าหน่วยงานได้ดำเนินการบริหารจัดการข้อมูลเป็นไปตามนโยบาย กฎ ระเบียบ หรือข้อบังคับที่ได้กำหนดไว้

ดังนั้นสิ่งที่ควรริเริ่มเป็นอันดับแรกของการวางแผนในการบริหารจัดการข้อมูล ก็คือ ธรรมาภิบาลข้อมูล เพราะเป็นเรื่องของการกำหนดบทบาทหน้าที่ ความรับผิดชอบ และการตัดสินใจ เพื่อสร้างความเชื่อมั่นว่าธรรมาภิบาลข้อมูล ความรับผิดชอบ และความเป็นเจ้าของหรือผู้มีส่วนได้เสียกับทรัพย์สินข้อมูลนั้นเป็นไปอย่างมีระเบียบ ถูกต้อง และมีความยั่งยืน โดยธรรมาภิบาลข้อมูลจะต้องเข้าไปมีส่วนร่วมในทุก ๆ องค์ประกอบหรือกิจกรรมของการบริหารจัดการข้อมูล

อย่างไรก็ตามการบริหารจัดการข้อมูลนั้นมีความหมายที่กว้างกว่าและเกี่ยวข้องกับแง่มุมของการใช้ข้อมูลและดำเนินงานในกระบวนการที่เกิดขึ้นซ้ำ ๆ ในแต่ละช่วงของระบบบริหารและกระบวนการจัดการข้อมูล หรือวงจรชีวิตของข้อมูล

ทั้งนี้หากภาครัฐมีธรรมาภิบาลข้อมูลที่ดีจะก่อให้เกิดการบริหารจัดการข้อมูลที่ดีเช่นกัน ส่งผลให้ข้อมูลมีความมั่นคงปลอดภัย มีคุณภาพ สามารถเปิดเผย เชื่อมโยง และแลกเปลี่ยนข้อมูลกันได้ มีคุณค่าทางเศรษฐกิจและสังคม และได้ รับความคุ้มค่าต่อการดำเนินงาน

ในบทที่ 3 จะกล่าวถึงรายละเอียดของกรอบธรรมาภิบาลข้อมูลภาครัฐ (Data Governance Framework for Government) สำหรับหน่วยงานภาครัฐ

บทที่ 3

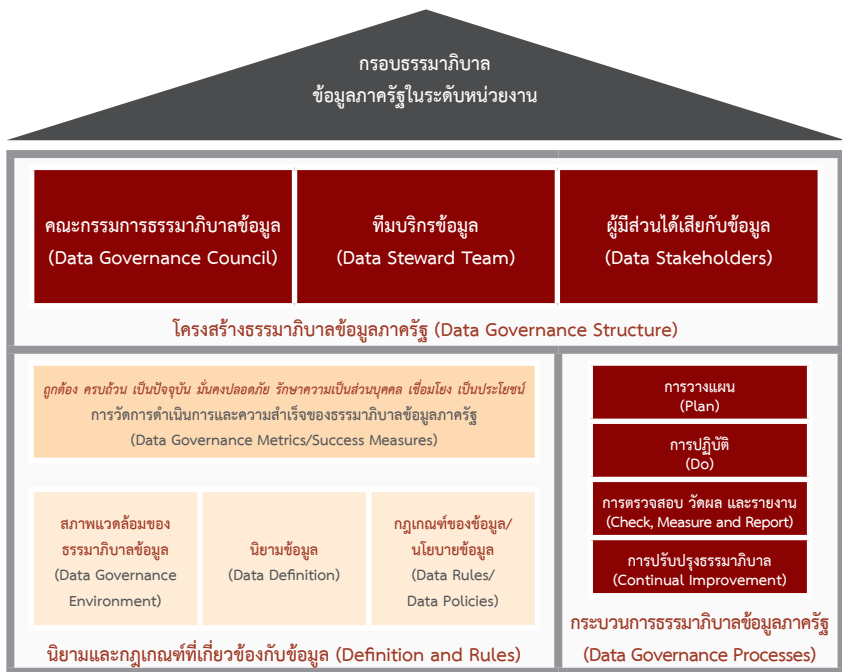
กรอบธรรมาภิบาล

ข้อมูลภาครัฐ

(DATA GOVERNANCE
FRAMEWORK FOR GOVERNMENT)



กรอบธรรมาภิบาลข้อมูลภาครัฐประกอบด้วยองค์ประกอบต่าง ๆ ผนวกเข้าด้วยกัน ทั้งในด้านของนิยามและกฎเกณฑ์ที่เกี่ยวข้องกับข้อมูล บุคคล และกระบวนการ ซึ่งองค์ประกอบเหล่านี้มีความสำคัญที่ก่อให้เกิดประสิทธิภาพและประสิทธิผลในการดำเนินงาน อันจะนำไปสู่การบรรลุเป้าหมายในการดำเนินงานตามที่กำหนดไว้ โดยสรุปรายละเอียดดังรูปที่ 9



รูปที่ 9 กรอบธรรมาภิบาลข้อมูลภาครัฐในระดับหน่วยงาน

จากรูปที่ 9 แสดงกรอบธรรมาภิบาลข้อมูลภาครัฐในระดับหน่วยงาน ประกอบด้วย นิยามและกฎเกณฑ์ที่เกี่ยวข้องกับข้อมูล (Definition and Rules) โครงสร้างธรรมาภิบาลข้อมูลภาครัฐ (Data Governance Structure) และ กระบวนการธรรมาภิบาลข้อมูลภาครัฐ (Data Governance Processes)

โดยบุคคลต่าง ๆ ที่เกี่ยวข้องกับโครงสร้างธรรมาภิบาลข้อมูลภาครัฐ จะถูกแต่งตั้งโดยผู้บริหารระดับสูงของหน่วยงาน เพื่อทำหน้าที่กำหนดยุทธศาสตร์และเป้าหมาย ตรวจสอบสภาพแวดล้อมของธรรมาภิบาลข้อมูล นิยามความหมายและขอบเขตของข้อมูล กำหนดกฎเกณฑ์และนโยบายข้อมูล และดำเนินการตรวจสอบการปฏิบัติตามกฎเกณฑ์และนโยบายข้อมูล ดังนี้

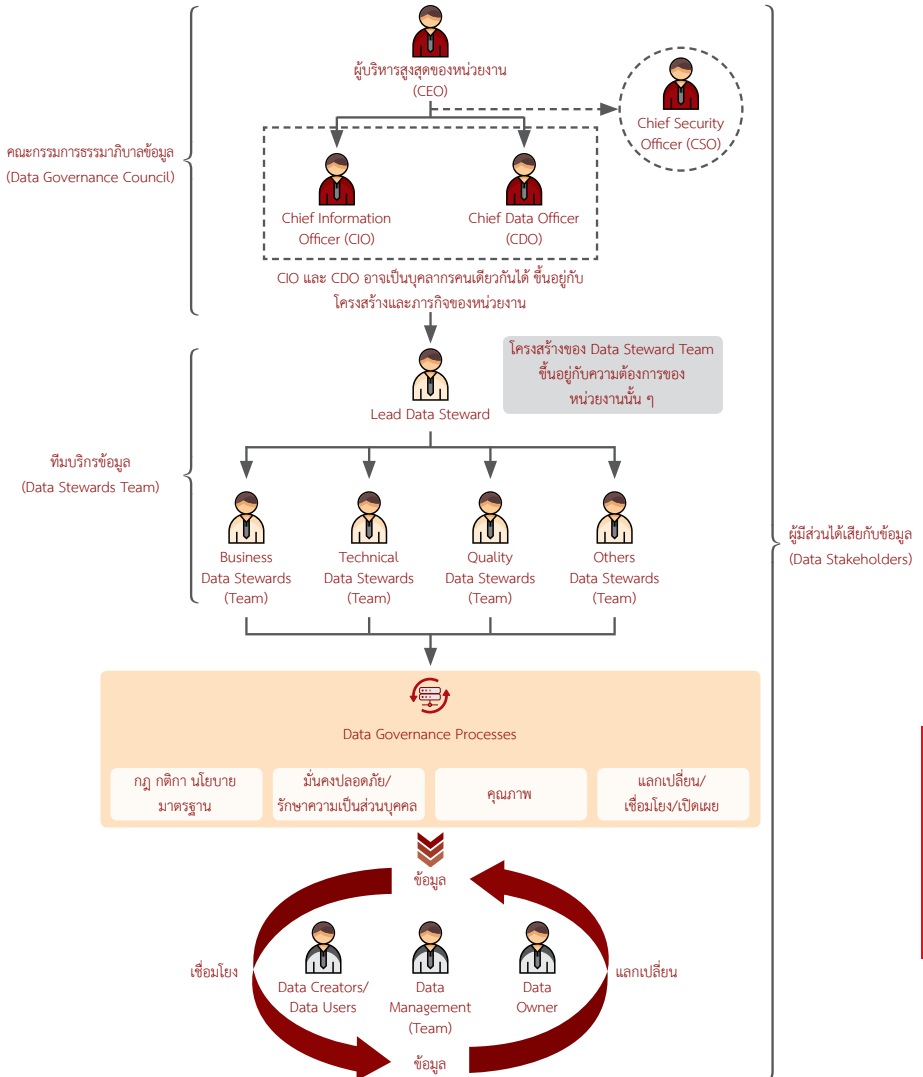
3.1 โครงสร้างธรรมาภิบาลข้อมูลภาครัฐ

(Data Governance Structure)

3.1.1 โครงสร้างของบุคลากรที่รับผิดชอบในธรรมาภิบาลข้อมูลภาครัฐ

(Data Governance Structure)

การกำหนดโครงสร้างธรรมาภิบาลข้อมูลภาครัฐเพื่อแสดงลำดับชั้นระหว่างกลุ่มบุคคลที่เกี่ยวข้องกับธรรมาภิบาลข้อมูลภาครัฐ และแสดงถึงสิทธิในการสั่งการตามลำดับชั้น ทั้งนี้จำนวนบุคลากรและความลึกของลำดับชั้นให้พิจารณาตามความเหมาะสมของแต่ละหน่วยงานของรัฐ หน่วยงานของรัฐสามารถจัดตั้งส่วนงานธรรมาภิบาลข้อมูลในรูปแบบที่แตกต่างกัน ได้แก่ (1) รูปแบบทีมเสมือน (Virtual Team) ที่คัดเลือกมาจากส่วนงานต่าง ๆ (2) รูปแบบที่มีส่วนงานรับผิดชอบชัดเจนซึ่งอาจจะจัดตั้งใหม่หรือกำหนดหน้าที่ให้กับส่วนงานที่มีหน้าที่คล้ายกับโครงสร้าง และ (3) รูปแบบผสมซึ่งจะต้องแยกหน้าที่ให้ชัดเจนระหว่างส่วนงานที่รับผิดชอบหลักกับทีมเสมือน รูปที่ 10 แสดงตัวอย่างโครงสร้างธรรมาภิบาลข้อมูลภาครัฐ ซึ่งแบ่งออกเป็น 3 ส่วน ประกอบด้วย (1) คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council) (2) ทีมบริการข้อมูล (Data Steward Team) และ (3) ผู้มีส่วนได้เสียกับข้อมูล (Data Stakeholders)



รูปที่ 10 ตัวอย่างโครงสร้างธรรมาภิบาลข้อมูลภาครัฐภายในหน่วยงาน

คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council) ประกอบไปด้วย ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer) ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer) ผู้บริหารข้อมูลระดับสูง (Chief Data Officer) ผู้บริหารด้านการรักษาความปลอดภัยระดับสูง (Chief Security Officer) ผู้บริหารจากส่วนงานต่าง ๆ ทั้งจากฝ่ายบริหารและฝ่ายเทคโนโลยีสารสนเทศ รวมไปถึงหัวหน้าทีมบริการข้อมูล (Lead Data Steward) คณะกรรมการธรรมาภิบาลข้อมูลมีอำนาจสูงสุดในธรรมาภิบาลข้อมูลภายในหน่วยงานภาครัฐ ซึ่งทำหน้าที่ตัดสินใจเชิงนโยบาย แก้ไขปัญหาและบริหารจัดการภายในคณะกรรมการธรรมาภิบาลข้อมูล ทั้งนี้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงอาจจะทำหน้าที่แทนผู้บริหารข้อมูลระดับสูง ซึ่งขึ้นอยู่กับความพร้อมของหน่วยงาน

ผู้บริหารข้อมูลระดับสูง (Chief Data Officer) มีหน้าที่นำข้อมูลและวิเคราะห์ข้อมูลของหน่วยงานภาครัฐเพื่อสร้างและส่งมอบเทคโนโลยี เครื่องมือ แนวทาง และวิธีการในการทำให้ข้อมูลของหน่วยงานภาครัฐมีคุณค่าและเกิดประโยชน์สูงสุดต่อหน่วยงานภาครัฐ เพื่อขยายผลต่อไปให้เกิดผลสัมฤทธิ์ในการส่งเสริมให้หน่วยงานภาครัฐต่าง ๆ ใช้ข้อมูลได้อย่างถูกต้องและมีประสิทธิภาพ นอกจากนี้ยังต้องวิเคราะห์และร่วมกับผู้บริหารส่วนอื่น ๆ เพื่อจัดทำยุทธศาสตร์และดำเนินการธรรมาภิบาลข้อมูลภาครัฐให้มีคุณภาพและการควบคุมอื่น ๆ เพื่อรักษาความสมบูรณ์ของข้อมูลของหน่วยงานภาครัฐ และนำแนวปฏิบัติและมาตรฐานของหน่วยงานภาครัฐไปปรับปรุงข้อมูลและยุทธศาสตร์ของประเทศ โดยในส่วนของการทำงานในระดับประเทศ ผู้บริหารข้อมูลระดับสูง จะต้องทำหน้าที่เป็นตัวกลางระหว่างหน่วยงานภาครัฐในการแลกเปลี่ยน เชื่อมโยงข้อมูล รวมไปถึงการจัดการความเสี่ยงที่อาจเกิดจากข้อมูลของหน่วยงานภาครัฐ

รวมถึงส่งเสริมนวัตกรรมที่ใช้ประโยชน์จากข้อมูลในการวิเคราะห์ปัญหา เพื่อแก้ไขจนสามารถลดปัญหาของประเทศที่เกิดขึ้นในปัจจุบัน และลดความเสี่ยงของปัญหาที่อาจเกิดขึ้นในอนาคตได้ พร้อมทั้งต้องวิเคราะห์หาเทคโนโลยีใหม่ ๆ มาใช้ในการวิเคราะห์ข้อมูลให้ตอบสนองความต้องการของประชาชนด้วย

ในบางหน่วยงาน กรณีที่ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงมีหน้าที่และความรับผิดชอบใกล้เคียงหรือสามารถทำหน้าที่ของผู้บริหารข้อมูลระดับสูงได้ ดังนั้นผู้บริหารเทคโนโลยีสารสนเทศระดับสูง และผู้บริหารข้อมูลระดับสูงจึงสามารถเป็นบุคคลเดียวกันได้ ผู้บริหารด้านการรักษาความปลอดภัยระดับสูง (Chief Security Officer) เป็นผู้บริหารที่มีบทบาทสูงสุดในการทำให้หน่วยงานภาครัฐมีความปลอดภัยเพียงพอสำหรับการทำงานทั้งด้านการบริหารจัดการดูแลและด้านข้อมูลทำให้เกิดการเชื่อมต่อระหว่างหน่วยงานภาครัฐ ตัวอย่างเช่น หน่วยงานภาครัฐไม่มีความกังวลเกี่ยวกับช่องโหว่ด้านความปลอดภัย ทำให้การทำงานของหน่วยงานภาครัฐเป็นไปได้อย่างราบรื่น ดังนั้นการมีผู้บริหารด้านการรักษาความปลอดภัยระดับสูงที่ดี สามารถลดความหวาดระแวงในการทำงานระหว่างส่วนงานต่าง ๆ ทำให้เพิ่มมูลค่าให้กับหน่วยงานภาครัฐได้ ดังนั้นหน้าที่หลักของผู้บริหารด้านการรักษาความปลอดภัยระดับสูง คือ การปรับปรุงความมั่นคงทางกายภาพและความปลอดภัยด้านเทคโนโลยีให้มากขึ้น รวมถึงต้องมีการทำงานร่วมกับผู้บริหารอื่น ๆ ในการตัดสินใจเกี่ยวกับลำดับความสำคัญของความต้องการด้านความปลอดภัย เพื่อกำหนดเป้าหมายและวัตถุประสงค์ของการป้องกันหน่วยงานเพื่อให้สอดคล้องกับแผนกลยุทธ์ของหน่วยงาน นอกจากนี้ยังต้องดูแลเครือข่ายของคณะกรรมการ ผู้บริหาร ผู้จัดการ และเจ้าหน้าที่รักษาความปลอดภัยและทำงานร่วมกับหน่วยงานด้านความมั่นคงในท้องถิ่น และหน่วยงานรักษาความปลอดภัยอื่น ๆ

ทีมบริการข้อมูล (Data Steward Team) ประกอบไปด้วย หัวหน้าบริการข้อมูล (Lead Data Steward) บริการข้อมูลด้านธุรกิจ (Business Data Stewards) บริการข้อมูลด้านเทคนิค (Technical Data Stewards) บริการข้อมูลด้านคุณภาพข้อมูล (Data Quality Stewards) รวมไปถึงบุคคลที่ทำหน้าที่เกี่ยวกับความมั่นคงปลอดภัย กฎหมาย และบุคคลที่ให้ความรู้เกี่ยวกับนโยบายข้อมูลและความรู้อื่น ๆ ที่จะสนับสนุนให้เกิดธรรมาภิบาลข้อมูลภาครัฐที่ดีภายในหน่วยงานภาครัฐ ทีมบริการข้อมูลรับคำสั่งโดยตรงจากคณะกรรมการธรรมาภิบาลข้อมูล ในขณะที่เดียวกันมีการให้ข้อมูลสนับสนุนในการตัดสินใจต่อคณะกรรมการธรรมาภิบาลข้อมูล โดยบริการข้อมูลด้านธุรกิจเป็นผู้ให้การสนับสนุนด้านธุรกิจ ขณะที่บริการข้อมูลด้านเทคนิคเป็นผู้ให้การสนับสนุนด้านเทคโนโลยีสารสนเทศ อย่างไรก็ตามบริการข้อมูลด้านธุรกิจและบริการข้อมูลด้านเทคนิคอาจจะเป็นบุคคลเดียวกัน ซึ่งขึ้นอยู่กับคุณสมบัติของบุคคลหรือความเหมาะสมของหน่วยงานรัฐ

หัวหน้าบริการข้อมูลทำหน้าที่เป็นผู้ควบคุมและสั่งการภายในทีมบริการข้อมูล และเป็นหนึ่งในคณะกรรมการธรรมาภิบาลข้อมูล

นอกเหนือจากคณะกรรมการธรรมาภิบาลข้อมูลและทีมบริการข้อมูล ยังมีผู้มีส่วนได้เสียกับข้อมูล (Data Stakeholders) อื่น ๆ ซึ่งทำหน้าที่ให้การสนับสนุนธรรมาภิบาลข้อมูลภาครัฐต่อทีมบริการข้อมูลและคณะกรรมการธรรมาภิบาลข้อมูล ประกอบไปด้วย เจ้าของข้อมูล (Data Owners) ทีมบริหารจัดการข้อมูล (Data Management Team) ผู้สร้างข้อมูล (Data Creators) และผู้ใช้ข้อมูล (Data Users) สำหรับรายละเอียดของบทบาทและความรับผิดชอบภายในโครงสร้างธรรมาภิบาลข้อมูลภาครัฐได้แสดงไว้ในหัวข้อถัดไป

3.1.2 บทบาทและความรับผิดชอบ (Roles and Responsibilities)

บทบาท (Roles) และความรับผิดชอบ (Responsibilities) ที่เหมาะสมจะนำไปสู่การดำเนินงานที่มีประสิทธิภาพและประสิทธิผลต่อหน่วยงาน ซึ่งการกำหนดบทบาทและความรับผิดชอบจะต้องไม่ขัดแย้งต่อกฎ ระเบียบ ข้อบังคับ หรือกฎหมาย รวมทั้งกำหนดสิทธิ หน้าที่ และความรับผิดชอบ ในการบริหารจัดการข้อมูลที่อยู่ในความครอบครองหรือควบคุมให้มีความชัดเจน โดยอาจแต่งตั้งหรือมอบหมายเจ้าหน้าที่เป็นรายบุคคลหรือคณะบุคคล ให้ความรับผิดชอบ และประกาศให้ผู้ที่เกี่ยวข้องหรือประชาชนรับทราบด้วยว่า เป็นไปตามที่กำหนดไว้ตามกฎหมายว่าด้วยการนั้น มีรายละเอียดดังนี้

ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer) ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer) และผู้บริหารข้อมูลระดับสูง (Chief Data Officer) คือ บุคคลที่ทำหน้าที่ กำหนดวิสัยทัศน์ ให้ข้อเสนอแนะ และอนุมัตินโยบายข้อมูล มาตรฐานข้อมูล แนวทางปฏิบัติงาน เกณฑ์การวัดคุณภาพ ระเบียบ และข้อบังคับอื่น ๆ ที่เกี่ยวข้องกับการจัดการข้อมูล รวมไปถึงการจัดลำดับความสำคัญและแก้ไขปัญหาที่เกี่ยวข้องกับข้อมูล

บริกรข้อมูลด้านธุรกิจ (Business Data Stewards) คือ บุคคลที่ทำหน้าที่รับผิดชอบในการนิยามความต้องการด้านคุณภาพและความมั่นคงปลอดภัย ซึ่งอาจจะได้รับมาจากผู้ใช้ข้อมูล (Data Users) หรือผู้มีส่วนได้เสียอื่น ๆ นิยามคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตาโดยการสนับสนุนจากผู้เชี่ยวชาญสถาปนิกข้อมูล (Data Architects) และนักวิเคราะห์ระบบ (System Analyst) ร่างนโยบายข้อมูลด้วยการช่วยเหลือจากทีมบริหารจัดการข้อมูล (Data Management Team) ตรวจสอบการปฏิบัติตามนโยบายข้อมูล ตรวจสอบคุณภาพ ตรวจสอบความมั่นคงปลอดภัยของข้อมูล วิเคราะห์ผลจากการตรวจสอบ

แล้วรายงานผลลัพธ์ไปยังคณะกรรมการธรรมาภิบาลข้อมูลและผู้ที่เกี่ยวข้องอื่น ๆ ให้ทราบ บริการข้อมูลด้านธุรกิจมักจะเป็นบุคคลที่มาจากฝ่ายธุรกิจแต่มีความเข้าใจด้านเทคโนโลยีสารสนเทศ

บริการข้อมูลด้านเทคนิค (Technical Data Stewards) คือ บุคคลที่ทำหน้าที่ให้การสนับสนุนด้านเทคโนโลยีสารสนเทศแก่บริการข้อมูลด้านธุรกิจ เช่น นิยามเมทาเดตาเชิงเทคนิคซึ่งอาจจะได้รับการช่วยเหลือจากทีมบริหารจัดการข้อมูล ให้ข้อเสนอแนะเชิงเทคนิคในการร่างนโยบายข้อมูล ตรวจสอบคุณภาพข้อมูล ความมั่นคงปลอดภัยของข้อมูล และการปฏิบัติตามนโยบายข้อมูลในเชิงเทคนิค ทั้งนี้บริการข้อมูลด้านเทคนิคมักจะเป็นบุคคลฝ่ายเทคโนโลยีสารสนเทศแต่มีความเข้าใจเกี่ยวกับธุรกิจ

บริการข้อมูลด้านคุณภาพข้อมูล (Data Quality Stewards) คือ บุคคลที่ทำหน้าที่ดำเนินการในเรื่องคุณภาพข้อมูล เช่น กำหนดนโยบายข้อมูลด้านคุณภาพ การตรวจวัดคุณภาพข้อมูล และการวิเคราะห์คุณภาพข้อมูล นอกจากนี้หน่วยงานอาจจะกำหนดบริการข้อมูลด้านอื่น ๆ เพื่อดูแลเรื่องต่าง ๆ โดยเฉพาะ เช่น บริการข้อมูลด้านความมั่นคงปลอดภัย บริการข้อมูลด้านการอบรม และให้ความรู้

เจ้าของข้อมูล (Data Owners) คือ บุคคลที่ทำหน้าที่รับผิดชอบดูแลข้อมูลโดยตรง สร้างความมั่นใจได้ว่าการบริหารจัดการข้อมูลสอดคล้องกับนโยบาย มาตรฐาน กฎระเบียบ หรือกฎหมาย เจ้าของข้อมูลทำการทบทวนและอนุมัติการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับข้อมูล เช่น การเปลี่ยนแปลงเมทาเดตาและเกณฑ์การทำดาตาคลีนซิง (Data Cleansing) นอกจากนี้

ยังมีหน้าที่ในการให้สิทธิในการเข้าถึงข้อมูลและจัดชั้นความลับของข้อมูล เจ้าของข้อมูลมักจะอยู่ในตำแหน่งบริหาร เช่น ผู้อำนวยการฝ่ายหรือหัวหน้าส่วนงานบุคคลเป็นเจ้าของข้อมูลบุคคล ผู้อำนวยการฝ่ายหรือหัวหน้าส่วนงานการเงินเป็นเจ้าของข้อมูลการเงิน

