ประกาศการประปาส่วนภูมิภาค
เรื่อง นโยบายธรรมาภิบาลข้อมูลและแนวปฏิบัติของการประปาส่วนภูมิภาค
พ.ศ. ๒๕๖๗

ด้วยพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ กำหนดให้หน่วยงานของรัฐต้องจัดให้มีการบริหารงานภาครัฐ และการจัดทำการบริการสาธารณะเป็นไปด้วยความสะดวก รวดเร็ว มีประสิทธิภาพ ตอบสนองต่อการให้บริการ และอำนวยความสะดวกแก่ประชาชน รวมถึงกำหนดให้มีการบริหารจัดการ บูรณาการข้อมูลภาครัฐ เพื่อการทำงานมีความสอดคล้อง และเชื่อมโยงข้อมูลเข้าด้วยกันอย่างมั่นคง ปลอดภัย มีธรรมาภิบาล ประกอบกับประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล ลงวันที่ ๑๒ มีนาคม ๒๕๖๓ เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ ตลอดจนกฎหมาย กฎระเบียบ และข้อกำหนดอื่นที่เกี่ยวข้อง กปภ. จึงกำหนดนโยบายธรรมาภิบาลข้อมูลและแนวปฏิบัติจำนวน ๖ ด้าน ดังนี้

๑. นโยบายข้อมูล (Data Policy)
๒. นโยบายคุณภาพข้อมูล (Data Quality Policy)
๓. การเชื่อมโยงและแลกเปลี่ยนข้อมูล (Data Integration and Exchange Policy)
๔. การจัดชั้นความลับข้อมูล (Data Classification Standard)
๕. ความมั่นคงปลอดภัยและความเป็นส่วนบุคคลของข้อมูล (Data Security and Privacy Policy)
๖. การเปิดเผยข้อมูล (Open Data Policy)

ขอบเขต (SCOPE)

ขอบเขตของนโยบายนี้ครอบคลุมการดำเนินงานของ กปภ. ในการบริหารจัดการ และการบูรณาการข้อมูล ได้แก่ นโยบายที่เกี่ยวกับเงื่อนไข ในการสร้าง การจัดเก็บรักษา การควบคุมคุณภาพ การประมวลผล การใช้ การแลกเปลี่ยน การเชื่อมโยง การเปิดเผย การรักษาความลับ และการทำลายข้อมูล

คำนิยาม (DEFINITIONS)

"กปภ."	การประปาส่วนภูมิภาค
"คณะกรรมการกำกับดูแลระบบสารสนเทศ ของ กปภ." หรือ "ITSC"	คณะกรรมการกำกับดูแลระบบสารสนเทศของ กปภ. (Information Technology Steering Committee: ITSC) มีหน้าที่ในการกำหนดนโยบายบริหารจัดการ และการพัฒนาติดตาม และประเมินผลของการดำเนินงานทางด้าน Digital Technology รวมถึงทำหน้าที่เป็นคณะกรรมการธรรมาภิบาลข้อมูล หรือ Data Governance Council
"คณะทำงานบริกรข้อมูล" หรือ "Data Steward Team"	คณะทำงาน ซึ่งประกอบด้วย หัวหน้าคณะทำงานบริกรข้อมูล และคณะทำงานบริกรข้อมูลด้าน Controller, Processor, Technician และ Auditor มีหน้าที่และความรับผิดชอบในการนำเสนอนโยบายข้อมูลแนวทางปฏิบัติงาน เกณฑ์การวัดคุณภาพ ระเบียบและข้อบังคับที่เกี่ยวข้องกับข้อมูล การจัดลำดับ

	ความสำคัญและแนวทางการแก้ไขปัญหาของข้อมูล รวมทั้งข้อมูลสนับสนุนการตัดสินใจต่อคณะกรรมการธรรมาภิบาลข้อมูล ตรวจสอบการปฏิบัติตามนโยบายข้อมูล ประเมินความพร้อมของการกำกับดูแลข้อมูล รายงานผลการตรวจสอบ ความมั่นคงปลอดภัยและคุณภาพข้อมูล
“ข้อมูล”	สิ่งที่สื่อความหมายให้รู้เรื่องราว ข้อเท็จจริง ข้อมูลหรือสิ่งใดๆ ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเอง หรือโดยผ่านวิธีการใดๆ และไม่ว่าจะได้จัดทำไว้ในรูปแบบของเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ฟิล์ม การบันทึกภาพ หรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้
“ข้อมูลส่วนบุคคล”	ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรง หรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ (ชื่อ - สกุล ที่อยู่ เลขบัตรประชาชน ข้อมูลสุขภาพ หมายเลขโทรศัพท์ e-mail และประวัติอาชญากรรม เป็นต้น)
“ข้อมูลที่เป็นเอกสาร”	ข้อมูลที่มีการจัดเก็บและบันทึกในรูปแบบของกระดาษ
“ข้อมูลที่ไม่เป็นเอกสาร”	ข้อมูลสารสนเทศ ข้อมูลคอมพิวเตอร์ ข้อมูลอิเล็กทรอนิกส์
“เจ้าของข้อมูล”	บุคคล/หน่วยงานที่รับผิดชอบเกี่ยวกับข้อมูล ที่สามารถบริหารจัดการและควบคุมชุดข้อมูล สร้าง แก้ไข ลบ กำหนดสิทธิ์ การเข้าถึง อนุญาต หรือปฏิเสธการเข้าถึงข้อมูล และเป็นผู้รับผิดชอบต่อความถูกต้อง ทันสมัย ความสมบูรณ์ และการทำลาย รวมถึงกำหนดระดับชั้นความลับ สิทธิ์การใช้งาน และความปลอดภัยของข้อมูล
“เจ้าของข้อมูลส่วนบุคคล”	บุคคลที่ข้อมูลนั้นสามารถระบุตัวตนไปถึงได้
“ผู้ควบคุมข้อมูลส่วนบุคคล”	บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวมใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
“ผู้ประมวลผลข้อมูลส่วนบุคคล”	บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุม ข้อมูลส่วนบุคคล
“ผู้ดูแลข้อมูล”	ผู้ที่ทำงานร่วมกับเจ้าของข้อมูลโดยตรง ทำหน้าที่จัดเก็บรักษาข้อมูล รวมถึงป้องกันภัยคุกคาม ทำการสำรองข้อมูล ดำเนินการตามขั้นตอนที่ระบุไว้ในนโยบายและแผนงานความมั่นคงปลอดภัย ทั้งทางด้านระบบสารสนเทศ และที่มิใช่สารสนเทศ

