(ร่าง) นโยบายธรรมาภิบาลข้อมูล (Data Governance Policy) จังหวัดสุรินทร์

หลักการ

จังหวัดสุรินทร์ เป็นส่วนราชการที่รับผิดชอบด้านการบริหารจัดการ การปกครอง การพัฒนา รวมทั้งการให้บริการสาธารณะ ดังนั้น เพื่อให้การดำเนินงานของจังหวัดฯ สอดคล้องกับพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 รวมทั้งกฎหมายอื่นที่เกี่ยวข้องและใช้บังคับอยู่ในปัจจุบัน จังหวัดฯ จึงกำหนดนโยบายและแนวปฏิบัติเกี่ยวกับธรรมาภิบาลข้อมูลภาครัฐ (Data Governance Policy) ขึ้น เพื่อเป็นกลไกสำคัญในการเปลี่ยนผ่านสู่รัฐบาลดิจิทัล นโยบายนี้ไม่ได้เป็นเพียงข้อบังคับทางเทคนิค แต่เป็นฐานรากในการสร้าง "ความเชื่อถือได้" ของข้อมูล เพื่อให้เกิดการบูรณาการข้อมูลภาครัฐอย่างมั่นคง ปลอดภัย และมีธรรมาภิบาลรองรับการเชื่อมโยงข้อมูลระหว่างหน่วยงาน (Government Data Exchange: GDX) ได้อย่างไร้รอยต่อ (Seamless)

ความสำคัญเชิงกลยุทธ์ของธรรมาภิบาลข้อมูล:

- **การยกระดับบริการภาครัฐ** ข้อมูลที่แม่นยำและเชื่อมโยงกันช่วยให้การบริการประชาชนสะดวก รวดเร็ว และลดความซ้ำซ้อน
- **ความถูกต้องและน่าเชื่อถือของข้อมูล** ข้อมูลถูกจัดการให้มีความครบถ้วน เป็นปัจจุบัน และตรวจสอบได้ เพื่อการตัดสินใจเชิงนโยบายที่แม่นยำ
- **การบริหารความเสี่ยงและปฏิบัติตามกฎหมาย** ป้องกันความเสี่ยงทางกฎหมายที่เกี่ยวข้องกับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล (PDPA) และ พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์
- **ความโปร่งใสและนวัตกรรม** สนับสนุนการเปิดเผยข้อมูลสาธารณะเพื่อให้ภาคส่วนต่างๆ นำไปต่อยอดได้อย่างมีประสิทธิภาพ

วัตถุประสงค์ (Objective)

- **เพื่อวางระบบการบริหารจัดการข้อมูล** กำหนดโครงสร้างและแนวทางปฏิบัติที่ชัดเจน ครอบคลุมตั้งแต่นโยบายจนถึงระดับปฏิบัติการ
- **เพื่อกำหนดหน้าที่และความรับผิดชอบ** สร้างความชัดเจนในบทบาทของบุคลากรทุกระดับในการกำกับดูแลข้อมูล
- **เพื่อประกันคุณภาพและความปลอดภัย** มั่นใจว่าข้อมูลที่นำไปใช้หรือแลกเปลี่ยนมีคุณภาพสูง มั่นคง ปลอดภัย และได้รับความยินยอมตามกฎหมาย

ขอบเขตการบังคับใช้

นโยบายนี้ครอบคลุมวงจรชีวิตข้อมูล (Data Lifecycle) และกระบวนการธรรมาภิบาลข้อมูลทั้งหมดของจังหวัดฯ โดยมีผลบังคับใช้กับบุคลากรทุกคน รวมถึงผู้บริหาร ข้าราชการ พนักงานราชการ ลูกจ้าง และผู้มีส่วนได้ส่วนเสียภายนอกที่เข้ามาเกี่ยวข้องกับการจัดการข้อมูลของจังหวัดฯ

