ประกาศกรมการจัดหางาน
เรื่อง นโยบายธรรมาภิบาลข้อมูลและการประยุกต์ใช้ปัญญาประดิษฐ์ (AI) ของกรมการจัดหางาน

ด้วยพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ กำหนดให้หน่วยงานของรัฐต้องจัดให้มีการบริหารงานภาครัฐ โดยการจัดทำการบริการสาธารณะเป็นไปด้วยความสะดวกรวดเร็ว มีประสิทธิภาพ ตอบสนองต่อการให้บริการและอำนวยความสะดวกแก่ประชาชน รวมถึงกำหนดให้หน่วยงานของรัฐจัดให้มีการบริหารจัดการ บูรณาการข้อมูลภาครัฐ เพื่อให้การทำงานมีความสอดคล้องและเชื่อมโยงข้อมูลเข้าด้วยกันอย่างมั่นคง ปลอดภัย มีธรรมาภิบาล ประกอบกับคณะกรรมการพัฒนารัฐบาลดิจิทัลออกประกาศ เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ ณ วันที่ ๑๒ มีนาคม ๒๕๖๓ โดยกำหนดให้มีธรรมาภิบาลข้อมูลภาครัฐใช้เป็นหลักการและแนวทางการดำเนินงานของหน่วยงานของรัฐ ตลอดจนในปัจจุบันเทคโนโลยีปัญญาประดิษฐ์ได้เข้ามามีบทบาทสำคัญในการยกระดับการให้บริการ กรมการจัดหางานจึงกำหนดกรอบการนำเทคโนโลยีดังกล่าวมาประยุกต์ใช้อย่างมีจริยธรรม โปร่งใส และมีมาตรฐาน ควบคู่ไปกับการบริหารจัดการข้อมูลของกรมการจัดหางาน

อาศัยอำนาจตามความในมาตรา ๑๒ แห่งพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ ประกอบข้อ ๓ และข้อ ๔ แห่งประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ ประกอบมาตรา ๓๒ แห่งพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน พ.ศ. ๒๕๓๔ และที่แก้ไขเพิ่มเติม กรมการจัดหางาน จึงประกาศนโยบายธรรมาภิบาลข้อมูล แนวปฏิบัติตามนโยบายธรรมาภิบาลข้อมูล และนโยบายการประยุกต์ใช้ปัญญาประดิษฐ์ (AI) ของกรมการจัดหางาน มีรายละเอียดตามเอกสารแนบท้ายประกาศนี้

จึงประกาศให้ทราบโดยทั่วกัน ทั้งนี้ ให้มีผลนับตั้งแต่บัดนี้เป็นต้นไป จนกว่าจะมีประกาศเปลี่ยนแปลง

ประกาศ ณ วันที่ ๑๒ พฤษภาคม พ.ศ. ๒๕๖๙

(นายสมชาย มรกตศรีวรรณ)
อธิบดีกรมการจัดหางาน

นโยบายธรรมาภิบาลข้อมูล

(Data Governance Policy)

ของกรมการจัดหางาน

๒๕๖๙ – V๑.๐

สารบัญ

๑. นโยบายธรรมาภิบาลข้อมูลของกรมการจัดหางาน

๑.๑ หลักการและเหตุผล

ตามพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ กำหนดให้หน่วยงานของรัฐจัดทำบริการสาธารณะผ่านระบบดิจิทัล เพื่ออำนวยความสะดวกและตอบสนองความต้องการของประชาชนได้อย่างรวดเร็วและมีประสิทธิภาพ โดยเน้นการบริหารจัดการและการบูรณาการข้อมูลภาครัฐให้มีความเชื่อมโยงกันอย่างมั่นคงปลอดภัยและมีธรรมาภิบาล ประกอบกับประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ ลงวันที่ ๑๒ มีนาคม ๒๕๖๓ ให้หน่วยงานของรัฐจัดให้มีธรรมาภิบาลข้อมูล เพื่อเป็นหลักการและแนวทางในการกำกับดูแลข้อมูลในระดับองค์กร ให้มีการจัดเก็บข้อมูลอย่างเป็นระบบ มีคุณภาพ ถูกต้อง และครบถ้วน เพื่อสนับสนุนการตัดสินใจเชิงนโยบายและการให้บริการประชาชนได้อย่างมีประสิทธิภาพสูงสุด

ตามที่กรมการจัดหางานมีวิสัยทัศน์ “กำลังแรงงานมีงานทำอย่างมีศักยภาพถ้วนหน้าทุกช่วงวัย ภายในปี ๒๕๗๐” โดยมีพันธกิจสำคัญในการส่งเสริมการมีงานทำ คุ้มครองคนหางาน บริหารตลาดแรงงานสู่ความสมดุล รวมถึงการบริหารจัดการการทำงานของคนต่างด้าว และการพัฒนาระบบเทคโนโลยีดิจิทัลเพื่อสนับสนุนการดำเนินงาน กรมการจัดหางานตระหนักดีว่า 'ข้อมูล (Data)' คือสินทรัพย์เชิงยุทธศาสตร์อันทรงคุณค่า (Strategic Asset) เช่น ข้อมูลคนหางาน ข้อมูลนายจ้าง/สถานประกอบการ ข้อมูลตำแหน่งงานว่าง และข้อมูลแรงงานต่างด้าวเป็นต้น เพื่อให้การบริหารจัดการข้อมูลของกรมการจัดหางานเป็นไปอย่างมีประสิทธิภาพและได้มาตรฐาน ข้อมูลมีคุณภาพ มีความมั่นคงปลอดภัย และสามารถนำไปใช้ประโยชน์ในการขับเคลื่อนภารกิจด้านการจัดหางานได้อย่างต่อเนื่อง รวมทั้งรองรับการเชื่อมโยง แลกเปลี่ยน และบูรณาการข้อมูลระหว่างหน่วยงานได้อย่างมีประสิทธิภาพ กรมการจัดหางานจึงได้กำหนดนโยบายธรรมาภิบาลข้อมูลขึ้น เพื่อเป็นกรอบมาตรฐานและแนวทางปฏิบัติในการบริหารจัดการข้อมูลอย่างเป็นระบบ ครอบคลุมทุกมิติ เพื่อการกำกับดูแลข้อมูลที่มีประสิทธิภาพ

๑.๒ วัตถุประสงค์

เพื่อกำหนดนโยบายและกรอบธรรมาภิบาลข้อมูลของกรมการจัดหางานให้สอดคล้องกับมาตรฐานรัฐบาลดิจิทัลและกฎหมายที่เกี่ยวข้อง โดยการบริหารจัดการข้อมูลให้ครอบคลุมตลอดวงจรชีวิตข้อมูล เพื่อให้ข้อมูลมีคุณภาพ มีความพร้อมใช้งาน มีความมั่นคงปลอดภัย และสามารถรองรับการเชื่อมโยงแลกเปลี่ยนข้อมูลได้อย่างมีประสิทธิภาพ ทั้งนี้นโยบายข้อมูลดังกล่าวให้มีผลบังคับใช้กับบุคลากรทุกระดับของกรมการจัดหางาน รวมถึงผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับข้อมูลของกรมการจัดหางาน เพื่อเสริมสร้างความเชื่อมั่นและเพิ่มประสิทธิภาพในการขับเคลื่อนภารกิจและการให้บริการประชาชนอย่างเป็นระบบและยั่งยืน

๑.๓ ขอบเขต

๑. การกำหนดสิทธิ หน้าที่ และความรับผิดชอบของบุคลากรทุกระดับที่มีส่วนเกี่ยวข้องกับการบริหารจัดการข้อมูล

๒. การบริหารจัดการกระบวนการทำงานแบบครบวงจร ตั้งแต่การวางแผน การดำเนินงาน การตรวจสอบและการปรับปรุงอย่างต่อเนื่อง เพื่อยกระดับระบบบริหารจัดการข้อมูลให้มีประสิทธิภาพ รองรับการเชื่อมโยงและบูรณาการข้อมูลทั้งภายในและภายนอกองค์กร ควบคู่กับการกำหนดมาตรการคุ้มครองข้อมูลให้มีความมั่นคงปลอดภัย

๓. การกำหนดมาตรการกำกับดูแลและยกระดับคุณภาพข้อมูล ให้มีความถูกต้อง ครบถ้วน ทันสมัย และมั่นคงปลอดภัย ควบคู่กับการคุ้มครองข้อมูลส่วนบุคคล เพื่อรองรับการเชื่อมโยง บูรณาการ และนำข้อมูลไปใช้ประโยชน์ได้อย่างมีประสิทธิภาพ

๔. การวัดผลการบริหารจัดการข้อมูล โดยดำเนินการประเมินความพร้อมด้านธรรมาภิบาลข้อมูลภาครัฐ การประเมินคุณภาพข้อมูล และการประเมินความมั่นคงปลอดภัยของข้อมูล

๕. การจำแนกข้อมูลและจัดหมวดหมู่ข้อมูลเพื่อกำหนดระดับสิทธิการเข้าถึงและการใช้ประโยชน์ของข้อมูลให้ชัดเจนตามกลุ่มผู้มีสิทธิในแต่ละระดับ

๖. การจัดทำคำอธิบายชุดข้อมูล (Metadata) และบัญชีข้อมูลภาครัฐ (Government Data Catalog) ให้มีความถูกต้องครบถ้วน และเป็นปัจจุบัน

๑.๔ บทนิยาม

หน่วยงานของรัฐ หมายความว่า ราชการส่วนกลาง ราชการส่วนภูมิภาค ราชการส่วนท้องถิ่น รัฐวิสาหกิจ องค์การมหาชน รัฐสภา ศาล องค์กรอิสระตามรัฐธรรมนูญ องค์กรอัยการ สถาบันอุดมศึกษาของรัฐ และหน่วยงานอิสระของรัฐ

ธรรมาภิบาลข้อมูลภาครัฐ หมายความว่า การกำหนดสิทธิ หน้าที่ และความรับผิดชอบของผู้มีส่วนได้เสียในการบริหารจัดการข้อมูลภาครัฐทุกขั้นตอน เพื่อให้การได้มาและการนำข้อมูลของหน่วยงานของรัฐไปใช้ เป็นไปอย่างถูกต้อง ข้อมูลมีความครบถ้วน เป็นปัจจุบัน มีการรักษาความเป็นส่วนบุคคล สามารถเชื่อมโยง แลกเปลี่ยน และบูรณาการข้อมูลระหว่างกันได้อย่างมีประสิทธิภาพและมั่นคงปลอดภัย เพื่อสนับสนุนการใช้ ข้อมูลเป็นหลักในการบริหารงานภาครัฐและการบริการสาธารณะ

หมวดหมู่ของข้อมูล (Data Category) หมายความว่า ตามกรอบธรรมาภิบาลข้อมูลภาครัฐแบ่งออก ได้เป็น ๕ หมวดหมู่ ได้แก่ ข้อมูลสาธารณะ ข้อมูลใช้ภายใน ข้อมูลส่วนบุคคล ข้อมูลความลับทางราชการ และ ข้อมูลความมั่นคง

ระดับชั้นข้อมูล (Data Classification Level) หมายความว่า ระดับชั้นข้อมูลเพื่อจัดการข้อมูลใน กระบวนงานที่เกี่ยวข้องกับภารกิจ โดยข้อมูลที่มีความอ่อนไหวแบ่งระดับชั้นออกเป็น ชั้นเปิดเผย (Open) ชั้นเผยแพร่ภายในองค์กร (Private) ชั้นลับ (Confidential) ชั้นลับมาก (Secret) และ ชั้นลับที่สุด (Top Secret) ซึ่งข้อมูลที่มีระดับชั้นลับ (Confidential) ลับมาก (Secret) และ ลับที่สุด (Top Secret) เป็นเพียง การจัดระดับชั้นข้อมูล ไม่ใช่การกำหนดให้ข้อมูลนั้นเป็นข้อมูลความลับทางราชการตามระเบียบการรักษา ความลับทางราชการ

ยุทธศาสตร์ด้านข้อมูล (Data Strategy) หมายความว่า แนวทาง กระบวนการ และกฎที่กำหนด วิธีการจัดการ วิเคราะห์ และดำเนินการกับข้อมูลของหน่วยงาน โดยยุทธศาสตร์ด้านข้อมูลช่วยในการตัดสินใจ เชิงนโยบายด้วยข้อมูล และช่วยคุ้มครองข้อมูลให้ปลอดภัยและเป็นไปตามข้อกำหนด ซึ่งยุทธศาสตร์ด้านข้อมูล ควรสอดคล้องกับยุทธศาสตร์และบทบาทขององค์กร (Organizational Strategy & Roles) มีสถาปัตยกรรม ข้อมูล (Data Architecture) วิสัยทัศน์การจัดการข้อมูล (Data management) ที่ชัดเจนและเหมาะสม มีตัวชี้วัดและการวัดความสำเร็จวัตถุประสงค์ของแผนงาน/โครงการทั้งในระยะสั้นและระยะยาว รวมทั้งมีการ ออกแบบและบทบาทความรับผิดชอบอย่างเหมาะสม

บัญชีข้อมูลภาครัฐ (Government Data Catalog) หมายความว่า เอกสารแสดงบรรดารายการของ ชุดข้อมูลสำคัญที่รวบรวมจากบัญชีข้อมูลของหน่วยงานภาครัฐ

ข้อมูลเปิดภาครัฐ (Open Data) หมายความว่า ข้อมูลที่หน่วยงานของรัฐต้องเปิดเผยต่อสาธารณะ ตามกฎหมายว่าด้วยข้อมูลข่าวสารของราชการในรูปแบบข้อมูลดิจิทัลที่สามารถเข้าถึงและใช้ได้อย่างเสรี ไม่ จำกัดแพลตฟอร์ม ไม่เสียค่าใช้จ่าย เผยแพร่ทำซ้ำ หรือใช้ประโยชน์ได้โดยไม่จำกัด

ข้อมูลหลัก (Master Data) หมายความว่า ข้อมูลที่ถูกสร้างขึ้นเป็นข้อมูลพื้นฐานที่มีความสำคัญต่อ การ ดำเนินงานเพื่อใช้งานร่วมกันภายในหน่วยงานเป็นหลักและขับเคลื่อนองค์กรให้บรรลุเป้าหมาย เช่น ข้อมูลพนักงาน, ข้อมูลโครงสร้างองค์กร, ข้อมูลแผนปฏิบัติการและงบประมาณประจำปี , ข้อมูลครุภัณฑ์ ทั้งนี้ หน่วยงานอาจแบ่งปันข้อมูลกับหน่วยงานอื่นตามวัตถุประสงค์ที่กำหนดขึ้น ไม่ได้จำกัดการใช้งานภายในองค์กรเท่านั้น เช่น ข้อมูลหลักของกรมการปกครองคือ เลขบัตรประชาชน ๑๓ หลัก ที่กรมสรรพากรนำมาไปใช้เป็นเลข ประจำตัวผู้เสียภาษีอากรได้

ข้อมูลอ้างอิง (Reference Data) หมายความว่า ข้อมูลที่ถูกสร้างขึ้น หรืออ้างอิงมาจากข้อมูลหลัก เพื่อกำหนดให้เป็นมาตรฐานและใช้งานร่วมกันในวงกว้าง โดยมีการระบุแหล่งที่มาที่ใช้อ้างอิงได้ชัดเจน หรือ มี หน่วยงานรับผิดชอบเป็นทางการ เช่น ข้อมูลชื่อจังหวัด ข้อมูลรหัสไปรษณีย์ ข้อมูลรหัสประเทศ

ข้อมูลแบ่งปัน (Shared data) หมายความว่า ข้อมูลอ่อนไหวที่ได้รับการจัดระดับชั้นข้อมูล ยกเว้นในระดับชั้นลับที่สุด ซึ่งสามารถแบ่งปันและแลกเปลี่ยนกันได้ระหว่างหน่วยงาน โดยจำเป็นต้องมีการกำหนดสิทธิ ในการเข้าถึงและใช้งาน รวมถึงการคุ้มครองข้อมูลให้มีความมั่นคงปลอดภัย

คำอธิบายชุดข้อมูลดิจิทัล (Metadata) หมายความว่า ข้อมูลที่ใช้อธิบายข้อมูลหลักหรือกลุ่มข้อมูลอื่น ๆ ที่เกี่ยวข้องทั้งกระบวนการเชิงธุรกิจ (ในที่นี้หมายถึง กระบวนการทำงานตามภารกิจของหน่วยงาน) และเชิงเทคโนโลยีสารสนเทศ กฎและข้อจำกัดของข้อมูล และโครงสร้างของข้อมูล เมทาดาตาช่วยให้หน่วยงานสามารถเข้าใจข้อมูล ระบบ และขั้นตอนการทำงานได้ดียิ่งขึ้น

มาตรฐานข้อมูล (Data Standards) หมายความว่า การกำหนดรูปแบบและข้อกำหนดของเมทาดาตาเพื่อให้สามารถเข้าใจได้ถูกต้องตรงกันตลอดทั้งหน่วยงาน ISO/IEC ๑๑๑๗๙ และ Dublin Core Metadata Initiative (DCMI) ได้กำหนดมาตรฐานเมทาดาตาสำหรับอธิบายชุดข้อมูล เช่น ชื่อข้อมูล ชื่อเจ้าของข้อมูล คำอธิบายข้อมูล ขอบเขตการจัดเก็บ รูปแบบข้อมูล ภาษา สิทธิการเข้าถึง ทั้งนี้มาตรฐานเมทาดาตามักจะอ้างถึงทั้งเมทาดาตาเชิงธุรกิจและเมทาดาตาเชิงเทคนิค แต่มักจะไม่รวมองค์ประกอบของฟิลด์ข้อมูลซึ่งเป็นคุณลักษณะเฉพาะของแต่ละชุดข้อมูล

เจ้าของข้อมูล (Data Owner) หมายความว่า บุคคล/คณะบุคคลที่ทำหน้าที่รับผิดชอบดูแลข้อมูลโดยตรง เพื่อสร้างความมั่นใจได้ว่าการบริหารจัดการข้อมูลสอดคล้องกับนโยบาย มาตรฐาน กฎระเบียบ หรือกฎหมาย โดยเจ้าของข้อมูลทำการทบทวนและอนุมัติการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับข้อมูล เช่น การเปลี่ยนแปลงเมทาดาตาและเกณฑ์การทำการทำข้อมูลให้ถูกต้องสมบูรณ์ (Data Cleansing) นอกจากนี้ยังมีหน้าที่ในการให้สิทธิในการเข้าถึงข้อมูลและการจัดระดับชั้นข้อมูล เจ้าของข้อมูลมักจะอยู่ในตำแหน่งบริหาร เช่น ผู้อำนวยการ ฝ่ายหรือหัวหน้าส่วนงาน

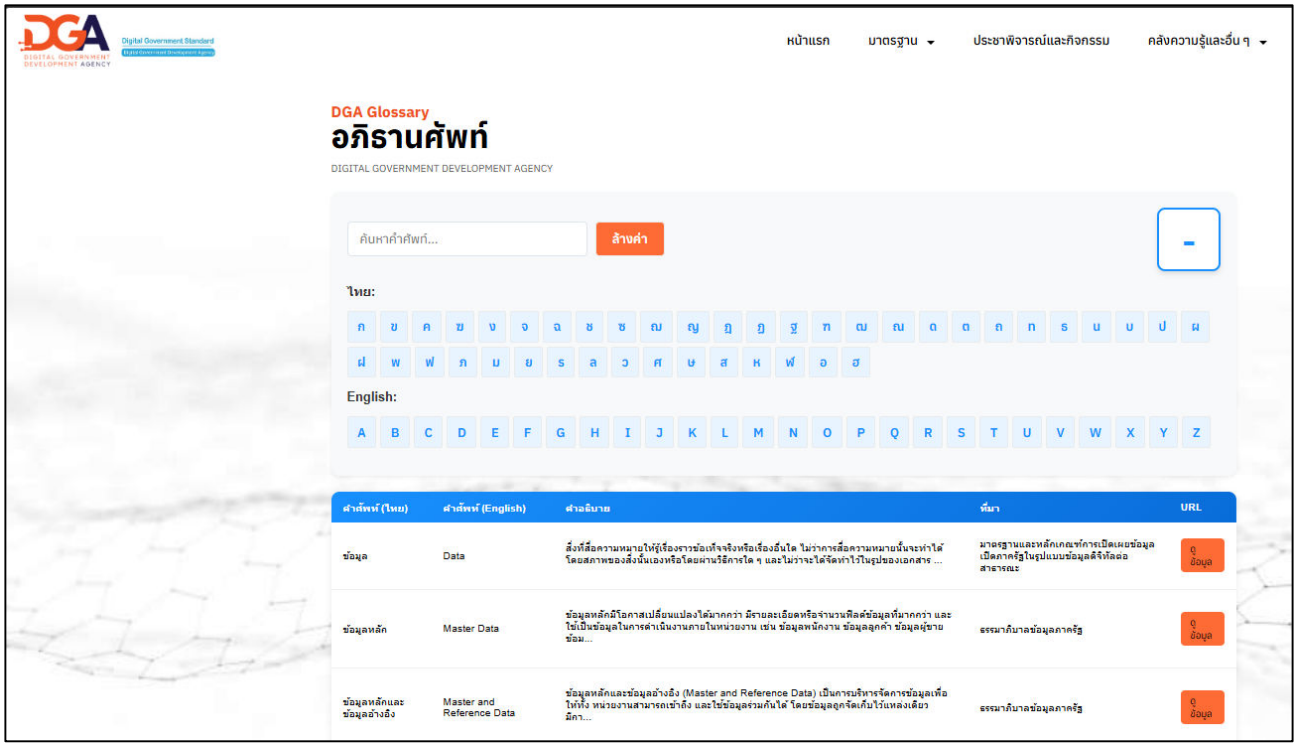
เจ้าหน้าที่ผู้รับผิดชอบดูแลข้อมูล (Data Agents) หมายความว่า บุคคลที่มีหน้าที่จัดเก็บข้อมูลให้ มั่นคงปลอดภัย รวมทั้งทบทวน หรือเสนออนุมัติการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับข้อมูล และรายงานบันทึก กิจกรรมการประมวลผลข้อมูล

เจ้าของข้อมูลส่วนบุคคล (Data Subject) หมายความว่า บุคคลธรรมดาที่ข้อมูลส่วนบุคคลเกี่ยวกับบุคคลนั้นระบุถึงได้ไม่ว่าทางตรงหรือทางอ้อม

คณะกรรมการธรรมาภิบาลข้อมูล หมายความว่า คณะกรรมการธรรมาภิบาลข้อมูลของกรมการจัดหางาน

คณะทำงานบริกรข้อมูล หมายความว่า คณะทำงานบริกรข้อมูลของกรมการจัดหางาน

รายละเอียดคำนิยามอื่นๆ ได้ที่ https://standard.dga.or.th/glossary/



รูป ๑ DGA Glossary อภิธานศัพท์ DIGITAL GOVERNMENT DEVELOPMENT AGENCY

๑.๕ กรอบธรรมาภิบาลข้อมูลของกรมการจัดหางาน

กรมการจัดหางาน ได้นำกรอบธรรมาภิบาลข้อมูลภาครัฐ (Data Governance Framework for Government) มาเป็นต้นแบบในการจัดทำกรอบธรรมาภิบาลข้อมูลของกรมการจัดหางาน เพื่อกำหนดทิศทาง นโยบาย และกลไกการบริหารจัดการข้อมูลของกรมอย่างเป็นระบบ และจัดให้มีมาตรฐานกลางในการจัดเก็บ การใช้ การแบ่งปัน และการคุ้มครองข้อมูลตลอดวงจรชีวิตข้อมูล ทั้งนี้ เพื่อสนับสนุนการนำข้อมูลไปใช้ในการกำหนดนโยบาย การวางแผน การปฏิบัติการ การติดตามตรวจสอบและประเมินผล ตลอดจนการปรับปรุงการให้บริการประชาชนอย่างมีประสิทธิภาพ

กรอบธรรมาภิบาลข้อมูลของกรมการจัดหางาน ประกอบด้วย ๓ องค์ประกอบหลัก ดังนี้

๑. โครงสร้างธรรมาภิบาลข้อมูล (Data Governance Structure)

๑) คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council) ประกอบด้วยผู้บริหารระดับสูงของหน่วยงาน ผู้บริหารจากส่วนงานต่าง ๆ ทั้งด้านภารกิจหลักและด้านเทคโนโลยีสารสนเทศ รวมถึงหัวหน้าทีมบริหารจัดการข้อมูล (Lead Data Steward) โดยมีอำนาจหน้าที่ในการกำหนดนโยบาย กรอบแนวทาง มาตรฐานข้อมูล และทิศทางการดำเนินงาน ตลอดจนกำกับดูแลการบริหารจัดการข้อมูลของกรมการจัดหางานให้มีคุณภาพ พร้อมใช้งาน มั่นคงปลอดภัย และคุ้มครองข้อมูลส่วนบุคคล ทั้งนี้ให้สอดคล้องกับภารกิจของกรมการจัดหางานและนโยบายรัฐบาลดิจิทัล

๒) คณะบริกรข้อมูล (Data Steward Team) ประกอบด้วยหัวหน้าบริกรข้อมูล (Lead Data Steward) บริกรข้อมูลด้านธุรกิจ (Business Data Stewards) บริกรข้อมูลด้านเทคนิค (Technical Data Stewards) บริกรข้อมูลด้านคุณภาพข้อมูล (Data Quality Stewards) รวมไปถึงบุคคลที่ทำหน้าที่เกี่ยวกับ ความมั่นคงปลอดภัย กฎหมาย และบุคคลที่ให้ความรู้เกี่ยวกับนโยบายข้อมูลและความรู้อื่น ๆ ที่จะสนับสนุน ให้เกิดธรรมาภิบาลข้อมูลภาครัฐที่ดีภายในหน่วยงานภาครัฐ ทีมบริกรข้อมูลรับคำสั่งโดยตรงจาก คณะกรรมการธรรมาภิบาลข้อมูล ในขณะเดียวกันมีการให้ข้อมูลสนับสนุนในการตัดสินใจต่อคณะกรรมการธรรมาภิบาลข้อมูล โดยบริกรข้อมูลด้านธุรกิจเป็นผู้ให้การสนับสนุนด้านธุรกิจ บริกรข้อมูลด้านเทคนิคเป็นผู้ให้การสนับสนุนด้านเทคโนโลยีสารสนเทศ และบริกรข้อมูลด้านคุณภาพข้อมูลเป็นผู้ให้การสนับสนุนด้านคุณภาพข้อมูล

๓) ผู้มีส่วนได้ส่วนเสียกับข้อมูล (Data Stakeholders) คือผู้ที่มีส่วนเกี่ยวข้องกับข้อมูล โดยได้รับผลกระทบทางตรงหรือทางอ้อมจากการใช้บริการข้อมูล ซึ่งทำหน้าที่ให้การสนับสนุนธรรมาภิบาลข้อมูลภาครัฐต่อทีมบริกรข้อมูลและคณะกรรมการธรรมาภิบาลข้อมูล ประกอบไปด้วย เจ้าของข้อมูล (Data Owners) ทีมบริหารจัดการข้อมูล (Data Management Team) ผู้สร้างข้อมูล (Data Creators) และผู้ใช้ข้อมูล (Data Users)

๒. กระบวนการธรรมาภิบาลข้อมูลภาครัฐ (Data Governance Processes)

กระบวนการธรรมาภิบาลข้อมูลภาครัฐ คือการกำกับดูแลและจัดการข้อมูลตลอดวงจรชีวิต ตั้งแต่การสร้าง การจัดเก็บ ไปจนถึงการทำลายข้อมูล โดยมีองค์ประกอบสำคัญเริ่มจากการเลือกข้อมูลเป้าหมายและการกำหนดมาตรฐานที่ครอบคลุมทั้งด้านคุณภาพ ความปลอดภัย และการปฏิบัติตามกฎหมาย พร้อมทั้งการบริหารจัดการบุคลากรเพื่อสร้างวัฒนธรรมองค์กรที่เหมาะสม ซึ่งการดำเนินงานจะขับเคลื่อนผ่านวงจรการพัฒนาอย่างต่อเนื่อง ๔ ขั้นตอน ได้แก่ การวางแผนเพื่อกำหนดนโยบายและขอบเขตงาน การลงมือปฏิบัติโดยบุคลากรทุกระดับตามมาตรฐานที่วางไว้ การตรวจสอบและวัดผลคุณภาพข้อมูลเพื่อรายงานประเด็นปัญหา และการนำผลลัพธ์มาปรับปรุงกระบวนการให้สอดคล้องกับกฎระเบียบหรือสภาพแวดล้อมที่เปลี่ยนแปลงไป เพื่อให้การบริหารจัดการข้อมูลภาครัฐมีความโปร่งใส มั่นคงปลอดภัย และมีประสิทธิภาพสูงสุดอย่างยั่งยืน

๓. นิยามและกฎเกณฑ์ที่เกี่ยวข้องกับข้อมูล (Definition and Rules)

ในองค์ประกอบนี้จะการกำหนดมาตรฐานและระเบียบปฏิบัติ เพื่อยกระดับคุณภาพข้อมูลอย่างเป็นรูปธรรม โดยมีเป้าหมายเชิงยุทธศาสตร์ให้ข้อมูลมีคุณลักษณะครบถ้วนสมบูรณ์ในทุกมิติ ได้แก่ ความถูกต้อง (Accuracy) ความครบถ้วน (Completeness) และความเป็นปัจจุบัน (Timeliness) ควบคู่ไปกับการดำรงความมั่นคงปลอดภัย (Security) การคุ้มครองความเป็นส่วนบุคคล (Privacy) ตลอดจนความสามารถในการเชื่อมโยงแลกเปลี่ยน (Interoperability) เพื่อให้ข้อมูลดังกล่าวสามารถนำไปใช้ประโยชน์ได้อย่างแท้จริง (Usability)

