MDG
MWA Data Governance

DATA GOVERNANCE GUIDELINE

แนวปฏิบัติการดำเนินการธรรมาภิบาลข้อมูล

การประปานครหลวง

V. 1.2

สิงหาคม 2567

สารบัญ

เห็นชอบโดยคณะกรรมการธรรมาภิบาลข้อมูล ในการประชุมครั้งที่ 5/2567

เมื่อวันที่ 29 สิงหาคม 2567

ส่วนที่ 1 การกำกับดูแลข้อมูล

1.1 หลักการและขอบเขต

แนวปฏิบัติการการดำเนินการธรรมาภิบาลข้อมูล ได้กำหนดขึ้นให้สอดคล้องตามนโยบายธรรมาภิบาลข้อมูล (Data Governance Policy) ซึ่งเป็นหนึ่งในองค์ประกอบตามกรอบธรรมาภิบาลข้อมูลภาครัฐ เพื่อเป็นประโยชน์ต่อหน่วยงานต่าง ๆ ในการนำไปประยุกต์ใช้เป็นแนวทางอ้างอิงในการกำกับดูแลและบริหารจัดการข้อมูลในหน่วยงานให้มีคุณภาพ มีความมั่นคงปลอดภัย มีความเป็นส่วนบุคคล และสามารถใช้ประโยชน์จากข้อมูลในการดำเนินงานตามภารกิจได้อย่างเต็มประสิทธิภาพ โดยมีผลบังคับใช้กับผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับข้อมูลตามโครงสร้างธรรมาภิบาลข้อมูล ซึ่งมีหน้าที่โดยตรงที่จะต้องสนับสนุน ดำเนินการ และปฏิบัติตามอย่างเคร่งครัด และผู้ใช้อื่นที่เกี่ยวข้องแต่ไม่มีหน้าที่ในการดูแลข้อมูลจะต้องให้ความร่วมมือในการดำเนินการตามแนวปฏิบัตินี้ โดยแนวปฏิบัตินี้จะครอบคลุมกระบวนการบริหารจัดการข้อมูลตลอดวงจรชีวิตของข้อมูล

1.2 นิยามคำศัพท์

คำศัพท์	ความหมาย
องค์กร	การประปานครหลวง
คณะกรรมการ	คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council) ของการประปานครหลวง
เจ้าของข้อมูล (Data Owner)	หน่วยงานที่ทำหน้าที่รับผิดชอบดูแลข้อมูลโดยตรง สร้างความมั่นใจได้ว่าการบริหารจัดการข้อมูลสอดคล้องกับนโยบาย มาตรฐาน กฎระเบียบ หรือกฎหมาย เจ้าของข้อมูลทำการทบทวนและอนุมัติการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับข้อมูล
หน่วยงานกำกับดูแลข้อมูล (Data Governance Officer)	กองบริหารและจัดการข้อมูล ฝ่ายยุทธศาสตร์และนวัตกรรมดิจิทัล ทำหน้าที่ช่วยเหลือและสนับสนุนกลุ่มบุคคลอื่น ๆ ที่ดำเนินการเกี่ยวกับการกำกับดูแลข้อมูลด้านต่าง ๆ
บริกรข้อมูลเชิงธุรกิจ (Business Data Stewards)	บุคลากรที่ได้รับมอบหมายให้ทำหน้าที่กำหนดนิยามความต้องการ ด้านคุณภาพและความมั่นคงปลอดภัยซึ่งอาจจะได้รับมาจากผู้ใช้ข้อมูล (Data Users) หรือผู้มีส่วนได้ส่วนเสียอื่น ๆ นิยามคำอธิบายข้อมูลโดยการสนับสนุนจากผู้ใช้ข้อมูล ร่างนโยบายข้อมูลด้วยการช่วยเหลือจากหน่วยงานกำกับดูแล ตรวจสอบการปฏิบัติตามนโยบายข้อมูล ตรวจสอบคุณภาพ ตรวจสอบ ความมั่นคงปลอดภัยของข้อมูล วิเคราะห์ผลจากการตรวจสอบ แล้วรายงานผลลัพธ์ไปยังคณะกรรมการธรรมาภิบาลข้อมูลและผู้ที่เกี่ยวข้องอื่น ๆ ให้ทราบ

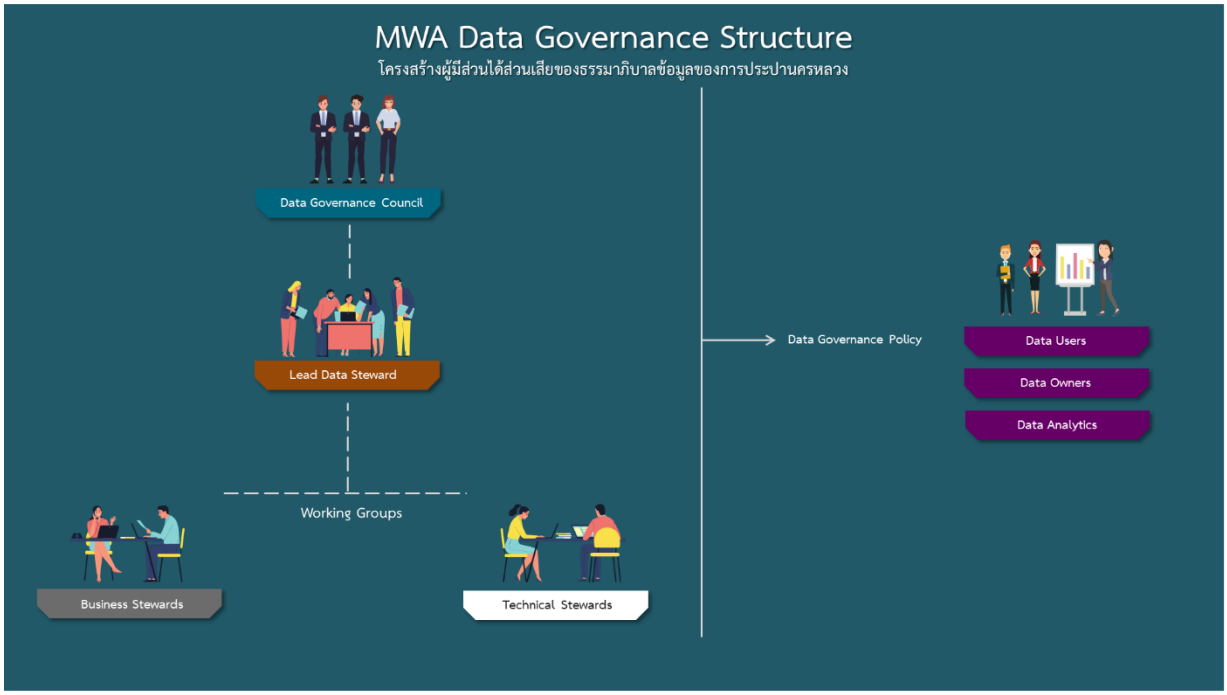
คำศัพท์	ความหมาย
บริกรข้อมูลเชิงเทคนิค (Technical Data Stewards)	บุคลากรที่ทำหน้าที่ให้การสนับสนุนด้านเทคโนโลยีสารสนเทศแก่บริกรข้อมูลด้านธุรกิจ เช่น นิยามเมทาดาตาเชิงเทคนิคซึ่งอาจจะได้รับการช่วยเหลือจากหน่วยงานกำกับดูแลข้อมูล ให้ข้อเสนอแนะเชิงเทคนิคในการร่างนโยบายธรรมาภิบาลข้อมูล ตรวจสอบคุณภาพข้อมูล ความมั่นคงปลอดภัยของข้อมูล และการปฏิบัติตามนโยบายธรรมาภิบาลข้อมูลในเชิงเทคนิค
ผู้ดูแลระบบสารสนเทศ (System Administrators)	บุคลากรที่มีหน้าที่ดูแลรับผิดชอบระบบสารสนเทศของหน่วยงาน
ข้อมูล (Data)	สิ่งที่สื่อความหมายให้รู้เรื่องราวข้อเท็จจริง หรือเรื่องอื่นใดไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้น หรือโดยผ่านวิธีการใด ๆ และไม่ว่าจะได้จัดทำไว้ทั้งการจัดเก็บในรูปของเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ภาพถ่ายดาวเทียม ฟิล์ม การบันทึกภาพ เสียง การจัดเก็บการบันทึกในเครื่องคอมพิวเตอร์ เครื่องมือตรวจวัด การสำรวจระยะไกล หรือวิธีอื่นใดที่ทำให้สิ่งบันทึกไว้ปรากฏได้ ข้อมูลในที่นี้ครอบคลุมทั้งข้อมูลที่มีโครงสร้าง ข้อมูลกึ่งโครงสร้าง และข้อมูลที่ไม่มีโครงสร้าง
ชุดข้อมูล (Dataset)	การนำข้อมูลจากหลายแหล่งมารวมเข้าด้วยกัน เพื่อจัดเป็นชุดให้ตรงตามลักษณะโครงสร้างของข้อมูล
ระบบสารสนเทศ (Information System)	ระบบงานที่นำเทคโนโลยีมาช่วยในการสร้างสารสนเทศที่สามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนา และควบคุมการติดต่อสื่อสาร ซึ่งประกอบด้วย เทคโนโลยี คอมพิวเตอร์ และเทคโนโลยีการสื่อสารโทรคมนาคม ได้แก่ ระบบคอมพิวเตอร์ (Computer System) ระบบเครือข่าย (Network System) ซอฟต์แวร์ (Software) ข้อมูล (Data) และสารสนเทศ (Information) เป็นต้น

1.3 การเผยแพร่และการทบทวน

แนวปฏิบัติการดำเนินการธรรมาภิบาลข้อมูลจะต้องทำการเผยแพร่โดยการประกาศเวียนในระบบอินทราเน็ต เพื่อให้เจ้าหน้าที่ทุกระดับในหน่วยงานได้รับทราบและถือปฏิบัติตามแนวปฏิบัตินี้อย่างเคร่งครัด โดยแนวปฏิบัติจะต้องมีการทบทวนเป็นประจำอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ รวมถึงเมื่อมีข้อเสนอแนะที่คณะกรรมการธรรมาภิบาลข้อมูลเห็นสมควร

1.4 โครงสร้างธรรมาภิบาลข้อมูลและบทบาทหน้าที่

โครงสร้างธรรมาภิบาลข้อมูลเป็นการกำหนดโครงสร้างบุคลากร และแสดงลำดับขั้นระหว่างกลุ่มบุคคลที่เกี่ยวข้องกับธรรมาภิบาลข้อมูล ตลอดจนการแสดงถึงสิทธิในการสั่งการตามลำดับขั้น



รูปที่ 1 โครงสร้างธรรมาภิบาลข้อมูล

โครงสร้างธรรมาภิบาลข้อมูลของการประปานครหลวง สามารถอธิบายได้ ดังนี้

บทบาท	หน้าที่และความรับผิดชอบ
คณะกรรมการธรรมาภิบาลข้อมูล	1. พิจารณากลั่นกรอง ทบทวน ปรับปรุง และให้ความเห็นชอบนโยบายข้อมูลองค์กรของ กปน. ให้เป็นไปตามกรอบธรรมาภิบาลข้อมูลภาครัฐและนำเสนอผู้ว่าการเพื่อพิจารณาอนุมัติ 2. ให้ความเห็นชอบ แนวทาง หลักเกณฑ์และวิธีปฏิบัติ การใช้ข้อมูล มาตรฐานข้อมูล เกณฑ์การวัดคุณภาพ การเปิดเผยข้อมูลให้กับหน่วยงานภายนอก เทคโนโลยีที่ใช้กำกับและจัดการข้อมูล ระเบียบข้อบังคับต่างๆ ที่เกี่ยวข้องกับข้อมูลของการประปานครหลวง เพื่อให้การดำเนินการธรรมาภิบาลข้อมูลเป็นไปอย่างมีประสิทธิภาพ 3. กำกับ เร่งรัด และติดตามดูแลให้หน่วยงานจัดทำบัญชีข้อมูลภายในหน่วยงานโดยระบุชุดข้อมูลและจัดระดับความสำคัญของข้อมูล 4. มีอำนาจแต่งตั้งคณะทำงานย่อย หรือเชิญหน่วยงานหรือบุคคลที่เกี่ยวข้องทั้งภายในและภายนอกองค์กรมาชี้แจง ให้ข้อมูล ให้คำปรึกษาและข้อเสนอแนะต่างๆ
หัวหน้าบริกรข้อมูล	1. ศึกษาและทำความเข้าใจ บริบทของทีมบริกรข้อมูลด้านต่าง ๆ ตามกรอบธรรมาภิบาลข้อมูล (Data Governance Framework) ที่ประกาศโดยภาครัฐและระดับสากล

บทบาท	หน้าที่และความรับผิดชอบ
	2. พิจารณา ให้ข้อเสนอแนะ และร่วมจัดทำ ทบทวน ปรับปรุง นโยบายและแนวทางปฏิบัติ ข้อกำหนด ระเบียบและวิธีการ เพื่อให้ข้อมูล พร้อมใช้งาน มีคุณภาพ มั่นคงปลอดภัย และรักษาความเป็นส่วนบุคคลให้กับผู้มีส่วนได้ส่วนเสียภายในองค์กร เสนอต่อคณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council) การประปานครหลวงพิจารณา 3. กำกับดูแล ตรวจสอบ ติดตามการปฏิบัติงาน ของคณะทำงานบริกรข้อมูลด้านต่าง ๆ ให้สอดคล้องกับนโยบายข้อมูลองค์กร 4. ส่งเสริมการสร้างความตระหนักรู้เกี่ยวกับนโยบายและแนวปฏิบัติ ให้กับผู้มีส่วนได้ส่วนเสีย 5. มีอำนาจเชิญหน่วยงาน หรือบุคคลที่เกี่ยวข้องทั้งภายในและภายนอกองค์กรมาชี้แจง ให้ข้อมูล ให้คำปรึกษาหรือข้อเสนอแนะต่าง ๆ 6. รายงานผลการดำเนินงานต่อคณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council) การประปานครหลวง รายปี
บริกรข้อมูลเชิงธุรกิจ	1. จัดทำร่าง ทบทวน ปรับปรุง แนวทางปฏิบัติ ข้อกำหนด ระเบียบและวิธีการ เพื่อให้ข้อมูลพร้อมใช้งาน มีคุณภาพ มีความมั่นคงปลอดภัย และรักษาความเป็นส่วนบุคคล ให้กับผู้มีส่วนได้ส่วนเสียทั้งหมด เสนอต่อคณะทำงานหัวหน้าบริกรข้อมูลพิจารณา 2. รวบรวมข้อมูล กำหนดวัตถุประสงค์การใช้งาน ระบุหมวดหมู่และลำดับ ชั้นความลับของข้อมูล 3. นิยามความต้องการด้านคุณภาพ และความมั่นคงปลอดภัยข้อมูล 4. นิยามคำอธิบายข้อมูล (Metadata) และจัดทำบัญชีข้อมูล (Data Catalog) ร่วมกับคณะทำงานบริกรข้อมูลเชิงเทคนิค 5. กำหนดแนวปฏิบัติด้านคุณภาพ การตรวจวัดคุณภาพ และการวิเคราะห์คุณภาพของข้อมูล 6. รายงานผลการดำเนินงานต่อคณะทำงานหัวหน้าบริกรข้อมูล รายปี
บริกรข้อมูลเชิงเทคนิค	1. จัดทำร่าง ทบทวน ปรับปรุง แนวทางปฏิบัติ ข้อกำหนด ระเบียบและวิธีการ ด้านเทคนิค 2. กำหนดโครงสร้างฐานข้อมูล กำหนดสิทธิการเข้าถึงข้อมูล (การสร้าง จัดเก็บ ใช้ เผยแพร่ และ ทำลาย) ของผู้ใช้งานและผู้มีส่วนได้เสีย ตามที่ได้กำหนดในคำอธิบายชุดข้อมูล หรือเมทาดาตา (Metadata) 3. เฝ้าระวัง และติดตามการใช้งานชุดข้อมูล เพื่อให้สอดคล้องกับ นโยบาย แนวปฏิบัติ ข้อกำหนด ระเบียบ วิธีการด้านเทคนิค และด้านคุณภาพข้อมูล 4. ดูแลการจัดเก็บ การเคลื่อนย้าย การใช้งาน และการปกป้องคุ้มครองข้อมูลให้มีความมั่นคงปลอดภัย ให้คำปรึกษา ข้อเสนอแนะด้านเทคนิค และทำงานร่วมกับคณะทำงานบริกรข้อมูลด้านต่าง ๆ เพื่อให้การกำกับดูแลข้อมูลมีคุณภาพและมีความมั่นคงปลอดภัย 5. รายงานผลการดำเนินงานต่อคณะทำงานหัวหน้าบริกรข้อมูล รายปี

ส่วนที่ 2 แนวปฏิบัติการบริหารและจัดการข้อมูล

2.1 แนวปฏิบัติการดำเนินการธรรมาภิบาลข้อมูล

2.1.1 กระบวนการทำงานและผู้เกี่ยวข้อง (SIPOC & RACI)

ตารางที่ 2.1 SIPOC

Supplier	Input	Process	Output	Customer	Time
กบจ.ฝยท.	คำสั่งคณะกรรมการธรรมาภิบาลข้อมูล กปน.เดิม	1. แต่งตั้ง/ทบทวนคณะกรรมการธรรมาภิบาลข้อมูล กปน. (DG Council) - กบจ.ฝยท.	1. คำสั่งคณะกรรมการธรรมาภิบาลข้อมูล กปน.	- DG Council - ฝยท.	ต.ค.-พ.ย.
1. ฝยท. 2. กบจ.ฝยท. 3. EA 4. ฝนย.	1. EA Business Domain 2. EA Data Architecture 2. เกณฑ์การเลือกชุดข้อมูล 3. แผนวิสาหกิจ	2. คัดเลือกรายการชุดข้อมูลตามเกณฑ์ที่กำหนด - DG Council	รายการชุดข้อมูลที่คัดเลือกประจำปีงบประมาณ	กบจ.ฝยท.	พ.ย.-ธ.ค.
หน่วยงานที่เกี่ยวข้องกับชุดข้อมูลที่คัดเลือก	1. รายการชุดข้อมูลที่คัดเลือกประจำปีงบประมาณ 2. คำสั่งคณะบริกรข้อมูลเดิม (Data Steward Team)	3. จัดทำร่างคำสั่งทบทวน / แต่งตั้งคณะบริกรข้อมูล (Lead, Business, Technical) - กบจ.ฝยท.	คำสั่งทบทวน/แต่งตั้งคณะบริกรข้อมูล (Data Steward Team)	- คณะบริกรข้อมูล - กบจ.ฝยท.	พ.ย.-ธ.ค.

Supplier	Input	Process	Output	Customer	Time
1. กบจ.ฝยท. 2. ฝพบ.	1.แผนการดำเนินงานประจำปีงบประมาณ 2.Training Need	4. จัดอบรมตามแผนการดำเนินงาน -ฝพบ., กบจ.ฝยท.	รายงานสรุปผลการอบรมและผลการประเมินความเข้าใจและการรับรู้	- DG Council - ฝยท.	ม.ค.-มี.ค.
กบจ.ฝยท.	1. แบบสอบถาม	5. สำรวจการรับรู้ด้านธรรมาภิบาลข้อมูล -กบจ.ฝยท., คณะทำงานหัวหน้าบริกรข้อมูล	รายงานผลสำรวจการรับรู้	- DG Council - ฝยท.	ม.ค. - ก.พ.
1. สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.) 2. กบจ.ฝยท. 3. DG Council	- กฎหมาย ระเบียบ นโยบาย แนวปฏิบัติ มาตรฐาน ภายนอก - นโยบายธรรมาภิบาลข้อมูล กปน. - แนวปฏิบัติการดำเนินการธรรมาภิบาลข้อมูล	6. จัดทำ/ทบทวนนโยบายแนวปฏิบัติ นำเสนอ DG Council เพื่อพิจารณา- กบจ.ฝยท.	นโยบายธรรมาภิบาลข้อมูล และแนวปฏิบัติการดำเนินการธรรมาภิบาลข้อมูล ที่จัดทำ/ทบทวน	พนักงาน กปน. (Data Stakeholder)	ม.ค.-ส.ค.
1. DG Council 2. กบจ.ฝยท.	นโยบายธรรมาภิบาลข้อมูลและแนวปฏิบัติการดำเนินการธรรมาภิบาลข้อมูล	7. จัดทำ/ทบทวน บัญชีข้อมูล, เมทาดาตา, เกณฑ์คุณภาพข้อมูลของชุดข้อมูลต่าง ๆ - คณะบริกรข้อมูล	1. บัญชีข้อมูล 2. เมทาดาตา 3. เกณฑ์ เงื่อนไข และมิติของคุณภาพข้อมูล	- คณะบริกรข้อมูล - Data Stakeholder	ม.ค.-มิ.ย.

Supplier	Input	Process	Output	Customer	Time
1. คณะบริกรข้อมูล 2. กบจ.ฝยท.	1. บัญชีข้อมูล 2. เมทาดาตา 3. เกณฑ์ เงื่อนไข และมิติของคุณภาพข้อมูล	8.ติดตามการดำเนินงาน - คณะทำงานหัวหน้าบริกรข้อมูล	รายงานผลการดำเนินงานการจัดทำบัญชีข้อมูล/เมทาดาตา/คุณภาพข้อมูล	- DG Council - คณะทำงานหัวหน้าบริกรข้อมูล	ม.ค.-มิ.ย.
คณะทำงานหัวหน้าบริกรข้อมูล	รายงานผลการดำเนินงานการจัดทำบัญชีข้อมูล/เมทาดาตา/คุณภาพข้อมูล	9.นำเสนอผลการดำเนินงานการต่อ DG Council เพื่อพิจารณาเผยแพร่ชุดข้อมูล – คณะทำงานหัวหน้าบริกรข้อมูล	ชุดข้อมูลที่ผ่านการพิจารณาเผยแพร่จาก DG Council	- กบจ.ฝยท.	ก.ค.
1. DG Council 2. กบจ.ฝยท.	1.นโยบายธรรมาภิบาลข้อมูล และแนวปฏิบัติการดำเนินการธรรมาภิบาลข้อมูล ที่จัดทำ/ทบทวน 2. ชุดข้อมูลที่ผ่านการพิจารณาเผยแพร่จาก DG Council	10. ประชาสัมพันธ์ตามแผนการสื่อสาร - กบจ.ฝยท.	สื่อประชาสัมพันธ์ผ่าน Website, Social, เสวนา/กิจกรรม	- พนักงาน กปน. (Data Stakeholder) - Open Data	ก.ค.-ก.ย.
คณะทำงานหัวหน้าบริกรข้อมูล	- รายงานผลการดำเนินงานการจัดทำบัญชีข้อมูล/เมทาดาตา/คุณภาพข้อมูล - รายงานผลสำรวจการรับรู้ - รายงานสรุปผลการอบรมและผลการประเมินความเข้าใจและการรับรู้	11.จัดทำรายงานผลการดำเนินงานด้านธรรมาภิบาลข้อมูลประจำปีงบประมาณนำเสนอ DG Council เพื่อทราบ - คณะทำงานหัวหน้าบริกรข้อมูล	รายงานผลการดำเนินงานด้านธรรมาภิบาลข้อมูลประจำปีงบประมาณ	- DG Council - ฝยท.	ก.ย.

