แนวนโยบายธรรมาภิบาลข้อมูลภาครัฐของ
สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

บทที่ 1 บทนำ (Introduction)

๑) ความเป็นมา

การทำงานของสำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (สป.ดศ.) จำเป็นต้องอาศัยข้อมูลจำนวนมาก ทั้งที่ได้รับจากภายนอกและจากการสร้างหรือประมวลผลขึ้นเอง ปัจจุบันข้อมูลมีหลายระดับหลายรูปแบบ กระจายในแต่ละ สำนักงาน/กอง/กลุ่ม/ศูนย์ โดยแต่ละ สำนักงาน/กอง/กลุ่ม/ศูนย์ มีการจัดเก็บในรูปแบบที่แตกต่างกันไป แต่ส่วนใหญ่แล้วมักจะเก็บในรูปแบบกระดาษและไฟล์ควบคู่กัน เมื่อมีการต้องแลกเปลี่ยนข้อมูลระหว่าง สำนักงาน/กอง/กลุ่ม/ศูนย์ อย่างไม่เป็นทางการ มักจะใช้วิธีการส่งเป็นไฟล์หรือกระดาษ โดยไม่มีกระบวนการอย่างชัดเจน ซึ่งหาก สำนักงาน/กอง/กลุ่ม/ศูนย์ ต้องการส่งข้อมูลระหว่างกันอย่างเป็นทางการจะต้องใช้วิธีการทำเป็นหนังสือราชการ ซึ่งทำให้ใช้ระยะเวลาและใช้ทรัพยากร

ปัญหาที่เกิดขึ้นจากการแลกเปลี่ยนข้อมูลในปัจจุบัน มีดังนี้

๑) การแลกเปลี่ยนข้อมูลไม่เป็นอัตโนมัติเมื่อมีการแก้ไขหรือปรับปรุงข้อมูล

๒) ไม่มีมาตรฐานในการแลกเปลี่ยนข้อมูลที่ชัดเจน

๓) การแลกเปลี่ยนข้อมูลเป็นไปได้ช้า เนื่องจากมีขั้นตอนในการรับส่งข้อมูล

๔) ไม่มีการวางแผนและออกแบบ

๕) เป้าหมายไม่ชัดเจน

๖) ไม่มีมาตรฐาน

๗) ไม่รองรับการเปลี่ยนแปลง

๒) วัตถุประสงค์ของแนวนโยบายธรรมาภิบาลข้อมูลภาครัฐ

๒.๑ เพื่อให้ สป.ดศ. มีนโยบายและแนวปฏิบัติสำหรับธรรมาภิบาลข้อมูลภาครัฐและการบริหารจัดการข้อมูล เพื่อมุ่งไปสู่การเป็นหน่วยงานที่ขับเคลื่อนด้วยข้อมูล (Data-driven Organization) โดยมีความสอดคล้องกับพระราชบัญญัติ ประกาศ ระเบียบ แนวปฏิบัติ หรือกฎหมายอื่นๆ ที่เกี่ยวข้อง

๒.๒ เพื่อกำหนดบทบาทหน้าที่ ขอบเขตความรับผิดชอบของผู้มีส่วนเกี่ยวข้องกับข้อมูลทั้งหมดใน สป.ดศ.

ตามกรอบธรรมาภิบาลข้อมูลภาครัฐ

๒.๓ เพื่อปกป้องรักษาข้อมูลของ สป.ดศ. จากความเสี่ยงหรือภัยคุกคาม และดูแลความลับหรือความเป็นส่วนบุคคลของข้อมูลได้อย่างถูกต้อง สอดคล้องตามกรอบธรรมาภิบาลข้อมูลภาครัฐ และมีการปรับปรุงอย่างต่อเนื่อง

๒.๔ เพื่อดูแลรักษามาตรฐานและคุณภาพข้อมูล ให้มีความน่าเชื่อถือและมีความมั่นคงปลอดภัยสอดคล้องตามหลักมาตรฐานสากล

๓) ขอบเขตของเนื้อหาภายในธรรมาภิบาลข้อมูลภาครัฐสำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

๓.๑) นโยบายข้อมูลฉบับนี้มีผลบังคับใช้กับข้อมูลของ สป.ดศ. ผู้บริหาร ข้าราชการ พนักงานราชการ ลูกจ้าง เจ้าหน้าที่ ผู้ใช้งาน และผู้ที่เกี่ยวข้อง โดยมีหน้าที่ที่จะต้องสนับสนุน ดำเนินการ และปฏิบัติตามอย่างเคร่งครัด

๓.๒) นโยบายข้อมูลฉบับนี้จะต้องดำเนินการเผยแพร่โดยวิธีการลงประกาศในระบบ e-office ของ สป.ดศ. ทั้งนี้ ควรดำเนินการทบทวนอย่างน้อยปีละหนึ่งครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ หรือเมื่อมีข้อเสนอแนะตามที่คณะกรรมการธรรมาภิบาลข้อมูลภาครัฐของ สป.ดศ. เห็นสมควร

๓.๓) นโยบายข้อมูลฉบับนี้ครอบคลุมข้อมูลทั้งหมดที่มีอยู่ใน สป.ดศ. โดยข้อมูลหมายถึง สิ่งที่สื่อความหมายให้รู้เรื่องราวข้อเท็จจริงหรือเรื่องอื่นใดไม่ว่าจะเป็นข้อความ เอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ภาพถ่ายดาวเทียม ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ เครื่องมือตรวจวัด การสำรวจระยะไกล หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้ ทั้งที่เป็นอิเล็กทรอนิกส์และไม่เป็นอิเล็กทรอนิกส์ และครอบคลุมการได้มาของข้อมูลในทุกทาง ดังนี้

๑) ข้อมูลจากแหล่งภายนอกที่ได้มาตามบทบาทหน้าที่

๒) ข้อมูลที่เกิดจากการปฏิบัติงานภายใน สป.ดศ.