ทีมบริหารจัดการข้อมูล (Data Management Team) มีหน้าที่หลักในการบริหารจัดการข้อมูลให้สอดคล้องกับ 10 องค์ประกอบ ตามรายละเอียดในหัวข้อ 2.3.2 องค์ประกอบในการบริหารจัดการข้อมูล ซึ่งมักจะเป็นเจ้าหน้าที่ภายในฝ่ายเทคโนโลยีสารสนเทศของหน่วยงาน ประกอบด้วย สถาปนิกข้อมูล (Data Architects) นักจัดการฐานข้อมูล (Database Administrators - DBA) นักวิเคราะห์ข้อมูล (Data Analysts) และนักวิทยาศาสตร์ข้อมูล (Data Scientists) ตรวจสอบการปฏิบัติตามนโยบายข้อมูล ทีมบริหารจัดการข้อมูลสนับสนุนกิจกรรมของธรรมาภิบาลข้อมูลภาครัฐ เช่น ช่วยเหลือในการนิยามเมทาดาตา ร่างนโยบายข้อมูลและมาตรฐานข้อมูล และกำหนดสิทธิการเข้าถึงข้อมูลโดย DBA

ผู้สร้างข้อมูล (Data Creators) คือ บุคคลที่ทำหน้าที่ บันทึก แก้ไข ปรับปรุง หรือลบข้อมูลให้สอดคล้องกับโครงสร้างที่ถูกกำหนดไว้ นอกจากนี้ยังมีหน้าที่ในการทำงานร่วมกับบริการข้อมูล เพื่อตรวจสอบและแก้ไขปัญหาด้านคุณภาพข้อมูลและความมั่นคงปลอดภัย

ผู้ใช้ข้อมูล (Data Users) คือ บุคคลที่ทำหน้าที่นำข้อมูลไปใช้งานทั้งในระดับปฏิบัติงานและระดับบริหาร และสนับสนุนธรรมาภิบาลข้อมูลภาครัฐโดยการให้ความต้องการในการใช้ข้อมูล พร้อมทั้งรายงานประเด็นปัญหาที่พบระหว่างการใช้ข้อมูล ทั้งด้านคุณภาพและความปลอดภัยของข้อมูลไปยังบริการข้อมูล

3.2 กระบวนการธรรมาภิบาลข้อมูลภาครัฐ (Data Governance Processes)

หลักพื้นฐานของการกำหนดกระบวนการและผลที่ได้รับ ตามลำดับขั้นตอนของข้อมูลหรือระบบบริหารและกระบวนการจัดการข้อมูล (วงจรชีวิตของข้อมูล) เริ่มตั้งแต่ การสร้างข้อมูล การจัดเก็บข้อมูล การใช้ข้อมูล การเผยแพร่ข้อมูล การจัดเก็บข้อมูลถาวร จนถึงการทำลายข้อมูลนั้น ประกอบด้วย การเลือกข้อมูล เพื่อดำเนินการธรรมาภิบาล การระบุเป้าหมาย การกำหนดมาตรฐาน และแนวปฏิบัติ รวมถึงการบริหารจัดการคน

1) การเลือกข้อมูลเพื่อดำเนินการธรรมาภิบาล ได้แก่ ข้อมูลส่วนบุคคล ข้อมูลความมั่นคง ข้อมูลความลับทางราชการ และข้อมูลสาธารณะ โดยกระบวนการซึ่งได้มาด้วยข้อมูลนั้นสามารถใช้วิธีการ เช่น กระบวนการวิศวกรรมย้อนกลับ (Reverse Engineering) การวิเคราะห์ข้อมูล (Data Analysis) การสำรวจข้อมูล (Survey)

2) การระบุเป้าหมาย ต้องพิจารณาครอบคลุมในประเด็น ดังต่อไปนี้ เป็นอย่างน้อย คือ คุณภาพข้อมูล การเข้าถึงและการจัดการ ความปลอดภัย และความเป็นส่วนตัว การปฏิบัติตามระเบียบและกฎหมาย ต้นทุนและประสิทธิภาพ

3) การกำหนดมาตรฐานและแนวปฏิบัติ เป็นการกำหนดมาตรฐานโดยทั่วไป แนวทางที่ใช้ เช่น การตั้งชื่อ คุณภาพของข้อมูล การโอนย้ายข้อมูล กระบวนการที่เกี่ยวข้องกับข้อมูล (Create Read Update Delete - CRUD) การเก็บข้อมูลถาวร (Archive)

4) การบริหารจัดการคน เช่น การสร้างวัฒนธรรมองค์กร การบริหารจัดการแรงงาน การสื่อสารที่ชัดเจน การสร้างความพึงพอใจกับผู้ที่มีส่วนได้เสีย การใช้ประโยชน์จากเทคโนโลยี ซึ่งจะช่วยให้การดำเนินงานสำเร็จลุล่วงได้ดี

3.2.1 กระบวนการธรรมาภิบาลข้อมูลภาครัฐ (Data Governance Processes)

กระบวนการธรรมาภิบาลข้อมูลภาครัฐ เป็นขั้นตอนที่ใช้สำหรับกำกับดูแล การดำเนินการใด ๆ ต่อข้อมูลให้เป็นไปตาม กฎ ระเบียบ ข้อบังคับ หรือนโยบาย ที่เกี่ยวข้องกับข้อมูล กระบวนการธรรมาภิบาลข้อมูลภาครัฐ เริ่มตั้งแต่ การวางแผนไปจนถึงการปรับปรุงอย่างต่อเนื่อง ดังนี้



รูปที่ 11 กระบวนการธรรมาภิบาลข้อมูลภาครัฐ

1) การวางแผน (Plan)

การวางแผนเริ่มตั้งแต่กำหนดวิสัยทัศน์และประเด็นปัญหา ซึ่งเป็นส่วนที่สำคัญเนื่องจากเป็นจุดเริ่มต้นที่จะกำหนด กฎระเบียบ นโยบาย มาตรฐาน หรือแนวทางปฏิบัติต่าง ๆ เพื่อใช้ในธรรมาภิบาลข้อมูลและการบริหารจัดการข้อมูล หลังจากที่ได้มีการกำหนดวิสัยทัศน์และประเด็นปัญหาที่ชัดเจนแล้ว ขั้นตอนถัดไป คือ การกำหนดขอบเขตการดำเนินการ ระยะเวลาดำเนินการ บุคคลที่เกี่ยวข้อง และต้นทุนที่ใช้ในการดำเนินงาน หลังจากนั้นนำแผนงาน กฎระเบียบ และนโยบายที่เกี่ยวข้องไปประกาศใช้อย่างเป็นทางการ

2) การปฏิบัติ (Do)

การปฏิบัติในที่นี้หมายถึงการดำเนินการใด ๆ ของบุคคลที่เกี่ยวข้องกับการบริหารจัดการข้อมูลและผู้ที่เกี่ยวข้องอื่น ๆ เช่น สถาปนิกข้อมูล นักออกแบบข้อมูล นักจัดการฐานข้อมูล วิศวกรข้อมูล นักวิเคราะห์ข้อมูล นักวิทยาการข้อมูล เจ้าของข้อมูล เจ้าของข้อมูลส่วนบุคคล ผู้สร้างข้อมูล ผู้บริหาร ผู้ใช้ข้อมูล ซึ่งต้องดำเนินการให้สอดคล้องกับกฎระเบียบ นโยบาย มาตรฐาน และแนวปฏิบัติที่ได้กำหนดไว้ ขณะที่บริกรข้อมูลจะให้ความรู้และสนับสนุนให้บุคคลที่เกี่ยวข้องสามารถปฏิบัติตามกฎระเบียบเหล่านั้น ทั้งนี้รายงานความก้าวหน้า ผลการปฏิบัติงาน และประเด็นปัญหาที่พบระหว่างปฏิบัติงาน จะถูกรายงานไปยังคณะกรรมการธรรมาภิบาลข้อมูล

3) การตรวจสอบ วัดผล และรายงาน (Check, Measure and Report)

ในการตรวจสอบบริกรข้อมูลจะดำเนินการตรวจสอบความสอดคล้องกันระหว่างกฎระเบียบ นโยบาย และมาตรฐานที่กำหนด กับการปฏิบัติงานของบุคคลที่เกี่ยวข้องกับการบริหารจัดการข้อมูลและผู้ที่เกี่ยวข้องอื่น ๆ พร้อมทั้งทำการวัดผลด้านคุณภาพข้อมูล หลังจากนั้นรายงานผลความสอดคล้อง

คุณภาพข้อมูล ความมั่นคงปลอดภัย และความเสี่ยงที่เกี่ยวข้องกับข้อมูลไปยัง คณะกรรมการธรรมาภิบาลข้อมูลและผู้ที่เกี่ยวข้อง เพื่อให้ทราบถึงผลการดำเนินงานและประเด็นปัญหาที่พบ

4) การปรับปรุงอย่างต่อเนื่อง (Continual Improvement)

ธรรมาภิบาลข้อมูลภาครัฐเป็นสิ่งที่ต้องดำเนินการอย่างต่อเนื่องตลอดระบบบริหารและกระบวนการจัดการข้อมูล หรือวงจรชีวิตของข้อมูล ทั้งนี้สภาพแวดล้อมหรือกฎหมายที่เปลี่ยนแปลง รายการความต้องการจากผู้บริหารและผู้มีส่วนได้เสีย รวมไปถึงผลการตรวจสอบ เช่น รายงานผลการตรวจสอบความสอดคล้องของการดำเนินงานต่อนโยบายข้อมูล รายงานคุณภาพข้อมูล รายงานความมั่นคงปลอดภัย รายงานความเสี่ยงต่อข้อมูล จะถูกใช้สำหรับการปรับปรุงกระบวนการธรรมาภิบาลข้อมูลภาครัฐ นโยบาย กฎ ระเบียบ ข้อบังคับที่เกี่ยวข้องกับข้อมูล เกณฑ์การประเมินความพร้อมของธรรมาภิบาลข้อมูลภาครัฐ เกณฑ์การวัดระดับคุณภาพข้อมูล และโครงสร้างธรรมาภิบาลข้อมูลภาครัฐ

3.2.2 แนวทางการจัดการกระบวนการธรรมาภิบาลข้อมูลภาครัฐ (Data Governance Process Guidelines)

แนวทางการจัดการกระบวนการธรรมาภิบาลข้อมูลภาครัฐจะช่วยให้เข้าใจถึงกระบวนการและสามารถนำไปประยุกต์ใช้ได้อย่างมีประสิทธิภาพ ซึ่งชี้ให้เห็นถึงความสัมพันธ์ระหว่างกระบวนการธรรมาภิบาลข้อมูล เครื่องมือ หรือเอกสารที่ใช้ในธรรมาภิบาลข้อมูล ผลลัพธ์ที่ได้จากธรรมาภิบาลข้อมูล และผู้ที่เกี่ยวข้องหรือผู้มีส่วนได้เสีย ดังแสดงในตารางที่ 14 แสดงตัวอย่างแผนภาพการดำเนินการธรรมาภิบาลข้อมูลภาครัฐ ดังแสดงในรูปที่ 12 และแสดงความสัมพันธ์ระหว่างกระบวนการ/กิจกรรม และผู้มีส่วนได้เสีย ดังแสดงในตารางที่ 15

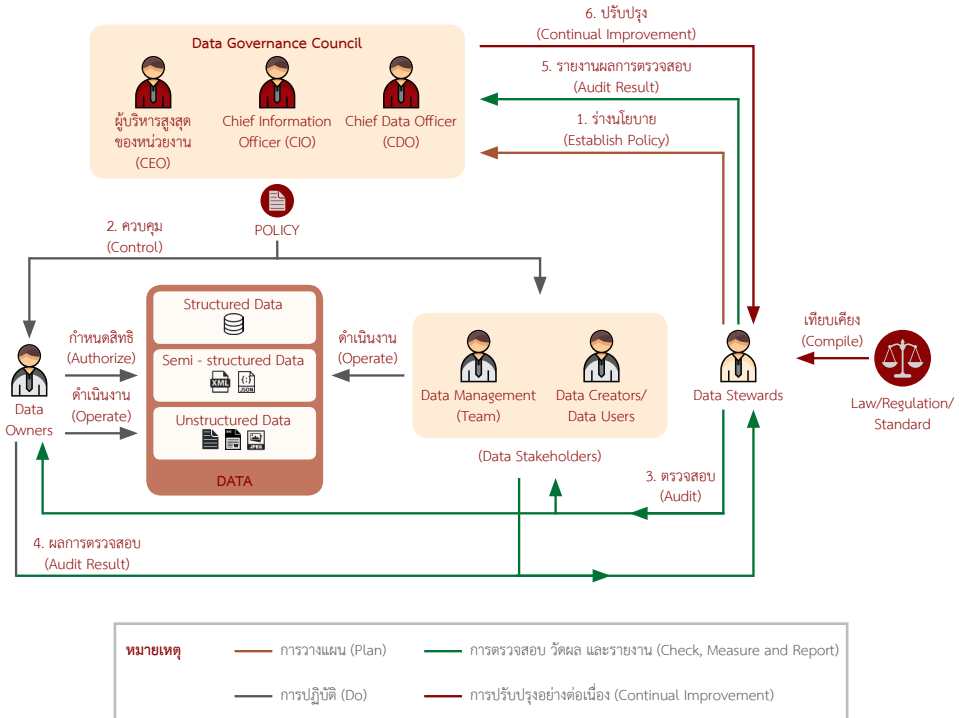
ตารางที่ 14 ความสัมพันธ์ระหว่างกระบวนการ ส่วนนำเข้า ส่วนนำออก และผู้มีส่วนได้เสียกับข้อมูล

กระบวนการ (Processes)	ส่วนนำเข้า (Input)	ส่วนนำออก (Output)	ผู้มีส่วนได้เสียกับข้อมูล (Data Stakeholder)
1 การวางแผน	(1) นโยบาย กฎ ระเบียบ ข้อบังคับ และกฎหมายที่เกี่ยวข้องกับข้อมูล (2) รายการชุดข้อมูล (3) รายการประเด็นปัญหาจากรายงานผลการตรวจสอบความสอดคล้องของการดำเนินงานต้นนโยบาย ข้อมูลรายงานคุณภาพข้อมูล รายงานความมั่นคงปลอดภัยต่อข้อมูล และรายงานความเสี่ยงต่อข้อมูล	(1) แผนดำเนินการ (ขอบเขต เวลา กลุ่มธรรมาภิบาลข้อมูล และต้นทุน)	(1) ผู้บริหารข้อมูลระดับสูง หรือผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (2) คณะกรรมการธรรมาภิบาลข้อมูล (3) บริการข้อมูลด้านธุรกิจ (4) บริการข้อมูลด้านเทคนิค (5) บริการข้อมูลด้านคุณภาพ
2 การปฏิบัติ	(1) นโยบาย กฎ ระเบียบ ข้อบังคับ และกฎหมายที่เกี่ยวข้องกับข้อมูล (2) แผนดำเนินการ (ขอบเขต เวลา และต้นทุน)	(1) รายงานความก้าวหน้าในการปฏิบัติงาน (2) ผลการปฏิบัติงาน (3) ประเด็นปัญหาที่พบบ่อยระหว่างปฏิบัติงาน	(1) ผู้บริหารงาน (2) ผู้ปฏิบัติงานที่เกี่ยวข้อง (3) บริการข้อมูลด้านธุรกิจ (4) บริการข้อมูลด้านเทคนิค (5) บริการข้อมูลด้านคุณภาพ

ตารางที่ 14 ความสัมพันธ์ระหว่างกระบวนการ ส่วนนำเข้า ส่วนนำออก และผู้มีส่วนได้เสียกับข้อมูล (ต่อ)

กระบวนการ (Processes)	ส่วนนำเข้า (Input)	ส่วนนำออก (Output)	ผู้มีส่วนได้เสียกับข้อมูล (Data Stakeholder)
3 การตรวจสอบ วัตถุ และ รายงาน	(1) นโยบาย กฎ ระเบียบ ข้อบังคับ และกฎหมายที่เกี่ยวข้องกับข้อมูล (2) เกณฑ์การประเมินความพร้อมของธรรมาภิบาลข้อมูลภาครัฐ ระดับคุณภาพข้อมูล	(1) รายงานผลการตรวจสอบความสอดคล้องของการดำเนินงานต่อนโยบายข้อมูล (2) รายงานคุณภาพข้อมูล รายงานความมั่นคงปลอดภัยข้อมูล และรายงานความเสี่ยงต่อข้อมูล	(1) บริกรข้อมูลด้านธุรกิจ (2) บริกรข้อมูลด้านเทคนิค (3) บริกรข้อมูลด้านคุณภาพ
4 การปรับปรุงธรรมาภิบาล	(1) นโยบาย กฎ ระเบียบ ข้อบังคับ และกฎหมายที่เกี่ยวข้องกับข้อมูล (2) โครงสร้างธรรมาภิบาลข้อมูลภาครัฐ (3) เกณฑ์การประเมินความพร้อมของธรรมาภิบาลข้อมูลภาครัฐ และระดับคุณภาพข้อมูล (4) รายงานผลการตรวจสอบความสอดคล้องของการดำเนินงานต่อนโยบายข้อมูล รายงานความมั่นคงปลอดภัยต่อข้อมูล และรายงานความเสี่ยงต่อข้อมูล (5) รายการความต้องการจากผู้บริหารและผู้มีส่วนได้เสีย	(1) กระบวนการธรรมาภิบาลข้อมูลภาครัฐ (2) นโยบาย กฎ ระเบียบ ข้อบังคับ และกฎหมาย ที่เกี่ยวข้องกับข้อมูล (3) เกณฑ์การประเมินความพร้อมของธรรมาภิบาลข้อมูลภาครัฐ และระดับคุณภาพข้อมูล (4) โครงสร้างธรรมาภิบาลข้อมูลภาครัฐ	(1) ผู้บริหารข้อมูลระดับสูงหรือผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (2) คณะกรรมการธรรมาภิบาลข้อมูล (3) บริกรข้อมูลด้านธุรกิจ (4) บริกรข้อมูลด้านเทคนิค (5) บริกรข้อมูลด้านคุณภาพ

รูปที่ 12 แสดงขั้นตอนการตรวจสอบความสอดคล้องระหว่างนโยบาย ข้อมูลกับการดำเนินงานของผู้ที่เกี่ยวข้องกับธรรมาภิบาลข้อมูลภาครัฐ และความสอดคล้องระหว่างนโยบายข้อมูลกับกฎหมาย



รูปที่ 12 ตัวอย่างแผนภาพการดำเนินการธรรมาภิบาลข้อมูลภาครัฐ

จากรูปที่ 12 แสดงให้เห็นตัวอย่างของการดำเนินการธรรมาภิบาลข้อมูลภาครัฐว่าบริการข้อมูล (Data Stewards) ทั้งด้านธุรกิจและด้านเทคนิคเป็นผู้ร่างนโยบายข้อมูล (Data Policies) ให้สอดคล้องกับกฎหมายหรือข้อกำหนดอื่น ๆ ที่เกี่ยวข้อง และนำเสนอคณะกรรมการธรรมาภิบาลข้อมูลซึ่งประกอบไปด้วย CEO CIO CDO และ/หรือผู้บริหารทั้งฝ่ายบริหารและฝ่ายเทคโนโลยีสารสนเทศพิจารณากำหนดนโยบายเพื่อควบคุมให้เจ้าของข้อมูล (Data Owners) และผู้มีส่วนได้เสียกับข้อมูลอื่น ๆ (Data Stakeholders) มีหน้าที่ในการปฏิบัติตามนโยบายข้อมูลที่กำหนดไว้

เจ้าของข้อมูลเป็นผู้กำหนดสิทธิการเข้าถึงและดำเนินงานใด ๆ กับข้อมูลที่ตนเป็นเจ้าของ ทั้งข้อมูลที่มีโครงสร้าง (เช่น ฐานข้อมูล) ข้อมูลกึ่งโครงสร้าง (เช่น Extensible Markup Language-XML) ข้อมูลที่ไม่มีโครงสร้าง (เช่น เสียง ภาพ ภาพเคลื่อนไหว) ขณะที่ผู้มีส่วนได้เสียกับข้อมูล เช่น ผู้บริหารจัดการฐานข้อมูล (Database Administrators) และผู้ใช้ข้อมูล (Data Users) ต้องดำเนินการกับข้อมูลให้สอดคล้องกับสิทธิที่ได้รับจากเจ้าของข้อมูล เช่น การเพิ่ม ลบ แก้ไข ประมวลผล นำไปใช้ แลกเปลี่ยน เผยแพร่ข้อมูล โดยมีบริการข้อมูลเป็นผู้ตรวจสอบความสอดคล้องกันของการดำเนินงานตามนโยบายข้อมูล ทั้งจากเจ้าของข้อมูลและผู้มีส่วนได้เสียกับข้อมูล พร้อมทั้งรายงานการตรวจสอบการดำเนินงานให้กับคณะกรรมการธรรมาภิบาลข้อมูลทราบ ทั้งนี้ คณะกรรมการธรรมาภิบาลข้อมูลต้องทบทวนนโยบายข้อมูล และผลการดำเนินงานจากรายงานการตรวจสอบเพื่อการปรับปรุง และกำหนดแนวทางในการธรรมาภิบาลที่มีประสิทธิภาพต่อไป

ตารางที่ 15 ความสัมพันธ์ระหว่างกระบวนการ/กิจกรรม และผู้มีส่วนได้เสียกับข้อมูล

กระบวนการ/กิจกรรม	ผู้มีส่วนได้เสียกับข้อมูล				
	คณะกรรมการ ธรรมาภิบาลข้อมูล	ทีมบริการข้อมูล	เจ้าของข้อมูล	ทีมบริหารจัดการ ข้อมูล	ผู้สร้างและใช้งาน ข้อมูล
กำหนดและปรับปรุงนโยบาย และมาตรฐานข้อมูล	A	R	S	S/C	S
ตรวจสอบการปฏิบัติตาม นโยบายข้อมูล	I	R	S	S/C	S
การประเมินความพร้อมของ ธรรมาภิบาลข้อมูลภาครัฐ	I	R	S	S	S
ประเมินความมั่นคงปลอดภัย และคุณภาพข้อมูล	I	R	S	S/C	S
รายงานผลการตรวจสอบ ความมั่นคงปลอดภัย และ คุณภาพข้อมูล	I	R	I	I	I
กำหนดสิทธิในการเข้าถึง ข้อมูล	I	R	A	S/C	I

หมายเหตุ : Responsible = ดำเนินการหลัก

Accountable = อนุมัติ

Support = ให้การสนับสนุน

Consulted = ให้คำปรึกษา

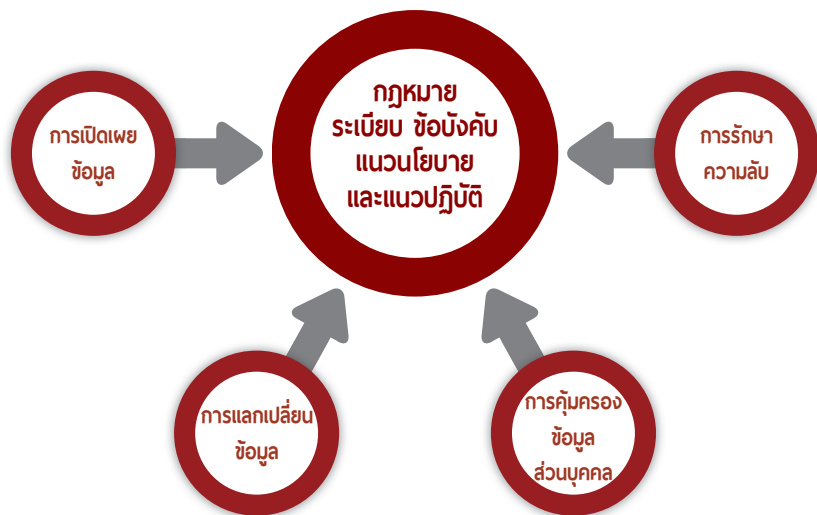
Informed = รับทราบข้อมูล

ตารางที่ 15 แสดงความสัมพันธ์ระหว่างกระบวนการ/กิจกรรม และ ผู้มีส่วนได้เสียกับข้อมูล โดย R หมายถึง ผู้มีหน้าที่ในการปฏิบัติงานตาม กระบวนการหรือกิจกรรมที่กำหนดไว้ A หมายถึง ผู้มีหน้าที่ในการทบทวนและ อนุมัติผลที่ได้รับจากปฏิบัติงาน S หมายถึง ผู้มีหน้าที่ในการสนับสนุนหรือ ให้การช่วยเหลือต่อการปฏิบัติงาน C หมายถึง ผู้มีหน้าที่ให้คำปรึกษาต่อผู้ปฏิบัติงาน และ I หมายถึง ผู้มีหน้าที่รับทราบผลการปฏิบัติงาน

3.3 สภาพแวดล้อมของธรรมาภิบาลข้อมูล (Data Governance Environment)

3.3.1 กฎหมาย ระเบียบ ข้อบังคับ แนวนโยบาย และแนวปฏิบัติที่เกี่ยวข้อง กับธรรมาภิบาลข้อมูลภาครัฐ

ปัจจุบันกฎหมายที่เกี่ยวข้องกับข้อมูล ข่าวสาร หรือสิทธิส่วนบุคคลในประเทศไทย มีประเด็นที่อาจส่งผลกระทบต่อหลักแนวคิดธรรมาภิบาลข้อมูลภาครัฐ ซึ่งหากหน่วยงานในประเทศไทยต้องการสร้างหรือปรับปรุงระบบภายในให้มี ธรรมาภิบาลข้อมูลภาครัฐ จะต้องพิจารณาประเด็นหลัก ๆ ที่เกี่ยวข้องกับ กฎหมาย ดังนี้



รูปที่ 13 กฎหมาย ระเบียบ ข้อบังคับ นโยบาย และแนวปฏิบัติที่เกี่ยวข้องกับธรรมาภิบาลข้อมูลภาครัฐ