Supplier	Input	Process	Output	Customer	Time
กบจ.ฝยท. ฝยท.	- แผนแม่บทด้านเทคโนโลยีดิจิทัล - DG Roadmap - รายงานผลการดำเนินงานด้านธรรมาภิบาลข้อมูลประจำปีงบประมาณ	12. จัดทำ/ทบทวนแผนการดำเนินงานประจำปีงบประมาณถัดไป กำหนดผู้รับผิดชอบแต่ละกิจกรรมและช่วงเวลา -กบจ.ฝยท.	แผนการดำเนินงานประจำปีงบประมาณถัดไป	- ฝยท.	ก.ย.

ตารางที่ 2.2 **RACI**

ลำดับ	กระบวนการ	บทบาทหน้าที่	DG Council	ผยท.	กบจ.ผยท.	ห้วหน้าบริการข้อมูล	บริการข้อมูลเชิงธุรกิจ	บริการข้อมูลเชิงเทคนิค	พนักงาน กปน. (Data Stakeholder)	ผู้ว่า กปน.	ฝพบ.
1	**แต่งตั้ง/ทบทวนคณะกรรมการธรรมาภิบาลข้อมูล กปน. (DG Council)**										
	คำสั่งคณะกรรมการธรรมาภิบาลข้อมูล กปน.		I	I	R					A	
2	**คัดเลือกรายการชุดข้อมูลตามเกณฑ์ที่กำหนด**										
	รายการชุดข้อมูลที่คัดเลือกประจำปีงบประมาณ		R		I						
3	**จัดทำร่างคำสั่งทบทวน / แต่งตั้งคณะบริกรข้อมูล**										
	คำสั่งทบทวน/แต่งตั้งคณะบริกรข้อมูล (Data Steward Team)		A		R	I	I	I			
4	**จัดอบรมตามแผนการดำเนินงาน**										
	รายงานสรุปผลการอบรมและผลการประเมินความเข้าใจและการรับรู้		I	I	R						R
5	**สำรวจการรับรู้ด้านธรรมาภิบาลข้อมูล**										
	รายงานผลสำรวจการรับรู้		I	I	R						
6	**จัดทำ/ทบทวนนโยบาย แนวปฏิบัติ นำเสนอ DG Council เพื่อพิจารณา**										
	นโยบายธรรมาภิบาลข้อมูล และแนวปฏิบัติด้านธรรมาภิบาลข้อมูล ที่ทบทวน/จัดทำใหม่ - ผู้ว่าการ อนุมัติ นโยบาย - DG Council อนุมัติ แนวปฏิบัติ		A		R	C	C	C	I	A	
7	**จัดทำ/ทบทวน บัญชีข้อมูล, เมทาดาตา, เกณฑ์คุณภาพข้อมูล ของชุดข้อมูลต่างๆ**										
	1. บัญชีข้อมูล 2. เมทาดาตา 3. เกณฑ์ เงื่อนไข และมิติของคุณภาพข้อมูล		I		C	C	R	R			
8	**ติดตามการดำเนินงาน**										
	รายงานผลการดำเนินงานการจัดทำบัญชีข้อมูล/เมทาดาตา/คุณภาพข้อมูล		I		C	R					
9	**นำเสนอผลการดำเนินงานต่อ DG Council เพื่อพิจารณาเผยแพร่ชุดข้อมูล**										
	ชุดข้อมูลที่ผ่านการพิจารณาจาก DG Council		A		I	R					
10	**ประชาสัมพันธ์ตามแผนการสื่อสาร**										
	สื่อประชาสัมพันธ์ ผ่าน Website, Social, เสวนา/กิจกรรม				R				I		
11	**จัดทำรายงานผลการดำเนินงานด้านธรรมาภิบาลข้อมูลประจำปีงบประมาณนำเสนอ DG Council เพื่อทราบ**										
	รายงานผลการดำเนินงานด้านธรรมาภิบาลข้อมูลประจำปีงบประมาณ		I	I	R	R					
12	**จัดทำ/ทบทวนแผนการดำเนินงานประจำปีงบประมาณถัดไป กำหนดผู้รับผิดชอบแต่ละกิจกรรมและช่วงเวลา**										
	แผนการดำเนินงานประจำปีงบประมาณถัดไป			I	R						

R	Responsible	Assigned to complete the task or deliverable.
A	Accountable	Has final decision-making authority and accountability for completion. Only 1 per task.
C	Consulted	An adviser, stakeholder, or subject matter expert who is consulted before a decision or action.
I	Informed	Must be informed after a decision or action.

2.1.2 การสร้างความรู้และความตระหนักด้านธรรมาภิบาลข้อมูล

จัดให้มีการดำเนินการตามแผนการสื่อสาร ดังนี้

ผู้ถ่ายทอดสาร/ผู้รับผิดชอบ	ผู้รับสาร	ระดับการเข้าร่วม	รูปแบบ/วิธีการ/ช่องทางการสื่อสาร			การประเมินการรับรู้	
			ภายใน	ภายนอก	กำหนดเวลา	วิธีการประเมิน	กำหนดเวลา
- กบจ.ฝยท. - ฝพบ.	พนักงาน กปน.	การสร้างความรู้ความเข้าใจกระบวนการธรรมาภิบาลข้อมูล ของ กปน.	- การอบรม - Web Site - Infographic - หนังสือเวียน		ไตรมาส 2	แบบประเมินผลการรับรู้และเข้าใจ	ไตรมาส 2
กบจ.ฝยท.	- คณะกรรมการธรรมาภิบาลข้อมูล - คณะบริกรข้อมูล	การอบรมเชิงปฏิบัติการ	- การอบรม		ไตรมาส 2-3	แบบประเมินผลการรับรู้และเข้าใจ	ไตรมาส 3
- คณะกรรมการธรรมาภิบาลข้อมูล - กบจ.ฝยท.	พนักงาน กปน.	เผยแพร่นโยบายและแนวปฏิบัติธรรมาภิบาลข้อมูล	- Web Site - หนังสือเวียน		ไตรมาส 2-4	สื่อสารผ่านหนังสือเวียนและ Web Site	ไตรมาส 2-4

2.2 แนวปฏิบัติการบริหารจัดการวงจรชีวิตของข้อมูล

2.2.1 วัตถุประสงค์

เพื่อให้การสร้าง (Create) การจัดเก็บข้อมูล (Store) การประมวลผลและการใช้ (Process and Use) การเปิดเผยและรักษาความลับ (Disclosure and Confidentiality) การเก็บถาวร (Archive) และการทำลาย (Destroy) ข้อมูล เป็นไปอย่างมีประสิทธิภาพ ถูกต้อง และสอดคล้องกับมาตรฐานและกฎระเบียบที่เกี่ยวข้อง โดยมุ่งเน้น การสร้างประโยชน์สูงสุดจากข้อมูลของ กปน. การเพิ่มประสิทธิภาพกระบวนการทำงานที่เกี่ยวข้องกับข้อมูล รวมถึงการจัดการผลกระทบและความเสี่ยงที่อาจเกิดขึ้นจากการใช้ข้อมูลอย่างเหมาะสม

2.2.2 นิยาม

1. **การสร้างข้อมูล (Create)** เป็นการสร้างข้อมูลขึ้นมาใหม่ หรือปรับปรุงข้อมูลขึ้นใหม่ โดยวิธีการบันทึกเข้าไปด้วยบุคคลหรือบันทึกอัตโนมัติด้วยอุปกรณ์อิเล็กทรอนิกส์ เช่น อุปกรณ์ตรวจจับสัญญาณ (Sensor) รวมถึงการซื้อข้อมูล หรือการรับข้อมูลจากหน่วยงานอื่นเพื่อนำมาจัดเก็บในภายหลัง
2. **การจัดเก็บข้อมูล (Store)** เป็นการจัดเก็บข้อมูลที่เกิดจากกระบวนการสร้างหรือข้อมูลที่ได้จากการ เชื่อมโยงและ/หรือแลกเปลี่ยนกับหน่วยงานอื่น ไม่ว่าจะจัดเก็บลงแฟ้มข้อมูล (File) หรือระบบการจัดการฐานข้อมูล (Database Management System - DBMS) เพื่อให้เกิดความมีระเบียบง่ายต่อการใช้งาน ข้อมูลไม่สูญหายหรือถูกทำลาย และช่วยให้ผู้ใช้งานสามารถประมวลผลข้อมูลต่าง ๆ ตามความต้องการได้อย่างรวดเร็ว
3. **การประมวลผลและใช้ข้อมูล (Processing and Use)** เป็นการนำข้อมูลที่จัดเก็บมาประมวลผล เช่น การถ่ายโอนข้อมูล การเปลี่ยนรูปแบบการจัดเก็บข้อมูล การวิเคราะห์ข้อมูล การจัดทำรายงาน เพื่อนำข้อมูลเหล่านั้นมาใช้งานให้เกิดประโยชน์ตามวัตถุประสงค์ รวมถึงการสำรอง (Backup) ข้อมูล โดยการคัดลอกข้อมูลที่ใช้งานอยู่ในปัจจุบันเพื่อทำสำเนา เช่น ใช้โปรแกรมในการสำรองข้อมูล เป็นการหลีกเลี่ยงความเสียหายที่จะเกิดขึ้นหากข้อมูลเกิดการเสียหายหรือสูญหาย ซึ่งสามารถนำข้อมูลที่สำรองไว้ในสื่อบันทึกข้อมูลกลับมาใช้งานได้ทันทีโดยการกู้คืน (Restore)
4. **การเปิดเผยและรักษาความลับ (Disclosure and Confidentiality)** เป็นการนำข้อมูลที่อยู่ในความครอบครองของหน่วยงาน เผยแพร่ตามช่องทางต่าง ๆ อย่างเหมาะสม อาทิ การเปิดเผยข้อมูล (Open data) การแบ่งปันข้อมูล (Sharing) การกระจายข้อมูล (Dissemination) การควบคุมการเข้าถึง (Access Control) การแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน (Exchange) และการกำหนดเงื่อนไขในการนำข้อมูลไปใช้ (Condition)
5. **กระบวนการจัดเก็บข้อมูลถาวร (Archive)** เป็นการย้ายข้อมูลที่มีช่วงอายุเกินช่วงใช้งานหรือไม่ได้ใช้งานแล้ว เพื่อเก็บรักษาถาวรโดยที่ข้อมูลนั้นไม่มีการลบ ปรับปรุง หรือแก้ไขอีก และสามารถนำกลับไปใช้งานได้ใหม่เมื่อต้องการ
6. **การทำลายข้อมูล (Destroy)** เป็นการทำลายข้อมูลที่มีการจัดเก็บถาวรเป็นระยะเวลานานหรือเกินกว่าระยะเวลาที่กำหนด

2.2.3 แนวปฏิบัติ

1. **แนวปฏิบัติการสร้างข้อมูล (Create)**
    - เจ้าของข้อมูลและคณะทำงานบริกรข้อมูล รวมถึงหน่วยงานที่เกี่ยวข้องร่วมกันออกแบบและกำหนดมาตรฐานการสร้างข้อมูลให้เป็นแบบแผน พร้อมทั้งกำหนดวิธีปฏิบัติการสร้างให้สอดคล้องกับความต้องการและวัตถุประสงค์ในการดำเนินงาน จากนั้นให้นำเสนอขออนุมัติคณะกรรมการเพื่อประกาศใช้
    - คณะทำงานบริกรข้อมูล จัดทำคำอธิบายข้อมูล (Metadata) เมื่อมีการสร้างชุดข้อมูล (Datasets) ตามมาตรฐานขั้นต่ำคำอธิบายข้อมูล และกำหนดให้ทำการ

ประเมินคุณค่าของชุดข้อมูล เพื่อสนับสนุนการคัดเลือกเป็นชุดข้อมูลคุณค่าสูง (High-Value Dataset)

- คณะทำงานบริกรข้อมูล จัดประชุม/อบรม/ประชาสัมพันธ์ให้ส่วนเกี่ยวข้องมีความรู้ความเข้าใจถึงวิธีปฏิบัติการสร้างอย่างถูกต้องตามขั้นตอนที่กำหนด
- คณะทำงานบริกรข้อมูลต้องมีการตรวจสอบและบันทึกข้อมูลตั้งต้นให้ถูกต้องครบถ้วน ตรงกับข้อเท็จจริงที่ตรงกับเอกสารต้นฉบับ โดยมีการบันทึกข้อมูลให้ตรงตามมาตรฐานการสร้างที่ได้หารือร่วมกันไว้ และในการสร้างต้องมีการระบุเจ้าของข้อมูลให้มีขอบเขตอำนาจดูแลข้อมูล ให้ทราบถึงแหล่งข้อมูลที่น่าเชื่อถือได้เท่านั้น
- เจ้าของข้อมูลตรวจสอบความถูกต้องของข้อมูลที่ถูกสร้างขึ้น แต่ถ้าข้อมูลถูกจัดเก็บไปแล้ว หากตรวจสอบพบว่าข้อมูลผิด ให้แจ้งคณะทำงานบริกรข้อมูลเชิงเทคนิคและเชิงธุรกิจเพื่อปรับปรุงแก้ไขข้อมูลให้ถูกต้องครบถ้วน
- คณะทำงานบริกรข้อมูล จัดอบรมชี้แจงให้ผู้สร้างข้อมูลตระหนักถึงความสำคัญและความจำเป็นในการรักษาความมั่นคงปลอดภัยของข้อมูล

2. แนวปฏิบัติการจัดเก็บข้อมูล (Store)

- คณะทำงานบริกรข้อมูลและหน่วยงานที่เกี่ยวข้องร่วมกันออกแบบและกำหนดมาตรฐานข้อมูลให้เป็นแบบเดียวกัน มีวิธีการจัดเก็บรักษาอย่างมั่นคงปลอดภัย และจัดทำข้อมูลอ้างอิง (Reference Data) เพื่อใช้สำหรับการตรวจสอบข้อมูล รวมถึงการกำหนดและออกแบบสภาพแวดล้อมของการจัดเก็บข้อมูลที่เอื้อต่อการรักษาความมั่นคงปลอดภัยและการบริหรจัดการคุณภาพของข้อมูล พร้อมทั้งกำหนดวิธีปฏิบัติการรวบรวมและการจัดเก็บรักษาให้สอดคล้องกับความต้องการและวัตถุประสงค์ในการดำเนินงาน จากนั้นให้นำเสนอขออนุมัติคณะกรรมการภายใต้ขอบเขตหน้าที่ความรับผิดชอบที่ได้รับมอบหมายเพื่อประกาศใช้
- คณะทำงานบริกรข้อมูลจัดประชุม/อบรม/ประชาสัมพันธ์ให้ส่วนเกี่ยวข้องมีความรู้ความเข้าใจถึงวิธีปฏิบัติการรวมรวม และการจัดเก็บรักษา และมีทักษะในการใช้เครื่องมือที่ใช้จัดเก็บรักษาข้อมูล อย่างถูกต้องตามขั้นตอนที่กำหนด
- การเก็บรวบรวมข้อมูลใดๆ ให้องค์กรมีประกาศแจ้งให้ผู้จัดเก็บและผู้ใช้รับทราบถึงเอกสารที่ต้องใช้ในการดำเนินการ เช่น หากผู้จัดเก็บหรือผู้ใช้ต้องการขอใช้ข้อมูล ให้ฝ่ายงานที่ติดประกาศและชี้แจงให้กับผู้จัดเก็บหรือผู้ใช้ทราบถึงเอกสารที่จำเป็นต้องขอใช้ข้อมูล เป็นต้น
- เจ้าของข้อมูลตรวจสอบความถูกต้องของข้อมูลที่ถูกสร้างขึ้น แต่ถ้าข้อมูลถูกจัดเก็บไปแล้ว หากตรวจสอบพบว่าข้อมูลผิด ให้แจ้งคณะทำงานบริกรข้อมูลเพื่อปรับปรุงแก้ไขข้อมูลให้ถูกต้องครบถ้วน

- การเปลี่ยนแปลงข้อมูลสามารถกระทำได้ หากเป็นการปรับปรุงเปลี่ยนแปลงให้เป็นปัจจุบัน ครบถ้วน ถูกต้อง เป็นไปเพื่อการควบคุมคุณภาพข้อมูล โดยต้องแจ้งให้คณะทำงานบริกรข้อมูลและเจ้าของข้อมูล ทราบด้วยทุกครั้ง
- คณะทำงานบริกรข้อมูลและเจ้าของข้อมูลกำหนดระดับชั้นความลับของข้อมูล สื่อบันทึกข้อมูล มีการพิจารณาจากปัจจัยต่าง ๆ โดยอ้างอิงเนื้อหาจากขั้นตอนปฏิบัติการจัดระดับชั้นความลับข้อมูล และแจ้งให้ผู้จัดเก็บและผู้ใช้ รวมถึงหน่วยงานภายในทราบและปฏิบัติตามอย่างเคร่งครัด เพื่อให้ข้อมูลมีความมั่นคงปลอดภัยและรักษาคุณภาพของข้อมูล
- คณะทำงานบริกรข้อมูลกำหนดสิทธิการเข้าถึงระบบและโปรแกรมที่เป็นไปตามขั้นตอนการดำเนินงานตามที่เจ้าของข้อมูลกำหนด โดยไม่ขัดต่อหลักกฎหมายที่ประกาศใช้อยู่
- คณะทำงานบริกรข้อมูลและเจ้าของข้อมูล จัดประชุมหารือเพื่อทบทวนการจัดระดับชั้นความลับของข้อมูล อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ เช่นการลาออก เปลี่ยนตำแหน่ง โอนย้าย สิ้นสุดการจ้าง การปรับโครงสร้าง หรือเมื่อมีการปรับปรุงระบบสารสนเทศ เป็นต้น เพื่อตรวจสอบและปรับปรุงระบบที่ใช้ในการให้บริการหรือระบบงานสารสนเทศให้มีความทันสมัย มีความปลอดภัยจากภัยคุกคามทางดิจิทัลและเพิ่มมาตรการป้องกันช่องโหว่
- คณะทำงานบริกรข้อมูลจัดอบรมชี้แจงให้ผู้สร้างและผู้ใช้ข้อมูลตระหนักถึงความสำคัญและความจำเป็นในการรักษาความมั่นคงปลอดภัยของข้อมูล
- คณะทำงานบริกรข้อมูลร่วมกันกำหนดวิธีและขั้นตอนการสำรองข้อมูลตามมาตรฐานสากล เพื่อให้องค์กร สามารถใช้ข้อมูลได้อย่างต่อเนื่อง เมื่อเกิดเหตุสุดวิสัย
- เจ้าของข้อมูลและคณะทำงานบริกรข้อมูลกำหนดระยะเวลาในการจัดเก็บข้อมูลที่ชัดเจน
- คณะทำงานบริกรข้อมูลทำการย้ายข้อมูลที่มีการจัดเก็บเกินระยะเวลาที่กำหนดแล้ว เพื่อจัดเก็บเป็นข้อมูลถาวรและแจ้งให้เจ้าของข้อมูลทราบ

3. แนวปฏิบัติการประมวลผลและการใช้ (Process and Use)

- คณะทำงานบริกรข้อมูลและหน่วยงานที่เกี่ยวข้อง ต้องกำหนดแนวปฏิบัติและมาตรฐานการประมวลผลข้อมูลและการใช้ข้อมูล ให้เป็นมาตรฐานเดียวกันทั้งองค์กร จากนั้นให้นำเสนอขออนุมัติจากคณะกรรมการ เพื่อประกาศใช้และทำการสื่อสารให้ผู้ที่เกี่ยวข้องรับทราบ
- การดำเนินการประมวลผลข้อมูลที่ไม่ใช่หมวดหมู่ข้อมูลสาธารณะ ให้เป็นไปตามขอบเขต เงื่อนไข หรือวัตถุประสงค์ตามหมวดหมู่ข้อมูลนั้น

- การประมวลผลและการใช้ข้อมูลต้องมีการบันทึกประวัติการประมวลผลและการใช้ข้อมูล เพื่อตรวจสอบย้อนกลับได้ โดยระบุให้ทราบถึงวัน เวลาและผู้ที่ประมวลผลข้อมูลจากฐานข้อมูลขององค์กร
- ผู้ใช้ข้อมูลต้องระบุตัวตนโดยใส่ Username และ Password ของตนเองเพื่อ Login เข้าเครื่องคอมพิวเตอร์ และใช้ Username และ Password ของหน่วยงานเพื่อ Login เข้าระบบทุกครั้ง และเมื่อผู้ใช้ข้อมูลประมวลผลแล้วเสร็จให้ Logout จากระบบทุกครั้ง ทั้งนี้ให้เป็นไปตามนโยบายการรักษาความมั่นคงปลอดภัยข้อมูล
- ผู้ใช้ข้อมูล ต้องประมวลผลและใช้ข้อมูล ตรงตามวัตถุประสงค์ที่แจ้งไว้กับเจ้าของข้อมูลแล้วเท่านั้นหากหน่วยงานผู้ใช้ข้อมูล ต้องการประมวลผลและใช้ข้อมูลเป็นอย่างอื่นที่นอกเหนือไปจากวัตถุประสงค์ที่แจ้งไว้กับเจ้าของข้อมูลต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อน
- ทุกชุดข้อมูลในระบบสารสนเทศต้องระบุสิทธิในการเข้าถึงข้อมูลเป็นเมทริกซ์ CRUD (Create – Read – Update – Delete) ในการระบุสิทธิการสร้าง เข้าถึงเพื่ออ่าน เข้าถึงเพื่อแก้ไข และลบข้อมูล และถ้าสิทธิในการเข้าถึงข้อมูลแต่ละหน่วยของข้อมูลในชุดเดียวกันไม่เท่ากัน ต้องทำเป็นเมทริกซ์ในระดับหน่วยของข้อมูล
- เจ้าของข้อมูลและคณะบริกรข้อมูลเชิงเทคนิค ร่วมกันจัดทำระบบสำหรับการบันทึกประวัติการประมวลผล - และการใช้ข้อมูล (Log Files) ของผู้ใช้ข้อมูล
- เจ้าของข้อมูลและคณะทำงานบริกรข้อมูลร่วมกันจัดทำวิธีป้องกันมิให้ผู้ใช้ข้อมูลหรือบุคคลอื่นที่ไม่ได้รับมอบหมายเข้าไปแก้ไขบันทึกประวัติการประมวลผลและการใช้ข้อมูล (Log Files) ได้
- ผู้สร้างและผู้ใช้ข้อมูล (หรือผู้ประมวลผลข้อมูล) ต้องปรับปรุงคำอธิบายข้อมูลและบัญชีข้อมูลให้มีความถูกต้อง ครบถ้วน และเป็นปัจจุบัน โดยให้เป็นไปตามแนวปฏิบัติการบริหารจัดการคำอธิบายข้อมูล
- การแก้ไขข้อมูลให้เป็นไปตามกระบวนการทำงานตามปกติของเจ้าหน้าที่องค์กรที่ได้รับมอบหมายในการแก้ไขข้อมูล
- การใช้งานข้อมูลที่สำคัญขององค์กร หรือข้อมูลที่ใช้งานร่วมกัน จะต้องมีการเชื่อมโยงข้อมูลจากแหล่งข้อมูลที่น่าเชื่อถือ (Trusted data source) ไม่ว่าจะเป็นข้อมูลภายใน หรือข้อมูลจากหน่วยงานภายนอก
- เจ้าของข้อมูล และคณะทำงานบริกรข้อมูลต้องทบทวนสิทธิการเข้าถึงเพื่อประมวลผลและใช้ข้อมูลของผู้ใช้งานอย่างน้อยปีละ 1 ครั้งหรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ เช่น การลาออก การเปลี่ยนตำแหน่ง โอนย้าย สิ้นสุดการจ้าง การปรับโครงสร้าง หรือเมื่อมีการปรับปรุงระบบสารสนเทศ