๓) ข้อมูลที่ได้จากการเชื่อมโยงและแลกเปลี่ยนตามความร่วมมือระหว่าง สป.ดศ. กับหน่วยงานภายนอก

๔) ข้อมูลที่ได้จากการจัดซื้อจัดจ้าง หรือการทำนิติกรรมสัญญา

๕) ข้อมูลข่าวสารสาธารณะ

๔) บทบาทหน้าที่ความรับผิดชอบ

๔.๑) ผู้บริหารข้อมูลระดับสูง (Chief Data Officer) ทำหน้าที่กำหนดวิสัยทัศน์ ให้ข้อเสนอแนะ อนุมัตินโยบายข้อมูล มาตรฐานข้อมูล แนวทางปฏิบัติงาน เกณฑ์การวัดคุณภาพ ระเบียบ และข้อบังคับอื่นๆ ที่เกี่ยวข้องกับข้อมูล รวมไปถึงการจัดลำดับความสำคัญและแก้ไขปัญหาที่เกี่ยวข้องกับข้อมูล

๔.๒) คณะกรรมการธรรมาภิบาลข้อมูลภาครัฐโดยคณะกรรมการพิจารณาข้อมูลข่าวสารและ

บริหารจัดการข้อมูลของ สป.ดศ. เป็นกลุ่มบุคคลที่ประกอบด้วย ผู้บริหารระดับสูงและผู้บริหารระดับสำนักงาน/กอง/กลุ่ม/ศูนย์ หรือผู้แทนที่ สป.ดศ. แต่งตั้ง ทำหน้าที่กำหนดทิศทางการดำเนินการสร้างธรรมาภิบาลข้อมูลภาครัฐให้สอดคล้องกับภารกิจและยุทธศาสตร์ของ สป.ดศ. ตัดสินใจเชิงนโยบาย แก้ไขปัญหา รวมถึงส่งเสริมสนับสนุนให้เกิดการมีส่วนร่วมและปรับปรุงการดำเนินงานอย่างต่อเนื่อง

๔.๓) ทีมบริกรข้อมูล (Data Stewards) เป็นกลุ่มบุคคลที่มีหน้าที่กำกับดูแล ติดตาม และรายงานผลการดำเนินงานธรรมาภิบาลข้อมูลภาครัฐ ครอบคลุมทั้งด้านธุรกิจ ด้านเทคนิค คุณภาพข้อมูล ความมั่นคงปลอดภัย และกฎหมาย โดยมุ่งเน้นการดำเนินงานและกำหนดมาตรฐานในการบริหารจัดการข้อมูล มีบทบาทหน้าที่ ดังนี้

๑) นิยามความต้องการด้านคุณภาพ และความมั่นคงปลอดภัย

๒) นิยามเมทาดาตา (Metadata) และบัญชีข้อมูล (Data Catalog)

๓) ร่างนโยบายข้อมูล มาตรฐาน และแนวปฏิบัติต่างๆ ที่เกี่ยวข้องกับข้อมูล

๔) ตรวจสอบการปฏิบัติตามนโยบายข้อมูล ตรวจสอบคุณภาพ ตรวจสอบความมั่นคงปลอดภัยของข้อมูล และวิเคราะห์ผลจากการตรวจสอบ

๕) ดำเนินการในเรื่องคุณภาพข้อมูล เช่น กำหนดนโยบายข้อมูลด้านคุณภาพ การตรวจวัดคุณภาพข้อมูล และการวิเคราะห์คุณภาพข้อมูล

๔.๔) ผู้ควบคุมข้อมูล (Data Controllers) เป็นระดับผู้อำนวยการสำนัก มีบทบาทหน้าที่ ดังนี้

๑) ตัดสินใจเกี่ยวกับแนวทางเก็บรวบรวม การใช้ การเผยแพร่หรือการเปิดเผยข้อมูล กำหนดอายุการใช้งานและระยะเวลาการจัดเก็บหลังสิ้นสุดการใช้งาน รวมถึงแนวทางการทำลายข้อมูลที่กำกับดูแล

๒) กำหนดขอบเขตการเข้าถึง แนวทางการจัดชั้นความลับและดำเนินงานใดๆ กับข้อมูลที่กำกับดูแล ทั้งข้อมูลที่มีโครงสร้าง (เช่น ฐานข้อมูล) ข้อมูลกึ่งโครงสร้าง (เช่น Extensible Markup Language – XML) ข้อมูลที่ไม่มีโครงสร้าง (เช่น เสียง ภาพ ภาพเคลื่อนไหว) พร้อมทั้งจัดให้มีการจัดทำทะเบียนข้อมูลให้เป็นปัจจุบัน

๓) รับผิดชอบดูแล บริหารจัดการ และรักษาคุณภาพข้อมูลให้สอดคล้องกับนโยบายข้อมูล มาตรฐาน กฎ ระเบียบ หรือกฎหมายที่เกี่ยวข้อง

๔) ทบทวน ประเมินประสิทธิผลของข้อมูลในภาพรวม และอนุมัติการดำเนินการต่างๆ ที่เกี่ยวข้องกับข้อมูลที่กำกับดูแล

๔.๕) ทีมบริหารจัดการข้อมูล (Data Management Team) เป็นกลุ่มบุคคลที่มีหน้าที่บริหารจัดการข้อมูลให้เป็นไปตามธรรมาภิบาลข้อมูลภาครัฐและการกำกับดูแลข้อมูลส่วนบุคคล มีบทบาทหน้าที่ ดังนี้

๑) ดำเนินการบริหารจัดการข้อมูลให้ครอบคลุมทั้งวงจรชีวิตของข้อมูล ตั้งแต่การสร้างข้อมูล (Data Creation) การจัดเก็บข้อมูล (Data Storage) การประมวลผลและใช้ข้อมูล (Data Processing and Use) การเชื่อมโยงและแลกเปลี่ยนข้อมูล (Data Linkage and Exchange) การเปิดเผยข้อมูล (Data Disclosure) และการทำลายข้อมูล (Data Destruction)

๒) บริหารจัดการข้อมูลในด้านต่าง ๆ เช่น สถาปัตยกรรมและความสัมพันธ์ของข้อมูล การสร้าง

แบบจำลองและออกแบบข้อมูล การจัดเก็บและดำเนินการกับข้อมูล การบูรณาการและเชื่อมโยงข้อมูล การวิเคราะห์ข้อมูล การจัดทำมาตรฐานชุดข้อมูลและรายละเอียด การรักษาความมั่นคงปลอดภัยและความเป็นส่วนบุคคลของข้อมูล และรักษาคุณภาพข้อมูล

๓) สนับสนุนกิจกรรมธรรมาภิบาลข้อมูลภาครัฐ เช่น ตรวจสอบให้มีการปฏิบัติตามนโยบายข้อมูล ช่วยเหลือในการจัดทำพจนานุกรมข้อมูล (Data Dictionary) นิยามเมทาดาตา (Metadata) บัญชีข้อมูล (Data Catalog) เป็นมาตรฐานสอดคล้องกันทั่วทั้ง สป.ดศ. และกำหนดสิทธิการเข้าถึงข้อมูลตามแนวทางที่ผู้ควบคุมข้อมูลกำหนด

๔) ให้คำแนะนำหรือข้อเสนอแนะแก่ผู้ควบคุมข้อมูล ผู้ใช้งานข้อมูลและผู้ที่เกี่ยวข้อง สอดคลองกับการดำเนินการตามนโยบายข้อมูล เพื่อกำกับดูแลให้ข้อมูลเป็นมาตรฐาน มีความมั่นคงปลอดภัย และการขอใช้ข้อมูลอย่างเหมาะสม

