นโยบายธรรมาภิบาลข้อมูล

Data Governance Policy

จังหวัดสิงห์บุรี







คำนำ

ปัจจุบันองค์กรทั่วโลกต่างให้ความสำคัญกับการรวบรวม จัดการ และใช้ประโยชน์จากข้อมูลเพิ่มมากขึ้นเรื่อย ๆ เพื่อปรับปรุงบริการหลักของตน อีกทั้งจำเป็นปฏิบัติตามข้อกฎหมาย กฎระเบียบและมาตรฐานการกำกับดูแลที่เพิ่มมากขึ้น เนื่องจากตระหนักดีว่าข้อมูลถือเป็นสินทรัพย์ที่สำคัญ (Data as Asset) ที่จะช่วยเพิ่มประสิทธิภาพในการทำงาน ช่วยในการวิเคราะห์ วางแผนและตัดสินใจเชิงนโยบาย และอำนวยความสะดวก ในการให้บริการ ส่งผลให้องค์กรจำเป็นต้องมีกระบวนการป้องกันความปลอดภัยของข้อมูล โดยมีขั้นตอนสำคัญคือการจำแนกหมวดหมู่และจัดชั้นความลับของข้อมูล เพื่อรับทราบการเข้าถึงและใช้ข้อมูล การลดความเสี่ยงภัยที่จะเกิดกับข้อมูล และการระบุชั้นความลับของข้อมูลจะช่วยให้หน่วยงานสามารถแบ่งปันข้อมูลทั้งภายในและภายนอกองค์กรได้ ดังนั้น การกำกับดูแลข้อมูลที่ดีต้องการให้องค์กรรักษาประสิทธิภาพ การทำงานได้เพิ่มมากขึ้น ในขณะเดียวกันต้องมีการจัดการข้อมูลอ่อนไหว (Sensitive Data) อย่างเหมาะสมและเป็นไปตามข้อกฎหมายที่เกี่ยวข้อง ประกอบกับจังหวัดสิงห์บุรีมีการบริหารและกระบวนการจัดการและคุ้มครองข้อมูลที่ครบถ้วน ตั้งแต่การจัดทำ การจัดเก็บ การจำแนกหมวดหมู่ การประมวลผลหรือใช้ข้อมูล การปกปิดหรือเปิดเผยข้อมูล การตรวจสอบ และการทำลาย ซึ่งเป็นไปตามมาตรา 8 แห่งพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 และประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัลเรื่อง ธรรมาภิบาลข้อมูลภาครัฐ ข้อ 4 (5) จำแนกหมวดหมู่ของข้อมูล เพื่อกำหนดนโยบายข้อมูลหรือกฎเกณฑ์เกี่ยวกับผู้มีสิทธิเข้าถึงและใช้ประโยชน์จากข้อมูลต่าง ๆ ภายในหน่วยงาน สำหรับให้ผู้ซึ่งมีหน้าที่เกี่ยวข้องปฏิบัติตามนโยบายหรือกฎเกณฑ์ได้อย่างถูกต้อง และสอดคล้องตามกฎหมายที่เกี่ยวข้อง อันจะนำไปสู่การบริหารจัดการข้อมูลภาครัฐอย่างเป็นระบบ อันจะนำไปสู่การพัฒนาระบบข้อมูลที่สำคัญของจังหวัด เพื่อประโยชน์ในการกำหนดหลักเกณฑ์และวิธีการเชื่อมโยง แลกเปลี่ยน และบูรณาการข้อมูลของหน่วยงานของรัฐอย่างเป็นระบบ ตลอดจนการพัฒนาศูนย์กลางข้อมูลเปิดภาครัฐเพื่อให้ประชาชนสามารถเข้าถึงและใช้ประโยชน์ได้อย่างมีประสิทธิภาพ

จากการประชุม คณะกรรมการธรรมาภิบาลข้อมูล ครั้งที่ 1/2569 เมื่อวันที่ 7 มกราคม 2569 ที่ประชุมมีมติเห็นชอบการปรับปรุง นโยบายธรรมาภิบาลข้อมูล (Data Governance Policy) จังหวัดสิงห์บุรี และกำหนดแนวปฏิบัติในการธรรมาภิบาลข้อมูล จึงได้จัดทำเอกสารฉบับนี้ขึ้น เพื่อใช้เป็นแนวทางในการดำเนินงานกำกับ ดูแล และบริหารจัดการข้อมูลของจังหวัดสิงห์บุรีทุกขั้นตอนได้อย่างเป็นระบบและมีความชัดเจนมากยิ่งขึ้น

นโยบายธรรมาภิบาลข้อมูล (Data Governance Policy) จังหวัดสิงห์บุรี

หลักการ

จังหวัดสิงห์บุรี เป็นส่วนราชการที่รับผิดชอบการให้บริการสาธารณะ โดยคำนึงถึงประโยชน์ของประชาชนเป็นสำคัญ เป็นไปตามพระราชบัญญัติปรับปรุงกระทรวง ทบวง กรม พ.ศ. ๒๕๔๕ และเพื่อให้ดำเนินงานสอดคล้องกับพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ รวมทั้งกฎหมายที่เกี่ยวข้อง

ขอบเขต (SCOPE)

ขอบเขตของนโยบายนี้ครอบคลุมวงจรชีวิตของข้อมูล (Data Life Cycle) และกระบวนการธรรมาภิบาลข้อมูล (Data Governance Process) การดำเนินงานตามภารกิจของจังหวัดสิงห์บุรี และมีผลบังคับใช้ไปถึงบุคลากร และ/หรือหน่วยงานภายในทั้งหมด ได้แก่ ผู้บริหาร ข้าราชการ พนักงานประจำ ลูกจ้างประจำ ลูกจ้างชั่วคราวผู้มีส่วนได้ส่วนเสีย เป็นต้น

วัตถุประสงค์

นโยบายธรรมาภิบาลข้อมูลของจังหวัดสิงห์บุรี เพื่อให้จังหวัดสิงห์บุรี มีนโยบายธรรมาภิบาลข้อมูลและบริหารจัดการข้อมูลอย่างเหมาะสมเพียงพอสอดคล้องกับภารกิจของหน่วยงาน ครอบคลุมโครงสร้างธรรมาภิบาลข้อมูล บทบาทและหน้าที่ความรับผิดชอบของผู้บริหารระดับสูง หน่วยงาน บุคลากรที่เกี่ยวข้อง

คำนิยาม (DEFINITIONS)

ข้อมูล	สิ่งที่สื่อความหมายให้รู้เรื่องราว ข้อเท็จจริง ข้อมูลหรือ สิ่งใด ๆ ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเอง หรือโดยผ่านวิธีการใด ๆ และไม่ว่าจะได้จัดทำไว้ในรูปแบบของเอกสาร แฟ้ม รายงาน หนังสือแผนผังแผนที่ ภาพวาด ภาพถ่าย ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้
ชุดข้อมูล	ข้อมูลที่รวบรวมมาจากหลายแหล่ง โดยจัดเป็นชุดให้ตรงตามลักษณะโครงสร้างของข้อมูล
ธรรมาภิบาลข้อมูลภาครัฐ	การกำหนดสิทธิในการตัดสินใจและความรับผิดชอบ ในการส่งเสริมให้เกิดกระบวนการจัดทำ การใช้งาน และการบริหารจัดการข้อมูล รวมถึงกระบวนการที่กำหนดบทบาท นโยบาย และมาตรฐานที่ช่วยสนับสนุนให้การดำเนินงานเกี่ยวกับข้อมูลมีประสิทธิภาพมากยิ่งขึ้น ซึ่งส่งผลให้หน่วยงานสามารถบรรลุเป้าหมายได้
คณะกรรมการธรรมาภิบาลข้อมูล	กลุ่มบุคคลที่มีอำนาจในการผลักดันให้เกิดธรรมาภิบาลข้อมูล โดยมีหน้าที่รับผิดชอบในการกำหนดเป้าหมาย กำกับดูแลและติดตามการดำเนินงาน รวมถึงให้คำปรึกษาและตัดสินประเด็นสำคัญที่เกี่ยวข้องกับข้อมูล สนับสนุน ส่งเสริม ผลักดันธรรมาภิบาลข้อมูลและการสื่อสารให้บุคลากรในจังหวัดตระหนักถึงความสำคัญของข้อมูล การใช้ข้อมูลอย่างปลอดภัย
คณะทำงานทีมบริกรข้อมูล	กลุ่มบุคคลที่มุ่งเน้นการดำเนินงานและนิยามคำอธิบายชุดข้อมูลทั้ง ร่างนโยบาย กำหนดมาตรฐาน ตรวจสอบการปฏิบัติงานวิเคราะห์ผลจากการตรวจสอบ ในการบริหารจัดการตามองค์ประกอบของการบริหารจัดการข้อมูล

ข้อมูลส่วนบุคคล	ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ
ข้อมูลที่เป็นเอกสาร	ข้อมูลที่มีการจัดเก็บและบันทึกในรูปแบบของกระดาษ
ข้อมูลที่ไม่เป็นเอกสาร	ข้อมูลสารสนเทศ ข้อมูลคอมพิวเตอร์ ข้อมูลอิเล็กทรอนิกส์
เจ้าของข้อมูล (Data Owner)	บุคคล/คณะบุคคลที่ทำหน้าที่รับผิดชอบดูแลข้อมูลโดยตรง เพื่อสร้างความมั่นใจได้ว่าการบริหารจัดการข้อมูลสอดคล้องกับนโยบาย มาตรฐาน กฎระเบียบ หรือกฎหมาย โดยเจ้าของข้อมูลทำการทบทวนและอนุมัติการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับข้อมูล เช่น การเปลี่ยนแปลงเมทาดาตาและเกณฑ์การทำข้อมูลให้ถูกต้องสมบูรณ์ (Data Cleansing) นอกจากนี้ ยังมีหน้าที่ในการให้สิทธิในการเข้าถึงข้อมูลและการจัดระดับชั้นข้อมูล เจ้าของข้อมูลส่วนใหญ่อยู่ในตำแห
ผู้ควบคุมข้อมูลส่วนบุคคล	บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
ผู้ประมวลผลข้อมูลส่วนบุคคล	บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล
ผู้ดูแลข้อมูล	ผู้ที่ทำงานร่วมกับเจ้าของข้อมูลโดยตรง ทำหน้าที่จัดเก็บรักษาข้อมูล รวมถึงป้องกันภัยคุกคาม ทำการสำรองข้อมูล ดำเนินการตามขั้นตอนที่ระบุไว้ในนโยบายและแผนงานความมั่นคงปลอดภัย ทั้งทางด้านระบบสารสนเทศและที่มิใช่สารสนเทศ
ผู้ใช้ข้อมูล	ผู้ที่ได้รับสิทธิการใช้ข้อมูลจากผู้รับผิดชอบ หรือได้รับมอบหมายให้ใช้ข้อมูลจากผู้บังคับบัญชา รวมถึงผู้ซึ่งได้รับความยินยอมให้ทำงานหรือทำผลประโยชน์ให้แก่หน่วยงาน
ระดับชั้นความลับ	การกำหนดการเปิดเผยข้อมูลต่อผู้อื่นให้เหมาะสมกับสถานะการใช้งาน ได้แก่ ลับที่สุด ลับมาก ลับ ปกปิด และเปิดเผยสู่ภายนอกได้
ความมั่นคงปลอดภัยของข้อมูล	การธำรงไว้ซึ่งความลับ ความถูกต้องครบถ้วน และการรักษาสภาพพร้อมใช้ของข้อมูล รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง ความรับผิด การห้าม ปฏิเสธความรับผิด และความน่าเชื่อถือ
เมทาดาตา (Metadata)	คำอธิบายชุดข้อมูลดิจิทัล เพื่อให้ทราบรายละเอียดเกี่ยวกับโครงสร้างของข้อมูล เนื้อหาสาระ รูปแบบการจัดเก็บ แหล่งข้อมูล และสิทธิในการเข้าถึงข้อมูล
บัญชีข้อมูลภาครัฐ (Government Data Catalog)	เอกสารแสดงบรรดารายการของชุดข้อมูลสำคัญที่รวบรวมจากบัญชีข้อมูลของหน่วยงานภาครัฐ