4. แนวปฏิบัติการเปิดเผยและรักษาความลับ (Disclosure and Confidentiality)

- คณะทำงานบริกรข้อมูลต้องกำหนดข้อตกลงห้ามผู้ใช้ข้อมูลเปิดเผยข้อมูลที่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง หลักเกณฑ์ นโยบาย แนวปฏิบัติขององค์กร ที่ประกาศใช้ ไม่ว่าข้อมูลจะอยู่ในรูปแบบใดก็ตาม
- การเปิดเผยข้อมูลที่เกี่ยวข้องกับเจ้าของข้อมูลส่วนบุคคล ต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล หรือได้รับคำร้องขอจากเจ้าของข้อมูลส่วนบุคคล ผู้สืบสิทธิ ทายาท ผู้แทนโดยชอบธรรม หรือผู้พิทักษ์ตามกฎหมาย โดยทำหนังสือให้ความยินยอมเปิดเผยข้อมูลเป็นลายลักษณ์อักษร
- หน่วยงานที่เกี่ยวข้องต้องจัดทำข้อมูลที่จะเปิดเผยให้อยู่ในรูปแบบที่ง่ายต่อการนำไปใช้ เช่น ไฟล์ Excel, CSV เป็นต้น
- คณะทำงานบริกรข้อมูลและเจ้าของข้อมูลต้องร่วมกันพิจารณาคัดเลือกชุดข้อมูลสำคัญที่ต้องการเผยแพร่ โดยต้องพิจารณาชุดข้อมูลที่มีคุณภาพและเป็นที่ต้องการของทุกภาคส่วน เพื่อส่งเสริมให้เกิดการนำไปใช้อย่างแพร่หลายและเกิดประโยชน์สูงสุด
- คณะทำงานบริกรข้อมูลพิจารณาข้อมูลที่จะเผยแพร่ โดยต้องอยู่ในชั้นความลับที่สามารถเผยแพร่ได้และต้องไม่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง หลักเกณฑ์ นโยบาย แนวปฏิบัติ ขององค์กร ที่ประกาศใช้
- คณะทำงานบริกรข้อมูลกำหนดวิธีปฏิบัติการเปิดเผยข้อมูล พร้อมทั้งระบุช่องทางการเปิดเผยข้อมูลที่เข้าถึงและนำไปใช้ได้ง่าย ตามมาตรฐานความปลอดภัยในระดับสากล จากนั้นให้นำเสนอขออนุมัติจากคณะกรรมการ เพื่อประกาศใช้
- คณะทำงานบริกรข้อมูลและเจ้าของข้อมูลต้องมีการจัดทำและแนบคำอธิบายข้อมูล (Metadata) ควบคู่ไปกับข้อมูลที่เปิดเผยผ่านช่องทางการเปิดเผยข้อมูล เพื่อให้ผู้ใช้ข้อมูลสามารถเข้าใจเกี่ยวกับบริบทของข้อมูลตามมาตรฐานขั้นต่ำขององค์กร
- คณะทำงานบริกรข้อมูล กำหนดวิธีปฏิบัติการตรวจสอบการเปิดเผยข้อมูล ให้เป็นไปอย่างเหมาะสมหรือเป็นไปตามแนวทางที่กำหนดไว้ เพื่อให้ได้ข้อมูลที่มีคุณภาพและเป็นการรักษาคุณภาพของข้อมูล จากนั้นให้นำเสนอขออนุมัติจากคณะกรรมการเพื่อประกาศใช้
- บุคลากรขององค์กร ต้องปฏิบัติตามขั้นตอนและวิธีการที่กำหนดอย่างเคร่งครัด และป้องกันมิให้มีการเปิดเผยข้อมูล โดยไม่ได้รับอนุญาต
- คณะทำงานบริกรข้อมูลทำการจัดประชุม/อบรม/ประชาสัมพันธ์ ให้ส่วนเกี่ยวข้องมีความรู้ความเข้าใจวิธีปฏิบัติการเปิดเผยและการรักษาความลับข้อมูล

5. แนวปฏิบัติการเก็บถาวรและทำลาย (Archive and destroy)

- คณะทำงานบริกรข้อมูลกำหนดระยะเวลาในการจัดเก็บข้อมูลที่เหมาะสมกับข้อมูลแต่ละประเภท

- คณะทำงานบริกรข้อมูลและเจ้าของข้อมูลศึกษาขนาดและชนิดของข้อมูลที่ต้องจัดเก็บ โดยเลือกเครื่องมือและกระบวนการที่เป็นมาตรฐานสากลในการจัดเก็บข้อมูล ให้อยู่ในสภาพที่พร้อมใช้งานได้ตลอดระยะเวลาในการจัดเก็บข้อมูล
- คณะทำงานบริกรข้อมูลกำหนดวิธีปฏิบัติการทำลายข้อมูล ทั้งนี้ต้องไม่ขัดต่อข้อตกลงระหว่างเจ้าของข้อมูลและไม่ขัดต่อ ข้อกฎหมายใด ๆ รวมถึง กำหนดแนวปฏิบัติการทำลายข้อมูล เมื่อข้อมูลนั้นไม่มีการใช้งานหรือมีการเก็บข้อมูลไว้นานเกินกว่าระยะเวลาที่กำหนด แต่ควรมีการเก็บรักษาคำอธิบายข้อมูลของข้อมูลที่ทำลายไว้ เพื่อใช้สำหรับการตรวจสอบภายหลัง
- คณะทำงานบริกรข้อมูลจัดการประชุม/อบรม/ประชาสัมพันธ์ ให้ส่วนเกี่ยวข้องมีความรู้ความเข้าใจวิธีปฏิบัติการทำลายข้อมูล
- คณะทำงานบริกรข้อมูลกำหนดอำนาจอนุมัติสิทธิ และการยืนยันตัวบุคคลของผู้ที่จะดำเนินการทำลายข้อมูล และเก็บ Log Files ไว้ด้วยทุกครั้ง
- หน่วยงานภายในองค์กร ถ้าต้องการย้ายข้อมูลหรือทำลายข้อมูลทั่วไป ต้องได้รับการอนุญาตจากคณะทำงานบริกรข้อมูลก่อนเท่านั้น สำหรับข้อมูลสำคัญ ข้อมูลความลับ ข้อมูลความมั่นคงต้องได้รับการอนุญาตจากคณะกรรมการ เท่านั้น
- ในกรณีที่เจ้าของข้อมูลส่วนบุคคล ผู้สืบสิทธิ ทายาท ผู้แทนโดยชอบธรรม หรือผู้พิทักษ์ตามกฎหมาย มีการคัดค้านการจัดเก็บ ความถูกต้อง หรือการกระทำใด ๆ เช่น การแจ้งให้ดำเนินการปรับปรุงแก้ไขข้อมูล ส่วนบุคคล หรือลบข้อมูลส่วนบุคคล เป็นต้น องค์กร จะดำเนินการบันทึกคำคัดค้านดังกล่าวไว้เป็น หลักฐานด้วยเพื่อเป็นหลักฐานในการกระทำนั้น

2.2.4 แนวปฏิบัติ

เพื่อให้การบริหารจัดการข้อมูลตามวงจรชีวิตข้อมูลเป็นไปได้อย่างมีประสิทธิภาพ บทบาทหน้าที่ความรับผิดชอบของผู้มีส่วนได้ส่วนเสียในแต่ละวงจรชีวิตแสดงดังตารางด้านล่าง โดยคำนิยามของบทบาทหน้าที่ในแต่ละกิจกรรมมีดังต่อไปนี้

R (Responsible) หมายถึง ผู้มีหน้าที่ในการปฏิบัติงานตามกระบวนการหรือกิจกรรมที่กำหนดไว้

A (Accountable) หมายถึง ผู้มีหน้าที่ในการทบทวนและอนุมัติผลที่ได้รับจากปฏิบัติงาน

S (Supportive) หมายถึง ผู้ที่มีหน้าที่ในการสนับสนุนหรือให้การช่วยเหลือต่อปฏิบัติงาน

C (Consulted) หมายถึง ผู้ที่ทำหน้าที่ให้คำปรึกษาต่อผู้ปฏิบัติงาน

I (Informed) หมายถึง ผู้ที่ทำหน้าที่รับทราบผลการปฏิบัติงาน

กิจกรรม	ผู้มีส่วนได้ส่วนเสีย (Stakeholders)						
	คณะกรรมการ	คณะทำงานบริกรข้อมูล			เจ้าของข้อมูล	ผู้ใช้งานข้อมูล	หน่วยงานภายนอก
		หัวหน้าบริกรข้อมูล	บริกรข้อมูลเชิงธุรกิจ	บริกรข้อมูลเชิงเทคนิค			
1. การสร้างข้อมูล (Create)							
กำหนดสิทธิการสร้างข้อมูลให้สอดคล้องกับแนวทางหรือมาตรฐานการจัดชั้นความลับ		*I*	*R*	*S*	*A*	*I*	*I*
ออกแบบการสร้างข้อมูลให้สอดคล้องกับนโยบายขององค์กร	*A*	*A*	*R*	*S*	*A*		
ทดสอบกระบวนการสร้างข้อมูล		*A*	*C*	*R*	*C*	*R*	
สร้างข้อมูลที่ไม่ขัดต่อกฎหมายและจากแหล่งข้อมูลที่เชื่อถือได้เท่านั้น		*I*	*C*	*S*	*R/A*	*R*	
จัดทำคำอธิบายข้อมูลและปรับปรุงให้เป็นปัจจุบัน	*I*	*A*	*R*	*S*	*A*	*C*	
การตรวจสอบการสร้าง ข้อมูลให้ตรงตามมาตรฐานที่กำหนด อาทิ ความถูกต้องของข้อมูล		*I*	*A*	*C*	*A*	*R*	
ปรับปรุงการสร้างข้อมูล	*I*	*A*	*R*	*S*	*C*	*R*	
สร้างความรู้ความเข้าใจในการสร้างข้อมูลแก่ผู้ที่เกี่ยวข้องขององค์กร	*A*	*R*	*R*	*R*	*C*	*I*	
2. การจัดเก็บข้อมูล (Store)							
กำหนดสิทธิการจัดเก็บรักษาข้อมูล และกำหนดชั้นความลับของข้อมูล และจัดเก็บให้สอดคล้องกับแนวทางหรือมาตรฐานการจัดชั้นความลับ	*I*	*A*	*R*	*S*	*A*	*I*	

กิจกรรม	ผู้มีส่วนได้ส่วนเสีย (Stakeholders)						
	คณะกรรมการ	คณะทำงานบริกรข้อมูล			เจ้าของข้อมูล	ผู้ใช้งานข้อมูล	หน่วยงานภายนอก
		หัวหน้าบริกรข้อมูล	บริกรข้อมูลเชิงธุรกิจ	บริกรข้อมูลเชิงเทคนิค			
ออกแบบการจัดเก็บรักษาข้อมูลให้สอดคล้องกับนโยบายขององค์กร	*A*	*C*	*R*	*R*	*C*		
ทดสอบกระบวนการจัดเก็บรักษาข้อมูล		*A*	*C*	*R*	*S*	*S*	
จัดเก็บข้อมูลที่ไม่ขัดต่อกฎหมายและจากแหล่งข้อมูลที่เชื่อถือได้เท่านั้น		*C*	*C*	*C*	*R/A*	*R*	
จัดทำคำอธิบายข้อมูลละปรับปรุงให้เป็นปัจจุบัน		*A*	*R*	*S*	*R*	*R*	
แจ้งให้ผู้ใช้บริการทราบถึงเหตุผลในการจัดเก็บข้อมูล		*C*	*C*	*S*	*R*	*R*	
การสำรองข้อมูลยามเกิดเหตุฉุกเฉิน	*I*	*I*	*C*	*R*			
การแก้ไขข้อมูลเมื่อข้อมูลไม่ถูกต้อง	*I*	*I*	*C*	*S*	*A*	*R*	
การตรวจสอบการจัดเก็บข้อมูลให้ตรงตามมาตรฐานที่กำหนด		*I*	*R*	*R*	*S*	*R*	
สร้างความรู้ความเข้าใจในการจัดเก็บข้อมูลแก่ผู้ที่เกี่ยวข้องขององค์กร	*A*	*R*	*R*	*S*	*R*	*I*	*I*
3. การประมวลผลและการใช้ข้อมูล (Process and Use)							
กำหนดแนวปฏิบัติและมาตรฐานการประมวลผลข้อมูลและการใช้ข้อมูลให้เป็นมาตรฐานเดียวกัน	*I*	*A*	*R*	*S*	*S*	*I*	*I*
ออกแบบการบันทึกประวัติการประมวลผลและการใช้ข้อมูล		*A*	*C*	*R*	*I*	*I*	
ทดสอบกระบวนการประมวลผลและการใช้ข้อมูล		*A*	*C*	*R*	*S*	*S*	

กิจกรรม	ผู้มีส่วนได้ส่วนเสีย (Stakeholders)						
	คณะกรรมการ	คณะทำงานบริกรข้อมูล			เจ้าของข้อมูล	ผู้ใช้งานข้อมูล	หน่วยงานภายนอก
		หัวหน้าบริกรข้อมูล	บริกรข้อมูลเชิงธุรกิจ	บริกรข้อมูลเชิงเทคนิค			
ตรวจสอบประวัติการประมวลผลและการใช้งานข้อมูลจากกระบวนการทดสอบและการใช้จริง		*A*	*C*	*C*	*R*	*R*	
ตรวจสอบว่าผู้ใช้ข้อมูลประมวลผลและใช้ข้อมูลตรวจตามวัตถุประสงค์ที่แจ้งไว้หรือไม่		*I*	*R*	*C*	*R*		
ตรวจสอบเรื่องการเชื่อมโยงข้อมูลจากแหล่งข้อมูลน่าเชื่อถือ		*A*	*C*	*R*	*S*	*S*	
การทบทวนสิทธิการเข้าถึงเพื่อประมวลผลและการใช้ข้อมูล		*I*	*R*	*S*	*A*	*I*	*I*
สร้างความรู้ความเข้าใจในการประมวลผลและการใช้ข้อมูลแก่ผู้ที่เกี่ยวข้องขององค์กร	*A*	*R*	*R*	*S*	*R*	*I*	*I*
4. การเปิดเผยและรักษาความลับ (Disclosure and Confidentiality)							
กำหนดสิทธิการเปิดเผยข้อมูลและการรักษาความลับข้อมูล ร่วมห้ามเปิดเผยข้อมูลขัดต่อข้อตกลงต่างๆ	*A*	*A*	*R*	*S*	*R*	*I*	*I*
ออกแบบฟอร์มให้ตรงตามข้อกำหนดสำหรับการเปิดเผยข้อมูลและรักษาความลับข้อมูลให้เจ้าของข้อมูลใช้งาน	*A*	*A*	*R*	*S*	*R*		
ตรวจสอบว่าข้อมูลอยู่ในรูปแบบที่พร้อมเปิดเผย		*A*	*R*	*C*	*R*	*S*	
กำหนดช่องทางการเปิดเผยข้อมูลที่เข้าถึงและนำไปใช้งานได้	*I*	*A*	*R*	*S*	*R*	*I*	

กิจกรรม	ผู้มีส่วนได้ส่วนเสีย (Stakeholders)						
	คณะกรรมการ	คณะทำงานบริกรข้อมูล			เจ้าของข้อมูล	ผู้ใช้งานข้อมูล	หน่วยงานภายนอก
		หัวหน้าบริกรข้อมูล	บริกรข้อมูลเชิงธุรกิจ	บริกรข้อมูลเชิงเทคนิค			
ทดสอบกระบวนเปิดเผยข้อมูลผ่านช่องทางต่างๆ ว่าตรงตามข้อกำหนดหรือไม่		*A*	*C*	*R*	*S*	*S*	
ตรวจสอบว่าบุคลากรปฏิบัติตามขั้นตอนและวิธีการสำหรับการเปิดเผยและรักษาความลับของข้อมูลอย่างเคร่งครัดหรือไม่		*I*	*R*	*C*	*R*	*I*	
สร้างความรู้ความเข้าใจในการเปิดเผยและรักษาความลับของข้อมูลแก่ผู้ที่เกี่ยวข้องขององค์กร	*A*	*R*	*R*	*S*	*R*	*I*	*I*
5. การเก็บถาวรและทำลาย (Archive and Destroy)							
กำหนดขั้นตอนและวิธีการจัดเก็บถาวรและการทำลายข้อมูล	*A*	*A*	*R*	*R*	*C*	*I*	
กำหนดระยะเวลาและเครื่องมือในการจัดเก็บข้อมูลตามประเภทของข้อมูลและการทำลายข้อมูล	*A*	*A*	*S*	*R*	*C*	*I*	
กำหนดการอนุมัติตามสิทธิและการยืนยันข้อมูลก่อนการจัดเก็บถาวรและการทำลายข้อมูล		*A*	*R*	*I*	*A*	*I*	
ทดสอบกระบวนการจัดเก็บถาวรและการทำลายข้อมูล		*A*	*C*	*R*	*S*	*S*	
ทำการจัดเก็บถาวรของข้อมูล		*A*	*C*	*R*	*S*	*S*	
ทำการทำลายข้อมูล		*A*	*C*	*R*	*S*	*S*	

กิจกรรม	ผู้มีส่วนได้ส่วนเสีย (Stakeholders)						
	คณะกรรมการ	คณะทำงานบริกรข้อมูล			เจ้าของข้อมูล	ผู้ใช้งานข้อมูล	หน่วยงานภายนอก
		หัวหน้าบริกรข้อมูล	บริกรข้อมูลเชิงธุรกิจ	บริกรข้อมูลเชิงเทคนิค			
แจ้งให้ผู้ใช้บริการทราบถึงเหตุผลในการจัดเก็บถาวรและการทำลายข้อมูล		*A*	*S*	*C*	*R*	*R*	
เก็บหลักฐานสำหรับการยินยอมและการคัดค้านสำหรับการจัดเก็บถาวรและการทำลายข้อมูล		*C*	*S*	*R*	*R*		
ปรับปรุงกระบวนการด้านการจัดเก็บและการทำลายข้อมูล	*A*	*A*	*R*	*C*	*R*		
สร้างความรู้ความเข้าใจในการจัดเก็บถาวรและการทำลายข้อมูลแก่ผู้ที่เกี่ยวข้องขององค์กร	*A*	*R*	*R*	*S*	*R*	*I*	*I*

2.3 แนวปฏิบัติการบริหารจัดการคำอธิบายข้อมูล

2.3.1 นิยามคำอธิบายข้อมูล

1) ความหมาย

คำอธิบายข้อมูล (Metadata) เป็นข้อมูลที่ใช้อธิบายข้อมูลหลักหรือกลุ่มข้อมูลอื่น ๆ ที่เกี่ยวข้องทั้งคำอธิบายข้อมูลเชิงธุรกิจ (Business Metadata) และคำอธิบายข้อมูลเชิงเทคนิค (Technical Metadata) เพื่อให้ทราบรายละเอียดเกี่ยวกับโครงสร้างของข้อมูล เนื้อหาสาระ รูปแบบการจัดเก็บ แหล่งข้อมูล และสิทธิในการเข้าถึงข้อมูลช่วยให้ผู้ใช้ข้อมูลเข้าใจชุดข้อมูลได้ดียิ่งขึ้น ทั้งนี้หน่วยงานที่เกี่ยวข้องต้องจัดทำคำอธิบายข้อมูล และมีการบริหารจัดการคำอธิบายข้อมูล เช่น เมื่อมีการเปลี่ยนโครงสร้างของข้อมูล ต้องมีการปรับปรุงคำอธิบายข้อมูลด้วย

2) มาตรฐาน

มาตรฐานคำอธิบายข้อมูลที่จัดทำขึ้นนี้ประกอบด้วย คำอธิบายข้อมูล (Metadata) สำหรับข้อมูลเชิงธุรกิจ (Business Metadata) ที่ให้รายละเอียดของชุดข้อมูลในด้านธุรกิจหรือการดำเนินงานของหน่วยงานภายใน และ ข้อมูลเชิงเทคนิค (Technical Metadata) ที่ให้รายละเอียดของข้อมูลระดับตัวแปร

คำอธิบายข้อมูล (Metadata) สำหรับชุดข้อมูลที่มีคุณค่าสูง ข้อมูลสำคัญ ข้อมูลหลัก และข้อมูลที่ถูกสร้าง จัดเก็บ และนำเข้าในระบบสารสนเทศ เป็นส่วนที่บังคับต้องทำคำอธิบายข้อมูลตามที่กำหนดในมาตรฐาน

คำอธิบายข้อมูลเชิงธุรกิจ (Business Metadata) บอกรายละเอียดของข้อมูลในด้านธุรกิจ และมีคำอธิบายข้อมูลในรายละเอียดที่เกี่ยวข้อง ได้แก่ ชื่อที่ใช้สื่อสาร, นิยามหรือความหมาย, เจ้าของข้อมูล, ผู้ดูแลข้อมูล เป็นต้น โดยผู้บันทึกรายละเอียด คือ บริกรข้อมูลเชิงธุรกิจ (Business Data Steward) สำหรับผู้ใช้คือ ผู้ใช้งานข้อมูล (Data User) นักวิเคราะห์ข้อมูล (Data Analyst) และนักวิทยาการข้อมูล (Data Scientist)