1) การเปิดเผยข้อมูล

การเปิดเผยข้อมูลเป็นสิ่งจำเป็นต่อการดำเนินงานของรัฐบาล ซึ่งแสดงความโปร่งใสในการดำเนินงานและความสามารถในการตรวจสอบได้จากภาคเอกชนและประชาชน รวมไปถึงการสนับสนุนให้ภาคเอกชนและประชาชนนำข้อมูลที่เปิดเผยไปสร้างนวัตกรรมด้านผลิตภัณฑ์และบริการ เพื่อยกระดับการพัฒนาประเทศ โดยแนวคิดการเปิดเผยข้อมูลเป็นที่ยอมรับของหน่วยงานระหว่างประเทศและรัฐบาลประเทศต่าง ๆ โดยในประเทศไทยมีกฎหมายที่เกี่ยวข้องกับการเปิดเผยข้อมูลดังนี้

- รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560 ในมาตราที่ 59 ได้ระบุว่า รัฐต้องเปิดเผยข้อมูลหรือข่าวสารสาธารณะในครอบครองของหน่วยงานของรัฐที่มีใช้ข้อมูลเกี่ยวกับความมั่นคงของรัฐหรือเป็นความลับของทางราชการ

- พระราชบัญญัติ (พ.ร.บ.) การบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 โดยมีการเปิดเผยข้อมูลหรือข่าวสารสาธารณะที่หน่วยงานของรัฐจัดทำและครอบครองในรูปแบบและช่องทางดิจิทัล เพื่อให้ประชาชนเข้าถึงโดยสะดวก มีส่วนร่วมและตรวจสอบการดำเนินงานของรัฐ และสามารถนำข้อมูลไปพัฒนาบริการและนวัตกรรมที่จะเป็นประโยชน์ต่อประเทศในด้านต่าง ๆ
- พระราชบัญญัติ (พ.ร.บ.) ข้อมูลข่าวสารของทางราชการ พ.ศ. 2540 โดยมี 3 ประเด็นที่เกี่ยวกับการเปิดเผยข้อมูล ได้ถูกระบุไว้ใน พ.ร.บ. ฉบับนี้ ได้แก่
 - ข้อมูลภาครัฐ ต้อง “เปิดเผยเป็นหลัก ปกปิดเป็นข้อยกเว้น”
 - กำหนดหลักเกณฑ์และกลไกการเปิดเผยข้อมูล
 - กำหนดประเภทข้อมูลที่เปิดเผยได้และเปิดเผยไม่ได้
- แนวทางปฏิบัติการเปิดเผยข้อมูลภาครัฐ (Government Open Data Publication Guidelines) ให้แนวทางปฏิบัติเพื่อการเปิดเผยข้อมูลภาครัฐ ซึ่งมีวัตถุประสงค์เพื่อเป็นแนวปฏิบัติสำหรับการเปิดเผยข้อมูลภาครัฐ¹ ได้แก่
 - แนวปฏิบัติและมาตรฐานเชิงเทคนิค เพื่อให้หน่วยงานภาครัฐนำไปใช้เป็นแนวปฏิบัติในการดำเนินการเกี่ยวกับการเปิดเผยข้อมูลของหน่วยงานให้เป็นไปในทิศทางเดียวกัน รวมถึงการกำหนดมาตรฐานเชิงเทคนิค รูปแบบวิธีการเผยแพร่ข้อมูลผ่านศูนย์กลางข้อมูลเปิดภาครัฐ หรือ data.go.th และการกำหนดสัญญาอนุญาต (License) ที่เหมาะสมสำหรับข้อมูลเปิดภาครัฐ

¹ <https://data.go.th/Documents.aspx>

- แบบฟอร์มคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตา เพื่อเป็นตัวอย่างการจัดทำคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตา โดยหน่วยงานสามารถนำไปประยุกต์ใช้งานที่เหมาะสมกับหน่วยงานได้
- คู่มือการเปิดเผยข้อมูล (Open Data Handbook) เพื่อสร้างความรู้ความเข้าใจให้แก่หน่วยงานภาครัฐ ภาคเอกชน และผู้ที่ต้องการศึกษาเกี่ยวกับข้อมูลเปิด (Open Data)
- คู่มือการนำข้อมูลขึ้นเผยแพร่บน data.go.th เพื่อให้ผู้ใช้งานสามารถศึกษาทำความเข้าใจการทำงานต่าง ๆ ของระบบได้ และสามารถตรวจสอบปัญหาที่เกิดจากการใช้งานและสามารถแก้ปัญหาในขั้นต้นได้
- คู่มือแสดงรายการชุดข้อมูลที่สำคัญ เพื่อเป็นการสร้างแหล่งข้อมูลที่ใช้ประกอบในการใช้งานที่เกี่ยวกับชุดข้อมูลที่สำคัญให้แก่หน่วยงานภาครัฐ ภาคเอกชน และผู้ที่ต้องการศึกษาเกี่ยวกับข้อมูลเปิด (Open Data)
- แนวปฏิบัติในการออกแบบความคิดเชิงนวัตกรรม (Data Innovation Guideline) เป็นคู่มือที่ช่วยให้เข้าใจปัญหาที่แท้จริง และสามารถออกแบบแนวทางแก้ไขปัญหาที่เป็นแนวคิดเชิงนวัตกรรมตลอดจนสามารถเข้าถึงชุดข้อมูล (Datasets) ต่าง ๆ เพื่อให้ได้มาซึ่งแนวทางในการแก้ปัญหา นอกจากนี้ผู้ที่ต้องการศึกษากระบวนการออกแบบนวัตกรรมสามารถนำไปประยุกต์หรือปรับใช้กับหน่วยงานได้

2) การเชื่อมโยงและแลกเปลี่ยนข้อมูล

การเชื่อมโยงและแลกเปลี่ยนข้อมูลเป็นสิ่งสำคัญต่อการบูรณาการ การดำเนินงานระหว่างหน่วยงานภาครัฐ ซึ่งเป็นประโยชน์ต่อหน่วยงานภาครัฐ และประชาชนในการขอใช้บริการจากภาครัฐ โดยมีกฎหมายที่เกี่ยวข้องกับการ เชื่อมโยงและแลกเปลี่ยนข้อมูล ดังนี้

- พระราชบัญญัติ (พ.ร.บ.) การบริหารงานและการให้บริการภาครัฐ ผ่านระบบดิจิทัล พ.ศ. 2562 โดยมีการพัฒนามาตรฐาน หลักเกณฑ์ และวิธีการ เกี่ยวกับดิจิทัล และพัฒนาโครงสร้างพื้นฐานด้านดิจิทัลที่จำเป็น ให้เป็นไปตาม มาตรฐานสากล เพื่อสร้างและพัฒนากระบวนการทำงานของหน่วยงานของรัฐ ให้มีความสอดคล้องและมีการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างกัน รวมทั้ง มีความมั่นคงปลอดภัยและน่าเชื่อถือ โดยมีการบูรณาการและสามารถทำงานร่วมกันอย่างเป็นเอกภาพ เกิดการพัฒนาการบริการภาครัฐที่มีประสิทธิภาพและนำไปสู่การบริหารราชการและการบริการประชาชนแบบบูรณาการ รวมทั้งให้ประชาชนเข้าถึงโดยสะดวก

- ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่ จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการใช้ข้อความ XML สำหรับการ แลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ระหว่างหน่วยงาน² มีวัตถุประสงค์ในการ สนับสนุนการใช้ข้อความ XML สำหรับการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ให้ มีความมั่นคงปลอดภัยและน่าเชื่อถือ รวมทั้งให้ผู้ประกอบการและหน่วยงาน ต่าง ๆ ได้มีแนวทางในการสร้างเอกสารอิเล็กทรอนิกส์ให้อยู่ในรูปแบบข้อความ XML ให้เป็นมาตรฐานเดียวกัน

² <https://standard.etda.or.th/wp-content/uploads/2017/08/20170523-ER-eDocumentStandard-V08-14F-0816.pdf>

- ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จําเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยรหัสสถานที่ออกหนังสือ³ ให้ข้อเสนอแนะสำหรับการกำหนดรหัสสถานที่ออกหนังสือรับรอง ซึ่งจะส่งผลให้ทราบที่มาของหนังสือรับรองและการอำนวยความสะดวกทางการค้า พร้อมการบริหารจัดการ มาตรฐานการแลกเปลี่ยนข้อมูลสารสนเทศด้านการค้าระหว่างประเทศผ่านระบบ National Single Window ให้เป็นไปในทิศทางเดียวกัน

3) การคุ้มครองข้อมูลส่วนบุคคล

การคุ้มครองข้อมูลส่วนบุคคล (Privacy Data Protection) เป็นสิ่งสำคัญที่ภาครฐต้องดำเนินการ โดยปัจจุบันมีการนำระบบสารสนเทศและการสื่อสารมาประยุกต์ใช้ประกอบการทำธุรกรรมทางอิเล็กทรอนิกส์อย่างแพร่หลาย ซึ่งหน่วยงานภาครฐอาจจะมีการรวบรวม จัดเก็บ ใช้ หรือเผยแพร่ข้อมูลส่วนบุคคลของผู้ใช้บริการในรูปของข้อมูลอิเล็กทรอนิกส์ เพื่อเป็นการป้องกันการละเมิดข้อมูลส่วนบุคคล ซึ่งเป็นสิทธิขั้นพื้นฐานสำคัญในความเป็นส่วนบุคคล (Privacy Right) ของประชาชนที่ต้องได้รับการคุ้มครอง อันจะทำให้ประชาชนมีความมั่นใจในการทำธุรกรรมทางอิเล็กทรอนิกส์ ดังนั้นการคุ้มครองข้อมูลส่วนบุคคลจําเป็นที่จะต้องนำมาวิเคราะห์เพื่อให้เกิดธรรมาภิบาลข้อมูลภาครฐที่ดี โดยมีกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล ดังนี้

- พระราชบัญญัติ (พ.ร.บ.) ข้อมูลข่าวสารของทางราชการ พ.ศ. 2540 กำหนดประเภทข้อมูลที่เปิดเผยได้และเปิดเผยไม่ได้ ซึ่งเป็นสิ่งที่จําเป็นต้องมีการพิจารณาในกรณีที่เป็นข้อมูลส่วนบุคคล เนื่องจากข้อมูลที่เป็นข้อมูลส่วนบุคคลจําเป็นต้องได้รับการคุ้มครองอย่างมีหลักเกณฑ์

³ <https://standard.etda.or.th/wp-content/uploads/2017/05/20170526-ER-CertificationLocations-V08-08F-0529.pdf>

- พระราชบัญญัติ (พ.ร.บ.) คัดกรองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้มีการกำหนดหลักเกณฑ์ กลไก และมาตรการที่กำกับดูแลเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล
- ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ (คธอ.) เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2553 ได้ระบุเรื่องการคุ้มครองข้อมูลส่วนบุคคลไว้ว่า “กำหนดให้ภาครัฐที่ให้บริการทางอิเล็กทรอนิกส์ต้องมีนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล”
- แนวปฏิบัติในการปกป้องข้อมูลที่ระบุตัวบุคคลได้ (Guideline to Protect the Personally Identifiable Information) ให้แนวปฏิบัติสำหรับหน่วยงานในการเตรียมข้อมูลให้เหมาะสมต่อการบูรณาการข้อมูลเข้าด้วยกัน โดยการนำเสนอขั้นตอนในการดำเนินการปกป้องข้อมูลที่ระบุตัวบุคคลได้นอกจากนั้นนำเสนอวิธีการเชื่อมโยงข้อมูลแบบรวมชุดข้อมูล (Integrated Datasets) การเชื่อมโยงข้อมูลผ่านตัวแบบข้อมูล (Data Model Market Place) และการเชื่อมโยงข้อมูลแบบกลุ่ม (Batch)

4) การรักษาความลับ

การรักษาความลับทางราชการเป็นสิ่งที่จำเป็นต่อการดำเนินงานของหน่วยงานภาครัฐ ซึ่งเป็นการป้องกันความเสียหายที่จะเกิดขึ้นต่อภาครัฐ ทั้งในด้านชื่อเสียง การเงิน ความสามารถในการพัฒนาประเทศ และความมั่นคงของประเทศ โดยมีกฎหมาย ระเบียบที่เกี่ยวข้องกับการรักษาความลับ ดังนี้

- พระราชบัญญัติ (พ.ร.บ.) ข้าราชการแห่งชาติ พ.ศ. 2562 ได้กำหนดข้อมูลข่าวสารที่สำนักข้าราชการแห่งชาติได้รับมาเนื่องจากการปฏิบัติหน้าที่ตาม พ.ร.บ. นี้ จะเปิดเผยมิได้ เว้นแต่เป็นการเปิดเผยต่อหน่วยข้าราชการหน่วยงานความมั่นคง นายกรัฐมนตรี หรือตามคำสั่งศาล ที่จะนำมาพิจารณาในธรรมาภิบาลข้อมูลภาครัฐ

- ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม ได้มีข้อกำหนดที่เกี่ยวข้องกับธรรมาภิบาลข้อมูลภาครัฐ ได้กำหนดนิยามข้อมูลข่าวสารลับ และกำหนดหลักเกณฑ์และวิธีการในการรักษาความลับของหน่วยงานภาครัฐ

- แนวทางปฏิบัติในการรักษาความปลอดภัยเกี่ยวกับบุคคล เอกสาร และสถานที่ที่จัดทำขึ้นจากระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. 2552 ควรนำมาพิจารณาในธรรมาภิบาลข้อมูลภาครัฐ

นอกจากการพิจารณากฎหมาย ระเบียบ และข้อบังคับที่มีอยู่ในปัจจุบัน หน่วยงานต้องพิจารณากฎหมาย ระเบียบ นโยบาย หรือ พ.ร.บ. ซึ่งมีกฎหมายที่เกี่ยวข้องกับเรื่องธรรมาภิบาลข้อมูลภาครัฐอีกด้วย ดังนี้

- 1) พระราชบัญญัติ (พ.ร.บ.) การบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 โดยกำหนดให้หน่วยงานรัฐจัดให้มีการบริหารงานและการจัดทำบริการสาธารณะในรูปแบบและช่องทางดิจิทัล โดยมีการบริหารจัดการและบูรณาการข้อมูลภาครัฐและการทำงานให้มีความสอดคล้องกันและเชื่อมโยงเข้าด้วยกันอย่างมั่นคงปลอดภัยและมีธรรมาภิบาล โดยมีมุ่งหมายในการเพิ่มประสิทธิภาพและอำนวยความสะดวกในการให้บริการและเข้าถึง

ประชาชน และในการเปิดเผยข้อมูลภาครัฐต่อสาธารณะและสร้างการมีส่วนร่วมของทุกภาคส่วน

2) พระราชบัญญัติ (พ.ร.บ.) การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ได้กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมและกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ต้องดำเนินการตามมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อรักษาสถานะของข้อมูล คอมพิวเตอร์หรือระบบคอมพิวเตอร์

3) ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ (ครอ.) เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555 โดยกำหนดให้มีมาตรฐานการรักษาความมั่นคงปลอดภัย การเข้าถึงข้อมูลสารสนเทศ ในระดับเคร่งครัด ระดับกลาง หรือระดับพื้นฐาน ให้หน่วยงานหรือองค์กร หรือส่วนงานของหน่วยงานหรือองค์กรปฏิบัติตาม มาตรฐาน

3.3.2 หลักการของสภาพแวดล้อมและวัฒนธรรมของหน่วยงานที่เอื้อต่อการมีธรรมาภิบาลข้อมูลภาครัฐ

ธรรมาภิบาลข้อมูลภาครัฐมีองค์ประกอบหลายอย่างที่สนับสนุนให้เกิดธรรมาภิบาลข้อมูลภาครัฐที่ดี ในขณะเดียวกันจะต้องคำนึงถึงข้อจำกัดที่อาจส่ง ผลในเชิงลบต่อการปรับเปลี่ยนหรือปฏิรูปให้เกิดธรรมาภิบาลข้อมูลภาครัฐ ในหน่วยงานด้วย วัฒนธรรมองค์กร และสภาพแวดล้อมเป็นหนึ่งในข้อจำกัดที่ อาจส่งผลต่อการเปลี่ยนแปลงในธรรมาภิบาลข้อมูลภายในหน่วยงานได้ เนื่องจาก แต่ละหน่วยงานล้วนมีวัฒนธรรมองค์กรและสภาพแวดล้อมที่แตกต่างกัน

ดังนั้นการตระหนักถึงวัฒนธรรมองค์กรและสภาพแวดล้อมที่แตกต่างกันมีความจำเป็นต่อการกำหนดโครงสร้าง นโยบาย บทบาทหน้าที่ การดำเนินงานที่เอื้อต่อธรรมาภิบาลข้อมูลภาครัฐ ตั้งแต่เริ่มต้น นอกจากนี้ยังต้องมีมาตรการรองรับกรณีที่มีการปรับเปลี่ยนโครงสร้างองค์กร เนื่องจากหากมีการปรับเปลี่ยนโครงสร้างองค์กร ธรรมาภิบาลข้อมูลภาครัฐก็จะเปลี่ยนตามไปด้วย

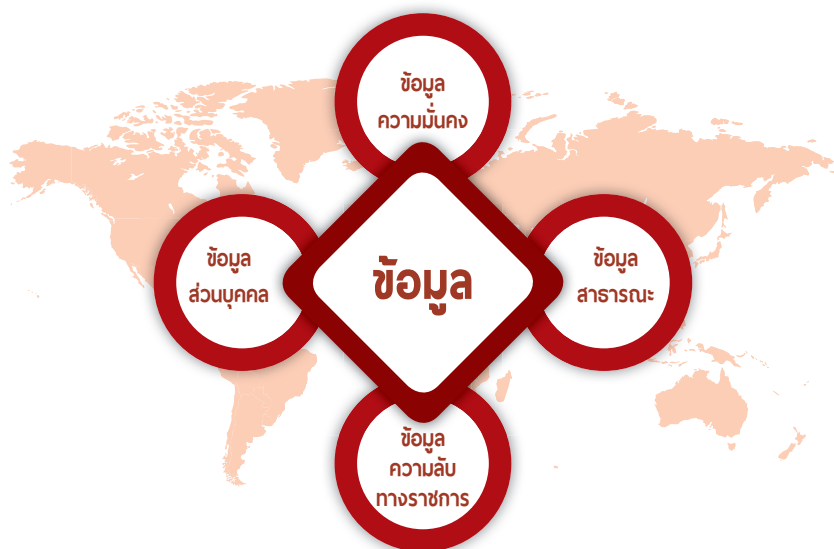
3.4 การนิยามข้อมูล

(Data Definition)

การนิยามข้อมูลต้องมีความถูกต้องและชัดเจน เพื่อสร้างความเข้าใจที่ตรงกันระหว่างผู้ที่เกี่ยวข้อง ทั้งนี้การจัดหมวดหมู่ของข้อมูลทำให้มองเห็นถึงภาพรวมของข้อมูล ขณะที่การทำเมทาเดตาเพื่อสร้างความเข้าใจต่อข้อมูลมากยิ่งขึ้น โดยมีรายละเอียดดังนี้

3.4.1 หมวดหมู่ของข้อมูล (Data Category)

ข้อมูลแบ่งออกได้เป็น 4 หมวดหมู่ ดังนี้



รูปที่ 14 หมวดหมู่ของข้อมูล

1) ข้อมูลส่วนบุคคล มีนิยามและที่มา ดังนี้

“ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ (พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562)

“ข้อมูลข่าวสารส่วนบุคคล” หมายความว่า ข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของบุคคล เช่น การศึกษา ฐานะการเงิน ประวัติสุขภาพ ประวัติอาชญากรรม หรือประวัติการทำงานบรรดาที่มีชื่อของผู้นั้น หรือมีเลขหมาย รหัส หรือสิ่งบอกลักษณะอื่นที่ทำให้รู้ตัวผู้นั้นได้ เช่น ลายพิมพ์นิ้วมือ แผ่นบันทึก ลักษณะเสียงของคนหรือรูปถ่าย และให้หมายความรวมถึงข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของผู้ที่ถึงแก่กรรมแล้วด้วย (พ.ร.บ. ข้อมูลข่าวสารของทางราชการ พ.ศ. 2540)

จากนิยามข้างต้น จึงได้ข้อสรุปว่า **ข้อมูลส่วนบุคคล** คือ **“ข้อมูลเกี่ยวกับสิ่งเฉพาะตัวของบุคคล ที่ทำให้สามารถระบุตัวหรือรู้ตัวของบุคคลนั้น ๆ ได้ ไม่ว่าจะเป็นข้อมูลการศึกษา ประวัติสุขภาพ ลายพิมพ์นิ้วมือ เป็นต้น”**

2) ข้อมูลความมั่นคง มีนิยามและที่มา ดังนี้

มาตรา 59 รัฐต้องเปิดเผยข้อมูลหรือข่าวสารสาธารณะในครอบครองของหน่วยงานของรัฐที่มีใช้ข้อมูลเกี่ยวกับความมั่นคงของรัฐหรือเป็นความลับของทางราชการตามที่กฎหมายบัญญัติ และต้องจัดให้ประชาชนเข้าถึงข้อมูลหรือข่าวสารดังกล่าวได้โดยสะดวก (รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560)

จากนิยามข้างต้น จึงได้ข้อสรุปว่า ข้อมูลความมั่นคง คือ “ข้อมูลเกี่ยวกับความมั่นคงของรัฐ ที่ทำให้เกิดความสงบเรียบร้อย การมีเสถียรภาพความเป็นปึกแผ่น ปลอดภัยจากภัยคุกคาม เป็นต้น”

3) ข้อมูลความลับทางราชการ มีนิยามและที่มา ดังนี้

“ข้อมูลข่าวสารลับ” หมายความว่า ข้อมูลข่าวสารตามมาตรา 14 หรือ มาตรา 15 ที่มีคำสั่งไม่ให้เปิดเผยและอยู่ในความครอบครองหรือควบคุมดูแลของหน่วยงานของรัฐ ไม่ว่าจะเป็นเรื่องที่เกี่ยวข้องกับการดำเนินงานของรัฐหรือที่เกี่ยวกับเอกชน ซึ่งมีการกำหนดให้มีชั้นความลับเป็น ชั้นลับ ชั้นลับมาก หรือ ชั้นลับที่สุด ตามระเบียบนี้โดยคำนึงถึงการปฏิบัติหน้าที่ของหน่วยงานของรัฐ และประโยชน์แห่งรัฐประกอบกัน (ระเบียบว่าด้วยการรักษาความลับของราชการ พ.ศ. 2544)

“สิ่งที่เป็นความลับของทางราชการ” หมายความว่า ข้อมูลข่าวสาร บริภัณฑ์ ยุทธรณ์ที่สงวน การรหัส ประมวลลับ และสิ่งอื่นใดบรรดาที่ถือว่าเป็นความลับของทางราชการ (ระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. 2552)

“ข้อมูลข่าวสารของราชการ” หมายความว่า ข้อมูลข่าวสารที่อยู่ในครอบครองหรือควบคุมดูแลของหน่วยงานของรัฐไม่ว่าจะเป็นข้อมูลข่าวสารเกี่ยวกับการดำเนินงานของรัฐหรือข้อมูลข่าวสารเกี่ยวกับเอกชน (พ.ร.บ. ข้อมูลข่าวสารของราชการ พ.ศ. 2540)

จากนิยามข้างต้น จึงได้ข้อสรุปว่า ข้อมูลความลับทางราชการ คือ “ข้อมูลที่อยู่ในความครอบครองหรือควบคุมดูแลของหน่วยงานของรัฐ ที่มีคำสั่งไม่ให้มีการเปิดเผย และมีการกำหนดชั้นความลับของข้อมูล”

4) ข้อมูลสาธารณะ มีนิยามและที่มา ดังนี้

มาตรา 59 รัฐต้องเปิดเผยข้อมูลหรือข่าวสารสาธารณะในครอบครองของหน่วยงานของรัฐที่มีใช้ข้อมูลเกี่ยวกับความมั่นคงของรัฐหรือเป็นความลับของทางราชการตามที่กฎหมายบัญญัติ และต้องจัดให้ประชาชนเข้าถึงข้อมูลหรือข่าวสารดังกล่าวได้โดยสะดวก (รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560)

“ข้อมูลข่าวสารสาธารณะ” หมายความว่า ข้อมูลข่าวสารของราชการที่หน่วยงานของรัฐต้องเปิดเผยให้ประชาชนได้รับรู้ รับทราบ หรือตรวจสอบได้โดยไม่จำเป็นต้องร้องขอ (ร่าง พรบ. ข้อมูลข่าวสารของราชการ)

จากนิยามข้างต้น จึงได้ข้อสรุปว่า ข้อมูลสาธารณะ คือ “ข้อมูลที่สามารถเปิดเผยได้ สามารถนำไปใช้ได้อย่างอิสระ ไม่ว่าจะเป็นข้อมูลข่าวสาร ข้อมูลส่วนบุคคล ข้อมูลอิเล็กทรอนิกส์ เป็นต้น”

3.4.2 คำอธิบายชุดข้อมูลดิจิทัล หรือเมทาดาตา (Metadata)

คำอธิบายชุดข้อมูลดิจิทัล หรือเมทาดาตา คือ “ข้อมูลที่ใช้กำกับและอธิบายข้อมูลหลักหรือกลุ่มของข้อมูลอื่น”⁴ แบ่งออกเป็น 2 กลุ่ม ดังนี้

