ด่วน

ที่ มท ๐๒๑๐.๕/ว ๑๕๐๑

กระทรวงมหาดไทย
ถนนอัษฎางค์ กทม. ๑๐๒๐๐

๙ เมษายน ๒๕๖๑

เรื่อง การแสดงความคิดเห็นต่อ (ร่าง) กรอบการกำกับดูแลข้อมูล (Data Governance Framework)

เรียน ผู้ว่าราชการจังหวัดทุกจังหวัด

ด้วยสำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) (สรอ.) โดยคณะกรรมการศึกษากระบวนการธรรมาภิบาลและการเปิดเผยข้อมูลดิจิทัลเพื่อการบริหารราชการแผ่นดิน ได้จัดทำ (ร่าง) กรอบการกำกับดูแลข้อมูล (Data Governance Framework) เวอร์ชัน ๑.๐ มีจำนวน ๕๑ หน้า เพื่อขับเคลื่อนการดำเนินงานเรื่อง การจัดการข้อมูลขนาดใหญ่ (Big Data) รวมทั้งให้ดำเนินการจัดตั้งศูนย์ข้อมูลภาครัฐ (Government Data Center) ตามข้อสั่งการของนายกรัฐมนตรีในการประชุมคณะรัฐมนตรี เมื่อวันที่ ๑๒ กันยายน ๒๕๖๐ และวันที่ ๒๖ กันยายน ๒๕๖๐ โดย สรอ. จะรวบรวมความคิดเห็นเสนอต่อคณะกรรมการศึกษากระบวนการธรรมาภิบาลฯ ซึ่งกำหนดประชุมครั้งต่อไปในวันที่ ๒๐ เมษายน ๒๕๖๑ ในการนี้ สรอ. ได้เปิดกว้างต่อการแสดงความคิดเห็นจากทุกภาคส่วน เมื่อจัดทำ (ร่าง) กรอบการกำกับดูแลข้อมูล แล้วเสร็จ สรอ. จะนำเสนอต่อคณะกรรมการขับเคลื่อนการบูรณาการฐานข้อมูลกลางภาครัฐ (ตามคำสั่งสำนักนายกรัฐมนตรี ที่ ๑๘๗/๒๕๕๘ ลงวันที่ ๒๐ กรกฎาคม ๒๕๕๘) ซึ่งมีนายกรัฐมนตรีเป็นประธาน และมีปลัดกระทรวงทุกกระทรวงร่วมเป็นกรรมการ เพื่อพิจารณาต่อไป

เพื่อเป็นการขับเคลื่อนให้เกิดการกำกับดูแลข้อมูลและการเปิดเผยข้อมูลดิจิทัลของหน่วยงานภาครัฐให้เป็นไปอย่างถูกต้องเหมาะสม กระทรวงมหาดไทยจึงขอประชาสัมพันธ์ ดังนี้

๑. ให้จังหวัดรับทราบการประชาพิจารณ์ (ร่าง) กรอบการกำกับดูแลข้อมูล (Data Governance Framework) เวอร์ชัน ๑.๐ โดยสามารถดาวน์โหลด (ร่าง) กรอบดังกล่าวได้ทาง www.ict.moi.go.th หัวข้อ “เรื่องน่าสนใจ” หรือตามรหัสคิวอาร์ (QR Code) ที่ส่งมาพร้อมนี้

๒. แสดงความคิดเห็น (ถ้ามี) และสอบถามข้อมูลเพิ่มเติมได้ที่ นายสุรกิจ สุขพัฒนานรากุล ฝ่ายนวัตกรรม ส่วนมาตรฐานและสถาปัตยกรรมองค์กร สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) โทร. ๐ ๒๖๑๒ ๖๐๐๐ ต่อ ๗๓๐๘ โทรสาร ๐ ๒๖๑๒ ๖๐๑๐ อีเมล : ins_division@ega.or.th ภายในวันที่ ๒๐ เมษายน ๒๕๖๑

จึงเรียนมาเพื่อทราบและพิจารณาดำเนินการต่อไป

ขอแสดงความนับถือ

(นายนิสิต จันทร์สมวงศ์)
รองปลัดกระทรวงมหาดไทย ปฏิบัติราชการแทน
ปลัดกระทรวงมหาดไทย

สำนักงานปลัดกระทรวง
ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
โทร.๐ ๒๒๘๒ ๖๕๖๐-๗๙ ต่อ ๕๑๑๐๑, ๐ ๒๒๘๑ ๗๙๗๙ (วิไลภรณ์)
โทรสาร ๐ ๒๒๘๒ ๖๕๖๐-๗๙ ต่อ ๕๑๕๕๓, ๐ ๒๒๘๑ ๑๕๖๗

ด่วน

บันทึกข้อความ

ส่วนราชการ กระทรวงมหาดไทย สำนักงานปลัดกระทรวงมหาดไทย โทร. ๐ ๒๒๘๑ ๗๙๗๙ (วิไลภรณ์)

ที่ มท ๐๒๑๐.๕/ว ๑๕๑๐ **วันที่** ๙ เมษายน ๒๕๖๑

เรื่อง การแสดงความคิดเห็นต่อ (ร่าง) กรอบการกำกับดูแลข้อมูล (Data Governance Framework)

เรียน หัวหน้าส่วนราชการระดับกรมและหัวหน้าหน่วยงานรัฐวิสาหกิจในสังกัดกระทรวงมหาดไทย

ด้วยสำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) (สรอ.) โดยคณะกรรมการศึกษากระบวนการธรรมาภิบาลและการเปิดเผยข้อมูลดิจิทัลเพื่อการบริหารราชการแผ่นดิน ได้จัดทำ (ร่าง) กรอบการกำกับดูแลข้อมูล (Data Governance Framework) เวอร์ชัน ๑.๐ มีจำนวน ๕๑ หน้า เพื่อขับเคลื่อนการดำเนินงานเรื่อง การจัดการข้อมูลขนาดใหญ่ (Big Data) รวมทั้งให้ดำเนินการจัดตั้งศูนย์ข้อมูลภาครัฐ (Government Data Center) ตามข้อสั่งการของนายกรัฐมนตรีในการประชุมคณะรัฐมนตรี เมื่อวันที่ ๑๒ กันยายน ๒๕๖๐ และวันที่ ๒๖ กันยายน ๒๕๖๐ โดย สรอ. จะรวบรวมความคิดเห็นเสนอต่อคณะกรรมการศึกษากระบวนการธรรมาภิบาลฯ ซึ่งกำหนดประชุมครั้งต่อไปในวันที่ ๒๐ เมษายน ๒๕๖๑ ในการนี้ สรอ. ได้เปิดกว้างต่อการแสดงความคิดเห็นจากทุกภาคส่วน เมื่อจัดทำ (ร่าง) กรอบการกำกับดูแลข้อมูล แล้วเสร็จ สรอ. จะนำเสนอต่อคณะกรรมการขับเคลื่อนการบูรณาการฐานข้อมูลกลางภาครัฐ (ตามคำสั่งสำนักนายกรัฐมนตรี ที่ ๑๘๗/๒๕๕๘ ลงวันที่ ๒๐ กรกฎาคม ๒๕๕๘) ซึ่งมีนายกรัฐมนตรีเป็นประธาน และมีปลัดกระทรวงทุกกระทรวงร่วมเป็นกรรมการ เพื่อพิจารณาต่อไป

เพื่อเป็นการขับเคลื่อนให้เกิดการกำกับดูแลข้อมูลและการเปิดเผยข้อมูลดิจิทัลของหน่วยงานภาครัฐให้เป็นไปอย่างถูกต้องเหมาะสม กระทรวงมหาดไทยจึงขอประชาสัมพันธ์ ดังนี้

๑. ให้ส่วนราชการและหน่วยงานรัฐวิสาหกิจในสังกัดกระทรวงมหาดไทยรับทราบการประชาพิจารณ์ (ร่าง) กรอบการกำกับดูแลข้อมูล (Data Governance Framework) เวอร์ชัน ๑.๐ โดยสามารถดาวน์โหลด (ร่าง) กรอบดังกล่าวได้ทาง www.ict.moi.go.th หัวข้อ “เรื่องน่าสนใจ” หรือตามรหัสคิวอาร์ (QR Code) ที่ส่งมาพร้อมนี้

๒. แสดงความคิดเห็น (ถ้ามี) และสอบถามข้อมูลเพิ่มเติมได้ที่ นายสุรกิจ สุขพัฒนานรากุล ฝ่ายนวัตกรรม ส่วนมาตรฐานและสถาปัตยกรรมองค์กร สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) โทร. ๐ ๒๖๑๒ ๖๐๐๐ ต่อ ๗๓๐๘ โทรสาร ๐ ๒๖๑๒ ๖๐๑๐ อีเมล : ins_division@ega.or.th ภายในวันที่ ๒๐ เมษายน ๒๕๖๑

จึงเรียนมาเพื่อทราบและพิจารณาดำเนินการต่อไป

(นายนิสิต จันทร์สมวงศ์)
รองปลัดกระทรวงมหาดไทย ปฏิบัติราชการแทน
ปลัดกระทรวงมหาดไทย

(Draft) Data Governance Framework

(ร่าง) กรอบการกำกับดูแลข้อมูล

เวอร์ชัน ๑.๐

สารบัญ

สารบัญตาราง

สารบัญภาพ

บทสรุปผู้บริหาร (EXECUTIVE SUMMARY)

ข้อมูลถือเป็นสินทรัพย์ที่สำคัญในการขับเคลื่อนการดำเนินงานของหน่วยงานเพื่อนำไปสู่เป้าหมายที่ได้กำหนดไว้ อย่างไรก็ตาม ณ ปัจจุบันหน่วยงานภาครัฐเผชิญกับอุปสรรคในด้านต่างๆ ที่เกี่ยวกับข้อมูลเป็นอย่างมาก ทั้งในเรื่องของความซ้ำซ้อนของข้อมูล ความมั่นคงปลอดภัยของข้อมูล (เช่น การรักษาความลับ การเข้าถึง และความเป็นส่วนตัว) คุณภาพของข้อมูล (เช่น ความถูกต้อง ความครบถ้วน และความเป็นปัจจุบัน) และการนำข้อมูลไปใช้ประโยชน์อย่างเป็นรูปธรรม ประเด็นเหล่านี้อาจเป็นผลมาจากการบริหารจัดการข้อมูลที่ไม่ครอบคลุมและไม่ชัดเจนของหน่วยงาน ดังนั้นหน่วยงานควรจะต้องมีมาตรการในการบริหารจัดการข้อมูลที่มีประสิทธิภาพ

การกำกับดูแลข้อมูล (Data Governance) ถือเป็นหัวใจสำคัญในการบริหารจัดการข้อมูล (Data Management) กล่าวคือ การกำกับดูแลข้อมูลเป็นกลไกในการกำหนดทิศทาง ควบคุม และทวนสอบการบริหารจัดการข้อมูล เพื่อให้มั่นใจได้ว่าหน่วยงานได้ดำเนินการบริหารจัดการข้อมูลเป็นไปตามนโยบาย กฎระเบียบ หรือข้อบังคับที่ได้กำหนดไว้ การกำกับดูแลข้อมูลที่ดีก่อให้เกิดการบริหารจัดการข้อมูลที่ดี ซึ่งส่งผลให้ข้อมูลมีความมั่นคงปลอดภัย มีคุณภาพ มีคุณค่าทางเศรษฐกิจและสังคม และได้รับความคุ้มทุนต่อการดำเนินงาน

เอกสารฉบับนี้ถูกจัดทำขึ้นเพื่อเป็นกรอบการกำกับดูแลข้อมูล มีองค์ประกอบหลักประกอบด้วย การกำหนดกฎเกณฑ์หรือนโยบายที่เกี่ยวข้องกับการดำเนินงานกับข้อมูล บทบาทและความรับผิดชอบในการกำกับดูแล และกระบวนการกำกับดูแล นั่นคือ บุคคลที่ได้รับบทบาทในการกำกับดูแลจะกำหนดขอบเขตและนโยบายข้อมูลขึ้นมาเพื่อกำกับดูแล ให้บุคคลที่เกี่ยวข้องกับการดำเนินงานกับข้อมูล (ตั้งแต่ สร้าง จัดเก็บ ใช้ เผยแพร่ ถึงทำลาย) สามารถปฏิบัติตามนโยบายที่ได้กำหนดไว้ กรอบการกำกับดูแลนี้จะเป็นแนวทางให้หน่วยงานรัฐ ทั้งส่วนราชการ รัฐวิสาหกิจ องค์การมหาชน และหน่วยงานของรัฐรูปแบบใหม่ นำไปปรับใช้ให้เข้ากับลักษณะเฉพาะของหน่วยงานหรือสถานการณ์ต่าง ๆ ที่เปลี่ยนแปลง

บทที่ ๑ บทนำ (INTRODUCTION)

๑.๑ ความเป็นมา

ข้อมูลจัดว่าเป็นหนึ่งในสินทรัพย์ที่สำคัญ และเป็นกลไกในการขับเคลื่อนการดำเนินงานของหน่วยงานเพื่อนำไปสู่เป้าหมายที่ได้กำหนดไว้ อย่างไรก็ตาม สถานการณ์ด้านการใช้ประโยชน์จากข้อมูลของหน่วยงานภาครัฐในปัจจุบันนั้นยังมีอุปสรรคในด้านต่าง ๆ ทั้งในด้านการจัดเก็บข้อมูล (เช่น ข้อมูลเดียวกันแต่จัดเก็บกระจายไปในหลายระบบ หลายส่วนงาน หรือหลายรูปแบบ) ด้านความมั่นคงปลอดภัยของข้อมูล (เช่น การรักษาความลับ การเข้าถึง และความเป็นส่วนตัว) และด้านคุณภาพของข้อมูล (เช่น ความถูกต้อง ความสมบูรณ์ ความต้องกัน ความเป็นปัจจุบัน ความพร้อมใช้ และตรงต่อการนำไปใช้)

สาเหตุของปัญหานั้นมาจากการขาดการวางแผนในการบริหารจัดการข้อมูลทั้งวงจรชีวิตของข้อมูล (จัดเก็บ ประมวลผล นำไปใช้ เปิดเผย และทำลาย) การบูรณาการข้อมูล อุปสรรคทางกฎระเบียบ รวมถึงการบริหารจัดการที่ไม่ครอบคลุมประเภทของข้อมูล นั่นคือ ข้อมูลที่เป็นโครงสร้าง (เช่น ฐานข้อมูล) กึ่งโครงสร้าง (เช่น เอ็กส์เอ็มแอล) และไม่มีโครงสร้าง (เช่น เสียง ภาพ และภาพเคลื่อนไหว) เป็นต้น

ดังนั้น เพื่อให้การนำข้อมูลไปใช้ก่อให้เกิดประโยชน์อย่างเต็มที่และมีประสิทธิภาพ จะต้องอาศัยกรอบการกำกับดูแลข้อมูล (Data Governance Framework) ที่เอื้อให้หน่วยงานภาครัฐต่าง ๆ สามารถนำไปใช้กำกับดูแล และบริหารจัดการข้อมูลภาครัฐทุกขั้นตอนอย่างเป็นระบบและมีความชัดเจนมากยิ่งขึ้น

๑.๒ วัตถุประสงค์

การจัดทำกรอบการกำกับดูแลข้อมูล เพื่อให้หน่วยงานภาครัฐสามารถนำไปผลักดัน และดำเนินการกำกับดูแลข้อมูล รวมถึงติดตามการบริหารจัดการข้อมูลภาครัฐให้มีความโปร่งใส ตรวจสอบได้ ส่งผลต่อคุณภาพ ความมั่นคงปลอดภัย และบูรณาการข้อมูลได้อย่างครบถ้วน ถูกต้อง และข้อมูลเป็นปัจจุบัน

๑.๓ หน่วยงานภาครัฐที่นำไปใช้

กรอบการกำกับดูแลข้อมูลนี้ครอบคลุมหน่วยงานภาครัฐทั้ง ๔ ประเภท คือ ส่วนราชการ รัฐวิสาหกิจ องค์การมหาชน และหน่วยงานของรัฐรูปแบบใหม่ ดังนี้

๑) ส่วนราชการ หมายถึง หน่วยงานที่รับผิดชอบการให้บริการสาธารณะทางปกครอง ซึ่งเป็นภารกิจหลักของรัฐ ให้บริการเป็นการทั่วไปและไม่มุ่งกำไร และมีความสัมพันธ์กับรัฐ

๒) รัฐวิสาหกิจ หมายถึง หน่วยงานที่รับผิดชอบบริการสาธารณะทางอุตสาหกรรมและพาณิชยกรรม มีวัตถุประสงค์เพื่อการแสวงหารายได้ ต้องสามารถเลี้ยงตัวเองจากการดำเนินงานเชิงพาณิชย์ แต่สามารถรับเงินงบประมาณสนับสนุนเป็นครั้งคราวหรือบางส่วนในบางกรณี

๓) องค์การมหาชน หมายถึง หน่วยงานที่รับผิดชอบบริการสาธารณะทางสังคมและวัฒนธรรม ไม่มีวัตถุประสงค์ในการแสวงหากำไร เป็นนิติบุคคลและมีความสัมพันธ์กับรัฐ ซึ่งประกอบด้วย รัฐจัดตั้ง ได้รับเงินอุดหนุนจากรัฐ หรือสามารถเลี้ยงตัวเองได้ และรัฐมีอำนาจบริหารจัดการ

๔) หน่วยงานของรัฐรูปแบบใหม่ หมายถึง

- องค์การของรัฐที่เป็นอิสระ (Independent Administrative Organization) ซึ่งเป็นหน่วยงานรูปแบบใหม่ที่จัดตั้งขึ้น เพื่อทำหน้าที่ในการควบคุมกำกับดูแลกิจกรรมของรัฐ ตามนโยบายสำคัญที่ต้องการความเป็นกลางอย่างเคร่งครัด
- กองทุนที่เป็นนิติบุคคล ซึ่งเป็นเครื่องมือทางเศรษฐกิจของรัฐ หมายถึง นิติบุคคลที่จัดตั้งขึ้นโดยตราเป็นพระราชบัญญัติ เนื่องจากต้องการอำนาจรัฐในการบังคับฝ่ายเดียวต่อภาคเอกชนหรือประชาชน ในการสมทบเงินเข้ากองทุน

๑.๔ ขอบเขตของเนื้อหาภายในกรอบการกำกับดูแลข้อมูล

ขอบเขตของกรอบการกำกับดูแลข้อมูลในเอกสารฉบับนี้ ประกอบด้วย บทที่ ๒ อธิบายถึงแนวคิดการกำกับดูแลข้อมูล เพื่อให้เข้าใจถึงความหมายของการกำกับดูแลข้อมูลและความสัมพันธ์กับการบริหารจัดการข้อมูล ประกอบไปด้วย นิยามของข้อมูล การบริหารจัดการข้อมูล ธรรมาธิบาลข้อมูล ความสัมพันธ์ระหว่างการบริหารจัดการข้อมูลกับธรรมาธิบาลข้อมูล และกรอบนโยบายข้อมูล บทที่ ๓ กล่าวถึงแก่นของกรอบการกำกับดูแลข้อมูล ประกอบด้วย สภาพแวดล้อมของการกำกับดูแลข้อมูล โครงสร้างของการกำกับดูแลข้อมูล กระบวนการกำกับดูแลข้อมูล การวัดการดำเนินการและประสิทธิภาพของการกำกับดูแลข้อมูล และแนวทางในการกำกับดูแลข้อมูล

บทที่ ๒ แนวคิดการกำกับดูแลข้อมูล (DATA GOVERNANCE CONCEPT)

๒.๑ ข้อมูล (Data)

ข้อมูล คือ “ข้อเท็จจริงซึ่งใช้เป็นพื้นฐานสำหรับการอธิบายเหตุผล การสนทนา หรือการคำนวณ[1] ข้อมูลเป็นองค์ประกอบหลักในการดำเนินงาน ซึ่งมีความสัมพันธ์กับกระบวนการปฏิบัติงาน เทคโนโลยีสารสนเทศ รวมถึงบุคคลากร เมื่อข้อมูลถูกใช้เป็นเครื่องมือในการขับเคลื่อนหน่วยงาน ข้อมูลจึงเปรียบเสมือนสินทรัพย์ที่มีความสำคัญเช่นเดียวกับสินทรัพย์ประเภทอื่น

ดังนั้นหน่วยงานจึงจำเป็นต้องมีมาตรการในการรักษาความมั่นคงปลอดภัยและคุณภาพของข้อมูล เช่น การรักษาความลับของข้อมูล (Confidentiality) การป้องกันไม่ให้เกิดเหตุการณ์ที่ทำให้ไม่สามารถใช้งานข้อมูลได้ (Loss of Availability) การรักษาความถูกต้องครบถ้วนของข้อมูล (Integrity) และทำให้ข้อมูลเป็นปัจจุบันอยู่เสมอ (Timeliness) เพื่อตอบสนองต่อการตัดสินใจได้อย่างมีประสิทธิภาพทั้งระดับปฏิบัติการและระดับยุทธศาสตร์

๒.๒ บัญชีข้อมูล (Data Catalog)

บัญชีข้อมูล คือ “รายการของชุดข้อมูล (Datasets) ที่หน่วยงานถือครองหรือบริหารจัดการ” (Australian Institute of Health and Welfare, 2014) บัญชีข้อมูลถูกใช้เป็นเครื่องมืออำนวยความสะดวกในการค้นหาชุดข้อมูลที่ต้องการ เพื่อแสดงเมทาดาตา (Metadata) หรือคำอธิบายเกี่ยวกับชุดข้อมูล เช่น ชื่อเจ้าของข้อมูล วันที่เริ่มต้นใช้งาน วันที่ทำการเปลี่ยนแปลงข้อมูลล่าสุด วัตถุประสงค์ในการจัดเก็บ และสถานที่จัดเก็บ บัญชีข้อมูลอาจจะอยู่ในรูปของตารางรายชื่อชุดข้อมูล หรือถูกพัฒนาเป็นแอปพลิเคชันซึ่งจะเพิ่มประสิทธิภาพในการค้นหาได้ดียิ่งขึ้น

๒.๓ นิยามของการกำกับดูแลข้อมูล (Data Governance)

การกำกับดูแลข้อมูล (Data Governance) ได้มีผู้เชี่ยวชาญจากหน่วยงานต่าง ๆ ให้คำนิยามไว้ดังต่อไปนี้

“กิจกรรมที่ประกอบด้วยการกำหนดอำนาจ การควบคุม และการตัดสินใจในการบริหารจัดการข้อมูล โดยที่ข้อมูลถูกจัดให้เป็นหนึ่งในสินทรัพย์ของหน่วยงาน” (Askham, N. ,2016)

“ระบบที่กำหนดถึงอำนาจการตัดสินใจ และหน้าที่ความรับผิดชอบต่อกระบวนการที่เกี่ยวข้องกับข้อมูล โดยที่มีแบบแผนที่ชัดเจนและได้รับการยอมรับ ซึ่งแบบแผนดังกล่าวต้องสามารถอธิบายได้ว่า ใครมีบทบาทในการทำอะไรกับข้อมูลชุดไหน เมื่อไหร่ ใช้หลักการและวิธีการใดในการใช้ข้อมูล” (Data Governance Institute, n.d.)