คำอธิบายข้อมูลเชิงเทคนิค (Technical Metadata) บอกรายละเอียดของข้อมูลที่เกี่ยวข้องกับแหล่งข้อมูล ได้แก่ แหล่งที่มาของข้อมูล Application/Table/Attribute นิยามหรือความหมาย, ผู้ดูแลแหล่งข้อมูล (system/database administrator) ประเภทข้อมูล (Data Type) เป็นต้น โดยผู้บันทึกรายละเอียด คือ บริกรข้อมูลเชิงเทคนิค (Technical Data Steward) สำหรับผู้ใช้งาน คือวิศวกรข้อมูล (Data Engineer), นักพัฒนาโปรแกรม (Programmer), นักวิเคราะห์ระบบ(System analyst)

โดยข้อมูลต่างๆจะมีการทำบัญชีข้อมูล (Data Catalog) เพื่อบริหารจัดหมวดหมู่กลุ่มชุดข้อมูลให้ง่ายต่อการใช้งานและสืบค้น

2.3.2 แนวปฏิบัติ

กระบวนการและบทบาทหน้าที่ในการจัดทำคำอธิบายข้อมูล มีดังนี้

1) การกำหนดมาตรฐานคำอธิบายข้อมูล

1.1) บริกรข้อมูลเชิงธุรกิจและบริกรข้อมูลเชิงเทคนิค จัดทำมาตรฐานคำอธิบายข้อมูล ดังนี้

- คำอธิบายข้อมูลเชิงธุรกิจ

- คำอธิบายข้อมูลเชิงเทคนิค

1.2) คณะกรรมการธรรมาภิบาลข้อมูลให้ความเห็นชอบ มาตรฐานคำอธิบายข้อมูล

2) การสร้างคำอธิบายข้อมูล

2.1) เจ้าของข้อมูล ทำการกำหนดชุดข้อมูลที่จะจัดทำคำอธิบายข้อมูล

2.2) บริกรข้อมูลเชิงธุรกิจและบริกรข้อมูลเชิงเทคนิค บันทึกคำอธิบายข้อมูลตามมาตรฐานคำอธิบายข้อมูลที่ได้กำหนดไว้

2.3) บริกรข้อมูลเชิงธุรกิจและบริกรข้อมูลเชิงเทคนิค รวบรวมและตรวจสอบความถูกต้องของคำอธิบายข้อมูลให้ตรงตามมาตรฐาน

2.4) เจ้าของข้อมูลสอบทานความถูกต้องของคำอธิบายข้อมูล ตามมาตรฐานคำอธิบายข้อมูลที่ได้กำหนดไว้อีกครั้ง

3) การปรับปรุงคำอธิบายข้อมูล

3.1) ผู้ใช้งานข้อมูลพบความไม่ถูกต้อง ไม่เป็นปัจจุบันของคำอธิบายข้อมูล ทำการแจ้งไปยังบริกรข้อมูลเชิงธุรกิจและบริกรข้อมูลเชิงเทคนิคทราบ

3.2) บริกรข้อมูลเชิงธุรกิจและบริกรข้อมูลเชิงเทคนิคแจ้งไปยังเจ้าของข้อมูล เพื่อร่วมกันตรวจสอบการเปลี่ยนแปลง (เพิ่ม/แก้ไข/ลบ) และทำการแก้ไขให้คำอธิบายข้อมูลมีความถูกต้อง

4) พิจารณาและสอบทานคำอธิบายข้อมูล

4.1) ผู้ใช้ข้อมูลและ/หรือ เจ้าของข้อมูล แจ้งปัญหาหรือข้อเสนอแนะของคำอธิบายข้อมูล รวมถึงมาตรฐานของคำอธิบายข้อมูลมีความเหมาะสมหรือไม่ และแจ้งไปยังบริกรข้อมูล

4.2) บริกรข้อมูลเชิงธุรกิจและบริกรข้อมูลเชิงเทคนิค สอบทานความถูกต้องของคำอธิบายข้อมูล ตามมาตรฐานคำอธิบายข้อมูลที่ได้กำหนดไว้ อย่างน้อย 1 ครั้งต่อปี

4.3) เจ้าของข้อมูล พิจารณา ความถูกต้องของคำอธิบายข้อมูล ให้เป็นปัจจุบัน

2.4 แนวปฏิบัติการบริหารจัดการคุณภาพข้อมูล

2.4.1. นิยามคุณภาพข้อมูล

คุณภาพข้อมูล (Data Quality) หมายถึง คุณลักษณะของข้อมูลตามองค์ประกอบและมาตรฐานที่กำหนด เพื่อทำให้ข้อมูลมีคุณภาพ น่าเชื่อถือ ไม่ขัดแย้งกับตรรกะเหตุผล สามารถนำไปใช้ในการบริหารจัดการในด้านต่าง ๆ เพื่อประกอบการตัดสินใจทางธุรกิจให้มีประสิทธิภาพและประสิทธิผล

องค์ประกอบของคุณภาพข้อมูลมี ดังนี้

1) มิติด้านคุณภาพข้อมูล

1.1) ความถูกต้อง (Accuracy) ข้อมูลจะมีความถูกต้องและเชื่อถือได้ขึ้นกับวิธีที่ใช้ในการควบคุมข้อมูลนำเข้า และการควบคุมการประมวลผล การควบคุมการนำเข้าเป็นการกระทำเพื่อให้เกิดความมั่นใจว่าข้อมูลนำเข้ามีความถูกต้องเชื่อถือได้

1.2) ความครบถ้วน (Completeness) ข้อมูลบางประเภทหากไม่ครบถ้วน จัดเป็นข้อมูลที่ด้อยคุณภาพได้เช่น ข้อมูลที่อยู่ลูกค้า มีบ้านเลขที่ แต่ไม่มี ตำบล/แขวง อำเภอ/เขต จังหวัด ข้อมูลเหล่านี้ไม่สามารถนำมาใช้ได้

1.3) ความสอดคล้องกัน (Consistency) ค่าข้อมูลในชุดข้อมูลเดียวกันต้องสอดคล้องกัน หรือการดึงข้อมูลค่าเดียวกันจากชุดข้อมูลที่แยกกัน ต้องไม่ขัดแย้งกัน

1.4) ความทันสมัย (Timeliness) ข้อมูลที่ดีนั้นนอกจากจะเป็นข้อมูลที่มีความถูกต้องเชื่อถือได้แล้ว จะต้องเป็นข้อมูลที่เป็นปัจจุบัน เพื่อให้ผู้ใช้สามาถนำเอาผลลัพธ์ที่ได้ไปใช้ได้ทันเวลา

1.5) ตรงตามความต้องการของผู้ใช้ (Relevancy) เป็นข้อมูลที่ตรงความต้องการและวัตถุประสงค์ของการใช้งาน และมีการประเมินความพึงพอใจและการปรับปรุงคุณภาพให้ตรงตามความต้องการของผู้ใช้

1.6) ความพร้อมใช้ (Availability) ข้อมูลควรเข้าถึงได้ง่าย สามารถใช้งานได้จริง และพร้อมใช้งาน

ตารางที่ 2.3 ตัวอย่างมิติด้านคุณภาพข้อมูล

ลำดับ	มิติด้านคุณภาพข้อมูล	ตัวอย่าง
1	ความถูกต้อง (Accuracy)	1) สถานที่ติดตั้งมาตรวัดน้ำตรงตามสถานที่ใช้น้ำจริง 2) ข้อมูลค่าความขุ่นของน้ำดิบอยู่ในช่วงที่เป็นไปได้ และเป็นที่ยอมรับทางเทคนิค
2	ความครบถ้วน (Completeness)	1) รายละเอียดข้อมูลของลูกค้า เช่น ชื่อ สถานที่ใช้น้ำ สถานที่ติดต่อ email ประเภทผู้ใช้น้ำ รหัสมาตรวัดน้ำ หมายเลขมาตรวัดน้ำ และ วันที่ติดตั้ง ครบถ้วน 2) จำนวนรายการข้อมูลความขุ่นของน้ำดิบครบตามช่วงเวลาที่กำหนด
3	ความสอดคล้องกัน (Data Consistency)	1) คำนำหน้าชื่อต้องสอดคล้องกับเพศที่ระบุมา 2) ข้อมูลความขุ่นของน้ำที่วัดได้จากสถานีที่อยู่ต้นน้ำและปลายน้ำต้องมีความสอดคล้องกันตามทิศทางการไหลของน้ำ
4	ความทันสมัย (Timeliness)	1) ข้อมูลการอ่านน้ำต้องได้รับการบันทึกในฐานข้อมูลทุก ๆ เดือน 2) แสดงผลข้อมูลคุณภาพน้ำบนแพลตฟอร์มออนไลน์ในช่วงเวลาที่กำหนด
5	ตรงตามความต้องการของผู้ใช้ (Relevancy)	1) ข้อมูลที่แสดงในใบแจ้งค่าน้ำตรงตามความต้องการของผู้ใช้น้ำ 2) ข้อมูลคุณภาพน้ำดิบสามารถถูกส่งออกในรูปแบบที่ต้องการได้

ลำดับ	มิติด้านคุณภาพข้อมูล	ตัวอย่าง
6	ความพร้อมใช้ (Availability)	1) ผู้ใช้น้ำสามารถเข้าถึงข้อมูลใบแจ้งค่าน้ำรายเดือนผ่านแอปพลิเคชั่นได้ 2) ข้อมูลคุณภาพน้ำดิบได้รับการคัดกรองก่อนการเผยแพร่สู่สาธารณะและมีคำอธิบายข้อมูลชัดเจนเพื่อการนำไปใช้ต่อยอด

2) มาตรฐาน

องค์ประกอบของมาตรฐานการจัดการคุณภาพข้อมูล อ้างอิงกรอบแนวคิดจาก ISO8000-61 โดยมีกระบวนการที่สำคัญ ดังต่อไปนี้

2.1) การวางแผนคุณภาพข้อมูล (Data Quality Planning) เป็นการวางแผนพัฒนา รวมถึงข้อตกลง ข้อกำหนด วัตถุประสงค์ และแผนงานโดยรวม เพื่อบรรลุการจัดการคุณภาพข้อมูล

2.1.1) การจัดการมาตรฐานและขั้นตอน ที่สนับสนุนทำให้เกิดคุณภาพข้อมูล

2.1.2) การวางแผนการดำเนินการคุณภาพข้อมูล เป็นการพัฒนาแผนเพื่อกำหนดบทบาท ความรับผิดชอบ การจัดลำดับงาน เงินทุน เครื่องมือ และเทคโนโลยีเพื่อดำเนินกิจกรรมอื่น ๆ ที่เกี่ยวข้องกับการจัดการคุณภาพข้อมูล

2.2) การควบคุมคุณภาพข้อมูล (Data Quality Control) เป็นกระบวนการเพื่อให้เกิดความมั่นใจว่าข้อมูลที่เกิดขึ้นเป็นไปตามข้อกำหนด

2.2.1) การจัดเตรียมข้อกำหนดของข้อมูล (Data Specifications) และคำแนะนำในการทำงานเพื่อให้มั่นใจว่าข้อมูลเป็นไปตามข้อกำหนด

2.2.2) การประมวลผลข้อมูล (Data Processing) เพื่อตรวจสอบว่าข้อมูลที่เกิดจากกระบวนการตรงตามข้อกำหนดของข้อมูล

2.2.3) การติดตามและควบคุมคุณภาพข้อมูล (Data Quality Monitoring and Control) เพื่อระบุและตอบสนองต่อกรณีที่การประมวลผลข้อมูลไม่เป็นไปตามข้อกำหนด

2.3) การประกันคุณภาพข้อมูล (Data Quality Assurance) เป็นกระบวนการประเมินระดับคุณภาพข้อมูลและประสิทธิภาพของกระบวนการที่เกี่ยวข้องกับคุณภาพข้อมูล

2.3.1) สอบทานปัญหาด้านคุณภาพข้อมูล เพื่อทำความเข้าใจลักษณะและขอบเขตของปัญหาด้านคุณภาพข้อมูล

2.3.2) กำหนดเกณฑ์การวัด (Measurement Criteria) เป็นการพัฒนาตัววัดและวิธีการวัดเพื่อสนับสนุนการวัดคุณภาพข้อมูล

2.3.3) การวัดคุณภาพข้อมูลและประสิทธิภาพของกระบวนการ ต้องมีวิธีการประเมินกระบวนการและผลของคุณภาพข้อมูล

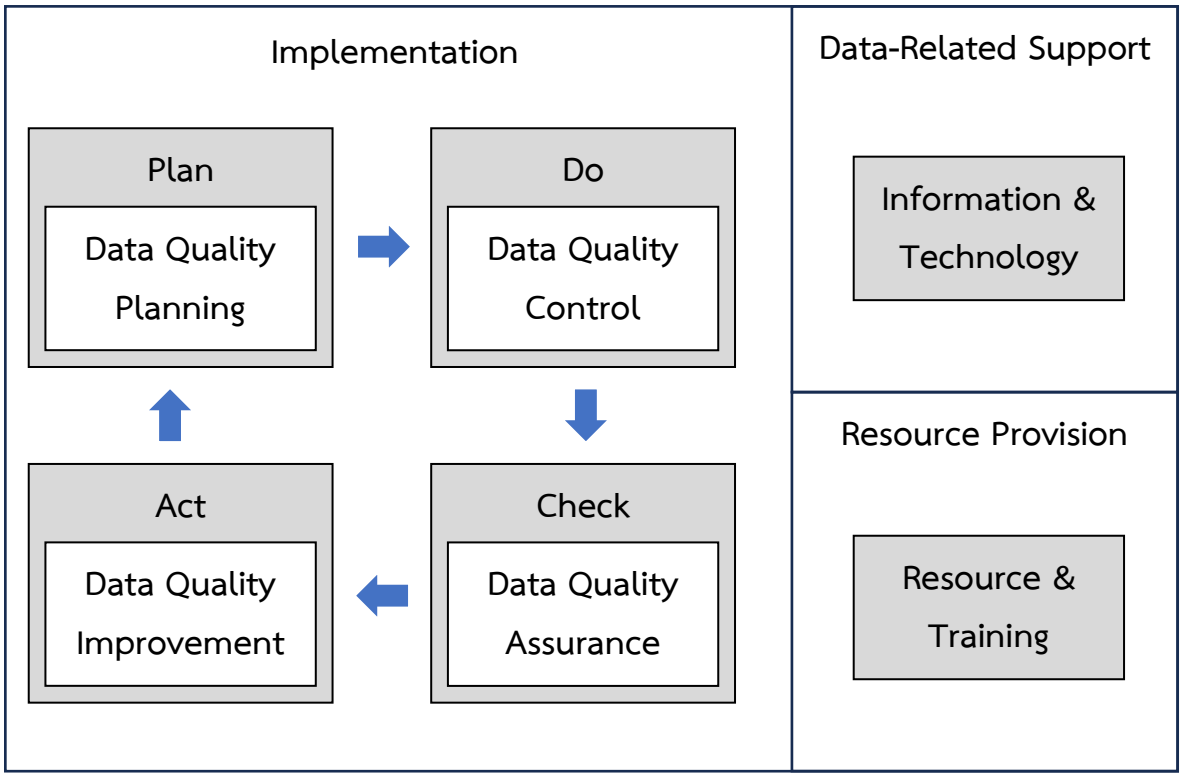
2.3.4) การประเมินผลการวัด วิเคราะห์ผลลัพธ์ของการวัดคุณภาพข้อมูลและประเมินผลกระทบของคุณภาพข้อมูลที่ไม่ดีและกระบวนการวัด

2.4) การปรับปรุงคุณภาพข้อมูล (Data Quality Improvement) เป็นกระบวนการนำเสนอการปรับปรุงคุณภาพข้อมูลอย่างยั่งยืน

2.4.1) การวิเคราะห์หาต้นเหตุและแนวทางแก้ไข โดยระบุสาเหตุของปัญหาด้านคุณภาพของข้อมูล พร้อมเสนอแนวทางแก้ไขเพื่อป้องกันไม่ให้เกิดขึ้นอีก

2.4.2) การปรับปรุงคุณภาพข้อมูล (Cleansing data) เพื่อแก้ไขปัญหาคุณภาพข้อมูลโดยใช้เครื่องมืออัตโนมัติและ/หรือมีผู้รับผิดชอบดำเนินการ

2.4.3) การปรับปรุงกระบวนการ เพื่อป้องกันไม่ให้เกิดปัญหาขึ้นซ้ำ ทั้งข้อมูลและกระบวนการที่ไม่เป็นไปตามข้อกำหนด



รูปที่ 2 มาตรฐานการจัดการคุณภาพข้อมูล ISO 8000-61:2016

2.4.2. แนวปฏิบัติ

1) กระบวนการและระเบียบวิธีปฏิบัติการจัดการคุณภาพข้อมูลมีขั้นตอน ดังนี้

1.1) การวางแผนคุณภาพข้อมูล เป็นหน้าที่ของเจ้าของข้อมูล

1) วางแผนด้านจัดสรรทรัพยากร เช่น ทรัพยากรบุคคล, เครื่องมือและงบประมาณ เป็นต้น และด้านกระบวนการแก้ปัญหา โดยมีการจัดลำดับความสำคัญของปัญหาที่รอการแก้ไข

1.2) การควบคุมคุณภาพข้อมูล เป็นหน้าที่ของเจ้าของข้อมูลหรือผู้ที่ได้รับมอบหมาย โดยการศึกษาลักษณะข้อมูล (Data Profiling) ประมวลผลและตรวจสอบคุณภาพข้อมูล

1) ระบุชุดข้อมูลที่ต้องทำการควบคุมคุณภาพ

2) ระบุข้อกำหนดของข้อมูล (Data Specification) ที่ต้องการควบคุมคุณภาพ เช่น เงื่อนไขทางธุรกิจ (Business Rule) และมิติคุณภาพข้อมูล โดยต้องมีการกำหนดมิติคุณภาพข้อมูลอย่างน้อย 1 มิติ

3) กำหนดระดับคุณภาพของข้อมูล (Data Quality Threshold) ในแต่ละชุดข้อมูลพร้อมทั้งหลักเกณฑ์ในการตรวจสอบ

4) ตรวจสอบข้อมูลที่กำหนด โดยอาจใช้เครื่องมือที่ช่วยในการประมวลผล เช่น SQL หรือ Excel เป็นต้น

5) นำเสนอผลการตรวจสอบคุณภาพข้อมูลผ่านทางรายงานและ/หรือ Dashboard

1.3) การประกันคุณภาพข้อมูล เป็นหน้าที่ของบริกรข้อมูลเชิงธุรกิจและบริกรข้อมูลเชิงเทคนิคร่วมกับเจ้าของข้อมูล โดยการประเมินทำความเข้าใจลักษณะและขอบเขตของปัญหาคุณภาพข้อมูล

1) ตรวจสอบปัญหาด้านคุณภาพข้อมูลในรายงานคุณภาพข้อมูล ทำความเข้าใจลักษณะและขอบเขตของปัญหา

2) กำหนด และ/หรือ ปรับปรุงเกณฑ์การวัด เช่น การพัฒนาตัววัด วิธีการวัด เพื่อสนับสนุนการวัดคุณภาพข้อมูลให้มีประสิทธิภาพมากขึ้น รวมถึงวัดระดับคุณภาพข้อมูลและประเมินกระบวนการวัดผ่านทางรายงานและ/หรือ (Dashboard)

3) สนับสนุนให้ผู้มีส่วนได้ส่วนเสียของข้อมูลร่วมทำการวัดระดับคุณภาพข้อมูลและประเมินกระบวนการวัดผ่านทางรายงานและ/หรือ (Dashboard)

4) ร่วมกันประเมินผลการวัด วิเคราะห์ผลลัพธ์ของการวัดคุณภาพข้อมูลและประเมินผลกระทบของคุณภาพข้อมูลที่ไม่ดีและกระบวนการวัด

1.4) การปรับปรุงคุณภาพข้อมูล เป็นหน้าที่ของเจ้าของข้อมูลหรือผู้ที่ได้รับมอบหมาย โดยนำเสนอการปรับปรุงคุณภาพข้อมูลอย่างยั่งยืน

1) ร่วมวิเคราะห์หาสาเหตุและการพัฒนาแนวทางแก้ไข โดยระบุสาเหตุของปัญหาด้านคุณภาพของข้อมูลและเสนอแนวทางแก้ไขเพื่อป้องกันไม่ให้เกิดขึ้นอีก

2) ปรับปรุงข้อมูลให้มีคุณภาพ เพื่อการแก้ไขปัญหาคุณภาพข้อมูลโดยใช้เครื่องมืออัตโนมัติและ/หรือดำเนินการโดยไม่ใช้เครื่องมืออัตโนมัติ เช่น ดำเนินการเขียนสคริปต์ด้วยภาษาคอมพิวเตอร์เพื่อปรับปรุงข้อมูลให้เป็นไปตามข้อกำหนด

3) เสนอแนวทางการป้องกันปัญหาของข้อมูลที่ไม่เป็นไปตามข้อกำหนด อาจเป็นการนำวิธีแก้ปัญหาไปขยายผล เพื่อใช้ป้องกันการเกิดขึ้นซ้ำของปัญหา อย่างเช่น เสนอให้มีการป้องกันการกรอกข้อมูลที่ไม่ถูกต้องบนโปรแกรมที่ใช้นำเข้าข้อมูล เช่น การกรอกคำนำหน้าชื่อสกุลของลูกค้า ต้องสอดคล้องกับเพศของลูกค้า เป็นต้น

2.4.3 ตัวอย่างการดำเนินงานตรวจสอบคุณภาพข้อมูล

ดำเนินการตรวจสอบข้อมูล โดย Data Quality Rule เป็นดังนี้

1) ชุดข้อมูลที่ต้องทำการควบคุมคุณภาพ : ค่าความเป็นกรด - ด่าง

2) ข้อกำหนดของข้อมูล (Data Specification)

- เงื่อนไขทางธุรกิจ (Business Rule)

• *ค่าความเป็นกรด-ด่าง: ต้องมีค่าอยู่ระหว่าง 0 ถึง 14*

• มิติคุณภาพข้อมูล

• *ความถูกต้องของข้อมูล (Data Accuracy): คอลัมน์ค่าความเป็นกรด-ด่างของน้ำดิบอยู่ในช่วงที่กำหนดตามเงื่อนไข*

3) ระดับคุณภาพของข้อมูล (Data Quality Threshold)

• กำหนดระดับคุณภาพของข้อมูล ดังนี้

• *พบค่าผิดปกติน้อยกว่าหรือเท่ากับ 10 เปอร์เซ็นต์ เป็นระดับสีเขียว*

• *พบค่าผิดปกติมากกว่า 10 เปอร์เซ็นต์ เป็นระดับสีแดง*

4) การประเมินคุณภาพข้อมูลตามหลักเกณฑ์คุณภาพข้อมูล

• จัดทำการศึกษาข้อมูล (Data Profiling) ใช้ script เพื่อตรวจสอบข้อมูลว่าตรงตามเงื่อนไขทางธุรกิจและตรงตามคุณลักษณะข้อมูล ดังนี้