เพื่อให้บรรลุเป้าหมายดังกล่าว จำเป็นต้องมีการบูรณาการองค์ประกอบสำคัญ ๓ ระดับ ได้แก่ สภาพแวดล้อมของธรรมาภิบาลข้อมูล ซึ่งเน้นการเตรียมความพร้อมด้านโครงสร้างพื้นฐานและวัฒนธรรมองค์กร นิยามข้อมูล ซึ่งเป็นการสร้างมาตรฐานความเข้าใจเชิงความหมาย (Semantics) และการจัดทำเมทาดาตา (Metadata) เพื่อลดความกำกวมในการสื่อสาร และกฎเกณฑ์หรือนโยบายข้อมูลที่เป็นข้อกำหนดลายลักษณ์อักษรในการกำกับดูแลสิทธิการเข้าถึงและวงจรชีวิตของข้อมูล เพื่อให้การบริหารจัดการข้อมูลเป็นไปอย่างมีประสิทธิภาพและตรวจสอบได้

รูป ๒ กรอบธรรมาภิบาลข้อมูลกรมการจัดหางาน

จากกรอบธรรมาภิบาลข้อมูลกรมการจัดหางาน ที่ได้มีการกำหนดโครงสร้างธรรมาภิบาลข้อมูล กระบวนการธรรมาภิบาลข้อมูลภาครัฐ และนิยามและกฎเกณฑ์ที่เกี่ยวข้องกับข้อมูล เพื่อให้มีความชัดเจนในการดำเนินการตามกรอบธรรมาภิบาลข้อมูลกรมการจัดหางาน และเพื่อให้สอดคล้องกับประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ กรมการจัดหางานได้มีการกำหนดเนื้อหารายละเอียดแบ่งออกเป็น ๖ เรื่อง ดังนี้

๑) การกำหนดสิทธิ บทบาทหน้าที่ และความรับผิดชอบของผู้ซึ่งมีหน้าที่เกี่ยวข้องกับการบริหารจัดการข้อมูลของหน่วยงาน (Roles and Responsibilities)

๒) การกำหนดกระบวนการธรรมาภิบาลข้อมูล (Data Governance Processes)

๓) การกำหนดมาตรการกำกับดูแล การควบคุม และยกระดับคุณภาพข้อมูล (Data quality control and improvement)

๔) การวัดผลการบริหารจัดการข้อมูล (Data management measurement)

๕) การจำแนกข้อมูลและหมวดหมู่ของข้อมูล (Data and Data Categories)

๖) คำอธิบายชุดข้อมูลดิจิทัล หรือเมทาดาตา (Metadata)

๒. การกำหนดสิทธิ บทบาทหน้าที่ และความรับผิดชอบของผู้ซึ่งมีหน้าที่เกี่ยวข้องกับการบริหารจัดการข้อมูลของหน่วยงาน (Roles and Responsibilities)

สิทธิ บทบาทหน้าที่ และความรับผิดชอบ คือ การจัดทำโครงสร้างธรรมาภิบาลข้อมูลภาครัฐ เพื่อระบุตัวบุคคลหรือกลุ่มบุคคลที่มีอำนาจตัดสินใจ มีหน้าที่ปฏิบัติ และมีความรับผิดชอบต่อข้อมูลในทุกวงจรชีวิต ตั้งแต่การจัดเก็บ การประมวลผล การทำลาย ไปจนถึงการเปิดเผยข้อมูล เพื่อให้ข้อมูลของกรมการจัดหางานมี ความถูกต้อง ความพร้อมใช้ ความเป็นปัจจุบัน และ มีความมั่นคงปลอดภัย เป็นไปตามมาตรฐานและกฎหมายที่เกี่ยวข้อง

๒.๑ โครงสร้างของบุคลากรที่รับผิดชอบในธรรมาภิบาลข้อมูลภาครัฐ (Data Governance Structure)

โครงสร้างธรรมาภิบาลข้อมูลภาครัฐ เพื่อแสดงลำดับขั้นระหว่างกลุ่มบุคคลที่เกี่ยวข้องกับธรรมาภิบาลข้อมูลภาครัฐ และแสดงถึงสิทธิ์ในการสั่งการตามลำดับขั้น ทั้งนี้กรมการจัดหางานได้กำหนดโครงสร้างของบุคลากรที่รับผิดชอบในธรรมาภิบาลข้อมูลภาครัฐ ดังนี้

๑) **คณะกรรมการธรรมาภิบาลข้อมูลของกรมการจัดหางาน** (DOE Data Governance Council) ประกอบด้วย ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม (Department Chief Information Officer : DCIO) เป็นประธานกรรมการ หัวหน้าผู้ตรวจราชการกรมเป็นรองประธานกรรมการ ผู้บริหารหน่วยงานระดับกองหรือเทียบเท่ากองเป็นกรรมการ หัวหน้าคณะทำงานบริกรข้อมูล (Lead Data Steward) เป็นกรรมการและเลขานุการ หัวหน้ากลุ่มงานที่ได้รับแต่งตั้งเป็นกรรมการและผู้ช่วยเลขานุการ

๒) **คณะทำงานบริกรข้อมูลของกรมการจัดหางาน** (DOE Data Steward Team) ประกอบด้วยหัวหน้าบริกรข้อมูล (Lead Data Steward) บริกรข้อมูลด้านธุรกิจ (Business Data Stewards) บริกรข้อมูลด้านเทคนิค (Technical Data Stewards) บริกรข้อมูลด้านคุณภาพข้อมูล (Data Quality Stewards) รวมไปถึงบุคคลที่ทำหน้าที่เกี่ยวกับความมั่นคงปลอดภัย กฎหมาย และบุคคลที่ให้ความรู้เกี่ยวกับนโยบายข้อมูลและความรู้อื่น ๆ ที่จะสนับสนุนให้เกิดธรรมาภิบาลข้อมูลภาครัฐที่ดี

๓) **ผู้มีส่วนได้เสียกับข้อมูล** (Data Stakeholders) ประกอบไปด้วย เจ้าของข้อมูล (Data Owners) ทีมบริหารจัดการข้อมูล (Data Management Team) ผู้สร้างข้อมูล (Data Creators) และผู้ใช้ข้อมูล (Data Users)

๒.๒ บทบาทและความรับผิดชอบ (Roles and Responsibilities)

บทบาท (Roles) และความรับผิดชอบ (Responsibilities) ที่เหมาะสมจะนำไปสู่การดำเนินงานที่มี ประสิทธิภาพและประสิทธิผลต่อหน่วยงาน ซึ่งบทบาทและความรับผิดชอบจะต้องไม่ขัดแย้งต่อกฎ ระเบียบ ข้อบังคับ หรือกฎหมาย รวมทั้งสิทธิ หน้าที่ และความรับผิดชอบในการบริหารจัดการข้อมูลที่อยู่ในความครอบครองหรือควบคุม ให้มีความชัดเจน โดยแต่งตั้งหรือมอบหมายเจ้าหน้าที่เป็นรายบุคคล หรือคณะบุคคลให้รับผิดชอบ และประกาศให้ผู้ที่เกี่ยวข้องหรือประชาชนรับทราบด้วยเป็นไปตามที่กำหนดไว้ ตามกฎหมายว่าด้วยการนั้น มีรายละเอียดดังนี้

๑) คณะกรรมการธรรมาภิบาลข้อมูลของกรมการจัดหางาน (Data Governance Council)

คือ คณะกรรมการที่กรมการจัดหางานแต่งตั้งขึ้นเพื่อทำหน้าที่กำหนดทิศทาง นโยบาย มาตรฐาน และกลไกการกำกับดูแลด้านข้อมูลของหน่วยงาน ให้เป็นไปอย่างเป็นระบบ มีความถูกต้อง ครบถ้วน เป็นปัจจุบัน ปลอดภัย และสอดคล้องกับกฎหมายและหลักธรรมาภิบาลข้อมูลภาครัฐ โดยมีบทบาทในการกำกับ ติดตาม และประเมินผลการบริหารจัดการข้อมูลของกรม เพื่อสนับสนุนการตัดสินใจเชิงนโยบาย การให้บริการประชาชน และการบูรณาการแลกเปลี่ยนข้อมูลระหว่างหน่วยงานอย่างมีประสิทธิภาพและโปร่งใส

มีอำนาจหน้าที่ ดังนี้

(๑) กำหนดนโยบายและมาตรฐานข้อมูล ทิศทางการจัดทำ และพิจารณาอนุมัตินโยบายธรรมาภิบาลข้อมูล มาตรฐานข้อมูล เกณฑ์คุณภาพข้อมูล และแนวปฏิบัติที่เกี่ยวข้อง ให้สอดคล้องกับภารกิจของกรมการจัดหางาน เพื่อให้การบริหารจัดการข้อมูลเป็นระบบ มั่นคงปลอดภัย และคุ้มครองข้อมูลส่วนบุคคล

(๒) ส่งเสริมการบูรณาการและการใช้ประโยชน์ข้อมูล ผลักดันการเชื่อมโยง แลกเปลี่ยน และบูรณาการข้อมูลทั้งภายในและภายนอกหน่วยงาน รวมถึงสนับสนุนการนำเทคโนโลยีและนวัตกรรมด้านข้อมูล มาการวิเคราะห์ข้อมูล การวิเคราะห์ตลาดแรงงานและยกระดับการให้บริการประชาชน

(๓) กำกับดูแลโครงสร้างและการดำเนินงานด้านข้อมูล แต่งตั้งคณะบริกรข้อมูล (Data Steward) หรือคณะทำงานที่เกี่ยวข้อง กำหนดบทบาทหน้าที่ให้ชัดเจน พร้อมกำกับ ติดตาม และประเมินผลการดำเนินงานให้เป็นไปตามนโยบายและมาตรฐานที่กำหนด

๒) คณะทำงานบริกรข้อมูลของกรมการจัดหางาน (Data Steward Team)

คือ คณะทำงานที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ด้านการกำกับดูแล บริหารจัดการ และควบคุมคุณภาพข้อมูลของกรมการจัดหางาน เพื่อให้การจัดการข้อมูลเป็นไปตามนโยบาย มาตรฐาน และกรอบธรรมาภิบาลข้อมูลของหน่วยงาน ตลอดจนสนับสนุนการใช้ประโยชน์ข้อมูลอย่างมีประสิทธิภาพ โปร่งใส และมั่นคงปลอดภัย

ประกอบด้วยบุคคลที่มีบทบาทหน้าที่ ดังนี้

(๒.๑) หัวหน้าคณะบริกรข้อมูล คือ บุคคลที่ทำหน้าที่รับผิดชอบในการกำกับดูแล และสนับสนุนอำนวยการการดำเนินงานของคณะทำงานบริกรข้อมูล ให้เป็นไปตามนโยบายและกรอบธรรมาภิบาลข้อมูลของกรมการจัดหางาน กำหนดแนวทางการปฏิบัติงาน ติดตามผลการดำเนินงาน และรายงานผลการบริหารจัดการข้อมูลในภาพรวมของหน่วยงาน

(๒.๒) บริกรข้อมูลด้านธุรกิจ (Business Data Stewards) คือ บุคคลที่ทำหน้าที่รับผิดชอบในการนิยามความต้องการด้านคุณภาพและความมั่นคงปลอดภัยซึ่งอาจจะได้รับมาจากผู้ใช้ข้อมูล (Data Users) หรือผู้มีส่วนได้เสียอื่น ๆ นิยามคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตาโดยการสนับสนุนจากผู้ใช้ข้อมูล สถาปนิก ข้อมูล (Data Architects) และนักวิเคราะห์ระบบ (System Analyst) ร่างนโยบายข้อมูลด้วยการช่วยเหลือ จากทีมบริหารจัดการข้อมูล (Data Management Team) ตรวจสอบการปฏิบัติตามนโยบายข้อมูล ตรวจสอบ คุณภาพ ตรวจสอบความมั่นคงปลอดภัยของข้อมูล วิเคราะห์ผลจากการตรวจสอบ แล้วรายงานผลลัพธ์ไปยังคณะกรรมการธรรมาภิบาลข้อมูลและผู้ที่เกี่ยวข้องอื่น ๆ ทั้งนี้ บริกรข้อมูลด้านธุรกิจจะต้องเป็นบุคคลที่มาจากหน่วยงานระดับกองที่เกี่ยวข้องกับภารกิจหลักของกรมการจัดหางาน และต้องมีอำนาจตัดสินใจโดยจะเป็นผู้อำนวยการหรือหัวหน้ากลุ่มงานที่ได้รับมอบหมาย

(๒.๓) บริกรข้อมูลด้านเทคนิค (Technical Data Stewards) คือ บุคคลที่ทำหน้าที่ให้การสนับสนุนด้านเทคโนโลยีสารสนเทศแก่บริกรข้อมูลด้านธุรกิจ เช่น นิยามเมทาดาตาเชิงเทคนิคซึ่งอาจจะได้รับการช่วยเหลือ จากทีมบริหารจัดการข้อมูล ให้ข้อเสนอแนะเชิงเทคนิคในการร่างนโยบายข้อมูล ตรวจสอบคุณภาพข้อมูล ความมั่นคงปลอดภัยของข้อมูล และการปฏิบัติตามนโยบายข้อมูลในเชิงเทคนิค ทั้งนี้บริกรข้อมูลด้านเทคนิค ส่วนใหญ่เป็นบุคคลฝ่ายเทคโนโลยีสารสนเทศแต่มีความเข้าใจเกี่ยวกับธุรกิจ

(๒.๔) บริกรข้อมูลด้านคุณภาพข้อมูล (Data Quality Stewards) คือ บุคคลที่ทำหน้าที่ดำเนินการในเรื่องคุณภาพข้อมูล เช่น กำหนดนโยบายข้อมูลด้านคุณภาพ การตรวจวัดคุณภาพข้อมูล และการวิเคราะห์ คุณภาพข้อมูล นอกจากนี้หน่วยงานอาจจะกำหนดบริกรข้อมูลด้านอื่น ๆ เพื่อดูแลเรื่องต่าง ๆ โดยเฉพาะ เช่น บริกรข้อมูลด้านความมั่นคงปลอดภัย บริการข้อมูลด้านการอบรมและให้ความรู้

๓) ผู้มีส่วนได้เสียกับข้อมูล (Data Stakeholders)

คือ บุคคลหรือหน่วยงานที่มีส่วนเกี่ยวข้องหรือได้รับผลกระทบ ทั้งทางตรงและทางอ้อมจากการบริหารจัดการและการใช้ประโยชน์ข้อมูลภายใต้กรอบธรรมาภิบาลข้อมูลภาครัฐ โดยมีหน้าที่สนับสนุนการกำกับดูแลข้อมูลให้เป็นไปตามนโยบายของคณะกรรมการธรรมาภิบาลข้อมูล เพื่อให้หน่วยงานสามารถดำเนินการธรรมาภิบาลข้อมูลและบริหารจัดการข้อมูลได้อย่างมี ประสิทธิภาพ และสร้างประโยชน์สูงสุด จึงมีการกำหนดบทบาทและความรับผิดชอบของผู้มีส่วนได้ส่วนเสีย กับข้อมูลในแต่ละด้าน ดังนี้

๓.๑) ด้านการบริหารจัดการข้อมูล

(๓.๑.๑) ผู้บริหารจัดการข้อมูลเชิงธุรกิจ / ภารกิจงาน ประกอบด้วย บุคลากรจากหน่วยงานระดับกองที่รับผิดชอบภารกิจหลักของกรมการจัดหางาน มีหน้าที่วิเคราะห์และประมวลผลข้อมูลด้านแรงงานเพื่อสนับสนุนการกำหนดนโยบาย การวางแผน และการตัดสินใจเชิงยุทธศาสตร์ โดยมุ่งเน้นการวิเคราะห์แนวโน้มตลาดแรงงาน สถานการณ์การมีงานทำ การเคลื่อนย้ายแรงงาน การบริหารจัดการแรงงานต่างด้าว และการให้บริการจัดหางานทั้งในและต่างประเทศ

รวมถึงเฝ้าระวังความผิดปกติหรือความเสี่ยงที่อาจกระทบต่อภารกิจของหน่วยงาน โดยใช้หลักสถิติและเครื่องมือวิเคราะห์ข้อมูลที่มีประสิทธิภาพ

(๓.๑.๒) ผู้บริหารจัดการข้อมูลเชิงเทคนิค ประกอบด้วย บุคลากรสังกัดศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือบุคลากรจากหน่วยงานภายในกรมที่มีความเชี่ยวชาญด้านเทคโนโลยีสารสนเทศ หรือบุคลากรภายนอกที่เป็นคู่สัญญากับกรมการจัดหางาน ทำหน้าที่รับผิดชอบในงานเทคโนโลยีสารสนเทศของหน่วยงาน ตรวจสอบการปฏิบัติตามนโยบายข้อมูล ทีมบริหารจัดการข้อมูลสนับสนุนกิจกรรมของธรรมาภิบาลข้อมูลภาครัฐ

๓.๒) ด้านธรรมาภิบาลข้อมูล

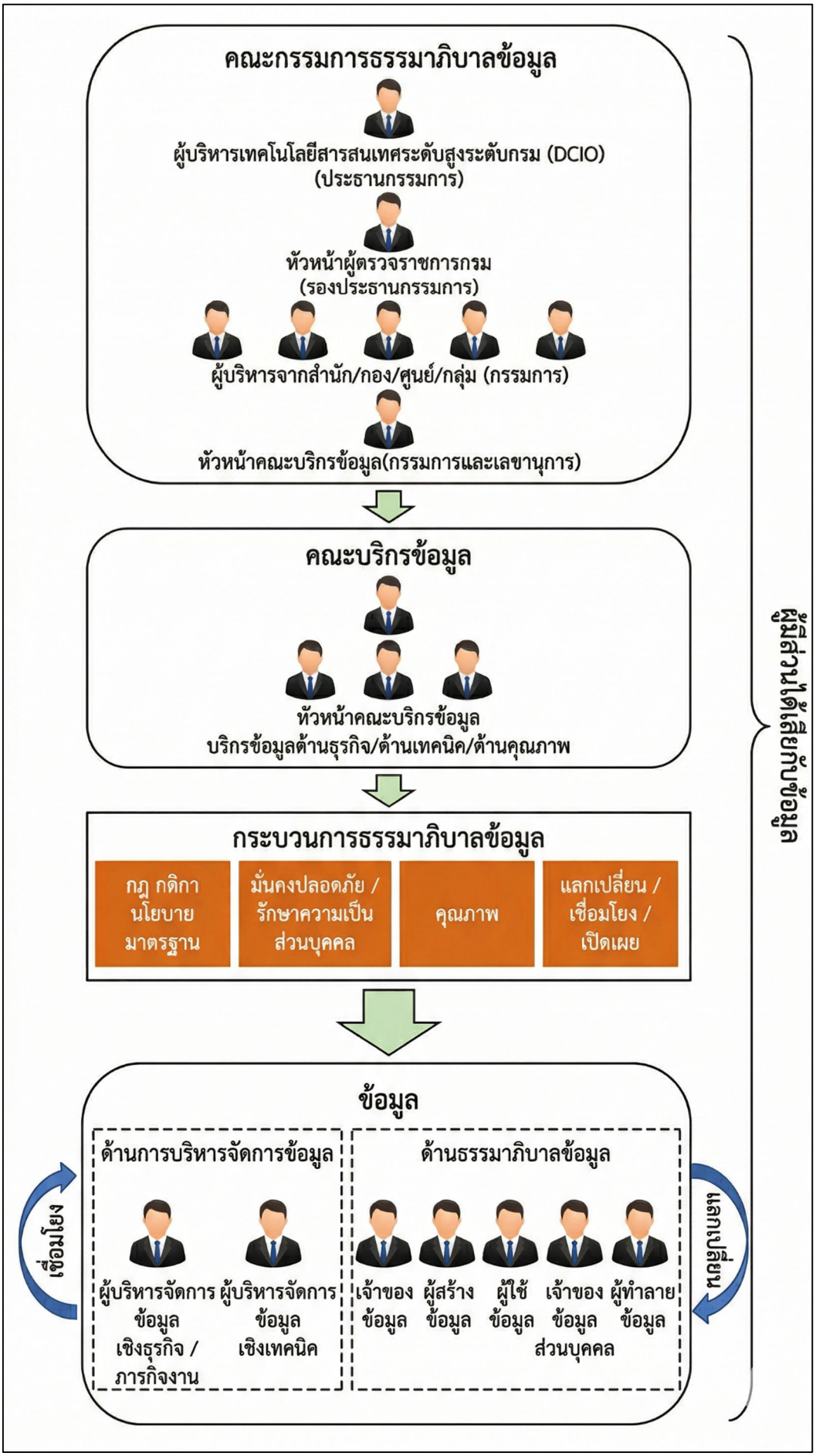
(๓.๒.๑) เจ้าของข้อมูล (Data Owners) คือ อธิบดีหรือหน่วยงานในสังกัดกรมการจัดหางาน เช่น ผู้อำนวยการกอง หรือหัวหน้ากลุ่มงานที่ได้รับการมอบหมายให้ดูแลข้อมูลของหน่วยงาน ที่ทำหน้าที่รับผิดชอบดูแลข้อมูลโดยตรง สร้างความมั่นใจได้ว่าการบริหารจัดการข้อมูลสอดคล้องกับนโยบาย มาตรฐาน กฎระเบียบ หรือกฎหมาย เจ้าของข้อมูลทำการทบทวนและอนุมัติการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับข้อมูล เช่น การเปลี่ยนแปลงเมทาดาตาและเกณฑ์การทำข้อมูลให้ถูกต้องสมบูรณ์ (Data Cleansing) นอกจากนี้ยังมีหน้าที่ในการให้สิทธิในการเข้าถึงข้อมูลและการจัดระดับชั้นข้อมูล

(๓.๒.๒) ผู้สร้างข้อมูล (Data Creators) คือ บุคคลที่ทำหน้าที่ บันทึก แก้ไข ปรับปรุง หรือลบข้อมูลให้ สอดคล้องกับโครงสร้างที่ถูกกำหนดไว้ นอกจากนี้ยังมีหน้าที่ในการทำงานร่วมกับบริกรข้อมูล เพื่อตรวจสอบ และแก้ไขปัญหาด้านคุณภาพข้อมูลและความมั่นคงปลอดภัย

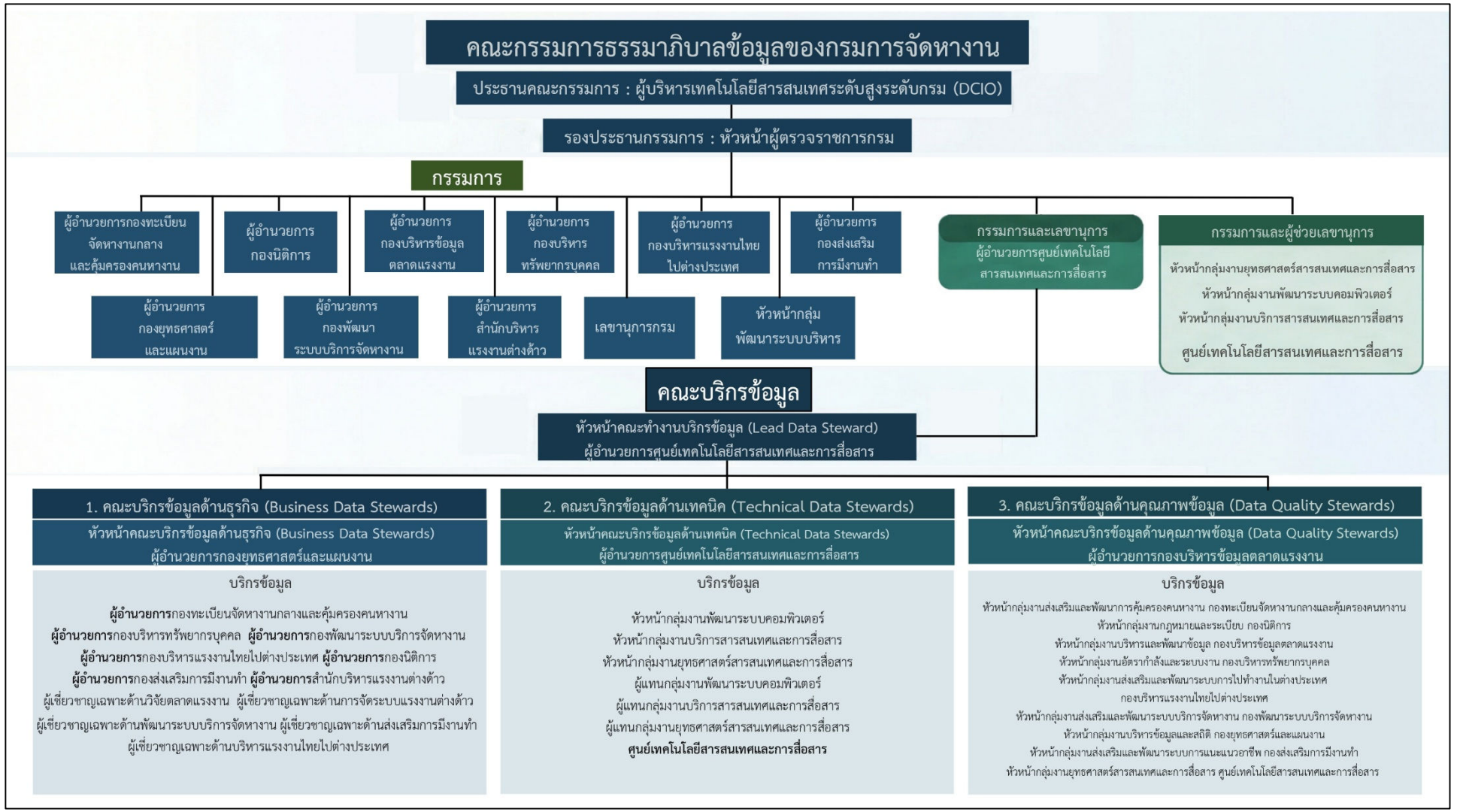
(๓.๒.๓) ผู้ใช้ข้อมูล (Data Users) คือ บุคคลที่ทำหน้าที่นำข้อมูลไปใช้งานทั้งในระดับปฏิบัติงานและระดับ บริหาร และสนับสนุนธรรมาภิบาลข้อมูลภาครัฐโดยการให้ความต้องการในการใช้ข้อมูล พร้อมทั้งรายงานประเด็นปัญหาที่พบระหว่างการใช้ข้อมูล ทั้งด้านคุณภาพและความปลอดภัยของข้อมูลไปยังบริกรข้อมูล

(๓.๒.๔) เจ้าของข้อมูลส่วนบุคคล (Data Subject) คือ บุคคลธรรมดาซึ่งข้อมูลส่วนบุคคลนั้นสามารถระบุตัวตนของบุคคลดังกล่าวได้ ไม่ว่าโดยทางตรงหรือทางอ้อม ทั้งนี้รวมถึงข้อมูลที่เมื่อประกอบกับข้อมูลอื่นแล้วสามารถใช้ในการระบุตัวบุคคลได้ด้วย

(๓.๒.๕) ผู้ทำลายข้อมูล (Data Destroyers) คือ บุคลากรที่ได้รับการกำหนดสิทธิจากเจ้าของข้อมูลให้มีสิทธิในการทำลายข้อมูล



รูปที่ ๓ โครงสร้างธรรมาภิบาลข้อมูลของกรมการจัดหางาน



รูปที่ ๔ โครงสร้างธรรมาภิบาลข้อมูลตามตำแหน่งงาน

๓. การกำหนดกระบวนการธรรมาภิบาลข้อมูล (Data Governance Processes)

เพื่อให้การบริหารจัดการข้อมูลของกรมการจัดหางานมีประสิทธิภาพ มั่นคงปลอดภัย และสอดคล้องกับมาตรฐานภาครัฐ กรมการจัดหางาน จึงกำหนดหลักพื้นฐานของกระบวนการและผลลัพธ์ที่จะเกิดขึ้นตาม วงจรชีวิตของข้อมูล (Data Lifecycle) ตั้งแต่การสร้าง การจัดเก็บ (รวมถึงการเก็บถาวร) การประมวลผล และการใช้ การเปิดเผย การทำลาย ไปจนถึงการเชื่อมโยงและการแลกเปลี่ยนข้อมูล โดยมีองค์ประกอบสำคัญ ๔ ประการ ดังนี้

๑) การจำแนกและเลือกข้อมูลเพื่อการกำกับดูแล (Data Selection) การเลือกข้อมูลเพื่อดำเนินการธรรมาภิบาล ได้แก่ ข้อมูลสาธารณะ ข้อมูลใช้ภายใน ข้อมูลส่วน บุคคล ข้อมูลความลับทางราชการ และข้อมูลความมั่นคง โดยกระบวนการซึ่งได้มาด้วยข้อมูลนั้นสามารถใช้ วิธีการ เช่น กระบวนการวิศวกรรมย้อนกลับ (Reverse Engineering) การวิเคราะห์ข้อมูล (Data Analysis) การสำรวจข้อมูล (Survey)

๒) การกำหนดเป้าหมาย (Goal Setting) เป็นการระบุเป้าหมาย ต้องพิจารณาครอบคลุมในประเด็นดังต่อไปนี้ เป็นอย่างน้อย คือ คุณภาพ ข้อมูล การเข้าถึงและการจัดการ ความปลอดภัยและความเป็นส่วนบุคคล การปฏิบัติตามระเบียบและกฎหมาย ต้นทุนและประสิทธิภาพ

๓) การกำหนดมาตรฐานและแนวปฏิบัติ (Standards and Guidelines) เป็นการกำหนดมาตรฐานทั่วไป เพื่อใช้เป็นแนวปฏิบัติร่วมกัน เช่น มาตรฐานการตั้งชื่อชุดข้อมูล มาตรฐานคุณภาพข้อมูล การโอนย้ายข้อมูล การจัดการกระบวนการ CRUD (Create, Read, Update, Delete) และหลักเกณฑ์การจัดเก็บข้อมูลถาวร (Archive)

๔) การบริหารจัดการบุคลากรและการกำกับดูแล (People Management) เป็นการมุ่งเน้นการสร้างวัฒนธรรมองค์กรให้เห็นความสำคัญของข้อมูล การสื่อสารที่ชัดเจนเพื่อลดแรงต้านในการเปลี่ยนแปลง การสร้างความพึงพอใจแก่ผู้มีส่วนได้เสีย และการนำเทคโนโลยีมาสนับสนุนการทำงาน ตลอดจนการกำกับดูแลให้บุคลากรปฏิบัติตามกฎระเบียบด้านความปลอดภัยอย่างเคร่งครัด