นโยบายธรรมาภิบาลข้อมูล (Data Governance Policy)

วัตถุประสงค์

เพื่อกำหนดแนวทางการดำเนินงานด้านธรรมาภิบาลข้อมูล เนื่องจากการกำหนดนโยบายข้อมูลจัดเป็นหนึ่งในองค์ประกอบตามกรอบการธรรมาภิบาลข้อมูล และให้การบริหารจัดการข้อมูลมีประสิทธิภาพ จึงต้องมีการกำหนดนโยบายที่ระบุอย่างชัดเจน สอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง หรือข้อกำหนดอื่น ๆ ที่เกี่ยวข้อง เพื่อให้นโยบายข้อมูลได้ถูกนำมาปฏิบัติอย่างมีประสิทธิภาพและต่อเนื่อง

นโยบาย

๑) กำหนดให้มีโครงสร้างคณะกรรมการธรรมาภิบาลข้อมูล และกำหนดบทบาทหน้าที่ความรับผิดชอบในการบริหารจัดการข้อมูล

๒) กำหนดหน่วยงานที่เป็นเจ้าของข้อมูลในการบริหารจัดการข้อมูลในแต่ละชุดข้อมูล

๓) กำหนดมาตรฐาน (Data Standard) และระเบียบปฏิบัติมาตรฐานและการบริหารจัดการคำอธิบายชุดข้อมูล (Metadata) ครอบคลุมบทบาทหน้าที่ความรับผิดชอบ กระบวนการจัดทำคำอธิบายชุดข้อมูล การควบคุม ดูแลและสอบทานคำอธิบายชุดข้อมูล

๔) กำหนดคำนิยามข้อมูล (Data Definition) ขอบเขตและลักษณะข้อมูล (Scope of Data) และลักษณะข้อมูล (Format of Data) ที่ครอบคลุมข้อมูลขนาดใหญ่ (Big data) และชุดข้อมูล

๕) จัดทำนโยบายธรรมาภิบาลข้อมูลที่ประกอบไปด้วย นโยบายคุณภาพข้อมูล (Data Quality Policy) นโยบายการแลกเปลี่ยนและเชื่อมโยงข้อมูล (Data Exchange and Integration Policy) การจัดชั้นความลับข้อมูล (Data Classification Standard) นโยบายความมั่นคงปลอดภัยและความเป็นส่วนบุคคลของข้อมูล (Data Security and Privacy Policy) และนโยบายการเปิดเผยข้อมูล (Open Data Policy)

๖) ธรรมาภิบาลข้อมูลตลอดวงจรชีวิตของข้อมูล (Data Life Cycle) ตั้งแต่กระบวน ๑) การสร้าง (Data Create) ๒) การจัดเก็บ (Data Store) ๓) การใช้ (Data Usage) ซึ่งประกอบด้วย การแลกเปลี่ยน การเชื่อมโยงข้อมูล และเปิดเผย (Data Exchange Integration & Disclosure) ๔) การรักษา (Data Achieve) ๕) การทำลาย (Data Destruction)

๗) กำหนดกระบวนการธรรมาภิบาลข้อมูลอย่างเป็นรูปธรรม

๘) จัดให้มีกระบวนการในการบริหารจัดการความเสี่ยงด้านข้อมูล เพื่อให้มีการบริหารจัดการข้อมูลที่ดีสอดคล้องกับชั้นความลับและความพร้อมใช้

๙) กำหนดให้มีการสื่อสารและเผยแพร่นโยบายข้อมูลให้กับผู้ที่เกี่ยวข้องทั้งภายในหน่วยงานและภายนอก

๑๐) ให้มีการฝึกอบรมเพื่อสร้างความตระหนักถึงธรรมาภิบาลข้อมูล และการบริหารจัดการข้อมูล โดยให้ครอบคลุมการบริหารจัดการทุกกระบวนการและวงจรชีวิตของข้อมูล

๑๑) ให้มีการประเมินผลการดำเนินงาน ทบทวน ตรวจสอบ และปรับปรุงนโยบายอย่างต่อเนื่องอย่างน้อยปีละ ๑ ครั้ง

นโยบายธรรมาภิบาลข้อมูล ประกอบด้วย ๕ หัวข้อหลัก ได้แก่

๑) นโยบายคุณภาพข้อมูล (Data Quality Policy)

๒) นโยบายการเชื่อมโยงและแลกเปลี่ยนข้อมูล (Data Integration and Exchange Policy)

๓) มาตรฐานการจัดชั้นความลับข้อมูล (Data Classification Standard)

๔) นโยบายความมั่นคงปลอดภัยและความเป็นส่วนบุคคลของข้อมูล (Data Security and Privacy Policy)

๕) นโยบายการเปิดเผยข้อมูล (Open Data Policy)

โดยมีรายละเอียด ดังนี้

๑. นโยบายคุณภาพข้อมูล (Data Quality Policy)

วัตถุประสงค์

เพื่อให้การควบคุมคุณภาพข้อมูล สำหรับการนำไปใช้ประโยชน์ในการบริหารงานและการให้บริการประชาชนของจังหวัดสิงห์บุรี โดยให้เป็นไปตามอำนาจหน้าที่และวัตถุประสงค์ในการดำเนินงานของจังหวัดตามที่กฎหมายกำหนด โดยข้อมูลที่ได้ทำการจัดเก็บจังหวัดจะคำนึงถึงคุณภาพข้อมูล (Data Quality) ในทุกชุดข้อมูล (Dataset)

นโยบาย

๑) กำหนดมาตรฐานข้อมูลให้เป็นแบบเดียวกัน และมีการควบคุมคุณภาพข้อมูลตลอดทั้งวงจรชีวิตข้อมูล (Data Lifecycle) ของข้อมูลที่ตนเองมีหน้าที่รับผิดชอบ

๒) กำหนดให้มีข้อกำหนดพื้นฐานของการบริหารจัดการคุณภาพข้อมูล (Data Quality Management) รวมถึงแนวทางการควบคุมและการปรับปรุงอย่างต่อเนื่อง

๓) ชุดข้อมูลทุกชุดต้องมีการวัดคุณภาพข้อมูล (Data Quality) ดังต่อไปนี้ ความถูกต้อง (Accuracy) ความครบถ้วน (Completeness) ความต้องกัน (Consistency) ความเป็นปัจจุบัน (Timeliness) ตรงตามความต้องการของผู้ใช้ (Relevancy) ความน่าเชื่อถือ (Data Integrity) และพร้อมใช้งาน (Availability) โดยทุกเกณฑ์เป็นเกณฑ์เชิงปริมาณ (Quantitative measurement)

๔) การกำหนดตัวชี้วัดคุณภาพข้อมูล เช่น ความถูกต้อง ความครบถ้วน ความต้องกัน ความเป็นปัจจุบัน ตรงตามความต้องการของผู้ใช้ และพร้อมใช้งาน

๕) รายงานคุณภาพข้อมูล ประกอบด้วยการกำหนดระดับมิติตัวชี้วัด และค่าเป้าหมายในการประเมินคุณภาพข้อมูล จะต้องแนบไปกับการใช้ชุดข้อมูล (Dataset) และชุดคำอธิบายข้อมูล

๖) การฝึกอบรมเพื่อสร้างความตระหนักถึงคุณภาพของข้อมูล

๒. นโยบายการเชื่อมโยงและแลกเปลี่ยนข้อมูล (Data Integration and Exchange Policy)

วัตถุประสงค์

เพื่อการแลกเปลี่ยนข้อมูลทั้งภายในและระหว่างหน่วยงานมีความมั่นคงปลอดภัย และข้อมูลมีคุณภาพ สามารถนำไปใช้ประโยชน์ได้อย่างมีประสิทธิภาพ โดยมีวิธีและแนวทางการนำข้อมูลไปเชื่อมโยงและแลกเปลี่ยนกับหน่วยงานภายนอก ให้สอดคล้องกับระเบียบ หลักเกณฑ์ และกฎหมายที่กำหนด บนพื้นฐานของประโยชน์ส่วนรวมเป็นสำคัญ

นโยบาย

๑) การแลกเปลี่ยนและการเชื่อมโยงข้อมูลของจังหวัดสิงห์บุรีกับหน่วยงานอื่น ให้ดำเนินการโดยเจ้าหน้าที่ ที่มีสิทธิให้กระทำการได้

๒) กำหนดแนวปฏิบัติในการจัดการเรื่องความมั่นคงปลอดภัย คุณภาพข้อมูล และผู้ประสานงานหรือช่องทางการติดต่อ

๓) กำหนดกระบวนการในการแลกเปลี่ยนข้อมูลให้ชัดเจนเริ่มตั้งแต่ขั้นตอนการเตรียมการ ขั้นตอนเริ่มดำเนินการ ขั้นตอนระหว่างดำเนินการ และขั้นตอนสิ้นสุดการดำเนินการ ให้ดำเนินการตามแนวทางปฏิบัติการ จัดทำบัญชีข้อมูล คุณภาพข้อมูล เชื่อมโยงข้อมูล และการเผยแพร่ข้อมูล

๔) กำหนดการคุ้มครองข้อมูลส่วนบุคคลในการแลกเปลี่ยนและเชื่อมโยงข้อมูล และให้เป็นไปตามนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) ของจังหวัดสิงห์บุรี

๕) กำหนดเมทาดาตาของชุดข้อมูลที่ต้องการแลกเปลี่ยนที่จำเป็นให้ครบถ้วน

๖) ทำสัญญาอนุญาตหรือข้อตกลงระหว่างหน่วยงานในการแลกเปลี่ยนข้อมูล การนำข้อมูลไปใช้ เทคโนโลยี และมาตรฐานทางเทคนิคที่ใช้ในการแลกเปลี่ยนข้อมูล

๗) บันทึกรายละเอียดและจัดเก็บข้อมูลการดำเนินงานที่เกิดขึ้นในแต่ละครั้งที่มีการแลกเปลี่ยนข้อมูล (Log File) ระหว่างหน่วยงาน เพื่อให้สามารถตรวจสอบได้

๘) สามารถตรวจสอบได้ว่าการแลกเปลี่ยนข้อมูลได้ดำเนินการอย่างเหมาะสม หรือเป็นไปตามแนวทางปฏิบัติ กระบวนการแลกเปลี่ยน และมาตรฐานตามที่กำหนด

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

๓. มาตราฐานการจัดชั้นความลับข้อมูล (Data Classification Standard)