“การกำหนดสิทธิ์และการควบคุม (การวางแผน การตรวจสอบ และการบังคับ) ในการบริหารจัดการข้อมูล” (DAMA International, 2009)

[1] https://www.merriam-webster.com/dictionary/data

“การจัดการข้อมูล จากมุมมองที่เกี่ยวข้องกับข้อมูล ทำให้องค์กรตระหนักถึงการจัดทำมาตรฐานข้อมูลที่เป็นระบบและการบูรณาการข้อมูล ทั้งข้อมูลที่อยู่ในระบบ ข้อมูลที่สัมพันธ์กับการดำเนินงานขององค์กร นโยบาย และกระบวนการปฏิบัติงานต่างๆ” (Kim, H. Y., & Cho, J. S., 2017)

จากนิยามต่าง ๆ ข้างต้น จึงได้ข้อสรุปว่า การกำกับดูแลข้อมูล (Data Governance) คือ “การกำหนดสิทธิในการตัดสินใจและความรับผิดชอบ ในการส่งเสริมให้เกิดกระบวนการจัดทำ การใช้งาน และการบริหารจัดการข้อมูล รวมถึงกระบวนการที่กำหนดบทบาท นโยบาย และมาตรฐาน ที่ช่วยสนับสนุนให้การดำเนินงานเกี่ยวกับข้อมูลมีประสิทธิภาพมากยิ่งขึ้น ซึ่งส่งผลให้หน่วยงานสามารถบรรลุเป้าหมายได้”

ในมุมมองของภาครัฐ การกำกับดูแลข้อมูลรัฐ (Government Data Governance) หมายถึง “การกำหนดสิทธิ หน้าที่ และความรับผิดชอบของผู้มีส่วนได้ส่วนเสียในการบริหารจัดการข้อมูลทุกขั้นตอน เพื่อให้การได้มาและการนำไปใช้ข้อมูลของหน่วยงาน ได้ถูกต้อง ครบถ้วน เป็นปัจจุบัน และสามารถเชื่อมโยงกันได้อย่างมีประสิทธิภาพและมั่นคงปลอดภัย โดยใช้ข้อมูลเป็นหลักในการขับเคลื่อนประเทศ เช่น การใช้ข้อมูลในการวิเคราะห์การตัดสินใจเชิงนโยบายและการบริหารราชการแผ่นดิน การเพิ่มประสิทธิภาพในการบริการประชาชน การเสริมสร้างและผลักดันธุรกิจที่เกิดจากการใช้นวัตกรรมข้อมูล”

ทั้งนี้องค์ประกอบหลักของธรรมาภิบาลข้อมูลที่ดีควรประกอบด้วย สามารถควบคุมวงจรชีวิตของข้อมูล มีนโยบายข้อมูลที่ชัดเจน มีการกำหนดบทบาทหน้าที่ของเจ้าของข้อมูล ข้อมูลมีเมทาดาตา ข้อมูลมีคุณภาพ ข้อมูลมีความมั่นคงปลอดภัย และรักษาความเป็นส่วนตัว (IGGI, 2005)

๒.๔ การบริหารจัดการข้อมูล (Data Management)

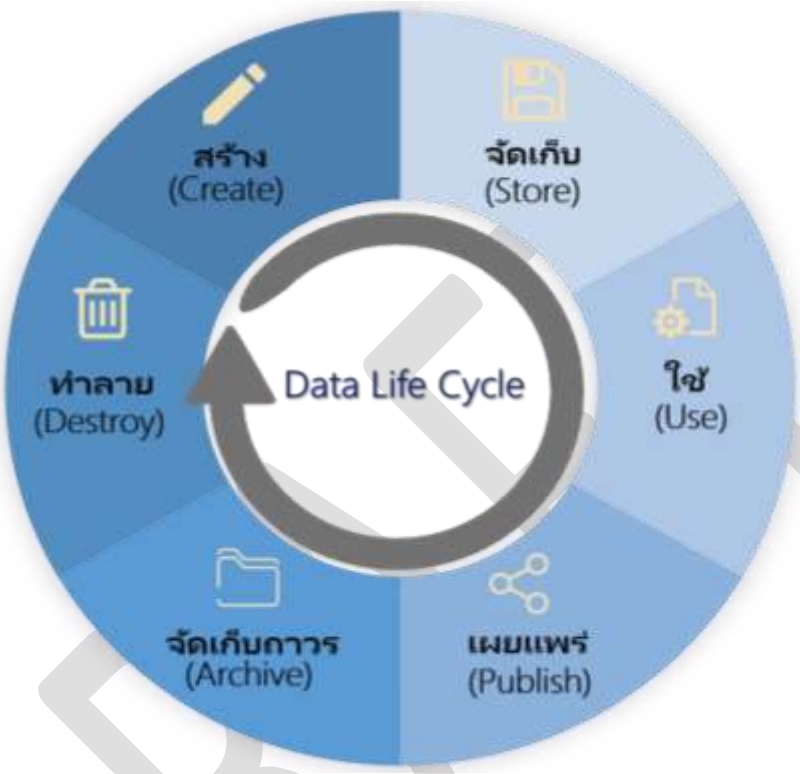
การบริหารจัดการข้อมูล คือ คำจำกัดความที่อธิบายถึงกระบวนการที่ใช้ในการวางแผน (Plan) ระบุ (Specify) เปิดใช้งาน (Enable) สร้าง (Create) รับ (Acquire) ดูแลรักษา (Maintain) ใช้ (Use) จัดเก็บถาวร (Archive) ดึงข้อมูล (Retrieve) ควบคุม (Control) และทำลายข้อมูล (Purge) (DAMA International, 2012) การบริหารจัดการข้อมูลเป็นสิ่งสำคัญสำหรับทุกหน่วยงาน โดยแต่ละหน่วยงานต่างต้องตระหนักว่าข้อมูลที่มีอยู่เป็นสินทรัพย์ที่มีค่า และเนื่องจากการเกิดขึ้นของข้อมูลที่มีปริมาณมหาศาล ไม่ว่าจะเป็นข้อมูลที่รวบรวมมาโดยอัตโนมัติจากระบบหรืออุปกรณ์ต่าง ๆ หรือข้อมูลที่เกิดขึ้นจากการป้อนข้อมูลหรือโต้ตอบกับผู้ใช้งาน ดังนั้นเพื่อให้หน่วยงานสามารถนำข้อมูลเหล่านี้ไปประมวลผลหรือใช้ในการตัดสินใจได้อย่างแม่นยำ จึงต้องได้รับการบริหารจัดการอย่างถูกต้องและเหมาะสม ตามวัตถุประสงค์สำหรับการบริหารจัดการข้อมูลของแต่ละหน่วยงาน ตัวอย่างเช่น

๑) เพื่อการจัดเก็บ นำมาใช้งาน และประมวลผลข้อมูลตามที่หน่วยงานต้องการ
๒) เพื่อควบคุม ตรวจสอบ และป้องกัน โดยใช้กระบวนการกำกับดูแลข้อมูลและความปลอดภัยของข้อมูล
๓) เพื่อจัดหมวดหมู่ และกำหนดมาตรฐานของข้อมูล โดยใช้การจำแนกข้อมูล และกำหนดกรอบการทำงานที่เป็นที่รู้จักแพร่หลาย
๔) เพื่อให้สามารถนำข้อมูลกลับมาใช้ได้ในภายหลัง โดยกำหนดข้อมูลให้อยู่ในรูปแบบที่เรียกใช้ได้อย่างมีประสิทธิภาพ
๕) เพื่อการปรับปรุงข้อมูลให้เป็นปัจจุบัน และมีความถูกต้องสมบูรณ์อยู่เสมอ

๖) เพื่อการปกป้องข้อมูลจากการลักลอบใช้งานหรือแก้ไขโดยมิชอบ รวมถึงจากเหตุการณ์ที่อาจเกิดจากภัยธรรมชาติหรือความบกพร่องภายในระบบคอมพิวเตอร์

๒.๔.๑ วงจรชีวิตของข้อมูล (Data Lifecycle)

วงจรชีวิตของข้อมูล คือ ลำดับขั้นตอนของข้อมูลตั้งแต่เริ่มสร้างข้อมูลไปจนถึงการทำลายข้อมูล ประกอบด้วย ๖ ขั้นตอน ดังต่อไปนี้



รูปที่ ๑ วงจรชีวิตของข้อมูล (Data Lifecycle)

๑) การสร้าง (Create) ประกอบด้วย การสร้างข้อมูลขึ้นมาใหม่จากการบันทึกเข้าไปด้วยมนุษย์หรืออุปกรณ์อิเล็กทรอนิกส์ (เช่น Sensor และอุปกรณ์ Internet of Things) การซื้อหรือการรับข้อมูลจากหน่วยงานอื่น

๒) การจัดเก็บ (Store) เป็นการเก็บรวบรวมข้อมูลที่เกิดจากการสร้างให้มีระเบียบ ง่ายต่อการใช้งาน ไม่สูญหายหรือถูกทำลาย และให้ผู้ใช้งานสามารถประมวลผลข้อมูลต่าง ๆ ตามความต้องการได้อย่างรวดเร็ว ไม่ว่าจะจัดเก็บลงแฟ้มข้อมูล (File) หรือระบบการจัดการฐานข้อมูล (Database Management System - DBMS)

๓) การใช้ (Use) เป็นการนำข้อมูลที่เก็บรวบรวมไว้มาประมวลผล (เช่น การถ่ายโอนข้อมูล การเปลี่ยนรูปแบบการจัดเก็บข้อมูล การวิเคราะห์ข้อมูล และการจัดทำรายงาน) เพื่อนำมาใช้ประโยชน์ตามวัตถุประสงค์

๔) การเผยแพร่ (Publish) ประกอบไปด้วย การแชร์ข้อมูล (Sharing) การกระจายข้อมูล (Dissemination) การควบคุมการเข้าถึง (Access Control) และการกำหนดเงื่อนไขในการนำข้อมูลไปใช้ (Condition)

๕) การจัดเก็บถาวร (Archive) เป็นการคัดลอกเอาข้อมูลที่ใช้งานอยู่มาเก็บรักษา โดยที่ข้อมูลนั้นจะไม่มีการลบ ปรับปรุง หรือแก้ไข แต่สามารถนำกลับไปใช้ใหม่ได้เมื่อมีความต้องการ

๖) การทำลาย (Destroy) เป็นการทำลายข้อมูล ซึ่งปกติจะเป็นการทำลายข้อมูลที่มีการจัดเก็บถาวรเป็นระยะเวลานาน ๆ หรือนานมากกว่าระยะเวลาที่กำหนด

๒.๔.๒ องค์ประกอบในการบริหารจัดการข้อมูล

สมาคมบริหารจัดการข้อมูลระหว่างประเทศ (Data Management Association International) ได้กำหนดองค์ประกอบในการบริหารจัดการข้อมูลเป็น ๑๐ องค์ประกอบ ดังนี้

๑) สถาปัตยกรรมข้อมูล (Data Architecture)
๒) การจำลองและการออกแบบข้อมูล (Data Modeling and Design)
๓) การจัดเก็บและการดำเนินการกับข้อมูล (Data Storage and Operations)
๔) การบูรณาการและการทำงานร่วมกัน (Data Integration and Interoperability)
๕) เอกสารและเนื้อหา (Documents and Content)
๖) ข้อมูลหลักและข้อมูลอ้างอิง (Master and Reference Data)
๗) คลังข้อมูล ทะเลสาบข้อมูล ระบบรายงานอัจฉริยะ และดาตาอนาไลติกส์ (Data Warehouse, Data Lake, Business Intelligence, and Data Analytics)
๘) เมทาดาตา (Metadata)
๙) ความมั่นคงปลอดภัยและการรักษาความเป็นส่วนบุคคลของข้อมูล (Data Security and Privacy)
๑๐) คุณภาพของข้อมูล (Data Quality)

๒.๔.๒.๑ สถาปัตยกรรมข้อมูล (Data Architecture)

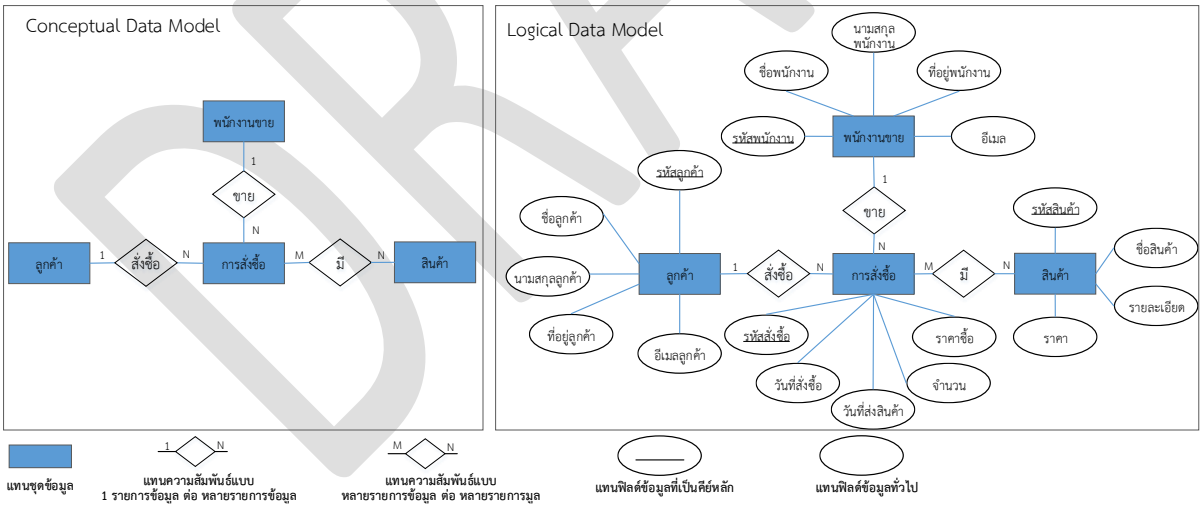
สถาปัตยกรรมข้อมูล (Data Architecture) เป็นส่วนหนึ่งของการพัฒนาสถาปัตยกรรมองค์กร (Enterprise Architecture) เป็นการอธิบายเกี่ยวกับกลุ่มข้อมูลทั้งหมดในหน่วยงาน ความสัมพันธ์ระหว่างข้อมูลกับกระบวนการธุรกิจ ความสัมพันธ์ระหว่างข้อมูลกับแอปพลิเคชัน สถาปัตยกรรมเทคโนโลยีข้อมูล สถาปัตยกรรมการบูรณาการข้อมูล และสถาปัตยกรรมเมทาดาตา เป็นต้น สถาปัตยกรรมข้อมูลช่วยให้มองเห็นภาพรวมของข้อมูลทั้งหน่วยงาน ซึ่งเป็นสิ่งจำเป็นในการวางแผนบริหารจัดการข้อมูล

วิธีดำเนินการ	• ทำความเข้าใจกับความต้องการข้อมูลหน่วยงาน • พัฒนาและดูแลแบบจำลองข้อมูลหน่วยงาน • สร้างความสอดคล้องกับข้อมูลหน่วยงานกับส่วนอื่นๆที่เกี่ยวข้อง เช่น ส่วนงาน กระบวนการธุรกิจ และแอปพลิเคชัน เป็นต้น กำหนดและดูแลสถาปัตยกรรมเทคโนโลยีข้อมูล
เครื่องมือ	• เครื่องมือจัดทำแบบจำลองข้อมูล (Data Modeling Tool) สำหรับจัดทำแบบจำลองข้อมูลระดับหน่วยงาน • เครื่องมือบริหารจัดการแบบจำลอง (Model Management Tool) สำหรับจัดเก็บแบบจำลองข้อมูลและควบคุมเวอร์ชันของแบบจำลองข้อมูล

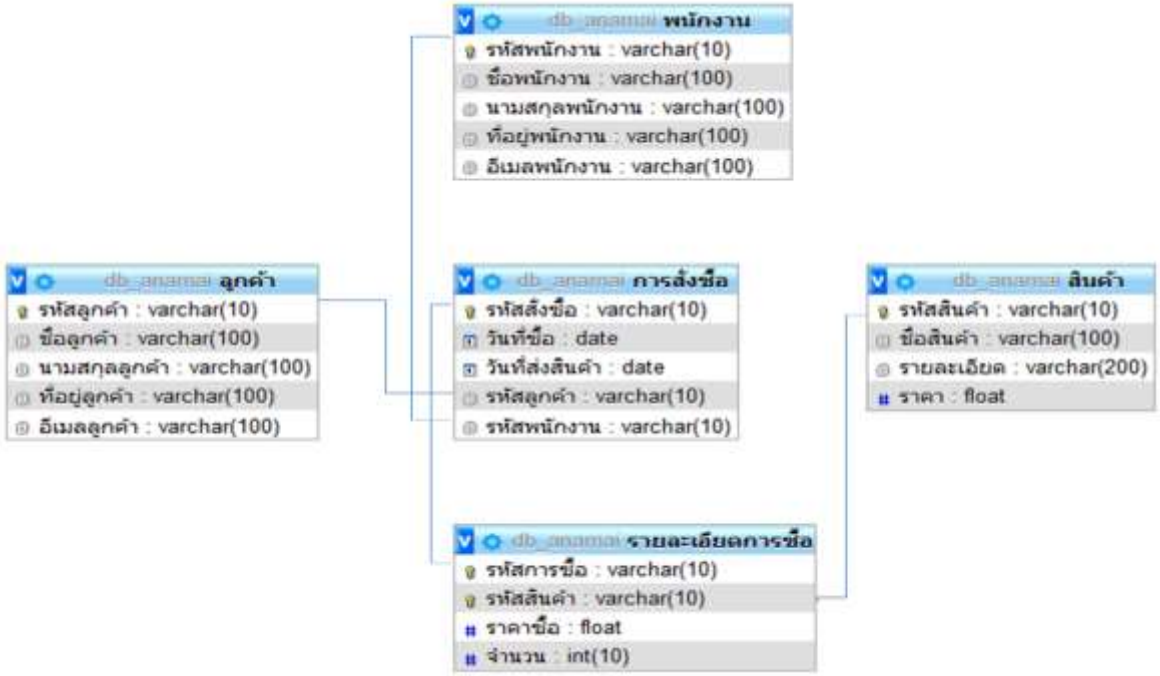
ผลที่ได้รับ	• แบบจำลองข้อมูลระดับหน่วยงาน (Enterprise Data Model) • ความสัมพันธ์ระหว่างข้อมูลกับส่วนงาน ข้อมูลกับกระบวนการธุรกิจ และข้อมูลกับแอปพลิเคชัน เป็นต้น • สถาปัตยกรรมเทคโนโลยีข้อมูล (Data Technology Architecture)
ผู้ที่เกี่ยวข้อง	• สถาปนิกข้อมูล (Data Architect) ทำหน้าที่พัฒนาสถาปัตยกรรมข้อมูลในภาพรวมของทั้งหน่วยงาน

๒.๔.๒.๒ การจำลองและการออกแบบข้อมูล (Data Modeling and Design)

การจำลองและการออกแบบข้อมูล (Data Modeling and Design) เป็นวิธีการวิเคราะห์ความต้องการของผู้ใช้งานระบบด้วยไดอะแกรม (Diagram) และข้อกำหนดต่าง ๆ ที่เกี่ยวข้อง ซึ่งเป็นเครื่องมือในการสื่อสารภายในหน่วยงานให้เข้าใจตรงกัน ในการระบุและกำหนดความต้องการข้อมูล ออกแบบโครงสร้างข้อมูล รวมถึงการแก้ปัญหาอื่น ๆ ตามความต้องการ ไดอะแกรมจะแสดงความสัมพันธ์ระหว่างข้อมูลที่เกี่ยวข้องกันพร้อมทั้งให้รายละเอียดโครงสร้างข้อมูล ไดอะแกรมถูกแบ่งออกเป็น ๓ ระดับ นั่นคือ แบบจำลองข้อมูลเชิงความคิด (Conceptual Data Model) แบบจำลองข้อมูลเชิงตรรกะ (Logical Data Model) และแบบจำลองข้อมูลเชิงกายภาพ (Physical Data Model) โดยการสร้างแบบจำลองและการออกแบบข้อมูลจะเริ่มตั้งแต่การวิเคราะห์ความต้องการของผู้ใช้ระบบ เพื่อกำหนด Conceptual Data Model ของข้อมูล หลังจากนั้นจะมีการกำหนด Logical Data Model ซึ่งให้รายละเอียดที่มากขึ้น จนกระทั่งออกแบบ Physical Data Model ในลำดับถัดมา



รูปที่ ๒ ตัวอย่าง Conceptual Data Model และ Logical Data Model สำหรับระบบการสั่งซื้อสินค้า



รูปที่ ๓ ตัวอย่าง Physical Data Model สำหรับระบบการสั่งซื้อสินค้า

จากรูปที่ ๒ Conceptual Data Model จะแสดงความสัมพันธ์ระหว่างข้อมูลลูกค้า ข้อมูลการสั่งซื้อ ข้อมูลพนักงาน และข้อมูลสินค้า ตัวอย่างเช่น ลูกค้า ๑ คน สามารถสั่งซื้อสินค้าได้หลายครั้ง (1:N) และการสั่งซื้อ ๑ ครั้งได้หลายสินค้า ขณะที่ ๑ สินค้าถูกซื้อได้หลายครั้ง (M:N) เป็นต้น ใน Logical Data Model จะเพิ่มรายละเอียดในส่วนของฟิลด์ข้อมูล เช่น ข้อมูลลูกค้าประกอบด้วย รหัสลูกค้า ชื่อลูกค้า นามสกุลลูกค้า ที่อยู่ลูกค้า และอีเมลลูกค้า จากรูปที่ ๓ Physical Data Model จะให้รายละเอียดทางด้านเทคนิค เช่น ประเภทข้อมูลและความกว้างของฟิลด์ข้อมูล เช่น รหัสลูกค้ามีประเภทข้อมูลเป็นข้อความ (Varchar) ด้วยความกว้าง ๑๐ ตัวอักษร และชื่อลูกค้ามีประเภทข้อมูลเป็นข้อความด้วยความกว้าง ๑๐๐ ตัวอักษร เป็นต้น

