



International Institute for
Trade and Development

นโยบายและแนวทางปฏิบัติธรรมาภิบาลข้อมูลภาครัฐ
สถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน)

งานสารสนเทศ
สำนักยุทธศาสตร์และสารสนเทศ
ปี ๒๕๖๙

นโยบายธรรมาภิบาลข้อมูลภาครัฐ สถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน)

๑. หลักการ

ด้วยรัฐบาลได้ให้ความสำคัญกับการบริหารจัดการข้อมูล เพื่อให้การปฏิบัติงานภายในหน่วยงานรัฐ และการแลกเปลี่ยนข้อมูลระหว่างหน่วยงานดำเนินการได้อย่างมีประสิทธิภาพ อันนำไปสู่การยกระดับบริการแก่ประชาชนและภาคธุรกิจได้อย่างแท้จริง จึงได้กำหนดให้นำหลักการของธรรมาภิบาลข้อมูลภาครัฐ (Data Governance for Government) มาเป็นกลไกในการกำหนดทิศทาง ควบคุม และทบทวนสอบการบริหารจัดการข้อมูลอย่างเป็นระบบบนพื้นฐานความมั่นคงปลอดภัยและควมมีคุณภาพของข้อมูล เพื่อให้ได้มาและการนำไปใช้ข้อมูลของหน่วยงานภาครัฐถูกต้อง ครบถ้วน เป็นปัจจุบัน รักษาความเป็นส่วนตัว และสามารถเชื่อมโยงกันได้อย่างมีประสิทธิภาพและมั่นคงปลอดภัย

สถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน) เป็นองค์กรที่ไม่แสวงหากำไร จัดตั้งขึ้นภายใต้กฎหมายของรัฐบาลไทยโดยมีสถานะเป็นองค์การมหาชน สถาบันดำเนินงานโดยอาศัยความร่วมมืออย่างใกล้ชิดกับรัฐบาลไทย องค์กรต่าง ประเทศอื่น ๆ และองค์กรระดับภูมิภาค และหน่วยงานอื่น ๆ ของรัฐ และภารกิจเกี่ยวกับประชาชน ซึ่งในการดำเนินงานตามภารกิจต่าง ๆ นั้น มีข้อมูลที่ถือเป็นทรัพย์สินสำคัญของสถาบัน ซึ่งต้องให้ความสำคัญในการบริหารจัดการข้อมูลภาครัฐทุกขั้นตอนเพื่อให้การได้มาและการนำข้อมูลของหน่วยงานไปใช้อย่างถูกต้อง รวมถึงติดตามการบริหารจัดการข้อมูลให้มีความโปร่งใส ตรวจสอบได้ ส่งผลต่อคุณภาพ ความมั่นคงปลอดภัย และบูรณาการข้อมูลได้อย่างครบถ้วน ถูกต้อง และข้อมูลเป็นปัจจุบัน

เนื่องด้วยสถาบันออกนโยบายและแนวทางปฏิบัติเป็นฉบับเดียวกัน จัดทำ อาศัยอำนาจตามความใน มาตรา ๑๒ แห่งพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ และ ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ ประกาศ ณ วันที่ ๑๒ มีนาคม พ.ศ. ๒๕๖๓ กำหนดให้หน่วยงานของรัฐดำเนินการให้เป็นไปตามธรรมาภิบาลข้อมูลภาครัฐ และจัดทำธรรมาภิบาลข้อมูลภาครัฐ ในระดับหน่วยงานให้สอดคล้องกับธรรมาภิบาลข้อมูลภาครัฐ เพื่อให้การบริหารงานภาครัฐ และการจัดทำบริการสาธารณะเป็นไปด้วยความสะดวก รวดเร็ว มีประสิทธิภาพ และตอบสนองต่อการให้บริการและการอำนวยความสะดวกแก่ประชาชน

ดังนั้น เพื่อให้สถาบันได้ดำเนินการบริหารจัดการข้อมูลภาครัฐตามกฎหมาย ระเบียบ สถาบันจึงได้จัดทำนโยบายธรรมาภิบาลข้อมูลภาครัฐ สถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน) ฉบับนี้ขึ้น โดยมุ่งหวังให้นโยบายข้อมูลของสถาบันยกระดับให้ข้อมูลทั้งหมดของสถาบันมีการจัดการอย่างมีระบบคุณภาพ มีความมั่นคงปลอดภัย มีความเป็นส่วนบุคคล และเป็นประโยชน์ต่อทุกภาคส่วนบนพื้นฐานของการคุ้มครองข้อมูลและรักษาผลประโยชน์ของประเทศและประชาชน และเพื่อใช้เป็นแนวทางในการดำเนินการที่สอดคล้องกับกรอบธรรมาภิบาลข้อมูลภาครัฐ (Data Governance Framework) อันถือเป็นภารกิจของคนทุกคนภายในองค์กรที่จะต้องร่วมมือกันดำเนินการตามธรรมาภิบาล ที่ได้มีการกำหนดและตกลงร่วมกันไว้แล้ว ซึ่งต้องทำอย่างต่อเนื่องสม่ำเสมอ จึงจะส่งผลให้ข้อมูลมีคุณภาพและองค์กรจะสามารถปรับเปลี่ยนตัวเองให้กลายเป็นองค์กรที่ขับเคลื่อนด้วยข้อมูลได้โดยแท้จริง เพื่อให้สถาบันมีการกำกับดูแลข้อมูลที่ครอบคลุมระบบบริหารและกระบวนการจัดการข้อมูลหรือวงจรชีวิตข้อมูล และเกิดผลเป็นรูปธรรม และมีการเผยแพร่ประชาสัมพันธ์นโยบายข้อมูลให้แก่บุคลากรหรือหน่วยงานที่เกี่ยวข้อง เพื่อให้มีความรู้ความเข้าใจต่อการปฏิบัติตามนโยบายข้อมูลภายใต้กรอบนโยบายข้อมูลของสถาบัน ต่อไป

๒. ขอบเขต

ขอบเขตของนโยบายฉบับนี้ ครอบคลุมการบริหารจัดการข้อมูลตลอดทั้งวงจรชีวิตของข้อมูล (Data Life Cycle) ตั้งแต่การสร้างหรือรวบรวม การจัดเก็บ การประมวลผล การใช้งาน การเปิดเผยหรือเผยแพร่ ไปจนถึงการทำลายข้อมูล รวมถึงกรอบกระบวนการธรรมาภิบาลข้อมูล (Data Governance Process) ที่เกิดขึ้นจากการดำเนินงานตามภารกิจทั้งหมดของสถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน)

นอกจากนี้ นโยบายฉบับนี้ยังมีผลบังคับใช้กับบุคลากรและหน่วยงานภายในทั้งหมดของสถาบันฯ ตลอดจนบุคคลภายนอกที่เกี่ยวข้อง ประกอบด้วย

(๑) บุคลากรภายใน ผู้บริหารระดับสูง เจ้าหน้าที่สถาบัน พนักงานประจำ ผู้ปฏิบัติงาน ลูกจ้างประจำ และลูกจ้างชั่วคราว ทุกระดับชั้น

(๒) บุคคลภายนอกและผู้มีส่วนได้ส่วนเสีย ที่ปรึกษา เจ้าหน้าที่จ้างเหมาบริการ (Outsource) คู่สัญญา หรือบุคคลภายนอกอื่นใดที่ได้รับมอบหมายหรือได้รับสิทธิ์ให้เข้าถึง ใช้งาน หรือบริหารจัดการข้อมูลของสถาบัน

๓. นิยาม

สถาบัน หรือ สคพ.	หมายถึง	สถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน)
ผู้บังคับบัญชา	หมายถึง	ผู้มีอำนาจสั่งการตามโครงสร้างของสถาบัน
คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council)	หมายถึง	คณะกรรมการธรรมาภิบาลข้อมูลของสถาบัน
ผู้บริหารระดับสูงด้านข้อมูล (Chief Data Officer)	หมายถึง	ผู้บริหารระดับสูงที่รับผิดชอบด้านการกำกับดูแลข้อมูลของสถาบัน
คณะทำงาน	หมายถึง	คณะทำงานจัดทำธรรมาภิบาลข้อมูลของสถาบัน
หัวหน้าหน่วยงาน	หมายถึง	ผู้อำนวยการสถาบัน รองผู้อำนวยการสถาบัน ที่ปรึกษา และหัวหน้าส่วนงานระดับสำนัก ฝ่าย ศูนย์ หรือผู้ที่ได้รับมอบหมาย
นโยบายข้อมูล (Data Policy)	หมายถึง	หนึ่งในพื้นฐานธรรมาภิบาลข้อมูลภาครัฐ เพื่อให้ธรรมาภิบาลข้อมูลภาครัฐมีประสิทธิภาพ จึงกำหนดนโยบายที่สอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง หลักเกณฑ์ นโยบาย และแนวทางปฏิบัติที่เกี่ยวข้อง
บริการข้อมูล (Data Steward)	หมายถึง	เจ้าหน้าที่ซึ่งได้รับแต่งตั้งจากคณะทำงานจัดทำธรรมาภิบาลข้อมูล

ผู้รับผิดชอบที่เกี่ยวข้องกับข้อมูล	หมายถึง	เจ้าหน้าที่ที่ทำหน้าที่ตรวจสอบดูแลข้อมูลโดยตรง ทำการทบทวนและอนุมัติการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับข้อมูลตามธรรมาภิบาลข้อมูลตลอดวงจรชีวิตของข้อมูล รวมถึงการให้สิทธิในการเข้าถึงข้อมูล และจัดชั้นความลับของข้อมูล
พจนานุกรมข้อมูล (Data Dictionary)	หมายถึง	ตารางหรือข้อมูลที่ใช้อธิบายรายละเอียดของข้อมูลในแต่ละแถวหรือคอลัมน์
สารสนเทศ (Information)	หมายถึง	ข้อมูล ข่าวสาร ในรูปแบบต่าง ๆ เช่น ตัวอักษร ตัวเลข สัญลักษณ์ รูปภาพ เสียง ที่ผ่านกระบวนการประมวลผล และบันทึกไว้อย่างเป็นระบบตามหลักวิชาการในสื่อประเภทต่าง ๆ เช่น หนังสือ วารสาร หนังสือพิมพ์ วิดีโอ ซีดีรอม ฐานข้อมูลอิเล็กทรอนิกส์ เป็นต้น เพื่อนำออกเผยแพร่และใช้ประโยชน์
ข้อมูล (Data)	หมายถึง	สิ่งที่สื่อความหมายให้รู้เรื่องราวข้อเท็จจริงหรือเรื่องอื่นใด ไม่ว่าจะสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเอง หรือโดยผ่านวิธีการใด ๆ และไม่ว่าจะได้จัดทำไว้ในรูปของ เอกสาร แฟ้ม รายงาน หนังสือ แผ่นผัง แผนที่ ภาพวาด ภาพถ่าย ภาพถ่ายดาวเทียม ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ เครื่องมือตรวจวัด การสำรวจระยะไกล หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้
ข้อมูลเปิด	หมายถึง	ข้อมูลที่สามารถนำไปใช้ได้โดยอิสระ สามารถนำกลับมาใช้ใหม่และ แจกจ่ายได้โดยใครก็ตาม แต่ต้องระบุแหล่งที่มาหรือเจ้าของงานและต้องใช้สัญญาอนุญาต หรือเงื่อนไขเดียวกันกับที่มาหรือตามเจ้าของงานกำหนด
ชุดข้อมูล (Datasets)	หมายถึง	การนำข้อมูลจากหลายแหล่งมารวบรวม เพื่อจัดเป็นชุดให้ตรงตามลักษณะโครงสร้างของข้อมูล
วงจรชีวิตข้อมูล (Data Life Cycle)	หมายถึง	ลำดับขั้นตอนของข้อมูลตั้งแต่เริ่มสร้างข้อมูลไปจนถึงการทำลายข้อมูลตามกรอบธรรมาภิบาลข้อมูลภาครัฐ
ความมั่นคงปลอดภัยของข้อมูล (Data Security)	หมายถึง	การดำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของข้อมูล ทั้งนี้เพื่อป้องกันการสูญหายเข้าถึง ใช้ เปลี่ยน แก้ไข หรือเปิดเผยข้อมูลโดยปราศจากอำนาจหรือโดยมิชอบ

