แนวทางปฏิบัติธรรมาภิบาลข้อมูลของ
สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

ด้วยพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายการบริหารงานและการจัดทำบริการสาธารณะดิจิทัลให้สอดคล้องเหมาะสม รวดเร็ว มีประสิทธิภาพ ตอบสนองต่อการเปลี่ยนแปลงของเทคโนโลยีและความต้องการของประชาชน รวมทั้งหน่วยงานของรัฐต้องจัดทำนโยบายการจัดการ “บูรณาการข้อมูลภาครัฐ” เพื่อให้การดำเนินงานของคณะกรรมการผู้บริหารเทคโนโลยีสารสนเทศภาครัฐมีความมั่นคง ปลอดภัย โปร่งใส สามารถบูรณาการและการใช้ประโยชน์จากข้อมูลดิจิทัลของหน่วยงานของรัฐและประชาชน เพื่อการกำหนดนโยบายการตัดสินใจและการบริหารงานที่เป็นประโยชน์ต่อสาธารณะ

วัตถุประสงค์

๑. เพื่อให้มีแนวทางปฏิบัติธรรมาภิบาลข้อมูลของสำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม สอดคล้องกับพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ตามกรอบธรรมาภิบาลข้อมูลภาครัฐ (Data Governance Framework for Government) ของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) รวมถึงกฎหมาย ประกาศ และระเบียบอื่น ๆ ที่เกี่ยวข้อง

๒. เพื่อกำหนดขอบเขตของธรรมาภิบาลข้อมูล การบริหารจัดการข้อมูลของสำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมในการรวบรวม ใช้ ประมวลผล และเปิดเผยข้อมูลของ สป.ดศ.

๓. เพื่อให้เป็นแนวทางในการปฏิบัติ พัฒนาและปรับปรุงธรรมาภิบาลข้อมูล รวมถึงการบริหารข้อมูลที่เหมาะสม มีประสิทธิภาพ และความคุ้มค่าตามความต้องการ ได้อย่างมั่นคงปลอดภัย

๔. เพื่อใช้เป็นแนวทางในการบริหารจัดการข้อมูลของ สป.ดศ.

ขอบเขต

แนวทางปฏิบัติธรรมาภิบาลข้อมูลของ สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเกี่ยวกับข้อมูลจัดเป็นหนึ่งในองค์ประกอบตามกรอบธรรมาภิบาลข้อมูลภาครัฐ เพื่อเป็นแนวทางให้ผู้มีส่วนได้ส่วนเสียเกี่ยวกับข้อมูลปฏิบัติตาม เพื่อให้ข้อมูลภายในหน่วยงานมีคุณภาพและมีความมั่นคงปลอดภัย ทั้งนี้ แนวปฏิบัติธรรมาภิบาลข้อมูลจะต้องสอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง หรือข้อกำหนดอื่น ๆ ที่เกี่ยวข้องมีการเผยแพร่และสื่อสารให้กับเจ้าหน้าที่ และผู้ที่เกี่ยวข้องทั้งภายในและภายนอกหน่วยงานอย่างทั่วถึงและจะต้องมีการทบทวนแนวปฏิบัตินี้อย่างสม่ำเสมอ เพื่อให้แนวปฏิบัติการดำเนินงานด้านธรรมาภิบาลข้อมูลนี้ได้ถูกนำไปปฏิบัติอย่างมีประสิทธิภาพและต่อเนื่อง

คำนิยาม

“สป.ดศ.” หมายถึง สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

“เจ้าหน้าที่” หมายถึง ข้าราชการ พนักงานราชการ ลูกจ้าง คณะบุคคลหรือผู้ปฏิบัติงานในสังกัด สป.ดศ.

“ธรรมาภิบาลข้อมูลภาครัฐ” หมายถึง การกำหนดสิทธิ หน้าที่ และความรับผิดชอบของผู้มีส่วนได้เสียในการบริหารจัดการข้อมูลภาครัฐทุกขั้นตอน เพื่อให้การได้มาและการนำข้อมูลของหน่วยงานของรัฐไปใช้อย่างถูกต้องครบถ้วน เป็นปัจจุบัน มีการรักษาความเป็นส่วนบุคคล รวมทั้งสามารถเชื่อมโยงแลกเปลี่ยน และบูรณาการระหว่างกันได้ อย่างมีประสิทธิภาพและมั่นคงปลอดภัย

“หัวหน้าหน่วยงาน” หมายถึง ปลัดกระทรวงฯ รองปลัดกระทรวงฯ ผู้ตรวจราชการกระทรวงฯ ผู้ช่วยปลัดกระทรวง ที่ปรึกษา และหัวหน้าส่วนราชการระดับ สำนักงาน/กอง/ศูนย์/กลุ่ม หรือผู้ที่ได้รับมอบหมาย

“ข้อมูล (Data)” หมายถึง สิ่งที่สื่อความหมายให้รู้เรื่องราวข้อเท็จจริงหรือเรื่องอื่นใด ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใด ๆ และไม่ว่าจะได้จัดทำไว้ในรูปของ เอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ภาพถ่ายดาวเทียม ฟิล์ม การบันทึกภาพ หรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ เครื่องมือตรวจวัด การสำรวจ ระยะไกล หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้

“หมวดหมู่ของข้อมูล (Data Category)” หมายความว่า ตามกรอบธรรมาภิบาลข้อมูลภาครัฐแบ่งออกได้เป็น ๕ หมวดหมู่ ได้แก่ ข้อมูลสาธารณะ ข้อมูลใช้ภายใน ข้อมูลส่วนบุคคล ข้อมูลความลับทางราชการ และข้อมูลความมั่นคง

“ระดับชั้นข้อมูล (Data Classification Level)” หมายความว่า ระดับชั้นข้อมูลเพื่อจัดการข้อมูลในกระบวนงานที่เกี่ยวข้องกับภารกิจ โดยข้อมูลที่มีความอ่อนไหวแบ่งระดับชั้นออกเป็น ชั้นเปิดเผย (Open) ชั้นเผยแพร่ภายในองค์กร (Private) ชั้นลับ (Confidential) ชั้นลับมาก (Secret) และ ชั้นลับที่สุด (Top Secret) ซึ่งข้อมูลที่มีระดับชั้น ลับ (Confidential) ลับมาก (Secret) และ ลับที่สุด (Top Secret) เป็นเพียงการจัดระดับชั้นข้อมูล ไม่ใช่การกำหนดให้ข้อมูลนั้นเป็นข้อมูลความลับทางราชการตามระเบียบการรักษาความลับทางราชการ

"ทีมบริกรข้อมูล (Data Stewards Team)" หมายถึง ทีมบริกรข้อมูลของ สป.ดศ. ด้านธุรกิจ ด้านเทคนิค และด้านคุณภาพข้อมูล

"บริกรข้อมูล (Data Stewards)" หมายถึง เจ้าหน้าที่ซึ่งได้รับแต่งตั้งจากคณะทำงานจัดทำธรรมาภิบาลข้อมูลของ สป.ดศ.