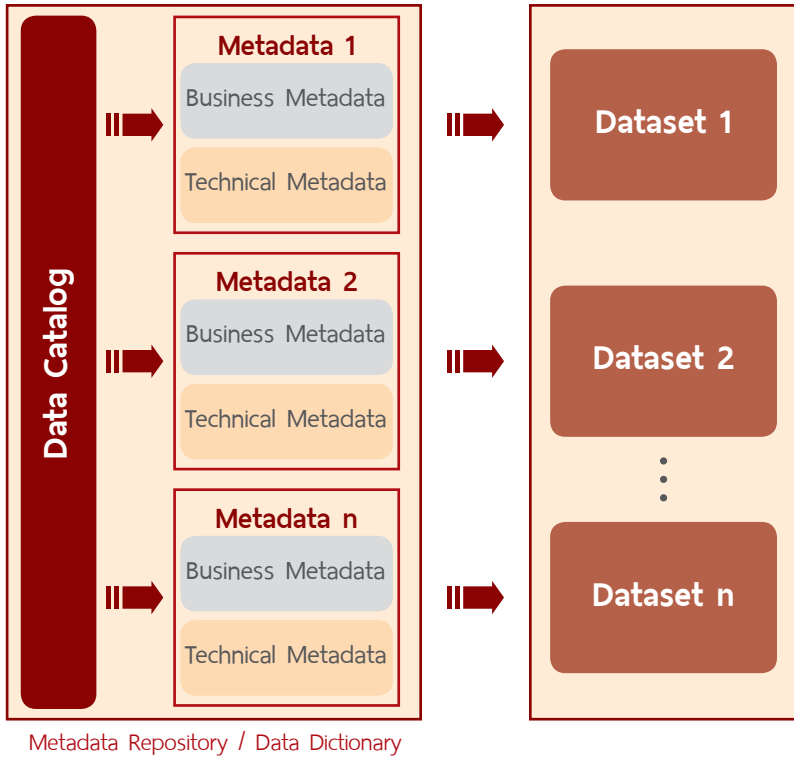
1) เมทาดาตาเชิงธุรกิจ (Business Metadata) ซึ่งให้รายละเอียดของชุดข้อมูล (Datasets) ในด้านธุรกิจ เหมาะสำหรับผู้ใช้งานข้อมูล (Data User) นักวิเคราะห์ข้อมูล (Data Analyst) และนักวิทยาการข้อมูล (Data Scientist) ตัวอย่างรายการเมทาดาตาเชิงธุรกิจ เช่น ชื่อข้อมูล ชื่อเจ้าของข้อมูล คำสำคัญ คำอธิบายอย่างย่อ วันที่เริ่มต้นใช้งาน วันที่ทำการเปลี่ยนแปลงข้อมูล ภาษาที่ใช้ ชื่อฟิลด์ข้อมูล (เช่น ชื่อพนักงาน นามสกุล เพศ) ในภาคผนวก ก อธิบายเมทาดาตาเชิงธุรกิจ ซึ่งไม่รวมชื่อฟิลด์ข้อมูล เนื่องจากชื่อฟิลด์ข้อมูลของแต่ละชุดข้อมูลมีความแตกต่างกัน

2) เมทาดาตาเชิงเทคนิค (Technical Metadata) ซึ่งให้รายละเอียดของชุดข้อมูล (Datasets) ในด้านเทคนิค (Technical) และปฏิบัติการ (Operational) เหมาะสำหรับผู้บริหารจัดการฐานข้อมูล (Database Administrator) ตัวอย่างรายการเมทาดาตาเชิงเทคนิค เช่น ชื่อตารางข้อมูล ในฐานข้อมูล ชื่อฟิลด์ข้อมูล ในตารางข้อมูล ประเภทข้อมูล (เช่น ตัวเลข ตัวหนังสือ หรือวันที่) ความกว้างของฟิลด์ข้อมูล (เช่น 10 ตัวอักษร 50 ตัวอักษร หรือ 100 ตัวอักษร) คีย์ข้อมูล (Primary Key หรือ Foreign Key) รวมไปถึงข้อมูลสำหรับการสำรองข้อมูล (Backup) และกู้คืนข้อมูล (Restore)

⁴ <https://data.go.th/~/document/14>

บัญชีข้อมูล คือ “รายการของชุดข้อมูลที่หน่วยงานถือครองหรือบริหารจัดการ” (Australian Institute of Health and Welfare, 2014) ซึ่งรายการของชุดข้อมูลที่จำแนกแยกแยะโดยการจัดกลุ่ม หรือจัดประเภท ข้อมูลที่อยู่ในความครอบครองหรือควบคุมของหน่วยงาน สามารถจัดเตรียมได้ ในรูปแบบของตารางรายชื่อชุดข้อมูล รายงาน หรือแอปพลิเคชัน บัญชีข้อมูล ถูกใช้เพื่ออำนวยความสะดวกในการค้นหาชุดข้อมูล (Datasets) หรือเมตาดาตา (Metadata) ซึ่งเป็นประโยชน์ต่อผู้ที่เกี่ยวข้องกับข้อมูล เช่น ผู้ใช้งานข้อมูล (Data User) ใช้สำหรับการค้นหาข้อมูลที่ต้องการใช้งาน นักวิเคราะห์ข้อมูล (Data Analyst) และนักวิทยาศาสตร์ข้อมูล (Data Scientist) ใช้สำหรับการค้นหา ข้อมูลที่ต้องการวิเคราะห์หรือประมวลผล บริกรข้อมูล (Data Stewards) ใช้สำหรับการค้นหาข้อมูลที่ต้องการตรวจสอบการปฏิบัติตามนโยบายข้อมูล (Data Policy Compliance) คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council) ใช้สำหรับการค้นหาข้อมูลที่ต้องการตัดสินใจหรือแก้ไขปัญหาเกี่ยวกับข้อมูลในระดับนโยบาย

คลังเมทาดาตา หรือพจนานุกรมข้อมูลเป็นเครื่องมือในการรวบรวมและจัดเก็บเมทาดาตา เพื่อสนับสนุนให้ผู้ที่ต้องการใช้ข้อมูลสามารถค้นหาและเข้าถึงได้โดยสะดวก อย่างไรก็ตามผู้ที่มีสิทธิในการเข้าถึงควรได้รับสิทธิ์ที่แตกต่างกันขึ้นอยู่กับบทบาทและความรับผิดชอบ เช่น ผู้ใช้งานข้อมูลสามารถเข้าถึงได้เฉพาะเมทาดาตาเชิงธุรกิจ ขณะที่บริการข้อมูลสามารถเข้าถึงได้ทั้งเมทาดาตาเชิงธุรกิจและเมทาดาตาเชิงเทคนิค โดยความสัมพันธ์ระหว่างบัญชีข้อมูล เมทาดาตา คลังเมทาดาตา พจนานุกรมข้อมูล และชุดข้อมูล แสดงดังรูปที่ 15



รูปที่ 15 ความสัมพันธ์ระหว่างบัญชีข้อมูล เมทาดาทา คลังเมทาดาทา
พจนานุกรมข้อมูล และชุดข้อมูล

จากรูปที่ 15 บัญชีข้อมูลเปรียบเสมือนสารบัญ เมนู หรือตัวชี้ไปยังเมทาดาทา ที่ถูกจัดเก็บอยู่ในคลังเมทาดาทา โดยเมทาดาทาจะให้รายละเอียดต่าง ๆ ที่เกี่ยวข้องกับชุดข้อมูลนั้น ๆ ทั้งนี้คลังเมทาดาทา หรือพจนานุกรมข้อมูลมักจะถูกพัฒนาให้อยู่ในรูปแบบของซอฟต์แวร์

3.5 กฎเกณฑ์ข้อมูล (Data Rules)

กฎเกณฑ์ข้อมูลมักจะอ้างถึงนโยบายและมาตรฐานที่เกี่ยวข้องกับข้อมูล โดยนโยบายข้อมูลอธิบายถึงข้อควรปฏิบัติและข้อห้ามปฏิบัติ ขณะที่มาตรฐานข้อมูลอธิบายถึงวิธีการหรือขั้นตอนการปฏิบัติ เพื่อเป็นหลักในการปฏิบัติเกี่ยวกับธรรมาภิบาลข้อมูลและการบริหารจัดการข้อมูลของหน่วยงาน ดังนั้นในการจัดทำมาตรฐานควรจะต้องสอดคล้องกับนโยบายข้อมูลที่กำหนดไว้ โดยทั้งนโยบายและมาตรฐานจะต้องสอดคล้องกับธรรมาภิบาลข้อมูลภาครัฐในระดับหน่วยงานและกฎหมายที่เกี่ยวข้อง เพื่อเป็นหลักและแนวทางในการปฏิบัติของหน่วยงาน รวมทั้งประกาศเผยแพร่ต่อผู้ที่เกี่ยวข้องและประชาชนทราบด้วย เป็นไปตามที่กำหนดไว้ตามกฎหมายว่าด้วยการนั้น ดังนี้

3.5.1 นโยบายข้อมูล (Data Policies)

การกำหนดนโยบายข้อมูลจัดเป็นหนึ่งในพื้นฐานของธรรมาภิบาลข้อมูลภาครัฐ ดังนั้นเพื่อให้ธรรมาภิบาลข้อมูลภาครัฐมีประสิทธิภาพ จึงต้องมีการกำหนดนโยบายที่ระบุอย่างชัดเจน สอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง หรือข้อกำหนดอื่น ๆ ที่เกี่ยวข้อง โดยผ่านการอนุมัติจากผู้บริหาร มีการเผยแพร่และสื่อสารให้กับเจ้าหน้าที่และผู้ที่เกี่ยวข้องทั้งภายในหน่วยงานและภายนอกหน่วยงาน รวมถึงควรมีการทบทวนนโยบายอย่างสม่ำเสมอ เพื่อให้นโยบายข้อมูลได้ถูกนำมาปฏิบัติอย่างมีประสิทธิภาพและต่อเนื่อง โดยนโยบายข้อมูลควรจะครอบคลุมระบบบริหารและกระบวนการจัดการข้อมูลหรือวงจรชีวิตของข้อมูล ซึ่งอาจจะประกอบไปด้วยนโยบายต่าง ๆ หรือหมวดนโยบาย ทั้งนี้หน่วยงานควรจัดทำนโยบายข้อมูลภายใต้กรอบนโยบายข้อมูล (Data Policy Framework) ดังนี้



นโยบายข้อมูล (Data Policy)



หมวดทั่วไป



หมวดการจัดเก็บข้อมูล
และทำลายข้อมูล



หมวดการประมวลผล
และการใช้ข้อมูล



หมวดการแลกเปลี่ยน
และการเชื่อมโยงข้อมูล



หมวดการเปิดเผย
ข้อมูล

รูปที่ 16 นโยบายข้อมูล

1) หมวดทั่วไป (General Domain)

เพื่อกำหนดนโยบายทั่วไปที่เกี่ยวข้องกับข้อมูล เช่น โครงสร้างที่เกี่ยวข้อง
หน้าที่ความรับผิดชอบ โดยมีรายละเอียด ดังนี้

- กำหนดบทบาทและความรับผิดชอบที่ประกอบกันเป็นโครงสร้าง
ธรรมาภิบาลข้อมูลภาครัฐ โดยต้องได้รับการมอบอำนาจและการอนุมัติจาก
ผู้บริหาร
- กำหนดกลุ่มบุคคลหรือบุคคลภายในหน่วยงาน เพื่อเป็นเจ้าของข้อมูล
ในการบริหารจัดการข้อมูลของหน่วยงาน เพราะหน่วยงานถือเป็นเจ้าของข้อมูล
ทุกประเภทที่เกิดจากการดำเนินงานภายในหน่วยงานนั้น ๆ
- กำหนดขอบเขตข้อมูลทีนโยบายข้อมูลครอบคลุม เช่น ข้อมูลที่มี
โครงสร้าง (ฐานข้อมูล และ CSV) ข้อมูลกึ่งโครงสร้าง (XML และ JSON) ข้อมูล
ที่ไม่มีโครงสร้าง (เอกสาร เสียง ภาพ และภาพเคลื่อนไหว)
- กำหนดนโยบาย มาตรการการรักษาความปลอดภัยของข้อมูล
เพื่อป้องกันการเข้าถึง การสูญหาย การทำลาย หรือการเปลี่ยนแปลงข้อมูล
โดยไม่ได้รับการอนุญาต

- นำระบบเทคโนโลยีสารสนเทศหรือระบบอัตโนมัติมาใช้ในการจัดทำเมทาดาตา
- ตรวจสอบความสอดคล้องกันระหว่างนโยบายข้อมูลกับการดำเนินการใด ๆ ของผู้มีส่วนได้เสีย อย่างน้อยปีละ 1 ครั้ง
- ทบทวนนโยบายข้อมูล อย่างน้อยปีละ 1 ครั้ง และให้ดำเนินการปรับปรุงอย่างต่อเนื่อง หากพบว่านโยบายข้อมูลยังไม่มีประสิทธิภาพเพียงพอ
- สื่อสารและเผยแพร่นโยบายข้อมูลให้กับผู้ที่เกี่ยวข้องทั้งภายในหน่วยงานและภายนอกหน่วยงาน
- สนับสนุนให้มีการฝึกอบรมเพื่อสร้างความตระหนักถึงธรรมาภิบาลข้อมูลภาครัฐ และการบริหารจัดการข้อมูล โดยให้ครอบคลุมทุกระบวนการของการบริหารจัดการและระบบบริหารและกระบวนการจัดการข้อมูล (วงจรชีวิตของข้อมูล)

2) หมวดการจัดเก็บข้อมูลและทำลายข้อมูล

(Data Storage and Destruction Domain)

เพื่อกำหนดนโยบายในการจัดเก็บข้อมูลและทำลายข้อมูลอย่างมีคุณภาพ มีการรักษาความปลอดภัยของข้อมูล โดยมีรายละเอียด ดังนี้

- กำหนดสภาพแวดล้อมของการจัดเก็บข้อมูลที่เกี่ยวข้องการรักษาความมั่นคงปลอดภัยและคุณภาพของข้อมูล
- กำหนดชั้นความลับของข้อมูล และจัดเก็บให้สอดคล้องกับแนวทางหรือมาตรฐานการจัดชั้นความลับของข้อมูล (Data Classification Guideline/Standard) ที่กำหนดไว้ เพื่อให้ข้อมูลมีความมั่นคงปลอดภัย และรักษาคุณภาพของข้อมูล
- กำหนดสิทธิการเข้าถึงข้อมูล และเครื่องมือที่ใช้ในการเข้าถึงข้อมูล

- จัดเก็บข้อมูลให้สอดคล้องกับความต้องการ และวัตถุประสงค์ในการดำเนินงาน โดยข้อมูลนั้นจะต้องมีความถูกต้อง สมบูรณ์ และเป็นปัจจุบันอยู่เสมอ ทั้งนี้ควรจัดทำเมทาตาสำหรับชุดข้อมูลที่มีการจัดเก็บ
- ในกรณีที่มีการร้องขอให้ทำลายข้อมูลส่วนบุคคลจากเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคล หรือหน่วยงานที่จัดเก็บต้องดำเนินการทำลายให้เร็วที่สุด ทั้งนี้ต้องไม่ขัดต่อข้อตกลงระหว่างเจ้าของข้อมูลส่วนบุคคลกับผู้ควบคุมข้อมูลส่วนบุคคล หรือไม่ขัดต่อข้อกำหนดใด ๆ
- กำหนดแนวทางในการทำลายข้อมูล เมื่อข้อมูลนั้นไม่มีการใช้งานหรือมีการเก็บข้อมูลไว้นานเกินกว่าระยะเวลาที่กำหนด แต่ควรมีการเก็บรักษาเมทาตาของข้อมูลที่ทำลายไว้ เพื่อใช้สำหรับการตรวจสอบภายหลัง
- สร้างความรู้ความเข้าใจในการจัดเก็บและทำลายข้อมูลแก่ผู้ที่เกี่ยวข้องทั้งภายในหน่วยงานและภายนอกหน่วยงาน

3) หมวดการประมวลผลข้อมูลและการใช้ข้อมูล

(Data Processing and Use Domain)

เพื่อกำหนดนโยบายในการประมวลผลข้อมูลและการใช้ข้อมูล ให้ได้ข้อมูลที่มีประสิทธิภาพ ถูกต้อง ตรงตามวัตถุประสงค์ของการใช้ข้อมูลให้เกิดประโยชน์ โดยมีรายละเอียด ดังนี้

- กำหนดแนวปฏิบัติและมาตรฐานของการประมวลผลข้อมูล และทำการสื่อสารให้แก่ผู้ที่เกี่ยวข้องรับทราบ
- การดำเนินการประมวลผลข้อมูลที่เป็นความลับ เช่น ข้อมูลส่วนบุคคล ให้เป็นไปตามขอบเขต เงื่อนไข หรือวัตถุประสงค์ในการยินยอมให้ดำเนินการกับข้อมูลส่วนบุคคลนั้น

- จัดทำเมทาดาตาสำหรับข้อมูลที่จัดเก็บอยู่ในคลังข้อมูล (Data Warehouse)
- ต้องมีการบันทึกประวัติการประมวลผลและการใช้ข้อมูล (Log File) เพื่อให้สามารถตรวจสอบย้อนกลับได้

4) หมวดการแลกเปลี่ยนและการเชื่อมโยงข้อมูล (Data Exchange and Integration Domain)

เพื่อกำหนดนโยบายในการแลกเปลี่ยนข้อมูลระหว่างหน่วยงานให้มีความมั่นคงปลอดภัย และข้อมูลมีคุณภาพ สามารถนำไปใช้ประโยชน์ได้อย่างมีประสิทธิภาพ โดยมีรายละเอียด ดังนี้

- กำหนดแนวปฏิบัติในการจัดการเรื่องความมั่นคงปลอดภัย คุณภาพข้อมูล และผู้ประสานงานหรือศูนย์ติดต่อ (Contact Center)
- กำหนดกระบวนการในการแลกเปลี่ยนข้อมูลให้ชัดเจนเริ่มตั้งแต่ขั้นตอนการเตรียมการ ขั้นตอนเริ่มดำเนินการ ขั้นตอนระหว่างดำเนินการ และขั้นตอนสิ้นสุดการดำเนินการ
- กำหนดเมทาดาตาของชุดข้อมูลที่ต้องการแลกเปลี่ยนที่จำเป็นให้ครบถ้วน
- ทำสัญญาอนุญาตหรือข้อตกลงในการแลกเปลี่ยนข้อมูลและการนำข้อมูลไปใช้
- กำหนดเทคโนโลยีและมาตรฐานทางเทคนิคที่ใช้ในการแลกเปลี่ยนข้อมูล
- บันทึกรายละเอียดและจัดเก็บข้อมูลการดำเนินงานที่เกิดขึ้นในแต่ละครั้งที่มีการแลกเปลี่ยนข้อมูล (Log File) ระหว่างหน่วยงาน เพื่อให้สามารถตรวจสอบย้อนกลับได้

- สามารถตรวจสอบได้ว่าการแลกเปลี่ยนข้อมูลได้ดำเนินการอย่างเหมาะสมหรือเป็นไปตามแนวทางปฏิบัติ กระบวนการแลกเปลี่ยน และมาตรฐานตามที่กำหนด

5) หมวดการเปิดเผยข้อมูล (Data Disclosure Domain)

เพื่อกำหนดนโยบายในการเปิดเผยข้อมูล เพื่อให้สามารถเปิดเผยข้อมูลได้อย่างถูกต้อง ตรงตามวัตถุประสงค์ของการให้ข้อมูลไปใช้ประโยชน์ โดยมีรายละเอียด ดังนี้

- ห้ามเปิดเผยข้อมูลที่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง นโยบาย แนวปฏิบัติ ไม่ว่าข้อมูลจะอยู่ในรูปแบบใดหรือสถานที่ใดก็ตาม
- ต้องได้รับการอนุญาตจากตัวแทนหน่วยงานหรือเจ้าของข้อมูลก่อนการเปิดเผยข้อมูล
- ควรมีการระบุช่องทางการเปิดเผยข้อมูลที่เข้าถึงและนำไปใช้ได้ง่าย
- ควรมีการเปิดเผยเมทาดาตาควบคู่ไปกับข้อมูลที่เปิดเผย
- สามารถตรวจสอบได้ว่าการเปิดเผยข้อมูลได้ถูกดำเนินการอย่างเหมาะสมหรือเป็นไปตามแนวทางที่ได้กำหนดไว้ เพื่อให้ได้ข้อมูลที่มีคุณภาพและเป็นการรักษาคุณภาพของข้อมูล

3.5.2 มาตรฐานข้อมูล (Data Standards)

มาตรฐานข้อมูลอ้างอิงถึงมาตรฐานที่เกี่ยวข้องกับการบริหารจัดการข้อมูลและการใช้ข้อมูล ซึ่งเป็นกลไกอย่างหนึ่งในธรรมาภิบาลข้อมูลภาครัฐ มีวัตถุประสงค์เพื่อสร้างความเข้าใจที่ตรงกัน และลดความหลากหลายของวิธีการปฏิบัติ เช่น มาตรฐานเมทาดาตา (Metadata Standard) มาตรฐาน

ชุดข้อมูล (Datasets Standard) มาตรฐานการจัดชั้นความลับของข้อมูล (Data Classification Standard) มาตรฐานเมทาดาทา (Metadata Standard) คือ การกำหนดรูปแบบและข้อกำหนดของเมทาดาทา เพื่อให้สามารถเข้าใจได้ถูกต้องตรงกันตลอดทั้งหน่วยงาน ISO/IEC 11179 และ Dublin Core Metadata Initiative (DCMI)⁵ ได้กำหนดมาตรฐานเมทาดาทาสำหรับอธิบายชุดข้อมูล เช่น ชื่อข้อมูล ชื่อเจ้าของข้อมูล คำอธิบายข้อมูล ขอบเขตการจัดเก็บรูปแบบข้อมูล ภาษา สิทธิการเข้าถึง ทั้งนี้มาตรฐานเมทาดาทามักจะอ้างอิงทั้งเมทาดาทาเชิงธุรกิจและเมทาดาทาเชิงเทคนิค แต่มักจะไม่รวมองค์ประกอบของฟิลด์ข้อมูล ซึ่งเป็นคุณลักษณะเฉพาะของแต่ละชุดข้อมูล มาตรฐานชุดข้อมูล (Datasets Standard) คือ การกำหนดรูปแบบและข้อกำหนดของข้อมูลที่มีการใช้ร่วมกันจากหลาย ๆ ส่วนงานหรือหน่วยงาน เพื่อลดความซ้ำซ้อนของข้อมูล ลดความยุ่งยากในการบริหารจัดการ และสนับสนุนให้ข้อมูลมีคุณภาพ ซึ่งส่วนงานหรือหน่วยงานต้องร่วมกันกำหนดเมทาดาทาขึ้นมาเพื่ออธิบายคุณลักษณะของชุดข้อมูลที่ใช้ร่วมกัน แล้วดำเนินการบูรณาการข้อมูลที่กระจายอยู่ตามส่วนงานหรือหน่วยงานต่าง ๆ เข้าด้วยกัน มาตรฐานชุดข้อมูลมักจะอธิบายถึงองค์ประกอบของฟิลด์ข้อมูล เช่น ชื่อฟิลด์ข้อมูล ประเภทข้อมูล (เช่น ตัวเลข ตัวหนังสือ วันที่) ช่วงค่าของข้อมูล และการอนุญาตให้ฟิลด์ข้อมูลเป็นค่าว่าง มาตรฐานการจัดชั้นความลับของข้อมูล (Data Classification Standard) คือ การกำหนดรูปแบบและข้อกำหนดของการจัดชั้นความลับของข้อมูล เพื่อป้องกันการเข้าถึงและสามารถนำข้อมูลไปใช้ได้อย่างเหมาะสม ชั้นความลับของข้อมูลมักถูกกำหนดให้สอดคล้องกับผลกระทบต่อหน่วยงานและความมั่นคงของประเทศ ตัวอย่างชั้นความลับ ได้แก่ ลับที่สุด ลับมาก

⁵ <http://dublincore.org/documents/dcmi-terms/>

ลับ และเปิดเผยได้ ตัวอย่างประเภทของผลกระทบ 1) ด้านชื่อเสียง เช่น ข้อมูลในเชิงลบของหน่วยงานถูกเปิดเผยส่งผลให้หน่วยงานหรือประเทศเสียชื่อเสียง 2) ด้านความต่อเนื่องของการดำเนินการ เช่น ข้อมูลระบบเครือข่ายถูกเปิดเผยทำให้ระบบเครือข่ายหรือระบบอินเทอร์เน็ตถูกโจมตี ซึ่งส่งผลให้การดำเนินงานของหน่วยงานหยุดชะงักหรือล่าช้า 3) ด้านการเงิน เช่น ข้อมูลบัตรเครดิตในหน่วยงานถูกเปิดเผย ทำให้สูญเสียงบประมาณของหน่วยงาน 4) ด้านทรัพยากรบุคคล เช่น ข้อมูลเงินเดือนถูกเปิดเผย ส่งผลให้บุคลากรคนสำคัญต้องลาออก

3.6 การวัดการดำเนินการและความสำเร็จของ ธรรมาภิบาลข้อมูลภาครัฐ (Data Governance Metrics and Success Measures)

การวัดการดำเนินการธรรมาภิบาลข้อมูลภาครัฐเป็นการประเมินความพร้อมของธรรมาภิบาลข้อมูล จะแสดงให้เห็นถึงสถานะปัจจุบันของหน่วยงานในเรื่องความพร้อมและความก้าวหน้าในการดำเนินการธรรมาภิบาลข้อมูล ซึ่งผลของการดำเนินการธรรมาภิบาลข้อมูลจะส่งผลถึงความสำเร็จของธรรมาภิบาลข้อมูลภาครัฐ ประกอบด้วย คุณภาพของข้อมูล ความมั่นคงปลอดภัยของข้อมูล และมูลค่าเชิงธุรกิจ ระดับความพร้อมที่สูงควรจะสะท้อนถึงความสำเร็จที่สูง อย่างไรก็ตามระดับความพร้อมกับความสำเร็จอาจจะไม่สอดคล้องกัน ซึ่งอาจจะมาจากสาเหตุอื่นหรือเกณฑ์การประเมินความพร้อมยังไม่มีประสิทธิภาพเพียงพอ ดังนั้นหน่วยงานควรจะค้นหาสาเหตุที่แน่ชัดพร้อมทั้งดำเนินการแก้ไขเกณฑ์การประเมินความพร้อมเพื่อให้สอดคล้องกับลักษณะเฉพาะของหน่วยงาน แนวทางการประเมินความพร้อมของธรรมาภิบาลข้อมูลภาครัฐ การประเมินคุณภาพของข้อมูล และการประเมินความมั่นคงปลอดภัยของข้อมูล มีรายละเอียดดังนี้