“ผู้ดูแลระบบสารสนเทศ”	พนักงานที่ได้รับมอบหมายจากผู้ว่าการ ให้มีหน้าที่รับผิดชอบในการดูแลรักษา และปรับปรุงระบบสารสนเทศให้สามารถทำงานได้อย่างต่อเนื่อง รวมทั้งจะต้องสอดส่องดูแลการใช้ระบบสารสนเทศของพนักงาน เพื่อให้เป็นไปตามขั้นตอน และแนวทางปฏิบัติการใช้งานเครือข่ายคอมพิวเตอร์และระบบสารสนเทศอย่างปลอดภัยของ กปภ.
“ผู้ใช้ข้อมูล”	ผู้ที่ได้รับสิทธิการใช้ข้อมูลจากผู้รับผิดชอบหรือได้รับมอบหมายให้ใช้ข้อมูลจากผู้บังคับบัญชา รวมถึงผู้ซึ่งได้รับความยินยอมให้ทำงานหรือทำผลประโยชน์ให้แก่ กปภ.
“ระดับชั้นความลับ”	การกำหนดการเปิดเผยข้อมูลต่อผู้อื่นให้เหมาะสมกับสถานะการใช้งาน ได้แก่ ลับที่สุด ลับมาก ลับ ปกปิด และเปิดเผยสู่ภายนอกได้
“ความมั่นคงปลอดภัยของข้อมูล”	การธำรงไว้ซึ่งความลับ ความถูกต้องครบถ้วน และการรักษาสภาพพร้อมใช้ของข้อมูล รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง ความรับผิด การห้ามปฏิเสธความรับผิด และความน่าเชื่อถือ
"Log Files"	ไฟล์ข้อมูลจราจรทางคอมพิวเตอร์ เป็นข้อมูลที่เกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ แสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการหรืออื่นๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์
“Metadata”	คำอธิบายชุดข้อมูลดิจิทัล เพื่อให้ทราบรายละเอียดเกี่ยวกับโครงสร้างของข้อมูล เนื้อหาสาระ รูปแบบการจัดเก็บ แหล่งข้อมูล และสิทธิ์ในการเข้าถึงข้อมูล
"Log in" / "Log on"	การใส่ Username และ Password เพื่อเข้าใช้งานคอมพิวเตอร์หรือเข้าสู่ระบบ
"Log off" / "Log out"	การยกเลิกหรือการออกจากการเชื่อมต่อจากคอมพิวเตอร์ หรือระบบโดยสมัครใจ
"Master Data"	ข้อมูลหลักที่เป็นข้อมูลที่ใช้ในการดำเนินงานภายในหน่วยงาน มีโอกาสเปลี่ยนแปลงได้ มีรายละเอียดหรือจำนวนฟิลด์ข้อมูลจำนวนมาก เช่น ข้อมูลพนักงาน ข้อมูลลูกค้า ข้อมูลผู้ขาย ข้อมูลสินค้า ข้อมูลครุภัณฑ์ ข้อมูลสถานที่ เป็นต้น
"Reference Data"	ข้อมูลอ้างอิงที่เป็นข้อมูลสากล มีการเปลี่ยนแปลงค่อนข้างน้อย เช่น รหัสไปรษณีย์ รหัสประเทศ หน่วยวัดระยะทาง เป็นต้น
“คลังข้อมูล”	เป็นข้อมูลที่ได้จากการเชื่อมโยงข้อมูล จากการรวบรวมข้อมูลจากแหล่งข้อมูลต่างๆ ที่มีหลากหลายรูปแบบมาเก็บในคลังข้อมูลโดยผ่านกระบวนการของ (ETL) ในรูปแบบข้อมูลที่มีโครงสร้างและถูกจัดทำให้อยู่ในรูปแบบเหมาะสมสำหรับการนำไปวิเคราะห์ข้อมูล

๑. นโยบายข้อมูล (Data Policy)