“ผู้รับผิดชอบที่เกี่ยวข้องกับข้อมูล (Data Agents)" หมายถึง เจ้าหน้าที่ที่ทำหน้าที่ตรวจสอบดูแลข้อมูลโดยตรง ทำการทบทวนและอนุมัติการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับข้อมูลตามธรรมาภิบาลข้อมูลตลอดวงจรชีวิตของข้อมูล รวมถึงการให้สิทธิในการเข้าถึงข้อมูลและจัดชั้นความลับของข้อมูล

“สารสนเทศ (Information)” หมายถึง ข้อมูล ข่าวสาร ในรูปแบบต่าง ๆ เช่น ตัวอักษร ตัวเลข สัญลักษณ์ รูปภาพ เสียง ที่ผ่านกระบวนการประมวลผล และบันทึกไว้อย่างเป็นระบบตามหลักวิชาการในสื่อประเภทต่าง ๆ เช่น หนังสือ วารสาร หนังสือพิมพ์ วีดีโอ ซีดีรอม ฐานข้อมูลอิเล็กทรอนิกส์ เป็นต้น เพื่อนำออกเผยแพร่ และ ใช้ประโยชน์

"วงจรชีวิตข้อมูล (Data Life Cycle)" หมายถึง ลำดับขั้นตอนของข้อมูลตั้งแต่เริ่มสร้างข้อมูลไปจนถึงการทำลายข้อมูล ตามกรอบธรรมาภิบาลข้อมูลภาครัฐ

“ชุดข้อมูล (Datasets)" หมายถึง การนำข้อมูลจากหลายแหล่งมารวบรวมเพื่อจัดเป็นชุดข้อมูล ให้ตรงตามลักษณะโครงสร้างของข้อมูล

“บัญชีข้อมูลภาครัฐ (Government Data Catalog)” หมายความว่า เอกสารแสดงบรรดารายการของชุดข้อมูลสำคัญที่รวบรวมจากบัญชีข้อมูลของหน่วยงานภาครัฐ

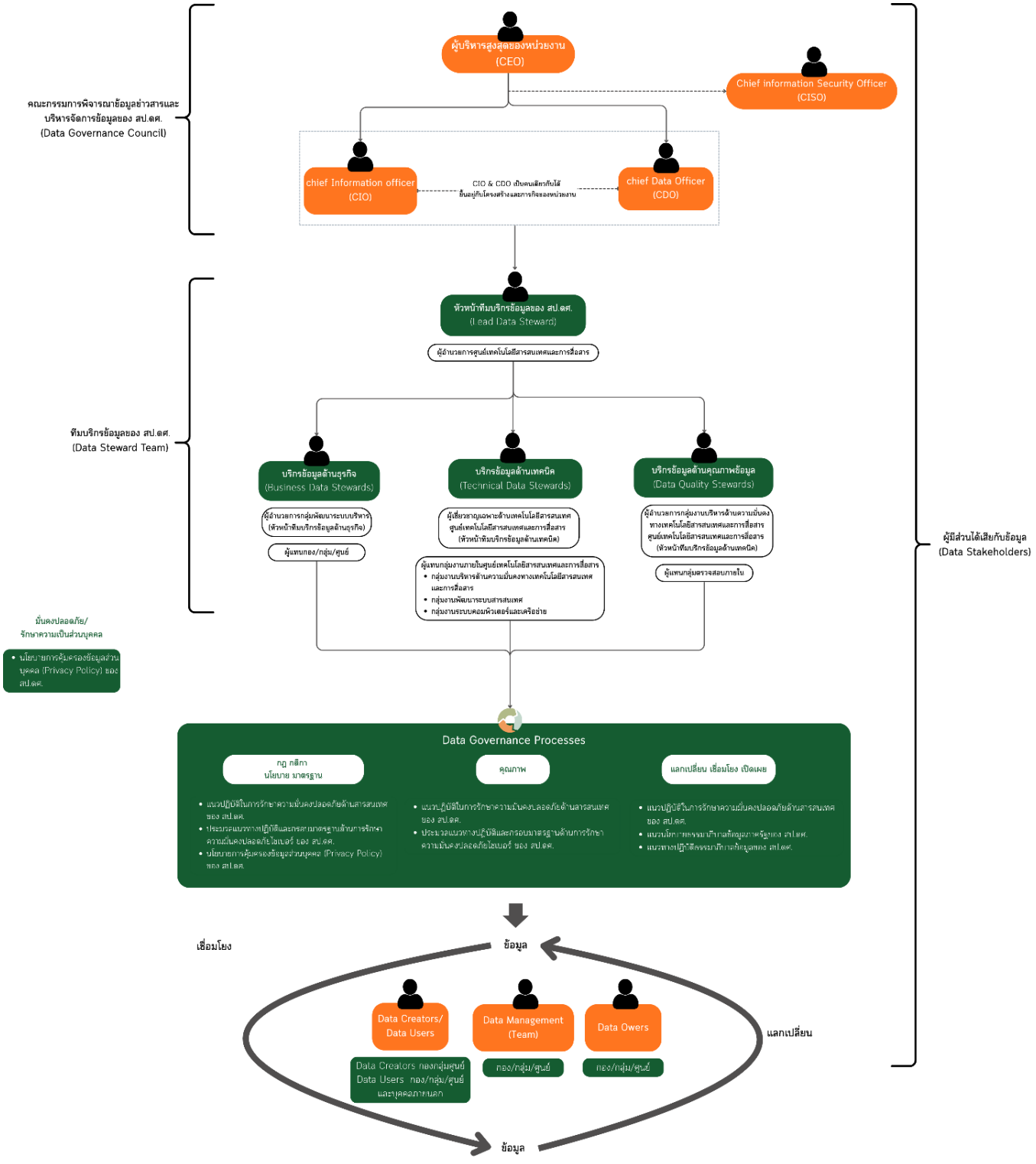
“บัญชีข้อมูล (Data Catalog)” หมายถึง เอกสารแสดงบรรดารายการของชุดข้อมูล ที่จำแนกแยกแยะโดยการจัดกลุ่มหรือจัดประเภทข้อมูลที่อยู่ในความครอบครองหรือควบคุมของหน่วยงานของรัฐ