วิธีการดำเนินการ	• วิเคราะห์ความต้องการข้อมูลของหน่วยงาน • ออกแบบและพัฒนาแบบจำลองของข้อมูล รวมถึงฐานข้อมูล
เครื่องมือที่ใช้	• เครื่องมือจัดทำแบบจำลองข้อมูล (Data Modeling Tool) • เครื่องมือบริหารจัดการแบบจำลอง (Model Management Tool) • ระบบการจัดการฐานข้อมูล (Database Management System - DBMS)
ผลที่ได้รับ	• ความต้องการของข้อมูล (Data Requirement) และข้อกำหนดทางธุรกิจ (Business Rules) • แบบจำลองข้อมูลเชิงแนวคิด (Conceptual Data Models) • แบบจำลองข้อมูลเชิงตรรกะ (Logical Data Models) • แบบจำลองข้อมูลเชิงกายภาพ (Pysical Data Models)
ผู้เกี่ยวข้อง	• สถาปนิกข้อมูล (Data Architect) • นักออกแบบข้อมูล (Data Modeler)

๒.๔.๒.๓ การจัดเก็บและการดำเนินการกับข้อมูล (Data Storage and Operations)

การจัดเก็บและการดำเนินการกับข้อมูล (Data Storage and Operations) เป็นการดำเนินการเพื่อจัดเก็บข้อมูล สำรองข้อมูล กู้คืนข้อมูล และปรับปรุงประสิทธิภาพของฐานข้อมูลให้พร้อมใช้งานตลอดเวลา เพื่อรักษาความมั่นคงปลอดภัยและความถูกต้องของข้อมูล

วิธีการดำเนินการ	• สนับสนุนในส่วนของฐานข้อมูล เช่น การจัดเก็บ การสำรอง การกู้คืน และปรับปรุงประสิทธิภาพของระบบการจัดการฐานข้อมูล • จัดการในส่วนของเทคโนโลยีด้านข้อมูล เช่น ศึกษาความต้องการของเทคโนโลยีด้านข้อมูล
เครื่องมือที่ใช้	• ระบบการจัดการฐานข้อมูล (Database Management System - DBMS) • เครื่องมือบริหารจัดการฐานข้อมูล (Database Administration Tool)
ผลที่ได้รับ	• แผนการสำรองและข้อมูลได้รับการสำรอง • แผนการกู้คืนข้อมูลและข้อมูลได้รับการกู้คืน • เกิดความต่อเนื่องทางธุรกิจ
ผู้เกี่ยวข้อง	• ผู้ดูแลระบบฐานข้อมูล (Database Administrator - DBA)

๒.๔.๒.๔ การบูรณาการและความสามารถในการทำงานร่วมกัน (Data Integration and Interoperability)

การบูรณาการข้อมูล (Data Integration) เป็นการรวบรวมข้อมูลจากหลาย ๆ แหล่งเข้ามาอยู่แหล่งเดียวกัน ซึ่งมักจะนำไปใช้ในการจัดทำข้อมูลหลัก (Master Data) คลังข้อมูล (Data Warehouse) ทะเลสาบข้อมูล (Data Lake) และการแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน รูปที่ ๕ แสดงความสัมพันธ์ระหว่างการบูรณาการข้อมูล คลังข้อมูล และทะเลสาบข้อมูล ความสามารถในการทำงานร่วมกัน (Interoperability) อ้างถึงคุณลักษณะของระบบต่าง ๆ ที่สามารถแลกเปลี่ยนข้อมูลกันหรือสื่อสารกันได้ด้วยมาตรฐานหรือข้อตกลงร่วมกันระหว่างระบบ เช่น การแลกเปลี่ยนข้อมูลผ่าน Application Programming Interfaces – API นั่นหมายความว่า การบูรณาการข้อมูลจะช่วยควบคุมคุณภาพข้อมูล ขณะที่การแลกเปลี่ยนข้อมูลจะสนับสนุนให้เกิดประสิทธิภาพของการดำเนินงานระหว่างส่วนงานหรือหน่วยงาน

วิธีการดำเนินการ	• กำหนดมาตรฐานและแบบจำลองอ้างอิงของการทำงานร่วมกัน • พัฒนาแผนการดำเนินงานการบูรณาการและการทำงานร่วมกัน
เครื่องมือที่ใช้	• Data Modelling Tool
ผลที่ได้รับ	• รายละเอียดของสิ่งที่เกี่ยวข้อง เช่น ฐานข้อมูล API

ผู้เกี่ยวข้อง	• สถาปนิกบูรณาการข้อมูล (Data Integration Architect) ทำหน้าที่ในการออกแบบกระบวนการและเทคโนโลยีในการบูรณาการข้อมูล • ผู้เชี่ยวชาญการบูรณาการข้อมูล (Data Integration Sepecialist) ทำหน้าที่ดำเนินการบูรณาการข้อมูลสอดคล้องกับที่ได้ออกแบบไว้ เช่น การดำเนินการตามกระบวนการ Extract Transform Load (ETL)

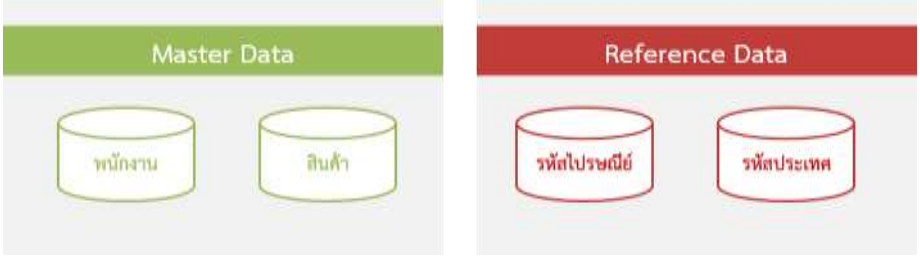
๒.๔.๒.๕ เอกสารและเนื้อหา (Documents and Content)

การบริหารจัดการเอกสารและเนื้อหา (Documents and Content) เป็นการวางแผนและการควบคุมกิจกรรมต่าง ๆ ที่เกี่ยวข้องกับเอกสารและเนื้อหา เช่น การจัดเก็บ การป้องกันความเสียหาย และการเข้าถึงข้อมูล ทั้งที่เก็บอยู่ในรูปแบบกระดาษและไฟล์อิเล็กทรอนิกส์ เช่น ข้อความ รูปภาพ เสียง และภาพเคลื่อนไหว เป็นต้น

วิธีการดำเนินการ	• พัฒนาระบบจัดการเอกสาร เพื่อการจัดเก็บ การเข้าถึง และการควบคุมความปลอดภัย
เครื่องมือที่ใช้	• Document Management Tool • Content Management Tool
ผลที่ได้รับ	• เอกสารหรือรายงาน
ผู้เกี่ยวข้อง	• พนักงานหรือเจ้าหน้าที่

๒.๔.๒.๖ ข้อมูลหลักและข้อมูลอ้างอิง (Master and Reference Data)

ข้อมูลหลักและข้อมูลอ้างอิง (Master and Reference Data) เป็นการจัดการข้อมูลเพื่อใช้ร่วมกันตลอดทั้งหน่วยงาน ซึ่งจะลดความซ้ำซ้อนและสร้างความมั่นใจว่าข้อมูลมีคุณภาพ นั่นคือ จะต้องมีการกำหนดมาตรฐานของข้อมูล จัดเก็บไว้จุดเดียวแล้วแชร์ข้อมูล (Share) ไปตลอดทั้งหน่วยงาน ความแตกต่างระหว่างข้อมูลหลัก (Master Data) กับข้อมูลอ้างอิง (Reference Data) คือข้อมูลอ้างอิงจะมีการเพิ่มหรือเปลี่ยนแปลงน้อย เช่น รหัสไปรษณีย์ รหัสประเทศ และหน่วยวัดระยะทาง ขณะที่ข้อมูลหลักมีโอกาสเพิ่มหรือเปลี่ยนแปลงได้ง่าย มีรายละเอียดหรือจำนวนฟิลด์ข้อมูลที่มาก และเป็นข้อมูลหลักที่ใช้ในการดำเนินงาน เช่น ข้อมูลพนักงาน ข้อมูลลูกค้า ข้อมูลผู้ขาย ข้อมูลสินค้า ข้อมูลพัสดุ และข้อมูลสถานที่ ดังแสดงในรูปที่ ๔



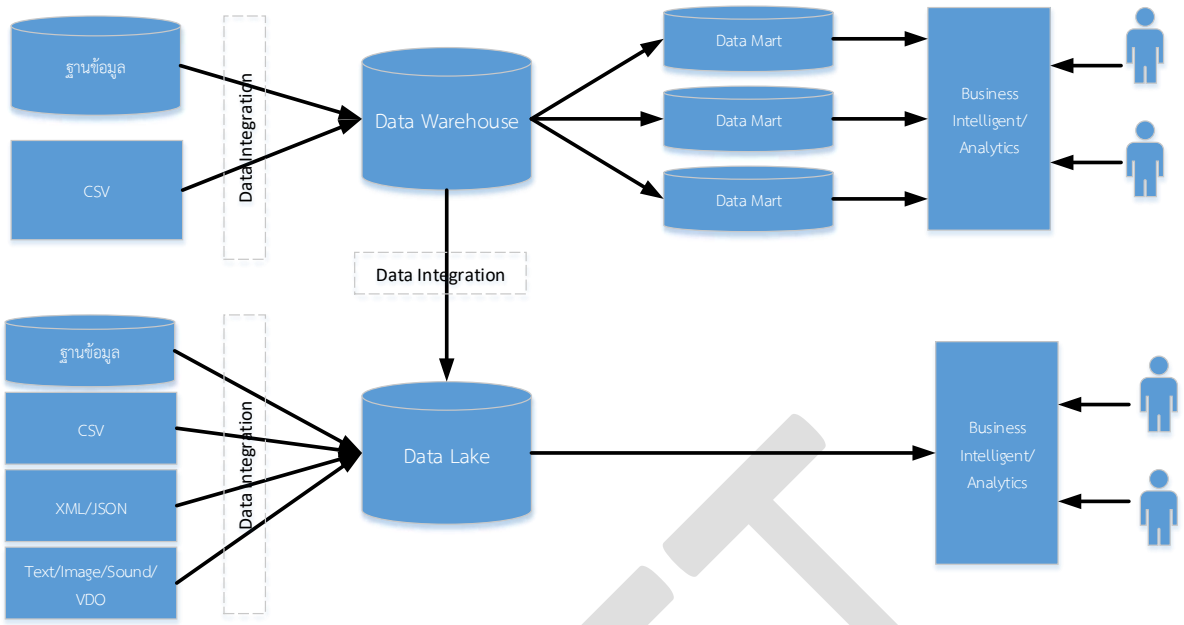
รูปที่ ๔ ตัวอย่างของข้อมูลหลักและข้อมูลอ้างอิง

วิธีการดำเนินการ	• ทำความเข้าใจเกี่ยวกับความต้องการข้อมูลทั้งข้อมูลหลักและข้อมูลอ้างอิง • กำหนดแหล่งที่มา (Source) ของข้อมูลหลักและข้อมูลอ้างอิง • ดำเนินการจัดทำข้อมูลหลักและข้อมูลอ้างอิง
เครื่องมือที่ใช้	• Master Data Management Tools • Reference Data Management Tools • Data Modelling Tools • Data Integration Tools
ผลที่ได้รับ	• ข้อมูลหลักและข้อมูลอ้างอิง
ผู้เกี่ยวข้อง	• สถาปนิกข้อมูล (Data Architect) • นักออกแบบข้อมูล (Data Modeler) • สถาปนิกบูรณาการข้อมูล (Data Integration Architect) • ผู้เชี่ยวชาญการบูรณาการข้อมูล (Data Integration Sepecialist)

๒.๔.๒.๗ คลังข้อมูล ทะเลสาบข้อมูล ระบบรายงานอัจฉริยะ และดาตาอนาไลติกส์ (Data Warehouse, Data Lake, Business Intelligence, and Data Analytics)

คลังข้อมูล (Data Warehouse) จะถูกใช้เป็นแหล่งเก็บข้อมูลกลางโดยอาศัยการบูรณาการข้อมูล (Data Integration) เพื่อรวบรวมข้อมูลจากแหล่งต่าง ๆ ข้อมูลที่อยู่ในคลังข้อมูลจะถูกจัดทำให้อยู่ในรูปแบบที่เหมาะสมสำหรับการนำไปวิเคราะห์ข้อมูล ทั้งในรูปแบบของรายงานอัจฉริยะ (Business Intelligence) และดาตาอนาไลติกส์ (Data Analytics)

ทะเลสาบข้อมูล (Data Lake) เป็นแหล่งการเก็บรักษาข้อมูลหลายรูปแบบ โดยที่ข้อมูลเหล่านี้ถูกเก็บรักษาไว้ในรูปแบบที่ใกล้เคียง หรือเหมือนกับรูปแบบที่ได้รับมาจากแหล่งข้อมูลต้นฉบับ และเป็นที่เก็บรักษาสำรองสำหรับข้อมูลต้นฉบับ



รูปที่ ๕ ความสัมพันธ์ระหว่างคลังข้อมูล ทะเลสาบข้อมูล ระบบรายงานอัจฉริยะ และดาตาอนาไลติกส์

จากรูปที่ ๕ คลังข้อมูลและทะเลสาบข้อมูลจะเกิดจากการรวบรวมข้อมูลจากแหล่งต่าง ๆ ซึ่งแต่ละแหล่งอาจจะมีรูปแบบของข้อมูลที่แตกต่างกัน การรวบรวมมักอาศัยวิธีการบูรณาการข้อมูล (ดูที่หัวข้อ ๒.๔.๒.๕) โดยข้อมูลจากคลังข้อมูลอาจจะถูกรวมเข้าไปยังทะเลสาบข้อมูลสำหรับการวิเคราะห์ข้อมูลที่ซับซ้อนยิ่งขึ้น ข้อมูลในคลังข้อมูลจะต้องถูกจัดกลุ่มออกเป็น ตลาดข้อมูล (Data Mart) สอดคล้องกับส่วนงานที่จะนำไปใช้ เช่น ตลาดข้อมูลของฝ่ายบุคคล ตลาดข้อมูลของฝ่ายการตลาด และตลาดข้อมูลของฝ่ายการเงิน เป็นต้น หลังจากนั้นตลาดข้อมูลก็จะถูกใช้สำหรับการทำรายงานอัจฉริยะ หรือการทำนายสิ่งที่จะเกิดขึ้นในอนาคตผ่านวิธีการของดาตาอนาไลติกส์

ในกรณีของทะเลสาบข้อมูลสามารถนำข้อมูลไปทำรายงานอัจฉริยะและดาตาอนาไลติกส์โดยไม่จำเป็นต้องสร้างตลาดข้อมูลหลังจากนั้นรายงานอัจฉริยะและผลการทำนายจะถูกนำไปใช้สำหรับสนับสนุนการตัดสินใจทั้งในระดับปฏิบัติการและระดับบริหาร

วิธีการดำเนินการ	• จัดเตรียมข้อมูลจากหลาย ๆ แหล่งมารวมกันในคลังข้อมูล • ประมวลข้อมูลสำหรับทำการวิเคราะห์
เครื่องมือที่ใช้	• Data Storage Tools • Data Integration Tools • Business Intelligence Tools • Statistics Tools • Machine Learning and AI Tools
ผลที่ได้รับ	• รายงาน และ Dashboard • ผลการทำนาย

ผู้เกี่ยวข้อง	• วิศวกรข้อมูล (Data Engineer) • ผู้เชี่ยวชาญการบูรณาการข้อมูล (Data Integration Specialist) • นักวิเคราะห์ข้อมูล (Data Analyst) • ผู้เชี่ยวชาญระบบธุรกิจอัจฉริยะ (BI Specialist) • นักวิทยาศาสตร์ข้อมูล (Data Sciencetist)

๒.๔.๒.๘ เมทาดาตา (Metadata)

เมทาดาตา เป็นข้อมูลที่ใช้อธิบายข้อมูลหลักหรือข้อมูลอื่น โดยการจัดการเมทาดาตา (Metadata Management) ในการบริหารจัดการเมทาดาตาเริ่มตั้งแต่การเก็บรวมรวม จัดกลุ่ม ดูแล และควบคุมเมทาดาตา ทั้งนี้ข้อมูลแต่ละชุดควรมีเมทาดาตา เพื่อให้ผู้ใช้งานเข้าใจว่าข้อมูลชุดนี้คือข้อมูลที่เกี่ยวข้องกับอะไร สามารถนำไปใช้งานอย่างไร มีข้อจำกัดอะไร และมีฟิลด์ข้อมูล (Data Field\Element) อะไรบ้าง

วิธีการดำเนินการ	• ทำความเข้าใจเกี่ยวกับความต้องการเมทาดาตา • กำหนดมาตรฐานของเมทาดาตา
เครื่องมือที่ใช้	• Data Catalog Managment Tool • Metadata Repository Management Tool
ผลที่ได้รับ	• เมทาดาตาที่มีคุณภาพและความมั่นคงปลอดภัย
ผู้เกี่ยวข้อง	• ผู้เชี่ยวชาญด้านเมทาดาตา (Metadata Specialist) • บริกรข้อมูล (Data Steward)

๒.๔.๒.๙ ความมั่นคงปลอดภัยและการรักษาความเป็นส่วนบุคคลของข้อมูล (Data Security and Privacy)

ความมั่นคงปลอดภัยของข้อมูล (Data Security) หมายรวมถึง การป้องกันข้อมูลในบริบทของการรักษาความลับ ความถูกต้อง ความพร้อมใช้งานของข้อมูล การระบุตัวตน การห้ามปฏิเสธความรับผิด โดยมีรายละเอียดดังนี้

- การรักษาความลับ (Confidentiality) เช่น การส่งข้อความที่ปกปิดหรือเป็นความลับจะต้องมีวิธีการที่ทำให้มั่นใจได้ว่าบุคคลที่ประสงค์จะส่งถึงหรือที่ได้รับอนุญาตเท่านั้นที่สามารถอ่านข้อความได้
- ความถูกต้องของข้อมูล (Integrity) เช่น ข้อความที่ใช้จะต้องมั่นใจได้ว่าเป็นข้อความที่ถูกต้องแท้จริง ไม่ได้ถูกดัดแปลงแก้ไขระหว่างทาง
- ความพร้อมใช้งานของข้อมูล (Availability) เช่น หากประสงค์จะใช้ข้อความใด เวลาใดจะต้องมั่นใจได้ว่าสามารถใช้ข้อมูลได้เสมอและต่อเนื่อง
- การระบุตัวตน (Authentication) เช่น การได้รับข้อความ ผู้รับต้องมั่นใจว่าเป็นข้อความที่ส่งมาจากบุคคลที่อ้างว่าเป็นผู้ส่งนั้นจริง

- การห้ามปฏิเสธความรับผิด (Non-Repudiation) เช่น การได้รับข้อความเกี่ยวกับการดำเนินการอย่างใดอย่างหนึ่งหรือเป็นข้อผูกพันทางสัญญา ต้องมั่นใจได้ว่าผู้ส่งไม่สามารถปฏิเสธว่าไม่ได้ส่งข้อความนั้น ผู้รับจะสามารถใช้สิ่งใดอ้างอิงเพื่อไม่ให้ผู้ส่งปฏิเสธ

โดยความปลอดภัยของข้อมูลต้องดำเนินการตั้งแต่การวางแผน จัดทำ และบังคับใช้ นโยบายด้านรักษาความปลอดภัย เพื่อสนับสนุน การพิสูจน์ตัวตน การกำหนดสิทธิ์ การเข้าถึงข้อมูล และการตรวจสอบข้อมูลอย่างเหมาะสม

นอกจากนี้ ต้องมีการรักษาความเป็นส่วนบุคคลของข้อมูล (Data Privacy) ตั้งแต่การรวบรวม จัดเก็บ ใช้ เผยแพร่ หรือดำเนินการอื่นใดเกี่ยวกับข้อมูล โดยจะต้องมีการระบุวัตถุประสงค์เป็นหลักฐานให้ชัดเจน ห้ามมิให้มีการเปิดเผย หรือแสดง หรือทำให้ปรากฏในลักษณะอื่นใดที่ไม่สอดคล้องกับวัตถุประสงค์ เว้นแต่จะได้รับความยินยอมจากเจ้าของข้อมูลนั้น ๆ หรือมีกฎหมายกำหนดให้สามารถกระทำสิ่งนั้นได้

วิธีการดำเนินการ	• กำหนดนโยบายและมาตรฐานด้านรักษาความปลอดภัย • บริหารจัดการวิธีการจัดเก็บ การประมาลผล เข้าถึงข้อมูล การนำไปใช้ การเปิดเผย และการทำลาย
เครื่องมือที่ใช้	• ระบบการจัดการฐานข้อมูล (Database Management System - DBMS) • Identity Management Technology • Change Control System • หนังสือให้ความยินยอม (Letter of Consent)
ผลที่ได้รับ	• นโยบายด้านรักษาความปลอดภัยและการรักษาความเป็นส่วนบุคคลของข้อมูล (Data Security and Privacy Policies) • มาตรฐานการดูแลข้อมูลส่วนบุคคล (Data Security and Privacy Standard)
ผู้เกี่ยวข้อง	• คณะกรรมการด้านเทคโนโลยีสารสนเทศ • ผู้ดูแลระบบความปลอดภัยของข้อมูล (Data Security Administrator) • บริกรข้อมูล (Data Steward)

๒.๔.๒.๑๐ คุณภาพของข้อมูล (Data Quality)