วัตถุประสงค์

เพื่อให้การประมวลผลข้อมูลและการใช้ข้อมูลที่มีประสิทธิภาพ ถูกต้อง ตรงตามวัตถุประสงค์ของการใช้ข้อมูลให้เกิดประโยชน์ รวมถึงวิธีการและแนวทางในการขอข้อมูลจากหน่วยงานที่เกี่ยวข้องทั้งภายในและภายนอก เพื่อนำมาใช้ในการประมวลผลและนำมาใช้ ทั้งนี้ การนำข้อมูลมาใช้ให้เป็นไปตามวัตถุประสงค์ตามที่แจ้ง หากนอกเหนือจากเหตุผลดังกล่าวข้างต้น จะต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อน

นโยบาย

๑) ชุดข้อมูลต้องมีการจัดลำดับชั้นความลับของข้อมูล การกำหนดชั้นความลับของข้อมูลและการกำหนดสิทธิ์การเข้าถึง เพื่อให้สอดคล้องกับแนวทางการจัดชั้นความลับของข้อมูล

๒) กำหนดแนวปฏิบัติและมาตรฐานของการประมวลผลข้อมูล และทำการสื่อสารให้แก่ผู้ที่เกี่ยวข้องรับทราบ

๓) ห้ามเปิดเผยข้อมูลที่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง หลักเกณฑ์ นโยบาย แนวปฏิบัติของจังหวัดสิงห์บุรี ที่ประกาศใช้ในปัจจุบัน ไม่ว่าข้อมูลจะอยู่ในรูปแบบใดหรือสถานที่ใดก็ตาม

๔) การดำเนินการประมวลผลข้อมูลที่เป็นความลับ เช่น ข้อมูลส่วนบุคคล ให้เป็นไปตามขอบเขตเงื่อนไข วัตถุประสงค์ในการยินยอมให้ดำเนินการกับข้อมูลส่วนบุคคลนั้น

๕) ต้องมีการเก็บบันทึกประวัติการเข้าถึงและการใช้ข้อมูล (Log Files) เพื่อให้สามารถตรวจสอบย้อนกลับได้

๖) บริกรข้อมูล เจ้าของข้อมูล และผู้มีส่วนได้ส่วนเสียกับข้อมูลที่เกี่ยวข้องต้องร่วมกัน จัดทำเมทาดาตา พร้อมคำอธิบาย (Metadata) สำหรับข้อมูลที่จัดเก็บอยู่ในฐานข้อมูล (Database) ในทุกชุดข้อมูล

๗) ต้องมีการทบทวนระดับชั้นความลับข้อมูล อย่างน้อยปีละ ๑ ครั้ง และให้ดำเนินการปรับปรุงอย่างต่อเนื่อง

๔. นโยบายความมั่นคงปลอดภัยและความเป็นส่วนบุคคลของข้อมูล (Data Security and Privacy Policy)

วัตถุประสงค์

เพื่อเป็นการกำหนดแนวทางในการบริหารจัดการความมั่นคงปลอดภัยของข้อมูลและความเป็นส่วนบุคคล ซึ่งจะต้องสอดคล้องกับนโยบายความมั่นคงปลอดภัยและความเป็นส่วนบุคคลของข้อมูล

นโยบาย

๑) การจัดทำสถาปัตยกรรมความมั่นคงปลอดภัยของข้อมูล (Data Security Architecture)

๒) การควบคุมการเข้าถึงข้อมูล (Data Access Control)

๓) การตรวจสอบความมั่นคงปลอดภัยของข้อมูล (Data Security Audit)

๔) การประเมินความปลอดภัยของข้อมูล (Data Security Assessment)

๕) การกำหนดเครื่องมือและเทคโนโลยีความมั่นคงปลอดภัยของข้อมูล (Data Security Tool/ Technology)

๕. นโยบายการเปิดเผยข้อมูล (Open Data Policy)

วัตถุประสงค์

เพื่อกำหนดนโยบายข้อมูลที่สามารถนำไปใช้ได้โดยอิสระ สามารถนำกลับมาใช้ใหม่และแจกจ่ายได้โดยใครก็ตาม แต่ต้องระบุแหล่งที่มาหรือเจ้าของงานและต้องใช้สัญญาอนุญาต หรือเงื่อนไขเดียวกันกับที่มาหรือตามเจ้าของข้อมูลกำหนด

นโยบาย

๑) กำหนดบทบาทหน้าที่ที่เกี่ยวข้องกับการเปิดเผยข้อมูล ได้แก่ กำหนดบุคคลหรือกลุ่มบุคคลที่มีสิทธิ์ตัดสินใจในการเปิดเผยข้อมูล กำหนดบุคคลหรือกลุ่มบุคคลในการดำเนินการและปรับปรุงการเปิดเผยข้อมูล และกำหนดบุคคลหรือกลุ่มบุคคลในการรับเรื่องและแก้ไขปัญหาเบื้องต้นในการเข้าถึงข้อมูลและการนำข้อมูลไปใช้

๒) ห้ามเปิดเผยข้อมูลที่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง นโยบาย แนวปฏิบัติ ไม่ว่าข้อมูลจะอยู่ในรูปแบบใดหรือสถานที่ใดก็ตาม

๓) ต้องได้รับการอนุญาตจากเจ้าของข้อมูล (Data Owner) ก่อนการเปิดเผยข้อมูล

๔) ให้มีการจัดเตรียมข้อมูลที่อยู่ในรูปแบบที่ได้จัดทำไว้เป็นมาตรฐานตามกำหนด และง่ายต่อการนำไปใช้

๕) มีการจัดทำเมทาดาตาควบคู่ไปกับข้อมูลที่เปิดเผย

๖) ให้มีการคัดเลือกชุดข้อมูลที่ต้องการเผยแพร่ โดยหน่วยงานเจ้าของข้อมูลหรือผู้ที่ได้รับมอบหมาย

๗) สามารถตรวจสอบได้ว่าการเปิดเผยข้อมูลได้ถูกดำเนินการอย่างเหมาะสมหรือเป็นไปตามแนวทางตามที่กำหนดไว้ เพื่อให้ได้ข้อมูลที่มีคุณภาพและเป็นการรักษาคุณภาพของข้อมูล

๘) ต้องปฏิบัติตามอย่างเคร่งครัด และป้องกันมิให้มีการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

เอกสารที่เกี่ยวข้อง

๑) พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒

๒) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

๓) พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐

๔) พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙

๕) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

๖) พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓

๗) พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๘) มรด.๖ มาตรฐานรัฐบาลดิจิทัลว่าด้วยกรอบธรรมาภิบาลข้อมูล

แนวปฏิบัติธรรมาภิบาลข้อมูลของจังหวัดสิงห์บุรี

๑. หลักการและเหตุผล

พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ กำหนดให้หน่วยงานของรัฐต้องจัดให้มีการบริหารงานภาครัฐและการจัดทำบริการสาธารณะในรูปแบบช่องทางดิจิทัล โดยมีการบริหารจัดการและการบูรณาการข้อมูลภาครัฐและการทำงานให้สอดคล้องกันและเชื่อมโยงเข้าด้วยกันอย่างมีธรรมาภิบาล และให้หน่วยงานของรัฐจัดทำและดำเนินการให้เป็นไปตามธรรมาภิบาลข้อมูลภาครัฐในระดับหน่วยงาน โดยมีประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัลเรื่องธรรมาภิบาลข้อมูลภาครัฐ ประกาศ ณ วันที่ ๑๒ มีนาคม ๒๕๖๓

จังหวัดสิงห์บุรี เป็นหน่วยงานภาครัฐ โดยคำนึงถึงความสำคัญของข้อมูลจัดเป็นหนึ่งในสินทรัพย์ที่สำคัญและเป็นกลไกในการขับเคลื่อน การดำเนินงานของจังหวัดสิงห์บุรีเพื่อนำไปสู่เป้าหมายที่ได้กำหนดไว้ อย่างไรก็ตามสถานการณ์ด้านการบริหารจัดการข้อมูลและการใช้ประโยชน์จากข้อมูลของจังหวัดสิงห์บุรีในปัจจุบันนั้นยังมีอุปสรรคในด้านต่าง ๆ ทั้งในด้านการจัดเก็บข้อมูล ด้านการเปิดเผยข้อมูล ด้านความมั่นคงปลอดภัยของข้อมูล และด้านคุณภาพของข้อมูล สาเหตุของปัญหานั้นอาจมาจากการขาดแนวทางธรรมาภิบาลข้อมูล การบริหารจัดการข้อมูลทั้งวงจรชีวิตของข้อมูล (สร้าง จัดเก็บ ประมวลผล นำไปใช้ เปิดเผย และทำลาย) ขาดการบูรณาการข้อมูล

ดังนั้น เพื่อแก้ไขปัญหาทางด้านข้อมูล และนำมาซึ่งการนำข้อมูลไปใช้ก่อให้เกิดประโยชน์อย่างมีประสิทธิภาพ จังหวัดสิงห์บุรีจำเป็นอย่างยิ่งต้องมีการจัดทำแนวปฏิบัติธรรมาภิบาลข้อมูลที่สามารถนำไปใช้กำกับ ดูแล และบริหารจัดการข้อมูลของจังหวัดสิงห์บุรีทุกขั้นตอนได้อย่างเป็นระบบและมีความชัดเจนมากยิ่งขึ้น

๒. วัตถุประสงค์

เพื่อให้จังหวัดสิงห์บุรีมีแนวปฏิบัติธรรมาภิบาลข้อมูลและบริหารจัดการข้อมูลอย่างเหมาะสมเพียงพอ สอดคล้องกับภารกิจของจังหวัดสิงห์บุรี ครอบคลุมโครงสร้างธรรมาภิบาลข้อมูล บทบาทและหน้าที่ความรับผิดชอบของผู้บริหารระดับสูง สำนัก กอง และบุคลากรที่เกี่ยวข้อง

๓. รายละเอียดแนวปฏิบัติ

๓.๑ นิยาม

๑	ข้อมูล (Data)	หมายถึง	สิ่งที่สื่อความหมายให้รู้เรื่องราวข้อเท็จจริงหรือเรื่องอื่นใด ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเอง หรือโดยผ่านวิธีการใด ๆ และไม่ว่าจะได้จัดทำไว้ในรูปของ เอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ภาพถ่ายดาวเทียม ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ เครื่องมือตรวจวัด การสำรวจระยะไกล หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้ (ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่องธรรมาภิบาลข้อมูลภาครัฐ)
๒	ชุดข้อมูล (Datasets)	หมายถึง	การนำข้อมูลจากหลายแหล่งมารวบรวม เพื่อจัดเป็นชุดให้ตรงตามลักษณะโครงสร้างของข้อมูล (ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่องธรรมาภิบาลข้อมูลภาครัฐ)