วัตถุประสงค์

เพื่อกำหนดแนวทางการดำเนินงานด้านธรรมาภิบาลข้อมูล และการบริหารจัดการข้อมูลอย่างมีประสิทธิภาพ จึงต้องมีการกำหนดนโยบายที่ชัดเจน สอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง หรือข้อกำหนดอื่นๆ ที่เกี่ยวข้อง โดยมีคณะกรรมการกำกับดูแลระบบสารสนเทศของ กปภ. (ITSC) เป็นผู้มอบนโยบายและกำกับดูแล เพื่อให้ข้อมูลถูกใช้งานอย่างมีประสิทธิภาพ และสอดคล้องกันระหว่างนโยบายข้อมูลกับการดำเนินการใดๆ ของผู้มีส่วนได้ส่วนเสีย

นโยบาย

๑. กำหนดให้มีโครงสร้างคณะกรรมการธรรมาภิบาลข้อมูล และกำหนดบทบาทหน้าที่ความรับผิดชอบในการบริหารจัดการข้อมูล

๒. กำหนดหน่วยงานที่เป็นเจ้าของข้อมูลในการบริหารจัดการข้อมูลในแต่ละชุดข้อมูล

๓. กำหนดขอบเขตข้อมูลที่อยู่ในความดูแลของผู้ครอบครองหรือควบคุมข้อมูล รวมถึงผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคล

๔. กำหนดกระบวนการธรรมาภิบาลข้อมูลอย่างเป็นรูปธรรม

๕. จัดทำนโยบายข้อมูลที่ประกอบไปด้วย 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. กำหนดให้มีการสื่อสาร และเผยแพร่นโยบายข้อมูลให้กับผู้ที่เกี่ยวข้องทั้งภายในหน่วยงานและภายนอก

๗. ให้มีการฝึกอบรมเพื่อสร้างความตระหนักถึงธรรมาภิบาลข้อมูล และการบริหารจัดการข้อมูล โดยให้ครอบคลุมการบริหารจัดการทุกกระบวนการและวงจรชีวิตของข้อมูล

๘. ต้องมีการทบทวน ตรวจสอบ และปรับปรุงนโยบายอย่างต่อเนื่อง อย่างน้อยปีละ ๑ ครั้ง

แนวปฏิบัติ

๑. หน่วยงานที่ได้รับมอบหมายร่วมมือกับหน่วยงานที่เกี่ยวข้อง แต่งตั้งคณะทำงานขึ้นมาดำเนินการและจัดทำรายละเอียดต่างๆ ที่เกี่ยวข้องตามนโยบายที่กำหนด

๒. ให้มีการตรวจสอบรายละเอียดต่างๆ จากผู้เชี่ยวชาญ อาจเป็นบุคคลหรือหน่วยงานภายใน/ภายนอกที่มีความรู้ความสามารถในด้านที่เกี่ยวข้องเป็นอย่างดี

๓. ปรับปรุง แก้ไข และตรวจทานรายละเอียดดังกล่าว เป็นไปตามข้อคิดเห็น/ข้อสังเกตของผู้เชี่ยวชาญ

๔. นำเสนอคณะกรรมการกำกับดูแลระบบสารสนเทศของ กปภ. (ITSC) ขออนุมัติใช้นโยบายและแนวปฏิบัติ พร้อมทั้งประกาศให้บุคคล หน่วยงานภายใน/ภายนอกรับทราบ และดำเนินการ

๕. ให้มีการอบรม/สื่อสารผ่านช่องทางที่กำหนดแก่ทุกหน่วยงาน เพื่อดำเนินการตามนโยบายและแนวปฏิบัติที่ประกาศ

๖. คณะทำงานบริกรข้อมูล (Data Steward Team) ร่วมกับหน่วยงานที่เกี่ยวข้องจัดประชุมติดตามผลการดำเนินการตามนโยบายและแนวปฏิบัติ เพื่อเป็นการตรวจสอบ ทบทวน และปรับปรุงนโยบายและแนวปฏิบัติ อย่างน้อยปีละ ๑ ครั้ง และดำเนินการจัดทำกระบวนการและแบบฟอร์มต่างๆ ที่จำเป็นต้องใช้ เพื่อให้การดำเนินงานมีประสิทธิภาพ

๗. หากมีการเปลี่ยนแปลงรายละเอียดอย่างมีนัยสำคัญ ให้มีการประชุมเพื่อมีมติทบทวน แก้ไข ปรับปรุงและนำเสนอขออนุมัติจากคณะกรรมการกำกับดูแลระบบสารสนเทศ ของ กปภ. (ITSC)

๒. นโยบายคุณภาพข้อมูล (Data Quality Policy)

วัตถุประสงค์

เพื่อให้การควบคุมคุณภาพข้อมูลในการนำไปใช้ประโยชน์สำหรับการบริหารงาน และการให้บริการของ กปภ. โดยให้เป็นไปตามอำนาจหน้าที่และวัตถุประสงค์ในการดำเนินงานของ กปภ. ตามที่กฎหมายกำหนด โดยข้อมูลที่ได้ทำการจัดเก็บ กปภ. จะคำนึงถึงคุณภาพข้อมูล (Data Quality) ในทุกชุดข้อมูล (Dataset) ของ กปภ.