๕) ให้คำแนะนำผู้ควบคุมข้อมูล ผู้ใช้ข้อมูล ผู้สร้างข้อมูลและผู้ที่เกี่ยวข้องอื่นๆ เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ให้สอดคล้องตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

๖) จัดทำทะเบียนข้อมูลกลางของ สป.ดศ. เพื่อทำการบันทึกข้อมูลที่เก็บรวบรวมหรือสร้างขึ้นอย่างเป็นระบบและจัดเก็บร่องรอยของการเปลี่ยนแปลงแก้ไขหรือกิจกรรมที่เกิดขึ้นกับข้อมูล

๔.๖) ผู้ใช้ข้อมูล (Data Users) เป็นบุคคลที่นำข้อมูลไปใช้งานตามบทบาทหน้าที่และความรับผิดชอบเพื่อวิเคราะห์ หรือวิจัย ทั้งในงานระดับปฏิบัติการและระดับบริหาร ต้องปฏิบัติตามแนวนโยบายข้อมูล มีความรับผิดชอบต่อความมั่นคงปลอดภัย การรักษาความลับ และการดำเนินการกับข้อมูลให้สอดคล้องกับสิทธิที่ได้รับ หากพบการรั่วไหลหรือปัญหาระหว่างการใช้ข้อมูลทั้งด้านคุณภาพและความปลอดภัย ต้องรีบแจ้งไปยังผู้ควบคุมข้อมูลดังกล่าวหรือทีมบริกรข้อมูล

๔.๗) ผู้สร้างข้อมูล (Data Creators) เป็นบุคคลที่ทำหน้าที่บันทึก แก้ไข ปรับปรุง หรือลบข้อมูลให้สอดคล้องกับโครงสร้างที่ถูกกำหนดไว้ นอกจากนี้ ยังมีหน้าที่ในการทำงานร่วมกับผู้ควบคุมข้อมูล ทีมบริหารจัดการข้อมูล และทีมบริกรข้อมูล เพื่อตรวจสอบและแก้ไขปัญหาด้านคุณภาพข้อมูลและความมั่นคงปลอดภัยให้สอดคล้องกับกฎ ระเบียบ นโยบาย หรือมาตรฐานข้อมูลของ สป.ดศ.

๔.๘) เจ้าของข้อมูลส่วนบุคคล (Data Subject) เป็นบุคคลผู้เป็นเจ้าของข้อมูลส่วนบุคคลหรือผู้มีสิทธิโดยชอบตามกฎหมาย

บทที่ 2 นโยบายข้อมูลสำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

๑. หมวดทั่วไป (General Domain)

๑) กำหนดบทบาท หน้าที่ และความรับผิดชอบของแต่ละบุคคลตามโครงสร้างธรรมาภิบาลข้อมูลภาครัฐ โดยต้องได้รับการมอบอำนาจและการอนุมัติจาก ปดศ. ในฐานะผู้บริหารระดับสูง (Chief Executive Officer : CEO) ของ สป.ดศ.

๒) กำหนดกลุ่มบุคคลหรือบุคคลภายใน สป.ดศ. เพื่อทำหน้าที่เป็นผู้ควบคุมข้อมูลในการบริหารจัดการข้อมูลของหน่วยงานภายใน สป.ดศ. เนื่องจากหน่วยงานภายใน สป.ดศ. ถือเป็นเจ้าของข้อมูลทุกประเภทที่เกิดจากการดำเนินงานภายในหน่วยงานนั้น

๓) กำหนดให้มีการประเมินผลการดำเนินการและความสำเร็จของธรรมาภิบาลข้อมูลภาครัฐ โดยอย่างน้อยต้องมีในเรื่อง ดังต่อไปนี้

๓.๑) กำหนดให้มีการประเมินความพร้อมธรรมาภิบาลข้อมูลภาครัฐ

๓.๒) กำหนดให้มีการประเมินคุณภาพข้อมูล เพื่อให้ข้อมูลมีความครบถ้วน ถูกต้องตรงกัน มีความเป็นปัจจุบัน ตรงตามความต้องการของผู้ใช้ และมีความพร้อมใช้

๓.๓) กำหนดให้มีการประเมินความมั่นคงปลอดภัยของข้อมูล เพื่อให้ข้อมูลมีการจัดชั้นความลับใช้งานเหมาะสม และความพร้อมใช้อยู่เสมอ

๔) ทบทวนนโยบายข้อมูล มาตรการรักษาความมั่นคงปลอดภัยของข้อมูล ตรวจสอบความสอดคล้องกันระหว่างนโยบายข้อมูลกับการดำเนินการใดๆ ของผู้มีส่วนได้เสีย อย่างน้อยปีละหนึ่งครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ

๕) กำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล เพื่อป้องกันการละเมิด การเข้าถึง การสูญหาย การทำลาย หรือการเปลี่ยนแปลงข้อมูล สอดคล้องกับธรรมาภิบาลข้อมูลภาครัฐและพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

๖) เผยแพร่ประชาสัมพันธ์นโยบายข้อมูลให้แก่บุคคลหรือหน่วยงานที่เกี่ยวข้องทั้งภายในและภายนอก สป.ดศ. เพื่อให้มีความรู้ความเข้าใจต่อการปฏิบัติตามอย่างเพียงพอ

๗) กำหนดให้แจ้งความมีอยู่ของชุดข้อมูลและกำหนดให้มีมาตรฐานรายละเอียดข้อมูล เช่น พจนานุกรมข้อมูล (Data Dictionary) เมทาดาตา (Metadata) บัญชีข้อมูล (Data Catalog) และการจัดชั้นความลับข้อมูล (Data Classification Level) เพื่อจัดลำดับความสำคัญของข้อมูลให้มีความมั่นคงปลอดภัยสารสนเทศอย่างเหมาะสม

๘) ส่งเสริมการนำระบบเทคโนโลยีสารสนเทศเพื่อใช้เป็นระบบกลางในการบริหารจัดการข้อมูลของ สป.ดศ. สำหรับจัดทำคำอธิบายเมทาดาตา (Metadata) และบัญชีข้อมูล (Data Catalog) ให้สอดคล้องกับมาตรฐานตามธรรมาภิบาลข้อมูลภาครัฐ

๙) สนับสนุนให้มีการฝึกอบรมเพื่อสร้างความตระหนักถึงธรรมาภิบาลข้อมูลภาครัฐ โดยให้ครอบคลุมทุกกระบวนการของการบริหารจัดการและวงจรชีวิตของข้อมูล