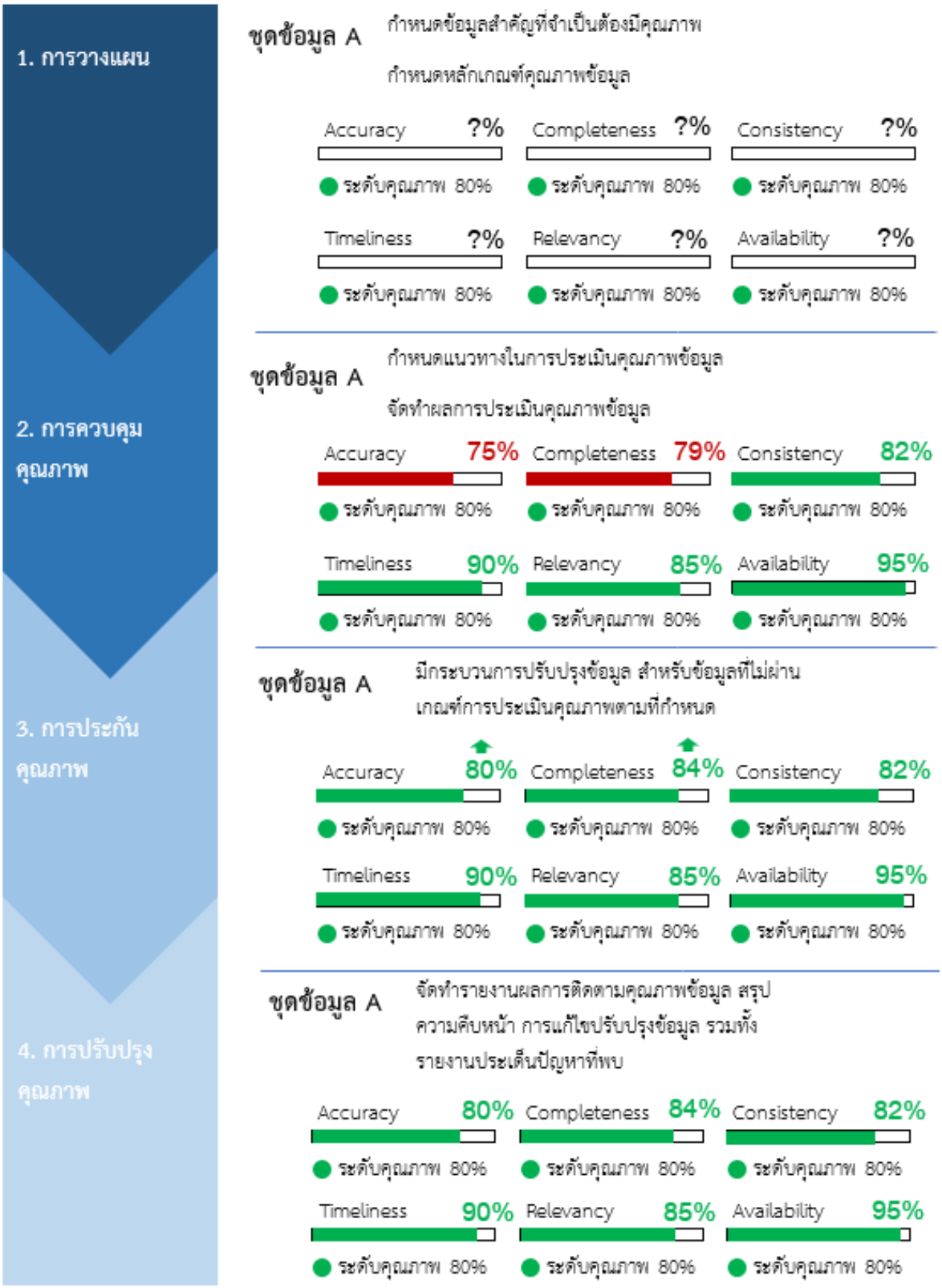
• *คอลัมน์ pH ค่าต้องอยู่ระหว่าง 0 - 14*

• ชุดข้อมูลที่ไม่เป็นไปตามระดับคุณภาพข้อมูล มีดังนี้

• คอลัมน์ pH พบความผิดปกติ ค่าที่ไม่ได้อยู่ระหว่าง 0 - 14 ดังนี้

Column	**pH < 0**	**pH > 14**
pH	xxx	xxx

กระบวนการจัดการคุณภาพข้อมูล



ตัวอย่างการวัดคุณภาพข้อมูลที่เป็นโครงสร้างสำหรับแต่ละชุดข้อมูล

มิติคุณภาพข้อมูล	รูปแบบการวัด	หน่วยวัด	ตัวอย่าง
ความถูกต้อง	แถว x ฟิลด์	ร้อยละ	ถ้าพบว่ามี 80 ฟิลด์ที่มีความถูกต้องตลอดทั้ง 1,000 คน ดังนั้นชุดข้อมูลนี้มีความถูกต้อง = (1000 x 80) / (1000 x 100) x 100 = 80
ความครบถ้วน	1) แถว 2) แถว x ฟิลด์ 3) แถว x ฟิล์ดที่จำเป็น	ร้อยละ	1) พิจารณาเฉพาะแถวข้อมูล ถ้าพบว่ามีการบันทึกข้อมูล 900 คน โดยไม่สนใจจำนวนฟิลด์ที่มีการบันทึก ดังนั้นข้อมูลชุดนี้มีความครบถ้วน = (900 / 1000) x 100 = 90 2) พิจารณาแถวและฟิลด์ข้อมูล ถ้าพบว่ามี 60 ฟิลด์จาก 100 ฟิลด์ ที่มีการบันทึกข้อมูลทั้ง 1,000 คน ดังนั้นข้อมูลชุดนี้มีความครบถ้วน = (1000 x 60) / (1000 x 100) x 100 = 60 3) พิจารณาแถวและฟิลด์ข้อมูลที่มีความจำเป็นเท่านั้น ถ้ากำหนดให้มี 80 ฟิลด์ที่มีความจำเป็นต้องบันทึกข้อมูล แล้วพบว่ามี 60 ฟิลด์จาก 80 ฟิลด์ ที่มีการบันทึกข้อมูลทั้ง 1,000 คน ดังนั้นข้อมูลชุดนี้มีความครบถ้วน = (1000 x 60) / (1000 x 80) x 100 = 75
ความต้องกัน	ฟิลด์	ร้อยละ	ถ้าพบว่ามี 20 ฟิลด์ที่เก็บซ้ำซ้อนกับชุดข้อมูลอื่นและมีรูปแบบของฟิลด์ที่แตกต่างกัน เช่น รูปแบบวันที่ รูปแบบรหัส ดังนั้น ข้อมูลชุดนี้มีความต้องกัน

มิติคุณภาพข้อมูล	รูปแบบการวัด	หน่วยวัด	ตัวอย่าง
			= ((100 – 20) / 100) x 100 = 80
ความทันสมัย	1) แถว 2) แถว x ฟิลด์	ร้อยละ	1) พิจารณาเฉพาะแถวข้อมูล ถ้ามีพนักงานใหม่ 10 คน และมีพนักงานเก่า 5 คนที่มีการเปลี่ยนแปลงข้อมูล ซึ่งยังไม่มีการบันทึกหรือปรับปรุงให้เป็นปัจจุบัน ดังนั้นข้อมูลชุดนี้มีความเป็นปัจจุบัน = 100 – ((10 + 5) / (1000 + 10) x 100) = 98.51 2) พิจารณาแถวและฟิลด์ข้อมูล ถ้ามีพนักงานใหม่ 10 คน และมีพนักงานเก่า 5 คนที่มีการเปลี่ยนชื่อและที่อยู่ ซึ่งยังไม่มีการบันทึกหรือปรับปรุงให้เป็นปัจจุบัน ดังนั้นข้อมูลชุดนี้มีความเป็นปัจจุบัน (หมายเหตุ : ชื่อและที่อยู่ นับเป็น 2 ฟิลด์) = 100 – (((10 x 2) + (5 x 2)) / ((1000 + 10) x 100) x 100) = 99.97
ตรงตามความต้องการใช้	ฟิลด์	ร้อยละ	ถ้าพบว่ามี 20 ฟิลด์ที่ไม่เคยถูกนำไปใช้ ดังนั้นข้อมูลชุดนี้มีความตรงตามความต้องการใช้ = ((100 – 20) / 100) x 100 = 80
ความพร้อมใช้	ชุดข้อมูล	ร้อยละ	= 100 ถ้าข้อมูลเก็บอยู่ในรูปแบบฐานข้อมูลหรือเว็บเซอร์วิส = 66.67 ถ้าข้อมูลเก็บอยู่ในรูปแบบไฟล์ XML JSON หรือ CSV = 33.33 ถ้าข้อมูลเก็บอยู่ในรูปแบบไฟล์ WORD PDF

มิติคุณภาพข้อมูล	รูปแบบการวัด	หน่วยวัด	ตัวอย่าง
			หมายเหตุ : ข้อมูลที่อยู่ในระดับที่ต่ำกว่าสามารถจัดให้อยู่ในระดับที่สูงขึ้นได้ ถ้ามีเครื่องมือหรือวิธีการที่ทำให้การนำข้อมูลไปใช้งานสะดวกมากขึ้น

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

2.5 แนวปฏิบัติการจัดหมวดหมู่และระดับชั้นความลับข้อมูล

2.5.1 นิยามหมวดหมู่และระดับชั้นความลับข้อมูล

1) ความหมาย

การกำหนดหมวดหมู่และระดับชั้นความลับของข้อมูลใช้กับข้อมูลทุกรูปแบบขององค์กร ด้วยการประเมินผลกระทบของข้อมูลหน่วยงาน เพื่อระบุหมวดหมู่และระดับชั้นความลับของข้อมูล รวมทั้งกำหนดระดับความปลอดภัยที่เหมาะสมสำหรับการสร้าง/จัดเก็บ การใช้ และการเข้าถึงชุดข้อมูล และเพื่อใช้กับบุคลากร รวมถึงตัวแทนบุคคลที่สามที่ได้รับอนุญาตให้เข้าถึงข้อมูลในหน่วยงาน พร้อมทั้งกำหนดบทบาทหน้าที่ของบุคลากรในการจัดหมวดหมู่และระดับชั้นความลับ เพื่อป้องกัน จัดการ และกำกับดูแลข้อมูลให้เหมาะสม

2) การกำหนดหมวดหมู่ของข้อมูล (Data Category)

ทุกชุดข้อมูลต้องมีการจัดหมวดหมู่ ดังต่อไปนี้

หมวดหมู่ข้อมูล	**คำอธิบาย**
ข้อมูลสาธารณะ (Open)	หมายถึง ข้อมูลที่สามารถเปิดเผยได้ ประชาชนทั่วไปสามารถนำไปใช้ได้อย่างอิสระ ไม่ว่าจะเป็นข้อมูลข่าวสาร ข้อมูลส่วนบุคคล ข้อมูลอิเล็กทรอนิกส์ เป็นต้น
ข้อมูลใช้ภายใน (Internal Use Only)	หมายถึง ข้อมูลสำหรับใช้ในการดำเนินกิจการภายในขององค์กรซึ่งไม่อนุญาตให้นำไปใช้งานภายนอกก่อนได้รับอนุญาต เช่น นโยบาย มาตรฐาน และขั้นตอนการปฏิบัติงาน ประกาศ และบันทึกภายในหน่วยงาน เป็นต้น
ข้อมูลส่วนบุคคล (Personal data)	หมายถึง ข้อมูลเกี่ยวกับสิ่งเฉพาะตัวของบุคคลที่ทำให้สามารถระบุตัวหรือรู้ตัวของบุคคลนั้น ๆ ได้ทั้งทางตรงหรือทางอ้อม ตามมาตรา 6 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
ข้อมูลข่าวสารลับ (Classified Information)	หมายถึง ข้อมูลที่อยู่ในความครอบครองหรือควบคุมดูแลขององค์กรที่มีคำสั่งไม่ให้มีการเปิดเผยตามระดับชั้นความลับ
ข้อมูลความมั่นคง (National Security Information)	หมายถึง ข้อมูลเกี่ยวกับความมั่นคงของรัฐ ที่ทำให้เกิดความสงบเรียบร้อย การมีเสถียรภาพความเป็นปึกแผ่น ปลอดภัยจากภัยคุกคาม เป็นต้น

3) ทุกชุดข้อมูลต้องมีการกำหนดระดับชั้นความลับข้อมูล (Data Classification) ดังต่อไปนี้

ระดับชั้นความลับ	**คำอธิบาย**
1. เปิดเผย (Open)	หมายถึง ข้อมูลที่ได้รับการเปิดเผยต่อสาธารณะชน ดังนั้นจึงไม่มีข้อจำกัดในการนำมาใช้ประโยชน์และไม่มีมีผลกระทบอย่างมีนัยสำคัญต่อการดำเนินงาน
2. เผยแพร่ภายในองค์กร (Private)	หมายถึง ข้อมูลที่ไม่ใช่ประเภท ลับ ลับมาก หรือ ลับที่สุด และเป็นข้อมูลเพื่อการใช้งานภายในองค์กรเท่านั้น การเปิดเผยหรือการเข้าถึงข้อมูลในระดับชั้นนี้ สามารถเข้าถึงได้โดยบุคคลภายในองค์กรได้แก่ กรรมการ ผู้บริหาร บุคลากร และ/หรือตัวแทนขององค์กรเท่านั้น ตามหน้าที่ที่ได้รับมอบหมายและสิทธิในการเข้าถึง
3. ลับ (Confidential)	หมายถึง ข้อมูลมีความสำคัญต่อการดำเนินงานตามภารกิจขององค์กร โดยต้องได้รับการควบคุมการเข้าถึงข้อมูลเฉพาะผู้มีอำนาจตามที่กำหนดในการเข้าถึงข้อมูลเท่าที่จำเป็นต่อการปฏิบัติงาน และห้ามเผยแพร่ต่อบุคคลภายนอกเว้นแต่จะได้รับอนุมัติเป็นลายลักษณ์อักษรโดยคณะกรรมการ หรือ หัวหน้าหน่วยงานเทียบเท่า ที่เป็นเจ้าของข้อมูลขึ้นไป โดยต้องมีการลงนามในเอกสารสัญญาการรักษาข้อมูลที่เป็นความลับ (Non-Disclosure Agreement) หรือข้อตกลงการแบ่งปันข้อมูล (Data Sharing Agreement) เว้นแต่การเผยแพร่ดังกล่าวเป็นไปตามอำนาจที่กฎหมายให้การรับรอง
4. ลับมาก (Secret)	หมายถึง ข้อมูลมีความสำคัญต่อการดำเนินงานตามภารกิจขององค์กร โดยต้องได้รับการควบคุมอย่างเข้มงวดโดยจำกัดการเข้าถึงข้อมูลเฉพาะผู้มีอำนาจตามที่กำหนดในการเข้าถึงข้อมูลเท่าที่จำเป็นต่อการปฏิบัติงาน ซึ่งอาจเป็นกลุ่มคนในหน่วยงานที่เกี่ยวข้องเท่านั้น เพื่อป้องกันการรั่วไหลไปสู่บุคคลที่ไม่เกี่ยวข้อง
5. ลับที่สุด (Top Secret)	หมายถึง ข้อมูลมีความสำคัญสูงต่อการดำเนินงานตามภารกิจขององค์กร โดยต้องได้รับการควบคุมอย่างเข้มงวดที่สุดโดยต้องจำกัดผู้มีอำนาจในการเข้าถึงข้อมูลให้น้อยที่สุดในระดับบุคคลและตำแหน่งงานเท่านั้น เพื่อป้องกันการรั่วไหลไปสู่บุคคลภายนอก และ/หรือ บุคคลที่ไม่เกี่ยวข้อง

2.5.2 แนวปฏิบัติ

1) การจำแนกหมวดหมู่ของข้อมูลในการแบ่งระดับชั้นความลับข้อมูล

1.1) เจ้าของข้อมูลจัดทำหมวดหมู่ชุดข้อมูล และกำหนดระดับชั้นความลับของข้อมูล (Data Classification) โดยอ้างอิงแผนผังการตัดสินใจจำแนกหมวดหมู่ข้อมูล ในการจัดทำหมวดหมู่ข้อมูล และเกณฑ์การประเมินระดับชั้นความลับของชุดข้อมูล (Scoring Data Classification Guideline) เพื่อทำการประเมินขั้นต้น เมื่อได้ระดับชั้นความลับแล้วนำมาตรวจสอบกับขั้นตอนปฏิบัติการจัดระดับชั้นความลับข้อมูลว่ามีความสอดคล้องกันหรือไม่ กรณีไม่สอดคล้องกัน ให้ประเมินและปรับปรุงระดับชั้นความลับของข้อมูลใหม่ เพื่อกำหนดระดับชั้นความลับของชุดข้อมูล

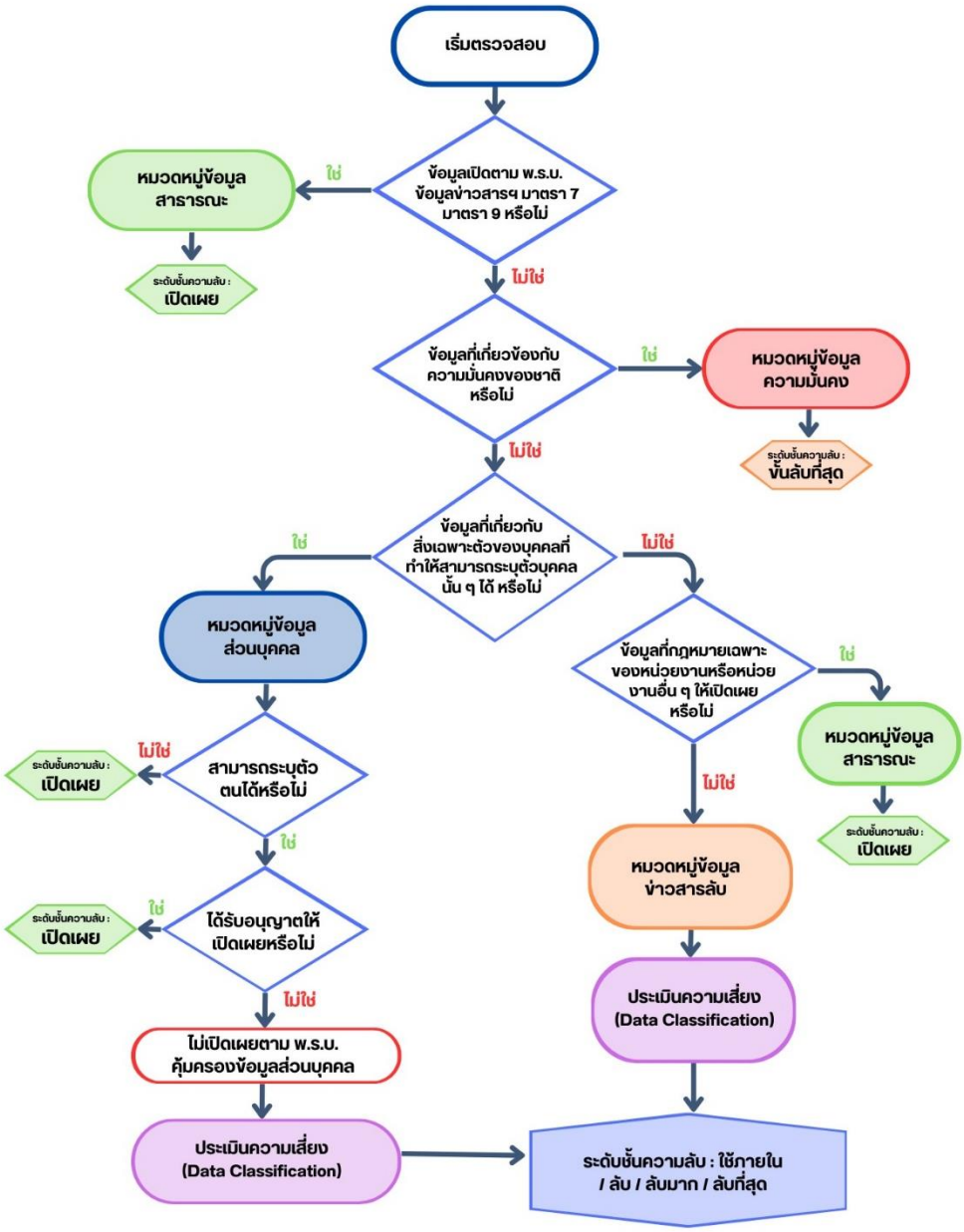
กรณีหมวดหมู่ข้อมูลส่วนบุคคล ให้จัดทำการประเมินผลกระทบต่อเจ้าของข้อมูล (Impact to data Subject) โดยอ้างอิงเกณฑ์การประเมินผลกระทบต่อเจ้าของข้อมูลส่วนบุคคล (Scoring Impact to Data Subject) เพื่อนำหมวดหมู่ชุดข้อมูล ระดับชั้นความลับของชุดข้อมูลและผลกระทบต่อเจ้าของข้อมูลมาประกอบการจัดทำคำอธิบายข้อมูล โดยกรณีเป็นหมวดหมู่ข้อมูลส่วนบุคคล จะต้องนำนโยบายและแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล และเอกสารที่เกี่ยวข้องในการกำกับดูแลข้อมูลส่วนบุคคลมาอ้างอิงประกอบการลงรายละเอียดของข้อมูลด้วย

1.2) บริกรข้อมูลเชิงธุรกิจจัดทำคำอธิบายข้อมูลเชิงธุรกิจ (Business Metadata)

1.3) บริกรข้อมูลเชิงเทคนิคจัดทำคำอธิบายชุดข้อมูลเชิงเทคนิค Technical Metadata หรือพจนานุกรมข้อมูล (Data Dictionary) ร่วมกับหน่วยงานผู้ดูแลข้อมูลและ ผู้ดูแลระบบสารสนเทศ

1.4) หน่วยงานเจ้าของข้อมูล สรุปรายละเอียดชุดข้อมูลตามขอบเขตที่กำหนด และแจ้งหน่วยงานที่รับผิดชอบในการนำเข้าบัญชีชุดข้อมูล (Data Catalog)

1.5) เกณฑ์การประเมินชั้นความลับของชุดข้อมูล (Scoring Data Classification Guideline) แสดงดังตารางด้านล่าง



รูปที่ 3 แผนผังการตัดสินใจจำแนกหมวดหมู่ข้อมูล

ตารางที่ 2.4 เกณฑ์การประเมินชั้นความลับของชุดข้อมูลด้านผลกระทบต่อองค์กร

ด้าน	ระดับผลกระทบ	คะแนน	คำอธิบาย
Business Aspect (ด้านธุรกิจ)	Low (น้อยมาก)	1	มีผลกระทบต่อกระบวนการดำเนินงานทำให้การดำเนินงานหยุดชะงักไม่เกิน 6 ชม.
	Rather Low (น้อย)	2	มีผลกระทบต่อกระบวนการดำเนินงาน ทำให้ การดำเนินงานหยุดชะงักมากกว่า 6 ชม. แต่ไม่เกิน 12 ชม.
	Moderate (ปานกลาง)	3	มีผลกระทบต่อกระบวน การดำเนินงาน ทำให้การดำเนินงานหยุดชะงักมากกว่า 12 ชม. แต่ไม่เกิน 24 ชม.
	Rather High (สูง)	4	มีผลกระทบต่อกระบวน การดำเนินงาน ทำให้การดำเนินงานหยุดชะงักมากกว่า 24 ชม. แต่ไม่เกิน 48 ชม.
	High (สูงสุด)	5	มีผลกระทบต่อกระบวนการดำเนินงาน ทำให้การดำเนินงานหยุดชะงักมากกว่า 48 ชม.
Financial Aspect (ด้านการเงิน)	Low (น้อยมาก)	1	น้อยกว่า / เท่ากับ 5 ล้านบาท
	Rather Low (น้อย)	2	มากกว่า 5 ล้านบาท แต่ไม่เกิน 10 ล้านบาท
	Moderate (ปานกลาง)	3	มากกว่า 10 ล้านบาท แต่ไม่เกิน 100 ล้านบาท
	Rather High (สูง)	4	มากกว่า 100 ล้านบาท แต่ไม่เกิน 300 ล้านบาท
	High (สูงสุด)	5	300 ล้านบาทขึ้นไป
Reputation Aspect (ด้านชื่อเสียง)	Low (น้อยมาก)	1	เผยแพร่ข่าวในวงจำกัดภายในองค์กร
	Rather Low (น้อย)	2	เผยแพร่ข่าวในวงกว้าง ทั่วทั้งองค์กร
	Moderate (ปานกลาง)	3	เผยแพร่ข่าวในวงกว้างตามสื่อสาธารณะต่าง ๆ ซึ่งสามารถชี้แจงหรือแก้ไขได้ภายใน 3-6 ชม.
	Rather High (สูง)	4	เผยแพร่ข่าวในวงกว้างตามสื่อสาธารณะต่าง ๆ อย่างต่อเนื่อง ซึ่งสามารถชี้แจงหรือแก้ไขได้ภายใน 6-12 ชม.
	High (สูงสุด)	5	มีการพาดหัวข่าวที่รุนแรงตามสื่อ สาธารณะ ต่าง ๆ อย่างต่อเนื่อง ซึ่งสามารถชี้แจงหรือแก้ไขได้เกินกว่า 12 ชม.

