นโยบายธรรมาภิบาลข้อมูล

นโยบายธรรมาภิบาลข้อมูล (Data Governance Policy) ประกอบด้วย ๖ หัวข้อหลัก ได้แก่ ๑) นโยบายธรรมาภิบาลข้อมูล (Data Governance Policy) ๒) นโยบายคุณภาพข้อมูล (Data Quality Policy) ๓) นโยบายการเชื่อมโยงและแลกเปลี่ยนข้อมูล (Data Integration and Exchange Policy) ๔) มาตรฐานการจัดชั้นความลับข้อมูล (Data Classification Standard) ๕) นโยบายความมั่นคงปลอดภัยและความเป็นส่วนบุคคลของข้อมูล (Data Security and Privacy Policy) และ ๖) นโยบายการเปิดเผยข้อมูล (Open Data Policy) รายละเอียด ดังนี้

๑. นโยบายธรรมาภิบาลข้อมูล (Data Governance Policy)

วัตถุประสงค์

เพื่อกำหนดแนวทางการดำเนินงานด้านธรรมาภิบาลข้อมูลตามกรอบการธรรมาภิบาลข้อมูล และให้การบริหารจัดการข้อมูลมีประสิทธิภาพ สอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง หรือข้อกำหนดอื่น ๆ ที่เกี่ยวข้อง เพื่อให้นโยบายธรรมาภิบาลข้อมูลได้ถูกนำมาปฏิบัติอย่างมีประสิทธิภาพและต่อเนื่อง

นโยบาย

๑. กำหนดให้มีโครงสร้างคณะกรรมการธรรมาภิบาลข้อมูล และกำหนดบทบาทหน้าที่ความรับผิดชอบในการบริหารจัดการข้อมูล

๒. กำหนดหน่วยงานที่เป็นเจ้าของข้อมูลในการบริหารจัดการข้อมูลในแต่ละชุดข้อมูล

๓. กำหนดมาตรฐานข้อมูล (Data Standard) ระเบียบปฏิบัติมาตรฐาน และการบริหารจัดการคำอธิบายชุดข้อมูล (Metadata) ให้ครอบคลุมบทบาทหน้าที่ความรับผิดชอบ กระบวนการจัดทำคำอธิบายชุดข้อมูล การควบคุมดูแลและการสอบทานคำอธิบายชุดข้อมูล

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

๕. จัดทำนโยบายธรรมาภิบาลข้อมูล ซึ่งประกอบด้วย นโยบายคุณภาพข้อมูล (Data Quality Policy) นโยบายการแลกเปลี่ยนและเชื่อมโยงข้อมูล (Data Exchange and Integration Policy) มาตรฐานการจัดชั้นความลับข้อมูล (Data Classification Standard) นโยบายความมั่นคงปลอดภัยและความเป็นส่วนบุคคลของข้อมูล (Data Security and Privacy Policy) และนโยบายการเปิดเผยข้อมูล (Open Data Policy)

๖. กำหนดธรรมาภิบาลข้อมูลตลอดวงจรชีวิตของข้อมูล (Data Lifecycle) ตั้งแต่กระบวนสร้างข้อมูลจนถึงกระบวนการทำลายข้อมูล ประกอบด้วย ๑) การสร้างข้อมูล (Data Create) ๒) การจัดเก็บข้อมูล (Data Store) ๓) การใช้ข้อมูล (Data Usage) ได้แก่ การแลกเปลี่ยนการเชื่อมโยงข้อมูล และการเปิดเผยข้อมูล (Data Exchange Integration & Disclosure) ๔) การรักษาข้อมูล (Data Achieve) และ ๕) การทำลายข้อมูล (Data Disclosure)

๗. กำหนดกระบวนการธรรมาภิบาลข้อมูลอย่างเป็นรูปธรรม

๘. จัดให้มีกระบวนการบริหารจัดการความเสี่ยงด้านข้อมูล และสอดคล้องตามการบริหาร ความเสี่ยงของหน่วยงาน เพื่อให้มีการบริหารจัดการข้อมูลที่ดี สอดคล้องกับชั้นความลับและความพร้อมใช้งาน

๙. กำหนดให้มีการสื่อสารและเผยแพร่นโยบายข้อมูลให้กับผู้ที่เกี่ยวข้องทั้งภายในและภายนอกหน่วยงาน

๑๐. จัดให้มีการฝึกอบรมเพื่อสร้างความตระหนักถึงธรรมาภิบาลข้อมูล และการบริหารจัดการข้อมูล โดยให้ครอบคลุมการบริหารจัดการทุกกระบวนการและวงจรชีวิตของข้อมูล