๑๐) พระราชบัญญัติ ประกาศ ระเบียบ แนวปฏิบัติ หรือกฎหมายที่เกี่ยวข้องกับแนวนโยบายข้อมูลนี้ที่ได้ประกาศใช้แล้ว ได้แก่

๑๐.๑) พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐

๑๐.๒) พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ และที่แก้ไขเพิ่มเติม

๑๐.๓) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม

๑๐.๔) พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒

๑๐.๕) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

๑๐.๖) พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๑๐.๗) ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่องธรรมาภิบาลข้อมูลภาครัฐ ลงวันที่ ๑๒ มีนาคม ๒๕๖๓

๑๐.๘) แนวปฏิบัติด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศของ สป.ดศ. ประจำปี ๒๕๖๔

๒. การสร้างข้อมูล (Data Creation)

๑) กำหนดให้มีแนวปฏิบัติเกี่ยวกับการสร้างข้อมูลให้มีความปลอดภัย ถูกต้อง น่าเชื่อถือ และเป็นประโยชน์ต่อผู้ใช้ข้อมูล

๒) ห้ามนำข้อมูลที่มีลักษณะดังต่อไปนี้เข้าสู่ระบบคอมพิวเตอร์อันเป็นการกระทำที่ขัดต่อกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

๒.๑) ข้อมูลที่บิดเบือน หรือปลอมไม่ว่าทั้งหมดหรือบางส่วน

๒.๒) ข้อมูลอันเป็นเท็จที่น่าจะเกิดความเสียหายต่อการรักษาความมั่นคงปลอดภัย ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจ หรือโครงสร้างพื้นฐาน หรือก่อให้เกิดความตื่นตระหนก

๒.๓) ข้อมูลอันเป็นความผิดเกี่ยวกับความมั่นคง หรือความผิดเกี่ยวกับการก่อการร้าย

๒.๔) ข้อมูลที่มีลักษณะอันลามกและอาจเข้าถึงได้

๒.๕) ข้อมูลที่ปรากฏภาพของผู้อื่น และเป็นภาพที่สร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ ซึ่งทำให้ผู้อื่นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

๓) ห้ามสร้างหรือทำซ้ำต่อข้อมูลของผู้อื่นอันเป็นการกระทำที่ขัดต่อกฎหมายว่าด้วยลิขสิทธิ์หรือกฎหมายเกี่ยวกับทรัพย์สินทางปัญญาอื่น เว้นแต่จะเป็นไปตามอำนาจที่กฎหมายรับรอง

๔) กำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัยของการสร้างข้อมูล โดยอย่างน้อยต้องครอบคลุมในเรื่องดังต่อไปนี้

๔.๑) การลงทะเบียนและการระบุตัวตน

๔.๒) การยืนยันตัวตน

๔.๓) การกำหนดสิทธิและทบทวนสิทธิ

๔.๔) ความรับผิดชอบต่อการสร้างข้อมูล

๕) ทบทวนสิทธิการเข้าถึงของผู้ใช้งานอย่างน้อยปีละครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ เช่น ผู้ใช้งานลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง หรือเมื่อมีการปรับปรุงระบบเทคโนโลยีสารสนเทศ

๖) กำหนดให้มีและจัดเก็บคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตา (Metadata) เมื่อมีการสร้างข้อมูล

๗) กำหนดให้มีการสร้างข้อมูล ที่มาจากแหล่งข้อมูลต้นทางโดยตรงหรือแหล่งข้อมูลที่น่าเชื่อถือ

๓. การจัดเก็บข้อมูล (Data Storage and Archive)

๑) กำหนดสภาพแวดล้อมและแนวปฏิบัติของการจัดเก็บข้อมูล เพื่อให้มีความมั่นคงปลอดภัย

๒) กำหนดชั้นความลับของข้อมูล และจัดเก็บให้สอดคล้องกับประเภทชั้นความลับข้อมูลตามที่กฎหมาย นโยบาย หรือแนวปฏิบัติกำหนด เพื่อให้ข้อมูลมีความมั่นคงปลอดภัยและรักษาคุณภาพของข้อมูล

๓) กำหนดสิทธิการเข้าถึง และเครื่องมือที่ใช้ในการเข้าถึงข้อมูลที่จัดเก็บ

๔) กำหนดให้มีการจัดเก็บข้อมูลโดยใช้วิธีการที่น่าเชื่อเถือได้ในการรักษาความถูกต้อง ครบถ้วน

๕) กำหนดให้มีการจัดทำคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตา (Metadata) ของข้อมูลที่มีการจัดเก็บและปรับปรุงให้เป็นปัจจุบัน

๖) กำหนดให้มีการจัดเก็บข้อมูลส่วนบุคคล โดยเก็บรวบรวมเท่าที่จำเป็นภายใต้อำนาจหน้าที่และวัตถุประสงค์อันชอบด้วยกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

๗) กำหนดให้มีการยกเลิกการจัดเก็บข้อมูลกรณีผู้ควบคุมข้อมูลได้รับการร้องขอจากเจ้าของข้อมูลส่วนบุคคล หรือเจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอม ตามที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลกำหนด

๘) กำหนดให้มีการจัดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวันนับแต่วันที่ ข้อมูลเข้าสู่ระบบคอมพิวเตอร์ โดยจัดเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการนับแต่เริ่มใช้บริการให้สอดคล้องตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

๙) กำหนดการจัดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ให้สอดคล้องตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ โดยผู้ดูแลระบบสารสนเทศจะต้องใช้วิธีการที่มั่นคงปลอดภัย อย่างน้อย ดังนี้

๙.๑) เก็บลงในสื่อที่รักษาความครบถ้วนถูกต้องแท้จริง (Integrity) และระบุตัวตน (Identification) ที่เข้าถึงสื่อได้

๙.๒) มีการรักษาความลับของข้อมูล และกำหนดชั้นความลับในการเข้าถึงและจัดเก็บข้อมูล เพื่อรักษาความน่าเชื่อถือของข้อมูล และไม่อนุญาตให้ผู้ดูแลระบบแก้ไขข้อมูลที่จัดเก็บไว้ได้

๙.๓) การจัดเก็บข้อมูลที่ระบุรายละเอียดผู้ใช้บริการเป็นรายบุคคลได้ (Identification and Authentication) เช่น Proxy Server NAT เป็นต้น

๑๐) กำหนดให้มีมาตรการรักษาความปลอดภัยในการจัดเก็บข้อมูล รวมทั้งกรณีที่มีการเคลื่อนย้ายอุปกรณ์ที่จัดเก็บข้อมูล เพื่อป้องกันมิให้มีการเข้าถึงโดยมิได้รับอนุญาต หรือลักลอบนำข้อมูลไปใช้ที่ก่อให้เกิดความเสียหายต่อ สป.ดศ.

