ประกาศองค์การตลาดเพื่อเกษตรกร

เรื่อง นโยบายการกำกับดูแลและบริหารจัดการข้อมูล (Data Governance Policy)

พ.ศ. ๒๕๖๗

๑. หลักการและเหตุผล

องค์การตลาดเพื่อเกษตรกร เป็นศูนย์กลางและช่องทางจำหน่ายสินค้าเกษตรที่มีความโดดเด่น น่าเชื่อถือด้านคุณภาพเพื่อช่วยเหลือเกษตรกรอย่างยั่งยืน ด้วยเทคโนโลยีและนวัตกรรมเพื่อเพิ่มขีดความสามารถในการแข่งขัน เนื่องด้วยเทคโนโลยีดิจิทัลในปัจจุบันเข้ามามีบทบาทสำคัญในการขับเคลื่อนธุรกิจ เป็นส่วนที่สำคัญในการบริหารจัดการข้อมูล เพื่อให้เกิดการขับเคลื่อนองค์กรด้วยข้อมูลที่ดีได้อย่างยั่งยืน และเป็นแนวทางที่จะช่วยให้สามารถกำหนด ทิศทาง ควบคุม ให้ข้อมูลมีคุณภาพที่ดี จึงได้มีการจัดทำ Data Governance การบริหารจัดการข้อมูล สอดคล้องกับกฎหมาย กรอบธรรมาภิบาลข้อมูลภาครัฐ และระเบียบปฏิบัติที่เกี่ยวข้อง การจัดทำแนวปฏิบัติด้านธรรมาภิบาลข้อมูลและการบริหารจัดการข้อมูลของ อ.ต.ก. ให้เป็นไปตามกรอบธรรมาภิบาลข้อมูลสำหรับ ผู้บริหาร พนักงาน ลูกจ้าง ตลอดจนผู้มีส่วนได้ส่วนเสีย

๒. ขอบเขต

เพื่อให้เป็นไปตามพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ รวมถึงกฎหมายที่เกี่ยวข้อง โดยให้ครอบคลุมการบริหารจัดการและการบูรณาการข้อมูล จึงได้มีการกำหนดนโยบายที่เกี่ยวกับเงื่อนไขและวิธีการสร้าง การจัดเก็บรักษา การควบคุมคุณภาพ การประมวลผล การใช้ การแลกเปลี่ยน การเชื่อมโยง การเปิดเผย การรักษาความลับ และการทำลายข้อมูล และมีผลบังคับใช้ไปถึงบุคลากรและ/หรือหน่วยงานภายในทั้งหมด ได้แก่ ผู้บริหาร พนักงาน ตลอดจนผู้มีส่วนได้ส่วนเสีย

๓. วัตถุประสงค์

๑. เพื่อใช้เป็นกรอบและแนวทางในการบริหารจัดการข้อมูลของ อ.ต.ก. สำหรับผู้บริหาร พนักงาน ลูกจ้าง ตลอดจนผู้มีส่วนได้ส่วนเสีย

๒. เพื่อให้การบริหารจัดการข้อมูลของ อ.ต.ก. สอดคล้องกับกฎหมาย กรอบธรรมาภิบาลข้อมูลภาครัฐ และระเบียบปฏิบัติที่เกี่ยวข้อง

๓. เพื่อใช้เป็นกรอบในการจัดทำแนวปฏิบัติด้านธรรมาภิบาลข้อมูลและการบริหารจัดการข้อมูลของ อ.ต.ก. ที่เป็นไปตามกรอบธรรมาภิบาลข้อมูลภาครัฐ

๔. ค่านิยาม

“อ.ต.ก." หมายความว่า องค์การตลาดเพื่อเกษตรกร

“ข้อมูล” หมายความว่า สิ่งที่สื่อความหมายให้รู้เรื่องราว ข้อเท็จจริง ข้อมูลหรือสิ่งใด ๆ ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเอง หรือโดยผ่านวิธีการใด ๆ และไม่ว่าจะได้จัดทำไว้ ในรูปแบบของเอกสาร แฟ้มรายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้

/“ข้อมูลที่...

"ข้อมูลที่เป็นเอกสาร" หมายความว่า ข้อมูลที่มีการจัดเก็บและบันทึกในรูปแบบของกระดาษ

"ข้อมูลที่ไม่เป็นเอกสาร" หมายความว่า ข้อมูลสารสนเทศ ข้อมูลคอมพิวเตอร์ ข้อมูลอิเล็กทรอนิกส์

"ชุดข้อมูล" หมายความว่า การนำข้อมูลจากหลายแหล่งมารวบรวม เพื่อจัดเป็นชุดให้ตรงตาม ลักษณะโครงสร้างของข้อมูล

"ข้อมูลหลัก" หมายความว่า ข้อมูลที่สร้างและใช้งานร่วมกันภายในขอบเขตการดำเนินงานตามภารกิจของหน่วยงาน เช่น ข้อมูลพนักงาน ข้อมูลลูกค้า ข้อมูลเกษตรกร ข้อมูลสินค้า ข้อมูลครุภัณฑ์ ข้อมูลสถานที่