๓	การบริหารจัดการข้อมูล (Data Management)	หมายถึง	คำจำกัดความที่อธิบายถึงกระบวนการที่ใช้ในการวางแผน (Plan) การระบุชี้ชัด (Specify) การเปิดใช้งาน (Enable) การสร้าง (Create) การรับ (Acquire) การดูแลรักษา (Maintain) การใช้งาน (Use) การจัดเก็บถาวร (Archive) การเรียกใช้ดึงข้อมูล (Retrieve) การควบคุม (Control) และ การทำลายข้อมูล (Purge)
๔	ธรรมาภิบาลข้อมูลภาครัฐ (Data Governance)	หมายถึง	การกำหนดสิทธิ หน้าที่ และความรับผิดชอบของผู้มีส่วนได้ส่วนเสียในการบริหารจัดการข้อมูลภาครัฐทุกขั้นตอน เพื่อให้การได้มาและการนำข้อมูลของหน่วยงานของรัฐไปใช้เป็นไปอย่างถูกต้อง ข้อมูลมีความครบถ้วน เป็นปัจจุบัน มีการรักษาความเป็นส่วนบุคคล สามารถเชื่อมโยง แลกเปลี่ยน และบูรณาการข้อมูลระหว่างกันได้อย่างมีประสิทธิภาพและมั่นคงปลอดภัย เพื่อสนับสนุนการใช้ข้อมูลเป็นหลักในการบริหารงานภาครัฐและการบริการสาธารณะ
๕	คณะกรรมธรรมาภิบาลข้อมูล (Data Governance Council)	หมายถึง	เป็นผู้มีอำนาจในการผลักดันให้เกิดธรรมาภิบาลข้อมูล โดยมีหน้าที่รับผิดชอบในการกำหนดเป้าหมาย กำกับดูแล และติดตามการดำเนินงาน รวมถึงให้คำปรึกษาและตัดสินประเด็นสำคัญที่เกี่ยวข้องกับข้อมูล สนับสนุน ส่งเสริม ผลักดันธรรมาภิบาลข้อมูลและการสื่อสารให้บุคลากรในองค์กร ตระหนักถึงความสำคัญของข้อมูล การใช้ข้อมูลอย่างปลอดภัย (จังหวัดสิงห์บุรี)
๖	ทีมบริกรข้อมูล (Data Steward Team)	หมายถึง	กลุ่มบุคคลที่มุ่งเน้นการดำเนินงาน และนิยามคำอธิบายชุดข้อมูล ร่างนโยบาย กำหนดมาตรฐาน ตรวจสอบการปฏิบัติงาน วิเคราะห์ผลจากการตรวจสอบ ในการบริหารจัดการตามองค์ประกอบของการบริหารจัดการข้อมูล
๗	การบริหารจัดการคุณภาพของข้อมูล (Data Quality Management)	หมายถึง	การกำหนดมาตรฐานและระเบียบแนวปฏิบัติการบริหารจัดการคุณภาพข้อมูล ครอบคลุมบทบาทหน้าที่ผู้รับผิดชอบ
๘	การรักษาความเป็นส่วนบุคคลของข้อมูล (Data Privacy)	หมายถึง	การรักษาความเป็นส่วนบุคคลของข้อมูลตามที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ กำหนด
๙	ข้อมูลหลัก (Master Data)	หมายถึง	ข้อมูลที่สร้างและใช้งานร่วมกันภายในขอบเขตการดำเนินงานตามภารกิจของหน่วยงาน เช่น ข้อมูลพนักงาน ข้อมูลลูกค้า ข้อมูลผู้ขาย ข้อมูลสินค้า ข้อมูลสถานที่ (DGA, ๒๐๑๘)

๑๐	คำอธิบายชุดข้อมูล (Metadata)	หมายถึง	ข้อมูลที่ใช้กำกับและอธิบายข้อมูลหลักหรือกลุ่มของข้อมูลอื่น
๑๑	การจัดการวงจรชีวิตข้อมูล (Data Life Cycle Management)	หมายถึง	ลำดับขั้นตอนของข้อมูล ตั้งแต่เริ่มสร้างข้อมูลไปจนถึง การทำลายข้อมูล ประกอบด้วย ๕ ขั้นตอน ดังนี้ การสร้างข้อมูล (Create) การจัดเก็บข้อมูล (Store) การใช้ข้อมูล (Use) การเผยแพร่ข้อมูล (Publish) การจัดเก็บข้อมูลถาวร (Archive) และการทำลายข้อมูล (Destroy)
๑๒	เจ้าของข้อมูล (Data Owner)	หมายถึง	บุคคลที่ทำหน้าที่รับผิดชอบดูแลข้อมูลโดยตรง สร้างความมั่นใจได้ว่าการบริหารจัดการข้อมูลสอดคล้องกับนโยบาย มาตรฐาน กฎระเบียบ หรือกฎหมาย เจ้าของข้อมูลทำการทบทวนและอนุมัติการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับข้อมูล
๑๓	ความมั่นคงปลอดภัยข้อมูล (Data Security)	หมายถึง	การป้องกันข้อมูลในบริบทของการรักษาความลับ ความถูกต้องของข้อมูล ความพร้อมใช้งานของข้อมูล
๑๔	ข้อมูลเปิดภาครัฐ (Open Data)	หมายถึง	ข้อมูลที่หน่วยงานของรัฐต้องเปิดเผยต่อสาธารณะอย่างน้อยตามกฎหมายว่าด้วยข้อมูลข่าวสารของราชการในรูปแบบข้อมูลดิจิทัล ที่สามารถเข้าถึงและใช้ได้อย่างเสรี ไม่จำกัดแพลตฟอร์ม ไม่เสียค่าใช้จ่าย เผยแพร่ ทำซ้ำ หรือใช้ประโยชน์ได้โดยไม่จำกัดวัตถุประสงค์
๑๕	หมวดหมู่ของข้อมูล (Data Category)	หมายถึง	ตามกรอบธรรมาภิบาลข้อมูลภาครัฐแบ่งออกได้เป็น ๕ หมวดหมู่ ได้แก่ ข้อมูลสาธารณะ ข้อมูลใช้ภายใน ข้อมูลส่วนบุคคล ข้อมูลความลับทางราชการ และข้อมูลความมั่นคง

๓.๒ แนวปฏิบัติธรรมาภิบาลข้อมูล (Data Governance Procedure)

เพื่อให้จังหวัดสิงห์บุรีมีแนวปฏิบัติที่สอดคล้องตามนโยบายธรรมาภิบาลข้อมูล และสามารถนำไปปฏิบัติได้อย่างมีประสิทธิภาพ จึงได้กำหนดรายละเอียด ดังนี้

๓.๒.๑ การจัดทำโครงสร้างธรรมาภิบาลข้อมูล (Data Governance Structure) ดังนี้

๑) คณะกรรมธรรมาภิบาลข้อมูล มีหน้าที่

(๑) กำหนดนโยบาย และขอบเขตของข้อมูลสำหรับการจัดทำธรรมาภิบาลข้อมูลของจังหวัดสิงห์บุรี

(๒) อนุมัตินโยบายและหลักเกณฑ์ในการบริหารจัดการข้อมูล เพื่อให้ข้อมูลมีความมั่นคงปลอดภัย มีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่สอดคล้องกับกฎหมายและสามารถเชื่อมโยงกันได้อย่างมีประสิทธิภาพ

(๓) กำกับ ติดตาม และตรวจสอบให้มีการปฏิบัติตามธรรมาภิบาลข้อมูลของจังหวัดสิงห์บุรีที่กำหนดอย่างต่อเนื่อง

(๔) ปฏิบัติหน้าที่อื่น ๆ ที่เกี่ยวข้องกับการดำเนินงานด้านธรรมาภิบาลข้อมูลตามที่ได้รับมอบหมาย

๒) ทีมบริกรข้อมูล (Data Steward Team) มีหน้าที่

(๑) จัดทำนโยบายและหลักเกณฑ์ในการบริหารจัดการข้อมูล เพื่อให้ข้อมูลมีความมั่นคง ปลอดภัย มีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่สอดคล้องกับกฎหมายและสามารถเชื่อมโยงกันได้อย่างมีประสิทธิภาพ เพื่อเสนอต่อคณะกรรมการธรรมาภิบาลข้อมูลของจังหวัดสิงห์บุรี

(๒) จัดทำแนวปฏิบัติสำหรับชุดข้อมูล (Dataset Guideline) โดยคำนึงถึง Data Security, Data Privacy และ Data Quality เพื่อเสนอต่อคณะกรรมการธรรมาภิบาลข้อมูลของจังหวัดสิงห์บุรี

(๓) ตรวรสอบความถูกต้อง ครบถ้วน ความเป็นปัจจุบันของข้อมูล เพื่อให้ข้อมูลมีมาตรฐานเดียวกัน และสามารถเชื่อมโยงกันได้อย่างมีประสิทธิภาพ

(๔) จัดทำบัญชีข้อมูล (Data Catalog) ที่ประกอบด้วย พจนานุกรมข้อมูล (Data Dictionary) และนิยามคำอธิบายชุดข้อมูล (Metadata) ของหน่วยงานเพื่อเสนอต่อคณะกรรมการธรรมาภิบาลข้อมูลของจังหวัดสิงห์บุรี

(๕) ตรวจสอบการบริหารจัดการข้อมูลให้เป็นไปตามนโยบายและหลักเกณฑ์ ตามที่คณะกรรมการธรรมาภิบาลข้อมูลของจังหวัดสิงห์บุรีกำหนด

(๖) จัดทำแผนการปรับปรุงชุดข้อมูลให้สอดคล้องกับกระบวนการเปิดเผยข้อมูลภาครัฐ โดยต้องกำหนดระยะเวลาในการปรับปรุงชุดข้อมูลอย่างต่อเนื่อง

(๗) จัดทำรายการข้อมูลของจังหวัดสิงห์บุรี เพื่อเปิดเผยข้อมูลภาครัฐในรูปแบบดิจิทัล

(๘) คัดเลือกชุดข้อมูลเพื่อนำเข้าระบบฐานข้อมูลกลาง เพื่อให้เกิดการแลกเปลี่ยนและเชื่อมโยงข้อมูลระหว่างหน่วยงานภายในจังหวัดสิงห์บุรีและภายนอกจังหวัดสิงห์บุรี

(๙) ตรวจสอบคุณภาพข้อมูลและวิเคราะห์ผลการตรวจสอบข้อมูล และรายงานผลให้คณะกรรมการธรรมาภิบาลข้อมูลของจังหวัดสิงห์บุรีทราบ

(๑๐) กำกับดูแล ติดตาม และประเมินผลการดำเนินงานด้านข้อมูลของจังหวัดสิงห์บุรี

(๑๑) ปฏิบัติหน้าที่อื่น ๆ ที่เกี่ยวข้องกับการดำเนินงานด้านธรรมาภิบาลข้อมูลตามที่ได้รับมอบหมาย

๓) ผู้มีส่วนได้ส่วนเสียกับข้อมูล (Data Stakeholder) ประกอบด้วย เจ้าของข้อมูล ผู้ดูแลข้อมูลผู้ใช้งาน ผู้สร้างข้อมูล มีหน้าที่

(๑) ปฏิบัติงานที่เกี่ยวข้องกับการสร้าง จัดเก็บ ใช้ รักษา และทำลายข้อมูล

(๒) ปฏิบัติตามนโยบายกำกับดูแลข้อมูลและแนวปฏิบัติที่เกี่ยวข้องกับธรรมาภิบาลข้อมูลของจังหวัดสิงห์บุรีอย่างเคร่งครัด และมีส่วนร่วมในการดำเนินธรรมาภิบาลข้อมูลของจังหวัดสิงห์บุรี