3.6.1 การประเมินความพร้อมของธรรมาภิบาลข้อมูลภาครัฐ (Data Governance Readiness Assessment)

การประเมินความพร้อมของธรรมาภิบาลข้อมูลภาครัฐจะทำให้เราได้ทราบถึงสิ่งที่เราได้ดำเนินการแล้ว และสิ่งใดบ้างที่ควรจะดำเนินการต่อไป เพื่อปรับปรุงการดำเนินงานให้เกิดประสิทธิภาพสูงสุด ระดับความพร้อมของธรรมาภิบาลข้อมูลภาครัฐถูกใช้เป็นเครื่องมือในการประเมินความพร้อมของธรรมาภิบาลข้อมูลภาครัฐ ซึ่งประกอบด้วย 6 ระดับดังนี้

- **ระดับ 0 : None** หมายถึง ไม่มีธรรมาภิบาลข้อมูลภาครัฐหรือมีแต่ไม่ได้ดำเนินการอย่างเป็นทางการ นั่นคือ มีการดำเนินงานบางส่วนและไม่มีการประกาศให้ทราบอย่างเป็นทางการ

- **ระดับ 1 : Initial** หมายถึง ไม่มีการกำหนดมาตรฐานของกระบวนการ นั่นคือ กระบวนการถูกกำหนดขึ้นมาเฉพาะกิจ (Adhoc) ทำให้แต่ละโครงการหรือบริการมีรูปแบบของกระบวนการที่แตกต่างกัน และอำนาจในการจัดการและธรรมาภิบาลข้อมูลส่วนใหญ่ถูกดำเนินการโดยฝ่ายเทคโนโลยีสารสนเทศ ทำให้การทำงานร่วมกันระหว่างฝ่ายธุรกิจและฝ่ายเทคโนโลยีสารสนเทศไม่สอดคล้องกัน

- **ระดับ 2 : Managed** หมายถึง เริ่มมีการกำหนดมาตรฐานของกระบวนการเฉพาะแต่ละส่วนงานหรือบริการ และมีการกำหนดบุคคลที่เกี่ยวข้องกับการกำกับติดตาม เช่น บริกรข้อมูลและเจ้าของข้อมูล

- **ระดับ 3 : Standardized** หมายถึง กระบวนการถูกกำหนดเป็นมาตรฐานของหน่วยงาน มีการกำหนดส่วนงานกลางในการกำกับและติดตามข้อมูล ซึ่งมาจากบุคคลด้านธุรกิจและเทคโนโลยีสารสนเทศมีการบังคับใช้นโยบายข้อมูลครอบคลุมทั้งหน่วยงาน มีการติดตาม วิเคราะห์ และรายงานคุณภาพข้อมูลหรือความมั่นคงปลอดภัย

- **ระดับ 4 : Advanced** หมายถึง กระบวนการถูกกำหนดเป็นมาตรฐานของหน่วยงาน มีการกำหนดส่วนงานกลางในการกำกับและติดตามข้อมูล ซึ่งมาจากบุคคลด้านธุรกิจและเทคโนโลยีสารสนเทศมีการบังคับใช้นโยบายข้อมูลครอบคลุมทั้งหน่วยงาน มีการติดตาม วิเคราะห์ และรายงานคุณภาพข้อมูลและความมั่นคงปลอดภัย

- **ระดับ 5 : Optimized** หมายถึง มีการดำเนินการสอดคล้องกับระดับ 4 วิเคราะห์สาเหตุของปัญหา (Root Cause) ประกอบไปด้วย ความไม่สอดคล้องในการปฏิบัติงานกับนโยบายข้อมูล (Non-Conformation) คุณภาพข้อมูลที่ต่ำ และความไม่คุ้มค่าในการบริหารจัดการข้อมูล ดำเนินการปรับปรุงกระบวนการ กฎเกณฑ์และนโยบายข้อมูล หรือโครงสร้างธรรมาภิบาลข้อมูลภาครัฐ เพื่อแก้ไขปัญหาที่พบจากผลการวิเคราะห์ และให้สอดคล้องกับความต้องการของผู้ที่เกี่ยวข้องและวัตถุประสงค์ที่เปลี่ยนไปของหน่วยงาน

ตารางที่ 16 ระดับความพร้อมของกรมการทะเบียนข้อมูลภาครัฐ

ระดับ	โครงสร้าง กรมการทะเบียนข้อมูลภาครัฐ	กระบวนการ กรมการทะเบียนข้อมูลภาครัฐ	นโยบายข้อมูล และการตรวจสอบ	การประเมินคุณภาพ ข้อมูล และความมั่นคง ปลอดภัย	การปรับปรุง อย่างต่อเนื่อง
0 : None	ไม่มีหรือมีแต่ไม่เป็นทางการ	ไม่มีหรือมีแต่ไม่เป็นทางการ	ไม่มีหรือมีแต่ไม่เป็นทางการ	ไม่มีหรือมีแต่ไม่เป็นทางการ	ไม่มีหรือมีแต่ไม่เป็นทางการ
1 : Initial	มีการกำหนดผู้กำกับดูแล อย่างไม่เป็นทางการ	กระบวนการยังไม่เป็นมาตรฐาน	ไม่มีหรือมีแต่ไม่เป็นทางการ	ไม่มีหรือมีแต่ไม่เป็นทางการ	ไม่มีหรือมีแต่ไม่เป็นทางการ
2 : Managed	มีการกำหนดผู้กำกับดูแลใน แต่ละส่วนงาน/บริการ	มีกระบวนการเป็นมาตรฐาน ส่วนงาน/บริการ	บังคับใช้ในส่วนงาน/ บริการ	ไม่มีหรือมีแต่ไม่เป็น ทางการ	ไม่มีหรือมีแต่ไม่เป็น ทางการ
3 : Standardized	มีส่วนกลางในกรมกำกับดูแล ซึ่งประกอบไปด้วยบุคคลด้าน ธุรกิจและเทคโนโลยีสารสนเทศ	มีกระบวนการเป็น มาตรฐานหน่วยงาน	บังคับใช้ทั้งหน่วยงาน	ประเมินคุณภาพข้อมูลหรือ ความมั่นคงปลอดภัย	ไม่มีหรือมีแต่ไม่เป็น ทางการ
4 : Advanced	มีส่วนกลางในกรมกำกับดูแล ข้อมูลซึ่งประกอบไปด้วยบุคคล ด้านธุรกิจและเทคโนโลยี สารสนเทศ	มีกระบวนการเป็นมาตรฐาน หน่วยงาน	บังคับใช้ทั้งหน่วยงาน	ประเมินคุณภาพข้อมูลและ ความมั่นคงปลอดภัย	ไม่มีหรือมีแต่ไม่เป็นทางการ
5 : Optimized	มีส่วนกลางในกรมกำกับดูแล ซึ่งประกอบไปด้วยบุคคลด้าน ธุรกิจและเทคโนโลยีสารสนเทศ	มีกระบวนการเป็นมาตรฐาน หน่วยงาน	บังคับใช้ทั้งหน่วยงาน	ประเมินคุณภาพข้อมูลและ ความมั่นคงปลอดภัย	มีการปรับปรุงกระบวนการ อย่างต่อเนื่อง

3.6.2 การประเมินคุณภาพของข้อมูล (Data Quality Assessment)

การประเมินคุณภาพของข้อมูลเป็นการตรวจสอบผลลัพธ์หรือความสำเร็จจากธรรมาภิบาลข้อมูลภาครัฐ โดยองค์ประกอบในการประเมินคุณภาพประกอบด้วย



รูปที่ 17 องค์ประกอบในการประเมินคุณภาพข้อมูล

1) **ข้อมูลมีความถูกต้อง (Accuracy)** ข้อมูลจะมีความถูกต้องและเชื่อถือได้ขึ้นกับวิธีการที่ใช้ในการควบคุมข้อมูลนำเข้า และการควบคุมการประมวลผล การควบคุมข้อมูลนำเข้าเป็นการกระทำเพื่อให้เกิดความมั่นใจว่าข้อมูลนำเข้ามีความถูกต้องเชื่อถือได้ เพราะถ้าข้อมูลนำเข้าไม่มีความถูกต้องแล้ว ถึงแม้จะใช้วิธีการวิเคราะห์และประมวลผลข้อมูลที่ตีเพียงใด ผลลัพธ์ที่ได้ก็จะไม่มีความถูกต้อง หรือนำไปใช้ไม่ได้ ข้อมูลนำเข้าจะต้องเป็นข้อมูลที่ผ่านการตรวจสอบว่าถูกต้องแล้ว ข้อมูลบางประเภทอาจต้องแปลงให้อยู่ในรูปแบบที่เครื่องคอมพิวเตอร์สามารถเข้าใจได้อย่างถูกต้อง ซึ่งอาจต้องพิมพ์ข้อมูลมาตรวจสอบก่อนการประมวลผล ถึงแม้ว่าจะมีการตรวจสอบข้อมูลนำเข้าแล้วก็ตามก็อาจทำให้ได้ข้อมูลที่ผิดพลาดได้ เช่น การเขียนโปรแกรมหรือใช้สูตรคำนวณผิดพลาด ดังนั้นจึงควรกำหนดวิธีการควบคุมการประมวลผล ได้แก่ การตรวจสอบยอดรวมที่ได้จากการประมวลผลแต่ละครั้ง หรือการตรวจสอบผลลัพธ์ที่ได้จากการประมวลผลด้วยเครื่องคอมพิวเตอร์กับข้อมูลสมมติที่มีการคำนวณด้วยว่ามีความถูกต้องตรงกันหรือไม่

2) **ข้อมูลมีความครบถ้วน (Completeness)** ข้อมูลบางประเภทหากไม่ครบถ้วน จัดเป็นข้อมูลที่ด้อยคุณภาพได้เช่นกัน เช่น ข้อมูลประวัติคนไข้ หากไม่มีหมู่เลือดของคนไข้ จะไม่สามารถใช้ได้ในกรณีที่ผู้ร้องขอข้อมูลต้องการข้อมูลหมู่เลือดของคนไข้ หรือข้อมูลที่อยู่ของลูกค้าที่กรอกผ่านแบบฟอร์ม ถ้ามีชื่อและนามสกุลโดยไม่มีข้อมูลบ้านเลขที่ ถนน แขวง/ตำบล เขต/อำเภอ หรือจังหวัด ข้อมูลเหล่านั้นก็ไม่สามารถนำมาใช้ได้เช่นกัน

3) **ข้อมูลมีความต้องกัน (Consistency)** ค่าข้อมูลในชุดข้อมูลเดียวที่สอดคล้องกับค่าในชุดข้อมูลอื่น นอกจากนี้คำจำกัดความของความสอดคล้องระบุว่าหากมีการดึงข้อมูลสองค่าจากชุดข้อมูลแยกต่างหากต้องไม่ขัดแย้งกัน

เช่น ข้อมูลวันที่หรือเวลาที่เก็บในฐานข้อมูลเจ้าหน้าที่ และฐานข้อมูลผู้ลงทะเบียนใช้บริการชุดข้อมูลที่มีรูปแบบต่างกัน ทั้งนี้ อาจเกิดขึ้นในขณะ ที่การออกแบบระบบมีการนำเข้าข้อมูลก็เป็นอีกสาเหตุหนึ่ง หรือแม้กระทั่งการ ใช้กฎตรวจวัดความถูกต้องของข้อมูลที่แตกต่างกัน

4) ข้อมูลมีความเป็นปัจจุบัน (Timeliness) ข้อมูลที่ตึ้นนนอกจากจะเป็นข้อมูลที่มีความถูกต้องเชื่อถือได้แล้วจะต้องเป็นข้อมูลที่เป็นปัจจุบัน ทั้งนี้ เพื่อให้ผู้ใช้นำเอาผลลัพธ์ที่ได้ไปใช้ได้ทันเวลา นั่นคือ จะต้องเก็บข้อมูลได้รวดเร็วเพื่อทันความต้องการของผู้ใช้ เช่น ตัวอย่างข้อมูลเจ้าหน้าที่ที่เข้ามาปฏิบัติงานโดยส่วนงานที่มีหน้าที่นำเข้าข้อมูลเข้าสู่ระบบได้มีการดำเนินการตามเวลาที่กำหนด คือทำให้ข้อมูลเป็นปัจจุบัน ซึ่งจะทำให้หน่วยงานที่เกี่ยวข้องสามารถนำข้อมูลที่เป็นปัจจุบันไปใช้ประโยชน์ได้อย่างมีประสิทธิภาพ

5) ข้อมูลตรงตามความต้องการของผู้ใช้ (Relevancy) ระดับของข้อมูล ที่บริหารจัดการต้องนำเสนอโดยตรงและมีประสิทธิภาพ โดยสามารถใช้งานได้ตามวัตถุประสงค์ ตัวอย่างเช่น ข้อมูลทางสถิติที่จะเป็นการนำเสนอในรูปแบบตาราง เข้าใจง่าย และข้อความอยู่ในหลาย ๆ ย่อหน้า ซึ่งสามารถใช้งานได้ตามความต้องการ

6) ข้อมูลมีความพร้อมใช้ (Availability) ข้อมูลควรเข้าถึงได้ง่าย สามารถใช้งานได้จริง และสามารถใช้งานได้ตลอดเวลา ตัวอย่างเช่น นักวิเคราะห์แผนงานต้องการข้อมูลบัญชีของการประกันภัยต่อเขตต่าง ๆ แต่ข้อมูลไม่พร้อมใช้งานจนกระทั่งต้องใช้คนเขียนโปรแกรมเพื่อดึงข้อมูลนั้นออกมา ในกรณีนี้ หากข้อมูลมีความพร้อมใช้ตรงกับความต้องการใช้ ผู้ใช้สามารถใช้ข้อมูลดังกล่าวได้ทันที

ตัวอย่างการวัดคุณภาพข้อมูลที่เป็นโครงสร้าง ดังแสดงในตารางที่ 17

ตารางที่ 17 ตัวอย่างการวัดคุณภาพข้อมูลที่เป็นโครงสร้างสำหรับ แต่ละชุดข้อมูล

คุณภาพข้อมูล	รูปแบบการวัด	หน่วยวัด	ตัวอย่าง
ความถูกต้อง	แถว × ฟิลด์	ร้อยละ	ถ้าพบว่ามี 80 ฟิลด์ที่มีความถูกต้องตลอดทั้ง 1,000 คน ดังนั้นชุดข้อมูลนี้มีความถูกต้อง $= (1,000 \times 80) / (1,000 \times 100) \times 100$ $= 80$
ความครบถ้วน	1) แถว 2) แถว × ฟิลด์ 3) แถว × ฟิลด์ที่จำเป็น	ร้อยละ	กรณีที่ 1 : พิจารณาเฉพาะแถวข้อมูล ถ้าพบว่ามีการบันทึกข้อมูล 900 คน โดยไม่สนใจจำนวนฟิลด์ที่มีการบันทึก ดังนั้นข้อมูลชุดนี้มีความครบถ้วน $= (900 / 1,000) \times 100$ $= 90$ กรณีที่ 2 : พิจารณาแถวและฟิลด์ข้อมูล ถ้าพบว่ามี 60 ฟิลด์จาก 100 ฟิลด์ที่มีการบันทึกข้อมูลทั้ง 1,000 คน ดังนั้นข้อมูลชุดนี้มีความครบถ้วน $= (1,000 \times 60) / (1,000 \times 100) \times 100$ $= 60$ กรณีที่ 3 : พิจารณาแถวและฟิลด์ข้อมูลที่มีความจำเป็นเท่านั้น ถ้ากำหนดให้มี 80 ฟิลด์ที่มีความจำเป็นต่อการบันทึกข้อมูล แล้วพบว่า มี 60 ฟิลด์จาก 80 ฟิลด์ที่มีการบันทึกข้อมูลทั้ง 1,000 คน ดังนั้นข้อมูลชุดนี้มีความครบถ้วน $= (1,000 \times 60) / (1,000 \times 80) \times 100$ $= 75$

คุณภาพข้อมูล	รูปแบบการวัด	หน่วยวัด	ตัวอย่าง
ความด้องกัน	ฟิลต์	ร้อยละ	ถ้าพบว่ามี 20 ฟิลต์ที่เก็บ้เข้าข้องกับชุดข้อมูลอื่นและมีรูปแบบของฟิลต์ที่แตกต่างกัน เช่น รูปแบบวันที่ รูปแบบรหัส ดังนั้นข้อมูลชุดนี้มีความความด้องกัน = $(100 - 20 / 100) \times 100$ = 80
ความเป็นปัจจุบัน	1) แถว 2) แถว x ฟิลต์	ร้อยละ	กรณีนี้ที่ 1 : พิจารณาเฉพาะแถวข้อมูล ถ้ามีพนักงานใหม่ 10 คน และมีพนักงานเก่า 5 คนที่มีการเปลี่ยนข้อมูล ซึ่งยังไม่มีการบันทึกหรือปรับปรุงให้เป็นปัจจุบัน ดังนั้นข้อมูลชุดนี้มีความเป็นปัจจุบัน = $100 - [(10 + 5) / (1,000 + 10) \times 100]$ = 98.51 กรณีนี้ที่ 2 : พิจารณาแถวและฟิลต์ข้อมูล ถ้ามีพนักงานใหม่ 10 คน และมีพนักงานเก่า 5 คนที่มีการเปลี่ยนชื่อและบ้านเลขที่ ซึ่งยังไม่มีการบันทึกหรือปรับปรุงให้เป็นปัจจุบัน ดังนั้นข้อมูลชุดนี้มีความเป็นปัจจุบัน = $100 - [[(10 \times 2) + (5 \times 2)] / [(1,000 + 10) \times 100] \times 100]$ = 99.97 หมายเหตุ : ชื่อและบ้านเลขที่นับเป็น 2 ฟิลต์
ตรงตามความต้องการใช้	ฟิลต์	ร้อยละ	ถ้าพบว่ามี 20 ฟิลต์ที่ไม่เคยถูกนำไปใช้ ดังนั้นข้อมูลชุดนี้มีความตรงตามความต้องการใช้ = $[(100 - 20) / 100] \times 100$ = 80
ความพร้อมใช้	ชุดข้อมูล	ร้อยละ	= 100 ถ้าข้อมูลเก็บอยู่ในรูปแบบ ฐานข้อมูล กำหนดให้ = 66.67 ถ้าข้อมูลเก็บอยู่ในรูปแบบ XML JSON และ CSV = 33.33 ถ้าข้อมูลเก็บอยู่ในรูปแบบ WORD PDF หมายเหตุ : ข้อมูลที่อยู่ในระดับที่ต่ำกว่าสามารถจัดให้อยู่ในระดับที่สูงขึ้นได้ ถ้ามีเครื่องมือหรือวิธีการที่ทำให้การนำข้อมูลไปใช้งานสะดวกมากขึ้น

หมายเหตุ : กำหนดให้ชุดข้อมูลพนักงาน มีจำนวน 1,000 แถว (คน) แต่ละแถวประกอบด้วย 100 คอลัมน์ (ฟิลด์)

3.6.3 การประเมินความมั่นคงปลอดภัยของข้อมูล (Data Security Assessment)

การประเมินความมั่นคงปลอดภัยของข้อมูลเป็นอีกหนึ่งวิธีในการวัดความสำเร็จจากธรรมาภิบาลข้อมูลภาครัฐ โดยใช้หลักเกณฑ์ในด้านต่าง ๆ ดังนี้

- 1) จัดทำนโยบายด้านความมั่นคงปลอดภัยของข้อมูลที่รวมถึงการป้องกันข้อมูลในบริบทของการรักษาความลับ ความถูกต้องของข้อมูล ความพร้อมใช้งานของข้อมูล
- 2) ข้อมูลมีการจัดชั้นความลับ (Data Classification) ข้อมูลควรมีการจัดชั้นความลับให้สอดคล้องกับกฎหมาย เงื่อนไข และข้อกำหนดต่าง ๆ รวมถึงการคำนึงถึงมูลค่า ความสำคัญ และความอ่อนไหวของข้อมูล กรณีที่ผู้ไม่ได้รับสิทธิในการเข้าถึงนั้นทำการเปิดเผยข้อมูลดังกล่าวด้วย การกำหนดระดับชั้นความลับ เช่น ข้อมูลลับ ข้อมูลลับมาก และข้อมูลเปิดเผยได้
- 3) กำหนดมาตรการควบคุมและป้องกันการเข้าถึงข้อมูล (Data Protection) การกำหนดมาตรการควบคุมและป้องกันการเข้าถึงข้อมูลต้องคำนึงถึงระดับชั้นความลับของข้อมูล เช่น ข้อมูลที่มีความอ่อนไหวต้องมีการกำหนดมาตรการควบคุมและป้องกันการเข้าถึงข้อมูลแบบพิเศษเพื่อป้องกันการเข้าถึงเพื่อเปิดเผยข้อมูลที่อ่อนไหวนั้น รวมถึงเพื่อป้องกันการดัดแปลง แก้ไข แต่งเติมข้อมูลโดยไม่ได้รับอนุญาต
- 4) ข้อมูลถูกใช้งานอย่างเหมาะสม การนำข้อมูลไปใช้ควรดำเนินการให้สอดคล้องกับสัญญาอนุญาตและไม่ขัดต่อกฎหมาย

5) ข้อมูลต้องมีความพร้อมใช้อยู่เสมอ ต้องมีการดำเนินการเตรียมความพร้อมไม่ว่าข้อมูลจะอยู่ในประเภทใดก็ตาม เช่น ข้อมูลในรูปแบบกระดาษ ต้องมีสถานที่จัดเก็บดูแล และสามารถเข้าถึงโดยผู้มีสิทธิได้อย่างสม่ำเสมอ ข้อมูลในรูปแบบอิเล็กทรอนิกส์ต้องมีการเตรียมความพร้อมเรื่องระบบงาน การสำรองข้อมูล รวมถึงมีแผนการดำเนินการในกรณีฉุกเฉินใด ๆ ที่อาจมีผลต่อการใช้ข้อมูลด้วย

ตารางที่ 18 ตัวอย่างการวัดความมั่นคงปลอดภัยของข้อมูล

ความมั่นคง ปลอดภัย ของข้อมูล	หน่วยวัด	ตัวอย่าง
ความลับ ความถูกต้อง ความพร้อมใช้	จำนวนชั้น	- จำนวนการพิจารณาทบทวนนโยบายความมั่นคงปลอดภัยสารสนเทศและมาตรการควบคุมและป้องกันการเข้าถึงข้อมูล - จำนวนการส่งเสริมสื่อสารสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัย - จำนวนการทดสอบความต่อเนื่องของการให้บริการและการนำข้อมูลกลับมาใช้
ความลับ ความถูกต้อง ความพร้อมใช้	ร้อยละ	- ร้อยละของการปฏิบัติตามนโยบายข้อมูลที่ได้กำหนดไว้ $= \frac{\text{จำนวนข้อกำหนดของนโยบายที่เป็นไปตามที่กำหนด}}{\text{จำนวนข้อกำหนดของนโยบายทั้งหมด}} \times 100$ - ร้อยละของจำนวนเหตุละเมิดความมั่นคงปลอดภัยที่ควบคุมได้ เช่น ร้อยละของการถูกเผยแพร่ข้อมูลโดยไม่ได้รับอนุญาต สูตรการคำนวณ $= \frac{\text{จำนวนเหตุละเมิดความมั่นคงปลอดภัยที่ควบคุมได้}}{\text{จำนวนเหตุละเมิดความมั่นคงปลอดภัยทั้งหมด}} \times 100$ - ร้อยละของจำนวนข้อร้องเรียนด้านความมั่นคงปลอดภัยข้อมูลที่ลดลง เช่น ร้อยละของจำนวนข้อร้องเรียนจากการเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับการอนุญาต สูตรการคำนวณ $= \frac{\text{จำนวนข้อร้องเรียนปีปัจจุบัน} - \text{ปีที่ผ่านมา}}{\text{จำนวนข้อร้องเรียนปีที่ผ่านมา}} \times 100$ - ร้อยละของความสำเร็จในการกู้คืนข้อมูลเมื่อมีเหตุฉุกเฉิน $= \frac{\text{จำนวนกู้คืนข้อมูลที่ความสำเร็จ}}{\text{จำนวนกู้คืนข้อมูลทั้งหมด}} \times 100$

บทสรุป

ธรรมาภิบาลข้อมูลภาครัฐ (Data Governance for Government)

เปรียบเสมือนเป็นแนวทางในการริเริ่มกำหนดกลไกต่าง ๆ ในธรรมาภิบาลข้อมูลภาครัฐ อย่างเป็นรูปธรรมเพื่อประโยชน์ในการบริหารจัดการข้อมูล ให้ได้ซึ่งข้อมูลที่มีคุณภาพ มีความปลอดภัย สร้างมูลค่า และสามารถเพิ่มศักยภาพในการดำเนินงานทั้งการเปิดเผยข้อมูล เชื่อมโยงและแลกเปลี่ยนข้อมูล และการสร้างประโยชน์จากข้อมูลต่อไปในอนาคต ซึ่งจะเป็นประโยชน์อย่างยิ่งต่อการดำเนินงานและการแข่งขันของประเทศ