เป็นการกำหนด สังเกตการณ์ การดูแลความถูกต้อง และปรับปรุงคุณภาพของข้อมูล ซึ่งคุณภาพของข้อมูลมีความจำเป็นต่อการใช้งาน เนื่องจากถ้าข้อมูลไม่มีคุณภาพจะส่งผลให้การดำเนินงานไม่มีประสิทธิภาพ โดยคุณภาพของข้อมูล ประกอบด้วย ข้อมูลมีความถูกต้อง (Accuracy) ข้อมูลมีความครบถ้วน (Completeness) ข้อมูลมีความต้องกัน (Consistency) ข้อมูลมีความเป็นปัจจุบัน (Timeliness) ข้อมูลมีความพร้อมใช้ (Availability) และข้อมูลตรงตามความต้องการของผู้ใช้ (Relevancy) ดังแสดงรายละเอียดเพิ่มเติมในบทที่ ๓.๔.๒ ระดับคุณภาพของข้อมูล (Data Quality Level)

วิธีการดำเนินการ	• พัฒนาและส่งเสริมการให้ความสำคัญกับคุณภาพของข้อมูล (Awareness)
เครื่องมือที่ใช้	• Data Cleansing Tools • Statistical Analysis Tools

ผลที่ได้รับ	• รายงานการรับรองคุณภาพของข้อมูล (Data Quality Certification Reports)
ผู้เกี่ยวข้อง	• นักวิเคราะห์คุณภาพของข้อมูล (Data Quality Analyst) • บริกรข้อมูล (Data Steward)

๒.๕ ความสัมพันธ์ระหว่างการบริหารจัดการข้อมูลกับการกำกับดูแลข้อมูล

จากผลการศึกษาที่เกี่ยวข้องการบริหารจัดการข้อมูลของสมาคมบริหารจัดการข้อมูลระหว่างประเทศ (Data Management Association International) จะเห็นว่า การกำกับดูแลข้อมูล (Data Governance) เป็นส่วนที่สำคัญในการบริหารจัดการข้อมูล (Data Management) เป็นกลไกในการกำหนดทิศทาง ควบคุม และทวนสอบการบริหารจัดการข้อมูล เพื่อให้มั่นใจได้ว่าหน่วยงานได้ดำเนินการบริหารจัดการข้อมูลเป็นไปตามนโยบาย กฎ ระเบียบ หรือข้อบังคับที่ได้กำหนดไว้

ดังนั้น สิ่งที่ควรริเริ่มเป็นอันดับแรกของการวางแผนในการบริหารจัดการข้อมูล ก็คือ การกำกับดูแลข้อมูล เพราะเป็นเรื่องของการกำหนดบทบาท หน้าที่ความรับผิดชอบ และการตัดสินใจ เพื่อสร้างความเชื่อมั่นว่าการกำกับดูแล ความรับผิดชอบ และความเป็นเจ้าของหรือผู้มีส่วนได้ส่วนเสียกับสินทรัพย์ข้อมูลนั้น เป็นไปอย่างมีระเบียบ ถูกต้อง และมีความยั่งยืน โดยการกำกับดูแลข้อมูลจะต้องเข้าไปมีส่วนร่วมในทุก ๆ องค์ประกอบหรือกิจกรรมของการบริหารจัดการข้อมูล

อย่างไรก็ตาม การบริหารจัดการข้อมูลนั้นมีความหมายที่กว้างกว่าและเกี่ยวข้องกับแง่มุมของการใช้ข้อมูลและดำเนินงานในกระบวนการที่เกิดขึ้นซ้ำ ๆ ในแต่ละช่วงของวงจรชีวิตของข้อมูล

ทั้งนี้ หากภาครัฐมีการกำกับดูแลข้อมูลที่ดีจะก่อให้เกิดการบริหารจัดการข้อมูลที่ดีเช่นกัน ซึ่งส่งผลให้ข้อมูลมีความมั่นคงปลอดภัย มีคุณภาพ สามารถเชื่อมโยงกันได้ มีคุณค่าทางเศรษฐกิจและสังคม และได้รับความคุ้มทุนต่อการดำเนินงาน

๒.๖ กรอบนโยบายข้อมูล (Data Policy Framework)

การกำหนดนโยบายข้อมูล (Data Policy) จัดเป็นพื้นฐานของการกำกับดูแลข้อมูลที่ดี ดังนั้น เพื่อให้การบริหารจัดการและการกำกับดูแลข้อมูลได้อย่างมีประสิทธิภาพ จึงต้องมีการกำหนดนโยบายที่ระบุอย่างชัดเจน สอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ คำสั่งหรือข้อกำหนดอื่น ๆ ที่เกี่ยวข้อง ผ่านการอนุมัติจากผู้บริหาร มีการเผยแพร่และสื่อสารให้กับเจ้าหน้าที่และผู้ที่เกี่ยวข้องทั้งภายในหน่วยงานและภายนอกหน่วยงาน รวมถึงควรมีการทบทวนนโยบายอย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่านโยบายข้อมูลได้ถูกนำมาปฏิบัติอย่างมีประสิทธิภาพและต่อเนื่อง โดยนโยบายข้อมูลควรมีการระบุอย่างน้อย ดังนี้

๒.๖.๑ หมวดทั่วไป (General Domain)

๑) กำหนดบทบาทและความรับผิดชอบที่ประกอบกันเป็นโครงสร้างการกำกับดูแลข้อมูล โดยต้องได้รับการมอบอำนาจและการอนุมัติจากผู้บริหาร
๒) กำหนดกลุ่มบุคคลหรือบุคคลภายในหน่วยงาน เพื่อเป็นเจ้าของข้อมูลในการบริหารจัดการข้อมูลของหน่วยงาน เพราะหน่วยงานถือเป็นเจ้าของข้อมูลทุกประเภทที่เกิดจากการดำเนินงานภายในหน่วยงานนั้น ๆ
๓) ตรวจสอบความสอดคล้องกันระหว่างนโยบายข้อมูลกับการดำเนินการใด ๆ ของผู้มีส่วนได้ส่วนเสีย อย่างน้อยปีละ ๑ ครั้ง

๔) ทบทวนนโยบายข้อมูล อย่างน้อยปีละ ๑ ครั้ง และให้ดำเนินการปรับปรุงอย่างต่อเนื่อง หากพบว่านโยบายข้อมูลยังไม่มีประสิทธิภาพเพียงพอ
๕) สื่อสารและเผยแพร่นโยบายข้อมูลให้กับผู้ที่เกี่ยวข้องทั้งภายในและภายนอกหน่วยงาน
๖) สนับสนุนให้มีการฝึกอบรมเพื่อสร้างความตระหนักถึงการมีการกำกับดูแลข้อมูล และการบริหารจัดการข้อมูล โดยให้ครอบคลุมทุกกระบวนการของการบริหารจัดการและวงจรชีวิตของข้อมูล

๒.๖.๒ หมวดการจัดเก็บข้อมูล (Data Storage Domain)

๑) กำหนดขอบเขตของข้อมูลที่จัดเก็บทั้งข้อมูลที่เป็นโครงสร้าง เช่น ฐานข้อมูล ข้อมูลแบบกึ่งโครงสร้าง เช่น เอ็กส์ เอ็ม แอล (XML) และข้อมูลไม่เป็นโครงสร้าง เช่น เอกสาร ภาพ เสียง หรือวีดีโอ
๒) กำหนดสภาพแวดล้อมของการจัดเก็บข้อมูลที่เอื้อต่อการรักษาความมั่นคงปลอดภัยและคุณภาพของข้อมูล
๓) กำหนดนโยบาย มาตรการการรักษาความปลอดภัยของข้อมูล เพื่อป้องกันการเข้าถึง การสูญหาย การทำลาย หรือการเปลี่ยนแปลงข้อมูลโดยไม่ได้รับการอนุญาต
๔) กำหนดชั้นความลับของข้อมูล และจัดเก็บให้สอดคล้องกับแนวทางหรือมาตรฐานการจัดชั้นความลับของข้อมูล (Data Classification Standard) ที่กำหนดไว้ เพื่อให้มั่นใจได้ว่าข้อมูลมีความมั่นคงปลอดภัย และรักษาคุณภาพของข้อมูล
๕) สร้างความรู้ความเข้าใจในการจัดเก็บข้อมูลแก่ผู้ที่เกี่ยวข้องทั้งภายในและภายนอกหน่วยงาน โดยมีการกำหนดสิทธิ์การเข้าถึงข้อมูล เครื่องมือที่ใช้ เป็นต้น
๖) จัดเก็บข้อมูลให้สอดคล้องกับความต้องการ และวัตถุประสงค์ในการดำเนินงาน โดยข้อมูลนั้นจะต้องมีความถูกต้อง สมบูรณ์ และเป็นปัจจุบันอยู่เสมอ
๗) กำหนดแนวทางในการทำลายข้อมูล เมื่อข้อมูลนั้นไม่มีการใช้งานหรือมีการเก็บข้อมูลไว้นานเกินกว่าระยะเวลาที่กำหนด และควรมีการเก็บรักษาเมทาดาตาของข้อมูลที่ทำลายไว้ เพื่อใช้สำหรับการตรวจสอบภายหลัง

๒.๖.๓ หมวดการประมวลผลข้อมูล (Data Processing Domain)

๑) จัดทำวิธีการ มาตรฐานของการประมวลผลข้อมูล และทำการสื่อสารให้แก่ผู้ที่เกี่ยวข้องรับทราบ
๒) ดำเนินการประมวลผลข้อมูลที่เป็นความลับ เช่น ข้อมูลส่วนบุคคล ให้เป็นไปตามขอบเขต เงื่อนไข หรือวัตถุประสงค์ในการยินยอมให้ดำเนินการกับข้อมูลส่วนบุคคลนั้น
๓) บันทึกการประมวลผลข้อมูล และบุคคลที่ทำการประมวลผลข้อมูล
๔) จัดทำเมทาดาตาสำหรับข้อมูลที่จัดเก็บอยู่ในคลังข้อมูล
๕) นำระบบเทคโนโลยีสารสนเทศหรือระบบอัตโนมัติมาใช้ในการจัดทำเมทาดาตา

๒.๖.๔ หมวดการแลกเปลี่ยนข้อมูล (Data Exchange Domain)

๑) กำหนดแนวปฏิบัติและสัญญาอนุญาตในการแลกเปลี่ยนข้อมูลเพื่อให้มั่นใจได้ว่าข้อมูลจะยังคงความมั่นคงปลอดภัยและรักษาคุณภาพของข้อมูล เช่น การจัดการเรื่องความมั่นคงปลอดภัยและคุณภาพข้อมูล ผู้ประสานงานหรือศูนย์ติดต่อ Contact Center)
๒) กำหนดกระบวนการในการแลกเปลี่ยนข้อมูลที่ชัดเจนตั้งแต่ เตรียมการ เริ่มดำเนินการ ระหว่างดำเนินการ และสิ้นสุดการดำเนินการ

๓) กำหนดรายการชุดข้อมูลมาตรฐาน เมทาดาตาของชุดข้อมูลมาตรฐาน และข้อข้อตกลงในการแลกเปลี่ยนข้อมูล
๔) กำหนดเทคโนโลยีและมาตรฐานทางเทคนิคที่ใช้ในการแลกเปลี่ยนข้อมูล
๕) ต้องมีการบันทึกการใช้งาน (Log File) เพื่อให้สามารถตรวจสอบย้อนกลับได้
๖) ตรวจสอบให้แน่ใจว่าการแลกเปลี่ยนข้อมูลถูกดำเนินการได้อย่างเหมาะสมหรือเป็นไป ตามแนวปฏิบัติ กระบวนการแลกเปลี่ยน และมาตรฐานที่กำหนด

๒.๖.๕ หมวดการใช้และการเปิดเผยข้อมูล (Data Use and Publish Domain)

๑) ห้ามเปิดเผยข้อมูลที่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง นโยบาย แนวปฏิบัติ ไม่ว่าข้อมูลจะอยู่ในรูปแบบใดหรือสถานที่ใดก็ตาม
๒) ต้องได้รับการอนุญาตจากตัวแทนหน่วยงานหรือเจ้าของข้อมูลก่อนการเปิดเผยข้อมูล
๓) ควรมีการระบุช่องทางการเปิดเผยข้อมูลที่เข้าถึงและนำไปใช้ได้ง่าย
๔) ควรมีการเปิดเผยเมทาดาตาควบคู่ไปกับข้อมูลที่เปิดเผย
๕) ต้องตรวจสอบให้แน่ใจว่าการเปิดเผยข้อมูลถูกดำเนินการได้อย่างเหมาะสมหรือเป็นไปตามแนวทางที่กำหนดเพื่อให้ได้ข้อมูลที่มีคุณภาพ และรักษาคุณภาพของข้อมูล

๒.๗ มาตรฐานข้อมูล (Data Standard)

การจัดทำมาตรฐานข้อมูลเป็นกลไกอย่างหนึ่งในการกำกับดูแลข้อมูล โดยนโยบายข้อมูลระบุสิ่งที่ควรทำหรือไม่ควรทำในการบริหารจัดการข้อมูล ขณะที่มาตรฐานข้อมูลอธิบายว่าสิ่งนั้นต้องทำอย่างไร การจัดทำมาตรฐานมีวัตถุประสงค์เพื่อสร้างความเข้าใจที่ตรงกันและลดความหลากหลายของวิธีการ ตัวอย่างมาตรฐานข้อมูล เช่น มาตรฐานชุดข้อมูล (Dataset Standard) มาตรฐานเมทาดาตา (Metadata Standard) และมาตรฐานชั้นความลับข้อมูล (Data Classification Standard)

มาตรฐานชุดข้อมูล (Dataset Standard) คือ การกำหนดรูปแบบและข้อกำหนดของข้อมูลที่มีการใช้ร่วมกันจากหลาย ๆ ส่วนงานหรือหน่วยงาน เพื่อลดความซ้ำซ้อนของข้อมูล ลดความยุ่งยากในการบริหารจัดการ และสนับสนุนให้ข้อมูลมีคุณภาพ ซึ่งส่วนงานหรือหน่วยงานต้องร่วมกันกำหนดเมทาดาตาขึ้นมาเพื่ออธิบายคุณลักษณะของชุดข้อมูลที่ใช้ร่วมกัน แล้วดำเนินการบูรณาการข้อมูล (Data Integration) ที่กระจายอยู่ตามส่วนงานหรือหน่วยงานต่าง ๆ เข้าด้วยกัน ให้สอดคล้องกับเมทาดาตาที่ได้กำหนดไว้

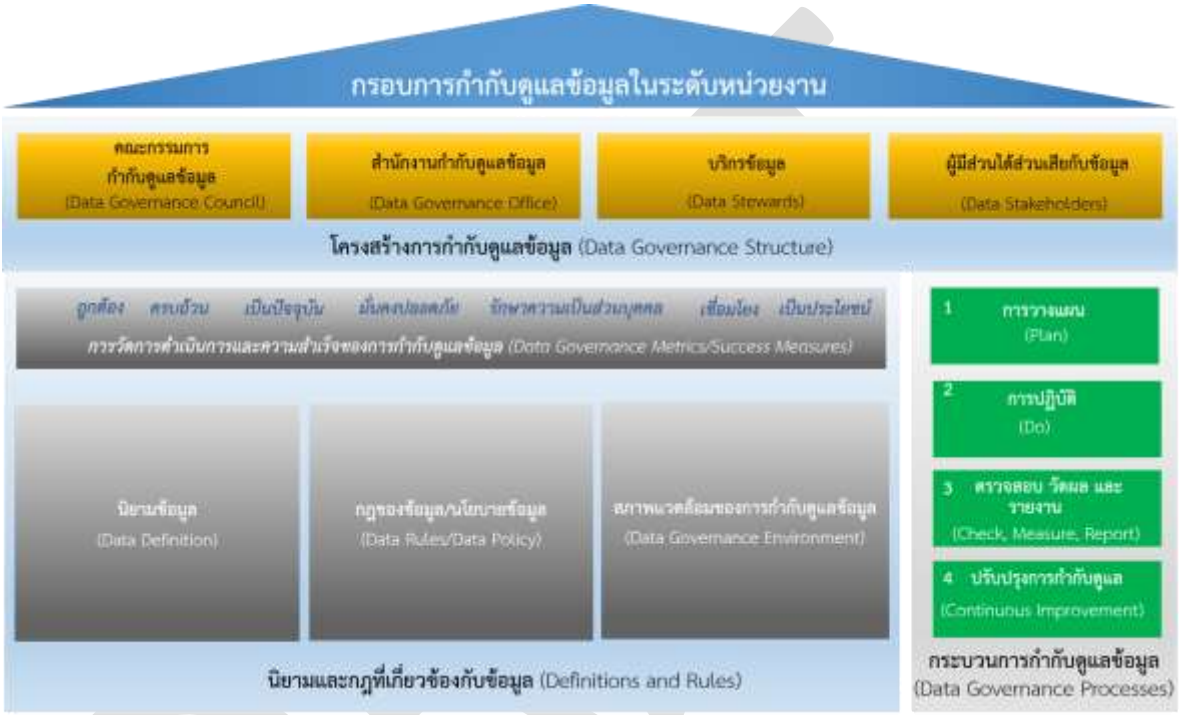
มาตรฐานเมทาดาตา (Metadata Standard) คือ การกำหนดรูปแบบและข้อกำหนดของเมทาดาตาเพื่อให้สามารถเข้าใจได้ถูกต้องตรงกัน ตัวอย่างการกำหนดมาตรฐาน เช่น เมทาดาตาต้องประกอบไปด้วย ๖ ส่วน ดังต่อไปนี้ ๑) ชื่อข้อมูล ๒) คำอธิบายข้อมูล ๓) คำสำคัญ ๔) วันที่ทำการเปลี่ยนแปลงข้อมูลล่าสุด ๕) ชื่อเจ้าของข้อมูล และ ๖) ฟิลด์ข้อมูล (Data Field/Element) โดยที่แต่ละฟิลด์ต้องประกอบไปด้วย ๔ ส่วน ดังต่อไปนี้ ๑) ชื่อฟิลด์ข้อมูล ๒) ประเภทข้อมูล เช่น ตัวเลข ตัวหนังสือ และวันที่ ๓) ช่วงค่าของข้อมูล เช่น จำนวนเงินต้องอยู่ในช่วง ๐ ถึง ๑ พันล้านบาท และ ๔) การยอมให้ฟิลด์ข้อมูลเป็นค่าว่างได้หรือไม่

มาตรฐานชั้นความลับข้อมูล (Data Classification Standard) คือ การกำหนดรูปแบบและข้อกำหนดของการจัดชั้นความลับของข้อมูล เพื่อป้องกันการเข้าถึงและสามารถนำข้อมูลไปใช้ได้อย่างเหมาะสม ชั้นความลับมักถูกกำหนดให้สอดคล้องกับผลกระทบต่อหน่วยงานและความมั่นคงของประเทศ ตัวอย่างประเภท

ของผลกระทบ ๑) ด้านชื่อเสียง เช่น ข้อมูลในเชิงลบของหน่วยงานถูกเปิดเผยส่งผลให้หน่วยงานหรือประเทศเสียชื่อเสียง ๒) ด้านความต่อเนื่องของการดำเนินการ เช่น ข้อมูลระบบเครือข่ายถูกเปิดเผยทำให้ระบบเครือข่ายหรือระบบอินเทอร์เน็ตถูกโจมตี ซึ่งส่งผลให้การดำเนินงานของหน่วยงานหยุดชะงักหรือล่าช้า ๓) ด้านการเงิน เช่น ข้อมูลบัตรเครดิตในหน่วยงานถูกเปิดเผย ทำให้สูญเสียงบประมาณของหน่วยงาน และ ๔) ด้านทรัพยากรบุคคล เช่น ข้อมูลเงินเดือนถูกเปิดเผย ส่งผลให้บุคคลากรคนสำคัญต้องลาออก ตัวอย่างชั้นความลับ เช่น ลับที่สุด ลับมาก ลับ ใช้ภายในหน่วยงาน และเปิดเผยได้

บทที่ ๓ กรอบการกำกับดูแลข้อมูล (DATA GOVERNANCE FRAMEWORK)

กรอบการกำกับดูแลข้อมูลประกอบด้วยองค์ประกอบต่าง ๆ ผนวกเข้าด้วยกัน ทั้งในด้านของนิยามและกฎที่เกี่ยวข้องกับข้อมูล บุคคล และกระบวนการ ซึ่งองค์ประกอบเหล่านี้มีความสำคัญที่ก่อให้เกิดประสิทธิภาพและประสิทธิผลในการดำเนินงาน อันจะนำไปสู่การบรรลุเป้าหมายในการดำเนินงานตามที่กำหนดไว้ โดยสรุปรายละเอียดดังรูปที่ ๖



รูปที่ ๖ กรอบการกำกับดูแลข้อมูลในระดับหน่วยงาน

จากรูปที่ ๖ แบบแสดงกรอบการกำกับดูแลข้อมูลในระดับหน่วยงาน ประกอบด้วย นิยามและกฎที่เกี่ยวข้องกับข้อมูล (Definitions and Rules) โครงสร้างการกำกับดูแลข้อมูล (Data Governance Structure) และกระบวนการกำกับดูแลข้อมูล (Data Governance Processes) โดยบุคคลต่าง ๆ ที่เกี่ยวข้องกับโครงสร้างการกำกับดูแลข้อมูล จะเป็นผู้กำหนดนิยามและกฎที่เกี่ยวข้องกับข้อมูลสำหรับใช้ในการสร้างการกำกับดูแลข้อมูล เพื่อให้สอดคล้องกับกระบวนการที่ได้กำหนดไว้ ดังรายละเอียดต่อไปนี้

๓.๑ สภาพแวดล้อมของการกำกับดูแลข้อมูล

๓.๑.๑ กฎหมาย ระเบียบ ข้อบังคับ และอื่น ๆ ที่เกี่ยวข้องกับการกำกับดูแลข้อมูล

ปัจจุบันกฎหมายที่เกี่ยวข้องกับข้อมูล ข่าวสาร หรือสิทธิส่วนบุคคลในประเทศไทย มี ๓ ประเด็นที่อาจส่งผลกระทบต่อหลักแนวคิดการกำกับดูแลข้อมูล ซึ่งหากหน่วยงานในประเทศไทยต้องการสร้างหรือปรับปรุงระบบภายในให้มีการกำกับดูแลข้อมูล จะต้องพิจารณาประเด็นหลัก ๆ ที่เกี่ยวข้องกับกฎหมาย ดังต่อไปนี้