(๓) ให้ข้อเสนอแนะ หรือแจ้งประเด็นปัญหาที่พบระหว่างการใช้ข้อมูล ทั้งด้าน คุณภาพ การรักษาความเป็นส่วนบุคคล และความมั่นคงปลอดภัยของข้อมูล ไปยังเจ้าของข้อมูล เพื่อนำมา ปรับปรุงข้อมูลให้ดียิ่งขึ้น

(๔) ให้ข้อคิดเห็น ข้อเสนอแนะแก่ทีมบริกรข้อมูลและคณะกรรมการธรรมาภิบาลข้อมูล

๓.๒.๒ กระบวนธรรมาภิบาลข้อมูล (Data Governance Process)

กระบวนการธรรมาภิบาลข้อมูลภาครัฐเป็นขั้นตอนที่ใช้สำหรับกำกับดูแลให้เป็นไปตาม กฎ ระเบียบ ข้อบังคับ หรือนโยบายที่เกี่ยวข้องกับข้อมูล กระบวนการธรรมาภิบาลข้อมูลจังหวัดสิงห์บุรี เริ่มตั้งแต่การวางแผน ไปจนถึงการปรับปรุงอย่างต่อเนื่อง ดังนี้

๑) การวางแผน เริ่มตั้งแต่กำหนดวิสัยทัศน์และประเด็นปัญหา ซึ่งเป็นส่วนที่สำคัญเนื่องจากเป็นจุดเริ่มต้นที่จะกำหนด กฎระเบียบ นโยบาย มาตรฐาน หรือแนวทางปฏิบัติต่าง ๆ เพื่อใช้ในธรรมาภิบาลข้อมูลและการบริหารจัดการข้อมูล หลังจากที่ได้มีการกำหนดวิสัยทัศน์และประเด็นปัญหาที่ชัดเจนแล้ว ขั้นตอนถัดไปคือการกำหนดขอบเขตการดำเนินการ ระยะเวลาดำเนินการ บุคคลที่เกี่ยวข้อง และต้นทุนที่ใช้ในการดำเนินงาน

๒) การปฏิบัติ ดำเนินการให้สอดคล้องกับ กฎ ระเบียบ นโยบาย มาตรฐาน และแนวปฏิบัติที่ได้กำหนดไว้

๓) การตรวจสอบ วัดผล และรายงาน ดำเนินการตรวจสอบความสอดคล้องตามกระบวนการธรรมาภิบาลข้อมูลและหลักเกณฑ์การบริหารจัดการข้อมูลที่กำหนด รวมถึงรายงานผลความสอดคล้อง

๔) การปรับปรุงอย่างต่อเนื่อง การปรับปรุง นิยาม นโยบาย กระบวนธรรมาภิบาลข้อมูล และกฎ ระเบียบ ข้อบังคับที่เกี่ยวข้องกับข้อมูล เกณฑ์การประเมินความพร้อมของธรรมาภิบาลข้อมูล เกณฑ์การวัดระดับคุณภาพข้อมูล และโครงสร้างธรรมาภิบาลข้อมูล

๓.๒.๓ แนวปฏิบัติในการประเมินผลธรรมาภิบาลข้อมูลภาครัฐ (Data Governance Assessment Guideline)

ทีมบริกรข้อมูล ดำเนินการประเมินการดำเนินการธรรมาภิบาลข้อมูลภาครัฐ ซึ่งเป็นการประเมินความพร้อมของธรรมาภิบาลข้อมูลที่จะแสดงให้เห็นถึงสถานะปัจจุบัน และความก้าวหน้าในการดำเนินการธรรมาภิบาลข้อมูลภาครัฐของจังหวัดสิงห์บุรี ซึ่งผลของการดำเนินการธรรมาภิบาลข้อมูลจะส่งผลถึงความสำเร็จของธรรมาภิบาลข้อมูลภาครัฐ ประกอบด้วย ๕ ด้าน

๑) โครงสร้างธรรมาภิบาลข้อมูลภาครัฐ
๒) กระบวนการธรรมาภิบาลข้อมูลภาครัฐ
๓) นโยบายและการตรวจสอบ
๔) การประเมินคุณภาพของข้อมูลและความมั่นคงปลอดภัยของข้อมูล
๕) การปรับปรุงอย่างต่อเนื่อง

การประเมินผลธรรมาภิบาลข้อมูลภาครัฐ ควรดำเนินการอย่างน้อยปีละ ๑ ครั้ง และ ให้รายงานผลการประเมินไปยังคณะกรรมการธรรมาภิบาลข้อมูลภาครัฐ

๓.๓ แนวปฏิบัติการบริหารจัดการข้อมูล (Data Management)

การบริหารจัดการข้อมูลเป็นสิ่งสำคัญ ซึ่งจังหวัดสิงห์บุรีตระหนักว่าข้อมูลที่มีอยู่เป็นทรัพย์สินที่มีค่า และจากการเกิดขึ้นของข้อมูลที่มีปริมาณมหาศาล ไม่ว่าจะเป็นข้อมูลที่รวบรวมมาโดยอัตโนมัติจากระบบหรืออุปกรณ์ต่าง ๆ หรือข้อมูลที่เกิดขึ้นจากการป้อนข้อมูลหรือโต้ตอบกับผู้ใช้งาน เพื่อให้จังหวัดสิงห์บุรีสามารถนำข้อมูลเหล่านี้ไปประมวลผลหรือใช้ในการตัดสินใจได้อย่างแม่นยำ จึงต้องได้รับการบริหารจัดการอย่างถูกต้องเหมาะสมและสอดคล้องกับวัตถุประสงค์ในการบริหารจัดการข้อมูล

๓.๓.๑ แนวปฏิบัติการบริหารจัดการข้อมูลตลอดวงจรชีวิต มีหลักปฏิบัติดังนี้

ธรรมาภิบาลข้อมูล (Data Governance) ให้ข้อมูลมีความสมบูรณ์ ถูกต้องและทันต่อเวลา และมีการกำหนดบทบาท หน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้อง รวมถึงกำหนดกระบวนการต่าง ๆ สำหรับธรรมาภิบาลข้อมูลตลอดวงจรชีวิตของข้อมูล (Data Life Cycle) ตั้งแต่กระบวนการสร้าง (Data Creation)การจัดเก็บ (Data Storage) การใช้ข้อมูล (Data Usage) การเปิดเผย (Data Publish) การจัดเก็บถาวร (Data Archival) และการทำลาย (Data Destroy) และบริหารจัดการข้อมูลเป็นไปอย่างถูกต้องครบถ้วน น่าเชื่อถือ และเป็นปัจจุบัน รายละเอียดวงจรชีวิตตามรูป



๑. การสร้างข้อมูล (Create) คือการสร้างข้อมูลขึ้นมาใหม่ ทั้งวิธีการจดบันทึกด้วยมือหรือการบันทึก ด้วยอุปกรณ์อิเล็กทรอนิกส์ต่าง ๆ

๒. การจัดเก็บข้อมูล (Store) คือการนำข้อมูลที่สร้างขึ้นมาจัดเก็บให้เป็นระเบียบ สะดวกและง่ายต่อการใช้งานตามวัตถุประสงค์ต่าง ๆ รักษาป้องกันไม่ให้สูญหายหรือถูกขโมย ไม่ว่าจะเป็นการจัดเก็บลงแฟ้มเอกสาร ระบบจัดการฐานข้อมูลในระบบคอมพิวเตอร์หรือระบบคลาวด์

๓. การใช้ข้อมูล (Use) คือการนำข้อมูลที่จัดเก็บมาใช้ประมวลผลให้เกิดประโยชน์ตรงตามวัตถุประสงค์ด้านการใช้งานต่าง ๆ เช่น การวิเคราะห์ข้อมูล การทำการตลาด เป็นต้น

๔. การเผยแพร่ข้อมูล (Publish) คือการนำข้อมูลไปเปิดเผย ไม่ว่าจะเป็นการส่งมอบเอกสาร การแลกเปลี่ยนข้อมูล การแชร์ข้อมูล การกระจายข้อมูลระหว่างบุคคล องค์กร เป็นต้น

๕. การจัดเก็บข้อมูลถาวร (Achieve) คือการคัดลอกข้อมูลเพื่อทำสำเนาสำหรับเก็บรักษา โดยไม่มีการลบปรับปรุง หรือแก้ไขข้อมูลนั้นอีก และนำไปใช้งานใหม่เมื่อต้องการ

๖. การทำลายข้อมูล (Destroy) คือการทำลายข้อมูลไม่ให้มีสภาพการใช้งาน เนื่องจากมีอายุนานเกินไป จนไม่เหมาะสมกับการใช้ประโยชน์อีก และเพื่อไม่ให้ข้อมูลถูกนำไปใช้งานที่ผิดวัตถุประสงค์ จึงจำเป็นต้องทำลายเอกสาร ตลอดจนไฟล์ข้อมูลต่าง ๆ ในระบบคอมพิวเตอร์หรือระบบคลาวด์

การบริหารจัดการข้อมูลเป็นสิ่งสำคัญสำหรับทุกหน่วยงาน ซึ่งแต่ละหน่วยงานต้องตระหนักว่าข้อมูลที่มีอยู่เป็นสินทรัพย์ที่มีค่า เพื่อให้หน่วยงานสามารถนำข้อมูลเหล่านี้ไปประมวลผลหรือใช้ในการตัดสินใจได้อย่างแม่นยำ จึงต้องได้รับการบริหารจัดการอย่างถูกต้อง เหมาะสม และสอดคล้องกับวัตถุประสงค์ในการบริหารจัดการข้อมูลของหน่วยงาน

๓.๓.๒ แนวปฏิบัติมาตรฐานการจัดทำบัญชีข้อมูล (Data Catalog Procedure) มีหลักปฏิบัติดังนี้

๑) เจ้าของข้อมูล ผู้ดูแลข้อมูล และทีมบริกรข้อมูล ต้องจัดทำและทบทวนคำอธิบายชุดข้อมูลอย่างสม่ำเสมอเพื่อเพิ่มประสิทธิภาพในการนำข้อมูลไปใช้อย่างครบถ้วนถูกต้อง โดยกำหนดแนวปฏิบัติในการจัดโครงสร้างข้อมูลสารสนเทศให้เป็นมาตรฐานตามหัวข้อดังนี้

๑.๑) การรวบรวมคำอธิบายชุดข้อมูล (Collected Metadata)

๑.๒) การใช้คำอธิบายชุดข้อมูล (Used Metadata)

๑.๓) การจัดเก็บคำอธิบายชุดข้อมูล (Stored Metadata)

๑.๔) การทบทวนและปรับปรุงคำอธิบายชุดข้อมูล (Review and Improve Metadata)

๒) ทีมบริกรข้อมูล มีหน้าที่จัดทำมาตรฐาน ตรวจสอบ บำรุงรักษา Metadata Repository ที่อยู่ในความรับผิดชอบอย่างสม่ำเสมอ ตามมาตรฐานที่กำหนดทุกชุดข้อมูลสำคัญอย่างครบถ้วน โดยมีการสอบทานอย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

๓) ทีมบริกรข้อมูล มีหน้าที่กำหนดให้มีกระบวนการควบคุม การเข้าถึงข้อมูล (Data Access Control) การกำหนดสิทธิ์ การปรับปรุงแก้ไขคำอธิบายชุดข้อมูล เพื่อป้องกันความเสี่ยงหรือข้อผิดพลาดในการปฏิบัติงาน