ข้อมูล	สิ่งที่สื่อความหมายให้รู้เรื่องราว ข้อเท็จจริง ข้อมูลหรือ สิ่งใดๆ ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเอง หรือโดยผ่านวิธีการใดๆ และไม่ว่าจะได้จัดทำไว้ในรูปแบบของเอกสาร แฟ้มรายงาน หนังสือแผนผังแผนที่ภาพวาด ภาพถ่าย ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏให้เห็นได้
ชุดข้อมูล	ข้อมูลที่รวบรวมมาจากหลายแหล่ง โดยจัดเป็นชุดให้ตรงตามลักษณะโครงสร้างของข้อมูล
ธรรมาภิบาลข้อมูลภาครัฐ	การกำหนดสิทธิในการตัดสินใจและความรับผิดชอบ ในการส่งเสริมให้เกิดกระบวนการจัดทำการใช้งาน และการบริหารจัดการข้อมูลรวมถึงกระบวนการที่กำหนดบทบาท นโยบาย และมาตรฐานที่ช่วยสนับสนุนให้การดำเนินงานเกี่ยวกับข้อมูลมีประสิทธิภาพมากยิ่งขึ้นซึ่งส่งผลให้หน่วยงานสามารถบรรลุเป้าหมายได้
ข้อมูลที่เป็นเอกสาร	ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ
ข้อมูลที่ไม่เป็นเอกสาร	ข้อมูลสารสนเทศ ข้อมูลคอมพิวเตอร์ ข้อมูลอิเล็กทรอนิกส์
เจ้าของข้อมูล	บุคคล/หน่วยงานที่รับผิดชอบเกี่ยวกับข้อมูล ที่สามารถบริหารจัดการและควบคุมชุดข้อมูล สร้าง แก้ไข ลบ กำหนดสิทธิการเข้าถึง อนุญาต หรือ ปฏิเสธการเข้าถึงข้อมูล และเป็นผู้รับผิดชอบต่อความถูกต้อง ทันสมัย ความสมบูรณ์ และการทำลาย รวมถึงกำหนดระดับชั้นความลับ สิทธิ์การใช้งาน และความปลอดภัยของข้อมูล
ผู้ควบคุมข้อมูลส่วนบุคคล	บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผย ข้อมูลส่วนบุคคล
ผู้ประมวลผลข้อมูลส่วนบุคคล	บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผย ข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวต้องไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคลอยู่ด้วย

ผู้ดูแลข้อมูล	ผู้ที่ทำงานร่วมกับเจ้าของข้อมูลโดยตรง ทำหน้าที่จัดเก็บรักษาข้อมูล รวมถึง ป้องกันภัยคุกคาม ทำการสำรองข้อมูล ดำเนินการตามขั้นตอนที่ระบุไว้ในนโยบายและแผนงานความมั่นคงปลอดภัย ทั้งทางด้านระบบสารสนเทศ และที่มิใช่สารสนเทศ
ผู้ใช้ข้อมูล	ผู้ที่ได้รับสิทธิการใช้ข้อมูลจากผู้รับผิดชอบ หรือได้รับมอบหมายให้ใช้ข้อมูลจากผู้บังคับบัญชา รวมถึงผู้ซึ่งได้รับความยินยอมให้ทำงานหรือทำผลประโยชน์ให้แก่หน่วยงาน
ระดับชั้นความลับ	การกำหนดการเปิดเผยข้อมูลต่อผู้อื่นให้เหมาะสมกับสถานะ การใช้งาน ได้แก่ ลับที่สุด ลับมาก ลับ ปกปิด และเปิดเผยสู่สาธารณะได้
ความมั่นคงปลอดภัยของข้อมูล	การธำรงไว้ซึ่งความลับ ความถูกต้องครบถ้วน และการรักษาสภาพพร้อมใช้ ของข้อมูล รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง ความรับผิด การห้าม ปฏิเสธความรับผิด และความน่าเชื่อถือ
เมทาดาตา	คำอธิบายชุดข้อมูลดิจิทัล เพื่อให้ทราบรายละเอียดเกี่ยวกับโครงสร้างของข้อมูล เนื้อหาสาระ รูปแบบการจัดเก็บ แหล่งข้อมูล และสิทธิในการเข้าถึงข้อมูล

นโยบายธรรมาภิบาลข้อมูล (Data Governance Policy) ประกอบด้วย 6 หัวข้อหลัก ได้แก่

1) นโยบายธรรมาภิบาลข้อมูล (Data Governance Policy)

2) นโยบายคุณภาพข้อมูล (Data Quality Policy)

3) นโยบายการเชื่อมโยงและแลกเปลี่ยนข้อมูล (Data Integration and Exchange Policy)

4) มาตรฐานการจัดชั้นความลับข้อมูล (Data Classification Standard)

5) นโยบายความมั่นคงปลอดภัย และความเป็นส่วนบุคคลของข้อมูล (Data Security and Privacy Policy)

6) นโยบายการเปิดเผยข้อมูล (Open Data Policy)