๓.๑ กระบวนการธรรมาภิบาลข้อมูลภาครัฐ (Data Governance Processes)

เพื่อให้การกำกับดูแลข้อมูลของกรมการจัดหางานเป็นไปตามนโยบาย ระเบียบ และหลักเกณฑ์ที่เกี่ยวข้องอย่างเป็นระบบและต่อเนื่อง กรมการจัดหางานจึงนำหลักการบริหารงานเชิงคุณภาพตามวงจร PDCA (Plan–Do–Check–Act) มาประยุกต์ใช้ในการดำเนินงาน ดังนี้

๑) การวางแผน (Plan)

กรมการจัดหางานจะดำเนินการวางแผน โดยเริ่มต้นจากวิสัยทัศน์และการวิเคราะห์ประเด็นปัญหาที่เกี่ยวข้อง ซึ่งถือเป็นขั้นตอนสำคัญ เนื่องจากเป็นพื้นฐานในการกำหนดกฎ ระเบียบ นโยบาย มาตรฐานข้อมูล หรือแนวทางปฏิบัติต่าง ๆ ที่ใช้สนับสนุนการดำเนินงานด้านธรรมาภิบาลข้อมูลและการบริหารจัดการข้อมูลของหน่วยงาน เมื่อได้กำหนดประเด็นปัญหาอย่างชัดเจนแล้ว ขั้นตอนต่อไปคือการกำหนดขอบเขตการดำเนินงาน ระยะเวลาดำเนินการ ผู้รับผิดชอบหรือผู้มีส่วนเกี่ยวข้อง ตลอดจนทรัพยากรและงบประมาณที่จำเป็นสำหรับการดำเนินงาน จากนั้นจึงนำแผนงาน กฎ ระเบียบ และนโยบายที่เกี่ยวข้องไปประกาศใช้และสื่อสารให้หน่วยงานที่เกี่ยวข้องนำไปปฏิบัติอย่างเป็นทางการ เพื่อให้การดำเนินงานเป็นไปในทิศทางเดียวกันและบรรลุวัตถุประสงค์ที่กำหนดไว้

ขั้นตอนการวางแผนด้านธรรมาภิบาลข้อมูล

กรมการจัดหางานจัดประชุมคณะทำงานบริกรข้อมูล เพื่อจัดทำและเสนอแผนการดำเนินงานด้านธรรมาภิบาลข้อมูลประจำปีต่อคณะกรรมการธรรมาภิบาลข้อมูลเพื่อพิจารณา โดยให้ดำเนินการจัดประชุมภายในไตรมาสที่ ๑ ของทุกปี และดำเนินการจัดทำรายงานการประชุมเป็นลายลักษณ์อักษร ทั้งนี้ วาระการประชุมอย่างน้อยต้องครอบคลุมประเด็นดังต่อไปนี้ ดังนี้

๑. การทบทวนองค์ประกอบและรายชื่อคณะกรรมการธรรมาภิบาลข้อมูลและคณะทำงานบริกรข้อมูล ให้มีความเหมาะสมและสอดคล้องกับภารกิจด้านการกำกับดูแลข้อมูล

๒. การทบทวนนโยบาย ระเบียบ มาตรฐาน แนวปฏิบัติ และกฎหมายที่เกี่ยวข้องกับการกำกับดูแลข้อมูล

๓. การรายงานความเสี่ยง ปัญหา และอุปสรรคที่เกี่ยวข้อง

๔. การพิจารณาความต้องการด้านทรัพยากร ทักษะ ความรู้ และขีดความสามารถที่จำเป็นต่อการดำเนินงาน

๕. การรายงานผลการประเมินคุณภาพข้อมูล

๖. การปรับปรุงธรรมาภิบาลข้อมูลของกรมการจัดหางาน

๒) การปฏิบัติ (Do)

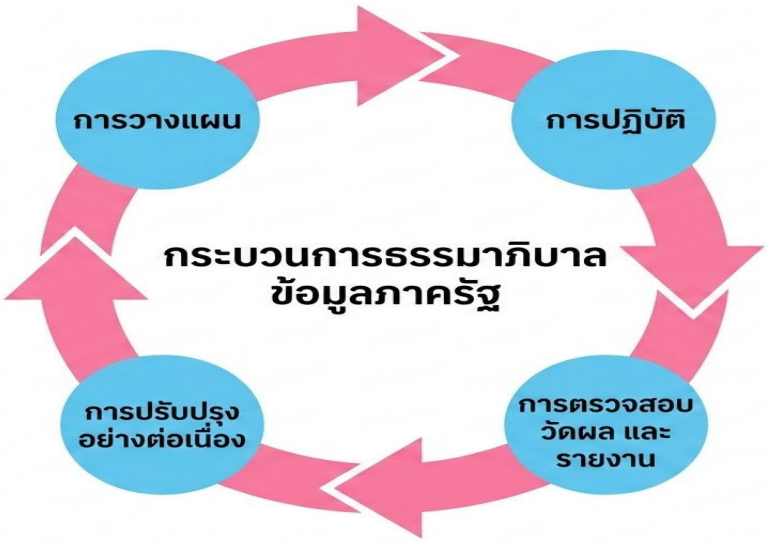
กรมการจัดหางาน ให้คณะทำงานบริกรข้อมูลมีหน้าที่ดำเนินการตามกรอบนโยบายและแนวทางด้านการบริหารจัดการข้อมูล การวางแผนมาตรการรับมือและสามารถจัดการได้อย่างมีประสิทธิภาพ โดยบุคลากรและผู้มีส่วนเกี่ยวข้องกับข้อมูลในบทบาทต่าง ๆ ที่ต้องดำเนินกิจกรรม ที่เกี่ยวข้องกับการกำกับดูแลข้อมูล ต้องปฏิบัติงานให้สอดคล้องกับกฎระเบียบ นโยบาย มาตรฐาน และแนวปฏิบัติที่หน่วยงานกำหนด โดยมีบริกรข้อมูลทำหน้าที่ให้คำแนะนำและสนับสนุนการดำเนินงาน ทั้งนี้ ความก้าวหน้า ผลการปฏิบัติงาน และประเด็นปัญหาที่พบจะถูกรายงานต่อคณะกรรมการธรรมาภิบาลข้อมูลเพื่อใช้ในการกำกับและติดตามการดำเนินงาน กรณีที่คณะทำงานบริกรข้อมูลไม่สามารถให้คำแนะนำหรือตัดสินใจได้ ให้คณะทำงานบริกรข้อมูลนำเสนอและจัดประชุมคณะกรรมการธรรมาภิบาลข้อมูลเป็นการเฉพาะเพื่อให้ที่ประชุมพิจารณาและมีมติต่อไป กรณีที่คณะกรรมการธรรมาภิบาลข้อมูลต้องการความความเห็นจากผู้เชี่ยวชาญภายนอก ให้ดำเนินการจัดให้มีผู้เชี่ยวชาญภายนอกเพื่อให้ความเห็นและข้อเสนอแนะเป็นครั้งไป

๓) การตรวจสอบ วัดผล และรายงาน (Check Measure and Report)

กรมการจัดหางาน ติดตามและประเมินผลการดำเนินงานด้านการบริหารจัดการข้อมูล โดยบริกรข้อมูลทำหน้าที่ตรวจสอบความสอดคล้องระหว่างกฎระเบียบ นโยบาย และมาตรฐานที่กำหนดกับการปฏิบัติงานของผู้ที่เกี่ยวข้อง พร้อมทั้งประเมินคุณภาพข้อมูล ความมั่นคงปลอดภัย และความเสี่ยงที่เกี่ยวข้อง จากนั้นจัดทำรายงานผลการตรวจสอบและผลการประเมินดังกล่าวเสนอต่อคณะกรรมการธรรมาภิบาลข้อมูลและผู้ที่เกี่ยวข้อง เพื่อรับทราบผลการดำเนินงานและใช้ประกอบการพิจารณาแก้ไขปัญหาหรือพัฒนาการบริหารจัดการข้อมูลให้มีประสิทธิภาพยิ่งขึ้น

๔) การปรับปรุงอย่างต่อเนื่อง (Continual Improvement)

กรมการจัดหางาน พัฒนาและปรับปรุงการดำเนินงานด้านธรรมาภิบาลข้อมูลอย่างสม่ำเสมอตลอดวงจรชีวิตของข้อมูล เพื่อให้สอดคล้องกับสภาพแวดล้อม กฎหมาย และความต้องการของผู้บริหารและผู้มีส่วนได้ส่วนเสียที่อาจเปลี่ยนแปลงไป โดยนำผลการตรวจสอบและประเมินผลต่าง ๆ เช่น รายงานความสอดคล้องของการดำเนินงานต่อนโยบายข้อมูล รายงานคุณภาพข้อมูล รายงานด้านความมั่นคงปลอดภัย และรายงานความเสี่ยงที่เกี่ยวข้องกับข้อมูล มาใช้เป็นข้อมูลประกอบในการปรับปรุงกระบวนการธรรมาภิบาลข้อมูล นโยบาย กฎระเบียบ แนวปฏิบัติ เกณฑ์การประเมินความพร้อมและโครงสร้างการกำกับดูแลข้อมูลของกรมการจัดหางาน เพื่อให้การบริหารจัดการข้อมูลมีประสิทธิภาพ



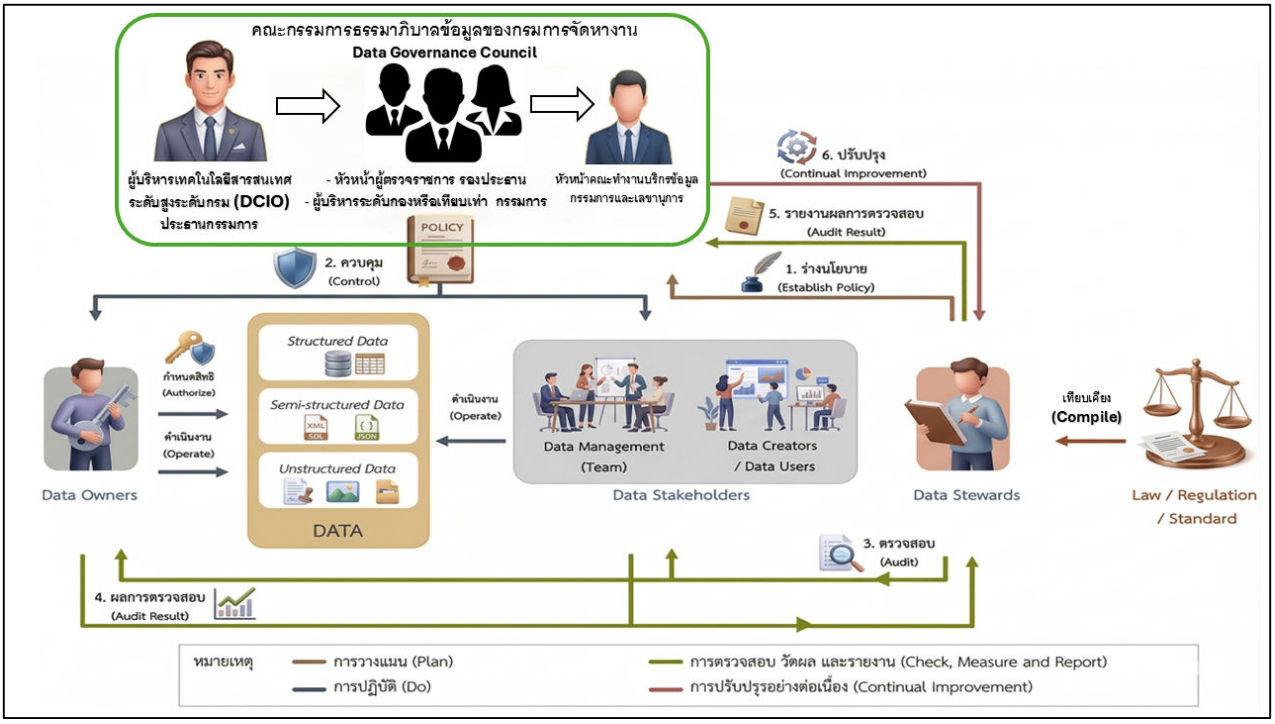
รูป ๕ กระบวนการธรรมาภิบาลข้อมูลภาครัฐของกรมการจัดหางาน

๓.๒ แนวทางการจัดการกระบวนการธรรมาภิบาลข้อมูลภาครัฐ (Data Governance Process Guidelines)

แนวทางการดำเนินกระบวนการธรรมาภิบาลข้อมูลภาครัฐมีส่วนช่วยให้หน่วยงานสามารถทำความเข้าใจโครงสร้างและขั้นตอนของการบริหารจัดการข้อมูลได้อย่างเป็นระบบ และสามารถนำไปประยุกต์ใช้ในการปฏิบัติงานได้อย่างมีประสิทธิภาพ โดยสะท้อนให้เห็นถึงความเชื่อมโยงระหว่างกระบวนการธรรมาภิบาลข้อมูล เครื่องมือหรือเอกสารที่ใช้สนับสนุนการดำเนินงาน ผลลัพธ์ที่เกิดจากการดำเนินการตามหลักธรรมาภิบาลข้อมูล ตลอดจนบทบาทของผู้ที่เกี่ยวข้องหรือผู้มีส่วนได้ส่วนเสียในแต่ละขั้นตอนของการบริหารจัดการข้อมูล

ตารางที่ ๑ ความสัมพันธ์ระหว่างกระบวนการ ส่วนนำเข้า ส่วนนำออก และผู้มีส่วนได้เสียกับข้อมูล

กระบวนการ (Processes)	ส่วนนำเข้า (Input)	ส่วนนำออก (Output)	ผู้มีส่วนได้เสียกับข้อมูล (Data Stakeholder)
๑ การวางแผน	๑. นโยบาย กฎ ระเบียบ ข้อบังคับ และกฎหมายที่เกี่ยวข้องกับข้อมูล ๒. รายการชุดข้อมูล ๓. รายการประเด็นปัญหาจากรายงานผลการตรวจสอบความสอดคล้องของการดำเนินงานต่อนโยบายข้อมูล รายงานคุณภาพข้อมูล รายงานความมั่นคงปลอดภัยต่อข้อมูล และรายงานความเสี่ยงต่อข้อมูล	(๑) แผนดำเนินการ (ขอบเขต เวลา กลุ่มธรรมาภิบาลข้อมูล และต้นทุน)	๑. ผู้บริหารข้อมูลระดับสูง หรือผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ๒. คณะกรรมการธรรมาภิบาลข้อมูล ๓. บริกรข้อมูลด้านธุรกิจ ๔. บริกรข้อมูลด้านเทคนิค ๕. บริกรข้อมูลด้านคุณภาพ
๒ การปฏิบัติ	๑. นโยบาย กฎ ระเบียบ ข้อบังคับ และกฎหมายที่เกี่ยวข้องกับข้อมูล ๒. แผนดำเนินการ (ขอบเขต เวลา และต้นทุน)	๑. รายงานความก้าวหน้าในการปฏิบัติงาน ๒. ผลการปฏิบัติงาน ๓. ประเด็นปัญหาที่พบระหว่างปฏิบัติงาน	๑. ผู้บริหารงาน ๒. ผู้ปฏิบัติงานที่เกี่ยวข้อง ๓. บริกรข้อมูลด้านธุรกิจ ๔. บริกรข้อมูลด้านเทคนิค ๕. บริกรข้อมูลด้านคุณภาพ
๓ การตรวจสอบ วัดผล และรายงาน	๑. นโยบาย กฎ ระเบียบ ข้อบังคับ และกฎหมายที่เกี่ยวข้องกับข้อมูล ๒. เกณฑ์การประเมินความพร้อมของธรรมาภิบาลข้อมูลภาครัฐ ระดับคุณภาพข้อมูล	(๑) รายงานผลการตรวจสอบความสอดคล้องของการดำเนินงานต่อนโยบายข้อมูล (๒) รายงานคุณภาพข้อมูล รายงานความมั่นคงปลอดภัยต่อข้อมูล และรายงานความเสี่ยงต่อข้อมูล	๑. บริกรข้อมูลด้านธุรกิจ ๒. บริกรข้อมูลด้านเทคนิค ๓. บริกรข้อมูลด้านคุณภาพ
๔ การปรับปรุงธรรมาภิบาล	๑. นโยบาย กฎ ระเบียบ ข้อบังคับ และกฎหมายที่เกี่ยวข้องกับข้อมูล ๒. โครงสร้างธรรมาภิบาลข้อมูลภาครัฐ ๓. เกณฑ์การประเมินความพร้อมของธรรมาภิบาลข้อมูลภาครัฐ และระดับคุณภาพข้อมูล ๔. รายงานผลการตรวจสอบความสอดคล้องของการดำเนินงานต่อนโยบายข้อมูล รายงานความมั่นคงปลอดภัยต่อข้อมูล และรายงานความเสี่ยงต่อข้อมูล ๕. รายการความต้องการจากผู้บริหารและผู้มีส่วนได้ส่วนเสีย	๑. กระบวนการธรรมาภิบาลข้อมูลภาครัฐ ๒. นโยบาย กฎ ระเบียบ ข้อบังคับ และกฎหมาย ที่เกี่ยวข้องกับข้อมูล ๓. เกณฑ์การประเมินความพร้อมของธรรมาภิบาลข้อมูลภาครัฐและระดับคุณภาพข้อมูล ๔. โครงสร้างธรรมาภิบาลข้อมูลภาครัฐ	๑. ผู้บริหารข้อมูลระดับสูงหรือผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ๒. คณะกรรมการธรรมาภิบาลข้อมูล ๓. บริกรข้อมูลด้านธุรกิจ ๔. บริกรข้อมูลด้านเทคนิค ๕. บริกรข้อมูลด้านคุณภาพ



รูปที่ ๖ แผนภาพการดำเนินการธรรมาภิบาลข้อมูลของกรมการจัดหางาน

จากแผนภาพนี้แสดงขั้นตอนการตรวจสอบความสอดคล้องระหว่าง นโยบายข้อมูล (Data Policy) กฎหมายที่เกี่ยวข้อง และการปฏิบัติงานจริงของบุคลากรในระบบธรรมาภิบาลข้อมูล โดยมีกระบวนการดำเนินงาน ดังนี้

๑) การร่างนโยบาย (Plan) บริกรข้อมูล (Data Stewards) ทั้งด้านธุรกิจ ด้านเทคนิค และด้านคุณภาพ ร่วมกันร่างนโยบายข้อมูลให้สอดคล้องกับกฎหมายและข้อบังคับ เพื่อนำเสนอต่อคณะกรรมการธรรมาภิบาลข้อมูลพิจารณาอนุมัติ

๒) การปฏิบัติตามนโยบาย (Do) เจ้าของข้อมูล(Data Owner) และผู้มีส่วนได้เสีย (Data Stakeholders) นำนโยบายไปปฏิบัติในการบริหารจัดการข้อมูล เช่น สิทธิ์การเข้าถึงข้อมูล ให้เป็นไปตามนโยบายที่กำหนด ผู้มีส่วนได้เสีย เช่น ผู้ดูแลฐานข้อมูล (DBA) และผู้ใช้ข้อมูล (Data User) ต้องปฏิบัติงานกับข้อมูล (เพิ่ม ลบ แก้ไข ประมวลผล) ตามขอบเขตสิทธิ์ที่ได้รับจากเจ้าของข้อมูลเท่านั้น

๓) การตรวจสอบและรายงาน (Check Measure and Report) บริกรข้อมูลจะทำหน้าที่ตรวจสอบความสอดคล้องระหว่างการดำเนินงานจริงกับนโยบายที่กำหนดไว้ พร้อมสรุปรายงานผลเสนอต่อคณะกรรมการธรรมาภิบาลข้อมูล

๔) การปรับปรุงอย่างต่อเนื่อง (Continual Improvement) คณะกรรมการธรรมาภิบาลข้อมูล ทบทวนนโยบายและผลการดำเนินงาน เพื่อนำมาปรับปรุงและกำหนดแนวทางธรรมาภิบาลข้อมูลให้มีประสิทธิภาพยิ่งขึ้น

๔. การกำหนดมาตรการกำกับดูแล การควบคุม และยกระดับคุณภาพข้อมูล (Data quality control and improvement)

กรมการจัดหางาน ยกระดับมาตรฐานการบริหารจัดการข้อมูลให้เป็นไปตามหลักธรรมาภิบาลข้อมูล เพื่อให้การดำเนินภารกิจด้านการส่งเสริมการมีงานทำและการบริหารจัดการแรงงานเป็นไปอย่างมีประสิทธิภาพ โดยกำหนดมาตรการกำกับดูแล การควบคุม และยกระดับคุณภาพข้อมูล ให้มีความถูกต้อง ครบถ้วน และเป็นปัจจุบันในระดับมาตรฐานสากล ควบคู่ไปกับการวางระบบรักษาความมั่นคงปลอดภัยสารสนเทศที่เข้มงวดเพื่อป้องกันการรั่วไหลหรือการเข้าถึงข้อมูลโดยมิชอบ และให้ความสำคัญสูงสุดกับการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายเพื่อมิให้เกิดการละเมิดสิทธิของผู้ใช้บริการ ส่งเสริมให้เกิดการเชื่อมโยง แลกเปลี่ยน และบูรณาการฐานข้อมูลด้านแรงงานร่วมกับหน่วยงานภาคีเครือข่ายอย่างเป็นระบบ อันจะนำไปสู่การใช้ประโยชน์จากข้อมูลเชิงยุทธศาสตร์ที่มีประสิทธิภาพสูงสุดในการขับเคลื่อนเศรษฐกิจและสังคมของประเทศอย่างยั่งยืน

๔.๑ การบริหารจัดการข้อมูล (Data Management)

การบริหารจัดการข้อมูล คือ “คำจำกัดความที่อธิบายถึงกระบวนการที่ใช้ในการวางแผน (Plan) ระบุ (Specify) เปิดใช้งาน (Enable) สร้าง (Create) รับ (Acquire) ดูแลรักษา (Maintain) ใช้ (Use) จัดเก็บถาวร (Archive) ดึงข้อมูล (Retrieve) ควบคุม (Control) และทำลายข้อมูล (Purge)”

การบริหารจัดการข้อมูลเป็นสิ่งสำคัญสำหรับทุกหน่วยงาน ซึ่งแต่ละหน่วยงานต้องตระหนักว่าข้อมูลที่มีอยู่เป็นทรัพย์สินที่มีค่า และจากข้อมูลที่มีปริมาณมหาศาล ไม่ว่าจะเป็นข้อมูลที่รวบรวมมาโดยอัตโนมัติจากระบบหรืออุปกรณ์ต่าง ๆ หรือข้อมูลที่เกิดขึ้นจากการป้อนข้อมูลหรือโต้ตอบกับผู้ใช้งาน เพื่อให้หน่วยงานสามารถนำข้อมูลเหล่านี้ไปประมวลผลหรือใช้ในการตัดสินใจได้อย่างแม่นยำ จึงต้องได้รับการบริหารจัดการอย่างถูกต้องเหมาะสม และสอดคล้องกับวัตถุประสงค์ในการบริหารจัดการข้อมูลของหน่วยงาน เช่น

๑) การจัดเก็บ นำมาใช้งาน และประมวลผลข้อมูลตามวัตถุประสงค์ความจำเป็นของหน่วยงาน

๒) การควบคุม ตรวจสอบ และป้องกัน โดยใช้กระบวนการธรรมาภิบาลข้อมูลภาครัฐและความ ปลอดภัยของข้อมูล

๓) การจัดหมวดหมู่ และกำหนดมาตรฐานของข้อมูล โดยใช้การจำแนกข้อมูล และกรอบการทำงานที่เป็นที่รู้จักแพร่หลาย

๔) กำหนดข้อมูลให้อยู่ในรูปแบบที่เรียกใช้ได้อย่างมีประสิทธิภาพ

๕) การปรับปรุงข้อมูลให้เป็นปัจจุบัน และมีความถูกต้องสมบูรณ์อยู่เสมอ

๖) การปกป้องข้อมูลจากการลักลอบใช้งานหรือแก้ไขโดยมิชอบ รวมถึงจากเหตุการณ์ที่อาจเกิด จากภัยธรรมชาติหรือความบกพร่องภายในระบบคอมพิวเตอร์

ซึ่งในการบริหารจัดการข้อมูลนั้น มีองค์ประกอบในการบริหารจัดการตลอดทั้งระบบบริหารและกระบวนการจัดการข้อมูล หรือวงจรชีวิตของข้อมูล ดังรูป

รูปที่ ๗ ระบบบริหารและกระบวนการจัดการข้อมูล หรือวงจรชีวิตของข้อมูล และองค์ประกอบในการบริหารจัดการข้อมูล

๔.๑.๑ ระบบบริหารและกระบวนการจัดการข้อมูล หรือวงจรชีวิตของข้อมูล (Data Life Cycle)

ระบบบริหารและกระบวนการจัดการข้อมูล หรือวงจรชีวิตของข้อมูล คือ “ลำดับขั้นตอนของข้อมูล ตั้งแต่เริ่มสร้างข้อมูลไปจนถึงการทำลายข้อมูล” ประกอบด้วย ๖ ขั้นตอน ดังนี้

๑) กระบวนการสร้างข้อมูล (Create) เป็นการสร้างข้อมูลขึ้นมาใหม่ โดยวิธีการบันทึกเข้าไปด้วยบุคคลหรือบันทึกอัตโนมัติด้วยอุปกรณ์อิเล็กทรอนิกส์ เช่น อุปกรณ์ตรวจจับสัญญาณ (Sensor) รวมถึงการแลกเปลี่ยนข้อมูลหรือการรับข้อมูลจากหน่วยงานอื่น

๒) กระบวนการจัดเก็บข้อมูล (Store) เป็นการจัดเก็บข้อมูลที่เกิดจากกระบวนการสร้าง หรือข้อมูลที่ได้จากการแลกเปลี่ยนกับหน่วยงานอื่น เพื่อให้มีระเบียบง่ายต่อการใช้งาน ไม่สูญหาย หรือถูกทำลาย และให้ผู้ใช้งานสามารถประมวลผลข้อมูลต่าง ๆ ตามความต้องการได้อย่างรวดเร็ว ไม่ว่าจะจัดเก็บลงแฟ้มข้อมูล (File) หรือระบบการจัดการฐานข้อมูล (Database Management System - DBMS)

๓) กระบวนการใช้ข้อมูล (Use) เป็นการนำข้อมูลที่จัดเก็บมาประมวลผล เช่น การถ่ายโอนข้อมูล การเปลี่ยนรูปแบบการจัดเก็บข้อมูล การวิเคราะห์ข้อมูล การจัดทำรายงาน เพื่อนำข้อมูลเหล่านั้นมาใช้งานให้เกิดประโยชน์ตามวัตถุประสงค์ รวมถึงการสำรอง (Backup) ข้อมูล โดยการคัดลอกข้อมูลที่ใช้งาน ทำสำเนาข้อมูลเป็นการหลีกเลี่ยงความเสียหายที่จะเกิดขึ้นหากข้อมูลเกิดการเสียหายหรือสูญหาย ซึ่งสามารถนำข้อมูลที่สำรองไว้ในสื่อบันทึกข้อมูลกลับมาใช้งานได้ทันที โดยการกู้คืน (Restore)

๔) กระบวนการเผยแพร่ข้อมูล (Publish) เป็นการแชร์ข้อมูล (Sharing) การกระจายข้อมูล (Dissemination) การควบคุมการเข้าถึง (Access Control) การแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน (Exchange) เงื่อนไขในการนำข้อมูลไปใช้ (Condition)

๕) กระบวนการจัดเก็บข้อมูลถาวร (Archive) เป็นการคัดลอกเอาข้อมูลที่มีช่วงอายุเกินช่วงใช้งาน หรือไม่ได้ใช้งานแล้ว เพื่อทำสำเนาสำหรับการเก็บรักษา โดยที่ข้อมูลนั้นไม่มีการลบ ปรับปรุง หรือแก้ไขอีก และ สามารถนำกลับไปใช้งานได้ใหม่เมื่อต้องการ

๖) กระบวนการทำลายข้อมูล (Destroy) เป็นการทำลายข้อมูล ซึ่งปกติจะเป็นการทำลายข้อมูลที่มี การจัดเก็บถาวรเป็นระยะเวลานานหรือเกินกว่าระยะเวลา ๑๐ ปี

เพื่อให้การบริหารจัดการข้อมูลในทุกขั้นตอน ตั้งแต่การสร้าง การใช้ การจัดเก็บ จนถึงการทำลาย เป็นไปในมาตรฐานเดียวกัน และมีความสอดคล้องกับกฎหมายและระเบียบที่เกี่ยวข้อง กรมการจัดหางานจึงมีข้อกำหนดในการดำเนินงาน ในการบริหารประสิทธิภาพของข้อมูล ดังนี้

๑) ด้านการกำกับดูแล ให้มีความโปร่งใส ตรวจสอบได้ และสอดคล้องกับอำนาจหน้าที่ตามกฎหมาย โดยมีการกำหนดบทบาทและความรับผิดชอบ บุคลากร เข้าถึงและใช้ข้อมูลได้เฉพาะตามสิทธิ์ที่ได้รับอนุญาต ทั้งนี้การดำเนินงานด้านข้อมูลเป็นไปตามกฎหมายที่เกี่ยวข้อง เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พระราชบัญญัติการปฏิบัติราชการทางอิเล็กทรอนิกส์ และระเบียบงานสารบรรณ รวมทั้งต้องมีการจัดเก็บหลักฐานหรือบันทึกการดำเนินงานในแต่ละกระบวนการ เพื่อรองรับการตรวจสอบจากหน่วยงานกำกับดูแลทั้งภายในและภายนอก