๑) การเปิดเผยข้อมูล

- รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. ๒๕๖๐ ในมาตราที่ ๕๙ ได้ระบุว่า รัฐต้องเปิดเผยข้อมูลหรือข่าวสารสาธารณะในครอบครองของหน่วยงานของรัฐที่มิใช่ข้อมูลเกี่ยวกับความมั่นคงของรัฐหรือเป็นความลับของทางราชการ
- พระราชบัญญัติ (พ.ร.บ.) ข้อมูลข่าวสารของทางราชการ พ.ศ. ๒๕๔๐ โดยมี ๓ ประเด็นที่เกี่ยวกับการเปิดเผยข้อมูล ได้ถูกระบุไว้ใน พ.ร.บ. ฉบับนี้ ได้แก่
  - ข้อมูลภาครัฐ ต้อง “เปิดเผยเป็นหลัก ปกปิดเป็นข้อยกเว้น”
  - กำหนดหลักเกณฑ์และกลไกการเปิดเผยข้อมูล
  - กำหนดประเภทข้อมูลที่เปิดเผยได้และเปิดเผยไม่ได้

๒) การคุ้มครองข้อมูลส่วนบุคคล

- การกำหนดประเภทข้อมูลที่เปิดเผยได้และเปิดเผยไม่ได้ ที่ระบุไว้ใน พ.ร.บ. ข้อมูลข่าวสารของทางราชการ พ.ศ. ๒๕๔๐ เป็นสิ่งที่จำเป็นต้องมีการพิจารณาในกรณีที่เป็นข้อมูลส่วนบุคคล เนื่องจากข้อมูลที่เป็นข้อมูลส่วนบุคคลจำเป็นต้องได้รับการคุ้มครองอย่างมีหลักเกณฑ์
- ประกาศ คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ (คธอ.) เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ ได้ระบุเรื่องการคุ้มครองข้อมูลส่วนบุคคลไว้ว่า “กำหนดให้ภาครัฐที่ให้บริการทางอิเล็กทรอนิกส์ต้องมีนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล”

๓) การรักษาความลับ

- ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๕๔ ได้มีข้อกำหนดที่เกี่ยวข้องกับการกำกับดูแลข้อมูล ได้แก่ กำหนดนิยามข้อมูลข่าวสารลับ และกำหนดหลักเกณฑ์และวิธีการในการรักษาความลับของหน่วยงานภาครัฐ
- แนวทางปฏิบัติในการรักษาความปลอดภัยเกี่ยวกับบุคคล เอกสาร และสถานที่ ที่จัดทำขึ้นจากระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. ๒๕๕๒ ควรนำมาพิจารณาในการกำกับดูแลข้อมูล

นอกจากการพิจารณากฎหมาย ระเบียบ และข้อบังคับที่มีอยู่ในปัจจุบัน หน่วยงานต้องพิจารณากฎหมาย ระเบียบ นโยบาย หรือ พ.ร.บ. ที่กำลังจะเกิดขึ้นในอนาคตควบคู่ไปกับการกำกับดูแลข้อมูลด้วย กฎหมายซึ่งกำลังอยู่ระหว่างการยกร่างที่เกี่ยวข้อง และอาจส่งผลกระทบต่อการกำกับดูแลข้อมูล ดังต่อไปนี้

๑) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม มีการยกร่าง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ... โดยมีการกำหนดหลักเกณฑ์ กลไก และมาตรการที่กำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลที่เป็นหลักการทั่วไป

๒) มีการยกร่าง พ.ร.บ. ข้อมูลข่าวสารสาธารณะ พ.ศ. ... ขึ้นมาใหม่ โดยจะทำการยกเลิก พ.ร.บ. ข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐ ซึ่งสาระสำคัญที่เกี่ยวข้องกับการกำกับดูแลข้อมูล คือ มีการกำหนดให้หน่วยงานของรัฐต้องจัดทำช่องทางในการเปิดเผยหรือเข้าถึงข้อมูลข่าวสารสาธารณะ

๓) มีการพิจารณาร่าง พ.ร.บ. Fin Tech โดยมีสาระสำคัญ ดังนี้

- ภาคธุรกิจเข้าถึงข้อมูลที่สามารถนำมาวิเคราะห์ วิจัย และพัฒนาผลิตภัณฑ์หรือบริการได้
- อำนวยความสะดวกในการทำธุรกรรมเกี่ยวกับการเงินการลงทุน การเข้าถึงข้อมูล และการพัฒนาเทคโนโลยีทางการเงิน

๔) คณะอนุกรรมการด้านการรักษาความลับของทางราชการทางอิเล็กทรอนิกส์ มีการพิจารณา ร่างระเบียบว่าด้วยการรักษาความลับของทางราชการด้วยวิธีการทางอิเล็กทรอนิกส์ พ.ศ. ... โดยออกภายใต้ พ.ร.บ. ข้อมูลข่าวสารราชการ พ.ศ. ๒๕๔๐ โดยเสนอให้มีการเพิ่มกำหนดหลักเกณฑ์และวิธีการในการรักษาความลับด้วยวิธีการทางอิเล็กทรอนิกส์ มีการร่าง พ.ร.บ. ข้อมูลความมั่นคงของรัฐและความลับของทางราชการ พ.ศ. ... เพื่อกำหนดคำนิยามและความหมายของคำว่า “ความมั่นคงของรัฐ” และ “ความลับของทางราชการ” พร้อมกับกำหนดหลักเกณฑ์และเงื่อนไขในการเปิดเผยหรือไม่เปิดเผยข้อมูล

๓.๑.๒ หลักการของวัฒนธรรมและสภาพแวดล้อมของหน่วยงานที่เอื้อต่อการมีการกำกับดูแล

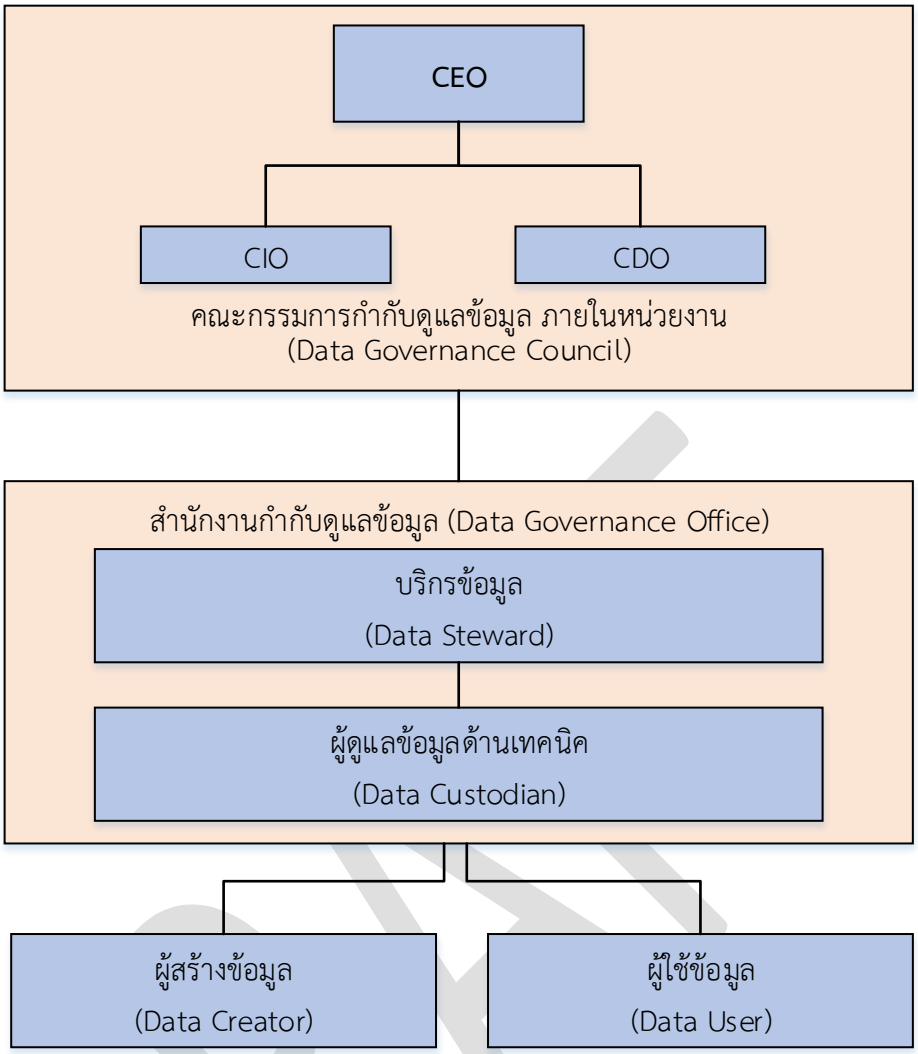
การจะทำให้เกิดการกำกับดูแลของข้อมูล จะต้องมีองค์ประกอบหลายอย่างที่สนับสนุนให้เกิดการกำกับดูแลข้อมูลที่ดี ในขณะเดียวกันจะต้องคำนึงถึงข้อจำกัดที่อาจส่งผลในเชิงลบต่อการปรับเปลี่ยนหรือปฏิรูปให้เกิดการกำกับดูแลข้อมูลในหน่วยงานด้วย วัฒนธรรมองค์กรและสภาพแวดล้อมเป็นหนึ่งในข้อจำกัดที่อาจส่งผลต่อการเปลี่ยนแปลงในการกำกับดูแลข้อมูลหน่วยงานได้ เนื่องจากแต่ละหน่วยงานล้วนมีวัฒนธรรมองค์กรและสภาพแวดล้อมที่แตกต่างกัน

ดังนั้น ความตระหนักถึงวัฒนธรรมองค์กรและสภาพแวดล้อมที่แตกต่างกันมีความจำเป็นต่อการกำหนดโครงสร้าง นโยบาย บทบาทหน้าที่ การดำเนินงานที่เอื้อต่อการกำกับดูแลข้อมูล ตั้งแต่เริ่มต้น นอกจากนี้ยังต้องมีมาตรการรองรับกรณีที่มีการปรับเปลี่ยนโครงสร้างองค์กร เนื่องจากการกำกับดูแลข้อมูลก็จะเปลี่ยนตามไปด้วย

๓.๒ โครงสร้างของการกำกับดูแลข้อมูล (Data Governance Structure)

๓.๒.๑ โครงสร้างของบุคลากรที่รับผิดชอบในการจัดการกำกับดูแลข้อมูล (Data Governance Structure)

การกำหนดโครงสร้างการกำกับดูแลข้อมูลเพื่อแสดงความสัมพันธ์ลำดับขั้นระหว่างกลุ่มบุคคลที่เกี่ยวข้องกับการกำกับดูแลข้อมูล และแสดงถึงสิทธิ์ในการสั่งการตามลำดับขั้น โครงสร้างไม่ควรมีลำดับขั้นมากเกินไป เพราะจะทำให้การดำเนินงานช้า ขณะเดียวกันไม่ควรน้อยจนเกินไปเพราะจะทำให้ขาดอำนาจในการตัดสินใจ



รูปที่ ๗ ตัวอย่างโครงสร้างการกำกับดูแลข้อมูล

จากรูปที่ ๗ ผู้บริหารระดับสูง (Chief Executive Officer) ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer) หรือผู้อำนวยการหน่วยงาน (Chief Executive Officer) ทำหน้าที่ตัดสินใจเชิงนโยบายและบริหารจัดการภายในคณะกรรมการกำกับดูแลข้อมูล เช่น การกำหนดนโยบายข้อมูล กำหนดแนวทางปฏิบัติงาน

สำนักงานกำกับดูแลข้อมูล (Data Governance Office) ประกอบด้วย บริกรข้อมูล (Data Steward) และผู้ดูแลข้อมูลด้านเทคนิค (Data Custodian) ซึ่งรับคำสั่งโดยตรงจากคณะกรรมการกำกับดูแลข้อมูล และให้ข้อมูลสนับสนุนในการตัดสินใจต่อคณะกรรมการกำกับดูแลข้อมูล โดยบริกรข้อมูลเป็นผู้ให้การสนับสนุนด้านธุรกิจ ขณะที่ผู้ดูแลข้อมูลด้านเทคนิคเป็นผู้ให้การสนับสนุนด้านเทคโนโลยีสารสนเทศ ตามปกติผู้ดูแลข้อมูลด้านเทคนิคจะทำหน้าที่ตามคำสั่งของบริกรข้อมูล ส่วนเจ้าของข้อมูล (Data Owner) ไม่ได้รวมอยู่ในส่วนงานกำกับดูแลข้อมูล อย่างไรก็ตามเจ้าของข้อมูลจะทำงานร่วมกับหรือคล้ายกับบริกรข้อมูล เช่น บริกรข้อมูลจะทำหน้าที่ในการอนุญาตการเข้าถึงข้อมูลแทนเจ้าของข้อมูล แต่ในกรณีที่ข้อมูลจัดอยู่ในชั้นความลับอาจจำเป็นต้องได้รับอนุญาตจากเจ้าของข้อมูลก่อน บริกรข้อมูลทำหน้าที่ทวนสอบการดำเนินงานกับข้อมูลตามรอบการตรวจสอบ ในขณะที่เจ้าของข้อมูลทำหน้าที่ตรวจสอบการดำเนินงานโดยตรง เป็นต้น หน่วยงานสามารถจัดตั้ง

ส่วนงานกำกับดูแลข้อมูลในรูปแบบเสมือน (Virtual Team) หรือส่วนงานแยกออกมาจากส่วนงานอื่นอย่างชัดเจนได้

ผู้สร้างข้อมูล (Data Creator) และผู้ใช้ข้อมูล (Data User) ทำหน้าที่ระบุความต้องการในการใช้ข้อมูล ความมั่นคงปลอดภัย และระดับคุณภาพข้อมูลที่ต้องการ

๓.๒.๒ บทบาทและความรับผิดชอบ (Role and Responsibility)

บทบาท (Role) และความรับผิดชอบ (Responsibility) ที่เหมาะสมจะนำไปสู่การดำเนินงานที่มีประสิทธิภาพและประสิทธิผลต่อหน่วยงาน ซึ่งการกำหนดบทบาทและความรับผิดชอบจะต้องไม่ขัดแย้งต่อกฎระเบียบ ข้อบังคับ หรือกฎหมาย มีรายละเอียด ดังนี้

ผู้มีส่วนได้ส่วนเสียกับข้อมูล (Data Stakeholder) มีความหมายรวมถึงบุคคลหรือกลุ่มบุคคลทั้งหมดที่เกี่ยวข้องกับข้อมูล ไม่ว่าจะเป็นฝ่ายธุรกิจและฝ่ายไอที เช่น ผู้บริหารข้อมูลระดับสูง (Chief Data Officer) คณะกรรมการกำกับดูแลข้อมูล (Data Governance Council) สำนักงานกำกับดูแลข้อมูล (Data Governance Office) บริกรข้อมูล (Data Steward) ผู้ดูแลข้อมูลด้านเทคนิค (Data Custodian) ผู้สร้างข้อมูล (Data Creator) และผู้ใช้ข้อมูล (Data User) เป็นต้น

ผู้บริหารข้อมูลระดับสูง (Chief Data Officer) คือ บุคคลที่ทำหน้าที่กำหนดวิสัยทัศน์ ให้คำแนะนำและทำการตัดสินใจ เกี่ยวกับการกำกับดูแลและการบริหารจัดการข้อมูล เช่น การอนุมัตินโยบายข้อมูล กฎระเบียบ ข้อบังคับอื่น ๆ ที่เกี่ยวข้อง ผู้บริหารข้อมูลระดับสูงจะทำหน้าที่เป็นประธานของคณะกรรมการกำกับดูแลข้อมูล

คณะกรรมการกำกับดูแลข้อมูล (Data Governance Council) คือ กลุ่มบุคคลที่มาจากผู้บริหารระดับสูงของหน่วยงานทั้งฝ่ายธุรกิจและฝ่ายไอที เช่น ผู้บริหารข้อมูลระดับสูง ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ผู้อำนวยการหน่วยงาน และหัวหน้าส่วนงาน เป็นต้น ทำหน้าที่ในการกำหนดความต้องการ ให้ข้อเสนอแนะ และอนุมัติ นโยบายข้อมูล เกณฑ์การวัดคุณภาพ ระเบียบ และข้อบังคับอื่น ๆ ที่เกี่ยวข้องกับข้อมูล รวมไปถึงการจัดลำดับความสำคัญของข้อมูลในการกำกับดูแล

สำนักงานกำกับดูแลข้อมูล (Data Governance Office) คือ กลุ่มบุคคลที่ทำหน้าที่ในการให้การสนับสนุนทั้งทางด้านธุรกิจและไอทีต่อคณะกรรมการกำกับดูแลข้อมูล และบริการด้านต่าง ๆ ที่เกี่ยวข้องกับข้อมูล กลุ่มบุคคลนี้อาจจะประกอบไปด้วย บริกรข้อมูล (Data Steward) และผู้ดูแลข้อมูลด้านเทคนิค (Data Custodian)

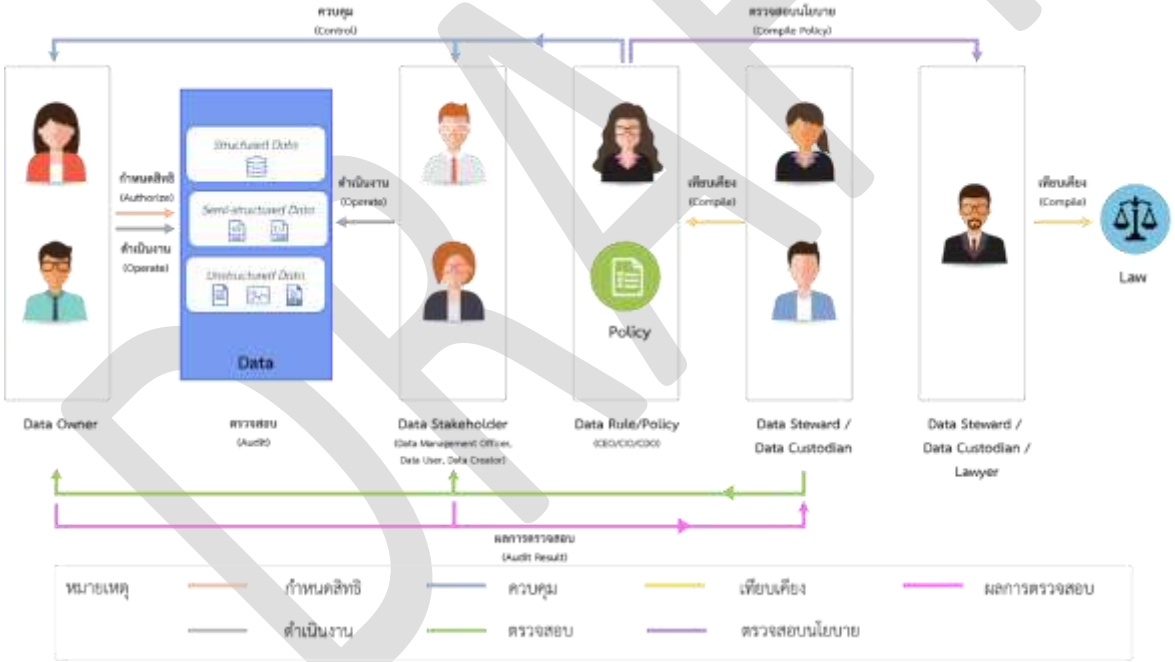
บริกรข้อมูล (Data Steward) คือ บุคคลที่ทำหน้าที่รับผิดชอบในการนิยามเมทาดาตา นิยามความต้องการด้านคุณภาพและความมั่นคงปลอดภัยซึ่งอาจจะได้รับมาจากผู้ใช้ข้อมูลหรือผู้มีส่วนได้ส่วนเสียอื่น ๆ ร่างนโยบายข้อมูลด้วยการช่วยเหลือจากผู้เชี่ยวชาญด้านการบริหารจัดการข้อมูล (Data Management Professional) ตรวจสอบความสอดคล้องกันระหว่างนโยบายกับการดำเนินการต่อข้อมูล ตรวจสอบคุณภาพข้อมูลหรือทำงานร่วมกับทีมคุณภาพข้อมูล (Data Quality Team) วิเคราะห์ผลจากการตรวจสอบ แล้วรายงานผลลัพธ์ไปยังคณะกรรมการกำกับดูแลข้อมูลและผู้ที่เกี่ยวข้องอื่น ๆ ให้ทราบ ลดความขัดแย้งระหว่างการประชุม บริกรข้อมูลมักจะเป็นบุคคลที่มาจากฝ่ายธุรกิจแต่มีความเข้าใจด้านไอที

ผู้ดูแลข้อมูลด้านเทคนิค (Data Custodian) คือ บุคคลที่ทำหน้าที่ให้การสนับสนุนด้านเทคโนโลยีสารสนเทศแก่บริกรข้อมูลเพื่อให้มั่นใจได้ว่าการดำเนินงานใด ๆ ของผู้ที่เกี่ยวข้องกับข้อมูลเป็นไปตามนโยบายข้อมูล คุณภาพข้อมูล ความมั่นคงปลอดภัยของข้อมูล และวัตถุประสงค์หรือเป้าหมายของข้อมูล ผู้ดูแลข้อมูลด้านเทคนิคมักจะเป็นบุคคลฝ่ายไอทีแต่ที่มีความเข้าใจเกี่ยวกับธุรกิจ

เจ้าของข้อมูล (Data Owner) คือ บุคคลที่ทำหน้าที่ตรวจสอบดูแลข้อมูลโดยตรง สร้างความมั่นใจได้ว่าการบริหารจัดการข้อมูลสอดคล้องกับนโยบาย มาตรฐาน กฎ ระเบียบ หรือกฎหมาย ทำการทบทวนและอนุมัติการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับข้อมูล เช่น การเปลี่ยนแปลงเมทาดาตาและเกณฑ์การทำความสะอาดข้อมูล (Data Cleansing) เป็นต้น ให้สิทธิในการเข้าถึงข้อมูล และจัดชั้นความลับของข้อมูล

ผู้สร้างข้อมูล (Data Creator) คือ บุคคลที่ทำหน้าที่ สร้าง แก้ไข ปรับปรุง หรือลบข้อมูลให้สอดคล้องต่อความต้องการของผู้ใช้ข้อมูล นอกจากนี้ยังมีหน้าที่ในการทำงานร่วมกับบริกรข้อมูล เพื่อตรวจสอบและแก้ไขปัญหาด้านคุณภาพข้อมูล

ผู้ใช้ข้อมูล (Data User) คือ บุคคลที่ทำหน้าที่ในการระบุความต้องการในการใช้ข้อมูลและรายงานประเด็นปัญหาที่พบระหว่างการใช้ข้อมูล ทั้งด้านคุณภาพ และความปลอดภัยของข้อมูลไปยังบริกรข้อมูล