บัญชีข้อมูล (Data Catalog)	หมายถึง	เอกสารแสดงบรรดารายการของชุดข้อมูล ที่จำแนกแยกแยะ โดยการจัดกลุ่มหรือจัดประเภทข้อมูลที่อยู่ในความครอบครองหรือควบคุมของหน่วยงานของรัฐ
เมทาดาดา (Metadata)	หมายถึง	ข้อมูลที่ใช้อธิบายข้อมูล โดยระบุรายละเอียดแหล่งข้อมูล และคำอธิบาย รายละเอียดเกี่ยวกับข้อมูล ซึ่งจะทำให้ผู้ใช้ข้อมูลทราบว่าข้อมูลมาจากแหล่งใด มีรูปแบบอย่างไร ช่วยอำนวยความสะดวกในการสืบค้นข้อมูล
คลังข้อมูล	หมายถึง	ข้อมูลที่ได้จากการเชื่อมโยงข้อมูลซึ่งเกิดจากการรวบรวมข้อมูลจากแหล่งข้อมูลต่าง ๆ ที่มีหลากหลายรูปแบบมาเก็บในคลังข้อมูล โดยผ่านกระบวนการของ Extract Transform Load (ETL) ในรูปแบบข้อมูลที่มีโครงสร้าง และถูกจัดทำให้อยู่ในรูปแบบที่เหมาะสมสำหรับการนำไปวิเคราะห์ข้อมูล
ดาตาเลค	หมายถึง	แหล่งสำหรับเก็บรวบรวมข้อมูลที่มีหลากหลายรูปแบบ ข้อมูลที่จัดเก็บเป็นข้อมูลที่มีโครงสร้าง ข้อมูลกึ่งโครงสร้าง และข้อมูลที่ไม่มีโครงสร้าง โดยข้อมูลถูกเก็บรักษาไว้ในรูปแบบที่เหมือนหรือใกล้เคียงกับรูปแบบที่ได้รับมาจากแหล่งข้อมูลต้นฉบับ และสามารถใช้เป็นสำเนาข้อมูลต้นฉบับได้
ดาตาอานาไลติกส์	หมายถึง	กระบวนการนำข้อมูลที่ได้จากการจัดเก็บด้วยวิธีต่าง ๆ นำมาเรียบเรียงจัดระเบียบ แยกประเภทชุดข้อมูล เพื่อนำมาวิเคราะห์หาความสัมพันธ์ของข้อมูลเพื่อนำมาใช้เพื่อตอบคำถามวัตถุประสงค์ที่ผู้วิเคราะห์ต้องการหาคำตอบ
ธรรมาภิบาลข้อมูลภาครัฐ	หมายถึง	การกำหนดสิทธิ หน้าที่ และความรับผิดชอบของผู้มีส่วนได้ส่วนเสียในการบริหารจัดการข้อมูลภาครัฐทุกขั้นตอน เพื่อให้การได้มาและการนำข้อมูลของหน่วยงานของรัฐไปใช้อย่างถูกต้อง ครบถ้วน เป็นปัจจุบัน รักษาความเป็นส่วนบุคคล และสามารถเชื่อมโยงแลกเปลี่ยน และบูรณาการ ระหว่างกันได้อย่างมีประสิทธิภาพและมั่นคงปลอดภัย
เจ้าหน้าที่	หมายถึง	เจ้าหน้าที่ทุกระดับของสถาบัน และพนักงานจ้างเหมาบริการซึ่งได้รับมอบหมายในการบริหารจัดการข้อมูลตามภารกิจ

หน่วยงานที่แลกเปลี่ยน เชื่อมโยงข้อมูล	หมายถึง	หน่วยงานอื่น ๆ ที่ได้รับอนุญาตจากสถาบัน และมีความร่วมมือ หรือแนวทางในด้านการบริหารจัดการข้อมูลกับหน่วยงานนั้น ๆ อย่างชัดเจน
บุคคลที่นำข้อมูลไปใช้	หมายถึง	เจ้าหน้าที่ของสถาบันทุกระดับ บุคคลภายนอก และหน่วยงานภายนอกที่ได้รับสิทธิการเข้าถึงข้อมูล
การบริหารจัดการข้อมูล (Data Management)	หมายถึง	ขั้นตอนการสร้างข้อมูล การรวบรวมข้อมูล การจัดเก็บ การจัดเก็บถาวร การทำลายข้อมูล การประมวลผลข้อมูล การใช้ข้อมูล การแลกเปลี่ยน การเชื่อมโยงข้อมูล และการเปิดเผยข้อมูลต่อสาธารณะ
เจ้าของข้อมูล (Data Owner)	หมายถึง	บุคคลที่ทำหน้าที่รับผิดชอบดูแลข้อมูลโดยตรง สร้างความมั่นใจว่าการบริหารจัดการข้อมูลสอดคล้องกับนโยบาย มาตรฐาน กฎระเบียบ หรือกฎหมาย ทบทวนและอนุมัติการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับข้อมูล
ผู้ควบคุมข้อมูล (Data Controller)	หมายถึง	เจ้าหน้าที่ที่ได้รับมอบหมายให้มีสิทธิในการจัดเก็บข้อมูลและทำลายข้อมูล
ผู้สร้างข้อมูล (Data Creators)	หมายถึง	ผู้ใช้ระบบสารสนเทศหรือบริการของสถาบัน ที่เป็นผู้ผลิตหรือนำเข้าข้อมูลเข้าสู่ระบบ
ผู้บริหารข้อมูล (Data Administrator / Data Manager)	หมายถึง	ผู้ที่สามารถจัดการข้อมูล และกำหนดสิทธิการเข้าถึงข้อมูล
ผู้ดูแลระบบแม่ข่าย (Server Administrator)	หมายถึง	บุคลากรที่มีหน้าที่ดูแลรับผิดชอบระบบแม่ข่ายของสถาบัน
ผู้ทำลายข้อมูล (Data Destroyers)	หมายถึง	บุคลากรที่ได้รับการกำหนดสิทธิจากเจ้าของข้อมูล ให้มีสิทธิในการทำลายข้อมูล

๔. นโยบายธรรมาภิบาลข้อมูล (Data Governance Policy) ประกอบด้วย ๖ หัวข้อหลัก ได้แก่

๔.๑ นโยบายธรรมาภิบาลข้อมูล (Data Governance Policy)

เพื่อกำหนดแนวทางการดำเนินงานด้านธรรมาภิบาลข้อมูล เนื่องจากการกำหนดนโยบายข้อมูลจัดเป็นหนึ่งในองค์ประกอบตามกรอบธรรมาภิบาลข้อมูล และเพื่อให้การบริหารจัดการข้อมูลมีประสิทธิภาพ จึงต้องมีการกำหนดนโยบายที่ระบุอย่างชัดเจน สอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง หรือข้อกำหนดอื่น ๆ ที่เกี่ยวข้อง เพื่อให้นโยบายข้อมูลได้ถูกนำมาปฏิบัติอย่างมีประสิทธิภาพและต่อเนื่อง

นโยบาย

- (๑) กำหนดให้มีโครงสร้างการกำกับดูแลข้อมูล พร้อมบทบาทและหน้าที่ความรับผิดชอบ
- (๒) กำหนดกลุ่มบุคคลหรือบุคคลเพื่อเป็นเจ้าของข้อมูลในการบริหารจัดการชุดข้อมูล

(๓) กำหนดขอบเขตของชุดข้อมูลให้อยู่ในรูปของข้อมูลที่มีโครงสร้าง ข้อมูลกึ่งโครงสร้าง หรือ ข้อมูลที่ไม่มีโครงสร้าง

(๔) กำหนดมาตรการการรักษาความมั่นคงปลอดภัยของข้อมูล เพื่อป้องกันการเข้าถึง การสูญหาย การทำลาย หรือการเปลี่ยนแปลงข้อมูลโดยไม่ได้รับการอนุญาต

(๕) ส่งเสริมการนำระบบเทคโนโลยีสารสนเทศ หรือระบบอัตโนมัติมาใช้ในการจัดทำเมทาเดตา (Metadata)

(๖) กำหนดให้มีการฝึกอบรม เพื่อสร้างความตระหนักรู้ถึงธรรมาภิบาลข้อมูลภาครัฐ อย่างน้อยปีละ ๑ ครั้ง

(๗) กำหนดให้มีการตรวจสอบการปฏิบัติตามนโยบายข้อมูล อย่างน้อยปีละ ๑ ครั้ง โดยคณะกรรมาธิการข้อมูล ทำหน้าที่ตรวจสอบ ติดตามผลการประเมิน เสนอข้อปรับปรุง และแนวทางแก้ปัญหาที่พบอย่างต่อเนื่อง

(๘) กำหนดให้มีการตรวจสอบความสอดคล้องระหว่างนโยบายข้อมูลและการดำเนินการใด ๆ ของผู้มีส่วนได้ส่วนเสีย อย่างน้อยปีละ ๑ ครั้ง

(๙) กำหนดให้มีการทบทวนนโยบายธรรมาภิบาลข้อมูลทุก ๑ ปี หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ

(๑๐) มีมาตรฐานการดำเนินการข้อมูลเปิด (Open Data)

๔.๒ นโยบายคุณภาพข้อมูล (Data Quality Policy)

เพื่อให้การควบคุมคุณภาพข้อมูลสำหรับการนำไปใช้ประโยชน์ในการบริหารงานและการให้บริการของสถาบัน เป็นไปตามอำนาจหน้าที่และวัตถุประสงค์ในการดำเนินงานของสถาบัน ตามที่กฎหมายกำหนด โดยข้อมูลที่ได้ทำการจัดเก็บนั้น สถาบันจะคำนึงถึงคุณภาพข้อมูล (Data Quality) ในทุกชุดข้อมูล (Dataset) ของสถาบัน

นโยบาย

(๑) กำหนดมาตรฐานข้อมูลให้เป็นแบบเดียวกัน และมีการควบคุมคุณภาพข้อมูลตลอดทั้งวงจรชีวิตข้อมูล (Data Life Cycle) ของข้อมูลที่ตนเองมีหน้าที่รับผิดชอบนั้น

(๒) กำหนดให้มีข้อกำหนดพื้นฐานของการบริหารจัดการคุณภาพข้อมูล (Data Quality Management) รวมถึงแนวทางการควบคุมและการปรับปรุงอย่างต่อเนื่อง

(๓) ชุดข้อมูลทุกชุดต้องมีการวัดคุณภาพข้อมูล (Data Quality) ดังต่อไปนี้ ความถูกต้อง (Accuracy) ความครบถ้วน (Completeness) ความสอดคล้องต้องกัน (Consistency) ความเป็นปัจจุบัน (Timeliness) ตรงตามความต้องการของผู้ใช้ (Relevancy) ความน่าเชื่อถือ (Data Integrity) และพร้อมใช้งาน (Availability) โดยทุกเกณฑ์ต้องเป็นเกณฑ์เชิงปริมาณ (Quantitative Measurement)

(๔) การกำหนดตัวชี้วัดคุณภาพข้อมูล เช่น ความถูกต้อง ความครบถ้วน ความสอดคล้องต้องกัน ความเป็นปัจจุบัน ตรงตามความต้องการของผู้ใช้ และพร้อมใช้งาน

๔.๓ นโยบายการเชื่อมโยงและแลกเปลี่ยนข้อมูล (Data Integration and Exchange Policy)

เพื่อให้การแลกเปลี่ยนข้อมูลทั้งภายในและระหว่างหน่วยงานมีความมั่นคงปลอดภัย และข้อมูลมีคุณภาพ สามารถนำไปใช้ประโยชน์ได้อย่างมีประสิทธิภาพ โดยมีวิธีและแนวทางการนำข้อมูลไปเชื่อมโยงและ