ซึ่งประกอบด้วยรายละเอียด ดังนี้

1. นโยบายธรรมาภิบาลข้อมูล (Data Governance Policy)

วัตถุประสงค์ เพื่อกำหนดแนวทางการดำเนินงานด้านธรรมาภิบาลข้อมูลเนื่องจากการกำหนดนโยบายข้อมูลจัดเป็นส่วนหนึ่งในองค์ประกอบตามกรอบธรรมาภิบาลข้อมูล และให้การบริหารจัดการข้อมูลมีประสิทธิภาพ จึงต้องมีการกำหนดนโยบายที่ระบุอย่างชัดเจน สอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง หรือข้อกำหนดอื่นๆ ที่เกี่ยวข้อง เพื่อให้นโยบายข้อมูลได้ถูกนำมาปฏิบัติอย่างมีประสิทธิภาพและต่อเนื่อง

นโยบาย

1. กำหนดให้มีโครงสร้างคณะกรรมการธรรมาภิบาลข้อมูล และกำหนดบทบาทหน้าที่ความรับผิดชอบในการบริหารจัดการข้อมูล

2. กำหนดหน่วยงานหรือกลุ่มบุคคล เพื่อเป็นเจ้าของข้อมูลในการบริหารจัดการข้อมูลในแต่ละชุดข้อมูล

3. กำหนดมาตรฐาน (Data Standard) และระเบียบปฏิบัติมาตรฐานและการบริหารจัดการคำอธิบายชุดข้อมูล (Metadata) ครอบคลุม บทบาทหน้าที่ความรับผิดชอบ กระบวนการจัดทำคำอธิบายชุดข้อมูลการควบคุม ดูแลและสอบทานคำอธิบายชุดข้อมูล

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

5. 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)

6. ธรรมาภิบาลข้อมูลตลอดวงจรชีวิตของข้อมูล (Data Life Cycle) ตั้งแต่กระบวน 1) การสร้าง (Data Create) 2) การจัดเก็บ (Data Store) 3) การใช้ (Data Usage) ซึ่งประกอบด้วย การแลกเปลี่ยน การเชื่อมโยงข้อมูล และเปิดเผย (Data Exchange Integration & Disclosure) 4) การรักษา (Data Achieve) 5) การทำลาย (Data Destruction)

7. กำหนดกระบวนการธรรมาภิบาลข้อมูลอย่างเป็นรูปธรรม

8. จัดให้มีกระบวนการในการบริหารจัดการความเสี่ยงด้านข้อมูล และสอดคล้องตามการบริหารความเสี่ยงของกระทรวง เพื่อให้มีการบริหารจัดการข้อมูลที่ดี สอดคล้องกับชั้นความลับและความพร้อมใช้

9. กำหนดให้มีการสื่อสารและเผยแพร่นโยบายข้อมูลให้กับผู้ที่เกี่ยวข้องทั้งภายในหน่วยงานและภายนอก

10. ให้มีการฝึกอบรมเพื่อสร้างความตระหนักถึงธรรมาภิบาลข้อมูล และการบริหารจัดการข้อมูล โดยให้ครอบคลุมการบริหารจัดการทุกกระบวนการและวงจรชีวิตของข้อมูล

11. ให้มีการประเมินผลการดำเนินงาน ทบทวน ตรวจสอบ และปรับปรุงนโยบายอย่างต่อเนื่องอย่างน้อย ปีละ 1 ครั้ง

2. **นโยบายคุณภาพข้อมูล (Data Quality Policy)**

วัตถุประสงค์ เพื่อให้การควบคุมคุณภาพข้อมูล สำหรับการนำไปใช้ประโยชน์ในการบริหารงานและการให้บริการประชาชนของจังหวัดสุรินทร์ โดยให้เป็นไปตามอำนาจหน้าที่และวัตถุประสงค์ในการดำเนินงานของจังหวัดสุรินทร์ตามที่กฎหมายกำหนด โดยข้อมูลที่ได้ทำการจัดเก็บนั้น จังหวัดสุรินทร์จะให้ความสำคัญและคำนึงถึงคุณภาพข้อมูล (Data Quality) ในทุกชุดข้อมูล (Dataset) ตลอดวงจรชีวิตข้อมูล

นโยบาย

1. กำหนดมาตรฐานข้อมูลให้เป็นแบบเดียวกัน และมีการควบคุมคุณภาพข้อมูลตลอดทั้งวงจรชีวิตข้อมูล (Data Lifecycle) ของข้อมูลที่ตนเองมีหน้าที่รับผิดชอบนั้น