นโยบาย

๑. มีการกำหนดมาตรฐานข้อมูลให้เป็นแบบเดียวกัน

๒. ชุดข้อมูลทุกชุดต้องมีเกณฑ์การวัดคุณภาพข้อมูล (Data Quality) อย่างน้อย ๑ เกณฑ์ต่อไปนี้ ความถูกต้อง (Accuracy) ความครบถ้วน (Completeness) ความต้องกัน (Consistency) ความเป็นปัจจุบัน (Timeliness) ตรงตามความต้องการของผู้ใช้ (Relevancy) และพร้อมใช้งาน (Availability) โดยทุกเกณฑ์เป็นเกณฑ์เชิงปริมาณ (Quantitative Measurement)

๓. มีการกำหนดตัวชี้วัดคุณภาพข้อมูล เช่น ความถูกต้อง ความครบถ้วน ความต้องกัน ความเป็นปัจจุบัน ตรงตามความต้องการของผู้ใช้ และพร้อมใช้งาน เป็นต้น

๔. เกณฑ์คุณภาพข้อมูลต้องดำเนินการ โดยเจ้าของข้อมูล ผู้ใช้ข้อมูล คณะทำงานบริกรข้อมูล (Data Steward Team) และอนุมัติโดยคณะกรรมการกำกับดูแลระบบสารสนเทศของ กปภ. (ITSC)

๕. มีการรายงานคุณภาพข้อมูล โดยจะต้องแนบรายงานกับการใช้ชุดข้อมูล (Dataset) และชุดคำอธิบายข้อมูล (Metadata)

๖. จัดให้มีกระบวนการตรวจสอบคุณภาพข้อมูล

๗. จัดให้มีการฝึกอบรมเพื่อสร้างความตระหนักถึงการจัดเก็บข้อมูล และคุณภาพของข้อมูล

แนวปฏิบัติ

๑. เจ้าของข้อมูล (Data Owner) ผู้ใช้ข้อมูล (Data User) และคณะทำงานบริกรข้อมูล (Data Steward Team) ร่วมกันออกแบบ และกำหนดมาตรฐานข้อมูลให้เป็นแบบเดียวกัน พร้อมทั้งกำหนดวิธีปฏิบัติการสร้าง การจัดเก็บรักษา การควบคุมคุณภาพข้อมูลและความมั่นคงปลอดภัยของข้อมูล ให้สอดคล้องกับวัตถุประสงค์การดำเนินงาน และนำเสนอขออนุมัติผู้บริหารที่มีอำนาจตัดสินใจ

๒. ชุดข้อมูลทุกชุดต้องมีเกณฑ์การวัดคุณภาพข้อมูลอย่างน้อย ๑ เกณฑ์ต่อไปนี้ ความถูกต้อง (Accuracy) ความครบถ้วน (Completeness) ความต้องกัน (Consistency) ความเป็นปัจจุบัน (Timeliness) ตรงตามความต้องการของผู้ใช้ (Relevancy) และพร้อมใช้งาน (Availability) โดยทุกเกณฑ์เป็นเกณฑ์เชิงปริมาณ (Quantitative measurement)

๑) ความถูกต้องของข้อมูลต้องมีการตรวจสอบและแก้ไข โดยคณะทำงานบริกรข้อมูล ถ้ามีความจำเป็นต้องมีการตรวจสอบข้ามฝ่าย สามารถประสานงานผ่านสายงานถึงคณะทำงานบริกรข้อมูลได้และต้องมีการยืนยันความถูกต้องก่อนนำไปใช้

๒) ความครบถ้วนของข้อมูลสามารถตรวจสอบได้ด้วยวิธีการ Data Profiling

๓) ความต้องกันของข้อมูลสามารถตรวจสอบได้กับมาตรฐานข้อมูลที่ตั้งไว้ในแต่ละชุดข้อมูล

๔) ความเป็นปัจจุบันต้องมีการเปรียบเทียบกับฟิลด์อ้างอิงที่เป็นเกณฑ์เวลาตามมาตรฐาน

๕) มีความตรงตามความต้องการของผู้ใช้ (Relevancy)

๖) มีความพร้อมใช้งาน (Availability)

๓. การกำหนดตัวชี้วัด และเกณฑ์คุณภาพข้อมูลต้องดำเนินการโดยเจ้าของข้อมูล (Data Owner) ผู้ใช้ข้อมูล (Data User) และคณะทำงานบริกรข้อมูล (Data Steward Team) และอนุมัติโดยคณะกรรมการกำกับดูแลระบบสารสนเทศ ของ กปภ. (ITSC)

๔. จัดทำรายงานคุณภาพข้อมูลจะต้องแนบไปกับการใช้ข้อมูลและคำอธิบายชุดข้อมูล (Metadata)

๕. เจ้าของข้อมูลร่วมจัดทำเกณฑ์คุณภาพข้อมูล โดยเกณฑ์คุณภาพข้อมูลของชุดข้อมูลจะนำคะแนนของทุกเกณฑ์มาหาผลรวมและคิดเป็นร้อยละ และมีการทบทวนอย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง

๖. มีกระบวนการตรวจสอบคุณภาพข้อมูลที่มีประสิทธิภาพ

๗. มีการอบรม สื่อสาร ให้ความรู้ความเข้าใจถึงวิธีการปฏิบัติเรื่องคุณภาพข้อมูล และมีทักษะในการใช้เครื่องมือที่ใช้วัดคุณภาพข้อมูลอย่างถูกต้องตามขั้นตอนที่กำหนด