แลกเปลี่ยนกับหน่วยงานภายนอก ให้สอดคล้องกับระเบียบ หลักเกณฑ์ และกฎหมายที่กำหนด บนพื้นฐานของประโยชน์ส่วนรวมเป็นสำคัญ

นโยบาย

(๑) การแลกเปลี่ยนและการเชื่อมโยงข้อมูลของสถาบัน กับหน่วยงานอื่น ให้ดำเนินการโดยเจ้าหน้าที่ที่มีสิทธิให้กระทำการได้

(๒) กำหนดแนวปฏิบัติในการจัดการเรื่องความมั่นคงปลอดภัย คุณภาพข้อมูล และผู้ประสานงานหรือช่องทางการติดต่อ

(๓) กำหนดกระบวนการในการแลกเปลี่ยนข้อมูลให้ชัดเจน เริ่มตั้งแต่ขั้นตอนการเตรียมการ ขั้นตอนการเริ่มดำเนินการ ขั้นตอนระหว่างดำเนินการ และขั้นตอนสิ้นสุดการดำเนินการ ให้ดำเนินการตามแนวทางปฏิบัติการจัดทำบัญชีข้อมูล คุณภาพข้อมูล การเชื่อมโยงข้อมูล และการเผยแพร่ข้อมูล

(๔) กำหนดการคุ้มครองข้อมูลส่วนบุคคลในการแลกเปลี่ยนและเชื่อมโยงข้อมูล และให้เป็นไปตามนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) ของสถาบัน

(๕) กำหนดเมทาดาตาของชุดข้อมูลที่ต้องการแลกเปลี่ยนที่จำเป็นให้ครบถ้วน

(๖) ทำสัญญาอนุญาตหรือข้อตกลงระหว่างหน่วยงานในการแลกเปลี่ยนข้อมูล การนำข้อมูลไปใช้ เทคโนโลยี และมาตรฐานทางเทคนิคที่ใช้ในการแลกเปลี่ยนข้อมูล

(๗) บันทึกรายละเอียดและจัดเก็บข้อมูลการดำเนินงานที่เกิดขึ้นในแต่ละครั้งที่มีการแลกเปลี่ยนข้อมูล (Log File) ระหว่างหน่วยงาน เพื่อให้สามารถตรวจสอบได้

(๘) สามารถตรวจสอบได้ว่าการแลกเปลี่ยนข้อมูลได้ดำเนินการอย่างเหมาะสม หรือเป็นไปตามแนวทางปฏิบัติ กระบวนการแลกเปลี่ยน และมาตรฐานตามที่กำหนด

๔.๔ มาตรฐานการจัดชั้นความลับข้อมูล (Data Classification Standard)

เพื่อให้การประมวลผลข้อมูลและการใช้ข้อมูลมีประสิทธิภาพ ถูกต้อง ตรงตามวัตถุประสงค์ของการใช้ข้อมูลให้เกิดประโยชน์ รวมถึงวิธีการและแนวทางในการขอข้อมูลจากหน่วยงานที่เกี่ยวข้องทั้งภายในและภายนอกเพื่อนำมาใช้ในการประมวลผลและนำมาใช้ ทั้งนี้ การนำข้อมูลมาใช้ให้เป็นไปตามวัตถุประสงค์ที่แจ้ง หากนอกเหนือจากเหตุผลดังกล่าวข้างต้น จะต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อน

นโยบาย

(๑) ชุดข้อมูลต้องมีการจัดลำดับชั้นความลับของข้อมูล การกำหนดชั้นความลับของข้อมูล และการกำหนดสิทธิการเข้าถึง เพื่อให้สอดคล้องกับแนวทางการจัดชั้นความลับของข้อมูล

(๒) ห้ามเปิดเผยข้อมูลที่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง นโยบาย แนวปฏิบัติ ไม่ว่าข้อมูลจะอยู่ในรูปแบบใดหรือสถานที่ใดก็ตาม

(๓) ต้องได้รับการอนุญาตจากตัวแทนหน่วยงานหรือเจ้าของข้อมูลก่อนการเปิดเผยข้อมูล

(๔) ต้องมีการระบุช่องทางการเปิดเผยข้อมูลที่เข้าถึงและนำไปใช้ได้ง่าย

(๕) ให้มีการเปิดเผยเมทาดาตา (Metadata) ควบคู่ไปกับข้อมูลที่เปิดเผย

(๖) สามารถตรวจสอบได้ว่าการเปิดเผยข้อมูลได้ถูกดำเนินการอย่างเหมาะสมหรือเป็นไปตามแนวทางที่ได้กำหนดไว้ เพื่อให้ได้ข้อมูลที่มีคุณภาพ และเป็นการรักษาคุณภาพของข้อมูล

(๗) การเปิดเผยข้อมูลส่วนบุคคล ให้ดำเนินการตามนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) ของสถาบันฯ

(๘) ต้องมีการทบทวนระดับชั้นความลับข้อมูลอย่างน้อยปีละ ๑ ครั้ง และให้ดำเนินการปรับปรุงอย่างต่อเนื่อง

๔.๕ นโยบายความมั่นคงปลอดภัยและความเป็นส่วนตัวของข้อมูล (Data Security and Privacy Policy)

เพื่อเป็นการกำหนดแนวทางในการบริหารจัดการความมั่นคงปลอดภัยของข้อมูลและความเป็นส่วนตัว ซึ่งจะต้องสอดคล้องกับนโยบายความมั่นคงปลอดภัยและความเป็นส่วนตัวของข้อมูล

นโยบาย

(๑) กำหนดให้มีผู้รับผิดชอบการรักษาความมั่นคงปลอดภัยของข้อมูล

(๒) กำหนดให้มีการรักษาความลับ (Confidentiality) โดยรักษาข้อมูลตามสภาพของการจัดชั้นความลับ และมีการกำหนดสิทธิการเข้าถึงข้อมูลนั้น

(๓) กำหนดให้มีความถูกต้องของข้อมูล (Integrity) โดยให้คงสภาพของข้อมูลหรือการรักษาความถูกต้องสมบูรณ์ของข้อมูลให้มีความถูกต้องและน่าเชื่อถือ รวมถึงมีการปกป้องข้อมูลให้ปราศจากการถูกเปลี่ยนแปลงโดยผู้ไม่มีสิทธิ

(๔) กำหนดให้มีความพร้อมใช้งานของข้อมูล (Availability) โดยให้ข้อมูลต้องพร้อมสำหรับการใช้งานได้เสมอ รวมถึงมีการสำรองข้อมูลไว้เมื่อเกิดภัยพิบัติหรือเหตุการณ์ที่ไม่คาดฝัน หากต้องการใช้ข้อมูล ผู้ใช้งานสามารถใช้ข้อมูลได้ทันทีและใช้ได้อย่างต่อเนื่อง

(๕) กำหนดให้มีการรักษาความเป็นส่วนตัวของข้อมูล (Data Privacy) ตั้งแต่การรวบรวม จัดเก็บ ใช้ เผยแพร่ หรือดำเนินการอื่นใดเกี่ยวกับข้อมูล โดยจะต้องมีการระบุวัตถุประสงค์เป็นหลักฐานให้ชัดเจน ห้ามมิให้มีการเปิดเผย หรือแสดง หรือทำให้ปรากฏในลักษณะอื่นใดที่ไม่สอดคล้องกับวัตถุประสงค์ เว้นแต่จะได้รับความยินยอมจากเจ้าของข้อมูลนั้น ๆ หรือมีกฎหมายกำหนดให้สามารถกระทำสิ่งนั้นได้

(๖) กรณีเกิดการรั่วไหลหรือมีการละเมิดข้อมูลส่วนบุคคล ให้ดำเนินการตามนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) ของสถาบันฯ

(๗) จัดให้มีการประเมินความมั่นคงปลอดภัยของข้อมูล

๔.๖ นโยบายการเปิดเผยข้อมูล (Open Data Policy)

เพื่อกำหนดนโยบายข้อมูลที่สามารถนำไปใช้ได้โดยอิสระ สามารถนำกลับมาใช้ใหม่และแจกจ่ายได้โดยใครก็ตาม แต่ต้องระบุแหล่งที่มาหรือเจ้าของงานและต้องใช้สัญญาอนุญาต หรือเงื่อนไขเดียวกันกับที่มาหรือตามที่เจ้าของข้อมูลกำหนด

นโยบาย

(๑) กำหนดบทบาทหน้าที่ที่เกี่ยวข้องกับการเปิดเผยข้อมูล ได้แก่ กำหนดบุคคลหรือกลุ่มบุคคลที่มีสิทธิตัดสินใจในการเปิดเผยข้อมูล กำหนดบุคคลหรือกลุ่มบุคคลในการดำเนินการและปรับปรุงการเปิดเผยข้อมูล และกำหนดบุคคลหรือกลุ่มบุคคลในการรับเรื่องและแก้ไขปัญหาเบื้องต้นในการเข้าถึงข้อมูลและการนำข้อมูลไปใช้

(๒) ห้ามเปิดเผยข้อมูลที่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง นโยบาย แนวปฏิบัติ ไม่ว่าจะข้อมูลจะอยู่ในรูปแบบใดหรือสถานที่ใดก็ตาม

(๓) ต้องได้รับการอนุญาตจากเจ้าของข้อมูล (Data Owner) ก่อนการเปิดเผยข้อมูลหรือการนำไปใช้

(๔) ให้มีการจัดเตรียมข้อมูลที่อยู่ในรูปแบบที่ได้จัดทำไว้เป็นมาตรฐานตามกำหนด และง่ายต่อการนำไปใช้งาน

(๕) มีการจัดทำเมตาดาตา (Metadata) ควบคู่ไปกับข้อมูลที่เปิดเผย

(๖) ให้มีการคัดเลือกชุดข้อมูลที่ต้องการเผยแพร่ โดยหน่วยงานเจ้าของข้อมูลหรือผู้ที่ได้รับมอบหมาย

(๗) สามารถตรวจสอบได้ว่าการเปิดเผยข้อมูลได้ถูกดำเนินการอย่างเหมาะสมหรือเป็นไปตามแนวทางที่ได้กำหนดไว้ เพื่อให้ได้ข้อมูลที่มีคุณภาพ และเป็นการรักษาคุณภาพของข้อมูล

(๘) ต้องปฏิบัติตามอย่างเคร่งครัด และป้องกันมิให้มีการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

๕. การทบทวนนโยบายข้อมูล

สถาบันฯ โดยคณะกรรมการจัดทำธรรมาภิบาลข้อมูล และทีมบริการข้อมูล (Data Stewards) ต้องร่วมกันดำเนินการทบทวนนโยบายธรรมาภิบาลข้อมูลของสถาบันฯ เมื่อมีการเปลี่ยนแปลงที่สำคัญ หรือทบทวนเป็นประจำตามความเหมาะสม

๖. แนวปฏิบัติด้านธรรมาภิบาลข้อมูล

ข้อมูลของสถาบันฯ ระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน) หรือ สถาบันฯ เป็นข้อมูลภาครัฐที่สำคัญของประเทศ โดยมีการให้บริการกับหน่วยงานภาครัฐ หน่วยงานเอกชน และประชาชนในวงกว้าง ดังนั้น จึงต้องมีธรรมาภิบาลข้อมูลและการกำกับดูแลที่ดี เพื่อให้ข้อมูลมีคุณภาพ พร้อมใช้ มีความเชื่อมโยงกัน และมีความมั่นคงปลอดภัย อันเป็นการสร้างประโยชน์ให้กับประเทศอย่างยั่งยืน

สถาบันฯ ได้นำแนวทางตามกรอบธรรมาภิบาลข้อมูลที่ประกอบด้วยองค์ประกอบต่าง ๆ ผสมผสานเข้าด้วยกัน ทั้งในด้านของนิยามและกฎเกณฑ์ที่เกี่ยวข้องกับข้อมูล บุคคล และกระบวนการ ซึ่งองค์ประกอบเหล่านี้มีความสำคัญที่ก่อให้เกิดประสิทธิภาพและประสิทธิผลในการดำเนินงาน อันจะนำไปสู่การบรรลุเป้าหมายในการดำเนินงานตามที่กำหนดไว้ ซึ่งโครงสร้างธรรมาภิบาลข้อมูล (Data Governance Structure) ประกอบด้วย