จากกรอบธรรมาภิบาลข้อมูลภาครัฐตามหัวข้อในบทที่ 3 ซึ่งแสดงให้เห็นถึงโครงสร้าง กระบวนการและหลักเกณฑ์ต่าง ๆ ทั้งนี้เพื่อให้ได้มาซึ่งธรรมาภิบาลข้อมูลภาครัฐที่ดีนั้น หน่วยงานควรคำนึงถึงการดำเนินงานดังนี้

1. บทบาทของผู้บริหาร ผู้บริหารระดับสูงของหน่วยงาน เป็นผู้ที่มีบทบาทสำคัญยิ่งในการผลักดันให้เกิดธรรมาภิบาลข้อมูลภาครัฐ ดังนั้นผู้บริหารระดับสูงของหน่วยงานต้องมีความมุ่งมั่นในการผลักดันให้เกิดธรรมาภิบาลข้อมูลภาครัฐ โดยผู้บริหารควรมีบทบาท ดังนี้

- สื่อสารถึงความสำคัญของธรรมาภิบาลข้อมูลภาครัฐ ขอบเขต นโยบาย และเป้าประสงค์ของธรรมาภิบาลข้อมูลภาครัฐ
- สนับสนุน ส่งเสริม จัดสรรทรัพยากรให้เพียงพอต่อการดำเนินงาน
- ทบทวนธรรมาภิบาลข้อมูลภาครัฐในหน่วยงาน และส่งเสริมให้เกิดธรรมาภิบาลข้อมูลภาครัฐอยู่เสมอ

2. จัดตั้งคณะทำงาน จัดตั้งคณะทำงานให้สอดคล้องกับหน้าที่ความรับผิดชอบของแต่ละตำแหน่งตามที่ได้กำหนดไว้ในกรอบธรรมาภิบาลข้อมูลภาครัฐ เช่น คณะกรรมการธรรมาภิบาลข้อมูล บริการข้อมูล ทั้งนี้หน่วยงานสามารถดูความเหมาะสมในการบริหารจัดการบุคลากรที่มีหน้าที่ในการปฏิบัติงานดังกล่าว นอกจากนั้นบางหน่วยงานอาจมีบุคลากรที่ทำหน้าที่ในลักษณะดังกล่าวอยู่ในปัจจุบัน อย่างไรก็ตามการกำหนดบทบาทหน้าที่ที่ชัดเจนจะส่งผลต่อการทำงานที่มีประสิทธิภาพและประสิทธิผลสูงสุดต่อหน่วยงาน

3. กำหนดกระบวนการธรรมาภิบาลข้อมูลภาครัฐ กำหนดกระบวนการธรรมาภิบาลข้อมูลภาครัฐ (Data Governance Process) ตามที่ได้กำหนดไว้ในกรอบธรรมาภิบาลข้อมูลภาครัฐ โดยพิจารณาถึง การเลือกข้อมูลเพื่อดำเนินการธรรมาภิบาล การระบุเป้าหมาย การกำหนดมาตรฐานและแนวปฏิบัติ รวมถึงการบริหารจัดการคน โดยกระบวนการธรรมาภิบาลข้อมูลภาครัฐเริ่มตั้งแต่การวางแผน การปฏิบัติ การตรวจสอบ วัดผลและรายงานไปจนถึงการปรับปรุงอย่างต่อเนื่อง

4. กำหนดนโยบาย กฎเกณฑ์ของข้อมูล การกำหนดนโยบายข้อมูลจัดเป็นหนึ่งในพื้นฐานของธรรมาภิบาลข้อมูลภาครัฐ นโยบายที่กำหนดสามารถใช้รายละเอียดตามที่ระบุในกรอบธรรมาภิบาลข้อมูลภาครัฐได้ โดยคำนึงถึงความสอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ คำสั่งหรือข้อกำหนดอื่น ๆ ที่เกี่ยวข้อง มีการเผยแพร่และสื่อสารให้กับเจ้าหน้าที่และผู้ที่เกี่ยวข้องทั้งภายในหน่วยงานและภายนอกหน่วยงานเพื่อดำเนินการต่อไป

5. การปฏิบัติงานต่าง ๆ ที่เกี่ยวข้องกับธรรมาภิบาลข้อมูลภาครัฐ

กลุ่มคนที่ได้กำหนดไว้ในธรรมาภิบาลข้อมูลภาครัฐตามที่ระบุในข้อที่ 2 มีหน้าที่ในการดำเนินงานที่แตกต่างกันออกไป โดยเริ่มตั้งแต่การวางแผน การลงมือปฏิบัติ การตรวจสอบ และปรับปรุงอย่างต่อเนื่อง ตามลำดับองค์ประกอบอย่างน้อยที่หน่วยงานจะต้องดำเนินการ ได้แก่

- สร้างการรับรู้ให้กับคนภายในหน่วยงาน
- ดำเนินการตามนโยบาย กฎเกณฑ์ของข้อมูล
- บริหารจัดการข้อมูล
- ส่งเสริมและสนับสนุนการแลกเปลี่ยน ตลอดจนการเชื่อมโยงข้อมูลระหว่างหน่วยงาน

6. ตรวจสอบเพื่อการประเมินผล

การทำงานในภาพรวมเพื่อเป็นข้อมูลที่ใช้สำหรับการตัดสินใจ เพื่อการปรับปรุงหรือพัฒนาในอนาคต และบรรลุตามเป้าหมายที่วางไว้ตลอดจนเป็นแนวทางในการบริหารจัดการต่อไปในกรอบธรรมาภิบาลข้อมูลภาครัฐนั้นจะต้องจัดทำอย่างสม่ำเสมอและต่อเนื่อง ดังนั้นหน่วยงานควรต้องดำเนินการและวัดผล ปรับปรุงประสิทธิภาพอยู่เสมอเพื่อยกระดับการดำเนินงานให้มีธรรมาภิบาลข้อมูลภาครัฐที่มีให้ดียิ่ง ๆ ขึ้นเพื่อประโยชน์ในการดำเนินงาน เพิ่มศักยภาพ ส่งผลดีทั้งต่อประชาชนและประเทศชาติต่อไป

ภาคผนวก



ภาคผนวก ก

แบบฟอร์มการจัดทำคำอธิบายชุดข้อมูลดิจิทัล หรือเมทาดาตา

ตารางที่ 19 แบบฟอร์มการจัดทำคำอธิบายชุดข้อมูลดิจิทัล หรือเมทาดาตา

ชื่อรายการ	คำอธิบาย	โปรตรระบุ
1) เลขที่เมทาดาตา	กำหนดเลขให้เป็น Unique	
2) ชื่อข้อมูล	ชื่อของข้อมูลที่กำหนดโดยหน่วยงานเจ้าของเรื่อง	
3) เจ้าของข้อมูล	ชื่อบุคคล ชื่อส่วนงาน หรือชื่อหน่วยงานที่รับผิดชอบข้อมูล และที่อยู่ที่สามารถติดต่อได้	
4) คำสำคัญ	หัวข้อ คำ หรือวลี ที่ใช้สำหรับการค้นเรื่องที่ต้องการได้	
5) คำอธิบายอย่างย่อ	บทคัดย่อของข้อมูลหรือ Abstract ที่บ่งบอกถึงเนื้อความในข้อมูลอย่างสั้น	
6) ผู้สนับสนุนหรือผู้ร่วมดำเนินการ	ผู้ที่สนับสนุนหรือผู้ร่วมดำเนินการเกี่ยวกับข้อมูล เช่น เจ้าของผลิตภัณฑ์ (Product Owner), ส่วนควบคุมคุณภาพ	
7) วันที่เริ่มต้นสร้าง	วัน เดือน ปี ที่เริ่มต้นใช้ข้อมูล (รูปแบบ YYYY-MM-DD เช่น 2015-02-25)	

ตารางที่ 19 แบบฟอร์มการจัดทำคำอธิบายชุดข้อมูลดิจิทัล หรือเมทาดาตา (ต่อ)

ชื่อรายการ	คำอธิบาย	โปรตรระบุ
8) วันที่ทำการเปลี่ยนแปลงข้อมูลล่าสุด	วัน เดือน ปี ล่าสุดที่มีการปรับปรุงข้อมูล (รูปแบบ YYYY-MM-DD เช่น 2015-02-25)	
9) แหล่งที่มา	แหล่งที่มา เช่น จากโครงการสำรวจ	
10) หน่วยย่อยที่สุดที่มีข้อมูล	หน่วยย่อยหรือขอบเขตที่น้อยที่สุดที่มีข้อมูล เช่น หมู่บ้าน จังหวัด ภาค ประเทศ	☐ บุคคล ☐ สถานประกอบการ ☐ คริวเรือน ☐ หมู่บ้าน ☐ ตำบล ☐ อำเภอ ☐ จังหวัด ☐ ภาค ☐ ประเทศ ☐ อื่น ๆ
11) รูปแบบการเก็บข้อมูล	รูปแบบที่บันทึกข้อมูล เช่น Database CSV/XLS VDO	☐ Database ☐ CSV/XLS ☐ XML/JSON ☐ Image/Diagram ☐ VDO ☐ Text/Document ☐ เอกสารกระดาษ ☐ อื่น ๆ

ตารางที่ 19 แบบฟอร์มการจัดทำคำอธิบายชุดข้อมูลดิจิทัล หรือเมทาดาตา (ต่อ)

ชื่อรายการ	คำอธิบาย	โปรตระรูป
12) ภาษาที่ใช้	ภาษาที่ใช้ เช่น ภาษาไทย ภาษาอังกฤษ ภาษาจีน ภาษาญี่ปุ่น	☐ ภาษาไทย ☐ ภาษาอังกฤษ ☐ จีน ☐ ญี่ปุ่น ☐ อื่น ๆ
13) URL	ระบุ URL เรื่องอื่น ๆ ที่เกี่ยวข้อง	
14) ขอบเขตที่เผยแพร่ข้อมูล	ขอบเขตหรือพื้นที่ในการนำเสนอ ข้อมูล เช่น ภายในหน่วยงาน ระหว่างหน่วยงาน	☐ ภายในหน่วยงาน ☐ ระหว่างหน่วยงาน ☐ ภายในขอบเขตความร่วมมือ ☐ ระหว่างประเทศ ☐ ไม่จำกัดขอบเขต
15) สิทธิในการเข้าถึงข้อมูล	สิทธิในการเข้าถึงข้อมูล อธิบายระดับการเข้าถึงข้อมูล เช่น View Modify	☐ View ☐ Modify
16) สิทธิในการใช้ข้อมูล	สิทธิ สัญญา หรือข้อตกลงในการใช้ชุดข้อมูล เช่น ใช้โดยอิสระ ให้เมื่อร้องขอ สัญญาอนุญาต	☐ ใช้โดยอิสระ ☐ ให้เมื่อร้องขอ ☐ สัญญาอนุญาต ☐ ขอบเขตความร่วมมือ ☐ อื่น ๆ

ภาคผนวก ข

บทบาท และความรับผิดชอบของผู้มีส่วนได้เสียกับข้อมูล

เพื่อให้หน่วยงานสามารถดำเนินการธรรมาภิบาลข้อมูลและบริหารจัดการข้อมูลได้อย่างมีประสิทธิภาพ และสร้างประโยชน์สูงสุด จึงมีการกำหนดบทบาทและความรับผิดชอบของผู้มีส่วนได้เสียกับข้อมูลในแต่ละด้าน ดังนี้

ตารางที่ 20 บทบาท และความรับผิดชอบของผู้มีส่วนได้เสียกับข้อมูล

บทบาท	ความรับผิดชอบ
ด้านการบริหารจัดการข้อมูล	
สถาปนิกข้อมูล (Data Architect)	- กำหนดโครงสร้างและความสัมพันธ์ของข้อมูล โดยพิจารณาจากความต้องการข้อมูล และวัตถุประสงค์ของหน่วยงาน - พัฒนาสถาปัตยกรรมข้อมูลในภาพรวมของทั้งหน่วยงาน โดยประเมินสถานะในปัจจุบัน และออกแบบเพื่อปรับปรุงสำหรับอนาคต - สร้างพิมพ์เขียว (Blueprint) สำหรับการบริหารจัดการข้อมูลต่าง ๆ เช่น การบูรณาการข้อมูล การไหลของข้อมูลตั้งแต่ต้นทางจนถึงปลายทาง
ผู้บริหารจัดการฐานข้อมูล (Database Administrator)	- บริหารจัดการ และควบคุมเกี่ยวกับระบบฐานข้อมูลภายในหน่วยงาน - กำหนดนโยบาย มาตรการ และมาตรฐานของระบบฐานข้อมูลทั้งหมดภายในหน่วยงาน ตัวอย่างเช่น รายละเอียดและวิธีการจัดเก็บข้อมูล การใช้งานฐานข้อมูล การรักษาความปลอดภัยของข้อมูลการสำรองข้อมูล การกู้คืนข้อมูล

ตารางที่ 20 บทบาท และความรับผิดชอบของผู้มีส่วนได้เสียกับข้อมูล (ต่อ)

บทบาท	ความรับผิดชอบ
วิศวกรข้อมูล (Data Engineer)	- ออกแบบวิธีการจัดเก็บ และเรียกใช้งานข้อมูล - จัดการเกี่ยวกับข้อมูลทั้งหมด ตั้งแต่ระดับชนิดของข้อมูล วางโครงสร้างของการเข้าและการออกของข้อมูล เพื่อให้ข้อมูลไหลได้อย่างไม่สะดุด
นักวิเคราะห์ข้อมูล (Data Analyst)	- นำข้อมูลมาวิเคราะห์แนวโน้มในเชิงธุรกิจ หรือ แก้ปัญหาจากสิ่งที่ผิดแปลกไปจากแนวโน้มเดิม โดยใช้ประสบการณ์ และหลักสถิติ - ใช้โมเดลหรือเครื่องมือในการทำรายงาน เพื่อสรุปข้อมูลสำหรับใช้ในการตัดสินใจ
นักวิทยาการข้อมูล (Data Scientist)	- นำข้อมูลจากหลาย ๆ แหล่ง และแปลงข้อมูล เพื่อหารูปแบบและความสัมพันธ์ของข้อมูล - สร้างแบบจำลอง และดำเนินการกับข้อมูลด้วยวิธีการต่าง ๆ เช่น Machine Learning หรือเขียนโปรแกรม เพื่อทำนายมุมมอง และคำตอบใหม่ ๆ
นักวิเคราะห์ระบบ (System Analyst)	วิเคราะห์และออกแบบระบบ โดยศึกษาเกี่ยวกับปัญหา รวบรวมความต้องการของผู้ใช้งานระบบ วิเคราะห์ระบบงานภายในหน่วยงาน
นักวิเคราะห์ธุรกิจ (Business Analyst)	- ศึกษาและวิเคราะห์ข้อมูลที่เกี่ยวข้องกับเทคโนโลยี กลยุทธ์ กลุ่มเป้าหมาย และหน่วยงานที่เกี่ยวข้อง - ทำความเข้าใจเป้าหมายและปัญหาของหน่วยงาน วิเคราะห์ความต้องการและหาคำตอบ เพื่อวางแผนด้านกลยุทธ์ เพื่อผลักดันให้เกิดการเปลี่ยนแปลง

ตารางที่ 20 บทบาท และความรับผิดชอบของผู้มีส่วนได้เสียกับข้อมูล (ต่อ)

บทบาท	ความรับผิดชอบ
นักออกแบบจำลองข้อมูล (Data Modeler)	- ออกแบบจำลองข้อมูล เช่น Entity Relationship Diagram และ Data Flow Diagram - ออกแบบและพัฒนาแบบจำลองข้อมูล (Data Model) เพื่ออธิบายลักษณะโครงสร้างและการทำงานของข้อมูลให้เห็นภาพได้มากขึ้น
ด้านธรรมาภิบาลข้อมูลภาครัฐ	
ผู้บริหารข้อมูลระดับสูง (Chief Data Officer)	- นำข้อมูลและวิเคราะห์ข้อมูล เพื่อสร้างและส่งมอบเทคโนโลยี เครื่องมือ แนวทาง และวิธีการในการทำให้ข้อมูลของหน่วยงานมีคุณค่า และเกิดประโยชน์สูงสุดต่อหน่วยงาน - วิเคราะห์และร่วมกับผู้บริหารส่วนอื่น ๆ เพื่อจัดทำยุทธศาสตร์และดำเนินการธรรมาภิบาลข้อมูลภาครัฐให้มีคุณภาพและการควบคุมอื่น ๆ เพื่อรักษาความสมบูรณ์ของข้อมูล - นำแนวปฏิบัติและมาตรฐานของหน่วยงานไปปรับปรุงข้อมูลและยุทธศาสตร์ของประเทศ - เป็นตัวกลางระหว่างหน่วยงานภาครัฐในการแลกเปลี่ยนเชื่อมโยงข้อมูล รวมไปถึงการจัดการความเสี่ยงที่อาจเกิดจากข้อมูลของหน่วยงานภาครัฐ - ส่งเสริมนวัตกรรมที่ใช้ประโยชน์จากข้อมูลในการวิเคราะห์ปัญหา - วิเคราะห์หาเทคโนโลยีใหม่ ๆ มาใช้ในการวิเคราะห์ข้อมูล

ตารางที่ 20 บทบาท และความรับผิดชอบของผู้มีส่วนได้เสียกับข้อมูล (ต่อ)

บทบาท	ความรับผิดชอบ
บริการข้อมูลด้านธุรกิจ (Business Data Stewards)	• นิยามความต้องการด้านคุณภาพและความมั่นคงปลอดภัย • นิยามเมทาดาตา • ร่างนโยบายข้อมูล มาตรฐาน และแนวปฏิบัติต่าง ๆ ที่เกี่ยวข้องกับข้อมูล • ตรวจสอบการปฏิบัติตามนโยบายข้อมูล ตรวจสอบคุณภาพ ตรวจสอบความมั่นคงปลอดภัยของข้อมูล วิเคราะห์ผลจากการตรวจสอบ
บริการข้อมูลด้านเทคนิค (Technical Data Stewards)	• ดำเนินการในเรื่องคุณภาพข้อมูล เช่น กำหนดนโยบายข้อมูลด้านคุณภาพ การตรวจวัดคุณภาพข้อมูล และการวิเคราะห์คุณภาพข้อมูล
บริการข้อมูลด้านคุณภาพข้อมูล (Data Quality Stewards)	• ดำเนินการในเรื่องคุณภาพข้อมูล เช่น กำหนดนโยบายข้อมูลด้านคุณภาพ การตรวจวัดคุณภาพข้อมูล และการวิเคราะห์คุณภาพข้อมูล
เจ้าของข้อมูล (Data Owner)	• รับผิดชอบดูแล และรักษาคุณภาพของข้อมูล • ทบทวนและอนุมัติการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับข้อมูล
ผู้สร้างข้อมูล (Data Creator)	• บันทึก แก้ไข ปรับปรุง หรือลบข้อมูลให้สอดคล้องกับโครงสร้างที่ถูกกำหนดไว้ • ทำงานร่วมกับบริการข้อมูลเพื่อตรวจสอบและแก้ไขปัญหาด้านคุณภาพข้อมูลและความปลอดภัยของข้อมูล
ผู้ใช้ข้อมูล (Data User)	• นำข้อมูลไปใช้งานทั้งในระดับปฏิบัติงานและระดับบริหาร • สนับสนุนธรรมาภิบาลข้อมูลภาครัฐ • รายงานประเด็นปัญหาที่พบระหว่างการใช้ข้อมูลทั้งด้านคุณภาพ และความปลอดภัยของข้อมูล

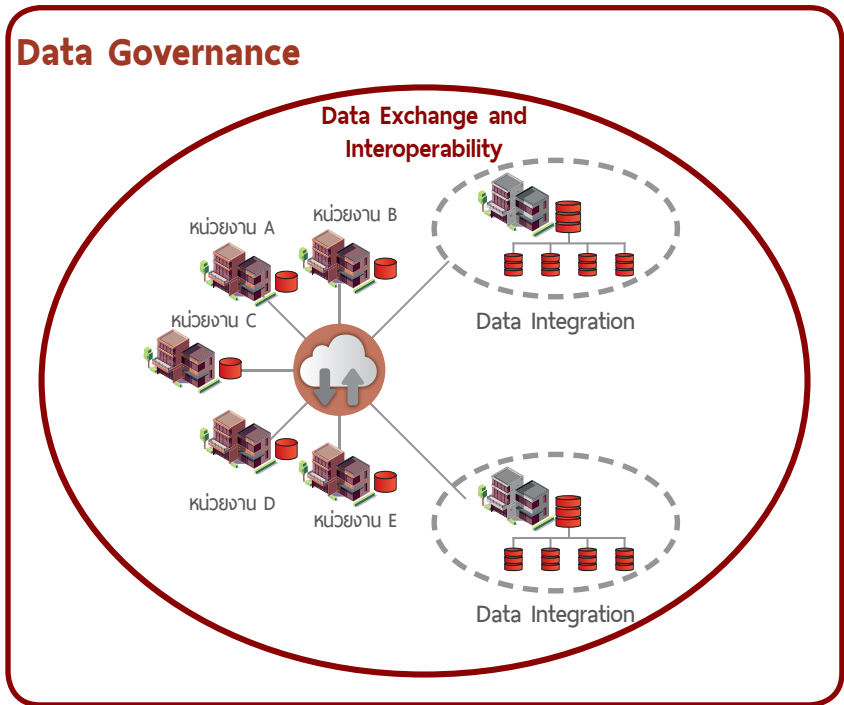
ภาคผนวก ค

แนวนโยบายและแนวปฏิบัติในการเชื่อมโยง และแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน

การเชื่อมโยงและแลกเปลี่ยนข้อมูลเป็นกระบวนการของการรับส่งข้อมูลหรือแบ่งปันข้อมูลภายในหน่วยงานหรือระหว่างหน่วยงาน ตัวอย่างการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ เช่น ข้อมูลกระบวนการยุติธรรม ข้อมูลการนำเข้า/ส่งออกสินค้าระหว่างประเทศ ข้อมูลภูมิสารสนเทศ ข้อมูลการบริหารจัดการน้ำ ข้อมูลเกษตรกรผู้มีรายได้น้อย ข้อมูลความมั่นคงประเทศ ทั้งนี้ข้อมูลที่มีการเชื่อมโยงและแลกเปลี่ยนต้องไม่เป็นข้อมูลเปิด (Open Data) หรือข้อมูลที่สามารถนำไปใช้ได้โดยอิสระ

ธรรมาภิบาลข้อมูลภาครัฐถือเป็นส่วนสำคัญที่จะช่วยให้การเชื่อมโยงและแลกเปลี่ยนข้อมูลมีประสิทธิภาพและประสิทธิผล ซึ่งส่งผลให้เกิดประโยชน์ต่อภาคประชาชน ภาครัฐ ตลอดจนภาคเอกชน อันจะส่งผลต่อความเจริญก้าวหน้าของประเทศ สอดคล้องกับรูปที่ 18 ซึ่งชี้ให้เห็นถึงธรรมาภิบาลข้อมูลภาครัฐเข้ามาควบคุมการบูรณาการข้อมูล (Data Integration) และการแลกเปลี่ยนข้อมูล (Data Exchange) เพื่อให้เกิดการเชื่อมโยงข้อมูลระหว่างหน่วยงาน (Interoperability) อย่างแท้จริง

Data Governance



รูปที่ 18 ความสัมพันธ์ระหว่างธรรมาภิบาลข้อมูลภาครัฐและการแลกเปลี่ยนข้อมูล

โดยกิจกรรมของธรรมาภิบาลข้อมูลภาครัฐที่เกี่ยวข้องกับการเชื่อมโยงและแลกเปลี่ยนข้อมูลควรประกอบไปด้วย 1) กำหนดบทบาทหน้าที่ของบุคคลที่เกี่ยวข้อง 2) กำหนดนโยบายการเชื่อมโยงและแลกเปลี่ยนข้อมูล และ 3) กำหนดแนวปฏิบัติในการเชื่อมโยงและแลกเปลี่ยนข้อมูล ดังนี้

1) กำหนดบทบาทหน้าที่ที่เกี่ยวข้องกับการเชื่อมโยงและแลกเปลี่ยนข้อมูล

1.1 กำหนดบุคคลหรือกลุ่มบุคคลที่มีสิทธิ์ตัดสินใจในการสนับสนุนข้อมูลให้หน่วยงานอื่น เช่น คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council) หรือคณะทำงาน

1.2 กำหนดบุคคลหรือกลุ่มบุคคลในการดำเนินการเชื่อมโยงและแลกเปลี่ยนข้อมูล เช่น บุคคลที่ทำหน้าที่ออกแบบกระบวนการและเทคโนโลยีในการเชื่อมโยงและแลกเปลี่ยนข้อมูล (Data Integration Architect) บุคคลที่ทำหน้าที่ดำเนินการเชื่อมโยงและแลกเปลี่ยนข้อมูลให้สอดคล้องกับที่ได้ออกแบบไว้ (Data Integration Specialist)

1.3 กำหนดบุคคลหรือกลุ่มบุคคลในการรับเรื่องและแก้ไขปัญหาเบื้องต้นในการเชื่อมโยงและแลกเปลี่ยนหรือขอใช้ข้อมูล เช่น ศูนย์ติดต่อ (Contact Center)

2) กำหนดนโยบายการเชื่อมโยงและแลกเปลี่ยนข้อมูล

ในหัวข้อ 3.3.1 ได้แสดงกรอบนโยบายข้อมูลในหมวดการเชื่อมโยงและแลกเปลี่ยนข้อมูล ดังนี้