2. กำหนดให้มีข้อกำหนดพื้นฐานของการบริหารจัดการคุณภาพข้อมูล (Data Quality Management) รวมถึงแนวทางการควบคุมและการปรับปรุงอย่างต่อเนื่อง

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

4. การกำหนดตัวชี้วัดคุณภาพข้อมูล เช่น ความถูกต้อง ความครบถ้วน ความต้องกัน ความเป็นปัจจุบัน ตรงตามความต้องการของผู้ใช้ และพร้อมใช้งาน

5. รายงานคุณภาพข้อมูล ประกอบด้วยการกำหนดระดับมิติตัวชี้วัด และค่าเป้าหมายในการประเมินคุณภาพข้อมูล จะต้องแนบไปกับการใช้ชุดข้อมูล (Dataset) และชุดคำอธิบายข้อมูล

6. การฝึกอบรมเพื่อสร้างความตระหนักถึงคุณภาพของข้อมูล

3. นโยบายการเชื่อมโยงและแลกเปลี่ยนข้อมูล (Data Integration and Exchange Policy)

วัตถุประสงค์ เพื่อการแลกเปลี่ยนข้อมูลทั้งภายในและระหว่างหน่วยงานมีความมั่นคงปลอดภัย และ ข้อมูลมีคุณภาพ สามารถนำไปใช้ประโยชน์ได้อย่างมีประสิทธิภาพ โดยมีวิธีและแนวทางการนำข้อมูลไป เชื่อมโยงและแลกเปลี่ยนกับหน่วยงานภายนอก ให้สอดคล้องกับระเบียบ หลักเกณฑ์ และกฎหมายที่กำหนด บนพื้นฐานของประโยชน์ส่วนรวมเป็นสำคัญ

นโยบาย

1. กำหนดแนวปฏิบัติในการจัดการเรื่องความมั่นคงปลอดภัย คุณภาพข้อมูล และผู้ประสานงานหรือศูนย์ติดต่อ (Contact Center)

2. กำหนดกระบวนการในการเชื่อมโยงและแลกเปลี่ยนข้อมูลให้ชัดเจน เริ่มตั้งแต่ขั้นตอนการเตรียมการ ขั้นตอนเริ่มดำเนินการ ขั้นตอนระหว่างดำเนินการ และขั้นตอนสิ้นสุด การดำเนินการ

3. กำหนดเมทาดาตาของชุดข้อมูลที่ต้องการเชื่อมโยงและแลกเปลี่ยนที่จำเป็นให้ครบถ้วน

4. ทำสัญญาอนุญาตหรือข้อตกลงในการเชื่อมโยงและแลกเปลี่ยนข้อมูลและการนำข้อมูลไปใช้

5. กำหนดเทคโนโลยีและมาตรฐานทางเทคนิคที่ใช้ในการเชื่อมโยงและแลกเปลี่ยนข้อมูล

6. บันทึกรายละเอียดและจัดเก็บข้อมูลการดำเนินงานที่เกิดขึ้นในแต่ละครั้งที่มีการเชื่อมโยงและแลกเปลี่ยนข้อมูล (Log File) ระหว่างหน่วยงาน เพื่อให้สามารถตรวจสอบย้อนกลับได้

7. สามารถตรวจสอบได้ว่าการเชื่อมโยงและแลกเปลี่ยนข้อมูลได้ดำเนินการอย่างเหมาะสมหรือ เป็นไปตามแนวทางปฏิบัติ กระบวนการการเชื่อมโยงและแลกเปลี่ยน และมาตรฐานตามที่กำหนด

8. กำหนดบุคคลหรือกลุ่มบุคคลในการดำเนินการเชื่อมโยงและแลกเปลี่ยนข้อมูล เช่น บุคคลที่ทำหน้าที่ออกแบบกระบวนการและเทคโนโลยีในการเชื่อมโยงและแลกเปลี่ยนข้อมูล (Data Integration Architect) บุคคลที่ทำหน้าที่ดำเนินการเชื่อมโยงและแลกเปลี่ยนข้อมูลให้สอดคล้องกับที่ได้ออกแบบไว้ (Data Integration Specialist)

4. มาตรฐานการจัดชั้นความลับข้อมูล (Data Classification Standard)

