

นโยบายธรรมาภิบาลข้อมูล (Data Governance Policy)

จังหวัดสุโขทัย

นโยบายธรรมาภิบาลข้อมูล (Data Governance Policy)

ของจังหวัดสุโขทัย

ธรรมาภิบาลข้อมูลภาครัฐ เป็นการกำหนดสิทธิในการตัดสินใจและความรับผิดชอบ ในการส่งเสริมให้เกิดกระบวนการจัดทำ การใช้งาน และการบริหารจัดการข้อมูล รวมถึงกระบวนการที่กำหนดบทบาท นโยบาย และมาตรฐานที่ช่วยสนับสนุนให้การดำเนินงานเกี่ยวกับข้อมูลมีประสิทธิภาพมากยิ่งขึ้น ซึ่งส่งผลให้หน่วยงานสามารถบรรลุเป้าหมายได้

จังหวัดสุโขทัยได้ให้ความสำคัญกับการจัดทำนโยบายธรรมาภิบาลข้อมูล เพื่อให้จังหวัดสุโขทัยมีนโยบายธรรมาภิบาลข้อมูล และบริหารจัดการข้อมูลอย่างเหมาะสม เพียงพอ สอดคล้องกับภารกิจของหน่วยงาน ครอบคลุม โครงสร้างธรรมาภิบาลข้อมูล บทบาท และหน้าที่ความรับผิดชอบของผู้บริหาร หน่วยงาน และบุคลากรที่เกี่ยวข้อง

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) นโยบายความมั่นคงปลอดภัยและความเป็นส่วนบุคคลของข้อมูล (Data Security and Privacy Policy)
6) นโยบายการเปิดเผยข้อมูล (Open Data Policy)

หลักการ

จังหวัดสุโขทัย เป็นส่วนราชการที่รับผิดชอบการให้บริการสาธารณะ โดยคำนึงถึงประโยชน์ของประชาชนเป็นสำคัญ เป็นไปตามพระราชบัญญัติปรับปรุงกระทรวง ทบวง กรม พ.ศ. 2545 และเพื่อให้ดำเนินงานสอดคล้องกับพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 รวมทั้งกฎหมายที่เกี่ยวข้องที่ใช้บังคับอยู่ในปัจจุบัน จึงกำหนดนโยบายและแนวปฏิบัติธรรมาภิบาลข้อมูลภาครัฐ ไว้ดังต่อไปนี้

ขอบเขต (Scope)

ขอบเขตของนโยบายนี้ครอบคลุมวงจรชีวิตของข้อมูล (Data Life Cycle) และกระบวนธรรมาภิบาลข้อมูล (Data Governance Process) การดำเนินงานตามภารกิจของจังหวัดสุโขทัย และมีผลบังคับใช้ไปถึงบุคลากรและ/หรือหน่วยงานภายในทั้งหมด ได้แก่ ผู้บริหาร ข้าราชการ พนักงานประจำ ลูกจ้างประจำ ลูกจ้างชั่วคราว ผู้มีส่วนได้ส่วนเสีย เป็นต้น

วัตถุประสงค์

เพื่อให้จังหวัดสุโขทัย มีนโยบายธรรมาภิบาลข้อมูลและบริหารจัดการข้อมูลอย่างเหมาะสมเพียงพอ สอดคล้องกับภารกิจของหน่วยงาน ครอบคลุม โครงสร้างธรรมาภิบาลข้อมูล บทบาทและหน้าที่ความรับผิดชอบของผู้บริหารระดับสูง หน่วยงาน บุคลากรที่เกี่ยวข้อง

คำนิยาม (Definitions)