๑๑) กำหนดให้มีการกำหนดช่วงระยะเวลาของข้อมูลที่มีการจัดเก็บเกินระยะเวลาที่กำหนดหรือไม่ได้ใช้งาน เพื่อทำสำเนาสำหรับจัดเก็บข้อมูลถาวร (Archive)

๑๒) กำหนดมาตรการรักษาความปลอดภัยของข้อมูลที่จัดเก็บถาวร เพื่อป้องกันข้อมูลไม่ให้มีการลบ ปรับปรุง หรือแก้ไขได้ รวมทั้งป้องกันมิให้ข้อมูลที่จัดเก็บถาวรรั่วไหลไปยังบุคคลที่ไม่ได้รับอนุญาต

๑๓) กำหนดให้มีมาตรการรักษาความปลอดภัยของการถ่ายโอนข้อมูลกับหน่วยงานภายนอกที่ผ่านช่องทางการสื่อสารทุกชนิด โดยต้องสอดคล้องตามแนวนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ สป.ดศ.

๑๔) กำหนดให้มีแนวปฏิบัติการทดสอบกู้คืนข้อมูลที่จัดเก็บถาวร สำหรับข้อมูลที่มีความสำคัญมากต่อการดำเนินงานของ สป.ดศ. เพื่อสอบทานความถูกต้อง ครบถ้วน ความพร้อมใช้งาน และคุณภาพข้อมูล

๑๕) ห้ามจัดเก็บข้อมูลส่วนตัวหรือข้อมูลที่ไม่เกี่ยวข้องกับการดำเนินงานของ สป.ดศ. สำหรับการจัดเก็บข้อมูลถาวรบนเครื่องแม่ข่ายที่ สป.ดศ. จัดสรรไว้

๑๖) กำหนดให้มีการทบทวนเกี่ยวกับช่วงระยะเวลาการจัดเก็บข้อมูล มาตรการ และแนวปฏิบัติที่เกี่ยวข้องกับการจัดเก็บข้อมูลถาวร อย่างน้อยปีละหนึ่งครั้ง

๔. การประมวลผลและใช้ข้อมูล (Data Processing and Use)

๑) กำหนดให้มีแนวปฏิบัติเกี่ยวกับการประมวลผลและการใช้ข้อมูลของ สป.ดศ.

๒) การประมวลผลข้อมูลที่มีชั้นความลับจะต้องปฏิบัติตามแนวปฏิบัติการจัดชั้นความลับของข้อมูล สป.ดศ. อย่างเคร่งครัด

๓) กำหนดให้มีการประมวลผลข้อมูลหรือใช้ข้อมูลส่วนบุคคล โดยประมวลผลหรือใช้ข้อมูลเท่าที่จำเป็นภายใต้อำนาจหน้าที่และวัตถุประสงค์อันชอบด้วยกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

๔) กำหนดให้มีการยกเลิกการประมวลผลข้อมูลหรือการใช้ข้อมูลส่วนบุคคล กรณีที่ผู้ควบคุมข้อมูลถอนความยินยอมตามที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลกำหนด

๕) ห้ามใช้ข้อมูลในเครือข่ายของ สป.ดศ. เพื่อประโยชน์ในเชิงธุรกิจเป็นการส่วนตัว หรือเพื่อเข้าสู่เว็บไซต์ที่ไม่เหมาะสม หรือใช้ข้อมูลอันก่อให้เกิดความเสียหายต่อ สป.ดศ.

๖) กำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัยในการประมวลผลข้อมูลและการใช้ข้อมูลที่ได้กำหนดลำดับชั้นข้อมูลตั้งแต่ลับขึ้นไป อย่างเพียงพอและมีประสิทธิภาพ

๗) กำหนดมีการจัดทำเมทาดาตาสำหรับข้อมูลที่จัดเก็บอยู่ในคลังข้อมูล (Data Warehouse) และการบันทึกประวัติการประมวลผลและการใช้ข้อมูล (Log File) เพื่อให้สามารถตรวจสอบย้อนกลับได้

๕. การเชื่อมโยงและแลกเปลี่ยนข้อมูล (Data Linkage and Exchange)

๑) กำหนดให้มีแนวปฏิบัติและมาตรฐานทางด้านเทคนิคที่จำเป็นต้องใช้เกี่ยวกับการเชื่อมโยงและการแลกเปลี่ยนข้อมูลดิจิทัลของ สป.ดศ.

๒) กำหนดให้มีคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตา (Metadata) สำหรับข้อมูลที่มีการเชื่อมโยงและการแลกเปลี่ยนข้อมูลดิจิทัลระหว่างกันที่จำเป็นให้ครบถ้วน

๓) กำหนดให้มีสัญญาหรือข้อตกลงระหว่างบุคคลหรือหน่วยงานภายนอก ในการเชื่อมโยงและแลกเปลี่ยนข้อมูล รวมถึงการนำข้อมูลที่ได้ไปใช้สำหรับภายนอกหน่วยงาน

๔) กำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัยเกี่ยวกับการเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัลเพื่อป้องกันมิให้มีการรับส่งข้อมูลที่ไม่สมบูรณ์ ส่งข้อมูลไปผิดที่ หรือมีการรั่วไหลของข้อมูล หรือ ข้อมูลถูกแก้ไขเปลี่ยนแปลง ทำซ้ำใหม่ หรือส่งซ้ำโดยมิได้รับอนุญาต

๕) ห้ามเชื่อมโยงและแลกเปลี่ยนเพื่อส่งต่อข้อมูลคอมพิวเตอร์ที่เป็นการกระทำความผิดตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

๖) กำหนดให้มีแนวปฏิบัติในการเก็บบันทึกข้อมูลจราจรทางคอมพิวเตอร์ (Log File) และตรวจสอบสิ่งผิดปกติต่างๆ ที่เกิดขึ้นในการเชื่อมโยงและแลกเปลี่ยนข้อมูล

๗) กำหนดมาตรฐานเปิดสำหรับการเชื่อมโยงและแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ในรูปแบบข้อความ XLS หรือ XLSX หรือ CSV หรือ JSON หรือ XML หรือมาตรฐานที่สูงกว่า และกำหนดกระบวนการทางธุรกิจเพื่อออกเป็นข้อกำหนดภายใน สป.ดศ.