ตารางที่ 2.5 เกณฑ์การประเมินชั้นความลับของชุดข้อมูลด้านผลกระทบต่อเจ้าของข้อมูลส่วนบุคคล

ด้าน	ระดับผลกระทบ	คะแนน	คำอธิบาย
Distinguishability (การแยกแยะ)	Low (น้อยมาก)	1	ไม่มีข้อมูลที่สามารถแยกแยะบุคคลได้ (รวมถึงกรณีที่ทำให้ Encryption, Marking หรือแปลงข้อมูลแล้ว)
	Moderate (ปานกลาง)	3	มีข้อมูลที่ต้องนำไปประกอบกับข้อมูลอื่นก่อน จึงจะสามารถแยกแยะบุคคลได้ เช่น ตำแหน่งงาน อายุงาน หรือการเข้าร่วมกิจกรรม
	High (สูงสุด)	5	มีข้อมูลที่แยกแยะบุคคลได้ชัดเจน เช่น ชื่อ-นามสกุล, รูปถ่ายใบหน้า, รหัสนักศึกษา เป็นต้น
Traceability / Location (การติดตาม / ระบุตำแหน่ง)	Low (น้อยมาก)	1	ไม่มีข้อมูลที่ระบุตำแหน่งหรือที่อยู่ของบุคคลได้อย่างชัดเจน เช่น ข้อมูลจังหวัด อำเภอ หรือขอบเขตตำแหน่งที่ไม่ระบุตำแหน่งบุคคลชัดเจน
	Moderate (ปานกลาง)	3	มีข้อมูลที่อยู่บางส่วน แต่ไม่สามารถระบุสถานที่ชัดเจนได้และต้องนำไปประกอบกับข้อมูลอื่นก่อนเพื่อระบุตัวบุคคล (เช่น มีเพียงข้อมูล อำเภอ จังหวัด รหัสไปรษณีย์ แต่ไม่มีเลขที่บ้าน, GPS, Location)
	High (สูงสุด)	5	มีข้อมูลที่ระบุตำแหน่งหรือที่อยู่ได้ชัดเจนที่สามารถระบุตัวบุคคลได้อย่างชัดเจน (เช่น เลขที่บ้านพร้อมอำเภอ, GPS , location)
Personal Asset (บ่งบอกถึงทรัพย์สิน/สถานะทางการเงิน)	Low (น้อยมาก)	1	ไม่มีข้อมูลทางการเงินหรือข้อมูลที่บ่งบอกถึงฐานะได้ และไม่ระบุถึงตัวบุคคลได้อย่างชัดเจน เช่น ช่องทางการชำระเงิน
	Moderate (ปานกลาง)	3	มีข้อมูลที่บ่งบอกฐานะ ทางการเงินได้โดยอ้อมและต้องนำไปประกอบกับข้อมูลอื่นก่อนเพื่อระบุตัวตน เช่น เงินเดือนที่ปรับขึ้น เงินสมทบกองทุน เงินบริจาค
	High (สูงสุด)	5	มีข้อมูลทางการเงินที่อาจถูกนำไปใช้ได้หรือมีข้อมูลแสดงถึงฐานะทางการเงินและระบุตัวบุคคลได้อย่างชัดเจน เช่น เงินเดือน
Sensitive Personal Data (ข้อมูลอ่อนไหว)	Low (น้อยมาก)	1	ไม่มีข้อมูลอ่อนไหว
	Rather Low (น้อย)	2	มีข้อมูลอ่อนไหว มีเหตุผลในการจัดเก็บและไม่ระบุตัวบุคคลได้อย่างชัดเจน
	Moderate (ปานกลาง)	3	มีข้อมูลอ่อนไหวแต่ไม่มีเหตุผลในการจัดเก็บ แต่ไม่สามารถระบุตัวบุคคลได้
	Rather High (สูง)	4	มีข้อมูลอ่อนไหว มีเหตุผลในการจัดเก็บ แต่ต้องนำไปประกอบกับข้อมูลอื่นก่อนเพื่อระบุตัวบุคคลได้
	High (สูงสุด)	5	มีข้อมูลอ่อนไหว ไม่มีเหตุผลในการจัดเก็บ นำไปประกอบกับข้อมูลอื่นก่อนเพื่อระบุตัวบุคคลได้ หรือ สามารถระบุตัวบุคคลได้อย่างชัดเจน

ตารางที่ 2.6 เกณฑ์คะแนนการประเมิน (Scoring Matrix Criteria Data Classification)

หมวดหมู่ข้อมูล	Classification Level	คะแนน (Score Matrix)
ข้อมูลสาธารณะ	เปิดเผย (Open)	1 – 35
ข้อมูลใช้ภายใน	เผยแพร่ภายในองค์กร (Private)	1 – 9
	ลับ (Confidential)	10 – 23
	ลับมาก (Secret)	24 – 35
ข้อมูลส่วนบุคคล	เปิดเผย (Open)	1 – 5
	เผยแพร่ภายในองค์กร (Private)	6 – 17
	ลับ (Confidential)	18 – 23
	ลับมาก (Secret)	24 – 35
ข้อมูลความลับ	เผยแพร่ภายในองค์กร (Private)	1 – 8
	ลับ (Confidential)	9 – 12
	ลับมาก (Secret)	15 – 27
	ลับที่สุด (Top Secret)	28 - 35
ข้อมูลความมั่นคง	ลับที่สุด (Top Secret)	1 - 35

ตารางที่ 2.7 ตัวอย่างการประเมินระดับผลกระทบเพื่อจัดระดับชั้นความลับของข้อมูล

ชื่อชุดข้อมูล	หมวดหมู่ข้อมูล	ผลกระทบต่อองค์กร			ผลกระทบต่อเจ้าของข้อมูลส่วนบุคคล				ระดับชั้นความลับของชุดข้อมูล	ผลรวมของคะแนนผลกระทบ 7 ด้าน	หมายเหตุตรวจสอบกับชั้นความลับหากไม่ตรงให้ปรับแก้ไข
		ด้านธุรกิจ	ด้านการเงิน	ด้านชื่อเสียง	การแยกแยะ	การติดตาม / ระบุตำแหน่ง	บ่งบอกถึงทรัพย์สิน/สถานะทางการเงิน	ข้อมูลอ่อนไหว			
A01	ข้อมูลความมั่นคง	*1*	*1*	*2*	*2*	*2*	*2*	*5*	ลับที่สุด (Top Secret)	*15*	ลับที่สุด (Top Secret)
A02	ข้อมูลส่วนบุคคล	*1*	*1*	*1*	*1*	*1*	*1*	*1*	เผยแพร่ภายในองค์กร (Private)	*7*	ลับมาก (Secret)
A03	ข้อมูลสาธารณะ	*1*	*1*	*1*	*1*	*2*	*2*	*1*	เปิดเผย (Open)	*9*	เปิดเผย (Open)
A04	ข้อมูลสาธารณะ	*1*	*3*	*3*	*3*	*3*	*3*	*3*	เปิดเผย (Open)	*19*	เปิดเผย (Open)
A05	ข้อมูลความลับ	*2*	*3*	*4*	*5*	*1*	*3*	*2*	ลับมาก (Secret)	*20*	ลับมาก (Secret)

1.6) เกณฑ์การประเมินผลกระทบต่อเจ้าของข้อมูลส่วนบุคคล (Scoring Impact to Data Subject) (กรณีหมวดหมู่ข้อมูลส่วนบุคคล) แสดงดังตารางด้านล่าง

ตารางที่ 2.8 ปัจจัยประกอบการประเมินผลกระทบ

ปัจจัยประกอบการประเมินผลกระทบ		
No	ปัจจัย	ตัวอย่างข้อมูล
1	มีข้อมูลที่แบ่งแยกบุคคล หรือสามารถเชื่อมโยงตัวบุคคลได้	ชื่อ-นามสกุล, รูปถ่ายใบหน้า, Digital, ID, วันเดือนปีเกิด, รหัสพนักงาน,ตำแหน่งงาน
2	มีข้อมูลที่ระบุตำแหน่ง ที่อยู่หรือช่องทางการติดต่อเจ้าของข้อมูล	ที่อยู่, หมายเลขโทรศัพท์, เลขที่เอกสาร (ที่สื่อถึงและมีผลกระทบต่อตัวบุคคล เช่น คำสั่งลงโทษทางวินัย การร้องเรียน การเบิกจ่ายค่ารักษาพยาบาล เป็นต้น)
3	มีข้อมูลที่บ่งบอกถึงฐานะทางการเงินทั้งทางตรงและทางอ้อม	การชำระเงิน, เงินประกัน, รายได้, เงินเดือน, ทรัพย์สิน, ข้อมูลบัตรเครดิต
4	มีข้อมูลอ่อนไหว ที่มีผลกระทบปานกลาง	เชื้อชาติ, เผ่าพันธุ์, ศาสนา, ข้อมูลสหภาพแรงงาน รวมถึงข้อมูลโซเชียลมีเดีย ข้อมูลการค้นหา และพฤติกรรมการใช้อินเทอร์เน็ตที่สามารถเชื่อมโยงไปหาข้อมูลดังกล่าวได้
5	มีข้อมูลอ่อนไหว ที่มีผลกระทบรุนแรง	พฤติกรรมทางเพศ, ความเห็นทางการเมือง, ประวัติอาชญากรรม, ข้อมูลสุขภาพ, ความพิการ, ข้อมูลทางพันธุกรรม, ข้อมูลชีวภาพ เช่น ข้อมูลภาพจำลองใบหน้า ข้อมูลจำลองม่านตา หรือ ข้อมูลจำลองลายนิ้วมือ

ตารางที่ 2.9 ผลกระทบต่อเจ้าของข้อมูลส่วนบุคคล

ผลกระทบต่อเจ้าของข้อมูลส่วนบุคคล (Impact to Data Subject)		
ระดับผลกระทบ (Impact level)	**คะแนน (Score Matrix)**	**Definition (TH)**
Low (น้อยมาก)	1	ไม่มีผลกระทบต่อเจ้าของข้อมูล
Rather Low (น้อย)	2	อาจก่อนให้เกิดความรำคาญ ต่อเจ้าของข้อมูล เช่น การนำเสนอประกันหรือบริการโดยที่เจ้าของข้อมูลไม่ได้รับความยินยอมหรือไม่เกี่ยวข้อง
Moderate (ปานกลาง)	3	อาจก่อให้เกิดความเสียหายต่อเจ้าของข้อมูลในด้านการสูญเสียทรัพย์สินความไม่เป็นส่วนตัว ถูกติดตามพฤติกรรม
Rather High (สูง)	4	อาจก่อให้เกิดความไม่ปลอดภัยต่อร่างกาย ความเป็นปกติสุขในการดำรงชีวิตของเจ้าของข้อมูล เช่น ถูกทำร้าย หรือถูกทำให้อับอาย
High (สูงสุด)	5	อาจก่อให้เกิดความเสียหายรุนแรง เช่น สูญเสียความเป็นตัวตนหรือถึงขั้นเสียชีวิต

ตารางที่ 2.10 เกณฑ์คะแนนการกำหนดผลกระทบต่อเจ้าของข้อมูล

ผลกระทบต่อเจ้าของข้อมูลส่วนบุคคล (Impact to data subject)			เงื่อนไข/ ปัจจัยการประเมิน
ระดับผลกระทบ	**คะแนน**	**คำอธิบาย**	**ปัจจัย**
High (สูงสุด)	5	อาจก่อให้เกิดความเสียหายรุนแรง เช่น สูญเสียความเป็นตัวตนหรือถึงขึ้นเสียชีวิต	(5) + (1 หรือ 2)
Rather High (สูง)	4	อาจก่อให้เกิดความไม่ปลอดภัยต่อร่างกาย ความเป็นปกติสุขในการดำรงชีวิตของเจ้าของข้อมูล เช่น ถูกทำร้าย หรือถูกทำให้อับอาย	(4) + (1 หรือ 2)
Moderate (ปานกลาง)	3	อาจก่อให้เกิดความเสียหายต่อเจ้าของข้อมูลในด้านการสูญเสียทรัพย์สินความไม่เป็นส่วนตัว ถูกติดตามพฤติกรรม	(1) + (2 หรือ 3)
Rather Low (น้อย)	2	อาจก่อนให้เกิดความรำคาญ ต่อเจ้าของข้อมูล เช่น การนำเสนอประกันหรือบริการโดยที่เจ้าของข้อมูลไม่ได้รับความยินยอมหรือไม่เกี่ยวข้อง	(1) หรือ (2) หรือ (2+3)
Low (น้อยมาก)	1	ไม่มีผลกระทบต่อเจ้าของข้อมูล	นอกเหนือจากเกณฑ์ข้างต้น ไม่มี (1) และ (2)

ตารางที่ 2.11 ตัวอย่างการประเมินระดับผลกระทบต่อเจ้าของข้อมูล

ชื่อชุดข้อมูล	ปัจจัยประเมินผลกระทบต่อเจ้าของข้อมูล (กรณีเป็นข้อมูลส่วนบุคคล)					ผลกระทบต่อเจ้าของข้อมูล	ระดับผลกระทบต่อเจ้าของข้อมูล	หมายเหตุ ตรวจสอบกับระดับผลกระทบหากไม่ตรงให้ปรับแก้ไข
	1. มีข้อมูลที่แบ่งแยกบุคคล หรือสามารถ เชื่อมโยงถึงตัว บุคคลได้	2. มีข้อมูลที่ระบุตำแหน่งที่อยู่ หรือช่องทางการติดต่อ เจ้าของข้อมูล	3. มีข้อมูลที่บ่งบอกถึงฐานะทางการเงินทั้งทางตรงและทางอ้อม	4. มีข้อมูลอ่อนไหวที่มีผลกระทบปานกลาง	5. มีข้อมูลอ่อนไหวที่มีผลกระทบรุนแรง			
-	✓	✗	✗	✗	✗	2	*Rather Low (น้อย)*	*Rather Low (น้อย)*
-	✓	✓	✗	✗	✗	3	*Moderate (ปานกลาง)*	*Moderate (ปานกลาง)*
-	✓	✗	✓	✓	✗	4	*Rather High (สูง)*	*Rather High (สูง)*
-	✓	✗	✓	✓	✓	5	*High (สูงสุด)*	*High (สูงสุด)*

2) การปรับปรุงหมวดหมู่ของข้อมูลในการแบ่งระดับชั้นความลับ

2.1) หากพบความไม่ถูกต้องหรือไม่เป็นปัจจุบันของหมวดหมู่ของข้อมูลในการแบ่งระดับชั้นความลับ ให้แจ้งให้คณะหัวหน้าบริการข้อมูลทราบทันที

2.2) บริกรข้อมูลเชิงธุรกิจ บริกรข้อมูลเชิงเทคนิคและเจ้าของข้อมูล ร่วมกันตรวจสอบและแก้ไขให้หมวดหมู่ของข้อมูลในการแบ่งระดับชั้นความลับมีความถูกต้อง

2.6 แนวปฏิบัติการแลกเปลี่ยนและเชื่อมโยงข้อมูล

2.6.1 นิยามการแลกเปลี่ยนและเชื่อมโยงข้อมูล

1) ความหมาย

การแลกเปลี่ยนและเชื่อมโยงข้อมูลเป็นกระบวนการที่สำคัญในการสื่อสารและการเชื่อมต่อระบบคอมพิวเตอร์ต่าง ๆ ระหว่างกัน เช่น เครือข่ายคอมพิวเตอร์หรือการเชื่อมต่อผ่านอินเทอร์เน็ต เพื่อแลกเปลี่ยนข้อมูลในรูปแบบต่าง ๆ หลังจากมีการเชื่อมต่อระบบขององค์กรที่แตกต่างกันเข้าด้วยกัน การแลกเปลี่ยนข้อมูล (Data exchange) จึงเกิดขึ้น ซึ่งการแลกเปลี่ยนข้อมูลเป็นกระบวนการที่ใช้ในการส่งหรือรับข้อมูลระหว่างอุปกรณ์หรือระบบคอมพิวเตอร์ที่เชื่อมต่อกันโดยใช้เทคโนโลยี โปรโตคอลหรือรูปแบบที่ถูกกำหนดไว้ การแลกเปลี่ยนและเชื่อมโยงข้อมูลมีบทบาทสำคัญในการเชื่อมต่อและแลกเปลี่ยนข้อมูลระหว่างองค์กร สามารถใช้ในการส่งข้อมูลที่เกี่ยวข้องกับเสียง ภาพ ข้อความ รวมถึงการส่งข้อมูลทางธุรกิจ เช่น การทำธุรกรรมทางการเงิน การส่งข้อมูลอาจอยู่ในรูปแบบไฟล์ หรือ รูปแบบอื่นๆ ตามเทคโนโลยีการส่งหรือรับข้อมูลที่เลือกใช้ เพื่อกำหนดแนวปฏิบัติและมาตรฐานด้านเทคนิคในการแลกเปลี่ยนและเชื่อมโยงข้อมูลดิจิทัลทั้งภายในหน่วยงานและระหว่างหน่วยงานอย่างมีประสิทธิภาพ และก่อให้เกิดประโยชน์ต่อภาคประชาชน ภาครัฐ และภาคเอกชน

2) ข้อกำหนดการเชื่อมโยงและแลกเปลี่ยนข้อมูล

1) การแลกเปลี่ยนและเชื่อมโยงข้อมูลภายในหน่วยงาน กำหนดให้ใช้รูปแบบที่เป็นมาตรฐานเปิด (Open Format) ทั้งในส่วนมาตรฐานข้อมูล เช่น XML และ JSON เป็นต้น มาตรฐานโปรโตคอล สื่อสาร เช่น SOAP, REST หรืออื่น ๆ ที่ได้รับการยอมรับจากมาตรฐานสากล

2) การแลกเปลี่ยนและเชื่อมโยงข้อมูลระหว่าง กปน. กับ หน่วยงานภายนอก ให้ดำเนินการตามมาตรฐานกลางของหน่วยงานหลักที่เป็นผู้รับผิดชอบ หรือตามที่ได้ตกลงกันไว้ใน MOU

3) กำหนดหน้าที่รับผิดชอบให้กับหน่วยงานสำหรับการแลกเปลี่ยนและเชื่อมโยงข้อมูล เช่น ผู้จัดการโครงการเป็นผู้ได้รับมอบหมายให้สร้างระบบสำหรับเการแลกเปลี่ยนและเชื่อมโยงข้อมูล

4) กำหนดขอบเขตสำหรับข้อมูลที่ต้องการแลกเปลี่ยน

- กำหนดแหล่งข้อมูล (Data Source) จากฐานข้อมูล ไฟล์ตารางคำนวณ (spreadsheets) แชร์ไดรฟ์ (Shared Drives) และแอปพลิเคชัน (Application) ให้ชัดเจน

- ชุดข้อมูล (Data set) จากแหล่งข้อมูลสำหรับแลกเปลี่ยน

5) ตรวจสอบความถูกต้องของข้อมูลที่ต้องการแลกเปลี่ยน ระดับชั้นความลับ คำอธิบายข้อมูล และอื่น ๆ ที่เกี่ยวข้อง

6) บันทึกเหตุการณ์ทุกครั้งที่มีการเชื่อมโยงและแลกเปลี่ยนข้อมูลเช่น บุคคล/หน่วยงานที่ส่งหรือรับข้อมูล ข้อมูลที่ได้รับหรือส่งออก วันและเวลา เป็นต้น

7) ปกป้องข้อมูลด้วยมาตรฐานความปลอดภัยที่เหมาะสม

2.6.2 แนวปฏิบัติ

1) การกำหนดความรับผิดชอบ

เจ้าของข้อมูลหรือผู้ที่ได้รับมอบหมาย กำหนดวิธีปฏิบัติและมาตรฐานทางด้านเทคนิคที่จำเป็นต้องใช้เกี่ยวกับการแลกเปลี่ยนและเชื่อมโยงข้อมูลของโครงการในความรับผิดชอบ

2) การดำเนินการแลกเปลี่ยนและเชื่อมโยงข้อมูล

2.1) ผู้ที่ได้รับมอบหมายกำหนดขอบเขตสำหรับข้อมูลที่ต้องการแลกเปลี่ยน

2.2) ผู้ที่ได้รับมอบหมายตรวจสอบคำอธิบายชุดข้อมูลที่จะทำการแลกเปลี่ยนและเชื่อมโยงให้ครบถ้วน ดังนี้