๓. การเชื่อมโยงและแลกเปลี่ยนข้อมูล (Data Integration and Exchange Policy)

วัตถุประสงค์

เพื่อให้การแลกเปลี่ยนข้อมูลทั้งภายใน และระหว่างหน่วยงานมีความมั่นคงปลอดภัย และข้อมูลมีคุณภาพ สามารถนำไปใช้ประโยชน์ได้อย่างมีประสิทธิภาพ โดยมีวิธี และแนวทางการนำข้อมูลไปเชื่อมโยง และแลกเปลี่ยนกับหน่วยงานภายนอกให้สอดคล้องกับระเบียบ หลักเกณฑ์ และกฎหมายที่กำหนดบนพื้นฐานของประโยชน์ส่วนรวมเป็นสำคัญ

นโยบาย

๑. กำหนดกระบวนการในการแลกเปลี่ยน และเชื่อมโยงข้อมูลให้ชัดเจน เริ่มตั้งแต่การเตรียมการ การเริ่มดำเนินการ ระหว่างดำเนินการ และสิ้นสุดการดำเนินการ

๒. กำหนดคำอธิบายชุดข้อมูล (Metadata) ของชุดข้อมูลที่ต้องการแลกเปลี่ยน และเชื่อมโยงข้อมูลที่จำเป็นให้ครบถ้วน และมีการเผยแพร่รายละเอียดคำอธิบายชุดข้อมูล (Metadata) ของชุดข้อมูลที่เผยแพร่

๓. กำหนดเทคโนโลยี และมาตรฐานทางเทคนิคที่ใช้ในการแลกเปลี่ยน และเชื่อมโยงข้อมูล

๔. กำหนดกระบวนการตรวจสอบการแลกเปลี่ยน เชื่อมโยงข้อมูลให้ดำเนินการอย่างถูกต้องเหมาะสม ข้อมูลมีความสอดคล้อง หรือเป็นไปตามแนวปฏิบัติ และตามมาตรฐานที่กำหนด

๕. มีการตรวจสอบการสอดคล้องกันของข้อมูล (Data Integrity Checking) ระหว่างหน่วยงานที่มีการแลกเปลี่ยนและเชื่อมโยงข้อมูล

๖. บันทึกรายละเอียด และจัดเก็บข้อมูลการดำเนินงานที่เกิดขึ้นในแต่ละครั้งที่มีการแลกเปลี่ยนและเชื่อมโยงข้อมูล มีการเก็บบันทึก (Log Files) ระหว่างหน่วยงาน เพื่อให้สามารถตรวจสอบย้อนกลับได้

๗. ทำสัญญาอนุญาต บันทึกข้อตกลง (Memorandum of Understanding: MOU) สัญญารักษาความลับ (Non-disclosure agreement: NDA) หรือข้อตกลงอื่นใด ว่าด้วยการเชื่อมโยงข้อมูลของ กปภ. หรือข้อตกลงในการแลกเปลี่ยนข้อมูล และการนำข้อมูลไปใช้

๘. มีมาตรการในการรักษาความมั่นคงปลอดภัยในการแลกเปลี่ยนและเชื่อมโยงข้อมูลอย่างเหมาะสม

แนวปฏิบัติ

๑. ทุกชุดข้อมูลที่มีการเชื่อมโยงกันระหว่างภายใน หรือภายนอกองค์กร นอกจากชุดข้อมูลที่มีการจัดส่งแล้ว จะต้องมีการจัดทำเอกสารมาตรฐานการเชื่อมโยงข้อมูล ประกอบด้วย ชื่อชุดข้อมูล คำอธิบายชุดข้อมูล (Metadata) ชั้นความลับของข้อมูล วันและเวลาในการส่งออกข้อมูล ซึ่งผ่านความเห็นชอบจากคณะทำงานบริกรข้อมูล (Data Steward Team) วันและเวลาที่ฝั่งผู้รับได้รับข้อมูล

๒. สำหรับหน่วยงานภายนอก ให้มีการทำสัญญาอนุญาตบันทึกข้อตกลง (Memorandum of Understanding) สัญญารักษาความลับ (Non-Disclosure Agreement) หรือข้อตกลงอื่นที่เกี่ยวข้องกับการแลกเปลี่ยนและเชื่อมโยง

๓. สำหรับการเชื่อมโยงภายใน ให้หน่วยงานภายในทำหนังสือขออนุมัติตามสายงาน เพื่อขอเชื่อมโยงข้อมูลบนฐานข้อมูล

๔. มีการตรวจสอบข้อมูล จะต้องอ้างอิงตามคำอธิบายชุดข้อมูล (Metadata) และข้อมูลอ้างอิงของชุดข้อมูลนั้น

๕. มีการกำหนดเทคโนโลยี และมาตรฐานทางเทคนิคที่ใช้ในการแลกเปลี่ยน และเชื่อมโยงข้อมูล

๖. มีการทำประวัติการส่ง การรับ และการเชื่อมโยงข้อมูลต้องทำผ่านระบบ และมีการเก็บบันทึก (Logging System) ด้วย

๗. มีการอบรม สื่อสาร ให้ความรู้ความเข้าใจถึงวิธีการปฏิบัติการแลกเปลี่ยน และเชื่อมโยงข้อมูลให้ผู้เกี่ยวข้องทราบ

๔. การจัดชั้นความลับข้อมูล (Data Classification Standard)