ข้อมูล	สิ่งที่สื่อความหมายให้รู้เรื่องราว ข้อเท็จจริง ข้อมูลหรือ สิ่งใด ๆ ไม่ว่าการสื่อความหมายนั้นจะทาได้โดยสภาพของสิ่งนั้นเอง หรือโดยผ่านวิธีการใด ๆ และไม่ว่าจะได้จัดทำไว้ในรูปแบบของเอกสาร แฟ้มรายงาน หนังสือแผนผัง แผนที่ ภาพวาด ภาพถ่าย ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ หรือวิธีอื่นใดที่ทาให้สิ่งที่บันทึกไว้ปรากฏได้
ชุดข้อมูล	ข้อมูลที่รวบรวมมาจากหลายแหล่ง โดยจัดเป็นชุดให้ตรงตามลักษณะโครงสร้างของข้อมูล
ธรรมาภิบาลข้อมูลภาครัฐ	การกำหนดสิทธิในการตัดสินใจและความรับผิดชอบ ในการส่งเสริมให้เกิดกระบวนการจัดทำ การใช้งาน และการบริหารจัดการข้อมูลรวมถึงกระบวนการที่กำหนดบทบาท นโยบาย และมาตรฐานที่ช่วยสนับสนุนให้การดำเนินงานเกี่ยวกับข้อมูลมีประสิทธิภาพมากยิ่งขึ้น ซึ่งส่งผลให้หน่วยงานสามารถบรรลุเป้าหมายได้

คณะกรรมธรรมาภิบาลข้อมูล	กลุ่มบุคคลที่มีอำนาจในการผลักดันให้เกิดธรรมาภิบาลข้อมูล โดยมีหน้าที่รับผิดชอบในการกำหนดเป้าหมาย กำกับดูแลและติดตาม การดำเนินงาน รวมถึงให้คำปรึกษาและตัดสินประเด็นสำคัญที่เกี่ยวข้องกับข้อมูล สนับสนุน ส่งเสริม ผลักดันธรรมาภิบาลข้อมูลและการสื่อสารให้บุคลากรในกระทรวง ตระหนักถึงความสำคัญของข้อมูล การใช้ข้อมูลอย่างปลอดภัย
คณะทำงานทีมบริกรข้อมูล	กลุ่มบุคคลที่มุ่งเน้นการดำเนินงานและนิยามคำอธิบายชุดข้อมูลทั้งเชิงธุรกิจและเทคโนโลยีสารสนเทศ ร่างนโยบาย กำหนดมาตรฐานตรวจสอบการปฏิบัติงานวิเคราะห์ผลจากการตรวจสอบ ในการบริหารจัดการตามองค์ประกอบของการบริหารจัดการข้อมูล
ข้อมูลส่วนบุคคล	ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ
ข้อมูลที่เป็นเอกสาร	ข้อมูลที่มีการจัดเก็บและบันทึกในรูปแบบของกระดาษ
ข้อมูลที่ไม่เป็นเอกสาร	ข้อมูลสารสนเทศ ข้อมูลคอมพิวเตอร์ ข้อมูลอิเล็กทรอนิกส์
เจ้าของข้อมูล	บุคคล/หน่วยงานที่รับผิดชอบเกี่ยวกับข้อมูล ที่สามารถบริหารจัดการและควบคุมชุดข้อมูล สร้าง แก้ไข ลบ กำหนดสิทธิการเข้าถึง อนุญาต หรือปฏิเสธการเข้าถึงข้อมูล และเป็นผู้รับผิดชอบต่อความถูกต้อง ทันสมัย ความสมบูรณ์ และการทำลาย รวมถึงกำหนดระดับชั้นความลับ สิทธิ์การใช้งานและความปลอดภัยของข้อมูล
ผู้ควบคุมข้อมูลส่วนบุคคล	บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคล
ผู้ประมวลผลข้อมูลส่วนบุคคล	บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล
ผู้ดูแลข้อมูล	ผู้ที่ทำงานร่วมกับเจ้าของข้อมูลโดยตรง ทำหน้าที่จัดเก็บรักษาข้อมูลรวมถึงป้องกันภัยคุกคาม ทำการสำรองข้อมูล ดำเนินการตามขั้นตอนที่ระบุไว้ในนโยบายและแผนงานความมั่นคงปลอดภัย ทั้งทางด้านระบบสารสนเทศและที่มิใช่สารสนเทศ