๘) กำหนดให้มีการระบุตัวตนของผู้ลงลายมือชื่อโดยการใช้ลายมือชื่ออิเล็กทรอนิกส์ รวมถึงกลไกการรับรองความถูกต้องของเอกสารอิเล็กทรอนิกส์สำหรับการเชื่อมโยงและแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ของ สป.ดศ. โดยการใช้ข้อความ XLS หรือ XLSX หรือ CSV หรือ JSON หรือ XML หรือมาตรฐานที่สูงกว่า

๙) กำหนดให้มีการตรวจสอบความถูกต้องครบถ้วนของข้อมูล XLS หรือ XLSX หรือ CSV หรือ JSON หรือ XML หรือมาตรฐานที่สูงกว่า และพิสูจน์เวลาการลงลายมือชื่ออิเล็กทรอนิกส์

๑๐) กำหนดให้มีแนวปฏิบัติหรือระเบียบในการดำเนินการเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัลระหว่างหน่วยงานของรัฐแห่งอื่นที่ได้จัดทำหรือรวบรวมข้อมูลดิจิทัลไว้เป็นข้อมูลหลักไม่ว่าทั้งหมดหรือบางส่วนโดยหน่วยงานของรัฐนั้นไม่ต้องจัดทำข้อมูลดังกล่าวขึ้นใหม่ทั้งหมด

๖. การเปิดเผยข้อมูล (Data Disclosure)

๑) ข้อมูลที่เปิดเผยต่อสาธารณะให้ปฏิบัติตามกฎหมายว่าด้วยข้อมูลข่าวสารของราชการ และแนวปฏิบัติการเปิดเผยข้อมูลอย่างเคร่งครัด

๒) กำหนดให้มีคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตา (Metadata) สำหรับข้อมูลที่ต้องเปิดเผย

๓) กำหนดให้มีช่องทางการเปิดเผยข้อมูลที่สามารถเข้าถึงและนำข้อมูลออกมาใช้งาน

๔) กำหนดเงื่อนไขและข้อกำหนดของข้อมูลที่นำมาเปิดเผยภายในเครือข่ายของ สป.ดศ. โดยข้อมูลที่เปิดเผยต้องไม่ขัดต่อกฎหมายเกี่ยวกับทรัพย์สินทางปัญญา เว้นแต่การเปิดเผยข้อมูลจะเป็นไปตามอำนาจที่กฎหมายรับรอง

๕) การเปิดเผยข้อมูลส่วนบุคคล ภายใต้อำนาจหน้าที่และวัตถุประสงค์ และดำเนินการใดๆ อันเกี่ยวข้องกับกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

๖) ห้ามเผยแพร่ข้อมูลที่เป็นการกระทำความผิดตามกฎหมาย นโยบาย และแนวปฏิบัติอันทำให้เกิดความเสียหายต่อ สป.ดศ.

๗) กำหนดให้มีการจัดลำดับชั้นความสำคัญของชุดข้อมูลที่มีคุณค่าสูง (High – Value dataset) เพื่อกำหนดให้อยู่ลำดับต้นในการคัดเลือกมาเผยแพร่

๘) กำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัยในการเปิดเผยข้อมูลที่กำหนดลำดับชั้นข้อมูลตั้งแต่ลับขึ้นไป อย่างเพียงพอและมีประสิทธิภาพ

๙) สนับสนุนการเผยแพร่ข้อมูลผ่านช่องทางที่ง่ายต่อการเข้าถึงข้อมูล

๑๐) กำหนดลักษณะของข้อมูลที่เผยแพร่ให้อยู่ในรูปแบบข้อมูลที่เครื่องสามารถประมวลผลได้

๑๑) ข้อมูลที่เผยแพร่จะต้องมีการบันทึกเวลา (Timestamps) ที่ช่วยให้ผู้ใช้งานสามารถระบุได้ว่าข้อมูลนั้นเป็นปัจจุบัน

๑๒) ข้อมูลที่เผยแพร่ต้องมาจากแหล่งที่เก็บข้อมูลโดยตรง ด้วยระดับความละเอียดสูงโดยไม่มีการปรับแต่งหรือเป็นข้อมูลรูปแบบสรุป (Summary Data)

๑๓) มีการตรวจสอบข้อมูลที่เผยแพร่จากหน่วยงานทั้งภายในและภายนอก สป.ดศ. เพื่อให้มั่นใจว่า สป.ดศ. มีข้อมูลที่เผยแพร่ที่มีคุณภาพ

๑๔) กำหนดให้มีข้อตกลงการเผยแพร่ข้อมูลที่เป็นชนิดเดียวกันที่ได้จากสองหน่วยงานขึ้นไป โดยมีการหารือร่วมกันระหว่างหน่วยงานที่เปิดเผยข้อมูลดังกล่าวถึงข้อดีข้อเสียในการพิจารณาการลงทุนทรัพยากร และความรวดเร็วในการดำเนินการเปิดเผยข้อมูล

๑๕) ชุดข้อมูลและรายการชุดข้อมูลที่เผยแพร่ จะต้องมีการจัดรูปแบบที่กำหนดเป็นมาตรฐานและกำหนดภายใต้หมวดหมู่เดียวกัน เพื่อให้ผู้ใช้ข้อมูลสามารถค้นหาและเข้าถึงข้อมูลได้ง่าย

๑๖) การเผยแพร่ข้อมูลต้องมีการตรวจสอบรูปแบบข้อมูลที่เผยแพร่ให้สอดคล้องกับมาตรฐานที่ สป.ดศ. กำหนด

๑๗) รูปแบบข้อมูลที่เผยแพร่ต้องเป็นข้อมูลที่เครื่องอ่านได้ (Machine – readable) มีความถูกต้องครบถ้วน ไม่มีผู้ใดถือครองกรรมสิทธิ์ (Non – proprietary) และไม่ขัดต่อกฎหมายเกี่ยวกับทรัพย์สินทางปัญญา

๗. การทำลายข้อมูล (Data Destruction)

๑) กำหนดให้มีแนวปฏิบัติการทำลายข้อมูล และกระบวนการพิจารณาอนุมัติทำลายจากผู้มีอำนาจ

๒) การทำลายข้อมูลที่มีลำดับชั้นข้อมูลตั้งแต่ลับขึ้นไป ให้ถือว่าปฏิบัติตามแนวปฏิบัติการทำลายข้อมูลที่มีชั้นความลับอย่างเคร่งครัด

๓) กำหนดให้มีคณะกรรมการทำลายข้อมูล และบทบาทหน้าที่ความรับผิดชอบ

๔) จัดเก็บคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตา (Metadata) ของข้อมูลที่ทำลายสำหรับตรวจสอบในภายหลัง

๕) ตรวจสอบความสอดคล้องแนวปฏิบัติการทำลายข้อมูลให้สอดคล้องต่อกฎหมาย นโยบาย และแนวปฏิบัติที่เกี่ยวข้องกับข้อมูลของ สป.ดศ.