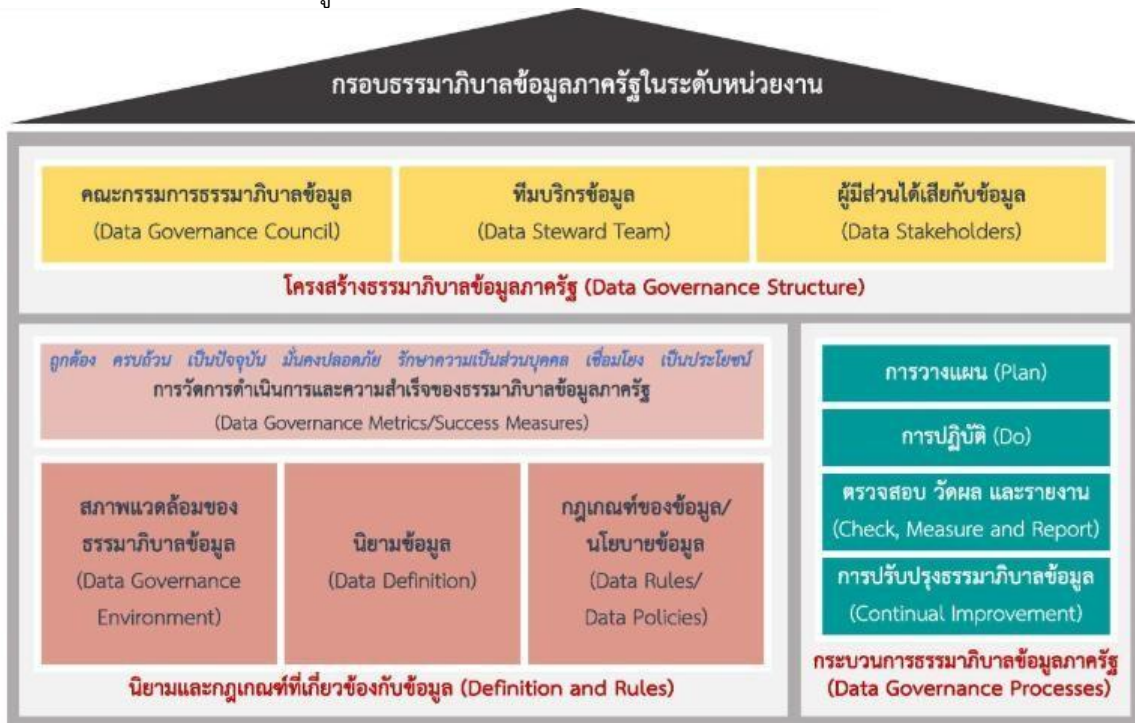
(๑) คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council)

(๒) คณะบริการข้อมูล (Data Steward Team)

(๓) ผู้มีส่วนได้ส่วนเสียกับข้อมูล (Data Stakeholders)

โดยมีกระบวนการธรรมาภิบาลข้อมูล (Data Governance Processes) มากำกับดูแลการดำเนินการหรือกิจกรรม ตลอดจนบุคคลที่เกี่ยวข้อง ซึ่งโครงสร้างธรรมาภิบาลข้อมูลจะถูกแต่งตั้งโดยสถาบันฯ เพื่อทำ

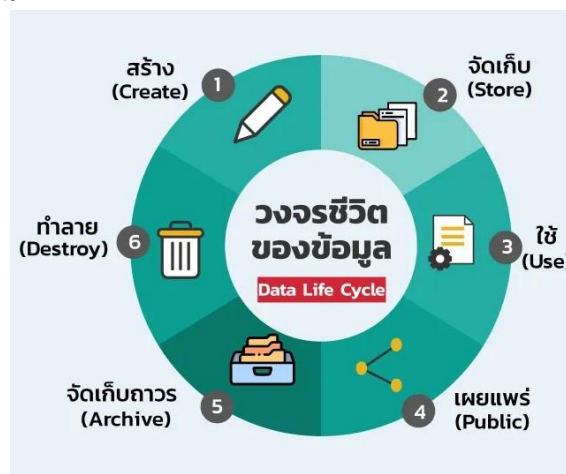
หน้าที่กำหนดยุทธศาสตร์และเป้าหมาย ตรวจสอบสภาพแวดล้อมของธรรมาภิบาลข้อมูล นิยามความหมาย และขอบเขตของข้อมูล กำหนดกฎเกณฑ์และนโยบายข้อมูล (Definition and Rules) และดำเนินการตรวจสอบการปฏิบัติตามกฎเกณฑ์และนโยบายข้อมูล โดยมีการรายงานไปยังผู้บริหารเพื่อปรับปรุงกฎเกณฑ์ นโยบาย และการดำเนินงานให้ถูกต้องเหมาะสมต่อไป



รูปภาพที่ ๑ กรอบธรรมาภิบาลข้อมูลของสถาบัน

๖.๑ การบริหารจัดการวงจรชีวิตของข้อมูล (Data Life Cycle Management)

ถ้าเปรียบข้อมูลเป็นสิ่งมีชีวิต ข้อมูลก็จะมีวงจรชีวิต กล่าวคือมีการเกิดขึ้น ตั้งอยู่ และดับไป เพียงแต่คุณลักษณะพิเศษของข้อมูลคือเป็นสิ่งไม่มีชีวิต จึงมีอายุยืนยาวตราบเท่าที่ไม่มีใครเข้าไปทำลาย วงจรชีวิตของข้อมูล จึงหมายถึงลำดับขั้นตอนตั้งแต่เริ่มสร้างข้อมูลไปจนถึงการทำลายข้อมูล ซึ่งตลอดทั้งวงจรชีวิตประกอบด้วย ๖ ขั้นตอน ดังนี้



รูปภาพที่ ๒ วงจรของข้อมูล

(๑) การสร้างข้อมูล (Create) คือ การสร้างข้อมูลขึ้นมาใหม่ ทั้งวิธีการจดบันทึกด้วยมือหรือการบันทึกด้วยอุปกรณ์อิเล็กทรอนิกส์ต่าง ๆ

(๒) **การจัดเก็บข้อมูล (Store)** คือ การนำข้อมูลที่สร้างขึ้นมาจัดเก็บให้เป็นระเบียบ สะดวกและง่ายต่อการใช้งานตามวัตถุประสงค์ต่าง ๆ รักษาป้องกันไม่ให้สูญหายหรือถูกขโมย ไม่ว่าจะเป็นการจัดเก็บลงแฟ้มเอกสาร ระบบจัดการฐานข้อมูลในระบบคอมพิวเตอร์ หรือระบบคลาวด์ (Cloud)

(๓) **การใช้ข้อมูล (Use)** คือ การนำข้อมูลที่จัดเก็บมาใช้ประมวลผลให้เกิดประโยชน์ตรงตามวัตถุประสงค์ด้านการใช้งานต่าง ๆ เช่น การวิเคราะห์ข้อมูล การทำการตลาด เป็นต้น

(๔) **การเผยแพร่ข้อมูล (Publish)** คือ การนำข้อมูลไปเปิดเผย ไม่ว่าจะเป็นการส่งมอบเอกสาร การแลกเปลี่ยนข้อมูล การแชร์ข้อมูล การกระจายข้อมูลระหว่างบุคคล หรือองค์กร เป็นต้น

(๕) **การจัดเก็บข้อมูลถาวร (Archive)** คือ การคัดลอกข้อมูลเพื่อทำสำเนาสำหรับเก็บรักษา โดยไม่มีการลบ ปรับปรุง หรือแก้ไขข้อมูลนั้นอีก และสามารถนำไปใช้งานใหม่เมื่อต้องการ

(๖) **การทำลายข้อมูล (Destroy)** คือ การทำลายข้อมูลไม่ให้มีสภาพการใช้งาน เนื่องจากมีอายุยาวนานเกินไปจนไม่เหมาะสมกับการใช้ประโยชน์อีก และเพื่อไม่ให้ข้อมูลถูกนำไปใช้งานที่ผิดวัตถุประสงค์ จึงจำเป็นต้องทำลายเอกสาร ตลอดจนไฟล์ข้อมูลต่าง ๆ ในระบบคอมพิวเตอร์หรือระบบคลาวด์

การบริหารจัดการข้อมูลเป็นสิ่งสำคัญสำหรับทุกหน่วยงาน ซึ่งแต่ละหน่วยงานต้องตระหนักว่าข้อมูลที่มีอยู่เป็นสินทรัพย์ที่มีค่า เพื่อให้หน่วยงานสามารถนำข้อมูลเหล่านี้ไปประมวลผลหรือใช้ในการตัดสินใจได้อย่างแม่นยำ จึงต้องได้รับการบริหารจัดการอย่างถูกต้อง เหมาะสม และสอดคล้องกับวัตถุประสงค์ในการบริหารจัดการข้อมูลของหน่วยงาน

๖.๒ หมวดการบริหารจัดการและประเมินคุณภาพข้อมูล (Data Quality Management)

- (๑) กำหนดให้มีหน่วยงานหรือผู้รับผิดชอบในการบริหารจัดการคุณภาพข้อมูล
- (๒) จัดให้มีการกำหนดคุณลักษณะข้อมูลที่มีคุณภาพ
- (๓) กำหนดหลักเกณฑ์คุณภาพของข้อมูล
- (๔) กำหนดให้มีการประเมินคุณภาพของข้อมูล
- (๕) จัดให้มีการควบคุมและติดตามให้ข้อมูลมีคุณภาพอยู่เสมอ

๖.๓ เกณฑ์การประเมินคุณภาพข้อมูล ให้ดำเนินการตามมิติคุณภาพข้อมูล ๕ มิติ ได้แก่

- (๑) ความถูกต้อง (Accuracy)
- (๒) ความสอดคล้องกัน (Consistency)
- (๓) ตรงตามความต้องการของผู้ใช้ (Relevancy)
- (๔) ความเป็นปัจจุบัน (Timeliness)
- (๕) ความพร้อมใช้ (Availability) ที่สอดคล้องตามองค์ประกอบในการประเมินคุณภาพข้อมูล

ตามกรอบธรรมาภิบาลข้อมูลภาครัฐ โดยแต่ละมิติมีรายละเอียดและตัวชี้วัด (Indicators) ดังนี้

มิติคุณภาพข้อมูล	รายละเอียด	รายการตัวชี้วัด
ความถูกต้องและสมบูรณ์ (Accuracy and Completeness)	ประเมินความถูกต้อง แม่นยำ ความน่าเชื่อถือของแหล่งข้อมูล และการมีกระบวนการตรวจสอบความถูกต้องของข้อมูล	<ul style="list-style-type: none">■ ข้อมูลมาจากแหล่งข้อมูลที่ น่าเชื่อถือ■ มีกระบวนการหรือเครื่องมือ ในการตรวจสอบจุดผิดพลาด หรือข้อบกพร่องของข้อมูล■ มีการตรวจสอบความครบถ้วนสมบูรณ์ของข้อมูล