วัตถุประสงค์

เพื่อให้การประมวลผลข้อมูล และการใช้ข้อมูลที่มีประสิทธิภาพ ถูกต้อง ตรงตามวัตถุประสงค์ของการใช้ข้อมูลให้เกิดประโยชน์ รวมถึงวิธีการและแนวทางในการขอข้อมูลจากหน่วยงานที่เกี่ยวข้องทั้งภายในและภายนอก เพื่อนำมาใช้ในการประมวลผล และนำมาใช้ ทั้งนี้การนำข้อมูลมาใช้ให้เป็นไปตามวัตถุประสงค์ตามที่แจ้ง หากนอกเหนือจากเหตุผลดังกล่าวข้างต้น จะต้องได้รับความยินยอมจากเจ้าของข้อมูล

นโยบาย

๑. ชุดข้อมูลต้องมีการจัดลำดับชั้นความลับของข้อมูล การกำหนดชั้นความลับของข้อมูล และการกำหนดสิทธิ์การเข้าถึง เพื่อให้สอดคล้องกับแนวทางการจัดชั้นความลับของข้อมูล

๒. กำหนดแนวปฏิบัติ และมาตรฐานของการประมวลผลข้อมูล และทำการสื่อสารให้แก่ผู้ที่เกี่ยวข้อง

๓. ห้ามเปิดเผยข้อมูลที่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง หลักเกณฑ์ นโยบาย และแนวปฏิบัติของ กปภ. ที่ประกาศใช้ในปัจจุบัน ไม่ว่าข้อมูลจะอยู่ในรูปแบบใดหรือสถานที่ใดก็ตาม

๔. การดำเนินการประมวลผลข้อมูลที่เป็นความลับ เช่น ข้อมูลส่วนบุคคล ให้เป็นไปตามขอบเขต เงื่อนไขหรือวัตถุประสงค์ในการยินยอมให้ดำเนินการกับข้อมูลส่วนบุคคลนั้น

๕. ต้องมีการเก็บบันทึกประวัติการเข้าถึง และการใช้ข้อมูล (Log Files) เพื่อให้สามารถตรวจสอบย้อนกลับได้

๖. คณะทำงานบริกรข้อมูล (Data Steward Team) เจ้าของข้อมูล และผู้มีส่วนได้ส่วนเสียกับข้อมูลที่เกี่ยวข้องต้องร่วมกัน จัดทำคำอธิบายชุดข้อมูล (Metadata) พร้อมคำอธิบายสำหรับข้อมูลที่จัดเก็บอยู่ในฐานข้อมูล (Database) ในทุกชุดข้อมูล

๗. ต้องมีการทบทวนระดับชั้นความลับข้อมูล อย่างน้อยปีละ ๑ ครั้ง และให้ดำเนินการปรับปรุงอย่างต่อเนื่อง

แนวปฏิบัติ

๑. ชุดข้อมูลต้องมีการจัดลำดับชั้นความลับของข้อมูลดังต่อไปนี้

ระดับที่ ๑) ข้อมูลสาธารณะ ได้แก่ ข้อมูลที่สามารถเปิดเผยได้ สามารถนำไปใช้ได้อย่างอิสระ

ระดับที่ ๒) ข้อมูลส่วนบุคคล ได้แก่ ข้อมูลเกี่ยวกับสิ่งเฉพาะตัวของบุคคลที่ทำให้สามารถระบุตัวหรือรู้ตัวของบุคคลนั้นๆ ได้ทั้งทางตรงหรือทางอ้อม

ระดับที่ ๓) ข้อมูลความลับทางราชการ ได้แก่ ข้อมูลที่อยู่ในความครอบครอง หรือควบคุมดูแลของหน่วยงานของรัฐที่มีคำสั่งไม่ให้มีการเปิดเผย

ระดับที่ ๔) ข้อมูลความมั่นคง ได้แก่ ข้อมูลเกี่ยวกับความมั่นคงของรัฐ ที่ทำให้เกิดความสงบเรียบร้อย การมีเสถียรภาพความเป็นปึกแผ่น ปลอดภัยจากภัยคุกคาม เป็นต้น

๒. การจัดลำดับชั้นความลับข้อมูลต้องดำเนินการโดยคณะทำงานบริกรข้อมูล (Data Steward Team) และอนุมัติโดยคณะกรรมการกำกับดูแลระบบสารสนเทศของ กปภ. (ITSC)

๓. มีการทบทวนระดับชั้นความลับข้อมูล อย่างน้อยปีละ ๑ ครั้ง

๔. ในแต่ละชุดข้อมูลถือว่ามีระดับชั้นความลับเท่ากัน สำหรับชุดข้อมูลที่มีระดับความลับเป็นข้อมูลส่วนบุคคล (ระดับที่ ๒) ข้อมูลความลับทางราชการ (ระดับที่ ๓) หรือข้อมูลความมั่นคง (ระดับที่ ๔) จำเป็นต้องระบุสิทธิ์ในการเข้าถึงข้อมูลภายในองค์กรด้วย

๕. การเผยแพร่ข้อมูลสาธารณะ (ระดับที่ ๑) ต้องได้รับการอนุมัติโดยคณะกรรมการกำกับดูแลระบบสารสนเทศของ กปภ. (ITSC)