“ข้อมูลเปิดภาครัฐ (Open Data)” หมายความว่า ข้อมูลที่หน่วยงานของรัฐต้องเปิดเผยต่อสาธารณะอย่างน้อยตามกฎหมายว่าด้วยข้อมูลข่าวสารของราชการในรูปแบบข้อมูลดิจิทัล ที่สามารถเข้าถึงและใช้ได้อย่างเสรี ไม่จำกัดแพลตฟอร์ม ไม่เสียค่าใช้จ่าย เผยแพร่ ทำซ้ำ หรือใช้ประโยชน์ได้โดยไม่จำกัดวัตถุประสงค์

“ข้อมูลแบ่งปัน (Shared data)” หมายความว่า ข้อมูลอ่อนไหวที่ได้รับการจัดระดับชั้นข้อมูล ยกเว้นในระดับชั้นลับที่สุด ซึ่งสามารถแบ่งปันและแลกเปลี่ยนกันได้ระหว่างหน่วยงาน โดยจำเป็นต้องมีการกำหนดสิทธิในการเข้าถึงและใช้งาน รวมถึงการคุ้มครองข้อมูลให้มีความมั่นคงปลอดภัย

“เมทาดาตา (Metadata)” หมายถึง ข้อมูลที่ใช้กำกับเพื่ออธิบายข้อมูลหรือกลุ่มของข้อมูลอธิบายรายละเอียดของข้อมูลหรือสารสนเทศ ทำให้ทราบรายละเอียดและคุณลักษณะข้อมูล

โครงสร้างธรรมาภิบาลข้อมูล (Data Governance Structure)



ตารางอธิบายโครงสร้างธรรมภิบาลข้อมูลของ สป.ดศ.

บทบาท	ผู้รับผิดชอบ	ความรับผิดชอบ
ผู้บริหารข้อมูลระดับสูง (Chief Data Officer)	ผู้บริหารข้อมูลระดับสูงตามที่ได้รับแต่งตั้ง	กำหนดวิสัยทัศน์ ให้ข้อเสนอแนะ อนุมัตินโยบายข้อมูล มาตรฐานข้อมูล แนวทางปฏิบัติงาน เกณฑ์การวัดคุณภาพ ระเบียบ และข้อบังคับอื่นๆ ที่เกี่ยวข้องกับข้อมูล รวมไปถึงการจัดลำดับความสำคัญและแก้ไขปัญหาที่เกี่ยวข้องกับข้อมูล
คณะกรรมการพิจารณาข้อมูลข่าวสารและบริหารจัดการข้อมูล	คณะกรรมการพิจารณาข้อมูลข่าวสารและบริหารจัดการข้อมูล	กำกับดูแล ติดตาม ตรวจสอบ รวมไปถึงการกำหนดนโยบาย กระบวนการ หลักเกณฑ์ แนวทาง มาตรการ ในการเก็บรวบรวม ใช้ เปิดเผยประมวลผล เชื่อมโยง/แลกเปลี่ยน และการบริหารจัดการข้อมูลของ สป.ดศ.
ผู้บริหารข้อมูล (Data Executive)	คณะกรรมการพิจารณาข้อมูลข่าวสารและบริหารจัดการข้อมูล	รับผิดชอบการบริหารจัดการข้อมูล ตั้งแต่การเก็บรวบรวม การใช้ การประมวลผล รวมถึงการเปิดเผยข้อมูลที่ได้รับจากทั้งหน่วยงานภายในและหน่วยงานภายนอกตามที่ สป.ดศ. กำหนด
เจ้าของข้อมูล/ ผู้ครอบครองข้อมูล (Data Owner/Possessor)	หัวหน้าส่วนราชการ ระดับ กอง/ศูนย์/กลุ่ม ที่เป็นเจ้าของข้อมูล	ตรวจสอบดูแลข้อมูลโดยตรง ทำการทบทวนและอนุมัติการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับข้อมูลตามธรรมาภิบาลข้อมูลตลอดวงจรชีวิตของข้อมูล รวมถึงการให้สิทธิในการเข้าถึงข้อมูลและจัดชั้นความลับของข้อมูล
ผู้สร้างข้อมูล (Data Creators)	บุคคล หน่วยงานระดับ กอง/ศูนย์/กลุ่ม คณะบุคคล คณะทำงาน หรือบุคคลอื่น ๆ ที่สร้างข้อมูล บันทึก แก้ไข ปรับปรุง หรือลบข้อมูล	บันทึก แก้ไข ปรับปรุง หรือลบข้อมูลให้สอดคล้องกับโครงสร้างที่ถูกกำหนดไว้ นอกจากนี้ยังมีหน้าที่ในการทำงานร่วมกับผู้ควบคุมข้อมูล ทีมบริหารจัดการข้อมูล และทีมบริกรข้อมูล เพื่อตรวจสอบและแก้ไขปัญหาด้านคุณภาพข้อมูลและความมั่นคงปลอดภัยให้สอดคล้องกับกฎ ระเบียบ นโยบาย หรือมาตรฐานข้อมูลของ สป.ดศ.
ผู้ใช้ข้อมูล (Data Users)	บุคคล หรือหน่วยงาน ทั้งภายในและภายนอก สป.ดศ.	บุคคลที่นำข้อมูลไปใช้งานตามบทบาทหน้าที่และความรับผิดชอบเพื่อวิเคราะห์ หรือวิจัย ทั้งในงานระดับปฏิบัติการและระดับบริหาร ต้องปฏิบัติตามแนวนโยบายข้อมูล มีความรับผิดชอบต่อความมั่นคงปลอดภัย การรักษาความลับ และการดำเนินการกับข้อมูลให้