มิติคุณภาพข้อมูล	รายละเอียด	รายการตัวชี้วัด
		<ul style="list-style-type: none"> ■ มีวิธีการจัดเก็บข้อมูลที่เป็นกลาง น่าเชื่อถือ และไม่สร้างข้อมูลที่มีอคติ (Bias)
<p>ความสอดคล้องกัน (Consistency)</p>	<p>ประเมินรูปแบบของข้อมูล ความสอดคล้องต้องกัน และการใช้มาตรฐานเดียวกันในการจัดทำข้อมูลของหน่วยงาน</p>	<ul style="list-style-type: none"> ■ มีการระบุ คำนิยาม และลักษณะของข้อมูลที่ต้องการอย่างชัดเจน ■ มีการจัดเก็บข้อมูลภายใต้มาตรฐานข้อมูลเดียวกัน หรือเป็นมาตรฐานข้อมูลที่สอดคล้องกัน ■ มีการตรวจสอบรูปแบบข้อมูล (Data Format) ภายในชุดข้อมูลเดียวกันให้เป็นมาตรฐานเดียว ■ ข้อมูลมีความเชื่อมโยงและเนื้อหาไม่ขัดแย้งกันเอง ■ มีการใช้กฎเกณฑ์และวิธีการตรวจวัดที่สอดคล้องกัน ทั้งภายในหน่วยงานและกับหน่วยงานภายนอก
<p>ตรงตามความต้องการ ของผู้ใช้ (Relevancy)</p>	<p>ประเมินว่าเป็นข้อมูลที่ผู้ใช้งานมีความต้องการ เป็นข้อมูลที่จำเป็นต่อทราบ และมีระดับความละเอียดที่เพียงพอต่อการนำไปใช้งานจริง</p>	<ul style="list-style-type: none"> ■ มีการกำหนดบทบาทและ ผู้รับผิดชอบข้อมูลที่ชัดเจน เพื่อตอบสนองการใช้งาน ■ ข้อมูลตรงตามความต้องการ และสอดคล้องกับวัตถุประสงค์ของการนำไปใช้งาน ■ มีการปรับปรุงคุณภาพข้อมูลให้ตรงตามความต้องการของผู้ใช้งานอย่างสม่ำเสมอ
<p>ความเป็นปัจจุบัน (Timeliness)</p>	<p>ประเมินการเผยแพร่ข้อมูล การปรับปรุงและปรับปรุงข้อมูลให้เป็นปัจจุบัน รวมถึงการกำหนดแผนระยะเวลาการดำเนินงานที่ชัดเจน</p>	<ul style="list-style-type: none"> ■ ข้อมูลมีความทันสมัยและเป็นปัจจุบัน ■ ข้อมูลมีการเผยแพร่และส่งต่อตรงตามเวลาที่กำหนด ■ มีการเผยแพร่ข้อมูลในระยะเวลาที่เหมาะสมกับสถานการณ์และการทำงาน

มิติคุณภาพข้อมูล	รายละเอียด	รายการตัวชี้วัด
ความพร้อมใช้(Availability)	ประเมินความพร้อมในการเข้าถึงและใช้งานข้อมูล รวมถึงการกำหนดช่องทางในการอำนวยความสะดวกเพื่อขอหรือเข้าใช้ข้อมูล	<ul style="list-style-type: none"> ■ ข้อมูลถูกจัดให้อยู่ในรูปแบบที่พร้อมนำไปใช้งานและเหมาะสมกับกลุ่มผู้ใช้งาน ■ มีการเผยแพร่ข้อมูลอย่างเหมาะสม โดยผู้ใช้สามารถเข้าถึงข้อมูลได้สะดวกตามสิทธิการเข้าถึงที่กำหนด ■ ข้อมูลอยู่ในรูปแบบที่สามารถอ่านหรือประมวลผลด้วยโปรแกรมคอมพิวเตอร์ได้ (Machine-readable) ■ มีคำอธิบายข้อมูล (Metadata) ที่อธิบายรายละเอียดได้ชัดเจนและเข้าใจง่าย

นโยบายและแนวทางปฏิบัติธรรมาภิบาลข้อมูลภาครัฐเพื่อเป็นหลักการในการบริหารจัดการข้อมูลภาครัฐของสถาบันมีดังนี้

๖.๔ หมวดหมู่ของข้อมูล (Data Category) ข้อมูลแบ่งออกได้ ๔ หมวดหมู่ ดังนี้



รูปภาพที่ ๓ หมวดหมู่ของข้อมูล (Data Category)

(๑) **ข้อมูลสาธารณะ** คือ ข้อมูลที่สามารถเปิดเผยได้ สามารถนำไปใช้ได้โดยอิสระ ไม่ว่าจะเป็นข้อมูลข่าวสาร ข้อมูลส่วนบุคคล ข้อมูลอิเล็กทรอนิกส์ เป็นต้น

(๒) **ข้อมูลความลับทางราชการ** คือ ข้อมูลที่อยู่ในความครอบครองหรือควบคุมดูแลของหน่วยงานของรัฐที่มีคำสั่งไม่ให้มีการเปิดเผย และมีการกำหนดชั้นความลับของข้อมูล

(๓) **ข้อมูลความมั่นคง** คือ ข้อมูลเกี่ยวกับความมั่นคงของรัฐที่ทำให้เกิดความสงบเรียบร้อย การมีเสถียรภาพ ความเป็นปึกแผ่น ปลอดภัยจากภัยคุกคาม เป็นต้น

(๔) **ข้อมูลส่วนบุคคล** คือ ข้อมูลเกี่ยวกับสิ่งเฉพาะตัวของบุคคลที่ทำให้สามารถระบุตัวหรือรู้ตัวของบุคคลนั้น ๆ ได้ ไม่ว่าจะเป็นข้อมูลการศึกษา ประวัติสุขภาพ ลายพิมพ์นิ้วมือ เป็นต้น

๖.๕ การจัดทำบัญชีข้อมูล (Data Catalog) การจัดทำบัญชีข้อมูล ประกอบด้วยรายละเอียด ดังนี้

(๑) เจ้าของข้อมูลหรือผู้ครอบครองข้อมูล มีหน้าที่กำหนดให้มีผู้รับผิดชอบที่เกี่ยวข้องกับข้อมูลของหน่วยงาน

(๒) ผู้รับผิดชอบที่เกี่ยวข้องกับข้อมูล มีหน้าที่กำหนดคำนิยามของชุดข้อมูล (List of Data) ดังนี้

- ความสัมพันธ์ของข้อมูล
- ชนิดข้อมูล (Reference/Master Data Definition) แบ่งเป็น
 - Reference Data หรือ ข้อมูลที่มีลักษณะและโครงสร้างที่เป็นความจริงและถูกต้อง ทำให้ข้อมูลไม่ค่อยเปลี่ยนแปลง ส่งผลให้ข้อมูล Reference Data ถูกเผยแพร่ไปยังแหล่งต่าง ๆ เพื่ออ้างอิงอยู่เสมอ
 - Master Data หรือ ข้อมูลที่มีโอกาสเปลี่ยนแปลงได้มากกว่า มีรายละเอียดหรือจำนวนฟิลด์ข้อมูลมากกว่า Reference Data และใช้เป็นข้อมูลในการดำเนินงานภายในหน่วยงาน
- ขอบเขตที่ดำเนินการ
- ชุดข้อมูลที่คาดว่าจะเกี่ยวข้อง
- กระบวนการหลักหรืองานหลักที่ได้รับมอบหมาย และกระบวนการย่อย
- ชุดข้อมูลที่เกี่ยวข้องกับกระบวนการย่อย แบ่งเป็น ชุดข้อมูลที่มีอยู่แล้ว และชุดข้อมูลที่ต้องจัดทำเพิ่มเติม

- รูปแบบของการเก็บข้อมูล
- ความพร้อมของชุดข้อมูล
- การเชื่อมโยงและแลกเปลี่ยนข้อมูลภายในหน่วยงาน

๖.๖ ผู้รับผิดชอบที่เกี่ยวข้องกับข้อมูล มีหน้าที่กำหนดพจนานุกรมข้อมูล (Data Dictionary)

- (๑) เลขที่เมทาดาทา (Metadata ID)
- (๒) ชื่อชุดข้อมูล (Dataset Name)
- (๓) เลขที่ข้อมูล (Data ID)
- (๔) ชื่อตารางข้อมูล (Table Name)
- (๕) ชื่อฟิลด์ข้อมูล (Field Name)
- (๖) คำอธิบายฟิลด์ (Description)
- (๗) ระดับชั้นความลับ (Classification)
- (๘) ประเภทข้อมูล (Data Type)
- (๙) ขนาดข้อมูล (Data Size)
- (๑๐) คุณลักษณะข้อมูล (Characteristic Type)
- (๑๑) แหล่งที่มาของค่าที่ระบุในฟิลด์ (Data Source)
- (๑๒) รูปแบบ (Data Format)
- (๑๓) เงื่อนไข (Condition)

๖.๗ หมวดคุณลักษณะข้อมูลเปิดภาครัฐที่จะถูกนำมาเปิดเผยต่อสาธารณะ

(๑) ข้อมูลเปิดต้องพร้อมใช้งาน และไม่เป็นข้อมูลส่วนบุคคล ข้อมูลความมั่นคง หรือมีข้อกเว้นในการเปิดเผยข้อมูล

(๒) ข้อมูลที่ได้จากแหล่งข้อมูลโดยตรง ไม่มีการปรับแต่ง อยู่ในรูปแบบข้อมูลสรุป หรืออยู่ในรูปแบบสถิติได้

(๓) ข้อมูลต้องเป็นปัจจุบัน และเปิดเผยในเวลาเร็วที่สุดเท่าที่เป็นไปได้ เพื่อเพิ่มประโยชน์ให้กับผู้ใช้ข้อมูล

(๔) ข้อมูลต้องเข้าถึงได้ง่าย ผู้ใช้ข้อมูลสามารถค้นหา เข้าถึง และใช้งานชุดข้อมูลได้หลายช่องทาง

(๕) ข้อมูลต้องมีโครงสร้าง สามารถอ่านได้ด้วยเครื่องคอมพิวเตอร์ (Machine-readable) และนำข้อมูลไปใช้งานต่อได้

(๖) ผู้ใช้ข้อมูลต้องสามารถนำข้อมูลไปใช้ได้อย่างอิสระ โดยไม่ต้องระบุตัวตน หรือเหตุผลของการนำไปใช้งาน

(๗) ข้อมูลต้องอยู่ในรูปแบบมาตรฐานเปิดที่สามารถใช้ได้หลายแพลตฟอร์ม ไม่จำกัดสิทธิ และต้องไม่ถือครองกรรมสิทธิ์หลังจากนำข้อมูลเปิดไปใช้ประโยชน์

(๘) ข้อมูลต้องไม่ขัดต่อกฎหมายว่าด้วยลิขสิทธิ์ สิทธิบัตร เครื่องหมายการค้า หรือความลับทางการค้า

(๙) ข้อมูลต้องสามารถใช้งานได้ตลอดเวลา และมีการควบคุมการเปลี่ยนแปลงของชุดข้อมูล

(๑๐) ผู้ใช้ข้อมูลต้องไม่เสียค่าใช้จ่ายในการเข้าถึงข้อมูล

ทั้งนี้ ในกรณีที่มีกฎหมายกำหนดรายละเอียดเกี่ยวกับคุณลักษณะของข้อมูลเปิดภาครัฐอย่างหนึ่งอย่างใดไว้เป็นการเฉพาะ ให้ปฏิบัติตามหลักเกณฑ์การเปิดเผยข้อมูลเปิดภาครัฐที่กำหนดไว้ตามกฎหมายว่าด้วยการนั้น

๖.๘ หมวดการสร้างและการรวบรวมข้อมูล

(๑) การสร้างและการรวบรวมข้อมูลส่วนบุคคล ให้ดำเนินการตามนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) ของสถาบัน

(๒) การสร้างและการรวบรวมข้อมูล มีการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล โดยปฏิบัติตามแนวปฏิบัติในการปกป้องข้อมูลที่ระบุตัวบุคคล และแนวปฏิบัติในด้านความมั่นคงปลอดภัยของ ข้อมูลส่วนบุคคลของสถาบัน ทั้งนี้ ให้เป็นไปตามที่กฎหมายกำหนด

(๓) การสร้างและการรวบรวมข้อมูลที่มีใช้ข้อมูลส่วนบุคคล โดยมีแหล่งกำเนิดข้อมูลจากภายนอกสถาบัน ต้องได้รับความยินยอมจากเจ้าของข้อมูล เว้นแต่โดยสภาพเป็นข้อมูลที่มีการเปิดเผยต่อสาธารณะหรือเป็นข้อมูลที่ต้องเปิดเผยตามกฎหมาย

(๔) บริการข้อมูลและเจ้าของข้อมูลต้องร่วมกันจัดให้มีคำอธิบายชุดข้อมูล และบัญชีข้อมูลที่มีความถูกต้อง ครบถ้วน และเป็นปัจจุบัน โดยให้เป็นไปตามมาตรฐานการบริหารจัดการเมทาดาตาของสถาบัน