๖. ข้อมูลระดับที่ ๒ เป็นต้นไปจะต้องมีกระบวนการในการร้องขอข้อมูล

๗. เจ้าของข้อมูล (Data Owner) มีหน้าที่ร่วมพิจารณา รับทราบ อนุมัติ และตรวจสอบการร้องขอข้อมูลส่วนบุคคล และการจัดลำดับชั้นความลับข้อมูลร่วมกับคณะทำงานบริกรข้อมูล (Data Steward Team)

๘. ระดับชั้นความลับข้อมูลจะต้องถูกระบุไว้ในคำอธิบายชุดข้อมูล (Metadata)

๙. การร้องขอข้อมูลต้องทำผ่านระบบและมีการเก็บบันทึก (Logging System)

๑๐. มีการอบรม สื่อสาร ให้ความรู้ความเข้าใจถึงวิธีการปฏิบัติการจัดชั้นความลับข้อมูลให้ผู้เกี่ยวข้องทราบ

๕. ความมั่นคงปลอดภัยและความเป็นส่วนบุคคลของข้อมูล (Data Security and Privacy Policy)

วัตถุประสงค์

เพื่อเป็นการกำหนดแนวทางในการบริหารจัดการความมั่นคงปลอดภัยของข้อมูล และความเป็นส่วนบุคคล 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)

แนวปฏิบัติ

๑. ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) ต้องแจ้งมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ให้แก่บุคลากร พนักงาน ลูกจ้างหรือบุคคลที่เกี่ยวข้องทราบ รวมถึงสร้างเสริมความตระหนักรู้ด้านความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลให้กับกลุ่มบุคคลดังกล่าว ปฏิบัติตามนโยบายที่กำหนดอย่างเคร่งครัด

๒. ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) ต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ซึ่งควรครอบคลุมถึงมาตรการป้องกันด้านการบริหารจัดการ (Administrative Safeguard) มาตรการป้องกันด้านเทคนิค (Technical Safeguard) และมาตรการป้องกันทางกายภาพ (Physical Safeguard) การเข้าถึงหรือควบคุมการใช้งานข้อมูลส่วนบุคคล (Access Control) โดยอย่างน้อย ต้องประกอบด้วยการดำเนินการดังต่อไปนี้

๑) การควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์ในการจัดเก็บ และประมวลผลข้อมูลส่วนบุคคลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

๒) การกำหนดเกี่ยวกับการอนุญาตหรือการกำหนดสิทธิ์ในการเข้าถึงข้อมูลส่วนบุคคล

๓) การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) เพื่อควบคุมการเข้าถึงข้อมูลส่วนบุคคลเฉพาะผู้ที่ได้รับอนุญาตแล้ว

๔) การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities) เพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลส่วนบุคคล การลักขโมยอุปกรณ์จัดเก็บหรือประมวลผลข้อมูลส่วนบุคคล

๕) การจัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง ลบ หรือถ่ายโอนข้อมูลส่วนบุคคล ให้สอดคล้องเหมาะสมกับวิธีการ และสื่อที่ใช้ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

๓. ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) อาจเลือกใช้มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่แตกต่างไปจากนี้ได้ หากมาตรฐานดังกล่าวมีมาตรการรักษาความมั่นคงปลอดภัยไม่ต่ำกว่านี้

๖. การเปิดเผยข้อมูล (Open Data Policy)

วัตถุประสงค์

เพื่อกำหนดนโยบายข้อมูลที่สามารถนำไปใช้ได้โดยอิสระ สามารถนำกลับมาใช้ใหม่ และเปิดเผยข้อมูลได้แต่ต้องระบุแหล่งที่มาหรือเจ้าของงาน และต้องใช้สัญญาอนุญาต หรือเงื่อนไขเดียวกันกับที่มาหรือตามเจ้าของข้อมูลกำหนด

นโยบาย

๑. กำหนดบทบาทหน้าที่ที่เกี่ยวข้องกับการเปิดเผยข้อมูล ได้แก่ กำหนดบุคคลหรือกลุ่มบุคคลที่มีสิทธิ์ตัดสินใจในการเปิดเผยข้อมูล กำหนดบุคคลหรือกลุ่มบุคคลในการดำเนินการ และปรับปรุงการเปิดเผยข้อมูล และกำหนดบุคคลหรือกลุ่มบุคคลในการรับเรื่อง และแก้ไขปัญหาเบื้องต้นในการเข้าถึงข้อมูล และการนำข้อมูลไปใช้

๒. ห้ามเปิดเผยข้อมูลที่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง นโยบาย แนวปฏิบัติของ กปภ. ไม่ว่าข้อมูลจะอยู่ในรูปแบบใดหรือสถานที่ใดก็ตาม

๓. ต้องได้รับการอนุญาตจากเจ้าของข้อมูล (Data Owner) ก่อนการเปิดเผยข้อมูล

๔. ให้มีการจัดเตรียมข้อมูลที่อยู่ในรูปแบบที่ได้จัดทำไว้เป็นมาตรฐานตามกำหนด และง่ายต่อการนำข้อมูลไปใช้

๕. มีการจัดทำคำอธิบายชุดข้อมูล (Metadata) ควบคู่ไปกับข้อมูลที่เปิดเผย

๖. ให้มีการคัดเลือกชุดข้อมูลที่ต้องการเผยแพร่ โดยหน่วยงานเจ้าของข้อมูลหรือผู้ที่ได้รับมอบหมาย