๔) เจ้าของข้อมูล ทำหน้าที่บันทึก จัดทำคำอธิบายชุดข้อมูล (Metadata)

๕) ผู้ใช้ข้อมูล มีหน้าที่ให้ข้อคิดเห็น เสนอแนะ รายงานปัญหาของเมทาดาตา เพื่อปรับปรุงเมทาดาตาให้เป็นปัจจุบัน

๓.๓.๓ แนวปฏิบัติการบริหารจัดการคุณภาพข้อมูล (Data Quality Management) มีองค์ประกอบการบริหารจัดการคุณภาพข้อมูล ได้แก่

๑) การกำหนดหลักเกณฑ์คุณภาพข้อมูล (Data Quality Requirement)

จังหวัดสิงห์บุรีจะต้องดำเนินการกำหนดหลักเกณฑ์คุณภาพข้อมูล อย่างน้อยดังนี้

(๑) กำหนดองค์ประกอบข้อมูลที่สำคัญ (Critical Data Elements หรือ CDE) ในแต่ละชุดข้อมูล โดยประเมินตามคุณลักษณะข้อมูลที่มีคุณภาพของจังหวัดสิงห์บุรี เพื่อจัดลำดับความสำคัญ

(๒) กำหนดระดับคุณภาพข้อมูล (Data Quality Threshold) ในแต่ละชุดข้อมูล เพื่อใช้ในการประเมินคุณภาพของชุดข้อมูล เป็นการกำหนดระดับในแต่ละมิติคุณภาพข้อมูล

๒) การประเมินคุณภาพข้อมูล (Data Quality Management)

(๑) กำหนดให้มีหน่วยงานหรือผู้รับผิดชอบในการบริหารจัดการคุณภาพข้อมูล

(๒) จัดให้มีการกำหนดคุณลักษณะข้อมูลที่มีคุณภาพ

(๓) จัดให้มีกำหนดหลักเกณฑ์คุณภาพของข้อมูล

(๔) จัดให้มีกำหนดให้มีการประเมินคุณภาพของข้อมูล

(๕) จัดให้มีการควบคุมและติดตามให้ข้อมูลมีคุณภาพอยู่เสมอ

เกณฑ์การประเมินคุณภาพข้อมูล ให้ดำเนินการตามมิติคุณภาพข้อมูล ๕ มิติ ได้แก่

๑. ความถูกต้อง

๒. ความสอดคล้องกัน

๓. ตรงตามความต้องการของผู้ใช้

๔. ความเป็นปัจจุบัน

๕. ความพร้อมใช้ที่สอดคล้องตามองค์ประกอบในการประเมินคุณภาพข้อมูลตามกรอบธรรมาภิบาลข้อมูลภาครัฐโดยแต่ละมิติ มีรายละเอียดและตัวชี้วัด (Indicators) ดังนี้

มิติคุณภาพข้อมูล	รายละเอียด	รายการตัวชี้วัด
ความถูกต้องของข้อมูล (Data Accuracy) และครบถ้วนของข้อมูล (Data Completeness)	ประเมินเรื่องความถูกต้อง แม่นยำ แหล่งข้อมูลที่น่าเชื่อถือ และมีกระบวนการตรวจสอบ	มีแหล่งข้อมูลที่น่าเชื่อถือ - มีกระบวนการหรือเครื่องมือตรวจสอบ จุดผิดพลาด บกพร่อง - มีการตรวจสอบความครบถ้วนของข้อมูล - มีวิธีเก็บข้อมูลมีความเป็นกลาง น่าเชื่อถือและไม่สร้างข้อมูล ที่มีอคติ - มีการระบุคำนิยามและลักษณะข้อมูลที่ต้องการ
ความสอดคล้องกันของข้อมูล (Data Consistency)	ประเมินเรื่องรูปแบบของข้อมูล ความสอดคล้องกันและมาตรฐานในการจัดทำข้อมูลของหน่วยงาน	- มีการเก็บข้อมูลใต้มาตรฐานข้อมูลเดียวกัน หรือมาตรฐานข้อมูลที่สอดคล้องกัน ทำให้สามารถใช้ประโยชน์ข้อมูลร่วมกันได้ - มีการตรวจสอบรูปแบบข้อมูลภายในชุดข้อมูลเดียวกันข้อมูลมีความเชื่อมโยงและไม่ขัดแย้งกัน - มีการใช้กฎ วิธีการตรวจวัดที่สอดคล้องกัน ทั้งหน่วยงานรวมถึงหน่วยงานภายนอก - มีการกำหนดบทบาทและผู้รับผิดชอบข้อมูล
ข้อมูลตรงตามความต้องการของผู้ใช้ (Relevancy)	ประเมินว่าเป็นข้อมูลที่ผู้ใช้ของผู้ใช้ต้องการ หรือเป็นข้อมูลที่จำเป็นต้องทราบ มีความละเอียดเพียงพอต่อนำไปใช้งาน	- ข้อมูลตรงตามความต้องการและวัตถุประสงค์ของการใช้งาน - มีการปรับปรุงคุณภาพให้ตรงตามความต้องการของผู้ใช้

มิติคุณภาพข้อมูล	รายละเอียด	รายการตัวชี้วัด
ความเป็นปัจจุบัน (Timeliness)	ประเมินเรื่องการเผยแพร่ข้อมูล การปรับปรุงข้อมูลและแผนเรื่องระยะเวลา	- ข้อมูลมีการเผยแพร่ ส่งตรงต่อเวลา - ข้อมูลมีความเป็นปัจจุบัน - ข้อมูลมีการเผยแพร่ข้อมูลในเวลาที่เหมาะสม - มีการจัดทำปฏิทินเผยแพร่ข้อมูล
ความพร้อมใช้ข้อมูล (Availability)	ประเมินความพร้อมใช้ของข้อมูล รวมไปถึงช่องทางในการขอหรือใช้ข้อมูล	- ข้อมูลถูกจัดในรูปแบบที่พร้อมนำไปใช้งานและเหมาะกับผู้ใช้งาน - มีการเผยแพร่ข้อมูลที่เหมาะสมและ สามารถเข้าถึงได้ โดยผู้ใช้สามารถเข้าถึงข้อมูลได้สะดวกตามสิทธิที่เหมาะสม - ข้อมูลสามารถอ่านด้วยโปรแกรมคอมพิวเตอร์ได้ - มีคำอธิบายข้อมูลที่ชัดเจน - มีคำอธิบายเพิ่มเติม แนวทาง/ขั้นตอนการขอข้อมูลที่ไม่เผยแพร่

การจัดระดับชั้นและการแบ่งปันข้อมูล

การจัดระดับชั้นข้อมูล (Data Classification) หมายความว่า การจำแนกชั้นของข้อมูล ในบริบทของการรักษาความปลอดภัยข้อมูลตามระดับของความอ่อนไหวและผลกระทบต่อบุคคล องค์กร และ ประเทศ หากมีการเปิดเผย เปลี่ยนแปลง หรือทำลายข้อมูลโดยไม่ได้รับอนุญาต โดยการจัดระดับชั้นข้อมูลจะช่วยกำหนดการควบคุมความปลอดภัยพื้นฐานที่เหมาะสมสำหรับการปกป้องข้อมูลนั้น ๆ ทั้งนี้ ข้อมูลสำคัญของบุคคล องค์กร และประเทศทั้งหมด ควรจัดชั้นตามระดับความอ่อนไหวหนึ่งในห้าของระดับชั้นข้อมูลหรือตามที่หน่วยงานกำหนด เพื่อให้หน่วยงานของรัฐสามารถจัดการข้อมูลในกระบวนงานที่เกี่ยวข้องกับภารกิจของหน่วยงานได้อย่างมีประสิทธิภาพ

๑) 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 ไม่ใช่การกำหนดให้ข้อมูลนั้นเป็นข้อมูลข่าวสารลับตามระเบียบการรักษาความลับทางราชการ

๒) การแบ่งปันข้อมูล (Data sharing) หมายความว่า ข้อมูลอ่อนไหวที่ได้รับการจัดระดับชั้นข้อมูล ยกเว้นในระดับชั้นลับที่สุด ซึ่งสามารถแบ่งปันและแลกเปลี่ยนกันได้ระหว่างหน่วยงาน โดยจำเป็นต้องมีการกำหนดสิทธิในการเข้าถึงและใช้งาน รวมถึงการคุ้มครองข้อมูลให้มีความมั่นคงปลอดภัย

๓) ข้อมูลแบ่งปัน (Shared data) หมายความว่า ข้อมูลสำคัญที่สอดคล้องกับยุทธศาสตร์ข้อมูล (Data Strategy) ภารกิจหลักและเป้าหมายของหน่วยงานและประเทศ รวมถึงข้อมูลอ่อนไหวที่ได้รับการจัดระดับชั้นเผยแพร่ภายในองค์กร ลับ และลับมาก ซึ่งสามารถแบ่งปันและแลกเปลี่ยนกันได้ระหว่างหน่วยงาน โดยจำเป็นต้องมีการกำหนดสิทธิใน การเข้าถึงและใช้งาน รวมถึงการคุ้มครองข้อมูลให้มีความมั่นคงปลอดภัย ไม่รวมถึงข้อมูลที่มีระดับชั้นลับที่สุด

๔) นายทะเบียนข้อมูลข่าวสารลับ หมายความว่า เจ้าหน้าที่ผู้ได้รับแต่งตั้งจากหัวหน้าหน่วยงานของรัฐ เพื่อทำหน้าที่ควบคุมและรับผิดชอบการดำเนินงานเกี่ยวกับข้อมูลข่าวสารลับขึ้นภายในหน่วยงานที่ตนรับผิดชอบ ทั้งนี้ นิยามต่าง ๆ ให้อ้างอิงระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔

๕) นายทะเบียนบัญชีข้อมูลหน่วยงาน หมายความว่า หัวหน้าหน่วยงานของรัฐ หรือผู้ที่ได้รับมอบหมายทำหน้าที่กำกับ ดูแล การลงทะเบียนบัญชีข้อมูลหน่วยงาน การตรวจสอบและแก้ไขบัญชีข้อมูลหน่วยงาน การเพิกถอนการลงทะเบียนบัญชีข้อมูลหน่วยงาน และอนุญาตใช้และเปิดเผยทะเบียนบัญชีข้อมูลของหน่วยงาน

ข้อมูลอ่อนไหว (Sensitive Data) หมายความว่า ข้อมูลที่มีระดับชั้นความลับหรือที่เป็นข้อมูลเกี่ยวข้องกับความมั่นคงที่ต้องได้รับการป้องกันจากการเข้าถึงโดยไม่ได้รับอนุญาต เพื่อคุ้มครองความเป็นส่วนตัว (privacy) หรือความปลอดภัย (security) ของบุคคลหรือองค์กร ซึ่งหากข้อมูลอ่อนไหว มีการเปิดเผยโดยไม่ได้รับอนุญาต จะมีแนวโน้มที่จะนำไปสู่ผลที่ไม่พึงประสงค์หรือส่งผลกระทบต่อบุคคล หน่วยงาน องค์กร หรือ ประเทศ ตัวอย่างเช่น ข้อมูลส่วนบุคคลที่อ่อนไหว (Sensitive Personal Data) ข้อมูลที่เกี่ยวข้องกับด้านความมั่นคง กฎหมาย เศรษฐกิจ การพาณิชย์