(๕) จัดชั้นความลับของข้อมูลที่จะเก็บรวบรวม ใช้ หรือเปิดเผย

(๖) จัดให้มีคำอธิบายชุดข้อมูลดิจิทัลของภาครัฐและบัญชีข้อมูลจากข้อมูลต่าง ๆ ที่รวบรวมให้มีความถูกต้อง ครบถ้วนและเป็นปัจจุบัน

๖.๙ หมวดการจัดเก็บข้อมูลและทำลายข้อมูล

(๑) กำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัยในการจัดเก็บข้อมูลและการรักษาคุณภาพของข้อมูล

(๒) กำหนดให้เจ้าของข้อมูลของสถาบันฯ จัดชั้นความลับของข้อมูล และดำเนินการตามมาตรฐานการจัดชั้นความลับข้อมูลของสถาบันฯ

(๓) กำหนดสิทธิการเข้าถึงข้อมูล และเครื่องมือที่ใช้ในการเข้าถึงข้อมูล

(๔) จัดเก็บข้อมูลให้สอดคล้องกับความต้องการและวัตถุประสงค์ในการดำเนินงานของสถาบันฯ โดยข้อมูลนั้นจะต้องมีความถูกต้อง สมบูรณ์ และเป็นปัจจุบันอยู่เสมอ โดยจัดทำเมทาเดตาสำหรับชุดข้อมูลที่มีการจัดเก็บ

(๕) กำหนดให้มีการสำรองข้อมูลเพื่อความมั่นคงปลอดภัย มิให้ข้อมูลสูญหาย และเป็นปัจจุบัน

(๖) กำหนดแนวทางในการทำลายข้อมูล เมื่อข้อมูลนั้นไม่มีการใช้งาน หรือมีการเก็บข้อมูลไว้นานเกินกว่าระยะเวลาที่กำหนด แต่ควรมีการเก็บรักษาเมทาเดตาของข้อมูลที่ทำลายไว้เพื่อใช้สำหรับการตรวจสอบภายหลัง

(๗) การจัดเก็บข้อมูลส่วนบุคคลและการทำลายข้อมูลส่วนบุคคล ให้ดำเนินการตามนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) ของสถาบันฯ

(๘) สร้างความรู้ความเข้าใจในการจัดเก็บและทำลายข้อมูลแก่ผู้ที่เกี่ยวข้องทั้งภายในและภายนอกสถาบันฯ

(๙) การเก็บข้อมูล สถาบันจะใช้วิธีตามที่กฎหมายกำหนดในการเก็บ รวบรวมใช้หรือเปิดเผยข้อมูลส่วนบุคคลของเจ้าของข้อมูล โดยสถาบันจะเก็บรวบรวม ข้อมูลส่วนบุคคลอย่างจำกัดและเท่าที่จำเป็น ตามวัตถุประสงค์ในการเก็บรวบรวมใช้ หรือเปิดเผยข้อมูล

(๑๐) การจัดเก็บ การจัดเก็บถาวร ต้องมีการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล และความเป็นส่วนตัวของข้อมูล ให้เป็นไปตามที่กฎหมายกำหนด หรือแนวปฏิบัติในการปกป้องข้อมูล หรือแนวปฏิบัติในด้านความมั่นคงปลอดภัยและชั้นความลับของข้อมูล

(๑๑) การจัดเก็บข้อมูล ต้องจัดเก็บลงในสื่อบันทึกข้อมูลและมีโครงสร้างข้อมูลตามมาตรฐานสถาปัตยกรรมข้อมูล ข้อมูลหลัก และข้อมูลอ้างอิง

(๑๒) การจัดเก็บถาวร ต้องเป็นการดำเนินการกับข้อมูลที่ไม่มีการลบ ปรับปรุง หรือแก้ไขอีกต่อไป และสามารถนำกลับมาใช้งานได้ โดยให้เป็นไปตามที่กฎหมายกำหนด

(๑๓) การจัดเก็บข้อมูลชั้นความลับที่เป็นข้อมูลความลับทางราชการ และข้อมูลความมั่นคง ต้องมีการเข้ารหัสข้อมูล

(๑๔) การสำรองข้อมูล ต้องจัดเก็บให้มีความถูกต้องครบถ้วนเป็นปัจจุบัน ตามมาตรฐานการสำรองข้อมูล

(๑๕) การทำลายข้อมูล ต้องเป็นการดำเนินการกับข้อมูลที่ไม่ต้องนำกลับมาใช้งานได้อีกต่อไป โดยให้เป็นไปตามที่กฎหมายกำหนด

๖.๑๐ หมวดการประมวลผลและการใช้ข้อมูล

(๑) สถาบันจะกำหนดให้มีการติดตามและประเมินผลการใช้งานข้อมูลอย่างน้อยปีละ ๑ ครั้ง โดยจัดทำเป็นรายงานเสนอไปยังผู้บริหาร

(๒) การดำเนินการประมวลผลข้อมูลที่เป็นความลับของข้อมูลส่วนบุคคล ให้เป็นไปตามนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) ของสถาบันฯ

(๓) การดำเนินการประมวลผลข้อมูลที่เป็นความลับของข้อมูลที่ไม่ใช่ข้อมูลส่วนบุคคล ให้เป็นไปตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔

(๔) จัดทำเมทาเดตาสำหรับข้อมูลที่จัดเก็บอยู่ในคลังข้อมูล (Data Warehouse)

(๕) ต้องจัดให้มีการบันทึกประวัติการประมวลผลและการใช้ข้อมูล (Log File) อย่างเป็นระบบ เพื่อให้สามารถตรวจสอบประวัติการทำงานย้อนกลับได้ โดยให้เป็นไปตามหลักเกณฑ์ที่กฎหมายกำหนด

(๖) การสร้างความตระหนักรู้ของผู้ใช้ข้อมูล รวมถึงความรับผิดชอบต่อผลของการนำข้อมูลไปใช้ การเข้าถึงและใช้ข้อมูลตามความจำเป็นในการปฏิบัติงานโดยไม่แสวงหาผลประโยชน์ส่วนตัว หรือเพื่อวัตถุประสงค์อื่นที่ไม่เหมาะสม และใช้ข้อมูลให้เป็นไปตามระดับความปลอดภัยที่กำหนด

(๗) สิทธิการประมวลผลและการทำงานของผู้ใช้ข้อมูล ต้องสอดคล้องกับวัตถุประสงค์และชั้นความลับของข้อมูล โดยเฉพาะอย่างยิ่งการเรียกใช้ข้อมูลความลับทางราชการและข้อมูลความมั่นคง จะต้องมีการกำหนดสิทธิการเข้าใช้อย่างเคร่งครัดตามที่กฎหมายกำหนด

(๘) การประมวลผลข้อมูลและการใช้ข้อมูลต้องมีการรักษาความมั่นคงปลอดภัยของข้อมูล ส่วนบุคคลตามแนวปฏิบัติในการปกป้องข้อมูลที่ระบุตัวบุคคล และแนวปฏิบัติในด้านความมั่นคงปลอดภัย และความเป็นส่วนบุคคลของข้อมูล โดยให้เป็นไปตามที่กฎหมายกำหนด

(๙) การประมวลผลและการใช้ข้อมูล ต้องมีความถูกต้อง (Accuracy) ความครบถ้วน (Completeness) ความต้องการ (Consistency) ความเป็นปัจจุบัน (Timeliness) และมีคุณภาพ (Quality)

๖.๑๑ หมวดการแลกเปลี่ยนและการเชื่อมโยงข้อมูล

(๑) การแลกเปลี่ยนและการเชื่อมโยงข้อมูลของสถาบันฯ กับหน่วยงานอื่น ให้ดำเนินการโดยเจ้าหน้าที่ที่มีสิทธิให้กระทำการได้

(๒) กำหนดแนวปฏิบัติในการจัดการเรื่องความมั่นคงปลอดภัย คุณภาพข้อมูล และผู้ประสานงานหรือช่องทางการติดต่อ

(๓) กำหนดกระบวนการในการแลกเปลี่ยนข้อมูลให้ชัดเจน เริ่มตั้งแต่ขั้นตอนการเตรียมการ ขั้นตอนเริ่มดำเนินการ ขั้นตอนระหว่างดำเนินการ และขั้นตอนสิ้นสุดการดำเนินการ ให้ดำเนินการตามแนวทางปฏิบัติการจัดทำบัญชีข้อมูล คุณภาพข้อมูล การเชื่อมโยงข้อมูล และการเผยแพร่ข้อมูล

(๔) การแลกเปลี่ยนและเชื่อมโยงข้อมูลต้องมีการจัดการด้านความมั่นคงปลอดภัยอย่างรัดกุม โดยเฉพาะข้อมูลส่วนบุคคล จะต้องดำเนินการตามแนวปฏิบัติในการปกป้องข้อมูลที่ระบุตัวบุคคล และสอดคล้องกับนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) ของสถาบันฯ รวมถึงกฎหมายที่เกี่ยวข้องอย่างเคร่งครัด

(๕) กำหนดเมทาดาตาของชุดข้อมูลที่ต้องการแลกเปลี่ยนที่จำเป็นให้ครบถ้วน

(๖) ทำสัญญาอนุญาตหรือข้อตกลงระหว่างหน่วยงานในการแลกเปลี่ยนข้อมูล การนำข้อมูลไปใช้เทคโนโลยี และมาตรฐานทางเทคนิคที่ใช้ในการแลกเปลี่ยนข้อมูล

(๗) บันทึกรายละเอียดและจัดเก็บข้อมูลการดำเนินงานที่เกิดขึ้นในแต่ละครั้งที่มีการแลกเปลี่ยนข้อมูล (Log File) ระหว่างหน่วยงาน เพื่อให้สามารถตรวจสอบได้

(๘) สามารถตรวจสอบได้ว่าการแลกเปลี่ยนข้อมูลได้ดำเนินการอย่างเหมาะสมหรือเป็นไปตามแนวทางปฏิบัติ กระบวนการแลกเปลี่ยน และมาตรฐานตามที่กำหนด

(๙) การเชื่อมโยงและการแลกเปลี่ยนข้อมูลของสถาบันฯ กับหน่วยงานอื่น ๆ จะต้องได้รับอนุญาตจากสถาบันฯ และมีความร่วมมือ หรือแนวทางในด้านการบริหาร จัดการข้อมูลกับหน่วยงานนั้น ๆ อย่างชัดเจน

(๑๐) เทคโนโลยีและวิธีการทางเทคนิคที่เกี่ยวข้องกับการเชื่อมโยงและการแลกเปลี่ยนข้อมูล ให้เป็นไปตามมาตรฐานสากล

(๑๑) บริการข้อมูลฝ่ายผู้ส่งจะเป็นผู้รับเรื่อง เมื่อฝ่ายผู้รับพบปัญหาใด ๆ เกี่ยวกับการเชื่อมโยงข้อมูล หรือคุณภาพข้อมูลที่ส่งไป

(๑๒) บริการข้อมูลของทั้ง ๒ ฝ่ายทำหน้าที่ในการตรวจสอบความถูกต้องของข้อมูล

(๑๓) บริการข้อมูลฝ่ายผู้ส่งมีหน้าที่ในการรับเรื่องปัญหาที่เกิดขึ้นในการเชื่อมโยงข้อมูล และประสานกับผู้ที่เกี่ยวข้องข้อต่อไป

(๑๔) ทุกชุดข้อมูลที่มีการเชื่อมโยงกันระหว่างสำนัก นอกจากชุดข้อมูลที่มีการจัดส่งแล้วจะต้องมีการจัดทำเอกสารมาตรฐานการเชื่อมโยงข้อมูล ซึ่งประกอบด้วย ชื่อชุดข้อมูล วันและเวลาการรับรองข้อมูล โดยบริการข้อมูลฝ่ายผู้ส่งข้อมูล คำอธิบายชุดข้อมูล (Metadata) ชั้นความลับของข้อมูล วันและเวลาในการส่งออกข้อมูล และวันและเวลาที่ผู้รับได้รับข้อมูล