ผู้ใช้ข้อมูล	ผู้ที่ได้รับสิทธิการใช้ข้อมูลจากผู้รับผิดชอบ หรือได้รับมอบหมายให้ใช้ข้อมูลจากผู้บังคับบัญชา รวมถึงผู้ซึ่งได้รับความยินยอมให้ทำงานหรือทำผลประโยชน์ให้แก่หน่วยงาน
ระดับชั้นความลับ	การกำหนดการเปิดเผยข้อมูลต่อผู้อื่นให้เหมาะสมกับสถานะ การใช้งาน ได้แก่ ลับที่สุด ลับมาก ลับ ปกปิด และเปิดเผยสู่ภายนอกได้
ความมั่นคงปลอดภัยของข้อมูล	การธำรงไว้ซึ่งความลับ ความถูกต้อง ครบถ้วน และการรักษาสภาพพร้อมใช้ของข้อมูล รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง ความรับผิด การห้าม ปฏิเสธความรับผิด และความน่าเชื่อถือ
เมทาดาตา	คำอธิบายชุดข้อมูลดิจิทัล เพื่อให้ทราบรายละเอียดเกี่ยวกับโครงสร้างของข้อมูล เนื้อหาสาระ รูปแบบการจัดเก็บ แหล่งข้อมูล และสิทธิ ในการเข้าถึงข้อมูล

นโยบายธรรมาภิบาลข้อมูล (Data Governance Policy)

1. นโยบายธรรมาภิบาลข้อมูล (Data Governance Policy)

วัตถุประสงค์

เพื่อกำหนดแนวทางการดำเนินงานด้านธรรมาภิบาลข้อมูลเนื่องจากการกำหนดนโยบายข้อมูลจัดเป็นหนึ่งในองค์ประกอบตามกรอบการธรรมาภิบาลข้อมูล และให้การบริหารจัดการข้อมูลมีประสิทธิภาพ จึงต้องมีการกำหนดนโยบายที่ระบุอย่างชัดเจน สอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง หรือข้อกำหนดอื่น ๆ ที่เกี่ยวข้อง เพื่อให้นโยบายข้อมูลได้ถูกนำมาปฏิบัติอย่าง มีประสิทธิภาพและต่อเนื่อง

นโยบาย

1. กำหนดให้มีโครงสร้างคณะกรรมการธรรมาภิบาลข้อมูล และกำหนดบทบาทหน้าที่ความรับผิดชอบในการบริหารจัดการข้อมูล

2. กำหนดหน่วยงานที่เป็นเจ้าของข้อมูลในการบริหารจัดการข้อมูลในแต่ละชุดข้อมูล

3. กำหนดมาตรฐาน (Data Standard) และระเบียบปฏิบัติมาตรฐานและการบริหารจัดการคำอธิบาย ชุดข้อมูล (Metadata) ครอบคลุม บทบาทหน้าที่ความรับผิดชอบ กระบวนการจัดทำคำอธิบายชุดข้อมูลการควบคุมดูแลและสอบทานคำอธิบายชุดข้อมูล

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) ซึ่งมีกระบวนดังนี้ (1) การสร้าง (Data Create) (2) การจัดเก็บ (Data Store) (3) การใช้ (Data Usage) ประกอบด้วย การแลกเปลี่ยน การเชื่อมโยงข้อมูล และเปิดเผย (Data Exchange Integration & Disclosure) (4) การรักษา (Data Achieve) (5) การทำลาย (Data Destruction)

7. กำหนดกระบวนการธรรมาภิบาลข้อมูลอย่างเป็นรูปธรรม

8. จัดให้มีกระบวนการในการบริหารจัดการความเสี่ยงด้านข้อมูล และสอดคล้องตามการบริหาร ความเสี่ยงของกระทรวง เพื่อให้มีการบริหารจัดการข้อมูลที่ดี สอดคล้องกับชั้นความลับและความพร้อมใช้