- ตรวจสอบคำอธิบายข้อมูลของชุดข้อมูลที่ต้องการแลกเปลี่ยนว่ามีความครบถ้วนเป็นปัจจุบันและสอดคล้องกับมาตรฐานคำอธิบายข้อมูลของ กปน. หรือตรงความต้องการของหน่วยงานที่ขอใช้ หากคำอธิบายไม่ครบถ้วนตามความต้องการ ทางผู้ที่ได้รับมอบหมายสามารถจัดทำคำอธิบายเพิ่มเติมตามความต้องการของหน่วยงานที่ขอใช้ได้

- ตรวจสอบชั้นความลับข้อมูลว่าอยู่ในระดับชั้นความลับที่สามารถเปิดเผยได้หรือไม่ นั่นคือต้องไม่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ ความมั่นคงของประเทศ ความลับทางราชการ และความเป็นส่วนตัว พร้อมทั้งตรวจสอบสิทธิของหน่วยงานที่สามารถนำข้อมูลไปใช้ได้ตามบทบาทและภารกิจ ตามกฎหมายของหน่วยงานนั้น ๆ ทั้งนี้ให้ปฏิบัติตามบนโยบายและแนวปฏิบัติของการจัดชั้นความลับข้อมูลและนโยบายการเปิดเผยข้อมูล อย่างเคร่งครัด

2.3) ผู้ที่ได้รับมอบหมาย ร่วมกับ กองบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ ฝ่ายโครงสร้างพื้นฐานเทคโนโลยีดิจิทัล กำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัยเกี่ยวกับการแลกเปลี่ยนและเชื่อมโยงข้อมูลเพื่อป้องกันมิให้มีการรับส่งข้อมูลที่ไม่สมบูรณ์ ส่งข้อมูลไปผิดที่ มีการรั่วไหลของข้อมูล ข้อมูลถูกแก้ไขเปลี่ยนแปลง ถูกทำซ้ำใหม่ หรือถูกส่งซ้ำโดยมิได้รับอนุญาต

2.4) ผู้ที่ได้รับมอบหมาย ร่วมกับ กองบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ ฝ่ายโครงสร้างพื้นฐานเทคโนโลยีดิจิทัล กำหนดให้ต้องจัดเก็บบันทึกหลักฐานของการแลกเปลี่ยนและเชื่อมโยงข้อมูล เพื่อใช้ตรวจสอบสิ่งผิดปกติต่าง ๆ ที่เกิดขึ้น

2.5) ผู้ที่ได้รับมอบหมาย ร่วมกับ กองบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ ฝ่ายโครงสร้างพื้นฐานเทคโนโลยีดิจิทัล ดำเนินการเปิดให้มีการเชื่อมต่อและแลกเปลี่ยนข้อมูล ทั้งนี้ห้ามมิให้มีการแลกเปลี่ยนและเชื่อมโยงข้อมูล ที่ผิดจากข้อตกลง มาตรฐานหรือกฎหมาย

3) การปรับเปลี่ยนแก้ไขการแลกเปลี่ยนและเชื่อมโยงข้อมูล

3.1) หากการรับส่งข้อมูลที่ไม่สมบูรณ์หรือไม่เป็นปัจจุบัน ให้แจ้งเจ้าของข้อมูล ผู้ดูแลระบบบริกรข้อมูลเชิงธุรกิจ บริกรข้อมูลเชิงเทคนิค หรือกองบริหารและจัดการข้อมูล ฝ่ายยุทธศาสตร์และนวัตกรรมดิจิทัล ทำการปรับปรุงให้เป็นปัจจุบัน

3.2) หากตรวจพบว่าข้อมูลที่แลกเปลี่ยนไม่ตรงตามระดับชั้นความลับ ส่งข้อมูลไปผิดที่ มีการรั่วไหลของข้อมูล มีการแก้ไขเปลี่ยนแปลง ถูกทำซ้ำใหม่ ถูกส่งซ้ำโดยมิได้รับอนุญาต ตรวจพบสิ่งผิดปกติ ให้หยุดการเชื่อมต่อและแลกเปลี่ยนข้อมูลชั่วคราวทันที และแจ้งแก่เจ้าของข้อมูล ผู้ที่ได้รับมอบหมาย และกองบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ ฝ่ายโครงสร้างพื้นฐานเทคโนโลยีดิจิทัลทันทีเพื่อร่วมกันตรวจสอบความถูกต้อง

3.3) หากตรวจพบการกระทำการใดๆ ในข้อ 3.2) หรือการกระทำที่ขัดต่อ MOU ในการแลกเปลี่ยนและเชื่อมโยงข้อมูล ให้รีบแจ้งกองบริหารและจัดการข้อมูล ฝ่ายยุทธศาสตร์และนวัตกรรมดิจิทัล เพื่อรายงานต่อคณะกรรมการธรรมาภิบาลข้อมูล เพื่อที่จะได้ตรวจสอบและระงับการบริการเชื่อมต่อและแลกเปลี่ยนข้อมูลชั่วคราวหรือถาวร ต่อไป

4) การพิจารณาและสอบทาน

4.1) เจ้าของข้อมูลและ/หรือผู้ที่ได้รับมอบหมายมีการตรวจสอบข้อมูลที่เชื่อมต่อและแลกเปลี่ยนระหว่างหน่วยงานทั้งภายในและภายนอกหน่วยงาน ว่ามีความถูกต้อง ปลอดภัย และ เป็นปัจจุบันอยู่เสมอ

4.2) เจ้าของข้อมูล และ/หรือผู้ที่ได้รับมอบหมาย มีการตรวจสอบกรอบเวลาตามข้อตกลงในการเชื่อมโยงและแลกเปลี่ยนข้อมูลอยู่เสมอ

4.3) จำเป็นต้องบรรจุวาระเกี่ยวกับการทบทวนความสอดคล้องของข้อมูลที่ถูกแลกเปลี่ยน ระดับชั้นความลับข้อมูลและคำอธิบายข้อมูล อย่างน้อยปีละ 1 ครั้ง

4.4) คณะกรรมการธรรมาภิบาลข้อมูล ควรมีการสอบทานนโยบายและแนวปฏิบัติการแลกเปลี่ยนและเชื่อมโยงข้อมูลให้สอดคล้องกับนโยบายกำกับดูและข้อมูลอื่น ๆ และ กฎหมาย อย่างน้อยปีละ 1 ครั้ง

2.7 แนวปฏิบัติการเปิดเผยข้อมูล

2.7.1 นิยามการเปิดเผยข้อมูล

การเปิดเผยข้อมูลเป็นกระบวนการที่ระบบหรือบุคคลให้ข้อมูลทั้งหมดหรือบางส่วน การเปิดเผยข้อมูลรวมถึงการเผยแพร่ข้อมูลบนสื่อสังคมออนไลน์หรือเว็บไซต์ต่างๆ จนถึงการเปิดเผยข้อมูลผ่านทางองค์กรหรือภาครัฐโดยใช้ช่องทางทางการเผยแพร่ต่าง ๆ เช่น การเปิดเผยข้อมูลผ่านการแถลงข่าว การเปิดเผยข้อมูลในรายงาน หรือการเปิดเผยข้อมูลผ่านเว็บไซต์ทางอินเทอร์เน็ต การเปิดเผยข้อมูลอาจมีวัตถุประสงค์หลายประเภท เช่น การเพิ่มความโปร่งใส การสื่อสารข้อมูลในเชิงพาณิชย์ การเผยแพร่ข้อมูลทางการวิชาการ หรือการเปิดเผยข้อมูลเพื่อให้ความรู้แก่สาธารณชนทั่วไป การเปิดเผยข้อมูลอาจมีผลกระทบต่อความเป็นส่วนตัว ดังนั้น ควรศึกษากฎหมายและนโยบายที่เกี่ยวข้องกับการเปิดเผยข้อมูล เพื่อรักษาความเป็นส่วนตัวและความปลอดภัยของข้อมูล และความเป็นเจ้าของข้อมูล อาทิ

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

2.7.2 แนวปฏิบัติ

กระบวนการและระเบียบวิธีปฏิบัติการเปิดเผยข้อมูล มีดังนี้

1) การกำหนดความรับผิดชอบ

1.1) เจ้าของข้อมูลจะต้องเปิดเผยข้อมูลในความรับผิดชอบต่อสาธารณะตามนโยบายธรรมาภิบาลข้อมูลของ กปน. และ ไม่ขัดต่อกฎหมายว่าด้วยข้อมูลข่าวสารของราชการ และมาตรฐานและหลักเกณฑ์การเปิดเผยข้อมูลเปิดภาครัฐในรูปแบบข้อมูลดิจิทัลต่อสาธารณะ

1.2) เจ้าของข้อมูลห้ามเปิดเผยข้อมูลความมั่นคงและข้อมูลความลับทางราชการที่อยู่ในความครอบครอง ของหน่วยงานรวมทั้งห้ามเปิดเผยข้อมูลที่เป็นการกระทำความผิดตามกฎหมาย นโยบายและแนวปฏิบัติอันทำให้เกิดความเสียหายต่อหน่วยงาน

2) การดำเนินการเปิดเผยข้อมูลในความรับผิดชอบในรูปแบบข้อมูลเปิดของหน่วยงานโดย ดำเนินการดังนี้

2.1) เจ้าของข้อมูลทำการเปิดเผยข้อมูลกำหนดลักษณะของข้อมูลที่เผยแพร่กำหนดให้อยู่ในรูปแบบที่เครื่องสามารถประมวลผลได้

2.2) เจ้าของข้อมูลหรือผู้ที่ได้รับมอบหมาย กำหนดให้มีคำอธิบายข้อมูลหรือเมทาดาตาสำหรับข้อมูลที่ต้องเปิดเผย โดยสามารถปฏิบัติตามนโยบาย แนวปฏิบัติ และ มาตรฐานของการจัดการคำอธิบายข้อมูล เช่น การกำหนดรายละเอียดข้อมูล วัตถุประสงค์ ประเภทข้อมูล เงื่อนไขสัญญาการนำไปใช้และอื่น ๆ

2.3) สำหรับข้อมูลเปิดเผยสู่สาธารณะ เจ้าของข้อมูลหรือผู้ที่ได้รับมอบหมาย ร่วมกับบริกรข้อมูลเชิงธุรกิจและบริกรข้อมูลเชิงเทคนิค ตรวจสอบระดับชั้นความลับว่าอยู่ในหมวดหมู่ข้อมูลสาธารณะ และเผยแพร่ข้อมูลที่ศูนย์กลางข้อมูลเปิดภาครัฐ (Government Open Data) ผ่านเว็บไซต์ data.go.th

2.4) หัวหน้าบริกรข้อมูลตรวจสอบมาตรการรักษาความมั่นคงปลอดภัยในการเปิดเผยข้อมูลที่กำหนดระดับชั้นข้อมูลอย่างเพียงพอและมีประสิทธิภาพ

2.5) หากการเปิดเผยนั้นเป็นการเปิดเผยบนช่องทางที่ดูแลรับผิดชอบโดยหน่วยงานอื่นให้ปฏิบัติตาม เอกสาร คู่มือ การนำข้อมูลขึ้นเผยแพร่ของหน่วยงานนั้น

3) การปรับเปลี่ยนแก้ไขการเปิดเผยข้อมูล

3.1) หากการเปิดเผยข้อมูลไม่ครบถ้วน หรือไม่เป็นปัจจุบัน ให้แจ้งเจ้าของข้อมูล บริกรข้อมูลเชิงธุรกิจ บริกรข้อมูลเชิงเทคนิค และกองบริหารและจัดการข้อมูล ฝ่ายยุทธศาสตร์และนวัตกรรมดิจิทัลปรับปรุงให้เป็นปัจจุบัน

3.2) หากข้อมูลที่เปิดเผย ไม่ตรงตามระดับชั้นความลับข้อมูล ให้หยุดการเปิดเผยข้อมูลชั่วคราวทันที และแจ้งแก่ เจ้าของข้อมูลและหัวหน้าบริกรข้อมูลทันที เพื่อทำการตรวจสอบความถูกต้อง

4) การพิจารณาและสอบทาน

4.1) ให้มีการตรวจสอบข้อมูลที่เผยแพร่สู่สาธารณะ เพื่อให้มั่นใจว่าหน่วยงานมีข้อมูลที่เผยแพร่ที่มีคุณภาพ

4.2) ให้มีการตรวจสอบรูปแบบข้อมูลที่เผยแพร่ให้สอดคล้องกับมาตรฐานที่หน่วยงานกำหนดอยู่เสมอ

4.3) เจ้าของข้อมูลต้องกำหนดรอบระยะเวลาในการตรวจสอบและปรับปรุงข้อมูลที่เปิดเผยเพื่อให้ข้อมูลถูกต้อง และเป็นปัจจุบัน

4.4) ให้มีการสอบทานนโยบายและแนวปฏิบัติการเปิดเผยข้อมูลให้สอดคล้องกับนโยบายกำกับดูและข้อมูลอื่น ๆ และกฎหมาย อย่างน้อยปีละ 1 ครั้ง

ส่วนที่ 3 แนวทางการประเมินการกำกับดูแลข้อมูลและการวัดความคุ้ม

3.1 หลักเกณฑ์ในการกำกับดูแลข้อมูลของ สคร.

การประเมินผลการดำเนินงานรัฐวิสาหกิจตามระบบประเมินผล (SE-AM) หัวข้อ “การดำเนินการด้านการกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร” (Data Governance and Big Data Management Implementation) กำหนดไว้ว่าการกำกับดูแลต้องครอบคลุมถึง กระบวนการกำกับดูแลข้อมูล โครงสร้างการกำกับดูแลข้อมูล นโยบายข้อมูลและการตรวจสอบ การวัดประสิทธิภาพกระบวนการและคุณภาพข้อมูล การวัดความคุ้มทุนและการปรับปรุงอย่างต่อเนื่อง โดยแนวทางการดำเนินงานดังกล่าวมีลักษณะเป็นระดับวุฒิภาวะ (Maturity Level) ดังนี้

ตารางที่ 3.1 ระดับการกำกับดูแลข้อมูลของรัฐวิสาหกิจ

ระดับที่	แนวทางการประเมิน
1	เริ่มมีแนวทางในการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร
2	มีกระบวนการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร ประกอบด้วย ● กระบวนการกำกับดูแลข้อมูลที่เป็นมาตรฐานหน่วยงาน ● โครงสร้างการกำกับดูแลข้อมูลที่ชัดเจน มีส่วนงานกลางในการกำกับดูแลซึ่งประกอบไปด้วยบุคคลด้านธุรกิจและไอที ● นโยบายข้อมูลและการตรวจสอบบังคับใช้ทั้งหน่วยงาน ● การวัดประสิทธิภาพกระบวนการและคุณภาพข้อมูล ● การวัดความคุ้มทุนและการปรับปรุงอย่างต่อเนื่อง
3	มีการถ่ายทอดกระบวนการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กรแก่ผู้มีส่วนได้ส่วนเสียที่สำคัญที่เกี่ยวข้องกับกระบวนการอย่างครบถ้วน โดยมีการแสดงการวิเคราะห์ที่ชัดเจนและมีการประเมินการรับรู้ของผู้มีส่วนได้ส่วนเสียที่สำคัญที่เกี่ยวข้องกับกระบวนการอย่างครบถ้วน รวมทั้งแสดงให้เห็นถึงแนวทางการนำกระบวนการไปปฏิบัติที่ชัดเจนเป็นรูปธรรม
4	มีการกำหนดการวัด ติดตาม วิเคราะห์ประเมิน ตัววัดผลลัพธ์ (Outcome) ของกระบวนการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร
5	มีการกำหนดการวัด ติดตาม วิเคราะห์ประเมิน ตัววัดผลลัพธ์ (Outcome) ของกระบวนการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร และมีการนำผลลัพธ์ที่สำคัญของกระบวนการ เข้าสู่กระบวนการทบทวน การกำกับดูแลด้านการบริหารจัดการดิจิทัล /จัดทำแผนปฏิบัติการดิจิทัลขององค์กร (ระยะยาว) มีการนำผลที่ได้จากการประเมินไปเรียนรู้ และจัดการความรู้ เพื่อนำไปปรับปรุงและทำนวัตกรรม โดยมีการจัดเก็บความรู้และนวัตกรรมที่ได้ลงระบบดิจิทัล

ทั้งนี้ การดำเนินงานตามระดับวุฒิภาวะดังกล่าว จะต้องดำเนินการตามกิจกรรมต่าง ๆ ที่กำหนดไว้ในแต่ละระดับให้ครบถ้วน จึงจะสามารถผ่านเกณฑ์การประเมินในแต่ละระดับที่กำหนดไว้ จากนั้นจึงเข้าสู่การประเมินในระดับถัดไป ไม่สามารถประเมินข้ามระดับได้

3.2 การวัดประสิทธิภาพกระบวนการจัดทำธรรมาภิบาลข้อมูล

ในการวัดประสิทธิภาพกระบวนการจัดทำธรรมาภิบาลข้อมูล ใช้แบบประเมินความพร้อมการจัดทำธรรมาภิบาลข้อมูลซึ่งประยุกต์จากหลักเกณฑ์ของการกำกับดูแลข้อมูลภาครัฐ (Data Governance และ DAMA-DMBOK โดยให้สามารถวัดและประเมินได้สะดวกและสอดคล้องกับแนวทางปฏิบัติการกำกับดูแลข้อมูลของ กปน. โดยได้จัดทำเป็นตารางและมีหัวข้อประเมิน ได้แก่

1. โครงสร้างธรรมาภิบาลข้อมูล
2. กระบวนการธรรมาภิบาลข้อมูล
3. นโยบายข้อมูลและการติดตามตรวจสอบ
4. การประเมินคุณภาพข้อมูล
5. การประเมินความมั่นคงปลอดภัยข้อมูล
6. การปรับปรุงกระบวนการธรรมภิบาลข้อมูลอย่างต่อเนื่อง

โดยรูปด้านล่าง อธิบายระดับการให้คะแนนความพร้อมการจัดทำธรรมาภิบาลข้อมูล

ระดับความพร้อมของธรรมาภิบาลข้อมูลภาครัฐ

ระดับ	1 โครงสร้างธรรมาภิบาลข้อมูลภาครัฐ	2 กระบวนการธรรมาภิบาลข้อมูลภาครัฐ	3 นโยบายข้อมูลและการตรวจสอบ	4 – 5 การประเมินคุณภาพข้อมูลและความมั่นคงปลอดภัย	6 การปรับปรุงอย่างต่อเนื่อง
0 : None	ไม่มีหรือมีแต่ไม่เป็นทางการ	ไม่มีหรือมีแต่ไม่เป็นทางการ	ไม่มีหรือมีแต่ไม่เป็นทางการ	ไม่มีหรือมีแต่ไม่เป็นทางการ	ไม่มีหรือมีแต่ไม่เป็นทางการ
1 : Initial	มีการกำหนดผู้กำกับดูแลอย่างไม่เป็นทางการ	กระบวนการยังไม่เป็นมาตรฐาน	ไม่มีหรือมีแต่ไม่เป็นทางการ	ไม่มีหรือมีแต่ไม่เป็นทางการ	ไม่มีหรือมีแต่ไม่เป็นทางการ
2 : Managed	มีการกำหนดผู้กำกับดูแลในแต่ละส่วนงาน/บริการ	มีกระบวนการเป็นมาตรฐานส่วนงาน/ บริการ	บังคับใช้ในส่วนงาน/ บริการ	ไม่มีหรือมีแต่ไม่เป็นทางการ	ไม่มีหรือมีแต่ไม่เป็นทางการ
3 : Standardized	มีส่วนงานกลางในธรรมาภิบาลข้อมูล ซึ่งประกอบไปด้วยบุคคลด้านธุรกิจและเทคโนโลยีสารสนเทศ	มีกระบวนการเป็นมาตรฐานหน่วยงาน	บังคับใช้ทั้งหน่วยงาน	ประเมินคุณภาพข้อมูลหรือความมั่นคงปลอดภัย	ไม่มีหรือมีแต่ไม่เป็นทางการ
4 : Advanced	มีส่วนงานกลางในธรรมาภิบาลข้อมูล ซึ่งประกอบไปด้วยบุคคลด้านธุรกิจและเทคโนโลยีสารสนเทศ	มีกระบวนการเป็นมาตรฐานหน่วยงาน	บังคับใช้ทั้งหน่วยงาน	ประเมินคุณภาพข้อมูลและความมั่นคงปลอดภัย	ไม่มีหรือมีแต่ไม่เป็นทางการ
5 : Optimized	มีส่วนงานกลางในธรรมาภิบาลข้อมูล ซึ่งประกอบไปด้วยบุคคลด้านธุรกิจและเทคโนโลยีสารสนเทศ	มีกระบวนการเป็นมาตรฐานหน่วยงาน	บังคับใช้ทั้งหน่วยงาน	ประเมินคุณภาพข้อมูลและความมั่นคงปลอดภัย	มีการปรับปรุงกระบวนการอย่างต่อเนื่อง

รายละเอียดแบบประเมินสำหรับวัดประสิทธิภาพกระบวนการจัดทำธรรมาภิบาลข้อมูลของ กปน. จะแสดงดังต่อไปนี้

แบบประเมินสำหรับวัดประสิทธิภาพกระบวนการจัดทำธรรมาภิบาลข้อมูลของ กปน.