(๑๕) การตรวจสอบข้อมูลจะต้องอ้างอิงตามคำอธิบายชุดข้อมูล (Metadata) และข้อมูลอ้างอิงของ ชุดข้อมูลนั้น

๖.๑๒ หมวดการเปิดเผยข้อมูล

(๑) ห้ามเปิดเผยข้อมูลที่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง นโยบาย แนวปฏิบัติ ไม่ว่าข้อมูลจะอยู่ในรูปแบบใดหรือสถานที่ใดก็ตาม

(๒) ต้องได้รับการอนุญาตจากตัวแทนหน่วยงานหรือเจ้าของข้อมูลก่อนการเปิดเผยข้อมูล

(๓) ต้องมีการระบุช่องทางการเปิดเผยข้อมูลที่เข้าถึงและนำไปใช้ได้ง่าย

(๔) ให้มีการเปิดเผยเมทาตาควบคุมเกี่ยวกับข้อมูลที่เปิดเผย

(๕) สามารถตรวจสอบได้ว่าการเปิดเผยข้อมูลได้ถูกดำเนินการอย่างเหมาะสมหรือเป็นไปตามแนวทางที่กำหนดไว้ เพื่อให้ได้ข้อมูลที่มีคุณภาพ และเป็นการรักษาคุณภาพของข้อมูล

(๖) การเปิดเผยข้อมูลส่วนบุคคล ให้ดำเนินการตามนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) ของสถาบันฯ

(๗) การเปิดเผยข้อมูลต่าง ๆ จะต้องเป็นไปตามที่กฎหมายกำหนด

(๘) สถาบันเปิดเผยข้อมูลส่วนบุคคลของเจ้าของข้อมูลในกรณีใด กรณีหนึ่ง ดังต่อไปนี้

- ได้รับความยินยอมจากเจ้าของข้อมูล
- เป็นความจำเป็นเพื่อการปฏิบัติงานของราชการหรือตามคำขอของเจ้าของข้อมูล รวมทั้งเปิดเผยเพื่อให้เกิดธุรกรรมหรือกิจกรรมใด ๆ ของเจ้าของข้อมูลสามารถดำเนินการได้โดยบรรลุ ตามวัตถุประสงค์ของเจ้าของข้อมูล

- เป็นความจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมาย
- เป็นการปฏิบัติงานตามกฎหมายหรือกฎเกณฑ์ของทางราชการหรือคำสั่งของ หน่วยงานที่มีอำนาจกำกับดูแล หรือที่มีอำนาจตามกฎหมาย

(๙) การเผยแพร่ข้อมูลหรือการเปิดเผยข้อมูลในรูปแบบดิจิทัล ต้องปฏิบัติตามแนวทางการเปิดเผยข้อมูลเปิดภาครัฐในรูปแบบดิจิทัลต่อสาธารณะของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

๖.๑๓ หมวดการรักษาความมั่นคงปลอดภัยของข้อมูล

(๑) กำหนดให้มีผู้รับผิดชอบการรักษาความมั่นคงปลอดภัยของข้อมูล

(๒) กำหนดให้มีการรักษาความลับ (Confidentiality) โดยรักษาข้อมูลตามสภาพของการจัดชั้นความลับและมีการกำหนดสิทธิการเข้าถึงข้อมูลนั้น

(๓) กำหนดให้มีความถูกต้องของข้อมูล (Integrity) โดยให้คงสภาพของข้อมูลหรือการรักษาความถูกต้องสมบูรณ์ของข้อมูลให้มีความถูกต้องและน่าเชื่อถือ รวมถึงมีการปกป้องข้อมูลให้ปราศจากการถูกเปลี่ยนแปลงโดยผู้ไม่มีสิทธิ

(๔) กำหนดให้มีความพร้อมใช้งานของข้อมูล (Availability) โดยให้ข้อมูลต้องพร้อมสำหรับการใช้งานได้เสมอ รวมถึงมีการสำรองข้อมูลไว้เมื่อเกิดภัยพิบัติหรือเหตุการณ์ที่ไม่คาดฝัน หากต้องการใช้ข้อมูล ผู้ใช้งานสามารถใช้ข้อมูลได้ทันทีและใช้ได้อย่างต่อเนื่อง

(๕) กำหนดให้มีการรักษาความเป็นส่วนบุคคลของข้อมูล (Data Privacy) ตั้งแต่การรวบรวม จัดเก็บ ใช้ เผยแพร่ หรือดำเนินการอื่นใดเกี่ยวกับข้อมูล โดยจะต้องมีการระบุวัตถุประสงค์เป็นหลักฐานให้ชัดเจน ห้ามมิให้มีการเปิดเผย หรือแสดง หรือทำให้ปรากฏในลักษณะอื่นใดที่ไม่สอดคล้องกับวัตถุประสงค์ เว้นแต่จะได้รับความยินยอมจากเจ้าของข้อมูลนั้น ๆ หรือมีกฎหมายกำหนดให้สามารถกระทำสิ่งนั้นได้

(๖) กรณีเกิดการรั่วไหลหรือมีการละเมิดข้อมูลส่วนบุคคล ให้ดำเนินการตามนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) ของสถาบันฯ

๖.๑๔ การเข้าถึงข้อมูล

การบริหารจัดการในการเข้าถึงข้อมูลกำหนดให้ผู้ใช้ข้อมูลต้องนำไปใช้อย่างเหมาะสมและสถาบันจะปกป้องข้อมูลด้วยมาตรการรักษาความมั่นคงปลอดภัยที่ได้รับการรับรองตามมาตรฐานสากล

๖.๑๕ การบูรณาการข้อมูลกับหน่วยงานอื่น

สถาบันมีการบูรณาการข้อมูลกับหน่วยงานอื่น โดยการจัดส่งข้อมูลเอกสาร หรือการเชื่อมโยงข้อมูลผ่านระบบ โดยใช้ข้อมูลเลขประจำตัวประชาชน ๑๓ หลัก หรือ ชื่อ สกุล เป็นเงื่อนไขในการเชื่อมโยงหรือ ตามมาตรฐานการแลกเปลี่ยนข้อมูลระหว่างระบบสารสนเทศอิเล็กทรอนิกส์ของ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) หรือตามมาตรฐานที่มติคณะรัฐมนตรีกำหนด หรือมีการตกลงเป็นลายลักษณ์อักษรเพื่อการเชื่อมโยงข้อมูลระหว่างหน่วยงาน โดยระบบจะทำการประมวลผลและตอบผลข้อมูลรายละเอียดตามแต่ละบริการ

๖.๑๖ การเก็บรักษาข้อมูล

สถาบันไม่มีหน้าที่ในการจัดเก็บข้อมูลของหน่วยงานที่แลกเปลี่ยนเชื่อมโยงข้อมูล แต่จะทำการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์และข้อมูลการใช้งานของผู้ใช้ข้อมูล ที่สอดคล้องตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ และที่แก้ไขเพิ่มเติม

๖.๑๗ การเผยแพร่และการทบทวน

สถาบันอาจจะพิจารณาทบทวนหรือแก้ไขปรับปรุงนโยบายและแนวปฏิบัติฉบับนี้ เพื่อให้สอดคล้องกับกฎหมาย ระเบียบ หรือนโยบายที่เกี่ยวข้อง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ

๖.๑๘ การจัดชั้นความลับข้อมูล

เพื่อกำหนดมาตรฐาน กระบวนการ บุคลากร หน้าที่และความรับผิดชอบ และเทคโนโลยีที่สถาบันต้องปฏิบัติในการจัดชั้นความลับของข้อมูล โดยมีแนวปฏิบัติดังนี้

(๑) ทุกชุดข้อมูลต้องมีการจัดลำดับชั้นความลับของข้อมูล ดังต่อไปนี้

● ระดับที่ ๑ ข้อมูลสาธารณะ ได้แก่ ข้อมูลที่สามารถเปิดเผยได้ สามารถนำไปใช้ได้อย่างอิสระ

● ระดับที่ ๒ ข้อมูลส่วนบุคคล ได้แก่ ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อมแต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

● ระดับที่ ๓ ข้อมูลความลับทางราชการ ได้แก่ ข้อมูลที่อยู่ในความครอบครอง หรือควบคุมดูแล ของหน่วยงานของรัฐที่มีคำสั่ง ไม่ให้มีการเปิดเผย ไม่ว่าจะเป็นเรื่องที่เกี่ยวกับการดำเนินงานของรัฐ หรือที่เกี่ยวกับเอกชน ซึ่งมีการกำหนดให้มีชั้นความลับเป็น ชั้นลับ ชั้นลับมาก หรือชั้นลับที่สุด

● **ระดับที่ ๔** ข้อมูลความมั่นคง ได้แก่ ข้อมูลเกี่ยวกับความมั่นคงของรัฐ ที่ส่งผลต่อความสงบเรียบร้อย เสถียรภาพความเป็นปึกแผ่น ตลอดจนปลอดภัยจากภัยคุกคาม

(๒) การจัดลำดับชั้นความลับข้อมูลต้องดำเนินการโดยบริการข้อมูลและอนุมัติโดยคณะกรรมการธรรมาภิบาลข้อมูล

(๓) ในการประชุมคณะกรรมการธรรมาภิบาลข้อมูล จำเป็นต้องบรรจุวาระเกี่ยวกับการทบทวนระดับชั้นความลับข้อมูล อย่างน้อยปีละ ๑ ครั้ง

(๔) ทุกฟิลต์ในแต่ละชุดข้อมูลถือว่ามีระดับชั้นความลับเท่ากัน สำหรับชุดข้อมูลที่มีระดับความลับเป็น **ระดับที่ ๒ ระดับที่ ๓ หรือระดับที่ ๔** จำเป็นต้องระบุสิทธิ์ในการเข้าถึงข้อมูลภายในองค์กรด้วย

(๕) การเผยแพร่ข้อมูล**ระดับที่ ๑** ต้องได้รับการอนุมัติจากผู้บริหารระดับสูงด้านข้อมูล

(๖) ข้อมูล**ระดับที่ ๒** เป็นต้นไปจะต้องมีกระบวนการในการร้องขอข้อมูล

(๗) บุคคลเจ้าของข้อมูล มีหน้าที่ร่วมพิจารณาและรับทราบการร้องขอข้อมูลส่วนบุคคล

(๘) เจ้าของข้อมูล มีหน้าที่อนุมัติการร้องขอข้อมูลร่วมกับบริการข้อมูล และตรวจสอบ ทบทวนการจัดลำดับชั้นความลับข้อมูล

(๙) บริการข้อมูล มีหน้าที่ตรวจสอบการใช้งานข้อมูลสาธารณะและประเมินผลกระทบของการคุ้มครองข้อมูล (Data Protection Impact Assessment: DPIA)

(๑๐) เจ้าของข้อมูลทำหน้าที่อนุมัติการร้องขอข้อมูลร่วมกับบริการข้อมูล

(๑๑) ในกรณีที่ผู้ร้องขอข้อมูลไม่ได้มีสิทธิ์ตามสิทธิ์การเข้าถึงข้อมูล จำเป็นต้องดำเนินการตามกระบวนการ ดังต่อไปนี้

● ข้อมูลส่วนบุคคล ต้องมีการร้องขอผ่านส่วนงานที่บุคคลนั้นสังกัด โดยแจ้งวัตถุประสงค์ให้ชัดเจน โดยบุคคลเจ้าของข้อมูลและบริการข้อมูลของฝ่ายทรัพยากรบุคคลต้องรับทราบและมีสิทธิ์ที่จะปฏิเสธการร้องขอนั้นวันแต่จะมีประกาศของสถาบันรองรับ

● ข้อมูลความลับทางราชการ ต้องมีการร้องขอผ่านส่วนงานที่เป็นเจ้าของข้อมูล โดยเจ้าของข้อมูลและบริการข้อมูลแต่ละสำนักต้องพิจารณาร่วมกัน ถ้าเป็นข้อมูลที่มีความอ่อนไหว หรือมีความเสี่ยงต้องได้รับการอนุมัติโดยคณะกรรมการธรรมาภิบาลข้อมูล