๒) ด้านความมั่นคงปลอดภัยและความเป็นส่วนตัวของข้อมูล เพื่อป้องกันการเข้าถึง การใช้หรือการเปิดเผยข้อมูลโดยมิชอบ โดยข้อมูลได้รับการจัดชั้นความลับ และมีระบบควบคุมการเข้าถึง ทั้งด้านกายภาพและระบบดิจิทัล เพื่อรักษาความลับของข้อมูล ป้องกันการแก้ไขหรือเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต เพื่อรักษาความถูกต้องครบถ้วนของข้อมูล รวมทั้งต้องคำนึงถึงการคุ้มครองข้อมูลส่วนบุคคลตั้งแต่ขั้นตอนการออกแบบระบบ โดยจัดให้มีมาตรการที่เหมาะสม เช่น การขอความยินยอม การจัดเก็บอย่างปลอดภัย และการเข้ารหัสข้อมูล (Encryption) ตามระดับความเสี่ยงของข้อมูล

๓) ด้านการบริหารจัดการคุณภาพข้อมูลและเมทาดาตา การบริหารจัดการให้ได้ข้อมูลที่มีคุณภาพ เชื่อถือได้ และสามารถนำไปใช้ประโยชน์ได้อย่างมีประสิทธิภาพ โดยเจ้าของข้อมูล (Data Owner) และบริกรข้อมูล (Data Steward) การจัดทำคำอธิบายข้อมูล (Metadata) เพื่อให้ผู้ใช้สามารถเข้าใจบริบทและนำข้อมูลไปใช้ได้อย่างถูกต้อง ข้อมูลต้องผ่านกระบวนการตรวจสอบคุณภาพก่อนนำไปใช้หรือเผยแพร่ สามารถติดตามเส้นทางของข้อมูล ได้ตลอดวงจรชีวิต เพื่อให้ทราบการเปลี่ยนแปลงหรือการถ่ายโอนข้อมูลในแต่ละขั้นตอน และรักษาความน่าเชื่อถือของชุดข้อมูลหลัก (Master Data) ของกรมการจัดหางาน

๔.๑.๒ องค์ประกอบในการบริหารจัดการข้อมูล (Data Management Component)

การบริหารจัดการข้อมูลของกรมการจัดหางานได้กำหนดองค์ประกอบในการบริหารจัดการข้อมูล ดังนี้

(๑) คำอธิบายชุดข้อมูลดิจิทัล หรือเมทาดาตา (Metadata) เป็นข้อมูลที่ใช้อธิบายรายละเอียดของชุดข้อมูล เช่น โครงสร้างข้อมูล กฎและข้อจำกัดของข้อมูล รวมถึงความเชื่อมโยงกับกระบวนการเชิงธุรกิจและเทคโนโลยีสารสนเทศ เพื่อช่วยให้สามารถเข้าใจและนำข้อมูลไปใช้ได้อย่างถูกต้อง การบริหารจัดการเมทาดาตาครอบคลุมการรวบรวม จัดหมวดหมู่ ดูแล และควบคุมข้อมูล โดยข้อมูลแต่ละชุดมีเมทาดาตากำกับ เพื่อให้ผู้ใช้งานทราบรายละเอียด วัตถุประสงค์ และองค์ประกอบของชุดข้อมูล เช่น รายการฟิลด์ข้อมูล เป็นต้น

การบริหารจัดการคำอธิบายชุดข้อมูลดิจิทัล หรือ เมทาดาตา	
วิธีการดำเนินการ	- ทำความเข้าใจเกี่ยวกับความต้องการในการจัดทำคำอธิบายชุดข้อมูลดิจิทัล หรือ เมทาดาตา - กำหนดมาตรฐานของคำอธิบายชุดข้อมูลดิจิทัล หรือเมทาดาตา
สิ่งที่นำเข้า	- คู่มือแนวปฏิบัติมาตรการการบริหารจัดการคำอธิบายชุดข้อมูลดิจิทัล หรือเมทา ดาตา เช่น พจนานุกรมข้อมูล (Data Dictionary) การตั้งชื่อข้อมูล (Data Naming)
เครื่องมือที่ใช้	- เครื่องมือบริหารจัดการบัญชีข้อมูล (Data Catalog Management Tools) - เครื่องมือบริหารจัดการคำอธิบายชุดข้อมูลดิจิทัล หรือเมทาดาตา (Metadata Repository Management Tools)
ผลที่ได้รับ	- เมทาดาตาที่มีคุณภาพ มีความสอดคล้อง และความมั่นคงปลอดภัย
ผู้เกี่ยวข้อง	- บริกรข้อมูล (Data Stewards) - นักวิเคราะห์ข้อมูล (Data Analyst)

ตารางที่ ๑ สรุปการบริหารจัดการคำอธิบายชุดข้อมูลดิจิทัล หรือ เมทาดาตา

(๒) ความมั่นคงปลอดภัยและการรักษาความเป็นส่วนบุคคลของข้อมูล (Data Security and Privacy)

ความมั่นคงปลอดภัยของข้อมูล (Data Security) หมายความว่า การป้องกันข้อมูลในบริบทของการรักษาความลับ ความถูกต้องของข้อมูล ความพร้อมใช้งานของข้อมูล จากข้อมูลของมาตรฐาน ISO/IEC๒๗๐๐๑ โดยมีรายละเอียด ดังนี้

- การรักษาความลับ (Confidentiality) หมายความว่า การรักษาปลอดภัยของข้อมูลตามระดับชั้น ของข้อมูล และมีการกำหนดสิทธิ์การเข้าถึงข้อมูล เนื่องจากข้อมูลในหน่วยงานมีหลายประเภทข้อมูล บางประเภทเป็นข้อมูลที่มีความสำคัญ หรืออ่อนไหว จึงต้องมีการรักษาความลับเพื่อลดความเสี่ยงของ การถูกคุกคาม และเป็นการป้องกันการรั่วไหลของข้อมูลโดยมิชอบ เช่น การส่งข้อมูลที่ปกปิดหรือเป็นความลับ ต้องมีวิธีการที่ทำ ให้ทราบได้ว่าบุคคลที่ต้องการส่งข้อมูลมาให้ หรือการที่ผู้ได้รับการอนุญาตให้เข้าถึงข้อมูลเท่านั้น ที่สามารถอ่านข้อมูลได้
- ความถูกต้องของข้อมูล (Integrity) หมายความว่า การคงสภาพของข้อมูลหรือการรักษาความถูกต้องสมบูรณ์ของข้อมูลให้มีความถูกต้องและน่าเชื่อถือ รวมถึงมีการปกป้องข้อมูลให้ปราศจากการถูกเปลี่ยนแปลงโดยผู้ไม่มีสิทธิ์ เช่น ข้อมูลที่ใช้จะต้องเป็นข้อมูลที่ถูกต้องอย่างแท้จริง ไม่มีการดัดแปลงหรือแก้ไข
- ความพร้อมใช้งานของข้อมูล (Availability) หมายความว่า การพร้อมในการใช้งานอยู่เสมอ กล่าวคือ ข้อมูลต้องพร้อมสำหรับการใช้งานอยู่เสมอ รวมถึงมีการสำรองข้อมูลไว้เมื่อเกิดภัยพิบัติหรือเหตุการณ์ ที่ไม่คาดฝัน เช่น หากต้องการใช้ข้อมูล ผู้ใช้งานสามารถใช้ข้อมูลได้ทันที และใช้ได้อย่างต่อเนื่อง

โดยความมั่นคงปลอดภัยของข้อมูลต้องดำเนินการตั้งแต่การวางแผน การจัดทำ การปฏิบัติตาม และการบังคับใช้นโยบายและขั้นตอนด้านการรักษาความปลอดภัย เพื่อสนับสนุนในด้านที่เกี่ยวข้องกับการพิสูจน์ ตัวตน การกำหนดสิทธิ์ การเข้าถึงข้อมูล การตรวจสอบ และความพร้อมใช้ของข้อมูลอย่างเหมาะสม นอกจากนี้ ต้องมีการรักษาความเป็นส่วนบุคคลของข้อมูล (Data Privacy) ตั้งแต่การรวบรวม จัดเก็บ ใช้ เผยแพร่ หรือดำเนินการอื่นใดเกี่ยวกับข้อมูล โดยจะต้องมีการระบุวัตถุประสงค์เป็นหลักฐานให้ชัดเจน ห้ามมิให้มีการเปิดเผย หรือแสดง หรือทำให้ปรากฏในลักษณะอื่นใดที่ไม่สอดคล้องกับวัตถุประสงค์ เว้นแต่จะ ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลนั้น ๆ หรือมีกฎหมายกำหนดให้สามารถกระทำสิ่งนั้นได้

การบริหารจัดการความมั่นคงปลอดภัยและการรักษาความเป็นส่วนบุคคลของข้อมูล	
วิธีการดำเนินการ	- กำหนดนโยบายและมาตรฐานด้านความปลอดภัยของข้อมูล - บริหารจัดการเกี่ยวกับข้อมูลตั้งแต่วิธีการจัดเก็บ การประมวลผล การเข้าถึงข้อมูล การนำไปใช้ การเปิดเผย และการทำลาย
สิ่งที่นำเข้า	- มาตรฐาน แนวปฏิบัติ และนโยบายที่เกี่ยวกับความปลอดภัยของข้อมูล - มาตรฐาน แนวปฏิบัติ และนโยบายที่เกี่ยวกับการรักษาความเป็นส่วนบุคคลของข้อมูล - มาตรฐานและหลักเกณฑ์การพิสูจน์และยืนยันตัวตนทางดิจิทัล
เครื่องมือที่ใช้	- ระบบการจัดการฐานข้อมูล (Database Management System - DBMS) - เทคโนโลยีจัดการข้อมูลเพื่อแสดงตัวตน (Identity Management Technology) - ระบบจัดการการเปลี่ยนแปลง (Change Control System) - หนังสือให้ความยินยอม (Letter of Consent)
ผลที่ได้รับ	- นโยบายด้านการรักษาความปลอดภัยและการรักษาความเป็นส่วนบุคคลของข้อมูล (Data Security and Privacy Policy) - มาตรฐานการจัดระดับชั้นข้อมูล (Data Classification Standard)
ผู้เกี่ยวข้อง	- ผู้บริหารจัดการฐานข้อมูล (Database Administrator) - บริกรข้อมูล (Data Stewards) - ผู้ตรวจสอบภายใน (Internal Auditor)

ตารางที่ ๒ สรุปการบริหารจัดการความมั่นคงปลอดภัยและการรักษาความเป็นส่วนบุคคลของข้อมูล

(๓) คุณภาพของข้อมูล (Data Quality)

คุณภาพของข้อมูล (Data Quality) เป็นเครื่องมือในการวัดความน่าเชื่อถือและประสิทธิภาพของการนำข้อมูลไปใช้ ต้องมีการวางแผน การดำเนินการ และการควบคุมกิจกรรมต่าง ๆ รวมถึงการปรับปรุง เพื่อให้ข้อมูลมีคุณภาพ เนื่องจากข้อมูลที่มีคุณภาพสูงทำให้การดำเนินงานของหน่วยงานเป็นไปอย่างมีประสิทธิภาพการทำให้ข้อมูลมีคุณภาพประกอบด้วย

- ความถูกต้องและสมบูรณ์ (Accuracy and Completeness)
- ความสอดคล้องกัน (Consistency)
- ตรงตามความต้องการของผู้ใช้ (Relevancy)
- ความเป็นปัจจุบัน (Timeliness)
- ความพร้อมใช้ (Availability)

ดังแสดงรายละเอียดเพิ่มเติมในข้อ ๕.๒ การประเมินคุณภาพของข้อมูล (Data Quality Assessment)

การบริหารจัดการคุณภาพของข้อมูล	
วิธีการดำเนินการ	- กำหนดข้อมูลที่จำเป็นต้องมีคุณภาพ - พัฒนาและส่งเสริมการให้ความสำคัญกับคุณภาพของข้อมูล (Awareness) - กำหนดขอบเขตของการประเมิน (Assessment) คุณภาพของข้อมูล - กำหนดและระบุลำดับความสำคัญ (Prioritize) ของการปรับปรุงข้อมูลให้มีคุณภาพ
สิ่งที่นำเข้า	- มาตรฐาน แนวปฏิบัติ และนโยบายที่เกี่ยวกับการทำให้ข้อมูลมีคุณภาพ เช่น การจัดทำโปรไฟล์ข้อมูล (Data Profiling) การทำข้อมูลให้ถูกต้องสมบูรณ์ (Data Cleansing) - เมทาดาตาทั้งด้านธุรกิจและเทคโนโลยีสารสนเทศ
เครื่องมือที่ใช้	- เครื่องมือในการทำข้อมูลให้ถูกต้องสมบูรณ์ (Data Cleansing Tools) - เครื่องมือวิเคราะห์ทางสถิติ (Statistical Analysis Tools)
ผลที่ได้รับ	- รายงานการรับรองคุณภาพของข้อมูล (Data Quality Certification Reports) - ข้อตกลงระดับคุณภาพของข้อมูล (Data Quality Service Level Agreements)
ผู้เกี่ยวข้อง	- นักวิเคราะห์ข้อมูล (Data Analyst) - บริกรข้อมูล (Data Stewards)

ตารางที่ ๓ สรุปการบริหารจัดการคุณภาพของข้อมูล

๔.๒ สภาพแวดล้อมของธรรมาภิบาลข้อมูล (Data Governance Environment)

กฎหมาย ระเบียบ ข้อบังคับ แนวนโยบาย และแนวปฏิบัติที่เกี่ยวข้องกับธรรมาภิบาลข้อมูลของกรมการจัดหางาน

ปัจจุบันกฎหมายที่เกี่ยวข้องกับข้อมูลข่าวสาร หรือสิทธิส่วนบุคคลในประเทศไทย มีประเด็นที่อาจ ส่งผลกระทบต่อหลักแนวคิดธรรมาภิบาลข้อมูลภาครัฐ ซึ่งหากกรมการจัดหางานต้องการสร้างหรือปรับปรุงระบบภายในให้มีธรรมาภิบาลข้อมูลภาครัฐ จะต้องพิจารณาประเด็นหลัก ๆ ที่เกี่ยวข้องกับกฎหมาย ดังนี้

รูปที่ ๘ กฎหมาย ระเบียบ ข้อบังคับ แนวนโยบาย และแนวปฏิบัติที่เกี่ยวข้องกับ ธรรมาภิบาลข้อมูลภาครัฐ

๑) การเปิดเผยข้อมูล

การเปิดเผยข้อมูลเป็นสิ่งจำเป็นต่อการดำเนินงานของรัฐบาล ซึ่งแสดงความโปร่งใสในการดำเนินงานและความสามารถในการตรวจสอบได้จากภาคเอกชนและประชาชน รวมไปถึงการสนับสนุนให้ ภาคเอกชนและประชาชนนำข้อมูลที่เปิดเผยไปสร้างนวัตกรรมผลิตภัณฑ์และบริการ เพื่อยกระดับการพัฒนา ประเทศ โดยแนวคิดการเปิดเผยข้อมูลเป็นที่ยอมรับของหน่วยงานระหว่างประเทศและรัฐบาลประเทศต่าง ๆ โดย ในประเทศไทยมีกฎหมายที่เกี่ยวข้องกับการเปิดเผยข้อมูล ดังนี้

(๑) รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. ๒๕๖๐ ในมาตราที่ ๕๙ ได้ระบุว่า รัฐต้องเปิดเผยข้อมูลหรือข่าวสารสาธารณะในครอบครองของหน่วยงานของรัฐที่มิใช่ข้อมูลเกี่ยวกับความมั่นคงของรัฐหรือเป็น ความลับของทางราชการ

(๒) พระราชบัญญัติการปฏิบัติราชการทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๖๕ มาตรา ๒๑ หน่วยงานของรัฐต้องเปิดเผยข้อมูลเกี่ยวกับการอนุญาตผ่านช่องทางอิเล็กทรอนิกส์ให้แล้วเสร็จโดยเร็ว

(๓) พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ.๒๕๖๒ โดยมี การเปิดเผยข้อมูลหรือข่าวสารสาธารณะที่หน่วยงานของรัฐจัดทำและครอบครองในรูปแบบและช่องทางดิจิทัล เพื่อให้ประชาชนเข้าถึงโดยสะดวก มีส่วนร่วมและตรวจสอบการดำเนินงานของรัฐ และสามารถนำข้อมูลไป พัฒนาบริการและนวัตกรรมที่จะเป็นประโยชน์ต่อประเทศในด้านต่าง ๆ

(๔) พระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. ๒๕๔๐ โดยมี ๓ ประเด็นที่เกี่ยวกับการ เปิดเผยข้อมูลได้ถูกระบุไว้ใน พ.ร.บ. ฉบับนี้ ได้แก่ ข้อมูลภาครัฐต้อง “เปิดเผยเป็นหลัก ปกปิดเป็นข้อยกเว้น”, กำหนดหลักเกณฑ์และกลไกการเปิดเผยข้อมูล, กำหนดประเภทข้อมูลที่เปิดเผยได้และเปิดเผยไม่ได้

(๕) แนวทางปฏิบัติการเปิดเผยข้อมูลภาครัฐ (Government Open Data Publication Guidelines) ให้แนวทางปฏิบัติเพื่อการเปิดเผยข้อมูลภาครัฐ ซึ่งมีวัตถุประสงค์เพื่อเป็นแนวปฏิบัติสำหรับการเปิดเผยข้อมูลภาครัฐ ได้แก่

- แนวปฏิบัติและมาตรฐานเชิงเทคนิค เพื่อให้หน่วยงานภาครัฐนำไปใช้เป็นแนวปฏิบัติในการ ดำเนินการเกี่ยวกับการเปิดเผยข้อมูลของหน่วยงานให้เป็นไปในทิศทางเดียวกัน รวมถึงการกำหนดมาตรฐานเชิง เทคนิค รูปแบบวิธีการเผยแพร่ข้อมูลผ่านศูนย์กลางข้อมูลเปิดภาครัฐ หรือ data.go.th และการกำหนดสัญญา อนุญาต (License) ที่เหมาะสมสำหรับข้อมูลเปิดภาครัฐ
- แบบฟอร์มคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตา เพื่อเป็นตัวอย่างการจัดทำคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตา โดยหน่วยงานสามารถนำไปประยุกต์ใช้งานที่เหมาะสมกับหน่วยงานได้
- คู่มือการเปิดเผยข้อมูล (Open Data Handbook) เพื่อสร้างความรู้ ความเข้าใจให้แก่ หน่วยงานภาครัฐ ภาคเอกชน และผู้ที่ต้องการศึกษาเกี่ยวกับข้อมูลเปิด (Open Data)
- คู่มือการนำข้อมูลขึ้นเผยแพร่บน data.go.th เพื่อให้ผู้ใช้งานสามารถศึกษาทำความเข้าใจการทำงานต่าง ๆ ของระบบได้ และสามารถตรวจสอบปัญหาที่เกิดจากการใช้งานและสามารถแก้ปัญหาในขั้นต้นได้
- คู่มือแสดงรายการชุดข้อมูลที่สำคัญ เพื่อเป็นการสร้างแหล่งข้อมูลที่ใช้ประกอบในการใช้ งานที่เกี่ยวกับชุดข้อมูลที่สำคัญให้แก่หน่วยงานภาครัฐ ภาคเอกชน และผู้ที่ต้องการศึกษาเกี่ยวกับข้อมูลเปิด (Open Data)
- แนวปฏิบัติในการออกแบบความคิดเชิงนวัตกรรม (Data Innovation Guideline) เป็น คู่มือที่ช่วยให้เข้าใจปัญหาที่แท้จริง และสามารถออกแบบแนวทางแก้ไขปัญหาที่เป็นแนวคิดเชิงนวัตกรรม ตลอดจนสามารถเข้าถึงชุดข้อมูล (Datasets) ต่าง ๆ เพื่อให้ได้มาซึ่งแนวทางในการแก้ปัญหา นอกจากนั้นผู้ที่ ต้องการศึกษากระบวนการออกแบบนวัตกรรมสามารถนำไปประยุกต์หรือปรับใช้กับหน่วยงานได้

๒) การเชื่อมโยงและแลกเปลี่ยนข้อมูล

การเชื่อมโยงและแลกเปลี่ยนข้อมูลเป็นสิ่งสำคัญต่อการบูรณาการในการดำเนินงานระหว่างหน่วยงานภาครัฐ ซึ่งเป็นประโยชน์ต่อกรมการจัดหางานและประชาชนในการขอใช้บริการจากภาครัฐ โดยมีกฎหมายที่เกี่ยวข้องกับการเชื่อมโยงและแลกเปลี่ยนข้อมูล ดังนี้

(๑) พระราชบัญญัติการปฏิบัติราชการทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๖๕ มาตรา ๑๕ การติดต่อหรือส่งเรื่องถึงกันในระหว่างหน่วยงานของรัฐด้วยกัน หรือระหว่างเจ้าหน้าที่ของรัฐกับหน่วยงานของรัฐ ที่ได้กระทำโดยวิธีการทางอิเล็กทรอนิกส์แล้ว ให้ถือว่าเป็นการชอบด้วยกฎหมายและใช้เป็นหลักฐานได้ตามกฎหมาย

(๒) พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ โดยมีการพัฒนามาตรฐาน หลักเกณฑ์ และวิธีการเกี่ยวกับดิจิทัล และพัฒนาโครงสร้างพื้นฐานด้านดิจิทัลที่จำเป็น ให้เป็นไปตามมาตรฐานสากล เพื่อสร้างและพัฒนากระบวนการทำงานของหน่วยงานของรัฐให้มีความสอดคล้องและมีการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างกัน รวมทั้งมีความมั่นคงปลอดภัยและน่าเชื่อถือ โดยมีการบูรณาการและสามารถทำงานร่วมกันอย่างเป็นเอกภาพ เกิดการพัฒนาการบริการภาครัฐที่มีประสิทธิภาพและนำไปสู่การบริหารราชการและการบริการประชาชนแบบบูรณาการ รวมทั้งให้ประชาชนเข้าถึงโดยสะดวก

(๓) ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ว่าด้วยการใช้ข้อความ XML สำหรับการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ระหว่างหน่วยงาน มีวัตถุประสงค์ในการสนับสนุนการใช้ข้อความ XML สำหรับการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ให้มีความมั่นคง ปลอดภัยและน่าเชื่อถือ รวมทั้งให้ผู้ประกอบการและหน่วยงานต่าง ๆ ได้มีแนวทางในการสร้างเอกสารอิเล็กทรอนิกส์ให้อยู่ในรูปแบบข้อความ XML ให้เป็นมาตรฐานเดียวกัน

(๔) ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ว่าด้วยรหัสสถานที่ออกหนังสือ ให้ข้อเสนอแนะสำหรับการกำหนดรหัสสถานที่ออกหนังสือรับรอง ซึ่งจะส่งผลให้ทราบที่มาของหนังสือรับรองและการอำนวยความสะดวกทางการค้า พร้อมการบริหารจัดการ มาตรฐานการแลกเปลี่ยนข้อมูลสารสนเทศด้านการค้าระหว่างประเทศผ่านระบบ National Single Window ให้เป็นไปในทิศทางเดียวกัน

๓) การคุ้มครองข้อมูลส่วนบุคคล

การคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection) เป็นสิ่งสำคัญที่ภาครัฐต้องดำเนินการ โดยปัจจุบันมีการนำระบบสารสนเทศและการสื่อสารมาประยุกต์ใช้ประกอบการทำธุรกรรมทาง อิเล็กทรอนิกส์อย่างแพร่หลาย ซึ่งหน่วยงานภาครัฐอาจจะมี การเก็บ รวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคลของ ผู้ใช้บริการในรูปของข้อมูลอิเล็กทรอนิกส์ เพื่อเป็นการป้องกันการละเมิดข้อมูลส่วนบุคคล ซึ่งเป็นสิทธิขั้นพื้นฐาน สำคัญในความเป็นส่วนบุคคล (Privacy Right) ของประชาชนที่ต้องได้รับการคุ้มครอง อันจะทำให้ประชาชนมี ความมั่นใจในการทำธุรกรรมทางอิเล็กทรอนิกส์ ดังนั้น การคุ้มครองข้อมูลส่วนบุคคลจำเป็นที่จะต้องนำมา วิเคราะห์เพื่อให้เกิดธรรมาภิบาลข้อมูลภาครัฐที่ดี โดยมีกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล ดังนี้

(๑) พระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. ๒๕๔๐ กำหนดประเภทข้อมูลที่เปิดเผยได้และเปิดเผยไม่ได้ ซึ่งเป็นสิ่งที่จำเป็นต้องมีการพิจารณาในกรณีที่เป็นข้อมูลส่วนบุคคล เนื่องจากข้อมูลที่เป็นข้อมูลส่วนบุคคลจำเป็นต้องได้รับการคุ้มครองอย่างมีหลักเกณฑ์

(๒) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ได้มีการกำหนดหลักเกณฑ์ กลไกและมาตรการที่กำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคล

(๓) แนวปฏิบัติในการปกป้องข้อมูลที่ระบุตัวบุคคลได้ โดยให้แนวปฏิบัติสำหรับหน่วยงานในการเตรียมข้อมูลให้เหมาะสมต่อการบูรณาการข้อมูลเข้าด้วยกัน โดยการนำเสนอขั้นตอนในการดำเนินการปกป้องข้อมูลที่ระบุตัวบุคคลได้ นอกจากนั้นนำเสนอวิธีการเชื่อมโยงข้อมูลแบบรวมชุดข้อมูล (Integrated Datasets) การเชื่อมโยงข้อมูลผ่านตัว แบบข้อมูล (Data Model Market Place) และการเชื่อมโยงข้อมูลแบบกลุ่ม (Batch)

๔) การรักษาความลับของทางราชการ

การรักษาความลับทางราชการเป็นสิ่งที่จำเป็นต่อการดำเนินงานของหน่วยงานภาครัฐซึ่งเป็นการป้องกันความเสียหายที่จะเกิดขึ้นต่อภาครัฐ ทั้งในด้านความมั่นคงของรัฐ และผลประโยชน์ของชาติตลอดจนความสามารถในการพัฒนาประเทศและภาพลักษณ์ โดยมีกฎหมายที่เกี่ยวข้อง ดังนี้

(๑) พระราชบัญญัติข่าวกรองแห่งชาติ พ.ศ.๒๕๖๒ ได้กำหนดข้อมูลข่าวสารที่สำนักข่าวกรองแห่งชาติได้รับมาเนื่องจากการปฏิบัติหน้าที่ตามนี้ จะเปิดเผยมิได้ เว้นแต่เป็นการเปิดเผยต่อหน่วยข่าวกรองหน่วยงานความมั่นคง นายกรัฐมนตรี หรือตามคำสั่งศาล ที่จะนำมาพิจารณาใน ธรรมาภิบาลข้อมูลภาครัฐ

(๒) ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ และที่แก้ไขเพิ่มเติม ได้มี ข้อกำหนดที่เกี่ยวข้องกับธรรมาภิบาลข้อมูลภาครัฐ ได้แก่ กำหนดนิยามข้อมูลความลับทางราชการและกำหนด หลักเกณฑ์และวิธีการในการรักษาความลับของหน่วยงานภาครัฐ ตลอดจนขั้นตอนและกระบวนการเกี่ยวกับการ ดำเนินการต่อข้อมูลความลับทางราชการ เช่น การปรับชั้นความลับ การยกเลิกชั้นความลับ

(๓) แนวทางปฏิบัติในการรักษาความปลอดภัยเกี่ยวกับบุคคล และสถานที่ที่กำหนดไว้ในระเบียบสำนักนายกรัฐมนตรี ว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. ๒๕๕๒ ควรนำมาพิจารณาในการ ดำเนินการตามกรอบธรรมาภิบาลข้อมูลภาครัฐ

กรมการจัดหางานมีการนำกฎหมาย ระเบียบ นโยบาย หรือ พ.ร.บ. ที่เกี่ยวข้องกับเรื่องธรรมาภิบาลข้อมูลภาครัฐเพิ่มเติม ดังนี้

(๑) พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ.๒๕๖๒ กำหนดให้หน่วยงานรัฐ จัดให้มีการบริหารงานและการจัดทำบริการสาธารณะในรูปแบบและช่องทางดิจิทัลโดยมีการบริหารจัดการและบูรณาการข้อมูลภาครัฐและการทำงานให้มีความสอดคล้องกันและเชื่อมโยงเข้าด้วยกันอย่างมั่นคงปลอดภัยและมีธรรมาภิบาล โดยมุ่งหมายในการเพิ่มประสิทธิภาพและอำนวยความสะดวกในการให้บริการและเข้าถึงประชาชน ในการเปิดเผยข้อมูลภาครัฐต่อสาธารณะ และสร้างการมีส่วนร่วมของทุกภาคส่วน

(๒) พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ได้กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมและกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ต้องดำเนินการตามมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อรักษาสถานะของข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์

(๓) ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ (คธอ.) เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕ โดยกำหนดให้มีมาตรฐานการรักษา ความมั่นคงปลอดภัยการเข้าถึงข้อมูลสารสนเทศ ในระดับเคร่งครัด ระดับกลาง หรือระดับพื้นฐาน ให้หน่วยงาน หรือองค์กร หรือส่วนงานของหน่วยงานหรือองค์กรปฏิบัติตามมาตรฐาน มีการระบุถึงการตรวจสอบประวัติบุคคล และการกำหนดเขตพื้นที่หวงห้ามไว้

๕. การวัดผลการบริหารจัดการข้อมูล (Data management measurement)

การวัดผลการดำเนินงานด้านธรรมาภิบาลข้อมูลภาครัฐ เป็นกระบวนการประเมินระดับความพร้อมของกรมการจัดหางานในการบริหารจัดการข้อมูลตามหลักธรรมาภิบาล โดยผลการดำเนินงานดังกล่าวส่งผลต่อความสำเร็จของการบริหารจัดการข้อมูลในด้านคุณภาพของข้อมูล ความมั่นคงปลอดภัยของข้อมูล และการใช้ประโยชน์จากข้อมูลเพื่อสนับสนุนภารกิจของหน่วยงาน ทั้งนี้กรมการจัดหางานได้กำหนดหลักเกณฑ์การประเมินให้สอดคล้องกับบริบท และภารกิจของกรมการจัดหางาน โดยแนวทางการประเมินประกอบด้วย การประเมินความพร้อมด้านธรรมาภิบาลข้อมูล การประเมินคุณภาพของข้อมูล และการประเมินความมั่นคงปลอดภัยของข้อมูล