บทบาท	ผู้รับผิดชอบ	ความรับผิดชอบ
		สอดคล้องกับสิทธิที่ได้รับ หากพบการรั่วไหลหรือปัญหาระหว่างการใช้ข้อมูลทั้งด้านคุณภาพและความปลอดภัย ต้องรีบแจ้งไปยังผู้ควบคุมข้อมูลดังกล่าวหรือทีมบริกรข้อมูล
ทีมบริกรข้อมูล (Data Stewards)	ทีมบริกรข้อมูล	กำกับดูแล ติดตาม และรายงานผลการดำเนินงานธรรมาภิบาลข้อมูล ครอบคลุมทั้งด้านธุรกิจ ด้านเทคนิค คุณภาพข้อมูล ความมั่นคงปลอดภัย และกฎหมาย โดยมุ่งเน้นการดำเนินงานและกำหนดมาตรฐานในการบริหารจัดการข้อมูล
ทีมบริหารจัดการข้อมูล (Data Management Team)	ทีมบริกรข้อมูล	บริหารจัดการข้อมูล ให้สอดคล้องกับองค์ประกอบ ต่อไปนี้ ● สถาปัตยกรรมข้อมูล ● การจำลองและการออกแบบข้อมูล ● การจัดเก็บและการดำเนินการกับข้อมูล ● การบูรณาการและความสามารถในการทำงานร่วมกัน ● การบริหารจัดการเอกสารและเนื้อหา ● ข้อมูลหลักและข้อมูลอ้างอิง ● คลังข้อมูล ดาตาเลค ระบบรายงานอัจฉริยะ และดาตาอนาไลติกส์ ● คำอธิบายชุดข้อมูลดิจิทัล หรือเมทาดาตา ● ความมั่นคงปลอดภัยและการรักษาความเป็นส่วนบุคคลของข้อมูล ● คุณภาพของข้อมูล รวมถึงตรวจสอบการปฏิบัติตามนโยบายข้อมูล สนับสนุนกิจกรรมของธรรมาภิบาลข้อมูล เช่น ช่วยเหลือในการนิยามเมทาดาตา (Metadata)
ผู้ควบคุมข้อมูล (Data Controller)	คณะทำงาน/คณะกรรมการ/หัวหน้าส่วนราชการระดับ กอง/ ศูนย์/กลุ่ม	ทำหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล ตามหลักธรรมาภิบาลข้อมูลภาครัฐ หรือตามข้อกำหนดกฎหมายที่เกี่ยวข้อง

วงจรชีวิตข้อมูล (Data Life Cycle)

กระบวนการธรรมาภิบาลข้อมูลภาครัฐ เป็นขั้นตอนที่ใช้สำหรับกำกับ ดูแลการดำเนินการใด ๆ ต่อข้อมูล ให้เป็นไปตามกฎ ระเบียบ ข้อบังคับ หรือนโยบายที่เกี่ยวข้องกับข้อมูล ขั้นตอนการจัดทำธรรมาภิบาลข้อมูลเริ่มตั้งแต่การวางแผนไปจนถึงการปรับปรุงอย่างต่อเนื่อง โดยมีรายละเอียดและแนวทางปฏิบัติ ดังต่อไปนี้

๑. การสร้างข้อมูล (Data Creation)

การสร้างข้อมูล (Data Creation) เป็นการสร้างข้อมูลขึ้นมาใหม่ หรือปรับปรุงข้อมูล ขึ้นใหม่ โดยวิธีการบันทึกเข้าไปด้วยบุคคลหรือบันทึกอัตโนมัติด้วยอุปกรณ์อัตโนมัติ การรับข้อมูลจากหน่วยงานอื่น เพื่อนำมาจัดเก็บทั้งข้อมูลที่เป็นกระดาษ และข้อมูลที่เป็นอิเล็กทรอนิกส์ทุกประเภท ให้ข้าราชการ เจ้าหน้าที่ ลูกจ้าง พนักงานราชการต้องปฏิบัติตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ การคุ้มครองข้อมูลส่วนบุคคล รวมทั้งกฎหมายอื่น ๆ ที่เกี่ยวข้อง โดยมีรายละเอียดดังต่อไปนี้

๑.๑ การสร้างข้อมูลต้องมี ความถูกต้อง ครบถ้วน เป็นปัจจุบัน ตรงตามความต้องการของผู้ใช้

๑.๒ หน่วยงานที่สร้างข้อมูล ต้องเป็นผู้ตรวจสอบและบันทึกข้อมูลให้ถูกต้อง ครบถ้วน ตรงกับข้อเท็จจริง รวมถึงต้องสร้างจิตสำนึกในการรับผิดชอบต่อข้อมูลที่สร้างขึ้น โดยไม่สร้างข้อมูลอันเป็นเท็จ

๑.๓ ข้อมูลที่สร้างขึ้นมาแล้วต้องกำหนดมาตรฐานการจัดเก็บข้อมูล

๒. การจัดเก็บข้อมูล (Data Store)

การจัดเก็บข้อมูล (Data Store) เป็นการจัดเก็บข้อมูลที่เกิดจากกระบวนการสร้าง หรือ ข้อมูลที่ได้จากการเชื่อมโยงและ/หรือแลกเปลี่ยนกับหน่วยงานอื่น ไม่ว่าจะจัดเก็บลงในแฟ้มข้อมูล (File) หรือ ระบบการจัดการฐานข้อมูล (Database Management System DBMS) เพื่อให้เกิดความมีระเบียบต่อการใช้งาน ข้อมูลไม่สูญหายหรือถูกทำลาย และช่วยให้ผู้ใช้งานสามารถประมวลผลข้อมูลต่าง ๆ ตามความต้องการได้อย่างรวดเร็ว

การจัดเก็บข้อมูล หมายความรวมถึง ข้อมูลทั้งที่เป็นกระดาษ และข้อมูลที่เป็นอิเล็กทรอนิกส์ทุกประเภท ไม่ว่าจะเป็นแฟ้มข้อมูลดิจิทัลทั่วไป (Digital Files) หรือแฟ้มข้อมูลที่ผ่านการประมวลผล (Information Files) หรือแฟ้มข้อมูลอื่น กล่าวคือ