● ข้อมูลความมั่นคง ต้องมีการร้องขอผ่านส่วนงานที่เป็นเจ้าของข้อมูล โดยต้องได้รับ การอนุมัติจากคณะกรรมการธรรมาภิบาลข้อมูลเท่านั้น

(๑๒) ระดับชั้นความลับข้อมูลจะต้องถูกระบุไว้ในคำอธิบายเมทาดาดา (Metadata)

(๑๓) การร้องขอข้อมูลต้องมีการเก็บบันทึกด้วย

๗. สิทธิ หน้าที่ และความรับผิดชอบของผู้ซึ่งมีหน้าที่เกี่ยวข้องกับการบริหารจัดการข้อมูลของสถาบัน (Roles and Responsibilities)

คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council) ของสถาบัน ประกอบด้วย ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงของสถาบัน (Chief Information Officer: CIO) เป็นประธานคณะกรรมการ และผู้บริหารจากสำนัก ฝ่าย ศูนย์ หรือกลุ่มงาน เป็นกรรมการ ซึ่งคณะกรรมการมีอำนาจสูงสุดในธรรมาภิบาลข้อมูลของสถาบันฯ ทำหน้าที่ตัดสินใจเชิงนโยบาย แก้ไขปัญหา และบริหารจัดการธรรมาภิบาลข้อมูลร่วมกับทีมบริการข้อมูล (Data Steward Team)

๘. โครงสร้างของบุคลากรที่รับผิดชอบในธรรมาภิบาลข้อมูลของสถาบัน

๘.๑ หัวหน้าหน่วยงาน (Chief Executive Officer : CEO)

๘.๑.๑ ผู้รับผิดชอบ: ผู้อำนวยการสถาบัน หรือผู้บริหารเทคโนโลยีสารสนเทศระดับสูง

๘.๑.๒ มีหน้าที่ตัดสินใจเชิงนโยบาย แก้ไขปัญหา บริหารจัดการและสนับสนุนธรรมาภิบาล ข้อมูล ภายในหน่วยงาน

๘.๒ ผู้บริหารข้อมูลระดับสูง (Chief Data Officer : CDO)

๘.๒.๑ ผู้รับผิดชอบ: ผู้อำนวยการสำนักยุทธศาสตร์และสารสนเทศ หรือผู้บริหารที่ได้รับมอบหมาย

๘.๒.๒ มีหน้าที่ให้ข้อเสนอแนะ และอนุมัตินโยบายข้อมูล มาตรฐานข้อมูล แนวทางปฏิบัติงาน เกณฑ์การวัดคุณภาพ ระเบียบ และข้อบังคับอื่น ๆ ที่เกี่ยวข้องกับข้อมูล รวมไปถึงการบริหารจัดการ การจัดลำดับความสำคัญ และแก้ไขปัญหาที่เกี่ยวข้องกับข้อมูล

๘.๓ คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Committee)

๘.๓.๑ ผู้รับผิดชอบ: คณะกรรมการทำงานจัดทำธรรมาภิบาลข้อมูลของสถาบัน

๘.๓.๒ มีหน้าที่ให้คำปรึกษา กำกับดูแลข้อมูล พร้อมเสนอแนะนโยบายและแนวทางการบริหารจัดการข้อมูล

๘.๔ เจ้าของข้อมูล (Data Owner)

๘.๔.๑ ผู้รับผิดชอบ: ผู้อำนวยการสำนักที่มีหน้าที่รับผิดชอบดูแลข้อมูลโดยตรง

๘.๔.๒ มีหน้าที่รับผิดชอบดูแลข้อมูลโดยตรง สร้างความมั่นใจได้ว่าการบริหารจัดการข้อมูล สอดคล้องกับนโยบาย มาตรฐาน กฎ ระเบียบ หรือ กฎหมาย เจ้าของข้อมูลทำการทบทวนและอนุมัติ การดำเนินการต่าง ๆ ที่เกี่ยวข้องกับข้อมูล เช่น การเปลี่ยนแปลงเมทาดาตา (Metadata) และเกณฑ์การทำ Data Cleansing รวมถึงการกำหนดสิทธิในการเข้าถึงข้อมูลและจัดชั้นความลับของข้อมูล

๘.๕ ทีมบริการข้อมูล (Data Stewards Team)

๘.๕.๑ ผู้รับผิดชอบ: หัวหน้าบริการข้อมูล (Lead Data Steward) บริการข้อมูล ด้านธุรกิจ ข้อมูลด้านเทคนิค บริการข้อมูลด้านคุณภาพข้อมูล รวมไปถึงบุคคลที่ทำหน้าที่เกี่ยวกับความมั่นคงปลอดภัย กฎหมาย และบุคคลที่ให้ความรู้เกี่ยวกับนโยบายข้อมูลและความรู้อื่น ๆ

๘.๕.๒ มีหน้าที่ ดังนี้

๑) กำหนด ทบทวนความต้องการด้านคุณภาพข้อมูล การรักษาความเป็นส่วนตัว บุคคล และความมั่นคงปลอดภัยของข้อมูล

๒) กำหนด ทบทวน และปรับปรุงกระบวนการให้สอดคล้องกับนโยบายข้อมูล เป้าประสงค์ ความต้องการของผู้มีส่วนได้ส่วนเสียกับข้อมูล รวมทั้งติดตามการดำเนินงานตามแผนที่กำหนด เพื่อนำมาปรับปรุงกระบวนการทำงาน

๓) กำหนดนิยามคำอธิบายชุดข้อมูลดิจิทัล พร้อมทั้งจัดทำบัญชีข้อมูลให้ครบถ้วน ตามความจำเป็นในการใช้งาน และตรงตามความต้องการของผู้มีส่วนได้ส่วนเสียกับข้อมูล

๔) วิเคราะห์ความพร้อมของธรรมาภิบาลข้อมูล ความต้องการด้านคุณภาพข้อมูล การรักษาความเป็นส่วนตัว และความมั่นคงปลอดภัยให้เหมาะสมกับสถานการณ์ปัจจุบัน เพื่อวางแผน การวัดและประเมินผล

๕) ตรวจสอบ วิเคราะห์และวัดผลการดำเนินงาน

๖) ให้ข้อเสนอแนะเชิงเทคนิคที่สอดคล้องกับนโยบาย เป้าประสงค์ และความต้องการ ของผู้มีส่วนได้ส่วนเสียกับข้อมูล

๗) กำหนดรายละเอียดที่เกี่ยวข้องกับการออกแบบระบบเทคโนโลยีสารสนเทศ รวมถึง โครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ เพื่อคุ้มครองข้อมูลส่วนบุคคล และรักษาความมั่นคงปลอดภัย

๘) สนับสนุนการดำเนินงานด้านเทคโนโลยีสารสนเทศและอื่น ๆ ที่เกี่ยวข้อง

๙) รายงานผลลัพธ์ไปยังคณะกรรมการดิจิทัลสถาบันและผู้เกี่ยวข้อง

๘.๖ ทีมบริหารจัดการข้อมูล (Data Management Team)

๘.๖.๑ ผู้รับผิดชอบ: นักเทคโนโลยีสารสนเทศ และเจ้าหน้าที่ที่ได้รับมอบหมาย

๘.๖.๒ มีหน้าที่หลักในการบริหารจัดการข้อมูล สอดคล้องกับ ๑๐ องค์ประกอบในการบริหาร จัดการข้อมูล ได้แก่

๑) สถาปัตยกรรมข้อมูล (Data Architecture)

๒) การจำลองและการออกแบบข้อมูล (Data Modeling and Design)

๓) การจัดเก็บและการดำเนินการกับข้อมูล (Data Storage and Operation)

๔) การบูรณาการและความสามารถในการทำงานร่วมกัน (Data Integration and Interoperability)

๕) การบริหารจัดการเอกสารและเนื้อหา (Document and Content Management)

๖) ข้อมูลหลักและข้อมูลอ้างอิง (Master and Reference Data)

๗) คลังข้อมูล ดาตาเลค ระบบรายงานอัจฉริยะ และดาตาอานาไลติกส์

๘) คำอธิบายชุดข้อมูลดิจิทัล หรือ Metadata

๙) ความมั่นคงปลอดภัยและการรักษาความเป็นส่วนตัวของข้อมูล (Data Security and Data Privacy)

๑๐) คุณภาพของข้อมูล (Data Quality)

๘.๗ ผู้สร้างข้อมูล (Data Creators)

๘.๗.๑ ผู้รับผิดชอบ: เจ้าหน้าที่ของหน่วยงานที่เป็นเจ้าของข้อมูล

๘.๗.๒ มีหน้าที่บันทึก แก้ไข ปรับปรุง หรือลบข้อมูลให้สอดคล้องกับโครงสร้างที่ถูกกำหนดไว้ รวมถึงทำงานร่วมกับทีมบริการข้อมูล เพื่อตรวจสอบ แก้ไขปัญหาด้านคุณภาพ และความมั่นคงปลอดภัยของข้อมูล

๘.๘ ผู้ใช้ข้อมูล (Data Users)

๘.๘.๑ ผู้รับผิดชอบ: เจ้าหน้าที่ของสถาบันทุกระดับ บุคคลภายนอก และหน่วยงานภายนอกที่ได้รับสิทธิการเข้าถึงข้อมูล

๘.๘.๒ มีหน้าที่นำข้อมูลไปใช้งาน ต้องสนับสนุนธรรมาภิบาลข้อมูลภาครัฐ โดยการให้ความสำคัญในการใช้ข้อมูล พร้อมทั้งรายงานประเด็นปัญหาที่พบระหว่างการใช้อ้างอิงข้อมูล ทั้งด้านคุณภาพและความปลอดภัยของข้อมูลไปยังทีมบริการข้อมูล

กฎหมาย ประกาศ ระเบียบ ข้อบังคับที่เกี่ยวข้อง

หมวดที่ ๑ พระราชบัญญัติ

๑. พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐ และที่แก้ไขเพิ่มเติม
๒. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม
๓. พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒
๔. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒
๕. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒
๖. พระราชบัญญัติการปฏิบัติราชการทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๖๕

หมวดที่ ๒ ระเบียบและประกาศมาตรฐาน

๗. ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔
๘. ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมนูญข้อมูลภาครัฐ พ.ศ. ๒๕๖๓
๙. ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง มาตรฐานและหลักเกณฑ์การเปิดเผยข้อมูลเปิดภาครัฐในรูปแบบข้อมูลดิจิทัลต่อสาธารณะ พ.ศ. ๒๕๖๓
๑๐. ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง มาตรฐานและหลักเกณฑ์การเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัล ว่าด้วยเรื่อง กรอบแนวทางการพัฒนามาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ พ.ศ. ๒๕๖๕
๑๑. ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง มาตรฐานรัฐบาลดิจิทัลว่าด้วยแนวทางการจัดทำบัญชีข้อมูลภาครัฐและแนวทางการลงทะเบียนบัญชีข้อมูลภาครัฐ พ.ศ. ๒๕๖๖
๑๒. ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง มาตรฐานรัฐบาลดิจิทัลว่าด้วยข้อเสนอแนะสำหรับการจัดทำนโยบายและแนวปฏิบัติการบริหารจัดการข้อมูล พ.ศ. ๒๕๖๖

หมวดที่ ๓ กรอบแนวทางและนโยบายหน่วยงาน

๑๓. กรอบการกำกับดูแลข้อมูล (Data Governance Framework) ของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
๑๔. กรอบแนวทางการเชื่อมโยงรัฐบาลอิเล็กทรอนิกส์แห่งชาติ
๑๕. นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ฉบับปี พ.ศ. ๒๕๖๕ สถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน)
๑๖. แนวปฏิบัติในการใช้เทคโนโลยีปัญญาประดิษฐ์แบบเจเนอเรทีฟ (Generative Artificial Intelligence) ในบริบทของการศึกษา มหาวิทยาลัยมหิดล พ.ศ. ๒๕๖๘