วัตถุประสงค์ เพื่อให้การประมวลผลข้อมูลและการใช้ข้อมูลที่มีประสิทธิภาพ ถูกต้อง ตรงตามวัตถุประสงค์ของการใช้ข้อมูลให้เกิดประโยชน์ รวมถึงวิธีการและแนวทางในการขอข้อมูลจากหน่วยงานที่เกี่ยวข้องทั้งภายในและภายนอก กำหนดระดับความสำคัญเพื่อควบคุมสิทธิการเข้าถึง และต้องได้รับการอนุญาตจากเจ้าของข้อมูลก่อนเปิดเผยทุกครั้ง โดยการนำข้อมูลมาใช้ให้เป็นไปตามวัตถุประสงค์ตามที่แจ้ง หากนอกเหนือจากเหตุผลดังกล่าวข้างต้น จะต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อนเปิดเผยทุกครั้ง

นโยบาย

1. ชุดข้อมูลต้องมีการจัดลำดับชั้นความลับของข้อมูล การกำหนดชั้นความลับของข้อมูล และการกำหนดสิทธิ์การเข้าถึง เพื่อให้สอดคล้องกับแนวทางการจัดชั้นความลับของข้อมูล

2. กำหนดแนวปฏิบัติและมาตรฐานของการประมวลผลข้อมูล และทำการสื่อสารให้แก่ผู้ที่เกี่ยวข้องรับทราบ

3. ห้ามเปิดเผยข้อมูลที่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง หลักเกณฑ์ นโยบาย แนวปฏิบัติของจังหวัดสุรินทร์ที่ประกาศใช้ในปัจจุบัน ไม่ว่าข้อมูลจะอยู่ในรูปแบบใดหรือสถานที่ใดก็ตาม

4. การดำเนินการประมวลผลข้อมูลที่เป็นความลับ เช่น ข้อมูลส่วนบุคคล ให้เป็นไปตามขอบเขต เงื่อนไขหรือวัตถุประสงค์ในการยินยอมให้ดำเนินการกับข้อมูลส่วนบุคคลนั้น

5. ต้องมีการเก็บบันทึกประวัติการเข้าถึงและการใช้ข้อมูล (Log Files) เพื่อให้สามารถตรวจสอบย้อนกลับได้

6. บริกรข้อมูล เจ้าของข้อมูล และผู้มีส่วนได้ส่วนเสียกับข้อมูลที่เกี่ยวข้องต้องร่วมกัน จัดทำเมทาดาตา (Meta Data) พร้อมคำอธิบายสำหรับข้อมูลที่จัดเก็บอยู่ในฐานข้อมูล (Database) ในทุกชุดข้อมูล

7. ต้องมีการทบทวนระดับชั้นความลับข้อมูลอย่างน้อยปีละ 1 ครั้ง และให้ดำเนินการปรับปรุงอย่างต่อเนื่อง

5. นโยบายความมั่นคงปลอดภัยและความเป็นส่วนบุคคลของข้อมูล (Data Security and Privacy Policy)

วัตถุประสงค์ เพื่อเป็นการกำหนดแนวทางในการบริหารจัดการความมั่นคงปลอดภัยของข้อมูล และความเป็นส่วนบุคคล ซึ่งจะต้องสอดคล้องกับนโยบายความมั่นคงปลอดภัยและความเป็นส่วนบุคคล ของข้อมูล โดยมุ่งเน้นหลัก CIA (Confidentiality, Integrity, Availability) และการคุ้มครองข้อมูลส่วนบุคคลอย่างเข้มงวดตามวัตถุประสงค์ที่แจ้งไว้

นโยบาย

1. การจัดทำสถาปัตยกรรมความมั่นคงปลอดภัยของข้อมูล (Data Security Architecture)
2. การควบคุมการเข้าถึงข้อมูล (Data Access Control)
3. การตรวจสอบความมั่นคงปลอดภัยของข้อมูล (Data Security Audit)
4. การประเมินความปลอดภัยของข้อมูล (Data Security Assessment)
5. การกำหนดเครื่องมือและเทคโนโลยีความมั่นคงปลอดภัยของข้อมูล (Data Security Tool / Technology)

6. นโยบายการเปิดเผยข้อมูล (Open Data Policy)

วัตถุประสงค์ เพื่อกำหนดนโยบายข้อมูลที่สามารถนำไปใช้ได้โดยอิสระ สนับสนุนการเผยแพร่ข้อมูลในรูปแบบ Machine-readable ที่ประมวลผลได้ง่าย โดยต้องมีการจัดทำเมทาดาตากำกับเพื่อให้สืบค้นได้สะดวก รวมถึงต้องระบุแหล่งที่มา และบางรายการข้อมูลอาจมีเงื่อนไขตามที่เจ้าของข้อมูลกำหนด