2.1 กำหนดแนวปฏิบัติในการจัดการเรื่องความมั่นคงปลอดภัย คุณภาพข้อมูล และผู้ประสานงานหรือศูนย์ติดต่อ (Contact Center)

2.2 กำหนดกระบวนการในการเชื่อมโยงและแลกเปลี่ยนข้อมูลให้ชัดเจน เริ่มตั้งแต่ขั้นตอนการเตรียมการ ขั้นตอนเริ่มดำเนินการ ขั้นตอนระหว่างดำเนินการ และขั้นตอนสิ้นสุดการดำเนินการ

2.3 กำหนดเมทาเดตาของชุดข้อมูลที่ต้องการเชื่อมโยงและแลกเปลี่ยนที่จำเป็นให้ครบถ้วน

2.4 ทำสัญญาอนุญาตหรือข้อตกลงในการเชื่อมโยงและแลกเปลี่ยนข้อมูล และการนำข้อมูลไปใช้

2.5 กำหนดเทคโนโลยีและมาตรฐานทางเทคนิคที่ใช้ในการเชื่อมโยง และแลกเปลี่ยนข้อมูล

2.6 บันทึกรายละเอียดและจัดเก็บข้อมูลการดำเนินงานที่เกิดขึ้นในแต่ละครั้งที่มีการเชื่อมโยงและแลกเปลี่ยนข้อมูล (Log File) ระหว่างหน่วยงาน เพื่อให้สามารถตรวจสอบย้อนกลับได้

2.7 สามารถตรวจสอบได้ว่าการเชื่อมโยงและแลกเปลี่ยนข้อมูลได้ดำเนินการอย่างเหมาะสมหรือเป็นไปตามแนวทางปฏิบัติ กระบวนการการเชื่อมโยงและแลกเปลี่ยน และมาตรฐานตามที่กำหนด

3) กำหนดแนวปฏิบัติการเชื่อมโยงและแลกเปลี่ยนข้อมูล

แนวปฏิบัติการเชื่อมโยงและแลกเปลี่ยนข้อมูลเป็นไปตามขั้นตอนต่อไปนี้

3.1 ตรวจสอบชั้นความลับของข้อมูล (Data Classification) ว่าอยู่ในชั้นความลับที่สามารถเปิดเผยได้หรือไม่ นั่นคือ ต้องไม่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ ความมั่นคงของประเทศ ความลับทางราชการ และความเป็นส่วนตัว พร้อมทั้งตรวจสอบสิทธิ์ของหน่วยงานที่สามารถนำข้อมูลไปใช้ได้ตามบทบาท และภารกิจตามกฎหมายของหน่วยงานนั้น ๆ

3.2 จัดทำเมทาดาทา (Metadata) ของชุดข้อมูลที่ร้องขอ ตัวอย่างองค์ประกอบของเมทาดาทา เช่น ชื่อข้อมูล คำอธิบายข้อมูล คำสำคัญ วันที่ทำการเปลี่ยนแปลงข้อมูลล่าสุด ชื่อหน่วยงานเจ้าของข้อมูล ฟิลด์ข้อมูล ทั้งนี้ ต้องตรวจสอบให้แน่ใจได้ว่าเมทาดาทามีฟิลด์ข้อมูลครบถ้วนสอดคล้องกับความต้องการของหน่วยงานที่ขอใช้ข้อมูล

3.3 จัดทำสัญญาอนุญาตหรือเงื่อนไขในการเชื่อมโยงและแลกเปลี่ยนและการนำข้อมูลไปใช้ ตัวอย่างส่วนประกอบของสัญญา เช่น วัตถุประสงค์ในการนำไปใช้ ขอบเขตในการนำไปใช้ ช่วงวันที่ในการเข้าถึง ความถี่ในการเข้าถึง ระดับการให้บริการ (Service Level Agreement-SLA) ช่วงเวลาในการนำไปใช้ ฟิลด์ที่สามารถเข้าถึง รายการข้อมูลที่สามารถเข้าถึง ในกรณีขอข้อมูลส่วนบุคคลเป็นรายคน ต้องจัดทำหนังสือแสดงความยินยอม (Consent Letter) เพื่อรับการยินยอมจากบุคคลนั้น ๆ ยกเว้นหน่วยงานที่ขอใช้ข้อมูลมีอำนาจตามกฎหมายโดยชอบธรรม พร้อมทั้งกำหนดเทคโนโลยีและมาตรฐานทางเทคนิคที่ใช้ในการเชื่อมโยงและแลกเปลี่ยนข้อมูล เช่น Representational State Transfer (REST) Simple Object Access Protocol (SOAP)

3.4 ไม่แสดงตัวตน (Anonymization) ในกรณีที่หน่วยงานที่ขอข้อมูลไม่มีอำนาจในการเข้าถึงข้อมูลส่วนบุคคลแต่ต้องการใช้ข้อมูลเพื่อการศึกษาหรือวิจัย ซึ่งสามารถอ้างอิง “แนวปฏิบัติในการปกป้องข้อมูลที่ระบุตัวบุคคลได้ (Guideline to protect the Personally Identifiable Information)” พร้อมทั้งตรวจสอบและปรับปรุงคุณภาพของข้อมูล (Data Quality) ให้อยู่ในเกณฑ์มาตรฐานก่อนการเชื่อมโยงและแลกเปลี่ยน

3.5 ดำเนินการเชื่อมโยงและแลกเปลี่ยนข้อมูลตามเงื่อนไขและมาตรฐานการเชื่อมโยงและแลกเปลี่ยนที่กำหนดไว้

3.6 ติดตามและควบคุมประสิทธิภาพระหว่างการเชื่อมโยงและแลกเปลี่ยนข้อมูล เพื่อรักษาไว้ซึ่งความปลอดภัยของข้อมูล คุณภาพข้อมูล และสอดคล้องกับระดับการให้บริการ

ภาคผนวก ง

แนวนโยบายและแนวปฏิบัติในการเปิดเผยข้อมูล และการขอใช้ข้อมูล

ข้อมูลเปิด (Open Data) คือ “ข้อมูลที่สามารถนำไปใช้ได้โดยอิสระ สามารถนำกลับมาใช้ใหม่และแจกจ่ายได้โดยใครก็ตาม แต่ต้องระบุแหล่งที่มาหรือเจ้าของงานและต้องใช้สัญญาอนุญาต หรือเงื่อนไขเดียวกันกับที่มา หรือตามเจ้าของงานกำหนด” ข้อมูลจากหน่วยงานภาครัฐที่สามารถเปิดเผยได้ จะอยู่ในรูปแบบที่เป็นมาตรฐานเปิด (Open Format) และไม่ใช่รูปแบบมาตรฐานเฉพาะ (Non-proprietary Format) ที่คนและเครื่องคอมพิวเตอร์สามารถอ่านและนำไปใช้ต่อยอดในการพัฒนาบริการในรูปแบบต่าง ๆ ได้ ข้อมูลเปิดถูกใช้เป็นเครื่องมือในการตรวจสอบความโปร่งใสในการดำเนินการของภาครัฐและความสามารถในการพัฒนาประเทศ ซึ่งสามารถวัดอันดับการเปิดเผยข้อมูลภาครัฐได้จากมาตรฐานตัวชี้วัด เช่น Open Data Index และ Open Data Barometer เพื่อให้อันดับการเปิดเผยข้อมูลภาครัฐสูงขึ้น หน่วยงานรัฐควรดำเนินการเปิดเผยตามหลักการเปิดเผยข้อมูล 8 ด้าน ดังนี้

1) **สมบูรณ์ (Completeness)** ข้อมูลภาครัฐทั้งหมดที่ไม่เกี่ยวข้องกับข้อมูลส่วนบุคคลหรือความมั่นคงจะต้องถูกเปิดเผยโดยข้อมูลดังกล่าวจะไม่ขัดกับ ข้อกำหนดในเรื่องความเป็นส่วนตัว ความมั่นคง และเอกลิทธิ์ที่ชอบด้วยเหตุผล

2) **ข้อมูลปฐมภูมิ (Primary)** ข้อมูลควรจะถูกเผยแพร่จากแหล่งที่เก็บข้อมูลโดยตรงด้วยระดับความละเอียดสูง ไม่มีการปรับแต่งหรือทำให้อยู่ในรูปแบบข้อมูลสรุป (Summary Data)

3) **ทันเวลา (Timeliness)** คือ ข้อมูลควรจะเป็นปัจจุบันและหากเป็นไปได้ อาจจะเป็นลักษณะ Real-time feed ซึ่งอาจจะพิจารณาตามความเหมาะสมในการเพิ่มรรถประโยชน์ของข้อมูลนั้น ๆ ชุดข้อมูลควรจะมีการบันทึกเวลา (Timestamps) หรือข้อมูลอื่น ๆ ที่ช่วยให้ผู้ใช้งานสามารถระบุได้ว่าข้อมูลนั้นเป็นปัจจุบัน

4) **สามารถเข้าถึงได้ (Accessibility)** ข้อมูลถูกเปิดเพื่อให้ผู้ใช้ที่หลากหลายและมีจุดประสงค์ต่างกันซึ่งข้อมูลดังกล่าวจะต้องมีการเผยแพร่อยู่บนอินเทอร์เน็ตโดยทุกคนจะต้องสามารถเข้าถึงข้อมูลเหล่านั้นได้และข้อมูลจะต้องรองรับการใช้งานจากทุกแพลตฟอร์ม

5) **เครื่องสามารถอ่านได้ (Machine Readability)** ข้อมูลจะต้องอยู่ในรูปแบบที่นำไปประมวลผลได้โดยอัตโนมัติ

6) **การไม่เลือกปฏิบัติ (Non-discriminatory)** ทุกคนสามารถนำข้อมูลไปใช้ได้โดยไม่ต้องมีการลงทะเบียนผู้ใช้

7) **ปลอดกรรมสิทธิ์ (Non-proprietary)** ข้อมูลที่เผยแพร่จะต้องอยู่ในรูปแบบมาตรฐานเปิดไม่ใช่รูปแบบมาตรฐานเฉพาะและไม่มีการใดมีสิทธิขาดในการเป็นเจ้าของแต่ผู้เดียว

8) **ใช้งานฟรี (License-free)** ข้อมูลจะต้องไม่มีปัญหาเรื่องลิขสิทธิ์ในการใช้งานสามารถใช้งานโดยไม่เสียค่าใช้จ่ายเพื่อเป็นการส่งเสริมการใช้งานอย่างแพร่หลายทำให้เกิดเป็นนวัตกรรมและบรรลุเป้าหมายที่หน่วยงานตั้งไว้ รวมทั้งเป็นการเพิ่มความโปร่งใสให้แก่หน่วยงานภาครัฐ ควรจะหลีกเลี่ยงข้อจำกัดในการใช้งานข้อมูล

โดยกิจกรรมของธรรมาภิบาลข้อมูลภาครัฐที่เกี่ยวข้องกับการเปิดเผยข้อมูล ควรประกอบไปด้วย 1) กำหนดบทบาทหน้าที่ของบุคคลที่เกี่ยวข้อง 2) กำหนดนโยบายการเปิดเผยข้อมูล และ 3) กำหนดแนวปฏิบัติในการเปิดเผยข้อมูล ดังนี้

1) กำหนดบทบาทหน้าที่ ที่เกี่ยวข้องกับการเปิดเผยข้อมูล

1.1 กำหนดบุคคลหรือกลุ่มบุคคลที่มีสิทธิ์ตัดสินใจในการเปิดเผยข้อมูล เช่น คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council) หรือ คณะทำงานเปิดเผยข้อมูล

1.2 กำหนดบุคคลหรือกลุ่มบุคคลในการดำเนินการและปรับปรุงการเปิดเผยข้อมูล

1.3 กำหนดบุคคลหรือกลุ่มบุคคลในการรับเรื่องและแก้ไขปัญหาเบื้องต้น ในการเข้าถึงข้อมูลและการนำข้อมูลไปใช้ เช่น ศูนย์ติดต่อ (Contact Center)

2) กำหนดนโยบายการเปิดเผยข้อมูล

ในหัวข้อ 3.3.1 ได้แสดงกรอบนโยบายข้อมูลในหมวดการเปิดเผยข้อมูล ดังนี้

2.1 ห้ามเปิดเผยข้อมูลที่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง นโยบาย แนวปฏิบัติ ไม่ว่าข้อมูลจะอยู่ในรูปแบบใดหรือสถานที่ใดก็ตาม

2.2 ต้องได้รับการอนุญาตจากตัวแทนหน่วยงานหรือเจ้าของข้อมูลก่อน การเปิดเผยข้อมูล

2.3 ควรมีการระบุช่องทางการเปิดเผยข้อมูลที่เข้าถึงและนำไปใช้ได้ง่าย

2.4 ควรมีการเปิดเผยเมทาดาตาควบคู่ไปกับข้อมูลที่เปิดเผย

2.5 สามารถตรวจสอบได้ว่าการเปิดเผยข้อมูลได้ถูกดำเนินการอย่างเหมาะสมหรือเป็นไปตามแนวทางที่ได้กำหนดไว้ เพื่อให้ได้ข้อมูลที่มีคุณภาพ และเป็นการรักษาคุณภาพของข้อมูล

3) กำหนดแนวปฏิบัติการเปิดเผยข้อมูล

แนวปฏิบัติการเปิดเผยข้อมูลเป็นไปตามขั้นตอนต่อไปนี้

3.1 คัดเลือกชุดข้อมูลที่ต้องการเผยแพร่ ทั้งนี้ควรจะต้องพิจารณาชุดข้อมูลที่มีคุณภาพและเป็นที่ต้องการของทุกภาคส่วน เพื่อส่งเสริมให้เกิดการนำไปใช้อย่างแพร่หลายและเกิดประโยชน์สูงสุด

3.2 พิจารณาชุดข้อมูลที่คัดเลือก ชุดข้อมูลที่คัดเลือกสำหรับเผยแพร่ นั้น ต้องอยู่ในชั้นความลับที่สามารถเผยแพร่ได้ นั่นคือ ต้องไม่ขัดต่อกฎหมายระเบียบ ข้อบังคับ ความมั่นคงของประเทศ ความลับทางราชการ และความเป็นส่วนตัว

3.3 จัดเตรียมข้อมูลให้อยู่ในรูปแบบที่ง่ายต่อการนำไปใช้ นั่นคือ ข้อมูลควรอยู่ในรูปแบบที่คอมพิวเตอร์สามารถอ่านได้ (Machine-Readable) หรือระดับการเปิดเผยข้อมูล ระดับ 3 ขึ้นไป เช่น รูปแบบของ Comma Separated Values - CSV Application Programming Interface - API รวมถึงการจัดทำคำอธิบายชุดข้อมูล (Metadata) เพื่อให้ผู้ใช้ข้อมูลสามารถเข้าใจเกี่ยวกับบริบทของข้อมูล เช่น เจ้าของข้อมูล วัตถุประสงค์ ขอบเขต วันที่เผยแพร่ ความถี่ในการปรับปรุง ความถี่ในการเผยแพร่ แหล่งที่มาของข้อมูล

3.4 นำชุดข้อมูลขึ้นเผยแพร่ หน่วยงานจะต้องกำหนดผู้รับผิดชอบหลักเพื่อนำชุดข้อมูลขึ้นเผยแพร่สู่สาธารณะ ซึ่งสามารถดำเนินการได้ ดังนี้

- เผยแพร่ผ่านเว็บไซต์หรือ Universal Resource Identifier
- URI ของหน่วยงาน พร้อมคำอธิบายชุดข้อมูล
- เผยแพร่ผ่านศูนย์กลางข้อมูลเปิดภาครัฐ โดยปฏิบัติตามเอกสาร คู่มือการนำข้อมูลขึ้นเผยแพร่บน data.go.th

- ผู้ใช้ข้อมูลถือได้ว่าเป็นผู้ที่มีส่วนร่วมในกระบวนการปรับปรุงคุณภาพของข้อมูลที่หน่วยงานได้เผยแพร่ผ่านช่องทางในการแสดงความคิดเห็นและการร้องขอข้อมูลที่ต้องการได้ ซึ่งการเปิดเผยข้อมูลที่มีคุณภาพและตรงกับความต้องการของผู้บริโภคนั้น จะช่วยให้เกิดการสร้างนวัตกรรมและยกระดับคุณภาพชีวิตของประชาชน

ภาคผนวก จ

แนวนโยบายและแนวปฏิบัติอื่น ๆ

ในส่วนนี้กล่าวถึงแผนการจัดทำนโยบาย มาตรฐาน และแนวปฏิบัติ เพื่อใช้ในธรรมาภิบาลข้อมูลและบริหารจัดการข้อมูลภายในหน่วยงานให้เป็นรูปธรรม มีรายละเอียดดังนี้

1) **นโยบายข้อมูล (Data Policy)** อธิบายถึงบทบาทหน้าที่ ข้อควรปฏิบัติ และข้อห้ามปฏิบัติในการบริหารจัดการข้อมูล นโยบายข้อมูลอาจจะประกอบไปด้วย นโยบายความมั่นคงปลอดภัยและความเป็นส่วนตัวส่วนบุคคลของข้อมูล (Data Security and Privacy Policy) นโยบายคุณภาพข้อมูล (Data Quality Policy) นโยบายการแลกเปลี่ยนและเชื่อมโยงข้อมูล (Data Exchange and Integration Policy) และนโยบายการเปิดเผยข้อมูล (Data Disclosure Policy)

2) **มาตรฐานการจัดชั้นความลับข้อมูล (Data Classification Standard)** อธิบายถึงรูปแบบและวิธีการจัดชั้นความลับของข้อมูลให้สอดคล้องกับผลกระทบหรือความเสียหายในด้านต่าง ๆ ได้แก่ เงิน ชื่อเสียง และความมั่นคง ทั้งในระดับบุคคล ระดับหน่วยงาน และระดับประเทศ ซึ่งจะ เป็นประโยชน์ในการกำหนดมาตรการรักษาความปลอดภัยของข้อมูล รวมถึง การอนุญาตให้สามารถทำการแลกเปลี่ยนหรือเปิดเผยข้อมูลได้

3) **มาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูล (Data Integration Standard)** เป็นการกำหนดรูปแบบ วิธีการ และเทคโนโลยีในการเชื่อมโยง และแลกเปลี่ยนข้อมูล เช่น มาตรฐานชุดข้อมูลอ้างอิงพื้นฐานสำหรับการแลกเปลี่ยนข้อมูล (Core Vocabulary) มาตรฐานชุดข้อมูลที่ควรเปิดเผยของ ประเทศ (National Open Datasets Standard)

4) แนวปฏิบัติในการปกป้องข้อมูลที่สามารถระบุตัวบุคคลได้ (Guideline to Protect the Personally Identifiable Information) ให้แนวทางสำหรับหน่วยงานที่จัดเก็บข้อมูลส่วนบุคคล ได้เตรียมข้อมูลให้เหมาะสมต่อการบูรณาการข้อมูลเข้าด้วยกัน เพื่อป้องกันไม่ให้หน่วยงานปลายทางทราบได้ว่าข้อมูลที่ได้รับเป็นของบุคคลใด

5) แนวปฏิบัติในด้านความมั่นคงปลอดภัยและความเป็นส่วนตัวของข้อมูล (Data Security and Privacy Guideline) ให้แนวทางในการบริหารจัดการความมั่นคงปลอดภัยของข้อมูลและความเป็นส่วนตัว ซึ่งจะต้องสอดคล้องกับนโยบายความมั่นคงปลอดภัยและความเป็นส่วนตัวของข้อมูล เช่น การจัดทำสถาปัตยกรรมความมั่นคงปลอดภัยของข้อมูล (Data Security Architecture) การควบคุมการเข้าถึงข้อมูล (Data Access Control) การตรวจสอบความมั่นคงปลอดภัยของข้อมูล (Data Security Audit) การประเมินความปลอดภัยของข้อมูล (Data Security Assessment) การกำหนดเครื่องมือและเทคโนโลยีความมั่นคงปลอดภัยของข้อมูล (Data Security Tool/Technology)

6) แนวปฏิบัติในด้านคุณภาพข้อมูล (Data Quality Guideline) ให้แนวทางในการวิเคราะห์คุณภาพข้อมูล (Data Profiling) และแนวปฏิบัติในการจัดเตรียมข้อมูลและทำความสะอาดข้อมูล (Data Preparation and Data Cleansing) เพื่อให้ข้อมูลอยู่ในรูปแบบที่เหมาะสมสำหรับการวิเคราะห์ข้อมูลและการนำไปใช้ตัดสินใจ

7) แนวปฏิบัติในการเปิดเผยข้อมูล เพื่อสร้างความรู้ ความเข้าใจให้แก่หน่วยงาน ภาคเอกชน และผู้ที่ต้องการศึกษาเกี่ยวกับข้อมูลเปิด (Open Data) ประกอบด้วย คู่มือการเปิดเผยข้อมูล (Open Data Handbook) Version 2 และแนวปฏิบัติในการเปิดเผยข้อมูลในรูปแบบ Public API

8) **แนวปฏิบัติในการออกแบบความคิดเชิงนวัตกรรมด้านข้อมูล (Data Innovation Guideline)** เป็นแนวปฏิบัติในการออกแบบความคิดเชิงนวัตกรรม (Guidelines for Data Innovation) เป็นคู่มือที่ช่วยให้เข้าใจปัญหาที่แท้จริง และสามารถออกแบบแนวทางแก้ไขปัญหาที่เป็นแนวคิดเชิงนวัตกรรม ตลอดจนสามารถเข้าถึงชุดข้อมูล (Datasets) ต่าง ๆ เพื่อให้ได้มาซึ่งแนวทางในการแก้ปัญหา นอกจากนั้นผู้ที่ต้องการศึกษากระบวนการออกแบบนวัตกรรมสามารถนำไปประยุกต์หรือปรับใช้กับหน่วยงานได้

9) **แนวปฏิบัติในการประเมินผลธรรมาภิบาลข้อมูลภาครัฐ (Data Governance Assessment Guideline)** ให้แนวทางในการประเมินผลธรรมาภิบาลข้อมูลภาครัฐ ประกอบด้วย การประเมินความพร้อมของธรรมาภิบาลข้อมูลภาครัฐ (Data Governance Readiness Assessment) การประเมินคุณภาพของข้อมูล (Data Quality Assessment) และการประเมินความมั่นคงปลอดภัยของข้อมูล (Data Security Assessment)

ภาคผนวก จ

แนวคิดธรรมาภิบาลข้อมูลจากต่างประเทศ

ในส่วนนี้อธิบายแนวคิดธรรมาภิบาลข้อมูลภาครัฐของหน่วยงานต่างประเทศ เพื่อใช้เป็นแนวทางในการจัดทำธรรมาภิบาลข้อมูลภาครัฐสำหรับหน่วยงานภาครัฐ ซึ่งมีรายละเอียดดังนี้

แนวคิดของ Data Governance Institute (DGI)

DGI (Thomas, 2009) เป็นหน่วยงานที่ให้แนวทางและแนวปฏิบัติในธรรมาภิบาลข้อมูลภาครัฐ โดยหน่วยงานต่าง ๆ จากทั่วโลกสามารถนำไปประยุกต์ใช้อย่างกว้างขวาง DGI เสนอธรรมาภิบาลข้อมูลภาครัฐ ซึ่งมี 10 องค์ประกอบ และถูกจัดกลุ่มเป็น 3 หมวด ดังนี้

1) กฎเกณฑ์ (Rules of Engagement)

- องค์ประกอบที่ 1 วิสัยทัศน์และภารกิจ (Vision and Mission)
- องค์ประกอบที่ 2 เป้าหมาย การวัดธรรมาภิบาล/การวัดความสำเร็จ และยุทธศาสตร์การจัดการเงินทุน (Goals, Governance Metrics/Success Measures, Funding Strategies)
- องค์ประกอบที่ 3 นิยามข้อมูลและกฎเกณฑ์ (Data Definitions and Rules)
- องค์ประกอบที่ 4 สิทธิในการตัดสินใจ (Decision Rights)
- องค์ประกอบที่ 5 ความสามารถในการตรวจสอบได้และการรับผิดชอบในผลของการดำเนินการ (Accountabilities)
- องค์ประกอบที่ 6 การควบคุมความเสี่ยง (Control)

2) โครงสร้างธรรมาภิบาลและบุคลากร (People and Organizational Bodies)

- องค์ประกอบที่ 7 ผู้มีส่วนได้เสีย (Data Stakeholders) คือ บุคลากรของหน่วยงานที่มีส่วนเกี่ยวข้องกับข้อมูล เช่น บุคคลที่ทำหน้าที่บันทึกข้อมูล ใช้ข้อมูล และกำหนดกฎเกณฑ์และความต้องการที่เกี่ยวข้องกับข้อมูล ผู้มีส่วนได้เสียระดับบริหาร (Executive Stakeholders) จะถูกกำหนดให้เป็น คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Board) เพื่อทำหน้าที่ ดูแลภาพรวมของธรรมาภิบาลข้อมูลภาครัฐ กำหนดนโยบายข้อมูล และแก้ไขปัญหา
- องค์ประกอบที่ 8 สำนักงานธรรมาภิบาลข้อมูล (Data Governance Office) คือ กลุ่มคนที่ทำหน้าที่ช่วยเหลือและสนับสนุนกลุ่มบุคคลอื่น ๆ ที่ ดำเนินการเกี่ยวกับธรรมาภิบาลข้อมูลภาครัฐ เช่น สนับสนุนการสื่อสารระหว่าง บุคคลในกิจกรรมที่เกี่ยวข้องกับธรรมาภิบาลข้อมูลภาครัฐ สนับสนุนการเข้าถึง แหล่งข้อมูล ให้ความรู้ที่เกี่ยวข้องกับธรรมาภิบาลข้อมูลภาครัฐ
- องค์ประกอบที่ 9 บริกรข้อมูล (Data Stewards) คือ บุคคลที่อยู่ใน คณะกรรมการบริกรข้อมูล (Data Stewardship Council) ทำหน้าที่ร่าง นโยบายข้อมูล ระบุมาตรฐานที่จะใช้ และอาจให้คำแนะนำต่อคณะกรรมการ ธรรมาภิบาลข้อมูล