9. กำหนดให้มีการสื่อสารและเผยแพร่นโยบายข้อมูลให้กับผู้ที่เกี่ยวข้องทั้งภายในหน่วยงานและภายนอก

10. ให้มีการฝึกอบรมเพื่อสร้างความตระหนักถึงธรรมาภิบาลข้อมูล และการบริหารจัดการข้อมูล โดยให้ครอบคลุมการบริหารจัดการทุกกระบวนการและวงจรชีวิตของข้อมูล

11. ให้มีการประเมินผลการดำเนินงาน ทบทวน ตรวจสอบ และปรับปรุงนโยบายอย่างต่อเนื่อง อย่างน้อยปีละ 1 ครั้ง

2. นโยบายคุณภาพข้อมูล (Data Quality Policy)

วัตถุประสงค์

เพื่อให้การควบคุมคุณภาพข้อมูล สำหรับการนำไปใช้ประโยชน์ในการบริหารงานและการให้บริการประชาชนของจังหวัดสุโขทัย โดยให้เป็นไปตามอำนาจหน้าที่และวัตถุประสงค์ในการดำเนินงานของจังหวัดตามที่กฎหมายกำหนด โดยข้อมูลที่ได้ทำการจัดเก็บนั้น จังหวัดจะคำนึงถึงคุณภาพข้อมูล (Data Quality) ในทุกชุดข้อมูล (Dataset)

นโยบาย

1. กำหนดมาตรฐานข้อมูลให้เป็นแบบเดียวกัน และมีการควบคุมคุณภาพข้อมูลตลอดทั้งวงจรชีวิตข้อมูล (Data Lifecycle) ของข้อมูลที่ตนเองมีหน้าที่รับผิดชอบนั้น

2. กำหนดให้มีข้อกำหนดพื้นฐานของการบริหารจัดการคุณภาพข้อมูล (Data Quality Management) รวมถึงแนวทางการควบคุมและการปรับปรุงอย่างต่อเนื่อง

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

4. การกำหนดตัวชี้วัดคุณภาพข้อมูล เช่น ความถูกต้อง ความครบถ้วน ความต้องกัน ความเป็นปัจจุบัน ตรงตามความต้องการของผู้ใช้ และพร้อมใช้งาน

5. รายงานคุณภาพข้อมูล ประกอบด้วย การกำหนดระดับมิติตัวชี้วัด และค่าเป้าหมายในการประเมินคุณภาพข้อมูล จะต้องแนบไปกับการใช้ชุดข้อมูล (Dataset) และชุดคำอธิบายข้อมูล

6. การฝึกอบรมเพื่อสร้างความตระหนักถึงคุณภาพของข้อมูล

3. นโยบายการเชื่อมโยงและแลกเปลี่ยนข้อมูล (Data Integration and Exchange Policy)

วัตถุประสงค์

เพื่อการแลกเปลี่ยนข้อมูลทั้งภายในและระหว่างหน่วยงานมีความมั่นคงปลอดภัย และข้อมูลมีคุณภาพ สามารถนำไปใช้ประโยชน์ได้อย่างมีประสิทธิภาพ โดยมีวิธีและแนวทางการนำข้อมูลไปเชื่อมโยงและแลกเปลี่ยนกับหน่วยงานภายนอก ให้สอดคล้องกับระเบียบ หลักเกณฑ์ และกฎหมายที่กำหนด บนพื้นฐานของประโยชน์ส่วนรวมเป็นสำคัญ

นโยบาย

1. กำหนดแนวปฏิบัติในการจัดการเรื่องความมั่นคงปลอดภัย คุณภาพข้อมูล และผู้ประสานงานหรือศูนย์ติดต่อ (Contact Center)