นโยบาย

1. กำหนดบทบาทหน้าที่ที่เกี่ยวข้องกับการเปิดเผยข้อมูล ได้แก่ กำหนดบุคคลหรือกลุ่มบุคคลที่มีสิทธิตัดสินใจในการเปิดเผยข้อมูล กำหนดบุคคลหรือกลุ่มบุคคลในการดำเนินการและปรับปรุงการเปิดเผยข้อมูล และกำหนดบุคคลหรือกลุ่มบุคคลในการรับเรื่องและแก้ไขปัญหาเบื้องต้น ในการเข้าถึงข้อมูลและการนำข้อมูลไปใช้
2. ห้ามเปิดเผยข้อมูลที่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง นโยบาย แนวปฏิบัติ ไม่ว่าข้อมูลจะอยู่ในรูปแบบใดหรือสถานที่ใดก็ตาม
3. ต้องได้รับการอนุญาตจากเจ้าของข้อมูล (Data Owner) ก่อนการเปิดเผยข้อมูลทุกครั้ง
4. ให้มีการจัดเตรียมข้อมูลที่อยู่ในรูปแบบที่ได้จัดทำไว้เป็นมาตรฐานตามกำหนด และง่ายต่อการนำไปใช้
5. มีการจัดทำเมทาดาตา (Meta Data) ควบคู่ไปกับรายการข้อมูลที่เปิดเผยต่อสาธารณะ
6. ให้มีการคัดเลือกชุดข้อมูลที่ต้องการเผยแพร่ โดยหน่วยงานเจ้าของข้อมูลหรือผู้ที่ได้รับมอบหมาย
7. สามารถตรวจสอบได้ว่าการเปิดเผยข้อมูลได้ถูกดำเนินการอย่างเหมาะสมหรือเป็นไปตามแนวทางที่ได้กำหนดไว้ เพื่อให้ได้ข้อมูลที่มีคุณภาพ และเป็นการรักษาคุณภาพของข้อมูล
8. ต้องปฏิบัติตามอย่างเคร่งครัด และป้องกันมิให้มีการเปิดเผยข้อมูล โดยไม่ได้รับอนุญาต

7. วงจรชีวิตข้อมูล 6 ขั้นตอน (Data Lifecycle Management)

จังหวัดสุรินทร์ บริหารจัดการข้อมูลผ่านวงจรชีวิตที่เข้มงวด เพื่อให้เกิดความรับผิดชอบ (Accountability) ในทุกขั้นตอน

1. **การสร้างข้อมูล (Create):** การจัดทำข้อมูลขึ้นใหม่ด้วยวิธีการบันทึกด้วยมือหรืออุปกรณ์อิเล็กทรอนิกส์
2. **การจัดเก็บข้อมูล (Store):** การนำข้อมูลไปจัดเก็บในระบบฐานข้อมูลหรือคลาวด์อย่างปลอดภัย และต้องมีการรักษาคุณภาพข้อมูลในขั้นตอนนี้ตามมาตรฐาน
3. **การใช้ข้อมูล (Use):** การนำข้อมูลมาประมวลผลหรือวิเคราะห์เพื่อสนับสนุนการปฏิบัติงานและการตัดสินใจ
4. **การเผยแพร่ข้อมูล (Publish):** การแลกเปลี่ยนข้อมูลระหว่างหน่วยงานหรือเปิดเผยต่อสาธารณะตามช่องทางที่กำหนด
5. **การจัดเก็บข้อมูลถาวร (Archive):** การคัดแยกและทำสำเนาข้อมูลเพื่อการรักษาไว้ในระยะยาว (Preservation) โดยไม่มีการปรับปรุงหรือเปลี่ยนแปลงข้อมูลนั้นอีก เพื่อใช้ในการอ้างอิงหรือตรวจสอบ
6. **การทำลายข้อมูล (Destroy):** การกำจัดข้อมูลที่หมดความจำเป็นหรือสิ้นสุดอายุการใช้งานอย่างถูกวิธี เพื่อป้องกันความเสี่ยงจากการรั่วไหลของข้อมูล

เอกสารที่เกี่ยวข้อง

1. พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562
2. พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549
3. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
4. พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540
5. พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549
6. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์พ.ศ. 2550
7. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
8. พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553