๕.๑ การประเมินความพร้อมของธรรมาภิบาลข้อมูลภาครัฐ (Data Governance Readiness Assessment)

การประเมินความพร้อมของธรรมาภิบาลข้อมูลภาครัฐ กรมการจัดหางานจะดำเนินการเพื่อปรับปรุงการดำเนินงานให้เกิดประสิทธิภาพสูงสุด ตามระดับความพร้อมของธรรมาภิบาลข้อมูลภาครัฐที่ได้กำหนดในการประเมินความพร้อมของธรรมาภิบาลข้อมูลภาครัฐ ซึ่งประกอบด้วย ๕ ระดับ ดังนี้

- ระดับ ๐ : None หมายถึง ไม่มีธรรมาภิบาลข้อมูลภาครัฐหรือมีแต่ไม่ได้ดำเนินการอย่างเป็น ทางการ นั่นคือ มีการดำเนินงานบางส่วนและไม่มีการประกาศให้ทราบอย่างเป็นทางการ

- ระดับ ๑ : Initial หมายถึง ไม่มีการกำหนดมาตรฐานของกระบวนการ นั่นคือ กระบวนการ ถูกกำหนดขึ้นมาเฉพาะกิจ (Adhoc) ทำให้แต่ละโครงการหรือบริการมีรูปแบบของกระบวนการที่แตกต่างกัน และอำนาจในการจัดการและธรรมาภิบาลข้อมูลส่วนใหญ่ถูกดำเนินการโดยฝ่ายเทคโนโลยีสารสนเทศทำให้การ ทำงานร่วมกันระหว่างฝ่ายธุรกิจและฝ่ายเทคโนโลยีสารสนเทศไม่สอดคล้องกัน

- ระดับ ๒ : Managed หมายถึง เริ่มมีการกำหนดมาตรฐานของกระบวนการเฉพาะแต่ละส่วนงาน หรือบริการ และมีการกำหนดบุคคลที่เกี่ยวข้องกับการกำกับติดตาม เช่น บริกรข้อมูลและเจ้าของข้อมูล

- ระดับ ๓ : Standardized หมายถึง กระบวนการถูกกำหนดเป็นมาตรฐานของหน่วยงาน มี การกำหนดส่วนงานกลางในการกำกับและติดตามข้อมูล ซึ่งมาจากบุคคลด้านธุรกิจและเทคโนโลยีสารสนเทศมี การบังคับใช้นโยบายข้อมูลครอบคลุมทั้งหน่วยงาน มีการติดตาม วิเคราะห์ และรายงานคุณภาพข้อมูลหรือ ความมั่นคงปลอดภัย

- ระดับ ๔ : Advanced หมายถึง กระบวนการถูกกำหนดเป็นมาตรฐานของหน่วยงาน มีการ กำหนดส่วนงานกลางและระบบในการกำกับและติดตามข้อมูล ซึ่งมาจากบุคคลด้านธุรกิจและเทคโนโลยี สารสนเทศมีการบังคับใช้นโยบายข้อมูลครอบคลุมทั้งหน่วยงาน มีการติดตาม วิเคราะห์ และรายงานคุณภาพ ข้อมูลและความมั่นคงปลอดภัย

- ระดับ ๕ : Optimized หมายถึง มีการดำเนินการสอดคล้องกับระดับ ๔ วิเคราะห์สาเหตุของ ปัญหา (Root Cause) ประกอบไปด้วย ความไม่สอดคล้องในการปฏิบัติงานกับนโยบายข้อมูล (Non Conformation) คุณภาพข้อมูลที่ต่ำ และความไม่คุ้มทุนในการบริหารจัดการข้อมูล โดยดำเนินการปรับปรุง กระบวนการ กฎเกณฑ์และนโยบายข้อมูลหรือโครงสร้างธรรมาภิบาลข้อมูลภาครัฐ เพื่อแก้ไขปัญหาที่พบจากผล การวิเคราะห์ และให้สอดคล้องกับความต้องการของผู้ที่เกี่ยวข้องและวัตถุประสงค์ที่เปลี่ยนไปของหน่วยงาน

ระดับ	โครงสร้างธรรมาภิบาลข้อมูลภาครัฐ	กระบวนการธรรมาภิบาลข้อมูลภาครัฐ	นโยบายข้อมูลและการตรวจสอบ	การประเมินคุณภาพข้อมูลและความมั่นคงปลอดภัย	การปรับปรุงอย่างต่อเนื่อง
๐ : None	ไม่มีหรือมีแต่ไม่เป็นทางการ	ไม่มีหรือมีแต่ไม่เป็นทางการ	ไม่มีหรือมีแต่ไม่เป็นทางการ	ไม่มีหรือมีแต่ไม่เป็นทางการ	ไม่มีหรือมีแต่ไม่เป็นทางการ
๑ : Initial	มีการกำหนดผู้กำกับดูแลอย่างไม่เป็นทางการ	กระบวนการยังไม่เป็นมาตรฐาน	ไม่มีหรือมีแต่ไม่เป็นทางการ	ไม่มีหรือมีแต่ไม่เป็นทางการ	ไม่มีหรือมีแต่ไม่เป็นทางการ
๒ : Managed	มีการกำหนดผู้กำกับดูแลในแต่ละส่วนงาน/บริการ	มีกระบวนการเป็นมาตรฐานส่วนงาน/บริการ	บังคับใช้ในส่วนงาน/บริการ	ไม่มีหรือมีแต่ไม่เป็นทางการ	ไม่มีหรือมีแต่ไม่เป็นทางการ
๓ : Standardized	มีส่วนงานกลางในธรรมาภิบาลข้อมูล ซึ่งประกอบไปด้วยบุคคลด้านธุรกิจและเทคโนโลยีสารสนเทศ	มีกระบวนการเป็นมาตรฐานหน่วยงาน	บังคับใช้ทั้งหน่วยงาน	ประเมินคุณภาพข้อมูลหรือความมั่นคงปลอดภัย	ไม่มีหรือมีแต่ไม่เป็นทางการ
๔ : Advanced	มีส่วนงานกลางในธรรมาภิบาลข้อมูล ซึ่งประกอบไปด้วยบุคคลด้านธุรกิจและเทคโนโลยีสารสนเทศ	มีกระบวนการเป็นมาตรฐานหน่วยงาน	บังคับใช้ทั้งหน่วยงาน	ประเมินคุณภาพข้อมูลและความมั่นคงปลอดภัย	ไม่มีหรือมีแต่ไม่เป็นทางการ
๕ : Optimized	มีส่วนงานกลางในธรรมาภิบาลข้อมูล ซึ่งประกอบไปด้วยบุคคลด้านธุรกิจและเทคโนโลยีสารสนเทศ	มีกระบวนการเป็นมาตรฐานหน่วยงาน	บังคับใช้ทั้งหน่วยงาน	ประเมินคุณภาพข้อมูลและความมั่นคงปลอดภัย	มีการปรับปรุงกระบวนการอย่างต่อเนื่อง

ตารางที่ ๔ ระดับความพร้อมของธรรมาภิบาลข้อมูลภาครัฐ

๕.๒ การประเมินคุณภาพของข้อมูล (Data Quality Assessment)

การประเมินคุณภาพของข้อมูล กรมการจัดหางานได้กำหนดการตรวจสอบผลลัพธ์หรือความสำเร็จตามองค์ประกอบในการประเมินคุณภาพข้อมูลของธรรมาภิบาลข้อมูลภาครัฐ โดยมีองค์ประกอบ ดังนี้

๑) ความถูกต้อง และสมบูรณ์ (Accuracy and Completeness) หมายความว่า ข้อมูลมี ความถูกต้องแม่นยำสูง มีความครบถ้วนสมบูรณ์ของข้อมูลที่เก็บรวบรวมมา และมีการตรวจสอบความถูกต้อง ระหว่างข้อมูลในส่วนต่าง ๆ ในทุกขั้นตอน เพื่อให้ข้อมูลถูกต้องเชื่อถือได้และให้ผลลัพธ์ตรงตามความต้องการ ผู้ใช้ (ข้อมูลครบถ้วน ข้อมูลไม่ขาดหาย กว้างพอและลึกพอสำหรับการใช้งาน)

๒) ความสอดคล้องกัน (Consistency) หมายความว่า ข้อมูลมีความสอดคล้องกันของ แนวคิด คำนิยาม วิธีการรหัส และการนำเสนอที่ทำให้ข้อมูลจากต่างแหล่ง ต่างเวลา สามารถเปรียบเทียบข้ามช่วงเวลา และบูรณาการข้อมูลเพื่อใช้ประโยชน์ร่วมกันได้

๓) ความเป็นปัจจุบัน (Timeliness) หมายความว่า ข้อมูลเป็นปัจจุบันทันสมัยเพียงพอต่อการ ใช้งานและพร้อมใช้งานตามที่กำหนดและในกรอบเวลาที่กำหนดไว้ หรือมีข้อมูลทันต่อการใช้งานทุกครั้งตามที่ ผู้ใช้ต้องการ

๔) ตรงตามความต้องการของผู้ใช้ (Relevancy) หมายความว่า ข้อมูลสามารถนำไปใช้ได้กับ งานที่ทำอยู่ เป็นข้อมูลที่ผู้ใช้งานต้องการ หรือเป็นข้อมูลที่จำเป็นต้องทราบ มีมุมมองและความละเอียด เพียงพอต่อการนำไปใช้งาน

๕) ความพร้อมใช้ (Availability) หมายความว่า ข้อมูลเข้าถึงได้ง่าย หรือมีข้อมูลนั้นอยู่ สามารถใช้งานได้จริง และสามารถใช้งานได้ตลอดเวลา

รูปที่ ๙ องค์ประกอบในการประเมินคุณภาพข้อมูล

๕.๓ การประเมินความมั่นคงปลอดภัยของข้อมูล (Data Security Assessment)

กรมการจัดหางานได้กำหนดหลักเกณฑ์การประเมินความมั่นคงปลอดภัยของข้อมูล เพื่อเป็นการวัดความสำเร็จจากธรรมาภิบาลข้อมูลภาครัฐ โดยใช้หลักเกณฑ์ในด้านต่าง ๆ ดังนี้

๑) จัดทำนโยบายด้านความมั่นคงปลอดภัยของข้อมูลที่รวมถึงการป้องกันข้อมูลในบริบทของการ รักษาความลับ ความถูกต้องของข้อมูล ความพร้อมใช้งานของข้อมูล

๒) ข้อมูลมีการจัดระดับชั้นข้อมูล (Data Classification) ข้อมูลควรมีการจำแนกชั้นของข้อมูลใน บริบทของการรักษาความปลอดภัยข้อมูลตามระดับของความอ่อนไหวและผลกระทบที่จะเกิดขึ้นต่อบุคคล องค์กร และประเทศ หากมีการเปิดเผย เปลี่ยนแปลง หรือทำลายข้อมูลโดยไม่ได้รับอนุญาต

๓) กำหนดมาตรการควบคุมและป้องกันการเข้าถึงข้อมูล (Data Protection) การกำหนดมาตรการ ควบคุมและป้องกันการเข้าถึงข้อมูลต้องคำนึงถึงระดับชั้นข้อมูล เช่น ข้อมูลที่มีความอ่อนไหวต้องมีการกำหนดมาตรการควบคุมและป้องกันการเข้าถึงข้อมูลแบบพิเศษ เพื่อป้องกันการเข้าถึงเพื่อเปิดเผยข้อมูลที่อ่อนไหวนั้น รวมถึงเพื่อป้องกันการดัดแปลงแก้ไขแต่งเติมข้อมูลโดยไม่ได้รับอนุญาต

๔) ข้อมูลถูกใช้งานอย่างเหมาะสม การนำข้อมูลไปใช้ควรดำเนินการให้สอดคล้องกับสัญญาอนุญาต และไม่ขัดต่อกฎหมาย

๕) ข้อมูลต้องมีความพร้อมใช้อยู่เสมอ ต้องมีการดำเนินการเตรียมความพร้อมไม่ว่าข้อมูลจะอยู่ใน ประเภทใดก็ตาม เช่น ข้อมูลในรูปแบบกระดาษต้องมีสถานที่จัดเก็บดูแล และสามารถเข้าถึงโดยผู้มีสิทธิได้ อย่างสม่ำเสมอ ข้อมูลในรูปแบบอิเล็กทรอนิกส์ต้องมีการเตรียมความพร้อมเรื่องระบบงาน การสำรองข้อมูล รวมถึงมีแผนการดำเนินการในกรณีฉุกเฉินใด ๆ ที่อาจมีผลต่อการใช้ข้อมูลด้วย

๖. การจำแนกข้อมูลและหมวดหมู่ของข้อมูล (Data and Data Categories)

ข้อมูล คือ “ข้อเท็จจริงซึ่งใช้เป็นพื้นฐานสำหรับการอธิบายเหตุผล การสนทนา หรือการคำนวณ” (Australian Institute of Health and Welfare, ๒๐๑๔) ข้อมูลจัดเป็นองค์ประกอบหลักในการขับเคลื่อน หน่วยงาน ซึ่งมีความสัมพันธ์กับกระบวนการปฏิบัติงาน เทคโนโลยีสารสนเทศ สถานที่ รวมถึงบุคลากร ข้อมูลจึงเปรียบเสมือนทรัพย์สินที่มีความสำคัญเช่นเดียวกับทรัพย์สินประเภทอื่น ดังนั้นหน่วยงานจึง จำเป็นต้องมีมาตรการในการรักษาความมั่นคงปลอดภัยและคุณภาพของข้อมูล เช่น การรักษาความลับของข้อมูล (Confidentiality) การป้องกันไม่ให้เกิดเหตุการณ์ที่ทำให้ไม่สามารถใช้งานข้อมูลได้ (Loss of Availability) การ รักษาความถูกต้องครบถ้วนของข้อมูล (Integrity) การทำให้ข้อมูลเป็นปัจจุบันอยู่เสมอ (Timeliness) ทั้งนี้ เพื่อ ตอบสนองต่อการตัดสินใจทั้งในระดับปฏิบัติการและระดับยุทธศาสตร์ได้อย่างมีประสิทธิภาพมากยิ่งขึ้น

๖.๑ ประเภทข้อมูล (Types of Data)

ข้อมูลถูกจัดแบ่งออกได้เป็น ๓ ประเภท ดังนี้

๑) ข้อมูลที่มีโครงสร้าง (Structured Data) เป็นข้อมูลที่มีการนิยามโครงสร้างของข้อมูลไว้ โดย นิยามความหมายและคุณสมบัติของแต่ละฟิลด์ข้อมูล โครงสร้างมีชั้นเดียวทำให้ง่ายต่อการค้นหา เช่น ตารางข้อมูลในฐานข้อมูล หรือข้อมูลในรูปแบบ CSV (Comma-Separated Values) ไฟล์

๒) ข้อมูลกึ่งโครงสร้าง (Semi-structured Data) เป็นข้อมูลที่มีการนิยามโครงสร้างของข้อมูลไว้ แต่โครงสร้างเป็นแบบลำดับขั้น (Hierarchy) เช่น Extensible Markup Language - XML JavaScript Object Notation – JSON

๓) ข้อมูลที่ไม่มีโครงสร้าง (Unstructured Data) เป็นข้อมูลที่ไม่ได้มีการนิยามโครงสร้างของข้อมูลไว้มักจะอยู่ในรูปแบบ เช่น ข้อความ รูปภาพ เสียง วีดิทัศน์

รูปที่ ๑๐ ประเภทข้อมูล

๖.๒ ชุดข้อมูล (Datasets)

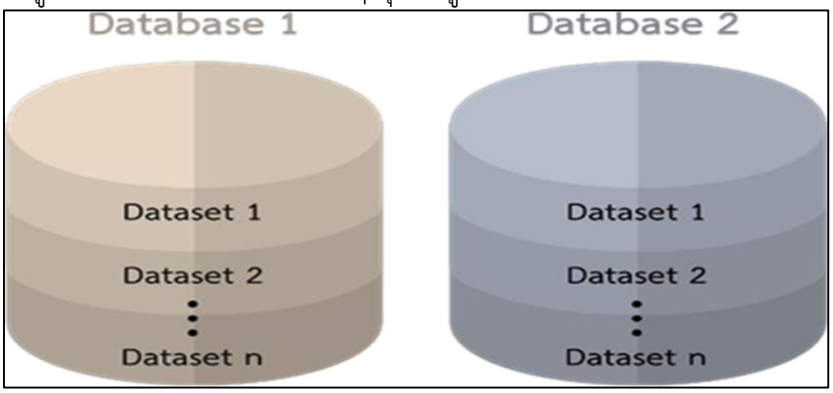
ชุดข้อมูล คือ การนำข้อมูลจากหลายแหล่งมารวบรวม เพื่อจัดเป็นชุดให้ตรงตามลักษณะโครงสร้างของข้อมูลหรือจากการใช้ประโยชน์ของข้อมูล ดังแสดงตัวอย่างชุดข้อมูลแรงงานในรูปแบบตารางข้อมูลหรือ ข้อมูลที่มีโครงสร้าง (Structured Data) มีทั้งหมด ๓ แถว ๕ ฟิลด์ (Data Field/Element/Attribute) ได้แก่ ชื่อ นามสกุล เพศ อายุ และตำแหน่งงาน

ชื่อ	นามสกุล	เพศ	อายุ	ตำแหน่งงาน
วิชัย	ใจดี	ชาย	๒๖	คอมพิวเตอร์
พิเชษฐ์	วิเศษศิลป์	ชาย	๒๘	บัญชี
วิมลมาส	วงศ์สกุล	หญิง	๒๕	การตลาด

ตารางที่ ๕ ตัวอย่างชุดข้อมูลแรงงาน

๖.๓ ฐานข้อมูล (Database)

ฐานข้อมูล คือ “กลุ่มข้อมูลที่มีความสัมพันธ์กันได้ถูกรวบรวมเข้าไว้ด้วยกัน ซึ่งสนับสนุนกิจกรรมของ หน่วยงาน” หรือกล่าวได้ว่าแต่ละฐานข้อมูลจะประกอบไปด้วย หลาย ๆ ชุดข้อมูลที่มีความสัมพันธ์กัน



รูปที่ ๑๑ ความสัมพันธ์ระหว่างฐานข้อมูลกับชุดข้อมูล

๖.๔ หมวดหมู่ของข้อมูล (Data Category)

ข้อมูลแบ่งออกได้เป็น ๕ หมวดหมู่ ดังนี้

๑) ข้อมูลสาธารณะ (Public Data) หมายความว่า ข้อมูลที่สามารถเปิดเผยได้ สามารถนำไปใช้ได้อย่างอิสระ ไม่ว่าจะเป็นข้อมูลข่าวสาร ข้อมูลส่วนบุคคล ข้อมูลอิเล็กทรอนิกส์ เป็นต้น

๒) ข้อมูลใช้ภายใน (Internal Use Only) หมายความว่า ข้อมูลสำหรับใช้ในการดำเนินกิจการภายในของหน่วยงาน ซึ่งไม่อนุญาตให้นำไปใช้งานภายนอกก่อนได้รับอนุญาตจากเจ้าของข้อมูล เช่น ร่างนโยบาย ร่าง มาตรฐาน และขั้นตอนการปฏิบัติงาน ประกาศ และบันทึกภายในหน่วยงานที่อยู่ระหว่างการขออนุมัติ เป็นต้น

๓) ข้อมูลส่วนบุคคล (Personal Data) หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม (หมายเหตุ ในกรณีที่ต้องดำเนินการตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลตามวัตถุประสงค์ของกฎหมายจะไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ)

๔) ข้อมูลความลับทางราชการ (Classified Information) หมายความว่า ข้อมูลข่าวสารตามมาตรา ๑๔ หรือมาตรา ๑๕ แห่งพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐ ที่มีคำสั่งไม่ให้เปิดเผยและอยู่ ในความครอบครองหรือควบคุมดูแลของหน่วยงานของรัฐ ไม่ว่าจะเป็นเรื่องที่เกี่ยวกับการดำเนินงานของรัฐ หรือที่เกี่ยวกับเอกชน ซึ่งมีการกำหนด ให้มีชั้นความลับเป็น ชั้นลับ ชั้นลับมาก หรือ ชั้นลับที่สุด ตามระเบียบว่า ด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ และที่แก้ไขเพิ่มเติม โดยคำนึงถึงการปฏิบัติหน้าที่ของ หน่วยงานของรัฐและประโยชน์แห่งรัฐประกอบกัน

๕) ข้อมูลความมั่นคง (National Security Information) หมายความว่า ข้อมูลภายใต้กรอบความ มั่นคงแห่งชาติ หรือ ภาวะที่ประเทศปลอดจากภัยคุกคามต่อเอกราช อธิปไตยบูรณภาพแห่งอาณาเขต สถาบัน ศาสนา สถาบันพระมหากษัตริย์ ความปลอดภัยของประชาชน การดำรงชีวิต โดยปกติสุขของประชาชน หรือที่ กระทบต่อผลประโยชน์แห่งชาติหรือการปกครองระบอบประชาธิปไตย อันมีพระมหากษัตริย์ทรงเป็นประมุข รวมทั้งความพร้อมของประเทศที่จะเผชิญสถานการณ์ต่าง ๆ อันเกิดจากภัยคุกคามทุกรูปแบบ และครอบคลุม ด้านความมั่นคงปลอดภัยของประเทศ (National Security) ในมิติเศรษฐกิจ อาหาร สุขภาพ สิ่งแวดล้อมและ สิทธิมนุษยชน ส่วนบุคคล ชุมชน การเมือง และการต่างประเทศ ที่สอดคล้องตามเป้าหมายของนโยบายและ แผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ

รูปที่ ๑๒ หมวดหมู่ของข้อมูล

๗. คำอธิบายชุดข้อมูล (Metadata) และบัญชีข้อมูลภาครัฐ (Government Data Catalog)

๗.๑ คำอธิบายชุดข้อมูลดิจิทัล หรือเมทาดาตา (Metadata)

คำอธิบายชุดข้อมูลดิจิทัล หรือเมทาดาตา คือ “ข้อมูลที่ใช้กำกับและอธิบายข้อมูลหลักหรือกลุ่มของข้อมูลอื่น” แบ่งออกเป็น ๒ กลุ่ม ดังนี้

๑) เมทาดาตาเชิงธุรกิจ (Business Metadata) ซึ่งให้รายละเอียดของชุดข้อมูล (Datasets) ในด้านภารกิจงาน เหมาะสำหรับผู้ใช้งานข้อมูล (Data User) นักวิเคราะห์ข้อมูล (Data Analyst) และนักวิทยาการข้อมูล (Data Scientist) ตัวอย่างรายการเมทาดาตาเชิงธุรกิจ เช่น ชื่อข้อมูล ชื่อเจ้าของข้อมูล คำสำคัญ คำอธิบายอย่างย่อ วันที่เริ่มต้นใช้งาน วันที่ทำการเปลี่ยนแปลงข้อมูล ภาษาที่ใช้ ชื่อฟิลด์ข้อมูล (เช่น ชื่อพนักงาน นามสกุล เพศ) ซึ่งไม่รวมชื่อฟิลด์ข้อมูล เนื่องจากชื่อฟิลด์ข้อมูลของแต่ละชุดข้อมูลมีความแตกต่างกัน สามารถ ศึกษาข้อมูลเพิ่มเติมได้ที่ มรด. ๓-๑ : ๒๕๖๕ มาตรฐานรัฐบาลดิจิทัลว่าด้วยแนวทางการจัดทำบัญชีข้อมูลภาครัฐ

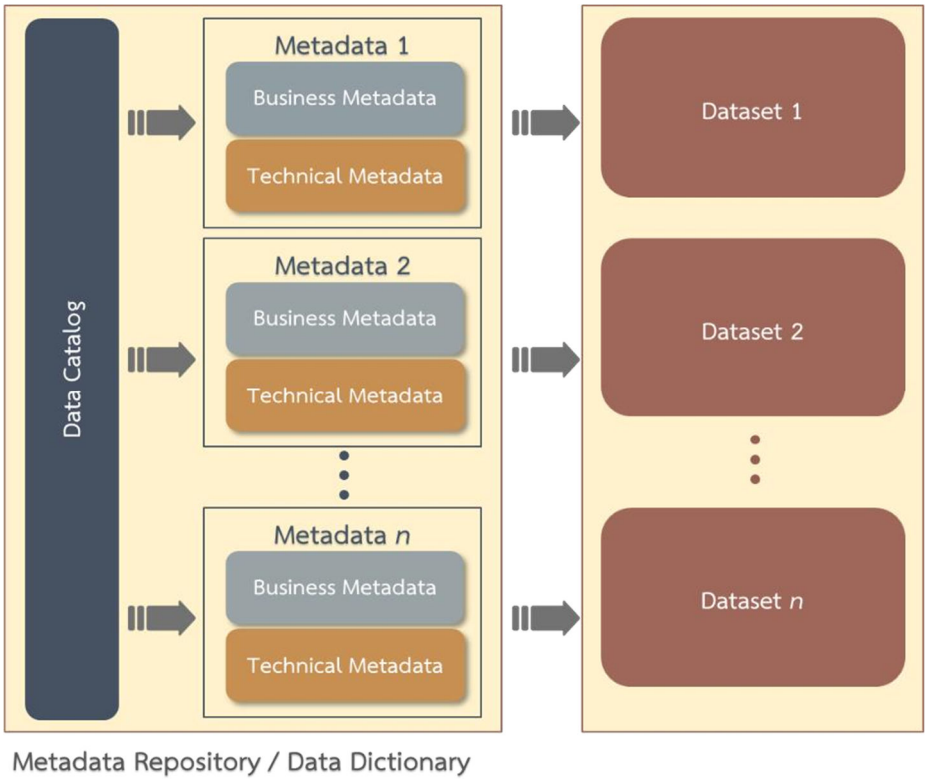
๒) เมทาดาตาเชิงเทคนิค (Technical Metadata) ซึ่งให้รายละเอียดของชุดข้อมูล (Datasets) ใน ด้านเทคนิค (Technical) และปฏิบัติการ (Operational) เหมาะสำหรับผู้บริหารจัดการฐานข้อมูล (Database Administrator) ตัวอย่างรายการเมทาดาตาเชิงเทคนิค เช่น ชื่อตารางข้อมูลในฐานข้อมูล ชื่อฟิลด์ข้อมูลใน ตารางข้อมูล ประเภทข้อมูล (เช่น ตัวเลข ตัวหนังสือ หรือวันที่) ความกว้างของฟิลด์ข้อมูล (เช่น ๑๐ ตัวอักษร ๕๐ ตัวอักษร หรือ ๑๐๐ ตัวอักษร) คีย์ข้อมูล (Primary Key หรือ Foreign Key) รวมไปถึงข้อมูลสำหรับการ สำรองข้อมูล (Backup) และกู้คืนข้อมูล (Restore)

๗.๒ บัญชีข้อมูล (Data Catalog)

บัญชีข้อมูล คือ “รายการของชุดข้อมูลที่หน่วยงานถือครองหรือบริหารจัดการ” (Australian Institute of Health and Welfare, ๒๐๑๔) ซึ่งรายการของชุดข้อมูลที่จำแนกแยกแยะโดยการจัดกลุ่ม หรือ จัดประเภทข้อมูลที่อยู่ในความครอบครองหรือควบคุมของหน่วยงาน สามารถจัดเตรียมได้ในรูปแบบของตาราง รายชื่อชุดข้อมูล รายงาน หรือแอปพลิเคชัน บัญชีข้อมูลถูกใช้เพื่ออำนวยความสะดวกในการค้นหาชุดข้อมูล (Datasets) หรือเมทาดาตา (Metadata) ซึ่งเป็นประโยชน์ต่อผู้ที่เกี่ยวข้องกับข้อมูล เช่น ผู้ใช้งานข้อมูล (Data User) ใช้สำหรับการค้นหาข้อมูลที่ต้องการใช้งาน นักวิเคราะห์ข้อมูล (Data Analyst) และนักวิทยาการข้อมูล (Data Scientist) ใช้สำหรับการค้นหาข้อมูลที่ต้องการวิเคราะห์หรือประมวลผล บริกรข้อมูล (Data Stewards) ใช้สำหรับการค้นหาข้อมูลที่ต้องการตรวจสอบการปฏิบัติตามนโยบายข้อมูล (Data Policy Compliance) คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council) ใช้สำหรับการค้นหาข้อมูลที่ต้องการตัดสินใจหรือแก้ไขปัญหาเกี่ยวกับข้อมูลในระดับนโยบาย

๗.๓ คลังเมทาดาตา (Metadata Repository)

คลังเมทาดาตา หรือพจนานุกรมข้อมูลเป็นเครื่องมือในการรวบรวมและจัดเก็บเมทาดาตา เพื่อสนับสนุนให้ผู้ที่ต้องการใช้ข้อมูลสามารถค้นหาและเข้าถึงได้โดยสะดวก อย่างไรก็ตามผู้ที่มีสิทธิในการเข้าถึง ควรได้รับสิทธิ์ที่แตกต่างกันขึ้นอยู่กับบทบาทและความรับผิดชอบ เช่น ผู้ใช้งานข้อมูลสามารถเข้าถึงได้เฉพาะ เมทาดาตาเชิงธุรกิจ ขณะที่บริกรข้อมูลสามารถเข้าถึงได้ทั้งเมทาดาตาเชิงธุรกิจและเมทาดาตาเชิงเทคนิค โดย ความสัมพันธ์ระหว่างบัญชีข้อมูล เมทาดาตา คลังเมทาดาตา และชุดข้อมูล แสดงได้ดังรูป



รูปที่ ๑๓ ความสัมพันธ์ระหว่างบัญชีข้อมูล เมทาดาตา คลังเมทาดาตา และชุดข้อมูล

จากรูปบัญชีข้อมูลเปรียบเสมือนสารบัญ เมนู หรือตัวชี้ไปยังเมทาดาตาที่ถูกจัดเก็บอยู่ใน คลังเมทาดาตา โดยเมทาดาตาจะให้รายละเอียดต่าง ๆ ที่เกี่ยวข้องกับชุดข้อมูลนั้น ๆ ทั้งนี้คลังเมทาดาตา หรือ พจนานุกรมข้อมูลมักจะถูกพัฒนาให้อยู่ในรูปแบบของซอฟต์แวร์