๑๑. จัดให้มีการประเมินผลการดำเนินงาน ทบทวน และตรวจสอบนโยบายอย่างต่อเนื่องอย่างน้อยปีละ ๑ ครั้ง

๒. นโยบายคุณภาพข้อมูล (Data Quality Policy)

วัตถุประสงค์

เพื่อให้การควบคุมคุณภาพข้อมูลสำหรับการนำไปใช้ประโยชน์ในการบริหารงานและการให้บริการประชาชนเป็นไปตามอำนาจหน้าที่และวัตถุประสงค์ในการดำเนินงานตามที่กฎหมายกำหนด โดยคำนึงถึงคุณภาพข้อมูล (Data Quality) ในทุกชุดข้อมูล (Dataset) ที่ได้ทำการจัดเก็บ

นโยบาย

๑. กำหนดมาตรฐานข้อมูลที่มีหน้าที่รับผิดชอบให้เป็นแบบเดียวกัน และควบคุมคุณภาพข้อมูลตลอดวงจรชีวิตของข้อมูล (Data Lifecycle)

๒. กำหนดให้มีข้อกำหนดพื้นฐานของการบริหารจัดการคุณภาพข้อมูล (Data Quality Management) รวมถึงแนวทางการควบคุมและการปรับปรุงอย่างต่อเนื่อง

๓. กำหนดให้มีการวัดคุณภาพข้อมูล (Data Quality) ในทุกชุดข้อมูล ได้แก่ ความถูกต้อง (Accuracy) ความครบถ้วน (Completeness) ความต้องกัน (Consistency) ความเป็นปัจจุบัน (Timeliness) ตรงตาม ความต้องการของผู้ใช้ (Relevancy) ความน่าเชื่อถือ (Data Integrity) และความพร้อมใช้งาน (Availability) โดยทุกเกณฑ์ เป็นเกณฑ์เชิงปริมาณ (Quantitative Measurement)

๔. กำหนดตัวชี้วัดคุณภาพข้อมูล เช่น ความถูกต้อง ความครบถ้วน ความต้องกัน ความเป็นปัจจุบัน ตรงตามความต้องการของผู้ใช้ และความพร้อมใช้งาน เป็นต้น

๕. กำหนดให้มีการรายงานคุณภาพข้อมูล ประกอบด้วย การกำหนดระดับมิติตัวชี้วัด และค่าเป้าหมายในการประเมินคุณภาพข้อมูล โดยแนบไปกับการใช้ชุดข้อมูล (Dataset) และชุดคำอธิบายข้อมูล

๖. จัดให้มีการฝึกอบรมเพื่อสร้างความตระหนักเกี่ยวกับคุณภาพของข้อมูล

๓. นโยบายการเชื่อมโยงและแลกเปลี่ยนข้อมูล (Data Integration and Exchange Policy)

วัตถุประสงค์

เพื่อให้การแลกเปลี่ยนข้อมูลทั้งภายในและระหว่างหน่วยงานมีความมั่นคงปลอดภัย และมีคุณภาพสามารถนำไปใช้ประโยชน์ได้อย่างมีประสิทธิภาพ โดยมีวิธีและแนวทางการนำข้อมูลไปเชื่อมโยงและแลกเปลี่ยนกับหน่วยงานภายนอก ให้สอดคล้องกับระเบียบ หลักเกณฑ์ และกฎหมายที่กำหนด บนพื้นฐานของประโยชน์ส่วนรวมเป็นสำคัญ

นโยบาย

๑. กำหนดแนวปฏิบัติในการจัดการเรื่องความมั่นคงปลอดภัย คุณภาพข้อมูล และผู้ประสานงานหรือศูนย์ติดต่อ (Contact Center)

๒. กำหนดกระบวนการเชื่อมโยงและแลกเปลี่ยนข้อมูลให้ชัดเจน ตั้งแต่ขั้นตอนการเตรียมการ การเริ่มดำเนินการ ระหว่างดำเนินการ และการสิ้นสุดการดำเนินการ

๓. กำหนดคำอธิบายชุดข้อมูล (Metadata) ของชุดข้อมูลที่ต้องการเชื่อมโยงและแลกเปลี่ยนที่จำเป็นให้มีความครบถ้วน