๖) กำหนดให้มีการจัดเก็บบันทึกรายละเอียดการทำลายข้อมูล และบันทึกการทำลายข้อมูลไว้ในทะเบียนควบคุม โดยให้เก็บรักษาไว้เป็นหลักฐานไม่น้อยกว่าหนึ่งปี

๗) กำหนดให้มีการทำลายข้อมูลส่วนบุคคลตามที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลหรือกฎหมายอื่นกำหนด

บทที่ ๓ กิจกรรมหลักในการดำเนินการ

๑. การจัดทำบัญชีข้อมูล (Data Catalog)

๑) กำหนดให้มีการสำรวจกระบวนการชุดข้อมูลที่เกี่ยวข้อง ทั้งนี้ หน่วยงานต้องจัดทำหรือทบทวนกระบวนการดำเนินงาน วิธีปฏิบัติ หรือบันทึกต่างๆ ที่เกี่ยวข้องให้สอดคล้องกับนโยบายข้อมูล แนวทางและมาตรการที่ สป.ดศ. กำหนด โดยคำนึงถึงหน่วยงานภายนอกที่เกี่ยวข้องด้วย

๒) กำหนดให้มีการระบุชุดข้อมูลและรายละเอียด โดยอย่างน้อยต้องมีในเรื่อง ดังต่อไปนี้

๒.๑) ความสัมพันธ์ของข้อมูล ได้แก่ หน่วยงานใดเป็นเจ้าของข้อมูล หน่วยงานใดเป็นผู้ใช้ข้อมูล

๒.๒) รูปแบบการจัดเก็บไฟล์ข้อมูล เช่น ไฟล์เอกสาร หรือแฟ้มกระดาษ

๒.๓) ความพร้อมของชุดข้อมูล เช่น ชั้นข้อมูล ความครบถ้วนถูกต้อง สมบูรณ์ พร้อมใช้ ความถี่ในการนำเข้าหรือจัดทำข้อมูล

๒.๔) ความพร้อมในการเชื่อมโยงและแลกเปลี่ยนข้อมูล เช่น เปิดให้ใช้งานสาธารณะหรือใช้งานเฉพาะภายในหน่วยงาน ชุดข้อมูลอยู่ในรูปแบบมาตรฐานพร้อมเชื่อมโยงหรือแลกเปลี่ยนหรือไม่

๒. การจำแนกข้อมูล (Data Classification)

๑) กำหนดหมวดหมู่ของข้อมูลให้เป็นไปตามธรรมาภิบาลข้อมูลภาครัฐ ได้แก่

๑.๑) ข้อมูลสาธารณะ คือ ข้อมูลที่สามารถเปิดเผยได้ สามารถนำไปใช้ได้อย่างอิสระ ไม่ว่าจะเป็นข้อมูลข่าวสาร ข้อมูลอิเล็กทรอนิกส์ เป็นต้น

๑.๒) ข้อมูลส่วนบุคคล คือ ข้อมูลเกี่ยวกับสิ่งเฉพาะตัวของบุคคล ที่ทำให้สามารถระบุตัวหรือรู้ตัวของบุคคลนั้นๆ ได้ ไม่ว่าจะเป็นข้อมูลการศึกษา ประวัติสุขภาพ ลายพิมพ์นิ้วมือ เป็นต้น

๑.๓) ข้อมูลความมั่นคง คือ ข้อมูลเกี่ยวกับความมั่นคงของรัฐที่ทำให้เกิดความสงบเรียบร้อย การมีเสถียรภาพความเป็นปึกแผ่น ปลอดภัยจากการคุกคาม เป็นต้น

๑.๔) ข้อมูลความลับทางราชการ คือ ข้อมูลที่อยู่ในความครอบครองหรือควบคุมดูแลของหน่วยงานของรัฐที่มีคำสั่งไม่ให้มีการเปิดเผย และมีการกำหนดชั้นความลับของข้อมูล

๒) กำหนดชั้นความลับของข้อมูล เพื่อป้องกันการเข้าถึงและสามารถนำข้อมูลไปใช้ได้อย่างเหมาะสม เช่น ลับที่สุด ลับมาก ลับ และเปิดเผยได้ โดยพิจารณาถึงผลกระทบ ดังต่อไปนี้

๒.๑) ด้านชื่อเสียง เช่น ข้อมูลในเชิงลบของหน่วยงานถูกเปิดเผยส่งผลให้ สป.ดศ. และประเทศเสียชื่อเสียง

๒.๒) ด้านความต่อเนื่องของการดำเนินการ เช่น ข้อมูลระบบเครือข่ายถูกเปิดเผยทำให้ระบบเครือข่ายหรือระบบอินเทอร์เน็ตถูกโจมตี ซึ่งส่งผลให้การดำเนินงานของ สป.ดศ. หยุดชะงักหรือล่าช้า

๒.๓) ด้านการเงิน เช่น ข้อมูลบัตรเครดิตของ สป.ดศ. ถูกเปิดเผย ทำให้สูญเสียงบประมาณ

๒.๔) ด้านทรัพยากรบุคคล เช่น ข้อมูลเงินเดือนถูกเปิดเผย

๓) กำหนดแนวทางมาตรการบริหารจัดการและการคุ้มครองข้อมูลให้เป็นไปตามการจำแนกข้อมูล

๔) กำหนดให้มีคำอธิบายข้อมูลหรือเมทาดาตา (Metadata) และพจนานุกรมข้อมูล (Data Dictionary) สำหรับทุกชุดข้อมูล โดยกำหนดให้การจัดทำคำอธิบายชุดข้อมูล (Metadata) เป็นไปตามมาตรฐานที่สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) หรือ สพร. กำหนด

๓. การจัดทำคำอธิบายข้อมูล (Metadata)

คำอธิบายชุดข้อมูล (Metadata) ๑๔ รายการ ตามมาตรฐานที่สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) หรือ สพร. กำหนด มีรายละเอียดดังนี้