๗.๔ รายละเอียดคำอธิบายชุดข้อมูลหรือเมทาดาตา (Metadata)

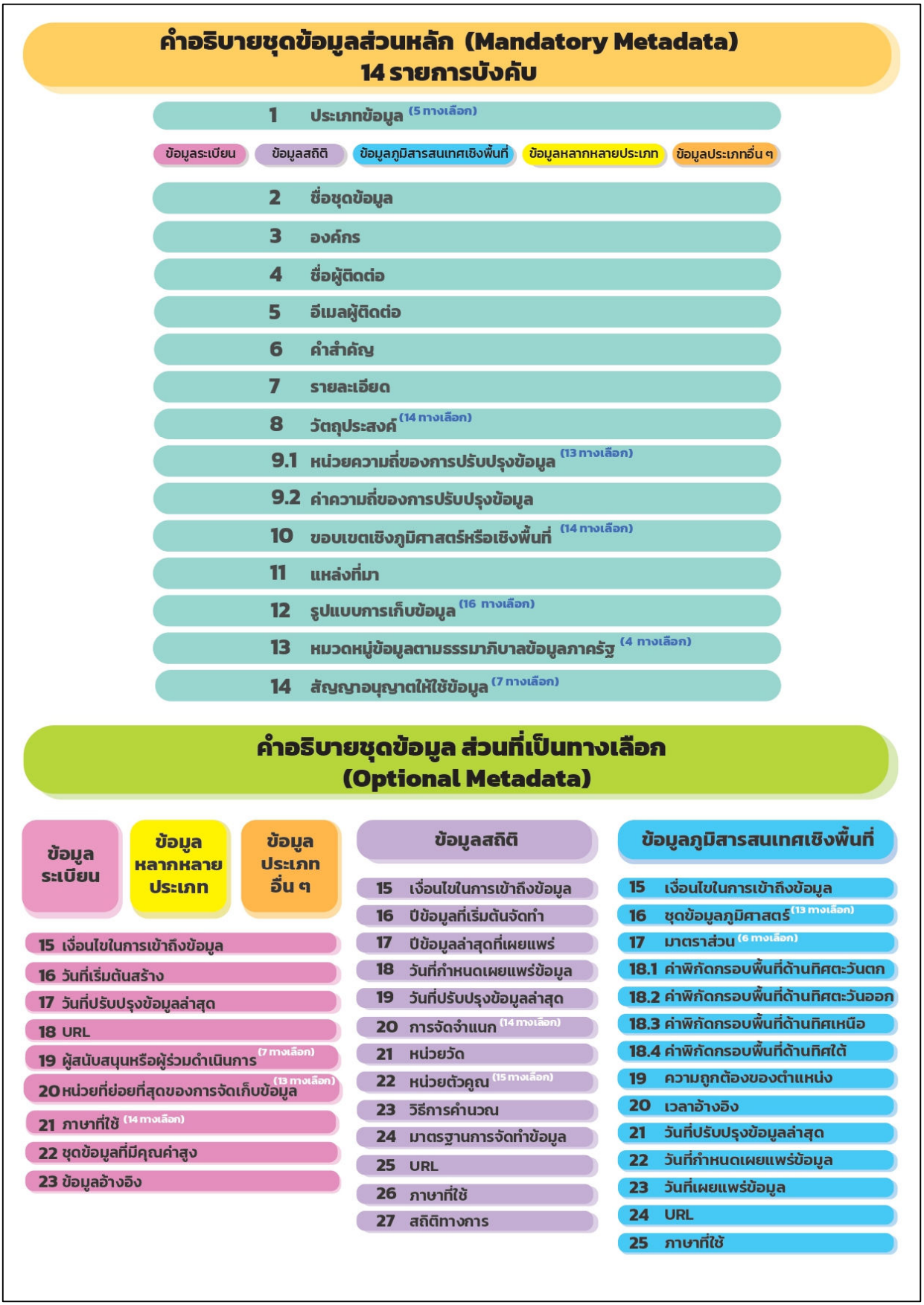
สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ร่วมกับ สำนักงานสถิติแห่งชาติ และสถาบันส่งเสริมการวิเคราะห์และบริหารข้อมูลขนาดใหญ่ภาครัฐ ได้ออกแบบมาตรฐานขั้นต่ำอ้างอิงตาม ISO/IEC ๑๑๑๗๙ และ Dublin Core Metadata Initiative (DCMI) และแผ่นแบบ (Template) เอกสาร ซึ่งเป็นการกำหนดมาตรฐานเมทาดาตาสำหรับชุดข้อมูลภาครัฐ เพื่อให้หน่วยงานภาครัฐนำมาตรฐานดังกล่าวไปใช้จัดทำบัญชีข้อมูลของหน่วยงานได้อย่างสอดคล้องกัน ดังนี้

๑) คำอธิบายชุดข้อมูลส่วนหลัก (Mandatory Metadata) เป็นรายละเอียดคำอธิบายชุดข้อมูลส่วนหลักที่ทุกชุดข้อมูลจำเป็นต้องมี โดย ๑ ชุดข้อมูล ประกอบด้วยคำอธิบายข้อมูลจำนวน ๑๔ รายการ ได้แก่ ประเภทข้อมูล ชื่อชุดข้อมูลองค์กร ชื่อผู้ติดต่อ อีเมลผู้ติดต่อ คำสำคัญ รายละเอียด วัตถุประสงค์ ความถี่ของการปรับปรุงข้อมูล ขอบเขตเชิงภูมิศาสตร์หรือเชิงพื้นที่ แหล่งที่มา รูปแบบในการเก็บข้อมูล หมวดหมู่ข้อมูลตามธรรมาภิบาลข้อมูลภาครัฐ และสัญญาอนุญาตให้ใช้ข้อมูล

๒) คำอธิบายชุดข้อมูลทางเลือก (Optional Metadata) เป็นส่วนของรายละเอียดคำอธิบายชุดข้อมูลเพิ่มเติมที่ช่วยให้รายละเอียดของคำอธิบายชุดข้อมูลมีความสมบูรณ์มากยิ่งขึ้น

๓) พจนานุกรมข้อมูล (Data Dictionary) เป็นส่วนหนึ่งของเมทาดาตาที่มีหน้าที่อธิบายข้อมูลภายในชุดข้อมูลอย่างละเอียดเป็นรายตัวแปร (Attribute) เพื่อสนับสนุนให้ผู้ที่ต้องการใช้ข้อมูลสามารถเข้าใจชุดข้อมูลในระดับตัวแปร มีประโยชน์ในการตัดสินใจว่าชุดข้อมูลนั้นมีข้อมูลตามที่ผู้ต้องการใช้กำลังค้นหาอยู่หรือไม่ โดยมีส่วนที่บังคับต้องทำการอธิบายข้อมูลรายตัวแปร ๓ รายการ ได้แก่ ชื่อตัวแปรข้อมูล ชนิดของตัวแปรข้อมูล และคำอธิบายตัวแปรข้อมูล

ในการจัดทำบัญชีข้อมูล (Data Catalog) นี้ กำหนดให้หน่วยงานจัดทำคำอธิบายชุดข้อมูลส่วนหลัก (Mandatory Metadata) ซึ่งเป็นส่วนที่บังคับต้องทำการอธิบายชุดข้อมูล โดยอาจทำคำอธิบายชุดข้อมูลตามข้อ ๒ และ ข้อ ๓ ด้วยหรือไม่ก็ได้

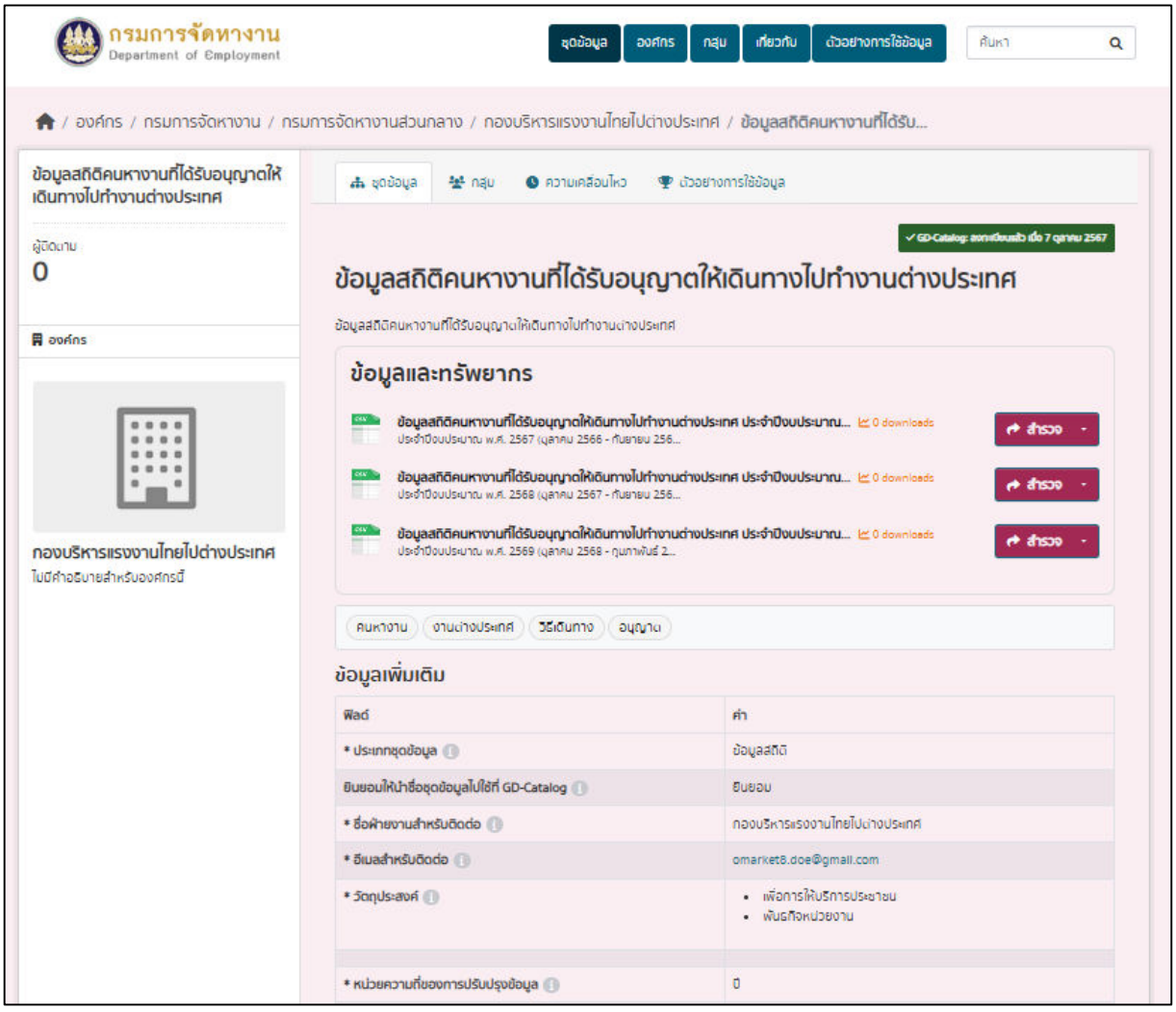


รูป ๑๔ แสดงคำอธิบายชุดข้อมูลหรือเมทาดาตา (Metadata)

๗.๕ บัญชีข้อมูลภาครัฐ (Government Data Catalog)

กรมการจัดหางานจัดทำบัญชีข้อมูลภาครัฐ (Government Data Catalog) เพื่อรวบรวมและจัดทำรายการชุดข้อมูลที่อยู่ในความรับผิดชอบของกรมการจัดหางาน สำหรับสนับสนุนการเปิดเผยข้อมูลภาครัฐ (Open Data) ตลอดจนการแลกเปลี่ยนและเชื่อมโยงข้อมูลระหว่างหน่วยงาน ทั้งนี้ เพื่ออำนวยความสะดวกให้หน่วยงานภาครัฐ ภาคเอกชน และประชาชน สามารถค้นหา เข้าถึง และนำข้อมูลไปใช้ประโยชน์ได้อย่างเหมาะสม โดยได้กำหนดคำอธิบายข้อมูล (Metadata) และรายละเอียดของชุดข้อมูลไว้อย่างชัดเจน เพื่อให้การบริหารจัดการข้อมูลของหน่วยงานเป็นไปอย่างมีประสิทธิภาพ และสอดคล้องกับหลักธรรมาภิบาลข้อมูลภาครัฐ โดยมีการเผยแพร่ผ่านบัญชีข้อมูลภาครัฐ (Government Data Catalog) ของกรมการจัดหางาน

บัญชีข้อมูลของกรมการจัดหางานต้องครอบคลุมชุดข้อมูลที่เกี่ยวข้องกับภารกิจหลักของหน่วยงาน ได้แก่ ข้อมูลด้านการส่งเสริมการมีงานทำ การให้บริการจัดหางานภายในประเทศ การจัดหางานไปทำงานต่างประเทศ การคุ้มครองคนหางาน การบริหารจัดการแรงงานต่างด้าว ข้อมูลข่าวสารตลาดแรงงาน ข้อมูลสถิติด้านการจ้างงาน รวมทั้งข้อมูลอื่นที่เกี่ยวข้องกับการดำเนินงานของกรมการจัดหางาน ทั้งนี้กรมการจัดหางานได้เริ่มต้นจัดทำชุดข้อมูลไว้ ๑๘ ชุดข้อมูล



รูป ๑๕ ตัวอย่างชุดข้อมูลในบัญชีข้อมูลภาครัฐ (Government Data Catalog) ของกรมการจัดหางาน

๘. แนวปฏิบัติตามนโยบายธรรมาภิบาลข้อมูลกรมการจัดหางาน

๘.๑ แนวปฏิบัติตามนโยบายฯ หมวดทั่วไป

เพื่อกำหนดแนวทางการดำเนินงานด้านธรรมาภิบาลข้อมูลของหน่วยงาน โดยการกำหนดนโยบายข้อมูลถือเป็นองค์ประกอบสำคัญตามกรอบธรรมาภิบาลข้อมูล เพื่อให้การบริหารจัดการข้อมูลเป็นไปอย่างมีประสิทธิภาพ โปร่งใส และตรวจสอบได้ จึงต้องมีการกำหนดนโยบายข้อมูลอย่างชัดเจน ให้สอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง หรือข้อกำหนดที่เกี่ยวข้อง โดยต้องได้รับความเห็นชอบจากผู้บริหาร และมีการเผยแพร่ สื่อสารให้เจ้าหน้าที่และผู้ที่เกี่ยวข้องรับทราบ รวมทั้งมีการทบทวนนโยบายอย่างสม่ำเสมอ เพื่อให้สามารถนำไปปฏิบัติได้อย่างมีประสิทธิภาพและต่อเนื่อง โดยกำหนดแนวปฏิบัติตามนโยบาย ดังนี้

๑ กำหนดให้มีโครงสร้างกำกับดูแลข้อมูล และกำหนดบทบาทหน้าที่ความรับผิดชอบในการบริหารจัดการข้อมูล

๒ บุคคลหรือหน่วยงานภายในให้ทำหน้าที่เป็นเจ้าของข้อมูล (Data Owner) เพื่อรับผิดชอบการบริหารจัดการข้อมูลของหน่วยงาน

๓ กำหนดนโยบายและมาตรการด้านความมั่นคงปลอดภัยของข้อมูล โดยให้ปฏิบัติตามแนวทางเอกสารการแจ้งเตือนและแนะนำแนวทางป้องกันความเสี่ยงทางไซเบอร์กรณีข้อมูลส่วนบุคคลรั่วไหล (Data Leak) ของสำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เพื่อป้องกันการเข้าถึง การสูญหาย การทำลาย หรือการเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต

๔ กำหนดมาตรฐานข้อมูล (Data Standard) และแนวปฏิบัติในการบริหารจัดการเมทาดาตา (Metadata) หรือคำอธิบายชุดข้อมูล โดยครอบคลุมบทบาทหน้าที่ กระบวนการจัดทำ การกำกับดูแล และการตรวจสอบความถูกต้องของเมทาดาตา

๕ นำเครื่องมือและเทคโนโลยีสารสนเทศเข้ามาช่วยในการบริหารจัดการข้อมูล

๖ เผยแพร่นโยบายข้อมูลให้กับผู้ที่เกี่ยวข้องทั้งภายในองค์กร และภายนอกองค์กร

๗ จัดฝึกอบรมเพื่อสร้างความตระหนักด้านธรรมาภิบาลข้อมูลภาครัฐและการบริหารจัดการข้อมูล โดยครอบคลุมกระบวนการบริหารจัดการข้อมูลและวงจรชีวิตข้อมูล (Data Lifecycle)

๘ การดำเนินงานด้านธรรมาภิบาลข้อมูล พร้อมทั้งติดตามและรายงานผลการดำเนินงานอย่างน้อยปีละ ๑ ครั้ง เพื่อนำไปปรับปรุงการดำเนินงานให้มีประสิทธิภาพยิ่งขึ้น

๙ ตรวจสอบความสอดคล้องระหว่างนโยบายข้อมูลกับการดำเนินงานของผู้มีส่วนได้ส่วนเสียอย่างน้อยปีละ ๑ ครั้ง

๑๐ ทบทวนและปรับปรุงนโยบายข้อมูลอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีความจำเป็น เพื่อให้เหมาะสมกับสภาพแวดล้อม และการดำเนินงานของหน่วยงานอย่างต่อเนื่อง

๘.๒ แนวปฏิบัติตามนโยบายฯ หมวดการจัดการข้อมูลตามวงจรชีวิตของข้อมูล (Data Life Cycle)

เพื่อให้การสร้างข้อมูล การจัดเก็บรักษาข้อมูล ตลอดจนไปจนถึงการทำลายข้อมูล ตามการจัดการข้อมูลตามวงจรชีวิตของข้อมูล (Data Life Cycle) เป็นไปอย่างมีประสิทธิภาพและมีการควบคุมคุณภาพข้อมูล สำหรับการใช้ประโยชน์จากข้อมูลในการบริหารงานและการให้บริการของกรมการจัดหางาน โดยเป็นไปตามอำนาจหน้าที่และวัตถุประสงค์ในการดำเนินงานของกรมการจัดหางาน รวมถึงการกำหนดแนวทางในการบริหารจัดการความมั่นคงปลอดภัยของข้อมูลและความเป็นส่วนบุคคล ซึ่งจะต้องสอดคล้องกับนโยบายความมั่นคงปลอดภัยสารสนเทศและนโยบายคุ้มครองข้อมูลส่วนบุคคลของกรมการจัดหางาน โดยมีแนวปฏิบัติตามนโยบาย ดังนี้

๑ สร้างชุดข้อมูลที่พิจารณาถึงความสำคัญตามภารกิจงาน ประโยชน์จากข้อมูล และมุมมองการนำไปใช้งานเพื่อให้เกิดประโยชน์สูงสุดในการใช้ข้อมูล

๒ กำหนดข้อมูลมาตรฐาน (Standard Data) เพื่อใช้เป็นข้อมูลอ้างอิง (Data Reference) ของหน่วยงาน โดยรูปแบบและโครงสร้างข้อมูลให้เป็นมาตรฐานเดียวกัน เพื่อให้สามารถใช้ข้อมูลร่วมกันได้อย่างถูกต้องและสอดคล้องกัน เช่น มาตรฐานข้อมูลด้านเพศ ศาสนา ระดับการศึกษา และสถานภาพสมรส เป็นต้น ทั้งนี้กรมการจัดหางานได้มีกำหนดชุดข้อมูลมาตราฐาน (Standard Data) ไว้ที่รายการ API ของระบบ Data LakeHouse ของกรมการจัดหางาน

๓ จัดเก็บและรวบรวมข้อมูล (Data Collection) ให้สอดคล้องกับวัตถุประสงค์ในการนำข้อมูลไปใช้ประโยชน์ในการดำเนินงานของหน่วยงาน โดยกรณีที่เป็นข้อมูลส่วนบุคคลต้องดำเนินการจัดเก็บและรวบรวมภายใต้ภารกิจของกรมการจัดหางานที่มีกฎหมายหรือระเบียบรองรับ ทั้งนี้ หากมีความจำเป็นต้องจัดเก็บข้อมูลส่วนบุคคลที่ไม่มีกฎหมายหรือระเบียบรองรับ ต้องแจ้งวัตถุประสงค์ในการจัดเก็บข้อมูลให้เจ้าของข้อมูลทราบอย่างชัดเจน และดำเนินการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลก่อนการเก็บรวบรวมข้อมูลดังกล่าว

๔ เผยแพร่ข้อมูลตามชุดข้อมูลที่กำหนดในรูปแบบข้อมูลเปิดภาครัฐ (Open Data) และกำหนด ให้มีการเชื่อมโยงและแลกเปลี่ยนข้อมูลกับหน่วยงานอื่น ตามแนวปฏิบัติที่กำหนดไว้ในนโยบายฯ หมวดการแลกเปลี่ยนและการเชื่อมโยงข้อมูล

๕ กำหนดชั้นความลับของข้อมูล (Data Classification) และกำหนดสิทธิในการเข้าถึงข้อมูล เครื่องมือที่ใช้ในการเข้าถึง ให้สอดคล้องกับระดับชั้นความลับของข้อมูลตามแนวทางหรือมาตรฐานที่กำหนด เพื่อให้ข้อมูลมีความมั่นคงปลอดภัยและคงไว้ซึ่งคุณภาพของข้อมูล

๖ ทบทวนสิทธิและวิธีในการเข้าถึงข้อมูลอย่างสม่ำเสมอ

๗ จัดเก็บข้อมูลที่เหมาะสมกับข้อมูลแต่ละประเภทและความจำเป็นใช้งานของข้อมูล

๘ จัดเก็บข้อมูลในรูปแบบการจัดเก็บถาวร ในกรณีที่ข้อมูลไม่มีการเปลี่ยนแปลงหรือแก้ไข แต่ยังมีความจำเป็นต้องเก็บรักษาไว้เพื่อใช้ประโยชน์ในการจัดทำสถิติของหน่วยงาน

๙ ทำลายข้อมูลเมื่อข้อมูลนั้นไม่มีการใช้งาน หรือมีการจัดเก็บเกินกว่าระยะเวลาที่กำหนด และในกรณีที่ข้อมูลยังไม่ได้กำหนดระยะเวลาการจัดเก็บ ให้เจ้าของข้อมูลพิจารณากำหนดระยะเวลาการจัดเก็บข้อมูลที่เหมาะสมเพื่อใช้เป็นแนวทางในการดำเนินการทำลายข้อมูลในอนาคต

๘.๓ แนวปฏิบัติตามนโยบายฯ หมวดการเข้าถึงและการใช้งานข้อมูล

เพื่อกำหนดแนวทางในการประมวลผลและการใช้งานข้อมูลให้เป็นไปอย่างมีประสิทธิภาพ ถูกต้อง และสอดคล้องกับวัตถุประสงค์ของการใช้ข้อมูล เพื่อให้เกิดประโยชน์ต่อการดำเนินงานของหน่วยงาน รวมทั้งกำหนดหลักเกณฑ์และแนวทางในการขอใช้ข้อมูลจากหน่วยงานที่เกี่ยวข้องทั้งภายในและภายนอก ทั้งนี้ การนำข้อมูลไปใช้ต้องเป็นไปตามวัตถุประสงค์ที่กำหนดไว้ หากมีความประสงค์จะใช้ข้อมูลนอกเหนือจากวัตถุประสงค์ดังกล่าว ต้องได้รับความยินยอมจากหน่วยงานเจ้าของข้อมูลก่อน โดยกำหนดแนวปฏิบัติตามนโยบาย ดังนี้

๑ กำหนดแนวปฏิบัติและมาตรฐานด้านการเข้าถึงข้อมูล (Data Access) การประมวลผลข้อมูล และการใช้งานข้อมูล (Data Usage)

๒ เจ้าของข้อมูล ผู้มีส่วนเกี่ยวข้องกับข้อมูล และบริกรข้อมูล ร่วมกันจัดทำเมทาดาตา (Metadata) หรือคำอธิบายข้อมูล สำหรับข้อมูลสำคัญที่กรมการจัดหางานกำหนดให้ต้องมีการจัดทำเมทาดาตา

๓ กำหนดสิทธิ์การเข้าถึงข้อมูลให้สอดคล้องกับการจัดชั้นความลับของข้อมูล และสอดคล้องกับภารกิจหรือบทบาทหน้าที่ตามที่เจ้าของข้อมูลกำหนด

๔ ประมวลผลข้อมูลที่มีความอ่อนไหวหรือเป็นข้อมูลความลับ เช่น ข้อมูลส่วนบุคคล ต้องดำเนินการภายใต้ขอบเขต เงื่อนไข และวัตถุประสงค์ตามที่ได้รับความยินยอม หรือเป็นไปตามกฎหมายและระเบียบที่เกี่ยวข้อง

๕ บันทึกประวัติการเข้าถึง การประมวลผล และการใช้งานข้อมูลในรูปแบบ Log File เพื่อให้สามารถตรวจสอบย้อนหลังได้

๖ การนำข้อมูลไปใช้ต้องเป็นไปตามวัตถุประสงค์ที่กำหนดไว้ เพื่อให้เกิดประโยชน์ต่อการดำเนินงานของหน่วยงาน หากมีความจำเป็นต้องใช้ข้อมูลนอกเหนือจากวัตถุประสงค์ดังกล่าว ต้องได้รับความยินยอมจากหน่วยงานเจ้าของข้อมูลหรือคณะกรรมการธรรมาภิบาลข้อมูลก่อน เว้นแต่เป็นการดำเนินการตามกฎหมาย ระเบียบของทางราชการ หรือมีการจัดทำบันทึกข้อตกลงในการใช้ข้อมูลเพื่อประโยชน์ต่อภารกิจของหน่วยงานราชการ

๘.๔ แนวปฏิบัติตามนโยบายฯ หมวดการแลกเปลี่ยนและการเชื่อมโยงข้อมูล

เพื่อกำหนดแนวทางการแลกเปลี่ยนและเชื่อมโยงข้อมูลระหว่างหน่วยงาน รวมถึงการขอใช้ข้อมูล ให้มีความมั่นคงปลอดภัย ข้อมูลมีคุณภาพ และสามารถนำไปใช้ประโยชน์ได้อย่างมีประสิทธิภาพ โดยการดำเนินการเชื่อมโยงและแลกเปลี่ยนข้อมูลกับหน่วยงานภายนอกต้องสอดคล้องกับระเบียบ หลักเกณฑ์ และกฎหมายที่เกี่ยวข้อง บนพื้นฐานของการใช้ข้อมูลเพื่อประโยชน์สาธารณะและภารกิจของหน่วยงานเป็นสำคัญ โดยมีแนวปฏิบัติตามนโยบาย ดังนี้

๑.หน่วยงานที่ร้องขอ กำหนดวัตถุประสงค์ กระบวนการ การแลกเปลี่ยน และการเชื่อมโยงข้อมูล (Data Integration) ให้มีความชัดเจน ครอบคลุมตั้งแต่ขั้นตอนการเตรียมการ การเริ่มดำเนินการ ระหว่างดำเนินการ และการสิ้นสุดกระบวนการ

๒ หน่วยงานที่ร้องขอ จัดทำชุดข้อมูลและจัดเตรียมเมทาดาตา (Metadata) หรือคำอธิบายชุดข้อมูลของข้อมูลที่มีการร้องขอ การแลกเปลี่ยนหรือการเชื่อมโยงให้ครบถ้วน ทั้งนี้ในกรณีที่มีการสร้างชุดข้อมูลใหม่ ให้กำหนดแนวทางในการจัดทำหรือแนบคำอธิบายชุดข้อมูลต้นฉบับเพื่อประกอบการแลกเปลี่ยนข้อมูลตามความเหมาะสม

๓ ต้องมีการจัดทำข้อตกลงหรือเอกสารที่เกี่ยวข้องกับการแลกเปลี่ยนหรือเชื่อมโยงข้อมูลอย่างใดอย่างหนึ่ง เช่น บันทึกข้อตกลงความร่วมมือ (Memorandum of Understanding: MOU) หนังสือขออนุญาตเชื่อมโยงและใช้ข้อมูล หรือเอกสารอื่นที่เกี่ยวข้องกับการใช้และการเปิดเผยข้อมูล โดยต้องจัดทำข้อเท็จจริง เพื่อประกอบการพิจารณา ดังต่อไปนี้

๓.๑ หน่วยงานมีอำนาจหน้าที่ตามกฎหมายที่จำเป็นต้องเข้าถึงหรือใช้ข้อมูลส่วนบุคคลนั้นอย่างไร ให้ระบุอำนาจหน้าที่ตามกฎหมายโดยละเอียด

๓.๒ ข้อมูลส่วนบุคคลที่หน่วยงานขอให้เปิดเผยเพื่อใช้ในการปฏิบัติงานตามอำนาจหน้าที่ ให้ระบุรายการข้อมูลส่วนบุคคลที่หน่วยงานร้องขอเฉพาะที่จำเป็นต้องใช้ในการปฏิบัติงานตามอำนาจหน้าที่

๓.๓ จัดทำข้อมูลและวิธีการจัดส่งข้อมูลส่วนบุคคล โดยกำหมดมาตรฐานในการรักษาความปลอดภัยข้อมูลส่วนบุคคล

๓.๔ การเชื่อมโยงข้อมูลด้วยวิธีการทางอิเล็กทรอนิกส์ ต้องสามารถแสดงให้เห็นถึงความจำเป็นอย่างต่อเนื่องที่จะเข้าถึงข้อมูลส่วนบุคคลโดยผ่านระบบเครือข่ายคอมพิวเตอร์อย่างไร หรือสามารถเข้าถึงข้อมูลส่วนบุคคลด้วยวิธีการอื่นใด

๔ กำหนดเทคโนโลยี มาตรฐานข้อมูล และมาตรฐานทางเทคนิคที่ใช้ในการแลกเปลี่ยนและเชื่อมโยงข้อมูล เพื่อให้การดำเนินการเป็นไปอย่างมีประสิทธิภาพและปลอดภัย