๔. ทำสัญญาอนุญาตหรือข้อตกลงในการเชื่อมโยงและแลกเปลี่ยนข้อมูลและการนำข้อมูลไปใช้

๕. กำหนดเทคโนโลยีและมาตรฐานทางเทคนิคที่ใช้ในการเชื่อมโยงและแลกเปลี่ยนข้อมูล

๖. บันทึกรายละเอียดและจัดเก็บข้อมูลการดำเนินงานที่เกิดขึ้นในแต่ละครั้งที่มีการเชื่อมโยงและแลกเปลี่ยนข้อมูล (Log File) ระหว่างระบบ ทั้งการเชื่อมโยงภายในหน่วยงานและการเชื่อมโยงระหว่างหน่วยงาน เพื่อให้สามารถตรวจสอบย้อนกลับได้

๗. ตรวจสอบการเชื่อมโยงและแลกเปลี่ยนข้อมูลให้มีการดำเนินการอย่างเหมาะสมหรือเป็นไปตามแนวทางปฏิบัติ กระบวนการการเชื่อมโยงและแลกเปลี่ยน และมาตรฐานตามที่กำหนด

๘. กำหนดบุคคลหรือกลุ่มบุคคลในการดำเนินการเชื่อมโยงและแลกเปลี่ยนข้อมูล เช่น บุคคลที่ทำหน้าที่ออกแบบกระบวนการและเทคโนโลยีในการเชื่อมโยงและแลกเปลี่ยนข้อมูล (Data Integration Architect) และบุคคลที่ทำหน้าที่ดำเนินการเชื่อมโยงและแลกเปลี่ยนข้อมูลให้สอดคล้องกับที่ได้ออกแบบไว้ (Data Integration Specialist) เป็นต้น

๔. มาตรฐานการจัดชั้นความลับข้อมูล (Data Classification Standard)

วัตถุประสงค์

เพื่อให้การประมวลผลข้อมูลและการใช้ข้อมูลเป็นไปอย่างมีประสิทธิภาพ ถูกต้อง ตรงตามวัตถุประสงค์ของการใช้ข้อมูลให้เกิดประโยชน์ รวมถึงกำหนดวิธีการและแนวทางในการขอข้อมูลจากหน่วยงานที่เกี่ยวข้องทั้งภายในและภายนอก เพื่อใช้ประโยชน์ในการปฏิบัติงานและการประมวลผล ทั้งนี้การนำข้อมูลมาใช้ให้เป็นไปตามวัตถุประสงค์ตามที่แจ้ง หากนอกเหนือจากเหตุผลดังกล่าวข้างต้น จะต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อน

นโยบาย

๑. กำหนดให้ชุดข้อมูลมีการจัดลำดับชั้นความลับของข้อมูล การกำหนดชั้นความลับของข้อมูล และการกำหนดสิทธิ์การเข้าถึง เพื่อให้สอดคล้องกับแนวทางการจัดชั้นความลับของข้อมูล

๒. กำหนดแนวปฏิบัติและมาตรฐานของการประมวลผลข้อมูล และสื่อสารให้แก่ผู้ที่เกี่ยวข้องรับทราบ

๓. ห้ามเปิดเผยข้อมูลที่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง หลักเกณฑ์ นโยบาย หรือแนวปฏิบัติของ สศช. ที่ประกาศใช้ในปัจจุบันทุกกรณี

๔. กำหนดให้การดำเนินการประมวลผลข้อมูลที่เป็นความลับ เช่น ข้อมูลส่วนบุคคล เป็นไปตามขอบเขตเงื่อนไขหรือวัตถุประสงค์ในการยินยอมให้ดำเนินการกับข้อมูลส่วนบุคคลนั้น เป็นต้น

๕. ต้องมีการเก็บบันทึกประวัติการเข้าถึงและการใช้ข้อมูล (Log Files) เพื่อให้สามารถตรวจสอบย้อนกลับได้

๖. กำหนดให้บริกรข้อมูล เจ้าของข้อมูล และผู้มีส่วนได้ส่วนเสียกับข้อมูลที่เกี่ยวข้อง ร่วมกันจัดทำคำอธิบายชุดข้อมูล (Metadata) สำหรับข้อมูลที่จัดเก็บอยู่ในฐานข้อมูล (Database) ในทุกชุดข้อมูล

๗. กำหนดให้ทบทวนระดับชั้นความลับข้อมูล อย่างน้อยปีละ ๑ ครั้ง

๕. นโยบายความมั่นคงปลอดภัยและความเป็นส่วนบุคคลของข้อมูล (Data Security and Privacy Policy)

วัตถุประสงค์

เพื่อกำหนดแนวทางในการบริหารจัดการข้อมูลให้มีความสอดคล้องกับนโยบายความมั่นคงปลอดภัยและความเป็นส่วนบุคคลของข้อมูล