รูปที่ ๘ ขั้นตอนการปฏิบัติงานของผู้ที่เกี่ยวข้อง

จากรูปที่ ๘ แสดงให้เห็นว่าเจ้าของข้อมูล (Data Owner) เป็นผู้กำหนดสิทธิการเข้าถึง และดำเนินงานใด ๆ กับข้อมูลที่ตนเป็นเจ้าของ ทั้งข้อมูลที่เป็นโครงสร้าง เช่น ฐานข้อมูล กึ่งโครงสร้าง เช่น เอ็กส์ เอ็ม แอล (XML) และไม่มีโครงสร้าง เช่น เสียง ภาพ และภาพเคลื่อนไหว ทั้งนี้อาจจะกำหนดให้บริกรข้อมูล (Data Steward) ทำหน้าที่ในการกำหนดสิทธิการเข้าใช้งานแทนเจ้าของข้อมูลได้ในบางกรณี โดยผู้มีส่วนได้ส่วนเสียกับข้อมูล (Data Stakeholder) มีหน้าที่ต้องดำเนินงานกับข้อมูลตามที่เจ้าของข้อมูล (Data Owner) กำหนดไว้ เช่น การเพิ่ม ลบ แก้ไข ประมวลผล นำไปใช้ แลกเปลี่ยน และเปิดเผยข้อมูล

ในการดำเนินงานดังกล่าวข้างต้นต้องสอดคล้องกับกฎเกณฑ์ของข้อมูล (Data Rule) หรือนโยบายข้อมูล (Data Policy) ที่หน่วยงานเป็นผู้กำหนด โดยมีบริกรข้อมูล (Data Steward) หรือผู้ดูแลข้อมูลด้านเทคนิค (Data Custodian) เป็นผู้ตรวจสอบการดำเนินงานของเจ้าของข้อมูล (Data Owner) และผู้มีส่วนได้ส่วนเสียกับข้อมูล (Data Stakeholder) ให้ยังคงการดำเนินงานที่สอดคล้องกับกฎเกณฑ์ของข้อมูล (Data Rule) หรือนโยบายข้อมูล (Data Policy) อยู่เสมอ ในขณะที่ผู้กำหนดกฎเกณฑ์ของข้อมูล (Data Rule) หรือนโยบายข้อมูล (Data Policy) เช่น ผู้บริหารระดับสูงของหน่วยงาน ต้องพิจารณาทบทวนกฎเกณฑ์ของข้อมูล (Data Rule) หรือนโยบายข้อมูล (Data Policy) ให้สอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับหรือข้อกำหนดอื่น ๆ ที่เกี่ยวข้องอยู่เสมอ โดยบริกรข้อมูล (Data Steward) ผู้ดูแลข้อมูลด้านเทคนิค (Data Custodian) หรือนักกฎหมาย (Lawyer) เป็นผู้สนับสนุนการดำเนินงานเพื่อให้กฎเกณฑ์ของข้อมูล (Data Rule) หรือนโยบายข้อมูล (Data Policy) เป็นปัจจุบันและมีประสิทธิภาพต่อไป

๓.๓ กระบวนการกำกับดูแลข้อมูล

หลักพื้นฐานของการกำหนดกระบวนการและผลที่ได้รับ ประกอบด้วย การเลือกข้อมูลเพื่อดำเนินการกำกับดูแล การระบุเป้าหมาย การกำหนดมาตรฐานและแนวปฏิบัติ รวมถึงการบริหารจัดการคน

๑. การเลือกข้อมูลเพื่อดำเนินการกำกับดูแล เช่น ข้อมูลส่วนบุคคล ข้อมูลความมั่นคง ข้อมูลความลับทางราชการ และข้อมูลสาธารณะ โดยกระบวนการซึ่งได้มาด้วยข้อมูลนั้นสามารถใช้วิธีการ เช่น กระบวนการย้อนกลับทางวิศวกรรม (Reverse Engineer) การวิเคราะห์ข้อมูล (Data Analysis) และการสำรวจข้อมูล (Survey)
๒. การระบุเป้าหมาย ต้องพิจารณาครอบคลุมในประเด็นดังต่อไปนี้เป็นอย่างน้อย คือ คุณภาพข้อมูล การเข้าถึงและการจัดการ ความปลอดภัยและความเป็นส่วนตัว การปฏิบัติตามระเบียบและกฎหมาย ต้นทุนและประสิทธิภาพ
๓. การกำหนดมาตรฐานและแนวปฏิบัติ เป็นการกำหนดมาตรฐานโดยทั่วไป แนวทางที่ใช้ ได้แก่ การตั้งชื่อ คุณภาพของข้อมูล การโอนย้ายข้อมูล กระบวนที่เกี่ยวข้องกับข้อมูล (Create Read Update Delete – CRUD) และการเก็บในหน่วยเก็บถาวร (Archive) เป็นต้น
๔. การบริหารจัดการคน เช่น การสร้างวัฒนธรรมองค์กร การบริหารจัดการแรงต้าน การสื่อสารที่ชัดเจน การสร้างความพึงพอใจกับผู้ที่มีส่วนได้ส่วนเสีย และการใช้ประโยชน์จากเทคโนโลยี ซึ่งจะช่วยให้การดำเนินงานสำเร็จลุล่วงได้ดี

๓.๓.๑ กระบวนการกำกับดูแลข้อมูล (Data Governance Process)

กระบวนการกำกับดูแลข้อมูล (Data Governance Process) เป็นขั้นตอนที่ใช้สำหรับกำกับดูแลการการดำเนินการใด ๆ ต่อข้อมูลให้เป็นไปตาม กฎ ระเบียบ ข้อบังคับ หรือนโยบายที่เกี่ยวข้องกับข้อมูล กระบวนการกำกับดูแลข้อมูลเริ่มตั้งแต่การวางแผนไปจนถึงการปรับปรุงอย่างต่อเนื่องดังรายละเอียดต่อไปนี้

๑) การวางแผน (Plan)

การวางแผนจะเริ่มตั้งแต่กำหนดประเด็นปัญหาซึ่งเป็นส่วนที่สำคัญเนื่องจากเป็นจุดเริ่มต้นที่จะกำหนดกฎระเบียบหรือแนวทางปฏิบัติต่างๆ เพื่อใช้ในการกำกับดูแลต่อไป เมื่อมีการกำหนดกฎระเบียบไว้

แล้วอาจมีการปรับปรุงเปลี่ยนแปลงให้เข้ากับสภาพแวดล้อมที่เปลี่ยนไป หลังจากที่ได้มีการกำหนดประเด็นปัญหาที่ชัดเจนแล้วกระบวนการถัดไปคือการเตรียมแผนงานและการวางแผนตามแผนงาน เพื่อที่จะได้กำหนดการดำเนินงานให้เป็นไปตามระยะเวลาและกรอบที่กำหนด ดังนั้น ในขั้นตอนนี้เพื่อให้สามารถดำเนินงานได้ตามเป้าหมายที่วางไว้ หลังจากนั้นนำแผนและนโยบายข้อมูลไปประกาศใช้อย่างเป็นทางการ

๒) การปฏิบัติ (Do)

บุคคลที่เกี่ยวข้องกับข้อมูลดำเนินการที่เกี่ยวข้องกับข้อมูล เช่น วิศวกรข้อมูล นักวิเคราะห์ข้อมูล นักวิทยาศาสตร์ข้อมูล และผู้ใช้ข้อมูล จะต้องดำเนินการให้สอดคล้องกับนโยบายข้อมูลที่ได้กำหนดไว้

๓) การตรวจสอบ, วัดผล และรายงาน (Check, Measure, Report)

บุคคลที่ทำหน้าที่กำกับดูแลข้อมูลจะดำเนินการกำกับดูแลสอดคล้องกับแผนงานที่กำหนดไว้ เพื่อให้บุคคลที่เกี่ยวข้องกับข้อมูลดำเนินการเป็นไปตามนโยบายที่กำหนด พร้อมทั้งทำการวัดผลด้านคุณภาพข้อมูลและรายงานผลไปยังผู้ที่เกี่ยวข้องเพื่อให้ทราบถึงผลการดำเนินงานและประเด็นปัญหาที่พบ

๔) การปรับปรุงอย่างต่อเนื่อง (Continuous Improvement)

รายการความต้องการที่จะปรับปรุงกระบวนการกำกับดูแลข้อมูลให้ดีขึ้นจากผู้บริหารและผู้มีส่วนได้ส่วนเสีย รวมไปถึงผลที่ได้รับจากการรายงานผลการตรวจสอบ (เช่น รายงานผลการตรวจสอบความสอดคล้องของการดำเนินงานต่อนโยบายข้อมูล รายงานคุณภาพข้อมูล และรายงานความมั่นคงปลอดภัย) จะถูกใช้สำหรับการปรับปรุงกระบวนการให้มีประสิทธิภาพดียิ่งขึ้น

๓.๓.๒ แนวทางการจัดการกระบวนการและผลที่ได้รับจากการดำเนินการ (Deliverables)

ตารางที่ ๑ ความสัมพันธ์ระหว่างกระบวนการ ส่วนนำเข้า ส่วนนำออก และผู้มีส่วนได้ส่วนเสีย

กระบวนการ (Processes)	ส่วนนำเข้า (Input)	ส่วนนำออก (Output)	ผู้มีส่วนได้ส่วนเสีย (Data Stakeholder)
๑ การวางแผน	(๑) นโยบาย กฎ ระเบียบ ข้อบังคับ และกฎหมายที่เกี่ยวข้องกับข้อมูล (๒) รายการชุดข้อมูล (๓) รายการประเด็นปัญหาจากรายงานผลการตรวจสอบความสอดคล้องของการดำเนินงานต่อนโยบายข้อมูล รายงานคุณภาพข้อมูล รายงานความมั่นคงปลอดภัยต่อข้อมูล หรือรายงานความเสี่ยงต่อข้อมูล	(๑) แผนดำเนินการ (ขอบเขต เวลา ทีมกำกับดูแลข้อมูล และต้นทุน)	(๑) ผู้บริหารข้อมูลระดับสูงหรือผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (๒) คณะกรรมการกำกับดูแลข้อมูล (๓) บริกรข้อมูล
๒ การปฏิบัติ	(๑) นโยบาย กฎ ระเบียบ ข้อบังคับ และกฎหมายที่เกี่ยวข้องกับข้อมูล (๒) แผนดำเนินการ (ขอบเขต เวลา ทีมกำกับดูแลข้อมูล และต้นทุน)	(๑) รายงานความก้าวหน้าในการปฏิบัติงาน (๒) ผลการปฏิบัติงาน	(๑) ผู้บริหารงาน (๒) ผู้ปฏิบัติงานที่เกี่ยวข้อง (๓) บริกรข้อมูล (๔) ผู้ดูแลข้อมูลด้านเทคนิค
๓ ตรวจสอบ วัดผล และรายงาน	(๑) นโยบาย กฎ ระเบียบ ข้อบังคับ และกฎหมายที่เกี่ยวข้องกับข้อมูล (๒) เกณฑ์การวัดระดับความพร้อมของการกำกับดูแลข้อมูล ระดับคุณภาพข้อมูล และระดับความมั่นคงปลอดภัยข้อมูลคุณภาพข้อมูล และระดับความมั่นคงปลอดภัยข้อมูล	(๑) รายงานผลการตรวจสอบความสอดคล้องของการดำเนินงานต่อนโยบายข้อมูล รายงานคุณภาพข้อมูล รายงานความมั่นคงปลอดภัยต่อข้อมูล หรือรายงานความเสี่ยงต่อข้อมูล	(๑) บริกรข้อมูล (๒) ผู้ดูแลข้อมูลด้านเทคนิค

ตารางที่ ๒ ความสัมพันธ์ระหว่างกระบวนการ ส่วนนำเข้า ส่วนนำออก และผู้มีส่วนได้ส่วนเสีย (ต่อ)

กระบวนการ (Process)	ส่วนนำเข้า (Input)	ส่วนนำออก (Output)	ผู้มีส่วนได้ส่วนเสีย (Data Stakeholder)
๔ ปรับปรุงการกำกับดูแล	(๑) นโยบาย กฎ ระเบียบ ข้อบังคับ และกฎหมายที่เกี่ยวข้องกับข้อมูล (๒) โครงสร้างการกำกับดูแลข้อมูล (๓) เกณฑ์การวัดระดับความพร้อมของการกำกับดูแลข้อมูล ระดับคุณภาพข้อมูล และระดับความมั่นคงปลอดภัยข้อมูล (๔) รายงานผลการตรวจสอบความสอดคล้องของการดำเนินงานต่อนโยบายข้อมูล รายงานคุณภาพข้อมูล และรายงานความมั่นคงปลอดภัย (๕) รายการความต้องการจากผู้บริหารและผู้มีส่วนได้ส่วนเสีย	(๑) นโยบาย กฎ ระเบียบ ข้อบังคับ และกฎหมาย ที่เกี่ยวข้องกับข้อมูล (๒) โครงสร้างการกำกับดูแลข้อมูล (๓) เกณฑ์การวัดระดับความพร้อมของการกำกับดูแลข้อมูล ระดับคุณภาพข้อมูล และระดับความมั่นคงปลอดภัยข้อมูล	(๑) ผู้บริหารข้อมูลระดับสูงหรือผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (๒) คณะกรรมการกำกับดูแลข้อมูล (๓) บริกรข้อมูล

๓.๔ การวัดการดำเนินการและความสำเร็จของการกำกับดูแลข้อมูล

การวัดการดำเนินการหรือการวัดระดับความพร้อมของการกำกับดูแล จะแสดงให้เห็นถึงสถานะปัจจุบันว่าหน่วยงานได้มีการดำเนินการกำกับดูแลข้อมูลมากน้อยขนาดไหน ซึ่งผลของการดำเนินงานกำกับดูแลจะส่งผลในระดับคุณภาพของข้อมูล ระดับความพร้อมที่สูงควรจะสะท้อนถึงคุณภาพข้อมูลที่สูง อย่างไรก็ตาม ระดับความพร้อมกับคุณภาพข้อมูลอาจจะไม่สอดคล้องกัน ซึ่งอาจจะมาจากสาเหตุอื่นหรือเกณฑ์การวัดระดับความพร้อมยังไม่มีประสิทธิภาพเพียงพอ ดังนั้น หน่วยงานควรจะค้นหาสาเหตุที่แน่ชัดพร้อมทั้งดำเนินการแก้ไขเกณฑ์การวัดระดับความพร้อมเพื่อให้สอดคล้องกับลักษณะเฉพาะของหน่วยงาน แนวทางการวัดระดับความพร้อมของการกำกับดูแลและระดับคุณภาพของข้อมูล มีรายละเอียดดังต่อไปนี้

๓.๔.๑ ระดับความพร้อมของการกำกับดูแลข้อมูล

การกำกับดูแลข้อมูลนอกจากจำเป็นต้องมีการดำเนินการที่เกิดประสิทธิภาพแล้ว การวัดระดับของการดำเนินงานเป็นอีกปัจจัยสำคัญ ซึ่งจะทำให้เราได้ทราบถึงสิ่งที่เราได้ดำเนินการแล้ว และสิ่งใดบ้างที่ควรจะดำเนินการต่อไป เพื่อปรับปรุงการดำเนินงานให้เกิดประสิทธิภาพสูงสุด ระดับความพร้อมของการกำกับดูแลข้อมูล ถูกใช้เป็นเครื่องมือในการวัดระดับการดำเนินงานในการกำกับดูแลข้อมูล ซึ่งประกอบด้วย ๖ ระดับ ดังต่อไปนี้

- ระดับ ๐ : None หมายถึง ไม่มีการกำกับดูแลข้อมูลหรือมีแต่ไม่ได้ดำเนินการอย่างเป็นทางการ นั่นคือ มีการดำเนินงานบางส่วนและไม่มีการประกาศให้ทราบอย่างเป็นทางการ
- ระดับ ๑ : Initial หมายถึง ไม่มีการกำหนดมาตรฐานของกระบวนการ นั่นคือ กระบวนการถูกกำหนดขึ้นมาเฉพาะกิจ ทำให้แต่ละโครงการมีรูปแบบของกระบวนการที่แตกต่างกัน และอำนาจในการจัดการและกำกับดูแลข้อมูลที่มีอยู่ในไอทีแต่มีข้อจำกัดต่อกระบวนการทางธุรกิจ การทำงานร่วมกันระหว่างธุรกิจและไอทีไม่สอดคล้องกัน
- ระดับ ๒ : Managed หมายถึง เริ่มมีการกำหนดมาตรฐานของกระบวนการเฉพาะแต่ละส่วนงานหรือบริการ และมีการกำหนดบุคคลที่เกี่ยวข้องกับการกำกับติดตาม เช่น บริกรข้อมูลและผู้รับผิดชอบข้อมูล เป็นต้น กระบวนการถูกนำไปใช้กับโครงการสำคัญ ๆ ภายในส่วนงาน
- ระดับ ๓ : Standardized หมายถึง กระบวนการถูกกำหนดเป็นมาตรฐานของหน่วยงาน มีการกำหนดส่วนงานกลางในการกำกับและติดตามข้อมูล ซึ่งมาจากบุคคลด้านธุรกิจและไอที มีการบังคับใช้นโยบายข้อมูลครอบคลุมทั้งหน่วยงาน คุณภาพข้อมูลถูกติดตามและถูกรายงานผล
- ระดับ ๔ : Advanced หมายถึง กระบวนการกำกับดูแลและคุณภาพข้อมูลถูกวัดและถูกรายงานผล
- ระดับ ๕ : Optimized หมายถึง มีการดำเนินการการวิเคราะห์ความคุ้มทุนในการดำเนินการกำกับดูแล วัตถุประสงค์ของการปรับปรุงกระบวนการกำกับข้อมูลถูกกำหนดขึ้นให้สอดคล้องกับการเปลี่ยนแปลงของวัตถุประสงค์ของหน่วยงาน และวัตถุประสงค์ของการปรับปรุงนี้จะถูกใช้เป็นเกณฑ์สำหรับการปรับปรุงกระบวนการกำกับและติดตาม

ระดับความพร้อมของการกำกับดูแลข้อมูลสรุปไว้ตามตารางที่ ๓

ตารางที่ ๓ ระดับความพร้อมของการกำกับดูแลข้อมูล

ระดับ	กระบวนการกำกับดูแล	โครงสร้างการกำกับดูแล	นโยบายข้อมูลและการตรวจสอบ	การวัดประสิทธิภาพกระบวนการและคุณภาพข้อมูล	การวัดความคุ้มทุนและการปรับปรุงอย่างต่อเนื่อง
๐ : None	ไม่มีหรือมีแต่ไม่เป็นทางการ	ไม่มีหรือมีแต่ไม่เป็นทางการ	ไม่มีหรือมีแต่ไม่เป็นทางการ	ไม่มีหรือมีแต่ไม่เป็นทางการ	ไม่มีหรือมีแต่ไม่เป็นทางการ
๑ : Initial	กระบวนการยังไม่เป็นมาตรฐาน	มีการกำหนดผู้กำกับดูแลอย่างไม่เป็นทางการ	ไม่มีหรือมีแต่ไม่เป็นทางการ	ไม่มีหรือมีแต่ไม่เป็นทางการ	ไม่มีหรือมีแต่ไม่เป็นทางการ
๒ : Managed	มีกระบวนการเป็นมาตรฐานส่วนงาน/บริการ	มีการกำหนดผู้กำกับดูแลในแต่ละส่วนงาน/บริการ	บังคับใช้ในส่วนงาน/ บริการ	ไม่มีหรือมีแต่ไม่เป็นทางการ	ไม่มีหรือมีแต่ไม่เป็นทางการ
๓: Standardized	มีกระบวนการเป็นมาตรฐานหน่วยงาน	มีส่วนงานกลางในการกำกับดูแล ซึ่งประกอบไปด้วยบุคคลด้านธุรกิจและไอที	บังคับใช้ทั้งหน่วยงาน	มีการวัดคุณภาพข้อมูล	ไม่มีหรือมีแต่ไม่เป็นทางการ
๔ : Advanced	มีกระบวนการเป็นมาตรฐานหน่วยงาน	มีส่วนงานกลางในการกำกับดูแล ซึ่งประกอบไปด้วยบุคคลด้านธุรกิจและไอที	บังคับใช้ทั้งหน่วยงาน	มีการวัดประสิทธิภาพกระบวนการและคุณภาพข้อมูล	ไม่มีหรือมีแต่ไม่เป็นทางการ
๕ : Optimized	มีกระบวนการเป็นมาตรฐานหน่วยงาน	มีส่วนงานกลางในการกำกับดูแล ซึ่งประกอบไปด้วยบุคคลด้านธุรกิจและไอที	บังคับใช้ทั้งหน่วยงาน	มีการวัดประสิทธิภาพกระบวนการและคุณภาพข้อมูล	มีการวัดความคุ้มทุนและดำเนินการปรับปรุงกระบวนการอย่างต่อเนื่อง

๓.๔.๒ ระดับคุณภาพของข้อมูล (Data Quality Level)

ระดับคุณภาพของข้อมูล (Data Quality Levels) เป็นการกำหนดระดับคุณภาพของข้อมูลโดยใช้หลักเกณฑ์ในด้านต่าง ๆ ประกอบด้วย ข้อมูลมีความถูกต้อง (Accuracy) ข้อมูลมีความครบถ้วน (Completeness) และข้อมูลมีความต้องกัน (Consistency) ข้อมูลมีความเป็นปัจจุบัน (Timeliness) ข้อมูลมีความพร้อมใช้ (Availability) และข้อมูลตรงตามความต้องการของผู้ใช้ (Relevancy)