๒.๑ ต้องจัดเก็บข้อมูลตามหมวดหมู่ โดย สป.ดศ. มีการกำหนดหมวดหมู่ของข้อมูล ดังนี้

๒.๑.๑ ข้อมูลสาธารณะ คือ ข้อมูลที่สามารถเปิดเผยได้ สามารถนำไปใช้ได้อย่างอิสระ ไม่ว่าจะเป็นข้อมูลข่าวสาร ข้อมูลอิเล็กทรอนิกส์ เป็นต้น

๒.๑.๒ ข้อมูลส่วนบุคคล คือ ข้อมูลเกี่ยวกับสิ่งเฉพาะตัวของบุคคล ที่ทำให้สามารถระบุตัวหรือรู้ตัวของบุคคลนั้นๆ ได้ ไม่ว่าจะเป็นข้อมูลการศึกษา ประวัติสุขภาพ ลายพิมพ์นิ้วมือ เป็นต้น

๒.๑.๓ ข้อมูลความมั่นคง คือ ข้อมูลเกี่ยวกับความมั่นคงของรัฐที่ทำให้เกิดความสงบเรียบร้อย การมีเสถียรภาพความเป็นปึกแผ่น ปลอดภัยจากการคุกคาม เป็นต้น

๒.๑.๔ ข้อมูลความลับทางราชการ คือ ข้อมูลที่อยู่ในความครอบครองหรือควบคุมดูแลของหน่วยงานของรัฐที่มีคำสั่งไม่ให้มีการเปิดเผย และมีการกำหนดชั้นความลับของข้อมูล

๒.๒ ต้องจัดเก็บข้อมูลตามชั้นความลับของข้อมูล โดย สป.ดศ.มีการจัดระดับชั้นความลับ ของข้อมูลแบ่งเป็น

๓ ชั้น ตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 ดังนี้

๒.๒.๑ ลับที่สุด หมายถึง ข้อมูลข่าวสารลับ ซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วน จะก่อให้เกิดความเสียหายแก่ประโยชน์ของรัฐอย่างร้ายแรงที่สุด

๒.๒.๒ ลับมาก หมายถึง ข้อมูลข่าวสารลับ ซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วน จะก่อให้เกิดความเสียหายแก่ประโยชน์ของรัฐอย่างร้ายแรง

๒.๒.๓ ลับ หมายถึง ข้อมูลข่าวสารลับ ซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วน จะก่อให้เกิดความเสียหายแก่ประโยชน์ของรัฐ

๒.๓ การจัดเก็บแฟ้มข้อมูลลับ ให้ปฏิบัติ ดังนี้

๒.๓.๑ ผู้ที่เป็นเจ้าของแฟ้มข้อมูลลับต้องตรวจสอบความถูกต้องของแฟ้มข้อมูลลับ ก่อนนำไปใช้งาน

๒.๓.๒ ต้องป้องกันแฟ้มข้อมูลลับที่มีการจัดเก็บไว้ในเครื่องคอมพิวเตอร์ที่ตนเองใช้งาน โดยเครื่องคอมพิวเตอร์ต้องมีการตั้งรหัสผ่าน หรือมีระบบรักษาความมั่นคงปลอดภัยตามที่ สป.ดศ.กำหนด และเมื่อมีการนำแฟ้มข้อมูลลับไปใช้งาน ให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ อย่างเคร่งครัด

๒.๓.๓ ต้องระมัดระวังใช้งานแฟ้มข้อมูลลับ การกระจาย หรือแจกจ่ายแฟ้มข้อมูลลับ ของ สป.ดศ.ไปยังกลุ่มผู้รับที่มีสิทธิหรือได้รับอนุญาตเท่านั้น

๒.๔ การจัดทำสำเนา การแปล การโอน การส่ง การรับ การเก็บรักษา การยืม การทำลาย และการเปิดเผยแฟ้มข้อมูลลับ ให้เป็นไปตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔

๒.๕ การจัดเก็บข้อมูลส่วนบุคคล ให้เก็บรวบรวมได้เท่าที่จำเป็น ภายใต้อำนาจหน้าที่และ วัตถุประสงค์อันชอบตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

๓. การประมวลผลข้อมูลและการใช้ข้อมูล (Data Processing and Use)

การประมวลผลข้อมูลและการใช้ข้อมูล (Data Processing and Use) เพื่อให้การประมวลผลข้อมูลและการใช้ข้อมูลที่มีประสิทธิภาพ ถูกต้อง ตรงตามวัตถุประสงค์ของการใช้ข้อมูลให้เกิดประโยชน์ รวมถึงวิธีการและแนวทางในการขอข้อมูลจากหน่วยงานต่าง ๆ ให้ดำเนินการ ดังนี้

๓.๑ การนำข้อมูลไปประมวลผลและการใช้ข้อมูลจะต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อน หรือเป็นไปตามข้อยกเว้นของกฎหมายที่เกี่ยวข้อง

๓.๒ การนำข้อมูลที่เป็นความลับไปประมวลผลข้อมูล ให้เป็นไปตาม เงื่อนไขหรือวัตถุประสงค์ในการยินยอมให้ดำเนินการกับข้อมูลนั้น หรือเป็นไปตามข้อยกเว้นของกฎหมายที่เกี่ยวข้อง

๓.๓ ต้องมีการบันทึกประวัติการประมวลผลและการใช้ข้อมูลเพื่อให้สามารถตรวจสอบย้อนหลังได้

๓.๔ ผู้ใช้ข้อมูลต้องเป็นผู้รับผิดชอบ หากมีการประมวลผลข้อมูลและการใช้ข้อมูลที่ไม่เป็นไป ตามกฎหมายกำหนด

๔. การเปิดเผยข้อมูลและการขอใช้ข้อมูล (Data Disclosure)

การเปิดเผยข้อมูลและการขอใช้ข้อมูล (Data Disclosure) เป็นการนำข้อมูลที่มีอยู่ในความครอบครองของหน่วยงาน เผยแพร่ตามช่องทางต่าง ๆ อย่างเหมาะสม อาทิ การเปิดเผยข้อมูล (Open Data) การแชร์ข้อมูล (Share) การควบคุมการเข้าถึง (Access Control) การแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน (Exchange) และการกำหนดเงื่อนไขในการนำข้อมูลไปใช้ (Condition) ให้ดำเนินการ ดังนี้

๔.๑ คัดเลือกข้อมูลที่ต้องการเผยแพร่ให้ปฏิบัติ ดังนี้

๔.๑.๑ เจ้าของข้อมูลและหน่วยงานที่เกี่ยวข้องต้องพิจารณาข้อมูลที่จะเผยแพร่ โดยข้อมูลที่สามารถเผยแพรได้ จะต้องไม่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ คำสั่งของ สป.ดศ.