๕ บันทึกและจัดเก็บรายละเอียดการดำเนินงานในแต่ละครั้งที่มีการร้องขอ แลกเปลี่ยน หรือเชื่อมโยงข้อมูลในรูปแบบ Log File ระหว่างหน่วยงาน เพื่อให้สามารถตรวจสอบย้อนหลังได้

๖ ระบบสารสนเทศที่เกี่ยวข้องกับการแลกเปลี่ยนและเชื่อมโยงข้อมูล สามารถตรวจสอบและติดตามการดำเนินการร้องขอ การแลกเปลี่ยน หรือการเชื่อมโยงข้อมูลได้

๗ บุคคลหรือหน่วยงานที่รับผิดชอบในการดำเนินการเชื่อมโยงและแลกเปลี่ยนข้อมูล เช่น ผู้รับผิดชอบในการออกแบบกระบวนการและเทคโนโลยีการเชื่อมโยงข้อมูล (Data Integration Architect) และผู้ปฏิบัติการเชื่อมโยงข้อมูลให้เป็นไปตามที่ออกแบบไว้ (Data Integration Specialist)

๘.๕ แนวปฏิบัติตามนโยบายฯ หมวดการเปิดเผยข้อมูล (Data Disclosure Domain)

เพื่อกำหนดนโยบายและแนวทางในการเปิดเผยข้อมูล (Open Data) ของหน่วยงาน ให้สามารถเปิดเผยข้อมูลได้อย่างถูกต้อง เหมาะสม และสอดคล้องกับวัตถุประสงค์ของการนำข้อมูลไปใช้ประโยชน์ โดยมีหลักเกณฑ์ วิธีการ และแนวทางในการเปิดเผยข้อมูลสำหรับภาคเอกชนและหน่วยงานภาครัฐที่มีความประสงค์ขอใช้ข้อมูล ทั้งนี้ การเปิดเผยข้อมูลต้องเป็นไปตามกฎหมาย ระเบียบ และข้อกำหนดที่เกี่ยวข้อง โดยมีแนวปฏิบัติตามนโยบาย ดังนี้

๑ บทบาทหน้าที่ของบุคคลหรือหน่วยงานที่เกี่ยวข้องกับการเปิดเผยข้อมูล ผู้รับผิดชอบดำเนินการและปรับปรุงข้อมูลที่เปิดเผย รวมถึงผู้รับผิดชอบในการรับเรื่องและแก้ไขปัญหาเบื้องต้นเกี่ยวกับการเข้าถึงและการนำข้อมูลไปใช้

๒ การเปิดเผยข้อมูลต้องไม่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง หลักเกณฑ์ นโยบาย หรือแนวปฏิบัติของหน่วยงานที่มีผลบังคับใช้ ไม่ว่าข้อมูลนั้นจะอยู่ในรูปแบบหรือแหล่งจัดเก็บใดก็ตาม

๓ การเปิดเผยข้อมูลได้รับอนุญาตจากเจ้าของข้อมูล (Data Owner) ก่อนดำเนินการเผยแพร่

๔ หน่วยงานเจ้าของข้อมูลหรือผู้ที่ได้รับมอบหมายเป็นผู้พิจารณาคัดเลือกชุดข้อมูลที่เหมาะสมสำหรับการเปิดเผย

๕ จัดเตรียมข้อมูลให้อยู่ในรูปแบบมาตรฐานที่กำหนด และมีความเหมาะสมต่อการนำไป ใช้ประโยชน์

๖ เปิดเผยข้อมูลที่สามารถเข้าถึงได้สะดวก และเอื้อต่อการนำข้อมูลไปใช้ประโยชน์

๗ กำหนดเมทาดาตา (Metadata) หรือคำอธิบายชุดข้อมูลควบคู่กับข้อมูลที่เปิดเผย เพื่อให้ผู้ใช้งานสามารถเข้าใจและนำข้อมูลไปใช้ได้อย่างถูกต้อง

๘ ตรวจสอบและติดตามการเปิดเผยข้อมูล เพื่อให้มั่นใจว่าการดำเนินการเป็นไปตามแนวทางที่กำหนด และรักษาคุณภาพของข้อมูลที่เผยแพร่

๙ ผู้รับผิดชอบข้อมูลนำชุดข้อมูลขึ้นเผยแพร่สู่สาธารณะ

๑๐ ควบคุมและกำกับดูแลการเปิดเผยข้อมูล เพื่อป้องกันการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต และให้มีการปฏิบัติตามนโยบายอย่างเคร่งครัด

๘.๖ แนวปฏิบัติตามนโยบายฯ หมวดความน่าเชื่อถือและคุณภาพข้อมูล

เพื่อกำหนดนโยบายในการควบคุมและพัฒนาคุณภาพข้อมูล รวมทั้งเสริมสร้างความน่าเชื่อถือของข้อมูลภายใต้การกำกับดูแลของกรมการจัดหางาน เพื่อให้หน่วยงานที่เกี่ยวข้องสามารถบริหารจัดการและควบคุมคุณภาพข้อมูลได้อย่างมีประสิทธิภาพ อันจะช่วยลดข้อผิดพลาดของข้อมูล และเพิ่มประสิทธิภาพในการนำข้อมูลไปใช้ประโยชน์และการวิเคราะห์ข้อมูล โดยมีแนวปฏิบัติตามนโยบาย ดังนี้

๑ บทบาทหน้าที่ของบุคคลหรือหน่วยงานที่เกี่ยวข้องกับการควบคุมและกำกับดูแลคุณภาพข้อมูลและชุดข้อมูลให้ครอบคลุมตลอดวงจรชีวิตข้อมูล (Data Lifecycle)

๒ จัดทำและจัดเก็บข้อมูลของหน่วยงานต้องคำนึงถึงคุณภาพข้อมูล โดยชุดข้อมูลต้องได้รับการประเมินตามมิติคุณภาพข้อมูล ได้แก่ ความครบถ้วน (Completeness) ความเป็นเอกลักษณ์ (Uniqueness) ความเป็นปัจจุบัน (Timeliness) ความเที่ยงตรง (Validity) ความถูกต้อง (Accuracy) และความสอดคล้องกัน (Consistency)

๓ ประเมินและติดตามคุณภาพข้อมูล เช่น ความถูกต้อง ความครบถ้วน ความสอดคล้อง ความเป็นปัจจุบัน ความตรงตามความต้องการของผู้ใช้ และความพร้อมใช้งานของข้อมูล

๔ จัดเก็บข้อมูลให้เอื้อต่อการรักษาความมั่นคงปลอดภัยและการคงไว้ซึ่งคุณภาพของข้อมูล

๕ ตรวจสอบ วิเคราะห์ และประเมินคุณภาพข้อมูลตามตัวชี้วัดและมิติของคุณภาพข้อมูลที่กำหนดไว้อย่างสม่ำเสมอ

๖ ข้อมูลหรือชุดข้อมูลที่ได้มาจากแหล่งภายนอกซึ่งอยู่นอกเหนือการกำกับดูแลของกรมการจัดหางาน ต้องผ่านการตรวจสอบและประเมินคุณภาพข้อมูลก่อนนำมาใช้ในการดำเนินงานของหน่วยงาน

๗ ทบทวนและปรับปรุงตัวชี้วัดคุณภาพข้อมูลอย่างน้อยปีละ ๑ ครั้ง เพื่อให้สอดคล้องกับการใช้งานข้อมูลและการดำเนินงานของหน่วยงานอย่างต่อเนื่อง

๘.๗ แนวปฏิบัติตามนโยบายฯ หมวดการป้องกันความเสี่ยงทางไซเบอร์กรณีข้อมูลส่วนบุคคลรั่วไหล (Data Leak)

เพื่อเป็นการป้องกันภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับการรั่วไหลของข้อมูลส่วนบุคคล (Data Leak) ซึ่งมีแนวโน้มเพิ่มสูงขึ้นอย่างต่อเนื่อง โดยพบว่ามีข้อมูลบัญชีผู้ใช้งานของหน่วยงาน เช่น ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ถูกเผยแพร่ในแหล่งต่าง ๆ เป็นจำนวนมาก ซึ่งข้อมูลที่รั่วไหลดังกล่าวสามารถถูกนำไปใช้ในการเข้าถึงระบบสารสนเทศ เว็บไซต์ สื่อสังคมออนไลน์ หรือแพลตฟอร์มที่เกี่ยวข้องโดยไม่ได้รับอนุญาต และอาจถูกใช้เป็นจุดเริ่มต้นในการเข้าถึงข้อมูลสำคัญ การยกระดับสิทธิ์ (Privilege Escalation) หรือการเคลื่อนย้ายภายในระบบเครือข่าย (Lateral Movement) ของหน่วยงาน โดยมีแนวปฏิบัติตามนโยบาย ดังนี้

๑ ดำเนินการตรวจสอบและปิดช่องโหว่ของระบบสารสนเทศอย่างเร่งด่วน โดยเฉพาะระบบเว็บไซต์และบริการที่เปิดให้เข้าถึงจากภายนอก รวมถึงปรับแต่งค่าความมั่นคงปลอดภัยของระบบให้เหมาะสมปิดบริการหรือพอร์ตที่ไม่จำเป็น และกำหนดมาตรการป้องกันการโจมตีผ่านช่องทางเว็บอย่างเหมาะสม

๒ สำรองข้อมูลอย่างน้อย ๓ ชุด และจัดเก็บข้อมูลสำรองในลักษณะที่แยกออกจากระบบหลักรวมถึงมีการสำรองแบบออฟไลน์ เพื่อรองรับกรณีระบบถูกโจมตีหรือเกิดเหตุขัดข้องที่กระทบต่อความต่อเนื่องในการให้บริการ

๓ ตรวจสอบการเข้าถึงระบบจากระยะไกล เช่น Remote Desktop Protocol (RDP) และVirtual Private Network (VPN) พร้อมเฝ้าระวังพฤติกรรมการใช้งานที่ผิดปกติ และกำหนดมาตรการยืนยันตัวตนที่เหมาะสมสำหรับการเข้าถึงจากภายนอก

๔ บังคับใช้การยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication: MFA) สำหรับระบบสำคัญ ระบบที่เปิดให้บริการจากภายนอก และบัญชีผู้ใช้งานที่มีสิทธิ์ระดับสูง พร้อมกำหนดรหัสผ่านให้มีความซับซ้อนและยากต่อการคาดเดา และควรกำหนดนโยบายรหัสผ่าน เช่น หลีกเลี่ยงการใช้รหัสผ่านซ้ำกำหนดรายการรหัสผ่านต้องห้าม (Blacklist) และส่งเสริมการใช้เครื่องมือจัดการรหัสผ่าน (PasswordManager)

๕ อัปเดตระบบปฏิบัติการ ซอฟต์แวร์ อุปกรณ์ และส่วนประกอบของระบบต่าง ๆ ให้เป็นปัจจุบันอยู่เสมอ โดยเฉพาะระบบที่เชื่อมต่อกับเครือข่ายภายนอก ระบบเว็บไซต์ ระบบจัดการเนื้อหา และซอฟต์แวร์ที่มีความเสี่ยงสูง

๖ ติดตั้งและปรับปรุงระบบป้องกันมัลแวร์ให้มีความทันสมัยอยู่เสมอ โดยเฉพาะการป้องกันมัลแวร์ที่มุ่งขโมยข้อมูลบัญชีผู้ใช้งาน ข้อมูลรับรองสำหรับเชื่อมต่อระบบ และข้อมูลสำคัญอื่นของหน่วยงาน

๗ ตรวจสอบอุปกรณ์ของผู้ใช้งาน โดยเฉพาะกรณีการปฏิบัติงานจากภายนอกหน่วยงานอุปกรณ์ของผู้ดูแลระบบและอุปกรณ์ที่ใช้เข้าถึงระบบสำคัญ เพื่อให้มั่นใจว่ามีมาตรการป้องกันที่เหมาะสม และไม่ตกอยู่ในภาวะเสี่ยงต่อการรั่วไหลของข้อมูล

๘ เฝ้าระวังและวิเคราะห์บันทึกการใช้งานระบบ (Log) อย่างต่อเนื่อง และนำข้อมูลที่เกี่ยวข้องกับภัยคุกคามมาใช้ในการตรวจจับและป้องกัน โดยเฉพาะความผิดปกติของการเข้าสู่ระบบ การเรียกใช้งานระบบจากตำแหน่งที่ไม่คุ้นเคย การใช้งานบัญชีสิทธิ์สูง และการเข้าถึงข้อมูลสำคัญที่ผิดไปจากปกติ

๙ ตรวจสอบและควบคุมการเข้าถึงของระบบหรือผู้ให้บริการภายนอกอย่างรัดกุม รวมถึงกำหนดสิทธิ์การเข้าถึงสำหรับระบบเชื่อมต่อ โปรแกรมประยุกต์ และ Application Programming Interface (API) ตามความจำเป็น จัดเก็บข้อมูลรับรอง กุญแจลับ และโทเคนสำหรับการเชื่อมต่ออย่างปลอดภัย และเฝ้าระวังการใช้งานที่ผิดปกติอย่างสม่ำเสมอ

๑๐ จัดให้มีระบบบริหารจัดการบัญชีผู้ใช้งานและสิทธิ์การเข้าถึงแบบรวมศูนย์ เพื่อควบคุมวงจรชีวิตบัญชีผู้ใช้งานอย่างเป็นระบบ ครอบคลุมการสร้าง การแก้ไข การระงับ และการยกเลิกบัญชี รวมถึงการเพิกถอนสิทธิ์ทันทีเมื่อมีการเปลี่ยนแปลงหน้าที่หรือพ้นสภาพการปฏิบัติงาน รวมถึงกำหนดกระบวนการยืนยันตัวตน (Identity Proofing) สำหรับการสร้างบัญชี การกู้คืนบัญชี และการเปลี่ยนแปลงข้อมูลสำคัญ เพื่อป้องกันการแอบอ้างตัวตน

๑๑ ควบคุมการกำหนดสิทธิ์การเข้าถึงตามหน้าที่และความจำเป็นของการปฏิบัติงาน พร้อมทบทวนสิทธิ์ของผู้ใช้งาน ผู้ดูแลระบบ และผู้เกี่ยวข้องภายนอกเป็นระยะ เพื่อลดความเสี่ยงจากการเข้าถึงข้อมูลหรือระบบเกินความจำเป็น รวมทั้งลดความเสี่ยงจากการใช้งานโดยไม่เหมาะสมจากบุคลากรภายใน

๑๒ กำหนดมาตรการป้องกันข้อมูลรั่วไหลอย่างเหมาะสม โดยจำแนกประเภทข้อมูลสำคัญจำกัดการเข้าถึงตามระดับความจำเป็น เข้ารหัสข้อมูลทั้งขณะจัดเก็บและขณะรับส่ง และควบคุมการส่งออกข้อมูลผ่านระบบอีเมล เว็บแอปพลิเคชัน ระบบคลาวด์ และอุปกรณ์พกพา เพื่อป้องกันการนำข้อมูลออกจากระบบโดยไม่ได้รับอนุญาต รวมถึงควบคุมการใช้งานข้อมูลผ่านเว็บเบราว์เซอร์ และป้องกันการจัดเก็บข้อมูลรับรองในลักษณะที่ไม่ปลอดภัย

๑๓ จัดให้มีการทดสอบความมั่นคงปลอดภัยของระบบอย่างสม่ำเสมอ เช่น การประเมินช่องโหว่การทดสอบเจาะระบบ และการตรวจสอบความมั่นคงปลอดภัยของเว็บไซต์ ระบบเชื่อมต่อ และบริการภายนอก เพื่อค้นหาและลดความเสี่ยงก่อนเกิดเหตุการณ์จริง รวมถึงกำหนดมาตรการควบคุมการใช้งานsession เช่น การกำหนดระยะเวลาหมดอายุของ session และการยกเลิก session เมื่อพบพฤติกรรมผิดปกติ

๑๔ สร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยให้กับผู้ใช้งาน ผู้ดูแลระบบ และผู้เกี่ยวข้องโดยให้ความรู้เกี่ยวกับการตั้งรหัสผ่านอย่างปลอดภัย การใช้งาน MFA การระวังภัยจากการหลอกลวงทางอิเล็กทรอนิกส์ การดูแลข้อมูลรับรองสำหรับเชื่อมต่อระบบ และแนวทางการปฏิบัติที่ปลอดภัยในการใช้งานระบบสารสนเทศของหน่วยงาน

๙. นโยบายการประยุกต์ใช้ปัญญาประดิษฐ์ (AI)

๙.๑ บทนำ

ปัจจุบันเทคโนโลยีปัญญาประดิษฐ์ (AI) และ Generative AI มีบทบาทสำคัญต่อการเปลี่ยนแปลงรูปแบบการทำงานในยุคดิจิทัล โดยสามารถวิเคราะห์ข้อมูลขนาดใหญ่และสร้างสรรค์เนื้อหาได้หลากหลายรูปแบบ เช่น ข้อความ ภาพ วิดีโอ เป็นต้น กรมการจัดหางาน ซึ่งมีภารกิจด้านการส่งเสริมการมีงานทำ การคุ้มครองคนหางาน และการบริหารจัดการแรงงานต่างด้าว เทคโนโลยีดังกล่าวเป็นเครื่องมือสำคัญที่ช่วยเพิ่มประสิทธิภาพและลดระยะเวลาในการดำเนินงาน อาทิ การวิเคราะห์แนวโน้มตลาดแรงงาน การจับคู่ตำแหน่งงาน (Job Matching) การให้บริการข้อมูลผ่านแชทบอท การจัดทำร่างหนังสือราชการ และการผลิตสื่อประชาสัมพันธ์ อย่างไรก็ตามการใช้งาน Generative AI ยังคงมีความเสี่ยงสำคัญที่ต้องเฝ้าระวัง เช่น การสร้างข้อมูลที่คลาดเคลื่อนจากความเป็นจริง (Hallucination) ซึ่งอาจส่งผลต่อความน่าเชื่อถือของกรมการจัดหางานในการเผยแพร่ข้อมูลที่ไม่ถูกต้อง โดยเฉพาะข้อมูลด้านตำแหน่งงาน สิทธิประโยชน์ และกฎหมายแรงงาน อันอาจก่อให้เกิดความเสียหายต่อประชาชน การนำข้อมูลส่วนบุคคลเข้าสู่ระบบ AI สาธารณะโดยขาดความตระหนัก อาจก่อให้เกิดการรั่วไหลของข้อมูล (Personal Data Leakage) การละเมิดทรัพย์สินทางปัญญา และความเสี่ยงด้านอคติหรือการเลือกปฏิบัติ (Bias and Discrimination) ซึ่งขัดต่อหลักสิทธิมนุษยชนและจริยธรรม

ดังนั้น เพื่อให้การนำ AI มาใช้เป็นไปอย่างมีประสิทธิภาพ ปลอดภัย โปร่งใส และสอดคล้องกับหลักธรรมาภิบาลข้อมูล กรมการจัดหางานจึงได้จัดทำนโยบายด้านปัญญาประดิษฐ์ (AI) เพื่อเป็นกรอบแนวทางปฏิบัติที่ชัดเจนให้บุคลากรทุกระดับให้สามารถนำเทคโนโลยีไปใช้ได้อย่างเหมาะสม มีความรับผิดชอบ ตรวจสอบได้ และลดผลกระทบหรือความเสี่ยงที่อาจเกิดขึ้นต่อกรมการจัดหางานและประชาชน

๙.๒ วัตถุประสงค์

๑ เพื่อให้ข้าราชการ พนักงานราชการ ลูกจ้าง ผู้ปฏิบัติงาน และผู้รับจ้างของกรมการจัดหางาน มีแนวทางปฏิบัติที่ชัดเจนในการนำเทคโนโลยี AI ไปประยุกต์ใช้สนับสนุนภารกิจหลักของหน่วยงาน ได้อย่างถูกต้อง เหมาะสม และมีประสิทธิภาพสูงสุด

๒ เพื่อให้การใช้เทคโนโลยี AI เป็นไปตามกฎหมาย กฎ ระเบียบ ประกาศ ข้อบังคับ และมาตรฐานที่เกี่ยวข้อง โดยเฉพาะอย่างยิ่งกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล (PDPA) ตลอดจนป้องกันความเสี่ยงที่เกิดจากการใช้งานผิดวัตถุประสงค์ ซึ่งอาจก่อให้เกิดข้อมูลเท็จ หรือการรั่วไหลของข้อมูลที่อาจส่งผลกระทบและสร้างความเสียหายต่อประชาชน

๓ เพื่อเสริมสร้างความตระหนักรู้และความเข้าใจให้แก่บุคลากรของกรมการจัดหางาน ในการใช้เทคโนโลยี AI อย่างมีความรับผิดชอบ รอบคอบ และระมัดระวัง เพื่อป้องกันไม่ให้เกิดอคติหรือการเลือกปฏิบัติในการให้บริการ และสามารถนำเทคโนโลยีดังกล่าวไปสร้างนวัตกรรมงานได้อย่างปลอดภัยภายใต้กรอบธรรมาภิบาลข้อมูลที่กรมฯ กำหนด

๙.๓ การกำหนดโครงสร้างการกำกับดูแลด้านปัญญาประดิษฐ์ (AI Governance Structure)

การกำหนดโครงสร้างการกำกับดูแลด้านปัญญาประดิษฐ์ (AI Governance Structure) เป็นการบริหารจัดการภายในของกรมการจัดหางาน ในการนำเทคโนโลยีปัญญาประดิษฐ์ มาประยุกต์ใช้ในภารกิจของกรมการจัดหางานให้เกิดประสิทธิภาพสูงสุด ปลอดภัย และสอดคล้องกับหลักธรรมาภิบาลข้อมูล (Data Governance) โดยกำหนดบทบาท หน้าที่ และความรับผิดชอบของคณะกรรมการ และบุคลากรที่เกี่ยวข้อง ดังนี้

๑) คณะกรรมการกำกับดูแลการประยุกต์ใช้ AI (AI Governance Council)

ให้ประกอบไปด้วยผู้บริหารระดับสูง ผู้บริหารหรือผู้แทนจากหน่วยงานระดับกองหรือกลุ่มงานที่เกี่ยวข้องกับการประยุกต์ใช้ AI และหัวหน้ากลุ่มงานจากศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร โดยมีหน้าที่ ดังนี้

- กำกับดูแล กำหนดทิศทางการดำเนินงานผ่านการกำหนดนโยบายและกลยุทธ์ ในเรื่องการนำปัญญาประดิษฐ์มาใช้งาน
- เฝ้าติดตามประสิทธิภาพ (Performance) และการปฏิบัติตามนโยบายและข้อกำหนดต่างๆ
- ประเมินผลการประยุกต์ใช้ AI ในปัจจุบัน และกำหนดแนวทางการดำเนินงานในอนาคต

๒) หน้าที่และความรับผิดชอบ (Role and Responsibility)

๒.๑) บุคลากรระดับนโยบาย (Strategic Level)

๒.๑.๑ ด้านกำกับดูแลการปฏิบัติงานเพื่อบรรลุเป้าหมายที่กำหนด

- กำหนดกลยุทธ์และเป้าหมายในการประยุกต์ใช้ AI ภายในหน่วยงาน
- กำหนดนโยบายที่เกี่ยวข้องกับการประยุกต์ใช้ AI และนโยบายในการกำกับดูแลการปฏิบัติงานของบุคลากรและผู้มีส่วนได้เสียที่เกี่ยวข้อง
- อนุมัติ พิจารณา หรือตัดสินใจด้านต่าง ๆ ที่เกี่ยวข้องกับการประยุกต์ใช้ AI เช่น แผนปฏิบัติงานในการประยุกต์ใช้ AI , การนำโมเดลปัญญาประดิษฐ์ (AI Model) ไปใช้งานจริง , ความสอดคล้องตามหลักการจริยธรรมปัญญาประดิษฐ์ , การแก้ไขประเด็นปัญหา และกำหนดแนวทางการดำเนินงาน
- เฝ้าติดตามประสิทธิภาพการทำงานของ AI และระดับความสำเร็จในการประยุกต์ใช้ AI เมื่อเทียบกับเป้าหมายที่กำหนด
- ประเมินผลประยุกต์ใช้งาน AI ที่ผ่านมาและกำหนดแนวทางการดำเนินงานในอนาคต

๒.๑.๒ ด้านการปฏิบัติงานให้สอดคล้อง (Conformance) ตามข้อกำหนดภายในและภายนอกองค์กร

กำหนดนโยบายในการกำกับดูแลการปฏิบัติงานของบุคลากรและผู้มีส่วนได้เสียที่เกี่ยวข้อง รวมถึงเฝ้าติดตามและประเมินผลการปฏิบัติงานให้เป็นไปตามนโยบายองค์กร หลักการจริยธรรม ปัญญาประดิษฐ์ กฎหมาย และข้อกำหนดที่เกี่ยวข้อง

๒.๑.๓ ด้านการควบคุมความเสี่ยงและผลกระทบที่อาจเกิดขึ้น

กำหนดระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) และพิจารณาความเหมาะสมของมาตรการเพื่อจำกัดความเสี่ยงให้อยู่ในขอบเขตที่ยอมรับได้

๒.๒) บุคลากรระดับปฏิบัติการ (Implementation Level)

๒.๒.๑ ด้านการปฏิบัติงานตามกลยุทธ์ในการประยุกต์ใช้ AI

- จัดเตรียมข้อมูลสำหรับนำเสนอคณะกรรมการกำกับดูแลฯ เพื่อประกอบการกำหนดกลยุทธ์ในการประยุกต์ใช้ AI เช่น กระบวนการหรือขั้นตอนปฏิบัติที่สามารถนำ AI มาประยุกต์ใช้ ประโยชน์ที่จะได้รับ ระดับความสำเร็จที่คาดหวัง ความพร้อมขององค์กร ความซับซ้อนในการดำเนินการและเวลาที่ใช้ในการดำเนินการ หลักการจริยธรรมปัญญาประดิษฐ์ กฎหมายและข้อกำหนดที่เกี่ยวข้อง เป็นต้น
- จัดทำแผนปฏิบัติงานในการประยุกต์ใช้ AI (AI Roadmap) ตามกลยุทธ์ที่คณะกรรมการกำกับดูแลฯ กำหนด
- จัดทำสถาปัตยกรรมที่เกี่ยวข้องกับการประยุกต์ใช้ AI (AI Architecture) และจัดเตรียมทรัพยากรที่จำเป็นในการดำเนินงานตามแผนปฏิบัติงานในการประยุกต์ใช้ AI

๒.๒.๒ ด้านการออกแบบ พัฒนา และนำ AI ไปประยุกต์ใช้

- ออกแบบโซลูชัน พัฒนา ทดสอบ และนำ AI ไปใช้งานพร้อมทั้งจัดทำเอกสารที่เกี่ยวข้อง
- จัดเตรียมข้อมูลและบริหารจัดการข้อมูลสำหรับทำงานร่วมกับ AI เพื่อให้ได้ข้อมูลที่มีคุณภาพและเหมาะสมในการใช้งานร่วมกับ AI
- จัดทำมาตรการในการรักษาความมั่นคงปลอดภัยและการคุ้มครองความเป็นส่วนตัว
- เฝ้าติดตามประสิทธิภาพการทำงานของ AI และระดับความสำเร็จในการประยุกต์ใช้ AI เพื่อนำเสนอคณะกรรมการกำกับดูแลฯ
- ประเมินผลการประยุกต์ใช้งาน AI ในปัจจุบัน และจัดทำข้อเสนอในการดำเนินงานในอนาคต เพื่อนำเสนอคณะกรรมการกำกับดูแลฯ

๒.๒.๓ ด้านการปฏิบัติตามข้อกำหนดภายในและภายนอกหน่วยงาน

- จัดทำขั้นตอนปฏิบัติ มาตรการ และเครื่องมือเพื่อควบคุมการปฏิบัติงานให้สอดคล้องตามนโยบายของหน่วยงาน หลักการจริยธรรมปัญญาประดิษฐ์ กฎหมายและข้อกำหนดที่เกี่ยวข้อง
- เฝ้าติดตามผลการปฏิบัติงานตามข้อกำหนดทั้งภายในและภายนอกองค์กร เพื่อนำเสนอคณะกรรมการกำกับดูแลฯ
- ประเมินผลมาตรการในการกำกับดูแล และจัดทำข้อเสนอในการดำเนินงานในอนาคต เพื่อนำเสนอคณะกรรมการกำกับดูแลฯ

๒.๒.๔ ด้านการควบคุมความเสี่ยงและผลกระทบที่อาจเกิดขึ้น

- ประเมินความเสี่ยงและผลกระทบที่อาจเกิดขึ้นจากการประยุกต์ใช้ AI
- จัดทำมาตรการเพื่อควบคุมความเสี่ยงให้อยู่ในขอบเขตที่ยอมรับได้
- กำหนดระดับการมีส่วนร่วมของมนุษย์ในการทำงานร่วมกับ AI เพื่อลดผลกระทบที่อาจเกิดขึ้น
- นำเสนอผลการดำเนินงานเกี่ยวกับการควบคุมความเสี่ยงต่อคณะกรรมการกำกับดูแลฯ

๓) การพัฒนาศักยภาพบุคลากร (Competency Building)

เพื่อให้บุคลากรของหน่วยงานมีความพร้อมในการปฏิบัติงานในยุคดิจิทัล สามารถประยุกต์ใช้เทคโนโลยีปัญญาประดิษฐ์ (AI) และข้อมูล (Data) ในการยกระดับประสิทธิภาพการให้บริการประชาชน และสนับสนุนการบริหารจัดการภาครัฐอย่างมีประสิทธิผล จึงกำหนดแนวทางการพัฒนาศักยภาพบุคลากร ดังนี้

๓.๑) การพัฒนาองค์ความรู้ด้านธุรกิจ (Business Competency)

มุ่งเน้นให้บุคลากรมีความเข้าใจบริบทภารกิจของหน่วยงาน สามารถนำเทคโนโลยี AI ไปประยุกต์ใช้ให้สอดคล้องกับกระบวนงาน และสร้างคุณค่าในการให้บริการประชาชน โดยมีองค์ความรู้ ดังนี้