๑) ข้อมูลมีความถูกต้อง (Accuracy) ข้อมูลจะมีความถูกต้องและเชื่อถือได้มากน้อยเพียงใดนั้นขึ้นกับวิธีการที่ใช้ในการควบคุมข้อมูลนำเข้า และการควบคุมการประมวลผล การควบคุมข้อมูลนำเข้าเป็นการกระทำเพื่อให้เกิดความมั่นใจว่าข้อมูลนำเข้ามีความถูกต้องเชื่อถือได้ เพราะถ้าข้อมูลนำเข้าไม่มีความถูกต้องแล้วถึงแม้จะใช้วิธีการวิเคราะห์และประมวลผลข้อมูลที่ดีเพียงใดผลลัพธ์ที่ได้ก็จะไม่มีความถูกต้อง หรือนำไปใช้ไม่ได้ ข้อมูลนำเข้าจะต้องเป็นข้อมูลที่ผ่านการตรวจสอบว่าถูกต้องแล้ว ข้อมูลบางอย่างอาจต้องแปลงให้อยู่ในรูปแบบที่เครื่องคอมพิวเตอร์สามารถเข้าใจได้อย่างถูกต้อง ซึ่งอาจต้องพิมพ์ข้อมูลมาตรวจเช็คด้วยมือก่อนการประมวลผลถึงแม้ว่าจะมีการตรวจสอบข้อมูลนำเข้าแล้วก็ตาม ก็อาจทำให้ได้ข้อมูลที่ผิดพลาดได้ เช่น เกิดจากการเขียนโปรแกรมหรือใช้สูตรคำนวณผิดพลาดได้ ดังนั้น จึงควรกำหนดวิธีการควบคุมการประมวลผล ได้แก่ การตรวจเช็คยอดรวมที่ได้จากการประมวลผลแต่ละครั้งหรือการตรวจสอบผลลัพธ์ที่ได้จากการประมวลผลด้วยเครื่องคอมพิวเตอร์กับข้อมูลสมมติที่มีการคำนวณด้วยว่ามีความถูกต้องตรงกันหรือไม่

๒) ข้อมูลมีความครบถ้วน (Completeness) ข้อมูลบางประเภทหากไม่ครบถ้วน จัดเป็นข้อมูลที่ด้อยคุณภาพได้เช่นกัน เช่น ข้อมูลประวัติคนไข้ หากไม่มีหมู่เลือดของคนไข้ จะไม่สามารถใช้ได้ในกรณีที่ผู้ร้องขอข้อมูลต้องการข้อมูลหมู่เลือดของคนไข้ หรือข้อมูลที่อยู่ของลูกค้าที่กรอกผ่านแบบฟอร์ม ถ้ามีชื่อและนามสกุลโดยไม่มีข้อมูลบ้านเลขที่ ถนน แขวง/ตำบล เขต/อำเภอ หรือจังหวัด ข้อมูลเหล่านั้นก็ไม่สามารถนำมาใช้ได้เช่นกัน

๓) ข้อมูลมีความต้องกัน (Consistency) คือ ค่าข้อมูลในชุดข้อมูลเดียวที่สอดคล้องกับค่าในชุดข้อมูลอื่น นอกจากนี้คำจำกัดความของความสอดคล้องระบุว่าหากมีการดึงข้อมูลสองค่าจากชุดข้อมูลแยกต่างหากต้องไม่ขัดแย้งกันโดยความสอดคล้องอาจมีการกำหนดไว้ในบริบทต่าง ๆ เช่น

- ระหว่างหนึ่งชุดของค่าลักษณะประจำและค่าลักษณะประจำอื่นที่ตั้งอยู่ภายในระเบียนเดียวกัน (Record Level)
- ระหว่างหนึ่งชุดของค่าลักษณะประจำและค่าลักษณะประจำอื่นที่กำหนดในระเบียนที่ต่างกัน (Cross-Record)
- ระหว่างหนึ่งชุดของค่าลักษณะประจำและค่าลักษณะประจำเดียวกันที่ตั้งอยู่ภายในระเบียนเดียวกันที่จุดที่แตกต่างกันในเวลา (ความสอดคล้องชั่วคราว)

ความสอดคล้องอาจคำนึงถึงแนวคิด "ความสมเหตุสมผล" ซึ่งในช่วงของการยอมรับจะถูกกำหนดในค่าของคุณลักษณะ ตัวอย่างของกฎความสอดคล้องตรวจสอบว่าภายในโครงสร้างลำดับชั้นของบริษัท จำนวนรวมของพนักงานในแต่ละไซต์ไม่ควรเกินจำนวนพนักงานทั้งหมดของบริษัท เป็นต้น

๔) ข้อมูลมีความเป็นปัจจุบัน (Timeliness) ข้อมูลที่ดีนั้นนอกจากจะเป็นข้อมูลที่มีความถูกต้องเชื่อถือได้แล้วจะต้องเป็นข้อมูลที่เป็นปัจจุบัน ทั้งนี้ เพื่อให้ผู้ใช้สามารถนำเอาผลลัพธ์ที่ได้ไปใช้ได้ทันเวลานั่นคือ จะต้องเก็บข้อมูลได้รวดเร็วเพื่อทันความต้องการของผู้ใช้

๕) ข้อมูลมีความพร้อมใช้ (Availability) หมายถึง ความง่ายในการเข้าถึงข้อมูลที่สนใจของผู้ที่จะใช้งาน โดยจะต้องมีข้อมูลที่สามารถใช้งานได้ซึ่งต้องมีข้อมูลที่ต้องการ ตัวอย่างเช่น นักวิเคราะห์แผนงานต้องการข้อมูลบัญชีของการประกันภัยต่อเขตต่าง ๆ แต่ข้อมูลไม่พร้อมใช้งานจนกระทั่งต้องใช้คนเขียนโปรแกรมเพื่อดึงข้อมูลนั้นออกมา ในกรณีนี้หากข้อมูลมีความพร้อมกับความต้องการใช้ ผู้ใช้สามารถใช้ข้อมูลดังกล่าวได้ทันที

๖) ข้อมูลตรงตามความต้องการของผู้ใช้ (Relevancy) ระดับของข้อมูลที่บริหารจัดการต้องการนำเสนอโดยตรงและมีประสิทธิภาพ โดยสามารถใช้งานได้ตามวัตถุประสงค์ ตัวอย่างเช่น ข้อมูลทางสถิติที่จะเป็นการนำเสนอในรูปแบบตารางเข้าใจง่าย และข้อความอยู่ในหลาย ๆ ย่อหน้า ซึ่งสามารถใช้งานได้ตามความต้องการ

ระดับคุณภาพของข้อมูลสามารถวัดออกมาในรูปแบบของร้อยละของคะแนนที่ได้ ดังตารางต่อไปนี้

ตารางที่ ๔ ระดับคุณภาพข้อมูล

ชื่อชุดข้อมูล	ระดับคุณภาพข้อมูล						
	ความถูกต้อง (ร้อยละ)	ความครบถ้วน (ร้อยละ)	ความต้องกัน (ร้อยละ)	ความเป็นปัจจุบัน (ร้อยละ)	ความพร้อมใช้ (ร้อยละ)	ตรงตามความต้องการใช้ (ร้อยละ)	ค่าเฉลี่ย
ชุดข้อมูลที่ ๑							
ชุดข้อมูลที่ ๒							
ชุดข้อมูลที่ ๓							
ชุดข้อมูลที่ ๔							
ชุดข้อมูลที่ ๕							
ค่าเฉลี่ย							

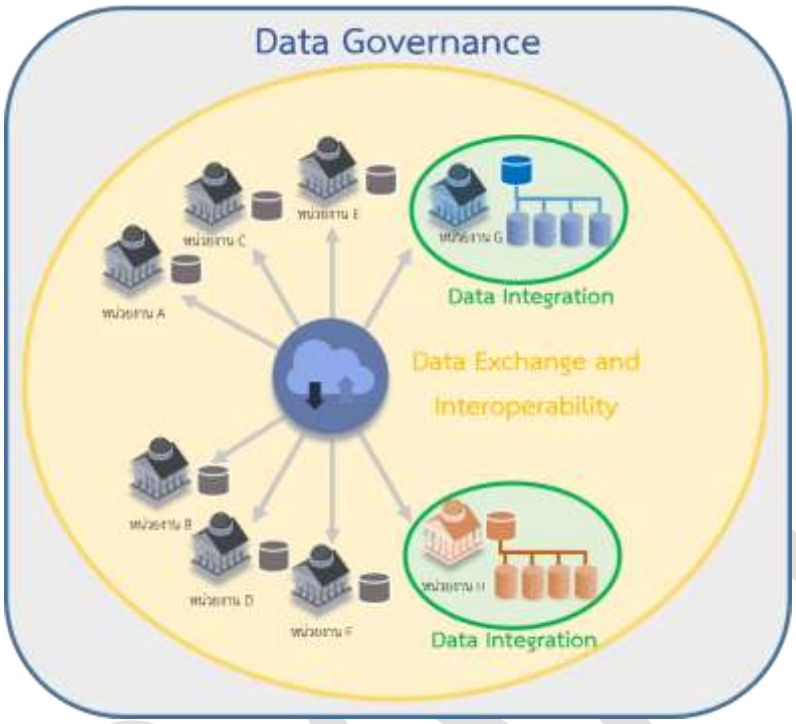
๓.๕ แนวทางการดำเนินการกำกับดูแลข้อมูล (Data Governance Guideline)

๓.๕.๑ การกำกับดูแลข้อมูลในการแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน

การแลกเปลี่ยนข้อมูลเป็นกระบวนการของการรับส่งข้อมูลหรือแบ่งปันข้อมูลภายในหน่วยงานหรือระหว่างหน่วยงาน ตัวอย่างการแลกเปลี่ยนข้อมูลภาครัฐ เช่น การแลกเปลี่ยนข้อมูลกระบวนการยุติธรรม ข้อมูลการนำเข้า/ส่งออกสินค้าระหว่างประเทศ ข้อมูลภูมิสารสนเทศ ข้อมูลการบริหารจัดการน้ำ ข้อมูลเกษตรกรผู้ยากจน และข้อมูลความมั่นคงประเทศ ทั้งนี้ ข้อมูลที่มีการแลกเปลี่ยนต้องไม่เป็นข้อมูลเปิด (Open Data) หรือข้อมูลที่สามารถนำไปใช้ได้โดยอิสระ

การกำกับดูแลข้อมูลถือเป็นส่วนสำคัญที่จะช่วยให้การแลกเปลี่ยนข้อมูลมีประสิทธิภาพและประสิทธิผล ซึ่งส่งผลให้เกิดประโยชน์ต่อภาคประชาชน ภาครัฐ ตลอดจนภาคเอกชน อันจะส่งผลต่อความเจริญก้าวหน้า

ของประเทศ สอดคล้องกับรูปที่ ๙ ซึ่งชี้ให้เห็นถึงการกำกับดูแลข้อมูลเข้ามาควบคุมการบูรณาการข้อมูล (Data Integration) และการแลกเปลี่ยนข้อมูล (Data Exchange) เพื่อให้เกิดการเชื่อมโยงข้อมูลระหว่างหน่วยงาน (Interoperability) อย่างแท้จริง



รูปที่ ๙ ความสัมพันธ์ระหว่างการกำกับดูแลข้อมูลและการแลกเปลี่ยนข้อมูล

โดยกิจกรรมของการกำกับดูแลข้อมูลที่เกี่ยวข้องกับการแลกเปลี่ยนข้อมูลควรประกอบไปด้วย ๑) กำหนดบทบาทหน้าที่ของบุคคลที่เกี่ยวข้อง ๒) กำหนดนโยบายการแลกเปลี่ยนข้อมูล และ ๓) กำหนดแนวปฏิบัติในการแลกเปลี่ยนข้อมูล ดังรายละเอียดต่อไปนี้

๑) กำหนดบทบาทหน้าที่ ที่เกี่ยวข้องกับการแลกเปลี่ยนข้อมูล

- ๑.๑) กำหนดบุคคลหรือกลุ่มบุคคลที่มีสิทธิ์ตัดสินใจในการเปิดเผยข้อมูล เช่น คณะกรรมการกำกับดูแลข้อมูล (Data Governance Council) หรือคณะทำงานเปิดเผยข้อมูล
- ๑.๒) กำหนดบุคคลหรือกลุ่มบุคคลในการดำเนินการแลกเปลี่ยนข้อมูล เช่น บุคคลที่ทำหน้าที่ออกแบบกระบวนการและเทคโนโลยีในการแลกเปลี่ยนข้อมูล (Data Integration Architect) และบุคคลที่ทำหน้าที่ดำเนินการแลกเปลี่ยนข้อมูลให้สอดคล้องกับที่ได้ออกแบบไว้ (Data Integration Specialist)
- ๑.๓) กำหนดบุคคลหรือกลุ่มบุคคลในการรับเรื่องและแก้ไขปัญหาเบื้องต้นในการแลกเปลี่ยนหรือขอใช้ข้อมูล เช่น ศูนย์ติดต่อ (Contact Center)

๒) กำหนดนโยบายการแลกเปลี่ยนข้อมูล

ในหัวข้อ ๒.๖.๔ ได้แสดงกรอบนโยบายการแลกเปลี่ยนข้อมูล ดังต่อไปนี้

๒.๑) กำหนดแนวปฏิบัติและสัญญาอนุญาตในการแลกเปลี่ยนข้อมูลเพื่อให้มั่นใจได้ว่าข้อมูลจะยังคงความมั่นคงปลอดภัยและรักษาคุณภาพของข้อมูล เช่น การจัดการเรื่องความมั่นคงปลอดภัยและคุณภาพข้อมูล ผู้ประสานงานหรือศูนย์ติดต่อ Contact Center)

๒.๒) กำหนดกระบวนการในการแลกเปลี่ยนข้อมูลที่ชัดเจนตั้งแต่ เตรียมการ เริ่มดำเนินการ ระหว่างดำเนินการ และสิ้นสุดการดำเนินการ

๒.๓) กำหนดรายการชุดข้อมูลมาตรฐาน เมทาดาตาของชุดข้อมูลมาตรฐาน และข้อตกลงในการแลกเปลี่ยนข้อมูล

๒.๔) กำหนดเทคโนโลยีและมาตรฐานทางเทคนิคที่ใช้ในการแลกเปลี่ยนข้อมูล

๒.๕) ต้องมีการบันทึกการใช้งาน (Log File) เพื่อให้สามารถตรวจสอบย้อนกลับได้

๒.๖) ตรวจสอบให้แน่ใจว่าการแลกเปลี่ยนข้อมูลถูกดำเนินการได้อย่างเหมาะสมหรือเป็นไปตามแนวปฏิบัติ กระบวนการแลกเปลี่ยน และมาตรฐานที่กำหนด

๓) กำหนดแนวปฏิบัติการแลกเปลี่ยนข้อมูล

แนวปฏิบัติการแลกเปลี่ยนข้อมูลเป็นไปตามขั้นตอนต่อไปนี้

๓.๑) กำหนดสิทธิ์ของหน่วยงานที่สามารถนำมาข้อมูลไปใช้ได้ตามบทบาทและภารกิจตามกฎหมายของหน่วยงานนั้น ๆ

๓.๒) จัดทำเมทาดาตา (Metadata) ของชุดข้อมูลที่ขอ ตัวอย่างองค์ประกอบของเมทาดาตา เช่น ชื่อข้อมูล คำอธิบายข้อมูล คำสำคัญ วันที่ทำการเปลี่ยนแปลงข้อมูลล่าสุด ชื่อหน่วยงานเจ้าของข้อมูล และฟิลด์ข้อมูล ทั้งนี้ต้องตรวจสอบให้แน่ใจได้ว่าเมทาดาตามีฟิลด์ข้อมูลครบถ้วนสอดคล้องกับความต้องการของหน่วยงานที่ขอใช้ข้อมูล

๓.๓) จัดทำสัญญาอนุญาตหรือเงื่อนไขการเข้าถึงและการใช้ข้อมูล ตัวอย่างส่วนประกอบของสัญญา เช่น วัตถุประสงค์ในการนำไปใช้ ขอบเขตในการนำไปใช้ ช่วงวันที่ในการเข้าถึง ความถี่ในการเข้าถึง ช่วงเวลาในการนำไปใช้ ฟิลด์ที่สามารถเข้าถึง และรายการที่สามารถเข้าถึง

- ในกรณีเป็นข้อมูลส่วนบุคคล (Personal Data) และเข้าถึงเป็นรายบุคคล หน่วยงานที่ขอใช้จะต้องได้รับการยินยอมจากเจ้าของข้อมูลก่อน พร้อมทั้งแจ้งผลการตอบรับการยินยอมไปยังหน่วยงานที่ถือครองข้อมูล
- ในกรณีเป็นข้อมูลส่วนบุคคลและเข้าถึงบางส่วนหรือทุกรายการ หน่วยงานที่ถือครองข้อมูลต้องมีมาตรการในการปกปิดไม่ให้หน่วยงานที่ขอใช้ข้อมูล สามารถทราบได้ว่าข้อมูลแต่ละรายการเป็นของบุคคลใด โดยอ้างอิง “แนวปฏิบัติในการปกป้องข้อมูลที่ระบุตัวบุคคลได้ (Guideline to protect the Personally Identifiable Information)”

๓.๔) ตรวจสอบชั้นความลับของข้อมูล (Data Classification) ว่าอยู่ในชั้นความลับที่สามารถเปิดเผยได้หรือไม่ นั่นคือ ต้องไม่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ ความมั่นคงของประเทศ ความลับทางราชการ และความเป็นส่วนตัว

๓.๕) ตรวจสอบและปรับปรุงคุณภาพของข้อมูล (Data Quality) ให้อยู่ในเกณฑ์ที่ยอมรับได้ก่อนการแลกเปลี่ยน

๓.๖) กำหนดเทคโนโลยีและมาตรฐานทางเทคนิคที่ใช้ในการแลกเปลี่ยนข้อมูล เช่น Representational State Transfer (REST) และ Simple Object Access Protocol (SOAP)

๓.๗) ต้องพิจารณาการเข้ารหัสข้อมูลก่อนการแลกเปลี่ยนข้อมูลบางประเภท เช่น ข้อมูลความมั่นคงประเทศ

๓.๘) ติดตามและควบคุมประสิทธิภาพระหว่างการแลกเปลี่ยนข้อมูล เพื่อรักษาไว้ซึ่งความปลอดภัยและคุณภาพข้อมูล โดยมีการกำหนดระดับการให้บริการ (Service Level Agreement-SLA)

๓.๕.๒ การกำกับดูแลในการเปิดเผยข้อมูลและการขอใช้ข้อมูล

ข้อมูลเปิด (Open Data) คือ “ข้อมูลที่สามารถนำไปใช้ได้โดยอิสระ สามารถนำกลับมาใช้ใหม่และแจกจ่ายได้โดยใครก็ตาม แต่ต้องระบุแหล่งที่มาหรือเจ้าของงานและต้องใช้สัญญาอนุญาต หรือเงื่อนไขเดียวกันกับที่มาหรือตามเจ้าของงานกำหนด”[2] ข้อมูลจากหน่วยงานภาครัฐที่สามารถเปิดเผยได้ ต้องเป็นข้อมูลส่วนบุคคลและไม่มีผลกระทบต่อความมั่นคงของประเทศ โดยการเปิดเผยข้อมูลจะอยู่ในรูปแบบที่เป็นมาตรฐานเปิด (Open Format) และไม่ใช่รูปแบบมาตรฐานเฉพาะ (Non-Proprietary Format) ที่คนและเครื่องคอมพิวเตอร์สามารถอ่านและนำไปใช้ต่อยอดในการพัฒนาบริการในรูปแบบต่าง ๆ ได้ ข้อมูลเปิดถูกใช้เป็นเครื่องมือในการตรวจสอบความโปร่งใสในการดำเนินการของภาครัฐและความสามารถในการพัฒนาประเทศ ซึ่งสามารถวัดอันดับการเปิดเผยข้อมูลภาครัฐได้จากมาตรฐานตัวชี้วัด เช่น Open Data Index และ Open Data Barometer เพื่อให้อันดับการเปิดเผยข้อมูลภาครัฐสูงขึ้น หน่วยงานรัฐควรดำเนินการเปิดเผยตามหลักการเปิดเผยข้อมูล ๘ ด้าน ดังต่อไปนี้

๑) Complete (สมบูรณ์) ข้อมูลภาครัฐทั้งหมดที่ไม่เกี่ยวข้องกับข้อมูลส่วนบุคคลหรือความมั่นคงจะต้องถูกเปิดเผยโดยข้อมูลดังกล่าวจะไม่ขัดกับข้อกำหนดในเรื่องความเป็นส่วนตัว ความมั่นคงและเอกสิทธิ์ที่ชอบด้วยเหตุผล

๒) Primary (ข้อมูลปฐมภูมิ) ข้อมูลควรจะถูกเผยแพร่จากแหล่งที่เก็บข้อมูลโดยตรงด้วยระดับความละเอียดสูง ไม่มีการปรับแต่งหรือทำให้อยู่ในรูปแบบข้อมูลสรุป (Summary Data)

๓) Timely (ทันเวลา) คือ ข้อมูลควรจะเป็นปัจจุบันและหากเป็นไปได้อาจจะเป็นลักษณะ Real-time feed ซึ่งอาจจะพิจารณาตามความเหมาะสมในการเพิ่มอรรถประโยชน์ของข้อมูลนั้น ๆ ชุดข้อมูลควรจะมีการบันทึกเวลา (Timestamps) หรือข้อมูลอื่น ๆ ที่ช่วยให้ผู้ใช้งานสามารถระบุได้ว่าข้อมูลนั้นเป็นปัจจุบัน

๔) Accessible (สามารถเข้าถึงได้) ข้อมูลถูกเปิดเพื่อให้ผู้ใช้ที่หลากหลายและมีจุดประสงค์ต่างกันซึ่งข้อมูลดังกล่าวจะต้องมีการเผยแพร่อยู่บนอินเทอร์เน็ตโดยทุกคนจะต้องสามารถเข้าถึงข้อมูลเหล่านั้นได้และข้อมูลจะต้องรองรับการใช้งานจากทุกแพลตฟอร์ม

๕) Machine readability (เครื่องสามารถอ่านได้) ข้อมูลจะต้องอยู่ในรูปแบบที่นำไปประมวลผลได้โดยอัตโนมัติ

๖) Non-discriminatory (การไม่เลือกปฏิบัติ) ทุกคนสามารถนำข้อมูลไปใช้ได้โดยไม่ต้องมีการลงทะเบียนผู้ใช้

[2] https://data.go.th/~/fdocument/14

๗) Non-proprietary (ปลอดกรรมสิทธิ์) ข้อมูลที่เผยแพร่จะต้องอยู่ในรูปแบบมาตรฐานเปิดไม่ใช่รูปแบบมาตรฐานเฉพาะและไม่มีองค์กรใดมีสิทธิขาดในการเป็นเจ้าของแต่ผู้เดียว

๘) License-free (ใช้งานฟรี) ข้อมูลจะต้องไม่มีปัญหาเรื่องลิขสิทธิ์ในการใช้งานสามารถใช้งานโดยไม่เสียค่าใช้จ่ายเพื่อเป็นการส่งเสริมการใช้งานอย่างแพร่หลายทำให้เกิดเป็นนวัตกรรมและบรรลุเป้าหมายที่หน่วยงานตั้งไว้รวมทั้งเป็นการเพิ่มความโปร่งใสให้แก่หน่วยงานภาครัฐ ควรจะหลีกเลี่ยงข้อจำกัดในการใช้งานข้อมูล