๔.๑.๒ ข้อมูลในการเปิดเผยควรเป็นข้อมูลที่สามารถเปิดเผยได้ และไม่ละเมิด ข้อมูลส่วนบุคคล เช่น ข้อมูลเชิงสถิติที่ไม่สามารถระบุตัวบุคคลได้ เป็นต้น

๔.๑.๓ กรณีเป็นข้อมูลส่วนบุคคล และเข้าถึงรายบุคคล โดยจำเป็นต้องใช้ฐานความยินยอม หน่วยงานที่ขอใช้ จะต้องได้รับการยินยอมจากเจ้าของข้อมูลก่อน พร้อมทั้ง แจ้งผลการตอบรับการยินยอมไปยังหน่วยงานที่ถือครองข้อมูล และในกรณีเป็นข้อมูลส่วนบุคคลอาจยินยอมให้เข้าถึงบางส่วนหรือทั้งหมดตามที่ขอ โดยหน่วยงานที่ถือครองข้อมูล ต้องมีมาตรการปกปิดไม่ให้หน่วยงานที่ขอใช้ข้อมูลทราบได้ว่าข้อมูลแต่ละรายการเป็นของบุคคลใด

๔.๒ การพิจารณาชุดข้อมูลที่คัดเลือก ต้องมีรายละเอียดที่อธิบายถึงความเป็นมาของข้อมูล เช่น ชื่อข้อมูล คำอธิบายข้อมูล คำสำคัญ วันที่ทำการเปลี่ยนแปลงข้อมูลล่าสุด ชื่อหน่วยงานเจ้าของข้อมูลและ ฟิลด์ข้อมูล ทั้งนี้ต้องตรวจสอบฟิลด์ข้อมูลว่าครบถ้วนสอดคล้องกับความต้องการของหน่วยงานที่ขอใช้ข้อมูล

๔.๓ การจัดเตรียมข้อมูลให้อยู่ในรูปแบบที่ง่ายต่อการนำไปใช้ ให้ปฏิบัติ ดังนี้

๔.๓.๑ ข้อมูลมีความพร้อมในการส่งต่อหรือเปิดเผยได้

๑) ต้องมีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย การเข้าถึง การใช้ การเปลี่ยนแปลง การแก้ไข หรือการเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบด้วยประการใด ๆ

๒) กรณีที่ต้องให้ข้อมูลส่วนบุคคลแก่บุคคลหรือหน่วยงานอื่นที่มิใช่ผู้ควบคุม ข้อมูลส่วนบุคคลต้องดำเนินการเพื่อป้องกันมิให้ผู้นั้นนำไปใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจ หรือโดยมิชอบด้วยประการใด ๆ

๓) ต้องมีระบบตรวจสอบ/แนวปฏิบัติเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคล เมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือที่ไม่เกี่ยวข้อง หรือเกินความจำเป็น ตามวัตถุประสงค์ในการเก็บรวบรวม ข้อมูลส่วนบุคคลนั้น หรือตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ

๔.๓.๒ การเชื่อมโยงข้อมูลที่มีการจัดเก็บและสามารถเข้าถึงได้ เพื่อตรวจสอบ หรือ เปิดเผยแก่ผู้ที่เกี่ยวข้อง

๔.๔ การนำชุดข้อมูลขึ้นเผยแพร่ ให้ดำเนินการ ดังนี้

๔.๔.๑ เก็บประวัติ (Log) การเปิดเผยแพร่ข้อมูล เพื่อให้สามารถตรวจสอบได้ และเป็นไปตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

๔.๔.๒ มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย การเข้าถึง การใช้ การเปลี่ยนแปลง การแก้ไขโดยมิชอบด้วยประการใด ๆ

๔.๕ การควบคุมสิทธิ์การเข้าถึงข้อมูล (Access Control) เพื่อให้การเข้าถึงและการใช้ข้อมูลเป็นไปอย่างปลอดภัย โปร่งใส และสามารถตรวจสอบได้ สป.ดศ.กำหนดแนวทางการควบคุมสิทธิ์การเข้าถึงข้อมูล ดังนี้

๔.๕.๑ การควบคุมสิทธิ์การเข้าถึงข้อมูลกำหนดให้อนุญาตเฉพาะผู้ที่มีความจำเป็นต้องใช้ข้อมูลตามหน้าที่ (Need-to-know) โดยการกำหนดสิทธิ์อิงตามบทบาทหน้าที่ของผู้ใช้งาน (Role-Based Access Control: RBAC) และข้อมูลทุกชุดต้องได้รับการจัดประเภทพร้อมกำหนดระดับความลับอย่างเหมาะสม (Classification and

Confidentiality Level)

๔.๕.๒ การร้องขอและอนุมัติสิทธิ์ให้ผู้ขอใช้ข้อมูลต้องดำเนินการยื่นคำขอใช้งานพร้อมระบุเหตุผลความจำเป็น โดยเจ้าของหรือผู้ครอบครองข้อมูลจะเป็นผู้พิจารณาอนุมัติสิทธิ์ และต้องจัดเก็บประวัติการให้สิทธิ์ (Audit Trail) เพื่อสามารถตรวจสอบย้อนหลังได้

๔.๕.๓ การทบทวนและเพิกถอนสิทธิ์ ให้ผู้สิทธิ์การเข้าถึงข้อมูลต้องได้รับการทบทวนอย่างน้อยปีละหนึ่งครั้ง และจะต้องเพิกถอนทันทีเมื่อเจ้าหน้าที่มีการเปลี่ยนบทบาทหน้าที่หรือพ้นจากตำแหน่ง เพื่อป้องกันการเข้าถึงโดยมิชอบ