3) กระบวนการธรรมาภิบาลข้อมูลภาครัฐ (The Process of Governing Data)

- องค์ประกอบที่ 10 กระบวนการธรรมาภิบาลข้อมูลภาครัฐ ประกอบด้วย กำหนดเป้าหมายและยุทธศาสตร์ เตรียมแผนงาน วางแผนงาน และงบประมาณ ออกแบบแผนดำเนินการ ประกาศใช้แผนดำเนินการ ธรรมาภิบาลข้อมูล และติดตามการดำเนินงาน/วัดผลการดำเนินงาน/รายงานผล การดำเนินงาน

แนวคิดของ Data Management Association International (DAMA International)

DAMA International (Henderson et al., 2017) เป็นองค์กรอิสระที่รวบรวมผู้เชี่ยวชาญด้านข้อมูลเข้าด้วยกัน เพื่อส่งเสริมให้เกิดความรู้ ความเข้าใจ และสนับสนุนให้เกิดการพัฒนาแนวคิด และแนวปฏิบัติในการบริหารจัดการข้อมูล โดยมีธรรมาภิบาลข้อมูลภาครัฐเป็นหนึ่งในองค์ประกอบหลักของการบริหารจัดการข้อมูล วัตถุประสงค์ของธรรมาภิบาลข้อมูลภาครัฐ เป็นการตรวจสอบเพื่อให้ทราบแน่ชัดว่าข้อมูลต่าง ๆ มีการบริหารจัดการอย่างถูกต้องตรงตามนโยบาย และแนวทางปฏิบัติที่ดีที่สุด รวมถึงมีการปฏิบัติตามกฎระเบียบ ซึ่งธรรมาภิบาลข้อมูลภาครัฐที่ดีต้องสอดคล้องกับยุทธศาสตร์ของหน่วยงาน มุ่งเน้นการลดความเสี่ยง ทั้งด้านความปลอดภัยของข้อมูล รักษาความเป็นส่วนตัว หรือปรับปรุงกระบวนการปฏิบัติงาน เพื่อให้ได้ข้อมูลที่มีคุณภาพ สำหรับเป้าหมายของธรรมาภิบาลข้อมูลภาครัฐ เพื่อให้หน่วยงานสามารถบริหารจัดการข้อมูลในลักษณะของทรัพย์สินได้ โดยนำเสนอหลักการ นโยบาย กระบวนการ กรอบธรรมาภิบาลข้อมูล และบริหารจัดการข้อมูล เพื่อเป็นแนวทางในการบริหารจัดการข้อมูลทุกระดับ DAMA International ได้กล่าวถึง โครงสร้างของบุคลากรที่รับผิดชอบในธรรมาภิบาลข้อมูลภาครัฐและกระบวนการธรรมาภิบาลข้อมูลภาครัฐ ดังนี้

1) โครงสร้างของบุคลากรที่รับผิดชอบในธรรมาภิบาลข้อมูลภาครัฐ ประกอบด้วย

- คณะกรรมการขับเคลื่อนธรรมาภิบาลข้อมูลภาครัฐ (Data Governance Steering Committee) เป็นผู้มีอำนาจสูงสุดในการขับเคลื่อนให้เกิดธรรมาภิบาลข้อมูลภาครัฐ โดยมีหน้าที่รับผิดชอบในธรรมาภิบาล สนับสนุน และระดมทุนของกิจกรรมที่เกี่ยวข้อง ส่วนใหญ่คณะกรรมการจะเป็นผู้บริหารระดับสูงของแต่ละหน่วยงานมาดำเนินงานร่วมกัน

- คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council) เป็นกลุ่มบุคคลที่ริเริ่ม และยกระดับการบริหารจัดการธรรมาภิบาลข้อมูลภาครัฐภายในหน่วยงาน ซึ่งคณะกรรมการจะเป็นผู้บริหารจากฝ่ายงานต่าง ๆ ทั้งจากฝ่ายบริหารและฝ่ายเทคโนโลยีสารสนเทศรวมไปถึงระดับหัวหน้างาน ทำหน้าที่จัดทำและตัดสินใจในเชิงนโยบาย

- สำนักงานธรรมาภิบาลข้อมูล (Data Governance Office) มีหน้าที่ในการนิยามข้อมูลและมาตรฐานข้อมูลในภาพรวมของทั้งหน่วยงาน โดยการประสานงานกับบริกรข้อมูล (Data Stewards) บริกรข้อมูลด้านเทคนิค (Technical Data Stewards) และเจ้าของข้อมูล (Data Owner)

- ทีมบริกรข้อมูล (Data Steward Team) กลุ่มบุคคลที่มุ่งเน้นการดำเนินงาน และกำหนดมาตรฐานในการบริหารจัดการตามองค์ประกอบของการบริหารจัดการข้อมูลอย่างน้อยหนึ่งองค์ประกอบ กลุ่มบุคคลที่เกี่ยวข้องประกอบไปด้วย บริกรข้อมูล (Data Stewards) บริกรข้อมูลด้านเทคนิค (Technical Data Stewards) และนักวิเคราะห์ข้อมูล (Data Analyst)

- คณะกรรมการธรรมาภิบาลข้อมูลภายในหน่วยงาน (Local Data Governance Committee) ในหน่วยงานขนาดใหญ่อาจมีผลงานที่ดูแลเกี่ยวกับธรรมาภิบาลข้อมูลภาครัฐโดยเฉพาะที่อยู่ภายใต้การทำงานขอคณะกรรมการธรรมาภิบาลข้อมูล

2) กระบวนการธรรมาภิบาลข้อมูลภาครัฐ เริ่มตั้งแต่การวางแผนไปจนถึงการดำเนินธรรมาภิบาลอย่างต่อเนื่อง มีรายละเอียดดังนี้

- การวางแผนธรรมาภิบาลข้อมูลภาครัฐโดยการกำหนดเป้าหมายหลักการ นโยบาย กลยุทธ์ และประเด็นปัญหาในธรรมาภิบาล มีการประเมินความพร้อมของหน่วยงาน เตรียมการสำหรับการบริหารการเปลี่ยนแปลง และดำเนินงานให้เป็นไปตามเป้าหมาย และระยะเวลาที่กำหนด

- ดำเนินการที่เกี่ยวข้องกับข้อมูลให้เป็นไปตามธรรมาภิบาลข้อมูลภาครัฐ เช่น การกำหนดมาตรฐานข้อมูล
- ดำเนินการธรรมาภิบาลข้อมูลภาครัฐในหน่วยงานให้สอดคล้องกับแผนงานที่ได้กำหนดไว้

ภาคผนวก ข

กรณีศึกษาธรรมาภิบาลข้อมูลจากต่างประเทศ

ในส่วนนี้กล่าวถึงกรณีศึกษาธรรมาภิบาลข้อมูลภาครัฐของหน่วยงานต่างประเทศ ซึ่งเป็นการประยุกต์ใช้แนวคิดธรรมาภิบาลข้อมูลภาครัฐ โดยมีรายละเอียดดังนี้

กรณีศึกษาของประเทศออสเตรเลีย

ประเทศออสเตรเลียมีหน่วยงานกลางในธรรมาภิบาลข้อมูลภาครัฐ เพื่อกำหนดมาตรฐานในการจัดเก็บ การใช้ การเชื่อมโยงระหว่างหน่วยงาน และการบริหารจัดการข้อมูลที่เกิดขึ้นภายในประเทศออสเตรเลีย อย่างไรก็ตาม หน่วยงานภาครัฐบางส่วนมีการกำหนดธรรมาภิบาลข้อมูลภาครัฐของหน่วยงานเอง เช่น Workplace Gender Equality Agency และ Australian Institute of Health and Welfare ซึ่งมีรายละเอียด ดังนี้

1) หน่วยงานกลางในธรรมาภิบาลข้อมูลภาครัฐ

ประเทศออสเตรเลียมีการจัดตั้ง Data Governance Australia (DGA) เพื่อธรรมาภิบาลข้อมูล และสร้างความเชื่อมั่นให้กับหน่วยงานต่าง ๆ (ทั้งภาครัฐและภาคเอกชน) ในการแลกเปลี่ยนข้อมูลโดยไม่ผิดข้อกำหนดฯ ซึ่งจะทำให้การดำเนินการของภาครัฐและภาคเอกชนที่ใช้ข้อมูลเป็นไปได้อย่างดี DGA ได้ก่อตั้งขึ้นเมื่อปี พ.ศ.2559 โดยคณะกรรมการบริหารเป็นผู้เชี่ยวชาญเกี่ยวกับข้อมูลจากหลากหลายองค์กร ได้แก่ มหาวิทยาลัย หน่วยงานภาครัฐ และหน่วยงานเอกชน

เป้าหมายของ DGA คือการสร้างมาตรฐานในกระบวนการเก็บ การใช้ และการบริหารจัดการข้อมูลที่เกิดขึ้นภายในประเทศออสเตรเลีย โดยทำหน้าที่ให้ข้อมูลเกี่ยวกับธรรมาภิบาลข้อมูลภาครัฐและการเชื่อมโยงข้อมูล

ระหว่างหน่วยงานกับผู้ที่เป็สมาชิก ซึ่งหน่วยงานที่เป็นสมาชิกจะได้รับการ
อบรมเรื่องต่าง ๆ ที่เกี่ยวข้องกับธรรมาภิบาลข้อมูลภาครัฐ ไม่ว่าจะเป็นข้อ
กำหนดในธรรมาภิบาล การแลกเปลี่ยนข้อมูลโดยไม่ขัดกับข้อกำหนด กฎหมาย
หรือนโยบายที่ถูกกำหนดโดยรัฐบาลกลางออสเตรเลีย นอกจากนี้ยังมีการให้
บริการข้อมูลที่เกี่ยวข้องกับสมาชิก โดยเฉพาะเรื่องเกี่ยวกับแนวโน้มธรรมาภิบาลข้อมูล
จากต่างประเทศอีกด้วย โดยประโยชน์ที่สมาชิกจะได้รับมี 7 ข้อ ดังนี้

- การสนับสนุนจากรัฐบาล โดยหน่วยงานที่เป็นสมาชิกจะได้รับการ
ดูแลในเรื่องที่สำคัญ เกี่ยวกับข้อมูล ได้แก่ ความเป็นส่วนบุคคล ความปลอดภัย
จากจู่โจมทางอินเทอร์เน็ต การควบคุมและดูแลข้อมูล การใช้ และความเสี่ง
ในการใช้งานข้อมูล
- มาตรฐานและคู่มือการใช้งาน มีการจัดทำคู่มือและมาตรฐานให้
ศึกษาเพื่อให้สมาชิกสามารถดำเนินกิจกรรมที่เกี่ยวข้องกับข้อมูลได้เป็นอย่างดี
- เครื่องหมายความไว้วางใจของ DGA โดยสมาชิกจะได้รับการดูแล
จนกระทั่งได้ตามมาตรฐานของ DGA ซึ่งการมีมาตรฐาน DGA จะทำให้สมาชิก
เป็นที่ยอมรับจากสมาชิกอื่น ๆ ทำให้การเชื่อมโยงข้อมูลกับหน่วยงานอื่น ๆ ที่
มีมาตรฐานเดียวกันเป็นไปได้ด้วยดี
- มาตรฐานของธรรมาภิบาลข้อมูลภาครัฐ มาตรฐานของ DGA เป็น
ที่ยอมรับจากมหาวิทยาลัยในเรื่องธรรมาภิบาลข้อมูลภาครัฐ
- หลักสูตร มีการกำหนดหลักสูตรการศึกษาต่าง ๆ ที่จะช่วยให้
สมาชิกมีความเข้าใจในธรรมาภิบาลรวมถึงหลักปฏิบัติในธรรมาภิบาลข้อมูลภาครัฐ
- กิจกรรม มีกิจกรรมส่งเสริมความเข้าใจในเรื่องธรรมาภิบาลข้อมูลภาครัฐ
ให้กับสมาชิกสามารถเข้าร่วมได้โดยไม่มีค่าใช้จ่าย
- งานวิจัยและบทความ สมาชิกสามารถอ่านบทความและงานวิจัย
ที่วิเคราะห์ธรรมาภิบาลข้อมูลภาครัฐ รวมถึงแนวโน้มการเปลี่ยนแปลงของ
ธรรมาภิบาลข้อมูลภาครัฐของโลกด้วย

อย่างไรก็ตามพันธกิจของหน่วยงานกลางเน้นในการแลกเปลี่ยนข้อมูลเป็นหลัก แต่ไม่ได้เน้นในเรื่องของโครงสร้างธรรมาภิบาลข้อมูลภาครัฐที่ชัดเจน ทั้งนี้โครงสร้างธรรมาภิบาลข้อมูลภาครัฐจะขึ้นอยู่กับแต่ละหน่วยงาน ซึ่งได้อธิบายไว้ในหัวข้อ ธรรมาภิบาลข้อมูลภาครัฐของ Workplace Gender Equality Agency และ Australian Institute of Health and Welfare

2) ธรรมาภิบาลข้อมูลภาครัฐของหน่วยงาน Workplace Gender Equality Agency (WGEA)

WGEA มีหน้าที่ในการส่งเสริมและปรับปรุงความเสมอภาคกันทางเพศในสถานที่ทำงานในประเทศออสเตรเลีย ซึ่งได้ดำเนินงานเรื่องความเสมอภาคกันทางเพศในสถานที่ทำงาน โดยการร่วมมือกับนายจ้างเพื่อให้คำปรึกษา แนะนำช่วยเหลือนายจ้างเรื่องความเสมอภาคทางเพศ เป้าหมายในการสร้างกรอบธรรมาภิบาลของหน่วยงานนี้ คือ การให้หน่วยงานมีนโยบายและขั้นตอนการจัดการข้อมูลที่ดีที่สุดในการปฏิบัติงาน สนับสนุนให้เกิดการจัดการข้อมูลที่มีประสิทธิภาพและกลายเป็นส่วนหนึ่งของการปฏิบัติงาน โดยมีธรรมาภิบาลเพื่อควบคุมการบริหารจัดการข้อมูลตลอดทั้งระบบบริหารและกระบวนการจัดการข้อมูลหรือวงจรชีวิตข้อมูล ได้แก่ การวางแผน การเก็บข้อมูล การวิเคราะห์ และการเปิดเผย ทั้งนี้แนวคิดของธรรมาภิบาลข้อมูลภาครัฐของหน่วยงานได้ร่างแบบศึกษามาจากกรอบธรรมาภิบาลของ DGI และกรอบการบริหารจัดการข้อมูลของ DAMA International

กรอบธรรมาภิบาลของหน่วยงานประกอบด้วย 3 ส่วนสำคัญ ได้แก่

- บุคลากร มีการกำหนดหน้าที่และความรับผิดชอบที่ชัดเจน ประกอบด้วย ขอบบริการข้อมูล (Data Stewards) และบริการข้อมูลด้านเทคนิค (Technical Data Stewards) รวมไปถึงบุคลากรอื่น ๆ ที่เกี่ยวข้องกับข้อมูล

- ธรรมาภิบาลและการปกครอง มีสาระสำคัญคือกลยุทธ์และเป้าหมายทางธุรกิจของหน่วยงานตลอดจนขอบเขตการทำงาน นอกจากนี้ยังได้กำหนดกิจกรรมการจัดการและการสนับสนุนทรัพยากรของหน่วยงานด้วย
- ระบบการดำเนินการ ประกอบด้วย นโยบาย ขั้นตอนความปลอดภัย อุปกรณ์ โปรแกรมคอมพิวเตอร์ แอปพลิเคชัน และเครื่องมือต่าง ๆ ที่สนับสนุนการจัดการข้อมูลที่มีประสิทธิภาพ รวมไปถึงมาตรฐานในการดำเนินงานเพื่อทำให้เกิดธรรมาภิบาลข้อมูลภาครัฐ โดยมีกลุ่มบุคลากรจำนวนหนึ่งทำหน้าที่สร้างมาตรฐาน และดำเนินงานเกี่ยวกับมาตรฐานของข้อมูล นอกจากนี้บุคลากรกลุ่มนี้ต้องมีการวัดมาตรฐานของข้อมูลในปีที่ผ่านมา และต้องมีการตรวจสอบการดำเนินการข้อมูลของบุคลากรที่เกี่ยวข้องกับข้อมูลอีกด้วย

3) ธรรมาภิบาลข้อมูลภาครัฐของหน่วยงาน Australian Institute of Health and Welfare (AIHW)

AIHW เป็นหน่วยงานที่ให้ข้อมูลที่น่าเชื่อถือเกี่ยวกับสุขภาพและสวัสดิการของออสเตรเลีย นอกจากนี้ยังสนับสนุนการพัฒนานโยบาย โครงการด้านสุขภาพและสวัสดิการของประเทศออสเตรเลีย

- ภาพรวมของธรรมาภิบาลข้อมูลภาครัฐของ AIHW ได้แก่
- คำอธิบายของแนวคิดหลักในการจัดการข้อมูล
- กฎหมายที่เกี่ยวข้องกับธรรมาภิบาลของ AIHW
- โครงสร้างและบทบาทของการจัดการข้อมูล
- ภาพรวมของนโยบายขั้นตอนและหลักเกณฑ์เกี่ยวกับข้อมูล AIHW
- ระบบและเครื่องมือที่สนับสนุนการจัดการข้อมูล
- แนวทางการปฏิบัติตามกฎระเบียบ
- แนวคิดธรรมาภิบาลข้อมูลภาครัฐ ได้แก่ การเก็บรวบรวมข้อมูล

ธรรมาภิบาลและการจัดการข้อมูล การลงทะเบียนข้อมูล มาตรฐานเมทาดาตา คู่มือเกี่ยวกับนโยบาย หลักเกณฑ์ และวิธีการในการดำเนินการ และเครื่องมือที่จะใช้ในการทำงาน

ธรรมาภิบาลข้อมูลภาครัฐของ AIHW มีรายละเอียด ดังนี้

- กฎหมาย นโยบายที่เกี่ยวข้องกับธรรมาภิบาลข้อมูลภาครัฐ มีการระบุถึงกฎหมายภายนอกหน่วยงานที่อาจจะเกี่ยวข้องกับการดำเนินธรรมาภิบาลข้อมูลภาครัฐของ AIHW นอกจากนี้ยังระบุถึงนโยบายการใช้ข้อมูลของหน่วยงาน
- โครงสร้างและบทบาทของ AIHW ในการจัดการข้อมูล มีการกำหนดบทบาทที่ชัดเจนภายในหน่วยงาน ตั้งแต่ บอร์ดบริหาร ไปจนถึงบุคลากรที่ทำงานกับข้อมูลโดยตรง รวมไปถึงผู้ตรวจสอบข้อมูล
- นโยบายข้อมูลและขั้นตอนในการปฏิบัติงาน ระบุถึงการดำเนินงานเกี่ยวกับข้อมูลภายใน AIHW นอกจากนี้ยังได้ระบุถึง Data Linkage ซึ่งระบุถึงการเชื่อมโยงข้อมูลระหว่างหน่วยงาน ว่าต้องมีมาตรฐานตามที่หน่วยงานกลางกำหนด
- ระบบ AIHW และเครื่องมือเพื่อสนับสนุน ระบุถึงมาตรฐานและเครื่องมือในธรรมาภิบาลข้อมูลภาครัฐ

โดยสรุปแล้ว ธรรมาภิบาลข้อมูลภาครัฐของประเทศออสเตรเลียเป็นส่วนสำคัญให้เป็นประเทศที่ติดอันดับ 1 ใน 3 ของ Global E-Government Index ทั้งนี้หลายหน่วยงานในประเทศออสเตรเลียมีการเปิดเผยธรรมาภิบาลข้อมูลภาครัฐสู่สาธารณะ ซึ่งสามารถนำไปเป็นแนวทางในการกำหนดธรรมาภิบาลข้อมูลภาครัฐของประเทศไทย

กรณีศึกษาของประเทศเกาหลีใต้

ในการพัฒนาข้อมูลขนาดใหญ่ สำหรับระบบการให้บริการบำนาญบำนาญแห่งชาติของประเทศเกาหลีใต้ (National Pension Service of South Korea) (Kim, H. Y., & Cho, J. S., 2017) ได้กำหนดธรรมาภิบาลข้อมูลภาครัฐ โดยมี 4 องค์ประกอบ ดังนี้

1) วัตถุประสงค์ (Objective)

ธรรมาภิบาลข้อมูลภาครัฐขนาดใหญ่มีความต้องการเพื่อสร้างมูลค่าทางธุรกิจแบบใหม่ ซึ่งจะช่วยให้บริการของข้อมูลขนาดใหญ่สามารถบรรลุเป้าหมาย

2) ยุทธศาสตร์ (Strategy)

- การคุ้มครองข้อมูลส่วนบุคคล (Personal Information Protection) ได้แก่ นิยามระดับของการคุ้มครองข้อมูลส่วนบุคคลและกำหนดอุปกรณ์สำหรับการคุ้มครองข้อมูลส่วนบุคคล
- ระดับคุณภาพข้อมูล (Data Quality Level) ได้แก่ ความพร้อมใช้ของผลการวิเคราะห์ที่ได้รับจากข้อมูลขนาดใหญ่ ความเชื่อมั่นในผลการวิเคราะห์ ข้อมูลขนาดใหญ่มีความสัมพันธ์กับวัตถุประสงค์ของการวิเคราะห์ หรือสิ่งที่ต้องการทำนาย และความสามารถในการผลักดันผลการวิเคราะห์ถูกนำไปใช้ในสถานการณ์จริง
- การเปิดเผยข้อมูลและความรับผิดชอบ (Data Disclosure and Responsibility) ได้แก่ การกำหนดหน้าที่ความรับผิดชอบของเจ้าของข้อมูล การกำหนดหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องในการบริหารจัดการข้อมูล และการกำหนดขอบเขตของการเปิดเผยข้อมูล

3) ส่วนประกอบ (Component)

- โครงสร้างของการบริหารจัดการข้อมูลขนาดใหญ่ (Organization) บุคคลที่อยู่ภายในโครงสร้างนี้มีบทบาทและความรับผิดชอบในการบริหารจัดการข้อมูล การบริหารจัดการความมั่นคงปลอดภัย และการบริหารจัดการคุณภาพข้อมูล
- การจัดทำมาตรฐานและแนวปฏิบัติ (Standardization and Guideline) เช่น แนวปฏิบัติในการกำหนดโครงสร้างข้อมูลและวิธีการประมวลผลข้อมูล
- นโยบายข้อมูลและกระบวนการเกี่ยวกับข้อมูล (Policy and Process) เช่น การควบคุมดูแลและการวัดประสิทธิภาพจากการดำเนินงานเกี่ยวกับข้อมูล

4) โครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ (IT Infrastructure)

โครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศสำหรับข้อมูลขนาดใหญ่ต้องการทรัพยากรด้านการคำนวณ (ซีพียู แรม) และอุปกรณ์แบบใหม่ ในการลงทุนด้านทรัพยากรและอุปกรณ์ต้องมีความเหมาะสมกับระดับการบริการและการบำรุงรักษาที่ได้รับ นอกจากนี้ยังต้องมีการควบคุมและตรวจสอบความสอดคล้องกันระหว่างการดำเนินการ (ตั้งแต่ การรวบรวมข้อมูล การประมวลผลข้อมูล การวิเคราะห์ข้อมูล และการนำเสนอผลการวิเคราะห์) กับนโยบายข้อมูลที่กำหนดไว้

กรณีศึกษาของสหราชอาณาจักร

สหราชอาณาจักรมีประเทศและหน่วยงานที่ได้ดำเนินการธรรมาภิบาลข้อมูลและบริหารจัดการข้อมูลดังนี้

1) **Scottish Government's Data Linkage** มีการบริหารจัดการข้อมูลของหน่วยงานภาครัฐอย่างมีประสิทธิภาพและมีความน่าเชื่อถือเพื่อประโยชน์ในการบริการสาธารณะในด้าน

- การแลกเปลี่ยนข้อมูลส่วนบุคคลระหว่างหน่วยงานภาครัฐ
- การเชื่อมโยงข้อมูลระหว่างหน่วยงานภาครัฐ
- การเผยแพร่ข้อมูลทั่วไปแก่สาธารณชน
- วิเคราะห์ข้อมูลที่มีอยู่ด้วยวิธีใหม่ ๆ (Data Innovation)

2) **British Academy** เน้นธรรมาภิบาลข้อมูลภาครัฐของผู้มีส่วนได้เสียกับข้อมูล เพื่อ

- การบริหารจัดการข้อมูล
- การจัดการเกี่ยวกับบุคคลที่มีส่วนได้เสียกับข้อมูล
- การกำหนดมาตรการและแนวปฏิบัติเกี่ยวข้อง
- การสร้างความโปร่งใสและตรวจสอบได้

จากผลการศึกษาแนวคิดและกรณีศึกษาจากต่างประเทศสรุปได้ว่าธรรมาภิบาลข้อมูลภาครัฐเป็นหนึ่งในองค์ประกอบหลักของการบริหารจัดการข้อมูลเพื่อมุ่งเน้นการลดความเสี่ยง ทั้งด้านความปลอดภัยของข้อมูล รักษาความเป็นส่วนตัวส่วนบุคคล หรือปรับปรุงกระบวนการเพื่อให้ได้ข้อมูลที่มีคุณภาพสามารถเชื่อมโยง แลกเปลี่ยน และเปิดเผยข้อมูลได้

บรรณานุกรม

- 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. Second Edition. Technics Publications.
- 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.