2. กำหนดกระบวนการในการเชื่อมโยงและแลกเปลี่ยนข้อมูลให้ชัดเจน เริ่มตั้งแต่ขั้นตอน การเตรียมการขั้นตอนเริ่มดำเนินการ ขั้นตอนระหว่างดำเนินการ และขั้นตอนสิ้นสุดการดำเนินการ

3. กำหนดเมทาดาตาของชุดข้อมูลที่ต้องการเชื่อมโยงและแลกเปลี่ยนที่จำเป็นให้ครบถ้วน

4. ทำสัญญาอนุญาตหรือข้อตกลงในการเชื่อมโยงและแลกเปลี่ยนข้อมูลและการนำข้อมูลไปใช้

5. กำหนดเทคโนโลยีและมาตรฐานทางเทคนิคที่ใช้ในการเชื่อมโยงและแลกเปลี่ยนข้อมูล

6. บันทึกรายละเอียดและจัดเก็บข้อมูลการดำเนินงานที่เกิดขึ้นในแต่ละครั้งที่มีการ เชื่อมโยงและแลกเปลี่ยนข้อมูล (Log File) ระหว่างหน่วยงาน เพื่อให้สามารถตรวจสอบย้อนกลับได้

7. สามารถตรวจสอบได้ว่าการเชื่อมโยงและแลกเปลี่ยนข้อมูลได้ดาเนินการอย่าง เหมาะสมหรือเป็นไปตามแนวทางปฏิบัติ กระบวนการการเชื่อมโยงและแลกเปลี่ยน และมาตรฐานตามที่กำหนด

8. กำหนดบุคคลหรือกลุ่มบุคคลในการดำเนินการเชื่อมโยงและแลกเปลี่ยนข้อมูล เช่น บุคคลที่ทาหน้าที่ออกแบบกระบวนการและเทคโนโลยีในการเชื่อมโยงและแลกเปลี่ยน ข้อมูล (Data Integration Architect) บุคคลที่ทำหน้าที่ดำเนินการเชื่อมโยงและแลกเปลี่ยนข้อมูลให้สอดคล้องกับที่ได้ออกแบบไว้ (Data Integration Specialist)

4. มาตรฐานการจัดชั้นความลับข้อมูล (Data Classification Standard)

วัตถุประสงค์

เพื่อให้การประมวลผลข้อมูลและการใช้ข้อมูลที่มีประสิทธิภาพ ถูกต้อง ตรงตามวัตถุประสงค์ของ การใช้ข้อมูลให้เกิดประโยชน์ รวมถึงวิธีการและแนวทางในการขอข้อมูลจากหน่วยงานที่เกี่ยวข้องทั้งภายในและภายนอก เพื่อนำมาใช้ในการประมวลผลและนำมาใช้ ทั้งนี้ การนำข้อมูลมาใช้ให้เป็นไปตามวัตถุประสงค์ตามที่แจ้ง หากนอกเหนือจากเหตุผลดังกล่าวข้างต้น จะต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อน

นโยบาย

1. ชุดข้อมูลต้องมีการจัดลำดับชั้นความลับของข้อมูล การกำหนดชั้นความลับของข้อมูล และการกำหนดสิทธิ์การเข้าถึง เพื่อให้สอดคล้องกับแนวทางการจัดชั้นความลับของข้อมูล

2. กำหนดแนวปฏิบัติและมาตรฐานของการประมวลผลข้อมูล และทำการสื่อสารให้แก่ผู้ที่เกี่ยวข้องรับทราบ

3. ห้ามเปิดเผยข้อมูลที่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง หลักเกณฑ์ นโยบาย แนวปฏิบัติของจังหวัดสุโขทัย ที่ประกาศใช้ในปัจจุบัน ไม่ว่าข้อมูลจะอยู่ในรูปแบบใดหรือสถานที่ใดก็ตาม

4. การดำเนินการประมวลผลข้อมูลที่เป็นความลับ เช่น ข้อมูลส่วนบุคคล ให้เป็นไปตามขอบเขต เงื่อนไข หรือวัตถุประสงค์ในการยินยอมให้ดำเนินการกับข้อมูลส่วนบุคคลนั้น