แบบประเมินสำหรับวัดประสิทธิภาพกระบวนการจัดทำธรรมาภิบาลข้อมูลของ กปน. มีดังนี้

รายการประเมิน	ระดับคะแนน					
	0	1	2	3	4	5
1 โครงสร้างธรรมาภิบาลข้อมูล (โครงสร้างธรรมาภิบาลข้อมูล มีคำสั่งแต่งตั้ง)						
- คณะกรรมการกำกับดูแลข้อมูล (Data Governance Council)						
- คณะทำงานธรรมาภิบาลข้อมูล (Data Steward Team)						
- ผู้มีส่วนได้ส่วนเสียกับข้อมูล (Data Stakeholder)						
2 กระบวนการธรรมาภิบาลข้อมูล (การเตรียมข้อมูล มีการดำเนินการ)						
2.1 นิยามข้อมูล (Data Definition)						
- หมวดหมู่ของข้อมูล (Data Category)						
- ระดับชั้นความลับข้อมูล (Data Classification)						
- คำอธิบายชุดข้อมูลดิจิทัล (Metadata)						
- พจนานุกรมข้อมูล (Data Dictionary)						
2.2 นโยบายข้อมูล (Data Policies)						
- นโยบายการบริหารจัดการวงจรชีวิตข้อมูล						
- นโยบายการบริหารจัดการคำอธิบายข้อมูล (Metadata Management Policy)						
- นโยบายคุณภาพข้อมูล (Data Quality Policy)						
- นโยบายการจัดหมวดหมู่และระดับชั้นความลับข้อมูล (Data Categories and Classification Policy)						
- นโยบายการเชื่อมโยงและแลกเปลี่ยนข้อมูล (Data Exchange Policy)						
- นโยบายการเปิดเผยข้อมูล (Open Data Policy)						
- นโยบายความมั่นคงปลอดภัยและความเป็นส่วนบุคคล (Data Security and Privacy Policy						
2.3 มาตรฐานข้อมูล (Data Standard)						
- แนวปฏิบัติการบริหารจัดการวงจรชีวิตข้อมูล						
- แนวปฏิบัติการบริหารจัดการคำอธิบายข้อมูล						
- แนวปฏิบัติการบริหารจัดการคุณภาพข้อมูล						
- แนวปฏิบัติการจัดหมวดหมู่และระดับชั้นความลับข้อมูล						
- แนวปฏิบัติการแลกเปลี่ยนและเชื่อมโยงข้อมูล						
- แนวปฏิบัติการเปิดเผยข้อมูล						
3 นโยบายข้อมูลและการติดตามตรวจสอบ						
3.1 การเตรียมการเชื่อมโยงข้อมูล มีการดำเนินการ						
- จัดทำชุดข้อมูล						
- จัดทำเมทาดาตา						

รายการประเมิน	ระดับคะแนน					
	0	1	2	3	4	5
- บันทึกชุดข้อมูล/ดัชนีข้อมูลลงในระบบบัญชีข้อมูล						
- จัดทำ API ชุดข้อมูลสำหรับการให้บริการ						
3.2 การเชื่อมโยง มีการดำเนินการ						
- จัดทำข้อตกลงการให้บริการข้อมูล						
- ให้บริการเว็บเซอร์วิช						
4-5 การประเมินคุณภาพข้อมูล และการประเมินความมั่นคงปลอดภัยข้อมูล						
- การกำหนดเป้าหมายของการประเมินคุณภาพข้อมูลในแต่ละครั้ง						
- การกำหนดผู้ใช้งานและบทบาทการใช้งานข้อมูล						
- การกำหนดความเสี่ยงที่เกี่ยวข้องกับข้อมูลที่ประเมินและผลกระทบที่อาจเกิดขึ้นต่อองค์กร						
- การจัดลำดับความสำคัญของประเด็นความเสี่ยงที่พบ						
6 การปรับปรุงกระบวนการ DG อย่างต่อเนื่อง						
- การนำผลประเมินมาวิเคราะห์หาสาเหตุและผลกระทบที่มีต่อองค์กร						
- การบริหารการเปลี่ยนแปลงความต้องการที่เกี่ยวข้องกับการกำกับดูแลข้อมูล						
- การทบทวนนโยบายธรรมาภิบาลข้อมูล						

จากแบบประเมินข้างต้น หัวข้อประเมินทั้ง 6 หัวข้อมีเกณฑ์คะแนนในแต่หัวข้อไม่เหมือนกัน แต่มีระดับของคะแนนตั้งแต่ระดับ 0 ถึงระดับที่ 5 ดังนี้

เกณฑ์การประเมิน	หัวข้อการประเมิน				
	1 โครงสร้างธรรมาภิบาลข้อมูล	2 กระบวนการธรรมาภิบาลข้อมูล	3 นโยบายข้อมูลและการติดตามตรวจสอบ	4-5 การประเมินคุณภาพข้อมูล และการประเมินความมั่นคงปลอดภัยข้อมูล	6 การปรับปรุงกระบวนการ DG อย่างต่อเนื่อง
ระดับ 0: None	ไม่มีหรือมีแต่ไม่เป็นทางการ	ไม่มีหรือมีแต่ไม่เป็นทางการ	ไม่มีหรือมีแต่ไม่เป็นทางการ	ไม่มีหรือมีแต่ไม่เป็นทางการ	ไม่มีหรือมีแต่ไม่เป็นทางการ
ระดับ 1: Initial/Ad Hoc	มีการกำหนดผู้กำกับดูแลอย่างไม่เป็นทางการ	กระบวนการยังไม่เป็นมาตรฐาน	มีการใช้นโยบายและการติดตามตรวจสอบแต่ไม่สม่ำเสมอ/ไม่เป็นทางการ	ไม่มีการประเมินด้านคุณภาพข้อมูลและความมั่นคงปลอดภัยข้อมูล	ไม่มีหรือมีแต่ไม่เป็นทางการ
ระดับ 2: Repeatable	เริ่มมีการกำหนดผู้มีหน้าที่กำกับดูแลข้อมูลบางส่วนงาน/บริการ	เริ่มมีการกำหนดกระบวนการกำกับดูแลข้อมูลบางส่วนงาน/บริการ	เริ่มบังคับใช้ในบางส่วนงาน/บริการ	เริ่มมีการสร้างความตระหนักด้านคุณภาพข้อมูลบางส่วนงาน/บริการ	เริ่มมีกระบวนการบริหารความต่อเนื่องในการกำกับดูแลข้อมูลในบางส่วนงาน/บริการ
ระดับ 3: Defined	มีการกำหนดผู้มีหน้าที่กำกับดูแลข้อมูลในทุกส่วนงาน/บริการ	มีการขยายผลการกำหนดกระบวนการกำกับดูแลข้อมูลครอบคลุมทุกส่วนงาน/บริการ	มีนโยบายที่ให้ความสำคัญกับการขับเคลื่อนองค์กรด้วยข้อมูล	มีการประเมินคุณภาพข้อมูล และ ความมั่นคงปลอดภัยข้อมูลครอบคลุมทุกส่วนงาน/บริการ	มีกระบวนการบริหารจัดการความต่อเนื่องในการกำกับดูแลข้อมูลครอบคลุมทุกส่วนงาน/บริการ
ระดับ 4: Managed	มีส่วนงานกลางด้านการกำกับดูแลข้อมูลซึ่งประกอบไปด้วยบุคคลทั้งด้านธุรกิจและไอที	มีกระบวนการบริหารจัดการความเสี่ยงที่เกี่ยวข้องกับข้อมูล	มีหลักเกณฑ์การวัดผลและประเมินผลการบริหารจัดการข้อมูล	มีการปรับปรุงคุณภาพข้อมูลที่สามารถวัดผลได้	มีกระบวนการบริหารจัดการความต่อเนื่องในการกำกับดูแลข้อมูลที่เป็นมาตรฐานขององค์กร
ระดับ 5: Optimized	มีการกำหนดผู้มีหน้าที่กำกับดูแลข้อมูลครอบคลุมทั้งองค์กรอย่างเป็นทางการ	มีการกำหนดกระบวนการกำกับดูแลข้อมูลให้เป็นมาตรฐาน	บังคับใช้ทั้งองค์กร	มีการสร้างความตระหนักด้านคุณภาพข้อมูลและกระบวนการกำกับดูแลข้อมูลครอบคลุมทั้งองค์กร	มีการปรับปรุงกระบวนการที่เกี่ยวข้องกับการกำกับดูแลข้อมูลอย่างต่อเนื่อง

3.3 การวัด ติดตาม วิเคราะห์ประเมิน ตัววัดผลลัพธ์

1. **Output**

ตัวชี้วัดที่ 1	ร้อยละของความสำเร็จของการจัดทำคำอธิบายข้อมูลและเกณฑ์คุณภาพข้อมูล
ผู้ติดตามและวัดผล	กองบริหารและจัดการข้อมูล ฝยท.
วิธีการคำนวณตัวชี้วัด	นับจากจำนวนชุดข้อมูลที่นำมาจัดทำคำอธิบายข้อมูลและเกณฑ์คุณภาพข้อมูลแล้วเสร็จตามเป้าหมาย
ความถี่ในการติดตาม	ปีละ 1 ครั้ง
เป้าหมาย	100 เปอร์เซ็นต์
ตัวชี้วัดที่ 2	ร้อยละจำนวนรายการข้อมูลที่มีการทบทวน
ผู้ติดตามและวัดผล	กองบริหารและจัดการข้อมูล ฝยท.
วิธีการคำนวณตัวชี้วัด	จำนวนคำอธิบายชุดข้อมูล (Metadata) ที่มีการทบทวนให้เป็นปัจจุบัน * 100 / จำนวนคำอธิบายชุดข้อมูล (Metadata) ทั้งหมด
ความถี่ในการติดตาม	ปีละ 1 ครั้ง
เป้าหมาย	80 เปอร์เซ็นต์
ตัวชี้วัดที่ 3	ร้อยละการประเมินคุณภาพของข้อมูล
ผู้ติดตามและวัดผล	กองบริหารและจัดการข้อมูล ฝยท.
วิธีการคำนวณตัวชี้วัด	จำนวนชุดข้อมูลที่มีการประเมินคุณภาพข้อมูล * 100 / จำนวนชุดข้อมูลทั้งหมด
ความถี่ในการติดตาม	ปีละ 1 ครั้ง
เป้าหมาย	80 เปอร์เซ็นต์

หมายเหตุ: Output เป็นการวัดเชิงปริมาณ

2. **Outcome**

ตัวชี้วัดที่ 1	ชุดข้อมูลที่ผ่านกระบวนการธรรมาภิบาลข้อมูล ที่เผยแพร่ผ่านศูนย์กลางข้อมูลเปิดภาครัฐ
ผู้ติดตามและวัดผล	กองบริหารและจัดการข้อมูล ฝยท.
วิธีการคำนวณตัวชี้วัด	จำนวนชุดข้อมูลที่ผ่านกระบวนการธรรมาภิบาลข้อมูล เผยแพร่ที่ศูนย์กลางข้อมูลเปิดภาครัฐ

ความถี่ในการติดตาม	ปีละ 1 ครั้ง
เป้าหมาย	อย่างน้อย 2 ชุดข้อมูล
ตัวชี้วัดที่ 2	ผลการประเมินประสิทธิภาพกระบวนการ (ปีงบประมาณ 2568 เป็นต้นไป)
ผู้ติดตามและวัดผล	กองบริหารและจัดการข้อมูล ฝยท.
วิธีการคำนวณตัวชี้วัด	แบบประเมินสำหรับวัดประสิทธิภาพกระบวนการจัดทำธรรมาภิบาลข้อมูล
ความถี่ในการติดตาม	ปีละ 1 ครั้ง
เป้าหมาย	ระดับ 4
ตัวชี้วัดที่ 3	เปอร์เซ็นต์ความถูกต้องของข้อมูล
ผู้ติดตามและวัดผล	กองบริหารและจัดการข้อมูล ฝยท.
วิธีการคำนวณตัวชี้วัด	ตรวจสอบตามเกณฑ์คุณภาพข้อมูล ต้องไม่ต่ำกว่าเกณฑ์ที่เจ้าของข้อมูลกำหนด และชุดข้อมูลที่ผ่านเกณฑ์ต้องไม่ต่ำกว่าร้อยละ 80 ของชุดข้อมูลทั้งหมดที่จัดทำในปีงบประมาณ
ความถี่ในการติดตาม	ปีละ 1 ครั้ง
เป้าหมาย	80 เปอร์เซ็นต์
ตัวชี้วัดที่ 4	ความสำเร็จของการจัดทำรายงานผลประโยชน์ที่ได้รับจากการจัดทำ Data Governance
ผู้ติดตามและวัดผล	กองบริหารและจัดการข้อมูล ฝยท.
วิธีการคำนวณตัวชี้วัด	รายงานผลประโยชน์ที่เป็นตัวเงินหรือไม่อยู่ในรูปตัวเงินที่ได้รับจากการจัดทำ Data Governance
ความถี่ในการติดตาม	ปีละ 1 ครั้ง
เป้าหมาย	100 เปอร์เซ็นต์

หมายเหตุ: Outcome เป็นการวัดเชิงคุณภาพ

3.4 แนวทางการวัดความคุ้มทุน

ความคุ้มทุนของการดำเนินงานด้านธรรมาภิบาลข้อมูลเป็นกระบวนการที่ช่วยประเมินผลตอบแทนที่ได้รับจากการดำเนินงานธรรมาภิบาลข้อมูลในองค์กร หรือการดำเนินการที่เกี่ยวข้องกับข้อมูล โดยคำนึงถึงมิติทางเศรษฐศาสตร์และสังคมที่เกี่ยวข้องกับการจัดการข้อมูลอย่างสมเหตุสมผล เป็นการเปรียบเทียบผลประโยชน์ที่ได้รับและต้นทุนของการดำเนินงานด้านการกำกับดูแลข้อมูล หากผลประโยชน์ที่ได้รับมีค่า

เท่ากับต้นทุนในการดำเนินงานจะถือเป็นจุดคุ้มทุนทางด้านการเงิน สะท้อนให้เห็นถึงความคุ้มค่าในการลงทุนกับการดำเนินงานดังกล่าว โดยผลประโยชน์การดำเนินงานด้านการกำกับดูแลข้อมูล สามารถแบ่งออกเป็น 2 ประเภท ได้แก่

1) ผลประโยชน์ทางตรงและทางอ้อมในรูปตัวเงิน คือ ผลประโยชน์ที่เกิดขึ้นโดยทางตรงและทางอ้อมจากการดำเนินงานด้านธรรมาภิบาลข้อมูล ที่สามารถคำนวณเป็นตัวเงินได้อาทิงบประมาณที่องค์กรใช้ในการลงทุน รายได้ที่สูงขึ้นขององค์กร ต้นทุนค่าดำเนินการขององค์กรที่ลดลง เป็นต้น

2) ผลประโยชน์ทางอ้อมที่ประเมินเป็นตัวเงินไม่ได้คือ ผลประโยชน์ที่มิได้เกิดขึ้นโดยทางตรงจากการดำเนินงานด้านธรรมาภิบาลข้อมูลแต่เป็นผลกระทบต่อเนื่องจากการดำเนินงานด้านธรรมาภิบาลข้อมูลที่ไม่สามารถคำนวณเป็นตัวเงิน เช่น จำนวนหน่วยงานที่นำข้อมูลเปิดขององค์กรไปใช้เพิ่มขึ้น ความปลอดภัยของข้อมูลที่เพิ่มสูงขึ้น ความพึงพอใจในการบริการข้อมูลที่มีคุณภาพต่อ ลูกค้า/ประชาชน เป็นต้น

กระบวนการวัดความคุ้มทุนด้านธรรมาภิบาลข้อมูลแบ่งเป็นขั้นตอน ดังนี้:

1. การระบุและเข้าใจมิติของความคุ้มค่า โดยระบุมิติหลักของความคุ้มค่าที่เกี่ยวข้อง เช่น การสร้างความเชื่อมั่นให้ผู้ใช้ข้อมูล เพิ่มความปลอดภัยของข้อมูล สร้างภาพลักษณ์ที่ดีให้กับองค์กร การลดค่าใช้จ่าย เป็นต้น

2. การกำหนดตัวชี้วัด: การกำหนดตัวชี้วัดที่เกี่ยวข้องกับมิติที่ระบุ เช่น ระดับความพึงพอใจของผู้ใช้ข้อมูล คุณภาพของข้อมูล การลดต้นทุนในการดำเนินการ การสร้างโอกาสในการหารายได้จากข้อมูล เป็นต้น

3. การเก็บข้อมูล: เก็บข้อมูลเกี่ยวกับตัวชี้วัดที่กำหนดขึ้น อาจเป็นการสำรวจความพึงพอใจของผู้ใช้ข้อมูล การรวบรวมข้อมูลอื่น ๆ ที่สามารถนำมาวิเคราะห์และประเมินได้

4. การวิเคราะห์ข้อมูล: วิเคราะห์ข้อมูลที่เก็บรวบรวมมา เพื่อหาความสัมพันธ์ระหว่างตัวชี้วัดและผลตอบแทนที่เกี่ยวข้องกับธรรมาภิบาลข้อมูล โดยคำนึงถึงทั้งเรื่องค่าใช้จ่าย ผลประโยชน์ที่จะได้รับ ความสัมพันธ์นี้อาจเป็นให้ผลเป็นเชิงบวกหรือเชิงลบ

5. การประเมินผลตอบแทน: จากการวิเคราะห์ข้อมูล สามารถประเมินผลตอบแทนที่ได้รับจากการดำเนินการที่เกี่ยวข้องกับธรรมาภิบาลข้อมูล อาจเป็นผลตอบแทนทางเศรษฐศาสตร์ที่สามารถคิดออกมาเป็นตัวเงิน เช่น การลดค่าใช้จ่ายในการดำเนินงาน หรือผลตอบแทนทางสังคมที่เป็นผลตอบแทนที่ไม่ใช่ตัวเงิน เช่น ระดับความพึงพอใจของผู้ใชข้อมูลที่เพิ่มขึ้น

6. การปรับปรุงและการดำเนินการ คือการใช้ข้อมูลและข้อเสนอแนะที่ได้รับจากการประเมินผลตอบแทนเพื่อปรับปรุงการดำเนินงานในด้านธรรมาภิบาลข้อมูล อาจเป็นการปรับปรุงนโยบายธรรมาภิบาลข้อมูล หรือการปรับปรุงกระบวนการจัดการข้อมูล

การวัดความคุ้มค่าด้านธรรมาภิบาลข้อมูลเป็นการช่วยให้องค์กรมีการจัดการข้อมูลอย่างมีประสิทธิภาพและสอดคล้องกับมาตรฐานของความสามารถในด้านธรรมาภิบาลข้อมูล รวมทั้งตอบสนองให้เป็นไปตามความคาดหวังของผู้ใช้ข้อมูล นอกจากนี้ยังช่วยเสริมสร้างภาพลักษณ์ขององค์กรและมีผลการดำเนินงานที่สอดคล้องตามนโยบายภาครัฐในเรื่องธรรมาภิบาลข้อมูล

ส่วนที่ 4 ภาคผนวก

ตัวอย่างแบบฟอร์ม

(แบบฟอร์มเปล่า)

* สามารถดาวน์โหลดเอกสารได้ที่ เว็บไซต์ MWA Data Governance

Template รายการชุดข้อมูล **(List of Data)**

รหัส Data Domain	รหัส Data Set	ชื่อ Data	คำอธิบาย Data	ผู้นำเข้าข้อมูล (Data Creator)	ผู้ใช้ข้อมูล (Data User)	เจ้าของข้อมูล (Data Owner)	กระบวนการทำงาน			ประเภทข้อมูล			ระบบสารสนเทศ	ความสอดคล้องกับ Domain ตาม IWA							
							Level 1	Level 2	Level 3	แบบมีโครงสร้าง	แบบกึ่งโครงสร้าง	แบบไม่มีโครงสร้าง		DD01 ข้อมูลปริมาณน้ำ (Water Volume Data)	DD02 ข้อมูลบุคลากร (Personnel Data)	DD03 ข้อมูลสินทรัพย์ (Physical asset data)	DD04 ข้อมูลปฏิบัติงานและการซ่อมบำรุง (Operational and Maintenance data)	DD05 ข้อมูลลูกค้า (Demography and customer data)	DD06 ข้อมูลการให้บริการ (Quality of service data)	DD07 ข้อมูลสินค้าบริการและการเงิน (Economic and financial data)	DD08 ข้อมูลเวลา (Time data)

หมายเหตุ : * อ้างอิงตามสถาปัตยกรรมองค์กร กปน. (MWA EA)

Template คำอธิบายข้อมูลเชิงธุรกิจ **(Business Metadata Form)**

Data Set ID	Data Set	Data Set Description	PURPOSE	Data Domain	Data Type	DATA OWNER	DATA OWNER PHONE NUMBER	UPDATE FREQUENCY	UPDATE FREQUENCY UNIT	STATUS	UPDATED DATE	UPDATED BY	APPROVED DATE	APPROVED BY	Tags	ชั้นความลับ	ขอบเขตเชิงภูมิศาสตร์หรือเชิงพื้นที่	แหล่งที่มา	สัญญาอนุญาตให้ใช้ข้อมูล	รูปแบบการจัดเก็บข้อมูล	หมายเหตุ

หมายเหตุ : * สามารถดาวน์โหลด Template ได้ที่ เว็บไซต์ MWA Data Governance

Template คำอธิบายข้อมูลเชิงธุรกิจ **(Business Term Form)**

BUSINESS TERM	THAI DESCRIPTION	ENGLISH DESCRIPTION	DATA DOMAIN	STATUS	UPDATED DATE	UPDATED BY	APPROVED DATE	APPROVED BY

Template คำอธิบายข้อมูลเชิงเทคนิค **(Application Form)**

System name	System thai description	Application name	Application thai description	Server name	Application owner e-mail	Application owner phone number	Application owner team	Operation support e-mail	Operation support phone number	Operation support team	Application status

Template คำอธิบายข้อมูลเชิงเทคนิค **(Table Form)**

Database type	Database software	db version	Table name	Thai table description	Purpose of table	Table type	Data Classification level	Declassification	Table status	Table created date	Table created by	Table updated date	Table updated by	Table owner team

Template คำอธิบายข้อมูลเชิงเทคนิค **(Attribute Form)**

Database name	Table name	Attribute name	Thai description	Datatype	Example	Is referenced?	Is Primary Key	Is Foreign Key	Is Required	Attribute status	Remark

Template แนวทางการตรวจสอบคุณภาพข้อมูล

ชุดข้อมูล	รายการ	มิติคุณภาพข้อมูล	เงื่อนไขทางธุรกิจ (Business Rule)	ระดับเกณฑ์คุณภาพ	ผลลัพธ์	หมายเหตุ
		ความถูกต้อง				
		ความครบถ้วน				
		ความสอดคล้องกัน				
		ความทันสมัย				
		ตรงตามความต้องการของผู้ใช้				
		ความพร้อมใช้				
		ความถูกต้อง				
		ความครบถ้วน				
		ความสอดคล้องกัน				
		ความทันสมัย				
		ตรงตามความต้องการของผู้ใช้				
		ความพร้อมใช้				
		ความถูกต้อง				
		ความครบถ้วน				
		ความสอดคล้องกัน				
		ความทันสมัย				
		ตรงตามความต้องการของผู้ใช้				
		ความพร้อมใช้				

ประวัติการแก้ไขเอกสาร

เวอร์ชั่น	ผู้จัดทำ	ผู้อนุมัติ	วันที่แก้ไขข้อมูล	รายละเอียดแก้ไข
1.1	คณะหัวหน้าบริกรข้อมูล	คณะกรรมการธรรมาภิบาลข้อมูล	31 ส.ค. 2566	เวอร์ชันเริ่มต้น
1.2	คณะหัวหน้าบริกรข้อมูล	คณะกรรมการธรรมาภิบาลข้อมูล	29 ส.ค. 2567	1.เพิ่มเติมแนวปฏิบัติการบริหารและจัดการวงจรชีวิตข้อมูล 2.เพิ่มเติมและแก้ไขแนวปฏิบัติการจัดหมวดหมู่และระดับชั้นความลับข้อมูล 3.เพิ่มเติมการวัดประสิทธิภาพกระบวนการจัดทำธรรมาภิบาลข้อมูล และแก้ไข Output และ Outcome