การจัดทำบัญชีข้อมูลภาครัฐ คือ รายการข้อมูลภาครัฐหรือบัญชีข้อมูลภาครัฐ เปรียบเสมือนสมุดหน้าเหลือง (Yellow pages) ที่รวบรวมรายการข้อมูลสำคัญจากหน่วยงานภาครัฐทั้งหมดพร้อมคำอธิบายข้อมูลหรือเมทาดาตา (Metadata) ที่เป็นพื้นฐานสำคัญในการกำกับดูแลข้อมูล การบูรณาการข้อมูลข้ามหน่วยงานเพื่อการวิเคราะห์ข้อมูลขนาดใหญ่ได้ โดยบัญชีข้อมูลจะให้ความสำคัญกับชุดข้อมูล (คลังข้อมูลที่พร้อมใช้) และเชื่อมต่อชุดข้อมูลดังกล่าวกับข้อมูลต่าง ๆ เพื่อให้ผู้ใช้ข้อมูลสามารถสามารถสืบค้น ร้องขอ ทราบแหล่งข้อมูล ระดับชั้นข้อมูลประเภท และรายละเอียดที่สำคัญของข้อมูลผ่านระบบสารสนเทศได้อย่างสะดวกและทันต่อเวลา และเพื่อให้เกิดการใช้ประโยชน์จากข้อมูลมากขึ้น จึงต้องมีการรวบรวมบัญชีข้อมูลที่สำคัญจากหน่วยงานเพื่อให้บริการต่อประชาชนและใช้งานภายในหน่วยงานผ่านระบบบัญชีข้อมูลภาครัฐ (GD Catalog) ซึ่งต้องมีการลงทะเบียนบัญชีข้อมูลภาครัฐ เป็นการบริหารจัดการบัญชีข้อมูลหน่วยงาน ภายใต้โครงการจัดทำบัญชีข้อมูลภาครัฐ ซึ่งเป็นการรวบรวมเฉพาะชื่อชุดข้อมูลสำคัญ คำอธิบายชุดข้อมูลหรือเมทาดาตา (Metadata) และทรัพยากร (Resource) ของข้อมูลผ่านช่องทางโปรแกรมการเชื่อมต่อ API จากระบบบัญชีข้อมูลหน่วยงานมาจัดเก็บไว้ที่ฐานข้อมูลกลางของระบบบัญชีข้อมูลภาครัฐ โดยที่ข้อมูล (Data) ยังคงจัดเก็บอยู่ที่หน่วยงานเจ้าของข้อมูล และผู้ใช้จะสามารถเข้าถึงได้ตามสิทธิการเข้าถึงข้อมูลที่หน่วยงานเจ้าของข้อมูลกำหนด

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.) ร่วมกับ สำนักงานสถิติแห่งชาติ (สสช.) และสถาบันส่งเสริมการวิเคราะห์และบริหารข้อมูลภาครัฐ (สวข.) ภายใต้สำนักงานส่งเสริมเศรษฐกิจดิจิทัล (DEPA) จึงได้จัดทำ แนวทางการจัดทำบัญชีข้อมูลภาครัฐ และแนวทางการลงทะเบียนบัญชีข้อมูลภาครัฐเพื่อเป็นแนวทางในการจัดทำบัญชีข้อมูล (Data Catalog) พัฒนาระบบบัญชีข้อมูลภาครัฐ (Government Data Catalog : GD Catalog) และขึ้นทะเบียนกับระบบบัญชีข้อมูลภาครัฐกลางที่ได้มาตรฐานและเป็นไปในทิศทางเดียวกัน

๔. แนวปฏิบัติในการควบคุมสิทธิ์การเข้าถึงข้อมูลที่สำคัญ (Access Control) ของจังหวัดสิงห์บุรี

เพื่อให้การใช้งานระบบสารสนเทศเป็นไปอย่างเหมาะสมมีประสิทธิภาพ และป้องกันปัญหาที่อาจจะเกิดขึ้น จากการใช้งานในลักษณะที่ไม่ถูกต้อง ซึ่งอาจส่งผลให้เกิดภัยคุกคามในลักษณะต่าง ๆ ต่อระบบสารสนเทศของหน่วยงาน จึงได้จัดทำ แนวปฏิบัติในการควบคุมสิทธิ์การเข้าถึงข้อมูลที่สำคัญ (Access Control) ขึ้น เพื่อเผยแพร่ให้บุคลากรและบุคคลภายนอกที่ปฏิบัติงานร่วมกับจังหวัดสิงห์บุรี ได้รับทราบและให้ความร่วมมือปฏิบัติตามอย่างเคร่งครัดต่อไป ตามรายละเอียดดังนี้

๑. แนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของจังหวัดสิงห์บุรี การเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control) และการใช้งานตามภารกิจเพื่อควบคุม การเข้าถึงสารสนเทศ (Business Requirements for Access Control)

๑.๑ จังหวัดสิงห์บุรี ดำเนินกิจการภายใต้กฎหมายไทย ดังนั้น การใช้งานคอมพิวเตอร์ และการเชื่อมต่อทางอินเทอร์เน็ต ให้ปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ และพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ หรือกฎหมายอื่นที่เกี่ยวข้อง

๑.๒ จังหวัดสิงห์บุรี ไม่สนับสนุน หรือยินยอมให้เจ้าหน้าที่ของหน่วยกระทำผิดต่อพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ และพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ หรือกฎหมายอื่นที่เกี่ยวข้อง

๑.๓ ระบบคอมพิวเตอร์และอุปกรณ์เครือข่ายถือเป็นทรัพย์สินของหน่วยงาน ห้ามผู้ไม่ได้รับการอนุญาตหรือผู้ที่ไม่เกี่ยวข้องใช้งานโดยมิได้รับอนุญาต หากผู้ใดกระทำการใด ๆ เป็นการบุกรุกเขตหวงห้ามหรือพยายามบุกรุกเข้าสู่ระบบเครือข่าย ถือเป็นการละเมิดตามกฎหมาย ต้องได้รับโทษตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ หรือกฎหมายอื่นที่เกี่ยวข้อง

๑.๔ สิทธิ์ในการเข้าถึงการใช้สารสนเทศ เป็นไปตามบทบาทหน้าที่ที่เกี่ยวข้อง หรือได้รับมอบหมายจากผู้บังคับบัญชา ไม่อนุญาตให้ผู้ที่ไม่เกี่ยวข้องกับสารสนเทศ หรือในส่วนที่ไม่เกี่ยวข้องกับตนเข้าใช้งาน

๑.๕ การยืมทรัพย์สินสารสนเทศจะต้องทำตามขั้นตอนการยืม และเมื่อสิ้นสุดการใช้งานหรือสิ้นสุดสัญญา หรือสิ้นสุดข้อตกลงการจ้างจะต้องคืนทรัพย์สินตามขั้นตอนการคืนทรัพย์สิน

๑.๖ การทำลายอุปกรณ์หรือสื่อบันทึกข้อมูล หรือสารสนเทศ ต้องทำตามระเบียบ สำนักนายกรัฐมนตรีว่าด้วยการพัสดุ พ.ศ. ๒๕๖๑

๑.๗ เครื่องคอมพิวเตอร์ และอุปกรณ์ประกอบที่สำคัญ จะต้องมีการกำหนดรหัสผ่าน (Password) ที่มีความยาวอย่างน้อย ๔-๖ ตัว เพื่อควบคุมการเข้าถึงและเพื่อป้องกันการเข้าถึงข้อมูล โดยไม่ได้รับอนุญาต

ภาคผนวก

การบริหารจัดการข้อมูลเป็นสิ่งสำคัญสำหรับทุกหน่วยงาน ซึ่งจังหวัดสิงห์บุรีตระหนักว่าข้อมูลที่มีอยู่เป็นทรัพย์สินที่มีค่า และจากการเกิดขึ้นของข้อมูลที่มีปริมาณมหาศาล ไม่ว่าจะเป็นข้อมูลที่รวบรวมมาโดยอัตโนมัติจากระบบหรืออุปกรณ์ต่าง ๆ หรือข้อมูลที่เกิดขึ้นจากการป้อนข้อมูลหรือโต้ตอบกับผู้ใช้งาน เพื่อให้จังหวัดสามารถนำข้อมูลเหล่านี้ไปประมวลผลหรือใช้ในการตัดสินใจได้อย่างแม่นยำ จึงต้องได้รับการบริหารจัดการอย่าง ถูกต้อง เหมาะสม และสอดคล้องกับวัตถุประสงค์ในการบริหารจัดการข้อมูลของหน่วยงาน เช่น

๑) เพื่อการจัดเก็บ นำมาใช้งาน และประมวลผลข้อมูลตามที่หน่วยงานต้องการ

๒) เพื่อควบคุม ตรวจสอบ และป้องกัน โดยใช้กระบวนการธรรมาภิบาลข้อมูลและความปลอดภัยของข้อมูล

๓) เพื่อจัดหมวดหมู่ และกำหนดมาตรฐานของข้อมูล โดยใช้การจำแนกข้อมูล และกำหนดกรอบการทำงานที่เป็นที่รู้จักแพร่หลาย

๔) เพื่อให้สามารถนำข้อมูลกลับมาใช้ได้ในภายหลัง โดยกำหนดข้อมูลให้อยู่ในรูปแบบที่เรียกใช้ได้อย่างมีประสิทธิภาพ

๕) เพื่อการปรับปรุงข้อมูลให้เป็นปัจจุบัน และมีความถูกต้องสมบูรณ์อยู่เสมอ

๖) เพื่อการปกป้องข้อมูลจากการลักลอบใช้งานหรือแก้ไขโดยมิชอบ รวมถึงจากเหตุการณ์ที่อาจเกิดจากภัยธรรมชาติหรือความบกพร่องภายในระบบคอมพิวเตอร์

ซึ่งในการบริหารจัดการข้อมูลนั้น มีองค์ประกอบในการบริหารจัดการบทบาทส่วนงาน ตลอดทั้งระบบบริหารและกระบวนการจัดการข้อมูล ตามวงจรชีวิตของข้อมูล



วงจรชีวิตของข้อมูลและองค์ประกอบในการบริหารจัดการข้อมูล

ระบบบริหารและกระบวนการจัดการข้อมูล ตามวงจรชีวิตของข้อมูล คือ “ลำดับขั้นตอนของข้อมูลตั้งแต่เริ่มสร้างข้อมูลไปจนถึงการทำลายข้อมูล” ประกอบด้วย ๖ ขั้นตอน ดังนี้

๑) กระบวนการสร้างข้อมูล (Create) เป็นการสร้างข้อมูลขึ้นมาใหม่ โดยวิธีการบันทึกเข้าไปด้วยบุคคลหรือบันทึกอัตโนมัติด้วยอุปกรณ์อิเล็กทรอนิกส์ เช่น อุปกรณ์ตรวจจับสัญญาณ (Sensor) รวมถึงการซื้อข้อมูลหรือ การรับข้อมูลจากหน่วยงานอื่น เพื่อนำมาจัดเก็บในภายหลัง โดยการดำเนินการเป็นไปตามบทบัญญัติของกฎหมาย และระเบียบที่เกี่ยวข้อง ดังนี้