๗. สามารถตรวจสอบได้ว่าการเปิดเผยข้อมูลได้ถูกดำเนินการอย่างเหมาะสมหรือเป็นไปตามแนวทางที่ได้กำหนดไว้ เพื่อให้ได้ข้อมูลที่มีคุณภาพ และเป็นการรักษาคุณภาพของข้อมูล

๘. ต้องปฏิบัติตามอย่างเคร่งครัด และป้องกันมิให้มีการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

แนวปฏิบัติ

๑. กำหนดบทบาทหน้าที่ที่เกี่ยวข้องกับการเปิดเผยข้อมูล ได้แก่ กำหนดบุคคลหรือกลุ่มบุคคลที่มีสิทธิ์ตัดสินใจในการเปิดเผยข้อมูล กำหนดบุคคลหรือกลุ่มบุคคลในการดำเนินการ และปรับปรุงการเปิดเผยข้อมูล และกำหนดบุคคลหรือกลุ่มบุคคลในการรับเรื่อง และแก้ไขปัญหาเบื้องต้นในการเข้าถึงข้อมูล และการนำข้อมูลไปใช้ ดังนี้

๑) คณะกรรมการกำกับดูแลระบบสารสนเทศของ กปภ. (ITSC) เป็นผู้ที่มีสิทธิ์ตัดสินใจในการเปิดเผยข้อมูล

๒) เจ้าของข้อมูล (Data Owner) ร่วมกับคณะทำงานบริกรข้อมูล (Data Steward Team) เป็นผู้ดำเนินการ และปรับปรุงการเปิดเผยข้อมูล

๓) มีศูนย์รับการติดต่อ (Contact Center) เป็นผู้รับเรื่องและแก้ไขปัญหาเบื้องต้นในการเข้าถึงข้อมูลและการนำข้อมูลไปใช้

๒. คณะทำงานบริกรข้อมูล (Data Steward Team) ร่วมกับเจ้าของข้อมูล (Data Owner) คัดเลือกชุดข้อมูลที่ต้องการเผยแพร่ โดยควรพิจารณาชุดข้อมูลที่มีคุณภาพ และเป็นที่ต้องการของทุกภาคส่วน เพื่อส่งเสริมให้เกิดการนำไปใช้อย่างแพร่หลาย และเกิดประโยชน์สูงสุด โดยชุดข้อมูลที่คัดเลือกสำหรับเผยแพร่นั้นต้องอยู่ในชั้นความลับที่สามารถเผยแพร่ได้ และต้องไม่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ ความมั่นคงของประเทศ ความลับทางราชการ และความเป็นส่วนตัว

๓. เจ้าของข้อมูล (Data Owner) ร่วมกับผู้ดูแลระบบเทคโนโลยีสารสนเทศ จัดเตรียมข้อมูลให้อยู่ในรูปแบบที่ง่ายต่อการนำไปใช้ในรูปแบบที่คอมพิวเตอร์สามารถอ่านได้ (Machine-Readable) เช่น รูปแบบของ Comma - Separated Values - CSV Application Programming Interface – API เป็นต้น

๔. จัดทำคำอธิบายชุดข้อมูล (Metadata) เพื่อให้ผู้ใช้ข้อมูลสามารถเข้าใจเกี่ยวกับบริบทของข้อมูล

๕. เจ้าของข้อมูลร่วมกับผู้ดูแลระบบบัญชีข้อมูลภาครัฐ เป็นผู้รับผิดชอบนำชุดข้อมูลขึ้นเผยแพร่สู่สาธารณะ ผ่านระบบบัญชีข้อมูลของ กปภ. เชื่อมต่อกับศูนย์กลางข้อมูลเปิดภาครัฐ โดยปฏิบัติตามเอกสารคู่มือการเปิดเผยและแลกเปลี่ยนข้อมูล

๖. เจ้าของข้อมูล (Data Owner) ร่วมกับผู้ดูแลระบบเทคโนโลยีสารสนเทศเป็นผู้ที่มีส่วนร่วมในกระบวนการปรับปรุงคุณภาพของข้อมูลที่หน่วยงานได้เผยแพร่ให้ข้อมูลมีคุณภาพ และตรงกับความต้องการของผู้ใช้ข้อมูล

๗. เอกสารที่เกี่ยวข้อง

๑. พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒

๒. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๓. พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐

๔. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

๕. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

๖. พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙

๗. พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓

๘. ประกาศคณะกรรมการธุรกรรมอิเล็กทรอนิกส์เรื่อง มาตรฐานการรักษาความปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕

๙. มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมอิเล็กทรอนิกส์ตามมาตรฐาน ISO/IEC 27001

๑๐. ระเบียบการประปาส่วนภูมิภาคว่าด้วยการใช้งานเครือข่ายคอมพิวเตอร์และระบบสารสนเทศอย่างปลอดภัย

๑๑. นโยบายความมั่นคงปลอดภัยด้านสารสนเทศของ กปภ.

ประกาศ ณ วันที่ ๑๗ กันยายน พ.ศ. ๒๕๖๗

(นายจักรพงศ์ คำจันทร์)
รองผู้ว่าการ (ปฏิบัติการ ๒) รักษาการแทน
ผู้ว่าการการประปาส่วนภูมิภาค