โดยกิจกรรมของการกำกับดูแลข้อมูลที่เกี่ยวข้องกับการเปิดเผยข้อมูลควรประกอบไปด้วย ๑) กำหนดบทบาทหน้าที่ของบุคคลที่เกี่ยวข้อง ๒) กำหนดนโยบายการเปิดเผยข้อมูล และ ๓) กำหนดแนวปฏิบัติในการเปิดเผยข้อมูล ดังรายละเอียดต่อไปนี้

๑) กำหนดบทบาทหน้าที่ ที่เกี่ยวข้องกับการเปิดเผยข้อมูล

- ๑.๑) กำหนดบุคคลหรือกลุ่มบุคคลที่มีสิทธิ์ตัดสินใจในการเปิดเผยข้อมูล เช่น คณะกรรมการกำกับดูแลข้อมูล (Data Governance Council) หรือคณะทำงานเปิดเผยข้อมูล
- ๑.๒) กำหนดบุคคลหรือกลุ่มบุคคลในการดำเนินการและปรับปรุงการเปิดเผยข้อมูล
- ๑.๓) กำหนดบุคคลหรือกลุ่มบุคคลในการรับเรื่องและแก้ไขปัญหาเบื้องต้นในการเข้าถึงข้อมูลและการนำข้อมูลไปใช้ เช่น ศูนย์ติดต่อ (Contact Center)

๒) กำหนดนโยบายการเปิดเผยข้อมูล

ในหัวข้อ ๒.๖.๕ ได้แสดงกรอบนโยบายการเปิดเผยข้อมูล ดังต่อไปนี้

- ๒.๑) ห้ามเปิดเผยข้อมูลที่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง นโยบาย แนวปฏิบัติ ไม่ว่าข้อมูลจะอยู่ในรูปแบบใดหรือสถานที่ใดก็ตาม
- ๒.๒) ต้องได้รับการอนุญาตจากตัวแทนหน่วยงานหรือเจ้าของข้อมูลก่อนการเปิดเผยข้อมูล
- ๒.๓) ควรมีการระบุช่องทางการเปิดเผยข้อมูลที่เข้าถึงและนำไปใช้ได้ง่าย
- ๒.๔) ควรมีการเปิดเผยเมทาดาตาควบคู่ไปกับข้อมูลที่เปิดเผย
- ๒.๕) ต้องตรวจสอบให้แน่ใจว่าการเปิดเผยข้อมูลถูกดำเนินการได้อย่างเหมาะสมหรือเป็นไปตามแนวทางที่กำหนดเพื่อให้ได้ข้อมูลที่มีคุณภาพ และรักษาคุณภาพของข้อมูล

๓) กำหนดแนวปฏิบัติการเปิดเผยข้อมูล

แนวปฏิบัติการเปิดเผยข้อมูลเป็นไปตามขั้นตอนต่อไปนี้

- ๓.๑) คัดเลือกชุดข้อมูลที่ต้องการเผยแพร่ ทั้งนี้ควรจะต้องพิจารณาชุดข้อมูลที่มีคุณภาพและเป็นที่ต้องการของทุกภาคส่วน เพื่อส่งเสริมให้เกิดการนำไปใช้อย่างแพร่หลายและเกิดประโยชน์สูงสุด
- ๓.๒) พิจารณาชุดข้อมูลที่คัดเลือก ชุดข้อมูลที่คัดเลือกสำหรับเผยแพร่นั้นต้องอยู่ในชั้นความลับที่สามารถเผยแพร่ได้ นั่นคือ ต้องไม่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ ความมั่นคงของประเทศ ความลับทางราชการ และความเป็นส่วนตัว
- ๓.๓) จัดเตรียมข้อมูลให้อยู่ในรูปแบบที่ง่ายต่อการนำไปใช้ นั่นคือ ข้อมูลควรอยู่ในรูปแบบที่คอมพิวเตอร์สามารถอ่านได้ง่าย (Machine-Readable) หรือระดับการเปิดเผยข้อมูลระดับ ๒ ขึ้นไป เช่น รูปแบบของ Comma-Separated Values – CSV และ

Application Programming Interface - API รวมถึงการจัดทำคำอธิบายชุดข้อมูล (Metadata) เพื่อให้ผู้ใช้ข้อมูลสามารถเข้าใจเกี่ยวกับบริบทของข้อมูล เช่น เจ้าของข้อมูล วัตถุประสงค์ ขอบเขต วันที่เผยแพร่ ความถี่ในการปรับปรุง ความถี่ในการเผยแพร่ และแหล่งที่มาของข้อมูล

๓.๔) นำชุดข้อมูลขึ้นเผยแพร่ หน่วยงานจะต้องกำหนดผู้รับผิดชอบหลัก เพื่อนำชุดข้อมูลขึ้นเผยแพร่สู่สาธารณะ ซึ่งสามารถดำเนินการได้ ดังนี้

- เผยแพร่ผ่านเว็บไซต์หรือ Universal Resource Identifier- URI ของหน่วยงานพร้อมคำอธิบายชุดข้อมูล
- เผยแพร่ผ่านศูนย์กลางข้อมูลเปิดภาครัฐ โดยปฏิบัติตามเอกสาร คู่มือการนำข้อมูลขึ้นเผยแพร่บน data.go.th
- ผู้ใช้ข้อมูลถือได้ว่าเป็นผู้ที่มีส่วนร่วมในกระบวนการปรับปรุงคุณภาพของข้อมูลที่หน่วยงานได้เผยแพร่ผ่านช่องทางในการแสดงความคิดเห็นและการร้องขอข้อมูลที่ต้องการได้ ซึ่งการเปิดเผยข้อมูลที่มีคุณภาพและตรงกับความต้องการของผู้บริโภคนั้น จะช่วยให้เกิดการสร้างนวัตกรรมและช่วยยกระดับคุณภาพชีวิตของประชาชน รวมถึงช่วยให้เกิดการสร้างงานใหม่ ๆ อีกด้วย

๓.๕.๓ แนวทางการดำเนินการกำกับดูแลข้อมูลอื่น ๆ

ในส่วนนี้ได้ให้แนวทางการดำเนินการกำกับดูแลข้อมูลบางส่วน เพื่อให้เกิดการปฏิบัติเกี่ยวกับการกำกับดูแลข้อมูลและบริหารจัดการข้อมูลภายในหน่วยงานอย่างเป็นรูปธรรม ประกอบด้วย

๑) แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ (ดูที่ https://ictlawcenter.etda.or.th/files/law/file/33/5a42315f04a4f439866e879220ff7227.pdf)

๒) ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการใช้ข้อความ XML สำหรับการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ระหว่างหน่วยงาน (ดูที่ https://standard.etda.or.th/wp-content/uploads/2017/08/20170523-ER-eDocumentStandard-V08-14F-0816.pdf)

๓) ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยรหัสสถานที่ออกหนังสือรับรอง (ดูที่ https://standard.etda.or.th/wp-content/uploads/2017/05/20170526-ER-CertificationLocations-V08-08F-0529.pdf)

๔) แนวทางปฏิบัติการเปิดเผยข้อมูลภาครัฐ (Government Open Data Publication Guidelines)

- แนวปฏิบัติและมาตรฐานเชิงเทคนิค (ดูที่ https://data.go.th/~/fdocument/14)
- แบบฟอร์มเมทาดาตา (ดูที่ https://data.go.th/~/fdocument/7)
- Open Data Handbook (ดูที่ https://data.go.th/~/document/6)
- คู่มือการนำข้อมูลขึ้นเผยแพร่บน data.go.th (ดูที่ https://data.go.th/~/document/13)

๕) แนวปฏิบัติในการปกป้องข้อมูลที่ระบุตัวบุคคลได้ (Guideline to protect the Personally Identifiable Information)

๖) แนวปฏิบัติในการออกแบบความคิดเชิงนวัตกรรม (Guidelines for Data Innovation)

แบบฟอร์มและตัวอย่างการจัดทำเมทาดาตา (ดูที่ ภาคผนวก ก และ ข ตามลำดับ)

ภาคผนวก

ภาคผนวก ก แบบฟอร์มการจัดทำเมทาดาตา

ตารางที่ ๕ แบบฟอร์มการจัดทำเมทาดาตา

เมทาดาตา	โปรดระบุ
๑) ชื่อเรื่อง (ชื่อของข้อมูลที่กำหนดโดยหน่วยงานเจ้าของเรื่อง)	
๒) หน่วยงานเจ้าของเรื่อง พร้อมที่ติดต่อ (ชื่อบุคคลหรือชื่อหน่วยงานที่รับผิดชอบ ข้อมูลและที่อยู่ที่สามารถติดต่อได้)	
๓) หัวเรื่องหรือคำสำคัญ ที่ใช้สำหรับอ้างอิงในการค้นหาข้อมูล (หัวข้อ คำ หรือวลี ที่ใช้สำหรับการค้นเรื่องที่ต้องการได้)	
๔) คำอธิบายอย่างย่อ (รายละเอียดเกี่ยวกับข้อมูล)	
๕) หน่วยงานที่ให้ข้อมูล พร้อมที่ติดต่อ (ชื่อบุคคลหรือชื่อหน่วยงานที่ให้ข้อมูล และที่อยู่ที่สามารถติดต่อได้)	
๖) ผู้สนับสนุน หรือผู้ร่วมดำเนินการ (บุคคลหรือหน่วยงานนอกเหนือจากผู้รับผิดชอบข้อมูล ที่สนับสนุนหรือร่วมดำเนินการ)	
๗) วันที่เริ่มต้น (วัน เดือน ปี ที่เริ่มต้นใช้ข้อมูล)	
๘) วันที่ปรับปรุงครั้งสุดท้าย (วัน เดือน ปี สุดท้ายที่มีการปรับปรุงข้อมูล)	
๙) วิธีการได้มา (วิธีการที่ได้ซึ่ง ข้อมูล เช่น การรายงานจากระบบทะเบียน, การสำรวจข้อมูล, การวิจัย, เป็นต้น)	☐ การรายงานจากระบบทะเบียน ☐ การสำรวจข้อมูล ☐ การวิจัย ☐ อื่น ๆ.....

๑๐) ประเภทการนำเสนอ (ประเภทการนำเสนอข้อมูล เช่น home page, รายงานวิชาการ, ตารางสถิติ, ผลงานวิจัย, เป็นต้น)	☐ Home page ☐ รายงานวิชาการ ☐ ตารางสถิติ ☐ ผลงานวิจัย ☐ อื่น ๆ.....
๑๑) รูปแบบการเก็บข้อมูลปฐมภูมิ (รูปแบบที่บันทึกข้อมูลปฐมภูมิ เช่น text/html, ASCII, database, image, etc.)	☐ Text/html ☐ ASCII ☐ Database ☐ Image ☐ อื่น ๆ.....
๑๒) รูปแบบการเก็บข้อมูลทุติยภูมิ (รูปแบบที่บันทึกข้อมูลทุติยภูมิ เช่น text/html, ASCII, database, image, etc.)	☐ Text/html ☐ ASCII ☐ Database ☐ Image ☐ อื่น ๆ.....
๑๓) รหัสอ้างอิงเพื่อการเข้าถึงข้อมูล (สัญลักษณ์ หรือ เลขที่ หรือ รหัสอ้างอิง ที่ระบุเฉพาะว่าเป็น ข้อมูล นั้นๆ เช่น URL)	
๑๔) แหล่งที่มา (ระบุแหล่งที่มาของข้อมูล)	
๑๕) ภาษาที่ใช้ (ภาษาที่ใช้ เช่น ภาษาไทย ภาษาอังกฤษ ภาษาอื่น ๆ)	☐ ภาษาไทย ☐ ภาษาอังกฤษ ☐ อื่น ๆ.....
๑๖) เรื่องที่เกี่ยวข้อง (ระบุ link เรื่องอื่นๆ ที่เกี่ยวข้อง)	
๑๗) สรุปขอบเขต (คำอธิบายถึงขอบเขตของข้อมูล)	
๑๘) ขอบเขตทางภูมิศาสตร์หรือเขตการปกครอง (ขอบเขต หรือ พื้นที่ในการนำเสนอ ข้อมูล เช่น เฉพาะ กทม., ทั่วประเทศ)	☐ กรุงเทพมหานคร ☐ ทั่วประเทศ ☐ อื่น ๆ.....
๑๙) หน่วยของการจัดเก็บข้อมูล (หน่วยของการจัดเก็บหรือรวบรวมข้อมูล เช่น หมู่บ้าน ครัวเรือน บุคคล สถานประกอบการ เป็นต้น)	☐ หมู่บ้าน ☐ ครัวเรือน ☐ บุคคล ☐ สถานประกอบการ ☐ อื่น ๆ.....

๒๐) หน่วยย่อยที่สุดที่มีข้อมูล (หน่วยย่อย หรือขอบเขตที่ย่อยที่สุดที่มีข้อมูล เช่น ข้อมูลระดับหมู่บ้าน, จังหวัด, ภาค, ประเทศ เป็นต้น)	☐ หมู่บ้าน ☐ ตำบล ☐ อำเภอ ☐ จังหวัด ☐ ภาค ☐ ประเทศ ☐ อื่น ๆ.....
๒๑) ระเบียบในการเข้าถึงข้อมูล	
๒๒) ระเบียบในการใช้ข้อมูล	

ภาคผนวก ข ตัวอย่างการจัดทำเมทาดาตา

ตารางที่ ๖ ตัวอย่างการจัดทำเมทาดาตา

เมทาดาตา	โปรดระบุ
๑) ชื่อเรื่อง (ชื่อของข้อมูล ที่กำหนดโดยหน่วยงานเจ้าของเรื่อง)	สำรวจภาวะการทำงาน
๒) หน่วยงานเจ้าของเรื่องพร้อมที่ติดต่อ (ชื่อบุคคลหรือชื่อหน่วยงานที่รับผิดชอบ ข้อมูลและที่อยู่ที่สามารถติดต่อได้)	สำนักงานสถิติแห่งชาติ
๓) หัวเรื่องหรือคำสำคัญที่ใช้สำหรับอ้างอิงในการค้นหา ข้อมูล (หัวข้อ คำ หรือวลี ที่ใช้สำหรับการค้นเรื่องที่ต้องการได้)	แรงงาน
๔) คำอธิบายอย่างย่อ (รายละเอียดเกี่ยวกับข้อมูล)	ผู้มีงานทำ, ผู้ว่างงาน, กำลังแรงงานปัจจุบัน, กำลังแรงงานที่รอฤดูกาล, กำลังแรงงานรวม, ผู้ไม่อยู่ในกำลังแรงงาน,งาน, อาชีพ, อุตสาหกรรม, สถานภาพการทำงาน, ชั่วโมงทำงาน, รายได้ของลูกจ้าง, ระยะเวลาของการหางานทำ, ระดับการศึกษาที่สำเร็จ
๕) หน่วยงานที่ให้ข้อมูล พร้อมที่ติดต่อ (ชื่อบุคคลหรือชื่อหน่วยงานที่ให้ข้อมูล และที่อยู่ที่สามารถติดต่อได้)	กลุ่มสถิติแรงงาน สำนักสถิติเศรษฐกิจและสังคม

๖) ผู้สนับสนุน หรือผู้ร่วมดำเนินการ (บุคคลหรือหน่วยงานนอกเหนือจากผู้รับผิดชอบ ข้อมูล ที่สนับสนุนหรือร่วมดำเนินการ)	-
๗) วันที่เริ่มต้น (วัน เดือน ปี ที่เริ่มต้นใช้ข้อมูล)	13 พฤศจิกายน 2560
๘) วันที่ปรับปรุงครั้งสุดท้าย (วัน เดือน ปี สุดท้ายที่มีการปรับปรุงข้อมูล)	30 กรกฎาคม 2560
๙) วิธีการได้มา (วิธีการที่ได้ซึ่ง ข้อมูล เช่น การรายงานจากระบบทะเบียน, การสำรวจข้อมูล, การวิจัย, เป็นต้น)	☐ การรายงานจากระบบทะเบียน ☑ การสำรวจข้อมูล ☐ การวิจัย ☐ อื่น ๆ.....
๑๐) ประเภทการนำเสนอ (ประเภทการนำเสนอข้อมูล เช่น home page, รายงานวิชาการ, ตารางสถิติ, ผลงานวิจัย, เป็นต้น)	☐ Home page ☑ รายงานวิชาการ ☐ ตารางสถิติ ☐ ผลงานวิจัย ☐ อื่น ๆ.....
๑๑) รูปแบบการเก็บข้อมูลปฐมภูมิ (รูปแบบที่บันทึกข้อมูลปฐมภูมิ เช่น text/html, ASCII, database, image, etc.)	☐ Text/html ☐ ASCII ☑ Database ☐ Image ☐ อื่น ๆ.....
๑๒) รูปแบบการเก็บข้อมูลทุติยภูมิ (รูปแบบที่บันทึกข้อมูลทุติยภูมิ เช่น text/html, ASCII, database, image, etc.)	☐ Text/html ☐ ASCII ☑ Database ☐ Image ☐ อื่น ๆ.....
๑๓) รหัสอ้างอิงเพื่อการเข้าถึงข้อมูล (สัญลักษณ์ หรือ เลขที่ หรือ รหัสอ้างอิง ที่ระบุเฉพาะว่าเป็น ข้อมูล นั้นๆ เช่น URL)	nso.go.th
๑๔) แหล่งที่มา (ระบุแหล่งที่มาของข้อมูล)	โครงการสำรวจ
๑๕) ภาษาที่ใช้ (ภาษาที่ใช้ เช่น ภาษาไทย ภาษาอังกฤษ ภาษาอื่น ๆ)	☑ ภาษาไทย ☑ ภาษาอังกฤษ

	☐ อื่น ๆ.....
๑๖) เรื่องที่เกี่ยวข้อง (ระบุ link เรื่องอื่นๆ ที่เกี่ยวข้อง)	http://www.molsw.go.th http://www.nesdb.go.th http://www.bot.or.th/
๑๗) สรุปขอบเขต (คำอธิบายถึงขอบเขตของข้อมูล)	ครัวเรือน
๑๘) ขอบเขตทางภูมิศาสตร์หรือเขตการปกครอง (ขอบเขต หรือ พื้นที่ในการนำเสนอ ข้อมูล เช่น เฉพาะ กทม., ทั่วประเทศ)	☐ กรุงเทพมหานคร ☑ ทั่วประเทศ ☐ อื่น ๆ.....
๑๙) หน่วยของการจัดเก็บข้อมูล (หน่วยของการจัดเก็บหรือรวบรวมข้อมูล เช่น หมู่บ้าน ครัวเรือน บุคคล สถานประกอบการ เป็นต้น)	☐ หมู่บ้าน ☐ ครัวเรือน ☑ บุคคล ☐ สถานประกอบการ ☐ อื่น ๆ.....
๒๐) หน่วยย่อยที่สุดที่มีข้อมูล (หน่วยย่อย หรือขอบเขตที่ย่อยที่สุดที่มีข้อมูล เช่น ข้อมูลระดับหมู่บ้าน, จังหวัด, ภาค, ประเทศ เป็นต้น)	☐ หมู่บ้าน ☐ ตำบล ☐ อำเภอ ☐ จังหวัด ☐ ภาค ☑ ประเทศ ☐ อื่น ๆ.....
๒๑) ระเบียบในการเข้าถึงข้อมูล	ผู้ใช้ทั่วไป
๒๒) ระเบียบในการใช้ข้อมูล	ระเบียบในการใช้ข้อมูลของสำนักงานสถิติแห่งชาติ

บรรณานุกรม

Askham, N. (2016). *Squaring the circle: Using a data governance framework to support data quality*. Experian Information Solutions, Inc.

Australian Institute of Health and Welfare. (2014). *Data Governance Framework*, retrieved ๕ มกราคม ๒๕๖๑, จาก https://www.aihw.gov.au/getmedia/0d59ee71-9abe-4806-8e87-ce9de81974d3/AIHW-data-governance-framework.pdf.aspx

Data Governance Institute. (n.d.). *HOW TO USE THE DGI DATA GOVERNANCE FRAMEWORK TO CONFIGURE YOUR PROGRA*, ค้นเมื่อ ๙ มกราคม ๒๕๖๑, จาก http://www.datagovernance.com/wp-content/uploads/2014/11/wp_how_to_use_the_dgi_data_governance_framework.pdf

DAMA International. (2009). *The DAMA Guide to the data management body of knowledge (DAMA-DMBOK Guide).* The Data Management Association International.

DAMA International (2012). *DAMA-DMBOK Functional Framework Version 3.02.*, ค้นเมื่อ ๒ มกราคม ๒๕๖๑, จาก https://dama.org/sites/default/files/download/DAMA-DMBOK2-Framework-V2-20140317-FINAL.pdf

DAMA United Kingdom. (2013). *THE SIX PRIMARY DIMENSIONS FOR DATA QUALITY ASSESSMENT.*, ค้นเมื่อ ๑๗ มกราคม ๒๕๖๑, จาก https://www.whitepapers.em360tech.com/wp-content/files_mf/1407250286DAMAUKDQDimensionsWhitePaperR37.pdf

INFORMATICA. (2015). *Data Governance Implementation*., ค้นเมื่อ ๙ มกราคม ๒๕๖๑, จาก https://www.informatica.com/content/dam/informatica-com/global/amer/us/collateral/service-offering/data-governance-implementation_service-offering_2239.pdf

INFORMATICA. (2006). *Monitoring Data Quality Performance Using Data Quality Metrics*., ค้นเมื่อ ๙ มกราคม ๒๕๖๑, จาก https://www.it.ojp.gov/documents/Informatica_Whitepaper_Monitoring_DQ_Using_Metrics.pdf

Intra-governmental Group on Geographic Information (IGGI). (2005). *The Principles of Good Data Management*. The Office of the Deputy Prime Minister.

Kim, H. Y., & Cho, J. S. (2017, June). Data Governance Framework for Big Data Implementation with a Case of Korea. *In Big Data (BigData Congress), 2017 IEEE International Congress on* (pp. 384-391). IEEE.

ORACLE. (2011). *Enterprise Information Management: Best Practices in Data Governance*., ค้นเมื่อ ๒๕ มกราคม ๒๕๖๑, จาก http://egovstandards.gov.in/sites/default/files/oea-best-practices-data-gov-400760.pdf