๑.๑) มีการรักษาความมั่นคงปลอดภัยและความเป็นส่วนบุคคลของข้อมูล

๑.๒) เจ้าของข้อมูล และบริกรข้อมูล เป็นผู้ร่วมกันจัดให้มีชุดข้อมูลและเมทาดาตาที่มีความถูกต้อง ครบถ้วน และเป็นปัจจุบัน

๑.๓) เจ้าของข้อมูล ต้องจัดชั้นความลับของข้อมูล

๒) กระบวนการจัดเก็บข้อมูล (Store) เป็นการจัดเก็บข้อมูลที่เกิดจากกระบวนการสร้าง หรือข้อมูลที่ได้จากการแลกเปลี่ยนกับหน่วยงานอื่น เพื่อให้มีระเบียบ ง่ายต่อการใช้งาน ไม่สูญหาย หรือถูกทำลาย และให้ผู้ใช้งาน สามารถประมวลผลข้อมูลต่าง ๆ ตามความต้องการได้อย่างรวดเร็ว ไม่ว่าจะจัดเก็บลงแฟ้มข้อมูล (File) หรือระบบการจัดการฐานข้อมูล (Database Management System - DBMS) โดยดำเนินการเป็นไปตามบทบัญญัติของ กฎหมาย และระเบียบที่เกี่ยวข้อง ดังนี้

๒.๑) มีการดำเนินการโดยบุคลากรของจังหวัดซึ่งมีหน้าที่รับผิดชอบการดำเนินการนั้น

๒.๒) มีการรักษาความมั่นคงปลอดภัยและความเป็นส่วนบุคคลของข้อมูล

๒.๓) การจัดเก็บข้อมูล ทำโดยจัดเก็บลงในสื่อบันทึกข้อมูลและมีโครงสร้างข้อมูล ข้อมูลหลัก และข้อมูลอ้างอิงตามที่กรมกำหนด

๒.๔) การจัดเก็บข้อมูล มีการสำรองข้อมูลที่จัดเก็บ ให้มีความถูกต้องครบถ้วนและเป็นปัจจุบัน โดยมีการสำรองข้อมูลที่ทำให้มั่นใจได้ว่าข้อมูลจะไม่สูญหายยกเว้นกรณีสุดวิสัย

๒.๕) ในกรณีที่การดำเนินการจัดเก็บข้อมูล ส่งผลต่อชุดข้อมูลและเมทาดาตา เจ้าของข้อมูลและบริกรข้อมูลต้องดำเนินการปรับปรุงชุดข้อมูลและเมทาดาตาให้มีความถูกต้อง ครบถ้วน และเป็นปัจจุบัน

๓) กระบวนการใช้ข้อมูล (Use) เป็นการนำข้อมูลที่จัดเก็บมาประมวลผล เช่น การถ่ายโอนข้อมูล การเปลี่ยนรูปแบบการจัดเก็บข้อมูล การวิเคราะห์ข้อมูล การจัดทำรายงาน เพื่อนำข้อมูลเหล่านั้นมาใช้งานให้เกิดประโยชน์ตามวัตถุประสงค์ รวมถึงการสำรอง (Backup) ข้อมูล โดยการคัดลอกข้อมูลที่ใช้งานอยู่ในปัจจุบัน เพื่อทำสำเนา เช่น ใช้โปรแกรมในการสำรองข้อมูล เป็นการหลีกเลี่ยงความเสียหายที่จะเกิดขึ้นหากข้อมูลเกิดการเสียหายหรือสูญหาย ซึ่งสามารถนำข้อมูลที่สำรองไว้ในสื่อบันทึกข้อมูลกลับมาใช้งานได้ทันที โดยการกู้คืน (Restore) โดยดำเนินการเป็นไปตามบทบัญญัติของกฎหมาย และระเบียบที่เกี่ยวข้อง ดังนี้

๓.๑) ให้มีการดำเนินการโดยบุคลากรของจังหวัดซึ่งมีหน้าที่รับผิดชอบการดำเนินการนั้น

๓.๒) มีการรักษาความมั่นคงปลอดภัยและความเป็นส่วนบุคคลของข้อมูล

๓.๓) ข้อมูลมีความถูกต้อง (Accuracy) ความครบถ้วน (Completeness) ความต้องกัน (Consistency) ความเป็นปัจจุบัน (Timeliness) ตรงตามความต้องการของผู้ใช้ (Relevancy) และมีความพร้อมใช้ (Availability)

๓.๔) มีการบันทึกประวัติการใช้ (Log File) เพื่อให้สามารถตรวจสอบย้อนกลับได้

๔) กระบวนการเผยแพร่ข้อมูล (Publish) เป็นการแชร์ข้อมูล (Sharing) การกระจายข้อมูล (Dissemination) การควบคุมการเข้าถึง (Access Control) การแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน (Exchange) และการกำหนดเงื่อนไขในการนำข้อมูลไปใช้(Condition) โดยดำเนินการโดยบุคลากรของจังหวัดซึ่งมีหน้าที่ รับผิดชอบการดำเนินการนั้น โดยให้เป็นไปตามบทบัญญัติของกฎหมาย และระเบียบที่เกี่ยวข้อง

๕) กระบวนการจัดเก็บข้อมูลถาวร (Archive) เป็นการคัดลอกเอาข้อมูลที่มีช่วงอายุเกินช่วงใช้งาน หรือไม่ได้ใช้งานแล้ว เพื่อทำสำเนาสำหรับการเก็บรักษา โดยที่ข้อมูลนั้นไม่มีการลบ ปรับปรุง หรือแก้ไขอีก และสามารถนำกลับไปใช้งานได้ใหม่เมื่อต้องการ โดยดำเนินการเป็นไปตามบทบัญญัติของกฎหมาย และระเบียบที่เกี่ยวข้อง ดังนี้

๕.๑) มีการดำเนินการโดยบุคลากรของกรมซึ่งมีหน้าที่รับผิดชอบการดำเนินการนั้น

๕.๒) มีการรักษาความมั่นคงปลอดภัยและความเป็นส่วนบุคคลของข้อมูล

๕.๓) การจัดเก็บถาวร เป็นการดำเนินการกับข้อมูลที่ไม่มีการลบ ปรับปรุงหรือแก้ไขอีกต่อไป และสามารถนำกลับมาใช้งานได้ใหม่เมื่อต้องการ

๕.๔) ในกรณีที่การดำเนินการจัดเก็บข้อมูลส่งผลต่อชุดข้อมูลและเมทาดาตา เจ้าของข้อมูลและบริกรข้อมูลต้องดำเนินการปรับปรุงชุดข้อมูลและเมทาดาตาให้มีความถูกต้อง ครบถ้วน และเป็นปัจจุบัน

๖) กระบวนการทำลายข้อมูล (Destroy) เป็นการทำลายข้อมูล ซึ่งปกติจะเป็นการทำลายข้อมูลที่มีการจัดเก็บถาวรเป็นระยะเวลานานหรือเกินกว่าระยะเวลาที่กำหนด โดยดำเนินการเป็นไปตามบทบัญญัติของกฎหมาย และระเบียบที่เกี่ยวข้อง ดังนี้

๖.๑) มีการดำเนินการโดยบุคลากรของจังหวัดซึ่งมีหน้าที่รับผิดชอบการดำเนินการนั้น

๖.๒) มีการรักษาความมั่นคงปลอดภัยและความเป็นส่วนบุคคลของข้อมูล

๖.๓) การทำลายข้อมูล เป็นการดำเนินการกับข้อมูลที่ไม่ต้องการนำกลับมาใช้งานได้อีกต่อไป

๖.๔) ในกรณีที่การทำลายข้อมูล ส่งผลต่อชุดข้อมูลและเมทาดาตา เจ้าของข้อมูล และบริกรข้อมูล ต้องดำเนินการปรับปรุงชุดข้อมูลและเมทาดาตาให้มีความถูกต้อง ครบถ้วน และเป็นปัจจุบัน

<u>บทบาทหน้าที่</u>

ผู้บริหารจัดการข้อมูล ประกอบด้วย เจ้าของข้อมูลและบริกรข้อมูล มีหน้าที่ความรับผิดชอบ คือ

- กำหนดโครงสร้างและความสัมพันธ์ของข้อมูล โดยพิจารณาจากความต้องการข้อมูล และวัตถุประสงค์ของหน่วยงาน
- พัฒนาสถาปัตยกรรมข้อมูลในภาพรวมของทั้งหน่วยงาน โดยประเมินสถานะ ในปัจจุบันและออกแบบเพื่อปรับปรุงสำหรับอนาคต
- บริหารจัดการ และควบคุมเกี่ยวกับระบบฐานข้อมูลภายในหน่วยงาน
- กำหนดนโยบาย มาตรการ และมาตรฐานของระบบฐานข้อมูลทั้งหมดภายใน หน่วยงาน เช่น รายละเอียดและวิธีการจัดเก็บข้อมูล การใช้งานฐานข้อมูล การรักษาความปลอดภัยของข้อมูล การสำรองข้อมูล การกู้คืนข้อมูล
- ออกแบบวิธีการจัดเก็บ และเรียกใช้งานข้อมูล
- จัดการเกี่ยวกับข้อมูลทั้งหมด ตั้งแต่ระบุชนิดของข้อมูล วางโครงสร้างของการเข้าและการออกของข้อมูล เพื่อให้ข้อมูลไหลได้อย่างไม่สะดุด
- วิเคราะห์และออกแบบระบบ โดยศึกษาเกี่ยวกับปัญหา รวบรวมความต้องการของผู้ใช้งานระบบ วิเคราะห์ระบบงานภายในหน่วยงาน
- ออกแบบและพัฒนาแบบจำลองข้อมูล (Data Model) เพื่ออธิบายลักษณะโครงสร้าง และการทำงานของข้อมูลให้เห็นภาพได้มากขึ้น

ทีมบริกรข้อมูล มีหน้าที่ความรับผิดชอบ คือ

- นำข้อมูลมาวิเคราะห์แนวโน้ม หรือแก้ปัญหาจากสิ่งที่ผิดแปลกไปจากแนวโน้มเดิม โดยใช้ประสบการณ์ และหลักสถิติ
- ใช้โมเดลหรือเครื่องมือในการทำรายงาน เพื่อสรุปข้อมูลสำหรับใช้ในการตัดสินใจ
- นำข้อมูลจากหลายๆ แหล่ง และแปลงข้อมูล เพื่อหารูปแบบและความสัมพันธ์ของข้อมูล
- สร้างแบบจำลอง และดำเนินการกับข้อมูลด้วยวิธีการต่างๆ เช่น Machine Learning หรือเขียนโปรแกรม เพื่อทำนายมุมมอง และคำตอบใหม่ๆ
- ศึกษาและวิเคราะห์ข้อมูลที่เกี่ยวข้องกับเทคโนโลยี กลยุทธ์ กลุ่มเป้าหมาย และหน่วยงานที่เกี่ยวข้อง
- ทำความเข้าใจเป้าหมายและปัญหาของหน่วยงาน วิเคราะห์ความต้องการ และหาคำตอบเพื่อวางแผนด้านกลยุทธ์ และผลักดันให้เกิดการเปลี่ยนแปลง

จังหวัดสิงห์บุรี