๔.๕.๔ การกำกับดูแลและตรวจสอบให้การเข้าถึงและใช้งานข้อมูลต้องมีการบันทึกและตรวจสอบผ่านระบบ Access Log โดยหากพบการใช้งานที่ผิดปกติหรือไม่เป็นไปตามนโยบาย จะต้องรายงานต่อคณะกรรมการบริหารจัดการข้อมูลเพื่อดำเนินการตามความเหมาะสม

๔.๕.๕ การให้สิทธิ์แบบแบ่งระดับให้การกำหนดสิทธิ์การเข้าถึงข้อมูลต้องพิจารณาตามระดับความอ่อนไหวของข้อมูล เช่น การเข้าถึงเฉพาะเมทาดาตา การเข้าถึงข้อมูลที่ไม่สามารถระบุตัวบุคคลได้ หรือการเข้าถึงข้อมูลฉบับเต็มภายใต้การควบคุมที่เข้มงวด

๕. กระบวนการจัดเก็บข้อมูลถาวร (Archive)

กระบวนการจัดเก็บข้อมูลถาวร (Archive) เป็นการย้ายข้อมูลที่มีช่วงอายุเกินช่วงการใช้งาน หรือไม่ได้ใช้งานแล้ว เพื่อเก็บรักษาถาวรโดยที่ข้อมูลนั้นไม่มีการลบ ปรับปรุง หรือแก้ไขอีก แต่สามารถนำกลับไปใช้งานได้ใหม่เมื่อต้องการ การจัดเก็บข้อมูลถาวร ให้ปฏิบัติ ดังนี้

๕.๑ กำหนดเครื่องมือและวิธีการที่จะใช้ในการจัดเก็บข้อมูล

๕.๒ กำหนดระยะเวลาในการจัดเก็บข้อมูลแต่ละประเภท

๕.๓ ต้องประสานความร่วมมือกับหน่วยงานที่เกี่ยวข้อง เพื่อกำหนดระยะเวลาในการ จัดเก็บข้อมูลที่เหมาะสมกับข้อมูลแต่ละประเภท

๕.๔ สร้างความรู้ความเข้าใจในการจัดเก็บข้อมูลแก่ผู้ที่เกี่ยวข้อง

๕.๕ ศึกษาข้อมูลที่ต้องจัดเก็บ โดยเลือกเครื่องมือและกระบวนการที่เป็นมาตรฐานในการ จัดเก็บข้อมูล ให้อยู่ในสภาพที่พร้อมใช้งานได้ตลอดเวลา

๖. การทำลายข้อมูล (Data Destruction)

การทำลายข้อมูล (Data Destruction) เป็นการทำลายข้อมูลที่มีการจัดเก็บถาวร เป็นระยะเวลานานหรือเกินกว่าระยะเวลากำหนด การทำลายข้อมูล ให้ปฏิบัติ ดังนี้

๖.๑ ให้กำหนดขั้นตอนและวิธีการทำลายข้อมูล

๖.๒ ต้องประสานความร่วมมือกับหน่วยงานที่เกี่ยวข้อง กำหนดวิธี ปฏิบัติการทำลายข้อมูล

๖.๓ หน่วยงานที่ได้รับมอบหมายต้องจัดประชุม/อบรม/ประชาสัมพันธ์ ให้ส่วนเกี่ยวข้อง มีความรู้ความเข้าใจวิธีปฏิบัติการทำลายข้อมูล

๖.๔ หน่วยงานที่เกี่ยวข้อง ต้องกำหนดสิทธิ์ของผู้ที่จะดำเนินการทำลายข้อมูลและ เก็บประวัติไว้ด้วยทุกครั้ง

๖.๕ หน่วยงานที่เกี่ยวข้องต้องอบรมชี้แจงให้ผู้ปฏิบัติและผู้ที่เกี่ยวข้อง มีความรู้ความเข้าใจ ในการจัดเก็บและทำลายข้อมูล ทั้งภายในและภายนอกหน่วยงาน

๖.๖ สร้างความรู้ความเข้าใจในการทำลายข้อมูลแก่ผู้ที่เกี่ยวข้อง

การเชื่อมโยงและแลกเปลี่ยนข้อมูล (Data Linkage and Exchange)

เพื่อให้การแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน มีความถูกต้อง ครบถ้วน ปลอดภัย และมีประสิทธิภาพ โดยมีวิธีและแนวทางการนำข้อมูลไปเชื่อมโยงและแลกเปลี่ยนกับหน่วยงานภายนอก ต้องสอดคล้องกับระเบียบ หลักเกณฑ์และกฎหมายที่กำหนด

๑. กำหนดเทคโนโลยีและมาตรฐานทางเทคนิคที่ใช้ในการแลกเปลี่ยน/เชื่อมโยงข้อมูล

๒. การเชื่อมโยงและการแลกเปลี่ยนข้อมูลของ สป.ดศ.กับหน่วยงานอื่น ๆ จะต้องได้รับอนุญาต จาก สป.ดศ. และต้องมีการกำหนดความร่วมมือ หรือแนวทางในด้านการบริหารจัดการข้อมูลร่วมกับ หน่วยงานนั้น ๆ อย่างชัดเจน เช่น บันทึกข้อตกลง (Memorandum of Understanding: MOU) สัญญารักษาความลับ (Non-Disclosure Agreement: NDA) เป็นต้น

๓. การเชื่อมโยงและการแลกเปลี่ยนข้อมูล ต้องมีการรักษาความมั่นคงปลอดภัยของข้อมูล ข้อมูลส่วนบุคคล โดยให้เป็นไปตามที่กฎหมายกำหนด

การจัดทำบัญชีข้อมูลของหน่วยงาน (Data Catalog)

๑. เจ้าของข้อมูลหรือผู้ครอบครองข้อมูลมีหน้าที่กำหนดให้มีผู้รับผิดชอบที่เกี่ยวข้องกับข้อมูลของหน่วยงาน

๒. ผู้รับผิดชอบที่เกี่ยวข้องกับข้อมูล มีหน้าที่กำหนดคำนิยามของชุดข้อมูล (List of Data) โดยอย่างน้อยต้องมีในเรื่อง ดังต่อไปนี้

๒.๑ ความสัมพันธ์ของข้อมูล ได้แก่ หน่วยงานใดเป็นเจ้าของข้อมูล หน่วยงานใดเป็นผู้ใช้ข้อมูล