นโยบาย

๑. จัดทำสถาปัตยกรรมความมั่นคงปลอดภัยของข้อมูล (Data Security Architecture) เพื่อเป็นกรอบในควบคุม กำกับดูแล และรักษาความมั่นคงปลอดภัยของข้อมูล รวมทั้ง ให้มีการทบทวนสถาปัตยกรรมความมั่นคงปลอดภัยของข้อมูลอย่างสม่ำเสมอ

๒. กำหนดให้มีการควบคุมการเข้าถึงข้อมูล (Data Access Control) ตามสิทธิ์การเข้าถึงที่คณะกรรมการธรรมาภิบาลกำหนด

๓. ตรวจสอบความมั่นคงปลอดภัยของข้อมูล (Data Security Audit) โดยจัดให้มีการตรวจสอบการเข้าถึงข้อมูลตามสิทธิ์ การทดสอบการเจาะระบบสำคัญ รวมทั้ง การตรวจสอบประวัติ (Log) การถูกโจมตีจากผู้ไม่ประสงค์ดีอย่างสม่ำเสมอ

๔. กำหนดให้มีการประเมินความปลอดภัยของข้อมูล (Data Security Assessment) โดยทบทวนความเสี่ยงด้านความมั่นคงปลอดภัยของข้อมูล ประเมินความเสี่ยง วางแผนการป้องกันความเสี่ยง และติดตามการดำเนินงานตามแผนการป้องกันความเสี่ยง

๕. จัดหาเครื่องมือและเทคโนโลยีความมั่นคงปลอดภัยของข้อมูล (Data Security Tool /Technology) เพื่อป้องกันและรับมือกรณีที่อาจถูกโจมตีจากผู้ไม่ประสงค์ดีต่ออุปกรณ์เครือข่าย โครงสร้างพื้นฐานทางสารสนเทศ ระบบหรือโปรแกรมที่อาจจะเกิดความเสียหายหรือข้อมูลส่วนบุคคลรั่วไหลไปยังบุคคลที่สามโดยไม่ได้รับอนุญาต

๖. นโยบายการเปิดเผยข้อมูล (Open Data Policy)

วัตถุประสงค์

เพื่อกำหนดนโยบายข้อมูลที่สามารถนำไปใช้ได้โดยอิสระ สามารถนำกลับมาใช้ใหม่และแจกจ่ายได้โดยใครก็ตาม แต่ต้องระบุแหล่งที่มาหรือเจ้าของงานและต้องใช้สัญญาอนุญาต หรือเงื่อนไขเดียวกันกับที่มาหรือตามเจ้าของข้อมูลกำหนด

นโยบาย

๑. กำหนดบทบาทหน้าที่ที่เกี่ยวข้องกับการเปิดเผยข้อมูล ได้แก่ กำหนดบุคคลหรือกลุ่มบุคคลที่มีสิทธิ์ตัดสินใจในการเปิดเผยข้อมูล และกำหนดบุคคลหรือกลุ่มบุคคลในการดำเนินการและปรับปรุงการเปิดเผยข้อมูลและกำหนดบุคคลหรือกลุ่มบุคคลในการรับเรื่องและแก้ไขปัญหาเบื้องต้นในการเข้าถึงข้อมูลและการนำข้อมูลไปใช้

๒. ห้ามเปิดเผยข้อมูลที่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง นโยบาย และ/หรือแนวปฏิบัติของ สศช. ในทุกกรณี

๓. กำหนดให้การเปิดเผยข้อมูลจำเป็นต้องได้รับการอนุญาตจากเจ้าของข้อมูล (Data Owner)

๔. จัดเตรียมข้อมูลตามรูปแบบที่ได้จัดทำไว้เป็นมาตรฐานตามกำหนด และง่ายต่อการนำไปใช้งาน

๕. จัดทำคำอธิบายชุดข้อมูล (Metadata) ควบคู่ไปกับข้อมูลที่เปิดเผย

๖. ให้มีการคัดเลือกชุดข้อมูลที่ต้องการเผยแพร่ โดยหน่วยงานเจ้าของข้อมูลหรือผู้ที่ได้รับมอบหมาย

๗. สามารถตรวจสอบได้ว่าการเปิดเผยข้อมูลได้ถูกดำเนินการอย่างเหมาะสมหรือเป็นไปตามแนวทางที่ได้กำหนดไว้ เพื่อให้ได้ข้อมูลที่มีคุณภาพ และเป็นการรักษาคุณภาพของข้อมูล

๘. ต้องปฏิบัติตามอย่างเคร่งครัด และป้องกันมิให้มีการเปิดเผยข้อมูล โดยไม่ได้รับอนุญาต

.....