ลำดับ	รายการ	คำอธิบาย
๑	ประเภทข้อมูล	ชุดข้อมูลนี้เป็นข้อมูลประเภทใด
๒	ชื่อชุดข้อมูล	ชื่อของชุดข้อมูลที่กำหนดโดยองค์กรที่รับผิดชอบข้อมูล
๓	องค์กร	ชื่อองค์กรที่รับผิดชอบข้อมูล
๔	ชื่อผู้ติดต่อ	ชื่อกอง สำนัก ฝ่าย หรือบุคคลที่ได้รับการมอบหมายให้รับผิดชอบข้อมูล
๕	อีเมลผู้ติดต่อ	อีเมลกอง สำนัก ฝ่าย หรือบุคคลที่ได้รับการมอบหมายให้รับผิดชอบข้อมูล
๖	คำสำคัญ	หัวข้อ คำ วลี หรือแท็ก (tag) ที่ใช้ระบุคำสำคัญในชุดข้อมูล
๗	รายละเอียด	คำอธิบายรายละเอียดที่สำคัญของชุดข้อมูลอย่างสั้น เช่น คำนิยาม ชุดข้อมูลเกี่ยวกับอะไร มีวิธีการจัดเก็บแบบใด กลุ่มเป้าหมายผู้ใช้งานข้อมูลเป็นใคร
๘	วัตถุประสงค์	อธิบายที่มาและวัตถุประสงค์ของการจัดทำชุดข้อมูล เช่น กฎหมาย ภารกิจ โครงการตามแผนยุทธศาสตร์ และเพื่อใช้ในการวิเคราะห์หรือตอบโจทย์ในประเด็นยุทธศาสตร์ในเรื่องใดที่ผู้ใช้ต้องการ
๙.๑	หน่วยความถี่ของการปรับปรุงข้อมูล	ความถี่ที่ข้อมูลในระบบคลังข้อมูลถูกปรับปรุง/เพิ่มหรือเปลี่ยนแปลง เช่น รายปี รายเดือน
๙.๒	ค่าความถี่ของการปรับปรุงข้อมูล	ตัวอย่างเช่น ถ้าชุดข้อมูลมีการปรับปรุงทุกๆ ๒ ปี ให้ใส่ “๒” สำหรับค่าความถี่ และ “รายปี” สำหรับหน่วยความถี่
๑๐	ขอบเขตเชิงภูมิศาสตร์หรือเชิงพื้นที่	มิติการจัดจำแนกข้อมูลพื้นที่ในระดับย่อยสุดที่ใช้ในการจัดเก็บข้อมูล
๑๑	แหล่งที่มา	แหล่งที่มาของข้อมูลที่นำมาจัดทำชุดข้อมูลพร้อมหน่วยงานที่จัดทำ เช่น รายงานผลการดำเนินงานของศูนย์ต่อต้านข่าวปลอม ฐานข้อมูลรายชื่อหมู่บ้านเน็ตประชารัฐ เป็นต้น

ลำดับ	รายการ	คำอธิบาย
๑๒	รูปแบบการเก็บข้อมูล	รูปแบบของการจัดเก็บข้อมูล เช่น ไฟล์ประเภท CSV XLS หรือ PDF
๑๓	หมวดหมู่ข้อมูลตามธรรมาภิบาลข้อมูลภาครัฐ	หมวดหมู่ข้อมูลตามธรรมาภิบาลข้อมูลภาครัฐ
๑๔	สัญญาอนุญาตให้ใช้ข้อมูล	สัญญาอนุญาตให้ใช้ข้อมูล ต้องสอดคล้องกับหมวดหมู่ข้อมูลตามธรรมาภิบาลข้อมูลภาครัฐ

บทที่ ๔ ติดตามและวัดผล

๑. การติดตามและวัดผล

๑) กำหนดให้มีการติดตามและวัดผลด้านธรรมาภิบาลข้อมูลภาครัฐ เช่น การดำเนินงานธรรมาภิบาลข้อมูลภาครัฐเป็นไปตามเป้าประสงค์ แผนการดำเนินงาน กระบวนการและมาตรการที่หน่วยงานกำหนดหรือไม่

๒) กำหนดให้มีวิธีการในการติดตาม วิเคราะห์ วัดผล ที่เหมาะสมและสอดคล้องตามเป้าประสงค์ของการจัดทำธรรมาภิบาลข้อมูลภาครัฐของ สป.ดศ.

๓) กำหนดให้มีการติดตาม วิเคราะห์ และวัดผล ปีละหนึ่งครั้ง

๔) กำหนดให้มีผู้รับผิดชอบในการติดตาม วัดผล วิเคราะห์ และประเมินผลสัมฤทธิ์

๒. การประเมินคุณภาพของข้อมูล (Data Quality Assessment)

กำหนดให้การประเมินคุณภาพของข้อมูล ต้องคำนึงถึงองค์ประกอบดังต่อไปนี้

๑) ความถูกต้อง (Accuracy)

๒) ความครบถ้วน (Completeness)

๓) ความสอดคล้องต้องกันกับค่าในชุดข้อมูลอื่น (Consistency)

๔) ความเป็นปัจจุบัน (Timeliness)

๕) ตรงตามความต้องการของผู้ใช้ (Relevancy)

๖) ความพร้อมใช้ (Availability)

๓. การประเมินความมั่นคงปลอดภัยของข้อมูล (Data Security Assessment)

กำหนดให้การประเมินความมั่นคงปลอดภัยของข้อมูล โดยใช้หลักเกณฑ์ดังต่อไปนี้

๑) มีการจัดชั้นความลับของข้อมูล (Data Classification)

๒) มีการกำหนดมาตรการควบคุมและป้องกันการเข้าถึงข้อมูล (Data Protection)

๓) มีการใช้งานข้อมูลอย่างเหมาะสม สอดคล้องต่อสัญญาอนุญาตและไม่ขัดต่อกฎหมาย

๔) มีความพร้อมใช้อยู่เสมอ

๔. การประเมินการรักษาความเป็นส่วนบุคคล (Data Privacy Protection Assessment)

กำหนดให้มีการประเมินการรักษาความเป็นส่วนบุคคล สอดคล้องตามที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลหรือกฎหมายอื่นกำหนด

บทที่ ๕ ตรวจสอบ ประเมิน และรายงานผล

๑. การติดตามและประเมินผล

๑) กำหนดให้มีแผนการตรวจสอบและประเมินผล วิธีการ และผู้รับผิดชอบ โดยพิจารณาถึงเป้าประสงค์ กระบวนการและผลลัพธ์ของการดำเนินงานด้านธรรมาภิบาลข้อมูลภาครัฐของ สป.ดศ.

๒) กำหนดให้มีหลักเกณฑ์และขอบเขตของการตรวจสอบและประเมินผล เป็นไปตามเป้าประสงค์ กระบวนการและผลลัพธ์ของการดำเนินงานด้านธรรมาภิบาลข้อมูลภาครัฐของ สป.ดศ.

๒. การรายงานผล

กำหนดให้มีการรายงานผลการติดตามและประเมินผลการดำเนินงานด้านธรรมาภิบาลข้อมูลภาครัฐของ สป.ดศ. และมีหลักฐานประกอบการพิจารณา โดยรายงานต้องมีหัวข้ออย่างน้อยดังนี้

๑) ผลการตรวจสอบ และประเด็นปัญหาที่พบ

๒) ความต้องการ ความคาดหวัง ผลการรับฟังความคิดเห็น และข้อร้องเรียนของผู้มีส่วนได้ส่วนเสียกับข้อมูล

๓) ผลการประเมินความเสี่ยงของข้อมูล แผนการดำเนินงาน และมาตรการด้านข้อมูลที่เกี่ยวข้อง

๔) ข้อเสนอแนะเพื่อการปรับปรุง