๒.๒ รูปแบบการจัดเก็บไฟล์ข้อมูล เช่น ไฟล์เอกสาร หรือแฟ้มกระดาษ

๒.๓ ความพร้อมของชุดข้อมูล เช่น ชั้นข้อมูล ความครบถ้วนถูกต้อง สมบูรณ์ พร้อมใช้ ความถี่ในการนำเข้าหรือจัดทำข้อมูล

๒.๔ ความพร้อมในการเชื่อมโยงและแลกเปลี่ยนข้อมูล เช่น เปิดให้ใช้งานสาธารณะหรือใช้งานเฉพาะภายในหน่วยงาน ชุดข้อมูลอยู่ในรูปแบบมาตรฐานพร้อมเชื่อมโยงหรือแลกเปลี่ยนหรือไม่

๓. ผู้รับผิดชอบที่เกี่ยวข้องกับข้อมูล มีหน้าที่กำหนดพจนานุกรมข้อมูล (Data Dictionary) อาทิเช่น

๓.๑ เลขที่เมทาดาตา (Metadata ID)

๓.๒ ชื่อชุดข้อมูล (Dataset Name)

๓.๓ เลขที่ข้อมูล (Data ID)

๓.๔ ชื่อตารางข้อมูล (Table Name)

๓.๕ ชื่อฟิลด์ข้อมูล (Field)

๓.๖ คำอธิบายฟิลด์ (Description)

๓.๗ ระดับชั้นความลับ (Classification)

๓.๘ ประเภทข้อมูล (Data Type)

๓.๙ ขนาดข้อมูล (Data Size)

๓.๑๐ คุณลักษณะข้อมูล (Characteristic Type)

๓.๑๑ แหล่งที่มาของค่าที่ระบุในฟิลด์ (Data Source)

๓.๑๒ รูปแบบ (Data Format)

๓.๑๓ เงื่อนไข (Condition)

การประเมินผลการกำกับดูแลข้อมูล (Data Governance Assessment)

เกณฑ์การประเมินผลการกำกับดูแลข้อมูล ให้ดำเนินการตามมิติคุณภาพข้อมูล ๕ มิติ ได้แก่ (๑) ความถูกต้อง (๒) ความสอดคล้องกัน (๓) ตรงตามความต้องการของผู้ใช้ (๔) ความเป็นปัจจุบัน และ (๕) ความพร้อมใช้ที่สอดคล้องตามองค์ประกอบในการประเมินผลการกำกับดูแลข้อมูลตามกรอบธรรมาภิบาลข้อมูลภาครัฐ โดยแต่ละมิติมีรายละเอียดและตัวชี้วัด (Indicators) ดังนี้

การกำกับดูแล	รายละเอียดการประเมินผลการกำกับดูแล	รายการตัวชี้วัด
กำกับดูแลข้อมูลให้มีความถูกต้องและสมบูรณ์ (Accuracy and Completeness)	ประเมินเรื่องความถูกต้องแม่นยำ แหล่งข้อมูลที่น่าเชื่อถือ และมีกระบวนการตรวจสอบ	• มีแหล่งข้อมูลที่น่าเชื่อถือ • มีกระบวนการหรือเครื่องมือตรวจสอบจุดผิดพลาดของข้อมูล • มีการตรวจสอบความครบถ้วนของข้อมูล • มีวิธีเก็บข้อมูลมีความเป็นกลาง น่าเชื่อถือ และไม่สร้างข้อมูลที่มีอคติ • มีการระบุคำนิยามและลักษณะข้อมูลที่ต้องการ
กำกับดูแลข้อมูลให้มีความสอดคล้องกัน (Consistency)	ประเมินเรื่องรูปแบบของข้อมูล ความสอดคล้องกัน และมาตรฐานในการจัดทำข้อมูลของหน่วยงาน	• มีการเก็บข้อมูลภายใต้มาตรฐานข้อมูลเดียวกันหรือมาตรฐานข้อมูลที่สอดคล้องกัน ทำให้สามารถใช้ประโยชน์ข้อมูลร่วมกันได้ • มีการตรวจสอบรูปแบบข้อมูลภายในชุดข้อมูลเดียวกันข้อมูลมีความเชื่อมโยงและไม่ขัดแย้งกัน • มีการใช้กฎ วิธีการตรวจวัดที่สอดคล้องกัน ทั้งหน่วยงาน รวมถึงหน่วยงานภายนอก • มีการกำหนดบทบาทและผู้รับผิดชอบข้อมูล
กำกับดูแลข้อมูลให้มีตรงตามความต้องการของผู้ใช้ (Relevancy)	ประเมินว่า เป็นข้อมูลที่ผู้ใช้ต้องการ หรือเป็นข้อมูลที่จำเป็นต้องทราบ มีความละเอียดเพียงพอต่อนำไปใช้งาน	• ข้อมูลตรงตามความต้องการและวัตถุประสงค์ของการใช้งาน • มีการปรับปรุงคุณภาพให้ตรงตามความต้องการของผู้ใช้
กำกับดูแลข้อมูลให้มีความเป็นปัจจุบัน (Timeliness)	ประเมินเรื่องการเผยแพร่ข้อมูล การปรับปรุงข้อมูล และแผนเรื่องระยะเวลา	• ข้อมูลมีการเผยแพร่ส่งต่อตรงเวลา/เวลาที่เหมาะสม • ข้อมูลมีความเป็นปัจจุบัน

การกำกับดูแล	รายละเอียดการประเมินผลการกำกับดูแล	รายการตัวชี้วัด
กำกับดูแลข้อมูลให้มีความพร้อมใช้ (Availability)	ประเมินความพร้อมใช้ของข้อมูล รวมไปถึงช่องทางในการขอหรือใช้ข้อมูล	• ข้อมูลถูกจัดในรูปแบบที่พร้อมนำไปใช้งาน และเหมาะสมกับผู้ใช้งาน • มีการเผยแพร่ข้อมูลที่เหมาะสมและสามารถเข้าถึงได้ โดยผู้ใช้สามารถเข้าถึงข้อมูลได้สะดวกตามสิทธิที่เหมาะสม • ข้อมูลสามารถอ่านด้วยโปรแกรมคอมพิวเตอร์ได้ • มีคำอธิบายข้อมูลที่ชัดเจน