- องค์ความรู้ด้าน AI Canvas ส่งเสริมให้บุคลากรมีความรู้ในด้านการวิเคราะห์และออกแบบการนำ AI ไปใช้ในกระบวนงาน โดยใช้เครื่องมือ AI เพื่อระบุปัญหา โอกาส และผลลัพธ์ที่คาดหวังอย่างเป็นระบบกำหนดกลยุทธ์และเป้าหมายในการประยุกต์ใช้ AI ภายในหน่วยงาน
- องค์ความรู้ด้าน AI-powered Organization Management ส่งเสริมให้บุคลากรมีความรู้ในด้านการบริหารหน่วยงานโดยใช้ AI เป็นเครื่องมือสนับสนุนการตัดสินใจ การวางแผน และการเพิ่มประสิทธิภาพการดำเนินงาน
- องค์ความรู้ด้าน AI Project Management ส่งเสริมให้บุคลากรมีความรู้ในด้านการบริหารโครงการด้าน AI ตั้งแต่การวางแผน การกำหนดขอบเขต การติดตามประเมินผล และการบริหารความเสี่ยงของโครงการ

๓.๒) การพัฒนาองค์ความรู้ด้านเทคโนโลยี (Technical Competency)

มุ่งเน้นให้บุคลากรมีพื้นฐานด้านเทคโนโลยีที่เกี่ยวข้องกับ AI และข้อมูล สามารถใช้งาน วิเคราะห์ และพัฒนานวัตกรรมได้อย่างเหมาะสม โดยมีองค์ความรู้ ดังนี้

- องค์ความรู้ด้าน AI Fundamentals ส่งเสริมให้บุคลากรมีความรู้ด้านพื้นฐานเกี่ยวกับการใช้งาน AI
- องค์ความรู้ด้าน Data Management ส่งเสริมให้บุคลากรมีความรู้ในด้านการจัดการข้อมูล การจัดเก็บ การประมวลผล การรักษาคุณภาพข้อมูล และการใช้ข้อมูลเพื่อการตัดสินใจ
- องค์ความรู้ด้าน Mathematics and Statistics ส่งเสริมให้บุคลากรมีความรู้ในด้านพื้นฐานคณิตศาสตร์และสถิติที่จำเป็นต่อการวิเคราะห์ข้อมูลและการพัฒนาโมเดล AI
- องค์ความรู้ด้าน Programming ส่งเสริมให้บุคลากรมีความรู้ในด้านทักษะการเขียนโปรแกรม เช่น Python หรือเครื่องมือที่เกี่ยวข้อง เพื่อใช้ในการพัฒนาและประยุกต์ใช้งาน AI

๓.๓) การพัฒนาองค์ความรู้ด้านการกำกับดูแล (Governance Competency)

มุ่งเน้นให้บุคลากรมีความเข้าใจด้านกฎหมาย จริยธรรม และธรรมาภิบาลข้อมูล เพื่อให้การใช้ AI และข้อมูลเป็นไปอย่างถูกต้อง โปร่งใส และตรวจสอบได้ โดยมีองค์ความรู้ ดังนี้

- องค์ความรู้ด้าน AI Governance ส่งเสริมให้บุคลากรมีความรู้ด้านการกำกับดูแลการใช้ AI ให้มีความโปร่งใส เป็นธรรม และลดความเสี่ยงจากการใช้งาน

- องค์ความรู้ด้าน Data Governance ส่งเสริมให้บุคลากรมีความรู้ในด้านธรรมาภิบาลข้อมูลภาครัฐ การกำหนดนโยบายข้อมูล การกำหนดสิทธิ์การเข้าถึง และการรักษาความปลอดภัยของข้อมูล

- องค์ความรู้ด้าน Roles & Responsibility ส่งเสริมให้บุคลากรมีความรู้ในด้านกำหนดบทบาทหน้าที่ของบุคลากรที่เกี่ยวข้องกับข้อมูลและ AI อย่างชัดเจน เพื่อให้เกิดความรับผิดชอบและการดำเนินงานที่มีประสิทธิภาพ

- องค์ความรู้ด้าน Legal & Ethical Implications ส่งเสริมให้บุคลากรมีความรู้ในด้านกฎหมายและจริยธรรมที่เกี่ยวข้องกับการใช้ข้อมูลและ AI เช่น การคุ้มครองข้อมูลส่วนบุคคล และการใช้เทคโนโลยีอย่างมีจริยธรรม

๙.๔ การกำหนดกลยุทธ์ในการประยุกต์ใช้ AI (AI Strategy)

๙.๔.๑ การกำหนดกลยุทธ์ในการประยุกต์ใช้ AI อย่างมีความรับผิดชอบ (Responsible AI Strategy)

ปัจจุบันเทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence: AI) ได้ถูกนำมาประยุกต์ใช้ในการดำเนินงานของภาครัฐอย่างแพร่หลาย โดยมีรูปแบบการใช้งานที่หลากหลายตามภารกิจและเป้าหมายของแต่ละหน่วยงาน สำหรับกรมการจัดหางาน การประยุกต์ใช้ AI ถือเป็นกลไกสำคัญในการยกระดับประสิทธิภาพการให้บริการประชาชน การบริหารจัดการแรงงาน และการเชื่อมโยงข้อมูลด้านการจ้างงานให้มีความรวดเร็ว ถูกต้อง และเป็นปัจจุบัน ทั้งนี้ เพื่อให้การนำ AI มาใช้เกิดผลสัมฤทธิ์อย่างเป็นรูปธรรมและสอดคล้องกับพันธกิจของกรมการจัดหางาน จึงจำเป็นต้องกำหนดกรอบแนวทางเชิงกลยุทธ์และแผนปฏิบัติการที่ชัดเจน โดยพิจารณาถึงโอกาส ประโยชน์ และความเป็นไปได้ในการดำเนินงาน ครอบคลุมปัจจัยสำคัญ ได้แก่ ศักยภาพของเทคโนโลยี ความพร้อมของข้อมูลและโครงสร้างพื้นฐาน ความพร้อมของบุคลากร ความซับซ้อนของกระบวนงาน ระยะเวลาในการพัฒนา ตลอดจนข้อจำกัดและความท้าทายที่อาจเกิดขึ้น

นอกจากนี้ การดำเนินงานด้าน AI ของกรมการจัดหางานจำเป็นต้องคำนึงถึงการใช้งานอย่างมีความรับผิดชอบ (Responsible AI) โดยให้ความสำคัญกับการบริหารความเสี่ยงและผลกระทบที่อาจเกิดขึ้นจากความคลาดเคลื่อนของผลลัพธ์ การเกิดอคติของระบบที่อาจนำไปสู่ความไม่เป็นธรรมในการให้บริการประชาชน หรือผลกระทบต่อข้อมูลส่วนบุคคล ทั้งนี้ ต้องดำเนินการภายใต้กรอบกฎหมาย มาตรฐาน และหลักจริยธรรมที่เกี่ยวข้องอย่างเคร่งครัด โดยมีแนวทางหลักในการกำหนดกลยุทธ์ในการประยุกต์ใช้ AI อย่างมีความรับผิดชอบ ดังนี้

๑) การระบุโอกาสและการสร้างนวัตกรรมบริการ

การประยุกต์ใช้ AI ต้องสอดคล้องกับวิสัยทัศน์และพันธกิจของกรมฯ ทั้งในระยะสั้นและระยะยาว โดยมุ่งเน้นการวิเคราะห์กระบวนการทำงาน (Process Analysis) เพื่อหาจุดเชื่อมโยงที่ AI จะสามารถเพิ่มประสิทธิภาพการให้บริการประชาชนได้สูงสุด เช่น การจับคู่งาน (Job Matching) หรือการวิเคราะห์แนวโน้มตลาดแรงงาน ทั้งนี้ การดำเนินงานต้องเกิดจากความร่วมมือระหว่างฝ่ายเทคนิคและฝ่ายปฏิบัติการ เพื่อให้มั่นใจว่านวัตกรรมที่พัฒนาขึ้นสามารถตอบโจทย์การใช้งานจริงและมีตัวชี้วัดความสำเร็จ (KPI) ที่ชัดเจน

๒) การกำหนดเป้าหมายในการประยุกต์ใช้ AI

การวิเคราะห์กระบวนการทำงานเพื่อระบุโอกาสในการนำปัญญาประดิษฐ์ (AI) มาประยุกต์ใช้ กรมฯ จำเป็นต้องดำเนินการจัดลำดับความสำคัญการดำเนินงาน เพื่อให้การขับเคลื่อนนวัตกรรมสอดคล้องกับทรัพยากรและบริบทของกรมการจัดหางาน โดยพิจารณาจากปัจจัยสำคัญ ดังนี้

- ผลสัมฤทธิ์และคุณค่าที่ได้รับ ประโยชน์เชิงประจักษ์ที่จะเกิดขึ้นต่อกระบวนงานและผู้รับบริการ
- ความสอดคล้องกับตัวชี้วัด ระดับความสำเร็จที่ตอบสนองต่อเป้าหมายหลักและตัวชี้วัดผลงานของกรมฯ

- ธรรมาภิบาลและจริยธรรม การออกแบบและพัฒนาระบบที่สอดคล้องกับหลักจริยธรรม AI กฎหมายคุ้มครองข้อมูลส่วนบุคคล และข้อกำหนดภาครัฐ

- ความพร้อมด้านทรัพยากร พิจารณาความพร้อมของงบประมาณ ฐานข้อมูลบุคลากร และโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ

- การบริหารการเปลี่ยนแปลงและความเสี่ยง ขีดความสามารถในการเปลี่ยนผ่านสู่ระบบดิจิทัล รวมถึงมาตรการรองรับความเสี่ยงและผลกระทบที่อาจเกิดขึ้น

- ความคุ้มค่าเชิงเวลา ความซับซ้อนทางเทคนิคเมื่อเปรียบเทียบกับระยะเวลาในการดำเนินการ

๓) การบริหารจัดการข้อมูลเชิงยุทธศาสตร์เพื่อรองรับ AI

กรมการจัดหางานมุ่งเน้นการวางรากฐานการบริหารจัดการข้อมูลเชิงยุทธศาสตร์ เพื่อเป็นกลไกสำคัญในการสนับสนุนการประยุกต์ใช้ปัญญาประดิษฐ์ (AI) อย่างเต็มประสิทธิภาพ โดยครอบคลุมวงจรชีวิตของข้อมูลตั้งแต่วิธีการคัดเลือกแหล่งข้อมูลที่มีความน่าเชื่อถือ การเตรียมข้อมูล (Data Preparation) ให้มีความพร้อมและเพียงพอต่อการประมวลผล ไปจนถึงการพัฒนาอัลกอริทึมให้มีสมรรถนะสูงสุด ยึดถือหลักเกณฑ์การประเมินคุณภาพข้อมูลในด้านความถูกต้องแม่นยำ (Accuracy) ความสะดวกในการเข้าถึง (Accessibility) ความครอบคลุม (Completeness) ความเป็นปัจจุบัน (Timeliness) และความสอดคล้องกับวัตถุประสงค์การใช้งาน ควบคู่ไปกับการบูรณาการทรัพยากรด้านบุคลากร เครื่องมือดิจิทัล และกระบวนงานที่เกี่ยวข้อง ภายใต้กรอบธรรมาภิบาลข้อมูล (Data Governance) เพื่อควบคุมกำกับดูแลให้ข้อมูลมีมาตรฐานสากล

๙.๔.๒ การบริหารจัดการความเสี่ยงจากการประยุกต์ใช้ AI (AI Risk Management)

เพื่อให้การนำระบบปัญญาประดิษฐ์ (AI) มาใช้ในภารกิจของกรมการจัดหางาน เป็นไปอย่างโปร่งใส มีจริยธรรม และลดผลกระทบเชิงลบต่อการบริการประชาชน ความเสี่ยงหลักที่ต้องเฝ้าระวังแบ่งออกเป็นด้านสำคัญ ดังนี้

๑) ความเสี่ยงด้านคุณภาพข้อมูล (Data Quality) เป็นความเสี่ยงที่ข้อมูลขององค์กรมีคุณภาพไม่เพียงพอ จนส่งผลให้การทำงานของ AI ไม่มีประสิทธิภาพตามเป้าหมายที่กำหนด หรือทำงานผิดพลาด เป็นต้น

๒) ความเสี่ยงด้านความไม่เป็นธรรมและการเลือกปฏิบัติ (Unfairness and Discrimination) เป็นความเสี่ยงที่ผลลัพธ์จากการทำงานของ AI นำไปสู่ความไม่เป็นธรรมและการเลือกปฏิบัติ ซึ่งอาจเกิดจากอคติที่มาจากการออกแบบและสร้างโมเดล(Bias Introduced by Engineering Decisions) หรือเกิดจากอคติที่มาจากข้อมูล (Data Bias) เช่น การใช้ข้อมูลที่ไม่มีความหลากหลายหรือมีความเอนเอียงมาฝึกสอน AI เป็นต้น

๓) ความเสี่ยงด้านภัยคุกคามทางไซเบอร์ (Cyber Attack) เป็นความเสี่ยงที่ AI ถูกโจมตี โดยมีวัตถุประสงค์ให้ AI ทำงานผิดพลาด หยุดการทำงาน หรือเกิดการรั่วไหลของข้อมูล เป็นต้น โดยอาศัยช่องโหว่ (Vulnerability) ของระบบ AI หรือโจมตีข้อมูลที่ใช้ในการฝึกสอน AI ทำให้ข้อมูลปนเปื้อนด้วยข้อมูลที่ก่อให้เกิดช่องโหว่

๔) ความเสี่ยงด้านการคุ้มครองความเป็นส่วนตัว (Privacy) เป็นความเสี่ยงที่ข้อมูลส่วนบุคคลถูกละเมิด โดยอาจเกิดจากการมีมาตรการในการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เหมาะสม ความผิดพลาดในการปฏิบัติงาน หรือถูกโจมตีโดยผู้ประสงค์ร้ายเป็นต้น

๕) ความเสี่ยงด้านการไม่ปฏิบัติตามกฎหมายและข้อกำหนดที่เกี่ยวข้อง (Non-compliance) เป็นความเสี่ยงที่ผลลัพธ์จากการทำงานของ AI นำไปสู่การละเมิดกฎหมายหรือข้อกำหนดที่เกี่ยวข้อง

๖) ความเสี่ยงด้านความน่าเชื่อถือหรือชื่อเสียง (Trust and Reputation) เป็นความเสี่ยงที่เกิดจากการทำงานหรือการตัดสินใจของ AI ที่ผิดพลาด หรือก่อให้เกิดผลกระทบเชิงลบ เช่น AI ทำงานผิดพลาดเนื่องจากอยู่ในสถานการณ์ที่ไม่เคยถูกทดสอบ หรือต้องตัดสินใจบนพื้นฐานข้อมูลที่ไม่เคยได้รับการฝึกสอนมาก่อน เป็นต้น

เพื่อลดความเสี่ยงและผลกระทบเชิงลบจากการประยุกต์ใช้ AI ดังกล่าว องค์กรจึงจำเป็นต้องมีการบริหารจัดการความเสี่ยง (Risk Management) เพื่อควบคุมความเสี่ยงในทุกกิจกรรมตลอดวงจรชีวิตของ AI (AI Lifecycle) ให้อยู่ในขอบเขตที่ยอมรับได้

๙.๕ การกำกับดูแลการปฏิบัติงานที่เกี่ยวข้องกับ AI (AI Operation)

การกำกับดูแลการปฏิบัติงานที่เกี่ยวข้องกับปัญญาประดิษฐ์ (AI Operation) ของกรมการจัดหางาน เพื่อใช้เป็นกรอบมาตรฐานในการดำเนินงาน ตั้งแต่กระบวนการออกแบบ พัฒนา ไปจนถึงการให้บริการแก่ประชาชน เพื่อสร้างความเชื่อมั่นและความโปร่งใสในภารกิจด้านการจัดหางาน

๙.๕.๑ การกำกับดูแลตลอดวงจรชีวิตของปัญญาประดิษฐ์ (AI Lifecycle)

กรมการจัดหางานกำหนดให้การบริหารจัดการระบบปัญญาประดิษฐ์ต้องครอบคลุมทุกระยะของวงจรชีวิต รักษาประสิทธิภาพและความถูกต้องของระบบ เพื่อให้บรรลุเป้าหมายในการประยุกต์ใช้ AI ดังนี้

๑) การออกแบบโซลูชัน (Solution Design) กำหนดวัตถุประสงค์และขอบเขตการใช้งาน AI ให้ชัดเจน สอดคล้องกับภารกิจของกรมฯ พร้อมประเมินผลกระทบและความเสี่ยงที่อาจเกิดขึ้นต่อผู้รับบริการ

๒) การจัดเตรียมข้อมูล (Data Preparation) คัดเลือกและจัดเตรียมข้อมูลที่มีคุณภาพ มีความถูกต้องและเป็นปัจจุบัน โดยต้องดำเนินการภายใต้ธรรมาภิบาลข้อมูล (Data Governance) และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) อย่างเคร่งครัด

๓) การสร้างโมเดล (Model Building) พัฒนาโมเดลโดยคำนึงถึงความแม่นยำและความเป็นธรรม (Fairness) เพื่อป้องกันไม่ให้เกิดความลำเอียง (Bias) ในการตัดสินใจหรือการคัดกรองข้อมูลไปใช้ตามภารกิจงาน

๔) การนำโมเดลไปใช้งาน (Deployment) ตรวจสอบความมั่นคงปลอดภัยของระบบและทดสอบประสิทธิภาพก่อนการนำไปใช้งานจริงในสภาพแวดล้อมจำกัด เพื่อลดความเสี่ยงเชิงระบบ

๕) การเฝ้าติดตามการประยุกต์ใช้ (Monitoring) กำหนดกลไกการติดตามการทำงานของ AI อย่างต่อเนื่อง เพื่อเฝ้าระวังความผิดปกติและรักษามาตรฐานความแม่นยำของผลลัพธ์

๖) การประเมินผลการประยุกต์ใช้ (Evaluation) ตรวจสอบประสิทธิภาพของระบบตามตัวชี้วัดที่กำหนด รวมถึงประเมินความพึงพอใจและผลกระทบที่เกิดขึ้นจริงต่อสาธารณะ

๗) การยุติการใช้งาน (Retirement) กำหนดให้มีการยกเลิกการใช้ระบบเมื่อสิ้นสุดภารกิจงาน หรือเมื่อเทคโนโลยีมีการเปลี่ยนแปลง โดยต้องมีการจัดการข้อมูลที่เกี่ยวข้องตามระเบียบรักษาความลับของทางราชการ

รูป ๑๖ การกำกับดูแลตลอดชีวิตของปัญญาประดิษฐ์ (AI Lifecycle) ของกรมการจัดหางาน

๙.๕.๒ การให้บริการปัญญาประดิษฐ์ (AI Service)

๑) การประกาศนโยบายและข้อมูลทั่วไปเกี่ยวกับการใช้งาน AI (Policy and General Disclosure)

การประกาศนโยบายและการเปิดเผยข้อมูลทั่วไปเกี่ยวกับการใช้งาน AI (Policy and General Disclosure) ในการให้บริการที่เกี่ยวข้องกับ AI กรมการจัดหางานควรกำหนดและเผยแพร่นโยบายที่เกี่ยวข้องให้ผู้ใช้งานรับทราบอย่างชัดเจนและครบถ้วน อาทิ นโยบายการใช้งาน AI (AI Usage Policy) แนวปฏิบัติตามหลักจริยธรรมปัญญาประดิษฐ์ (AI Ethics Principles) นโยบายด้านความมั่นคงปลอดภัย (Security Policy) และนโยบายคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) ต้องแจ้งให้ผู้ใช้ทราบอย่างชัดเจนถึงการนำเทคโนโลยีปัญญาประดิษฐ์ (AI) มาใช้ในกระบวนการให้บริการ โดยครอบคลุมรายละเอียดเกี่ยวกับวิธีการใช้งาน ข้อกำหนดและข้อจำกัด ความสามารถของระบบ ตลอดจนหลักการทำงานเบื้องต้นและลักษณะของผลลัพธ์ ข้อมูลดังกล่าวต้องเผยแพร่ผ่านคู่มือการใช้งาน คำถามที่พบบ่อย (FAQ) หรือข้อตกลงการใช้บริการ (Terms and Conditions) เพื่อสร้างความเข้าใจที่ถูกต้องและส่งเสริมการใช้งานอย่างเหมาะสม

๒) ช่องทางการติดต่อสื่อสาร (Communication Channel)

จัดให้มีช่องทางการติดต่อสื่อสารเพื่อเปิดรับความคิดเห็น (Feedback) ประเด็นปัญหา (Issue) และความผิดพลาด (Error) จากผู้ใช้งานระบบ เพื่อให้หน่วยงานสามารถนำข้อมูลดังกล่าวมาวิเคราะห์ ประเมินผล และดำเนินการปรับปรุงแก้ไขการให้บริการได้อย่างมีประสิทธิภาพ

๙.๖ การจัดทำชุดข้อมูลที่ผ่านการจัดทำ Data Governance สำหรับการประยุกต์ใช้ปัญญาประดิษฐ์ (AI)

การจัดทำและเตรียมความพร้อมชุดข้อมูล (Dataset) ที่ผ่านกระบวนการธรรมาภิบาลข้อมูล (Data Governance) อย่างเป็นระบบ เพื่อให้นำข้อมูลเหล่านี้ไปใช้ในการฝึกสอน (Training Model) และประมวลผลด้วยเทคโนโลยี AI ได้อย่างถูกต้อง แม่นยำ และปลอดภัย เพื่อให้ชุดข้อมูลดังกล่าวมีคุณภาพสูง ปราศจากความลำเอียง (Bias) และเคารพต่อสิทธิความเป็นส่วนตัวของประชาชน กรมการจัดหางานได้กำหนดแนวทางในการทำชุดข้อมูลที่ผ่านการจัดทำ Data Governance สำหรับการประยุกต์ใช้ปัญญาประดิษฐ์ (AI) ดังนี้

๑) กระบวนการจัดทำชุดข้อมูล

- กำหนดขอบเขตชุดข้อมูลที่สอดคล้องกับวัตถุประสงค์ในการไปใช้สำหรับ AI โดยต้องกำหนดชุดข้อมูลให้ชัดเจนว่าข้อมูลไหนใช้สำหรับ AI ได้ ไม่ว่าข้อมูลนั้นจะเป็นข้อมูลทางทะเบียนหรือทางสถิติ
- ดำเนินการทำความสะอาดข้อมูลเพื่อกำจัดข้อมูลที่ซ้ำซ้อน ข้อมูลที่ไม่สมบูรณ์ หรือข้อมูลที่มีความผิดปกติ เพื่อให้ชุดข้อมูลมีความพร้อมและมีมาตรฐานเดียวกัน
- การจัดทำข้อมูลนิรนาม โดยข้อมูลที่มีส่วนเกี่ยวข้องกับบุคคลจะต้องผ่านกระบวนการลบ หรือการทำข้อมูลที่ไม่ให้สามารถระบุตัวตนได้ เพื่อป้องกันการนำข้อมูลส่วนบุคคลไปให้ AI ประมวลผล
- การจัดทำคำอธิบายชุดข้อมูล ต้องมีการจัดทำคำอธิบายชุดข้อมูลหรือเมทาดาตา (Metadata) ตามที่กำหนดไว้ในธรรมาภิบาลข้อมูลของกรมการจัดหางาน เพื่อให้ผู้พัฒนาระบบ AI เข้าใจคุณลักษณะของชุดข้อมูลได้อย่างถูกต้อง

๒) ข้อกำหนดในการดำเนินการ

- การจัดทำและใช้ชุดข้อมูลต้องสอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) และพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล
- ต้องมีการบันทึกประวัติการเข้าถึงและการปรับปรุงแก้ไขชุดข้อมูล (Audit Trail) ในทุกขั้นตอนการทำงาน เพื่อให้สามารถตรวจสอบย้อนหลังได้
- การลดความลำเอียงของข้อมูล (Bias Mitigation) ชุดข้อมูลที่นำมาใช้ฝึกสอน AI ต้องมีความหลากหลายและครอบคลุมกลุ่มประชากรที่เกี่ยวข้องอย่างสมดุล เพื่อป้องกันไม่ให้ปัญญาประดิษฐ์เกิดอคติหรือการเลือกปฏิบัติในการให้บริการ

๓) ข้อห้ามในการดำเนินการ

- ห้ามใช้ข้อมูลส่วนบุคคลที่ยังไม่ผ่านการทำนิรนาม หรือข้อมูลที่สามารถระบุตัวตนของประชาชน หรือข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน (Sensitive Data) เช่น ศาสนา ประวัติอาชญากรรม หรือข้อมูลสุขภาพ ไปใช้ในการฝึกสอน AI (Training Model) โดยเด็ดขาด เว้นแต่จะได้รับความยินยอมอย่างชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล และผ่านความเห็นชอบจากคณะกรรมการธรรมาภิบาลข้อมูลของกรมการจัดหางาน

- ห้ามจัดเก็บข้อมูลนอกระบบที่กำหนด ห้ามนำชุดข้อมูลที่เตรียมไว้สำหรับ AI ไปจัดเก็บในอุปกรณ์ส่วนตัว หรือระบบคลาวด์ภายนอกที่ไม่ได้รับการรับรองมาตรฐานความปลอดภัยจากกรมการจัดหางาน

๔) ช่องทางการจัดเก็บและเผยแพร่ชุดข้อมูล

- ระบบบัญชีข้อมูล (DOE Data Catalog) ชุดข้อมูลสำหรับ AI ทุกชุด ต้องได้รับการขึ้นทะเบียนและเผยแพร่ในระบบ Data Catalog ของกรมการจัดหางาน โดยจะต้องแสดงรายละเอียดเชิงพจนานุกรมข้อมูล (Data Dictionary) คำอธิบายข้อมูล (Metadata) สถานะของคุณภาพข้อมูล และเงื่อนไขการนำไปใช้งาน สามารถค้นหา ขอสิทธิ์เข้าถึง และนำชุดข้อมูลไปประยุกต์ใช้ต่อยอดในการพัฒนาระบบปัญญาประดิษฐ์ได้อย่างมีประสิทธิภาพและถูกต้องตามนโยบาย

- ระบบ Data Lake ของกรมการจัดหางาน ต้องมีการแบ่งแยกพื้นที่ (Zone) จัดเก็บสำหรับชุดข้อมูล AI โดยเฉพาะ พร้อมทั้งกำหนดสิทธิ์การเข้าถึง (Access Control) ตามบทบาทหน้าที่อย่างเข้มงวด

๙.๗ แนวปฏิบัติตามนโยบายฯ หมวดการใช้ระบบปัญญาประดิษฐ์ (AI)

เพื่อกำหนดทิศทาง ข้อจำกัด และกรอบความรับผิดชอบในการนำระบบปัญญาประดิษฐ์ (AI) มาใช้ในการปฏิบัติราชการของ กรมการจัดหางาน ให้เกิดประสิทธิภาพสูงสุด มีความมั่นคงปลอดภัย โปร่งใส เป็นไปตามหลักธรรมาภิบาล และไม่ละเมิดสิทธิส่วนบุคคลของประชาชน จึงกำหนดแนวปฏิบัติตามนโยบาย ดังนี้

๑) การป้องกันอคติและการเลือกปฏิบัติ ห้ามใช้ระบบ AI ในการวิเคราะห์หรือตัดสินใจที่ส่งผลกระทบต่อสิทธิและโอกาสของประชาชน เช่น การมีอคติในการให้บริการจัดหางาน การเลือกปฏิบัติในการคัดกรองผู้สมัครงานตามเชื้อชาติ เพศ ศาสนา หรือความบกพร่องทางร่างกาย

๒) การคุ้มครองข้อมูลส่วนบุคคล ห้ามนำข้อมูลส่วนบุคคลหรือข้อมูลที่ละเอียดอ่อนของประชาชน ผู้สมัครงาน นายจ้าง หรือเจ้าหน้าที่ เช่น เลขประจำตัวประชาชน ข้อมูลสุขภาพ ไปประมวลผลในระบบ AI สาธารณะ โดยต้องปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล (PDPA) อย่างเคร่งครัด

๓) การกำกับดูแลการตัดสินใจที่สำคัญ การใช้ระบบ AI เพื่อสนับสนุนการพิจารณาในกระบวนการที่สำคัญ เช่น การอนุญาต อนุมัติ การพิจารณาความผิด หรือการบังคับใช้กฎหมาย จะต้องมีกระบวนการตรวจสอบและทบทวนผลลัพธ์โดยเจ้าหน้าที่ของรัฐ (Human in the Loop) ทุกครั้ง เพื่อความถูกต้องและเป็นธรรม

๔) การป้องกันการสร้างข้อมูลเท็จ ห้ามใช้ระบบ AI ในการสร้างข้อมูลเท็จ บิดเบือนข้อเท็จจริง หรือปลอมแปลงเอกสารราชการ ภาพ และเสียง (Deepfakes) อันจะทำให้เกิดความเข้าใจผิด หรือก่อให้เกิดความเสียหายต่อราชการและประชาชน

๕) การรักษาความลับทางราชการ ห้ามนำข้อมูลที่เป็นความลับของทางราชการ ข้อมูลภายในของกรมการจัดหางาน หรือข้อมูลที่ยังไม่เปิดเผยต่อสาธารณะ ป้อนเข้าสู่ระบบ AI ภายนอกเพื่อการวิเคราะห์หรือสร้างผลลัพธ์ใดๆ โดยเด็ดขาด

๖) การรักษาความมั่นคงปลอดภัยทางไซเบอร์ ห้ามใช้ระบบ AI ในลักษณะที่เป็นการคุกคาม โจมตี เจาะระบบ (Cyber Attacks) หรือกระทำการใดๆ ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศของกรมการจัดหางานหรือหน่วยงานอื่น

๗) การทบทวนและปรับปรุงแนวปฏิบัติ กรมการจัดหางานจะจัดให้มีการทบทวนและปรับปรุงแนวปฏิบัตินี้อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงทางเทคโนโลยีและบริบทที่เกี่ยวข้อง เพื่อให้มีความเหมาะสมและทันต่อสถานการณ์อย่างต่อเนื่อง