5. ต้องมีการเก็บบันทึกประวัติการเข้าถึงและการใช้ข้อมูล (Log Files) เพื่อให้สามารถตรวจสอบย้อนกลับได้

6. บริกรข้อมูล เจ้าของข้อมูล และผู้มีส่วนได้ส่วนเสียกับข้อมูลที่เกี่ยวข้องต้องร่วมกัน จัดทำเมทาดาตาพร้อมคำอธิบาย (Metadata) สำหรับข้อมูลที่จัดเก็บอยู่ในฐานข้อมูล (Database) ในทุกชุดข้อมูล

7. ต้องมีการทบทวนระดับชั้นความลับข้อมูล อย่างน้อยปีละ 1 ครั้ง และให้ดำเนินการปรับปรุงอย่างต่อเนื่อง

5. นโยบายความมั่นคงปลอดภัยและความเป็นส่วนบุคคลของข้อมูล (Data Security and Privacy Policy)

วัตถุประสงค์

เพื่อเป็นการกำหนดแนวทางในการบริหารจัดการความมั่นคงปลอดภัยของข้อมูลและความเป็นส่วนบุคคล ซึ่งจะต้องสอดคล้องกับนโยบายความมั่นคงปลอดภัยและความเป็นส่วนบุคคลของข้อมูล

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 สามารถนำกลับมาใช้ใหม่และแจกจ่ายได้โดยใครก็ตาม แต่ต้องระบุแหล่งที่มาหรือเจ้าของงานและต้องใช้สัญญาอนุญาต หรือเงื่อนไขเดียวกันกับที่มาหรือตามเจ้าของข้อมูลกำหนด

นโยบาย

1. กำหนดบทบาทหน้าที่ ที่เกี่ยวข้องกับการเปิดเผยข้อมูล ได้แก่ กำหนดบุคคลหรือกลุ่มบุคคลที่มีสิทธิ์ตัดสินใจในการเปิดเผยข้อมูล กำหนดบุคคลหรือกลุ่มบุคคลในการดำเนินการและปรับปรุงการเปิดเผยข้อมูล และกำหนดบุคคลหรือกลุ่มบุคคลในการรับเรื่องและแก้ไขปัญหาเบื้องต้นในการเข้าถึงข้อมูลและการนำข้อมูลไปใช้
2. ห้ามเปิดเผยข้อมูลที่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง นโยบาย แนวปฏิบัติ ไม่ว่าข้อมูลจะอยู่ในรูปแบบใดหรือสถานที่ใดก็ตาม
3. ต้องได้รับการอนุญาตจากเจ้าของข้อมูล (Data Owner) ก่อนการเปิดเผยข้อมูล
4. ให้มีการจัดเตรียมข้อมูลที่อยู่ในรูปแบบที่ได้จัดทำไว้เป็นมาตรฐานตามกำหนด และง่ายต่อการนำไปใช้
5. มีการจัดทาเมทาดาตาควบคู่ไปกับข้อมูลที่เปิดเผย
6. ให้มีการคัดเลือกชุดข้อมูลที่ต้องการเผยแพร่ โดยหน่วยงานเจ้าของข้อมูลหรือผู้ที่ได้รับมอบหมาย
7. สามารถตรวจสอบได้ว่าการเปิดเผยข้อมูลได้ถูกดำเนินการอย่างเหมาะสมหรือเป็นไปตามแนวทางที่ได้กำหนดไว้ เพื่อให้ได้ข้อมูลที่มีคุณภาพ และเป็นการรักษาคุณภาพของข้อมูล
8. ต้องปฏิบัติตามอย่างเคร่งครัด และป้องกันมิให้มีการเปิดเผยข้อมูล โดยไม่ได้รับอนุญาต

เอกสารที่เกี่ยวข้อง

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