"ข้อมูลอ้างอิง" หมายความว่า ข้อมูลอ้างอิง จะเป็นข้อมูลที่เป็นสากล มีการกำหนดให้เป็นมาตรฐาน และใช้งานร่วมกัน มีการเปลี่ยนแปลงค่อนข้างน้อย เช่น รหัสไปรษณีย์ รหัสประเทศ หน่วยวัดระยะทาง

"เมทาดาตา" หมายความว่า คำอธิบายชุดข้อมูลดิจิทัล เพื่อให้ทราบรายละเอียดเกี่ยวกับโครงสร้างของข้อมูล เนื้อหาสาระ รูปแบบการจัดเก็บ แหล่งข้อมูล และสิทธิในการเข้าถึงข้อมูล

"บัญชีข้อมูล" หมายความว่า เอกสารแสดงรายการของชุดข้อมูลที่จำแนกแยกแยะ โดยการจัดกลุ่มหรือจัดประเภทชุดข้อมูลที่อยู่ในความครอบครองหรือควบคุมของ อ.ต.ก.

"ข้อมูลส่วนบุคคล" หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

"เจ้าของข้อมูล" หมายความว่า เจ้าหน้าที่หรือหน่วยงานที่รับผิดชอบเกี่ยวกับข้อมูล มีอำนาจในการบริหารจัดการและควบคุมชุดข้อมูล สร้าง แก้ไข ลบ กำหนดสิทธิการเข้าถึง อนุญาตหรือปฏิเสธ การเข้าถึงข้อมูล และเป็นผู้รับผิดชอบต่อความถูกต้อง ทันสมัย ความสมบูรณ์ และการทำลาย รวมถึงกำหนดระดับชั้นความลับ สิทธิการใช้งาน และความปลอดภัยของข้อมูล

"ผู้ดูแลข้อมูล" หมายความว่า ผู้ที่ทำงานร่วมกับเจ้าของข้อมูลโดยตรง ทำหน้าที่จัดเก็บรักษาข้อมูลรวมถึงป้องกันภัยคุกคาม ทำการสำรองข้อมูล ดำเนินการตามขั้นตอน ที่ระบุไว้ในนโยบายและแผนงานความมั่นคงปลอดภัย ทั้งทางด้านระบบสารสนเทศ และที่มิใช่สารสนเทศ

"ผู้ใช้ข้อมูล" หมายความว่า ผู้ที่ได้รับสิทธิการใช้ข้อมูลจากผู้รับผิดชอบ หรือได้รับมอบหมายให้ใช้ข้อมูลจากผู้บังคับบัญชา รวมถึงผู้ซึ่งได้รับความยินยอมให้ทำงาน หรือทำผลประโยชน์ให้แก่หน่วยงาน

"ระดับชั้นความลับ" หมายความว่า การกำหนดการเปิดเผยข้อมูลต่อผู้อื่นให้เหมาะสมกับสถานะการใช้งาน ได้แก่ ลับที่สุด ลับมาก ลับ ปกปิด และเปิดเผยสู่ภายนอกได้

"ความมั่นคงปลอดภัยของข้อมูล" หมายความว่า การธำรงไว้ซึ่งความลับ ความถูกต้องครบถ้วน และการรักษาสภาพพร้อมใช้ของข้อมูล

"ธรรมาภิบาลข้อมูลภาครัฐ" หมายความว่า การกำหนดสิทธิในการตัดสินใจและ ความรับผิดชอบ ในการส่งเสริมให้เกิดกระบวนการจัดทำ การใช้งาน และการบริหารจัดการข้อมูลรวมถึงกระบวนการที่กำหนดบทบาท นโยบาย และมาตรฐานที่ช่วยสนับสนุนให้การดำเนินงานเกี่ยวกับข้อมูลมีประสิทธิภาพมากยิ่งขึ้น ซึ่งส่งผลให้หน่วยงานสามารถบรรลุเป้าหมายได้

/"คณะกรรมการ...

"คณะกรรมการธรรมาภิบาลข้อมูล" หมายความว่า กลุ่มบุคคลที่มีอำนาจในการผลักดัน ให้เกิดธรรมาภิบาลข้อมูล โดยมีหน้าที่รับผิดชอบในการกำหนดเป้าหมาย กำกับดูแลและติดตาม การดำเนินงาน รวมถึงให้คำปรึกษาและตัดสินประเด็นสำคัญที่เกี่ยวข้องกับข้อมูล สนับสนุน ส่งเสริม ผลักดันธรรมาภิบาลข้อมูลและการสื่อสารให้บุคลากรในหน่วยงานตระหนักถึงความสำคัญของข้อมูล การใช้ข้อมูลอย่างปลอดภัย

"คณะทำงานทีมบริกรข้อมูล" หมายความว่า กลุ่มบุคคลที่มุ่งเน้นการดำเนินงานและนิยามคำอธิบายชุดข้อมูล ทั้งเชิงธุรกิจและเทคโนโลยีสารสนเทศ ร่างนโยบาย กำหนดมาตรฐาน ตรวจสอบการปฏิบัติงาน และวิเคราะห์ผลจากการตรวจสอบในการบริหารจัดการตามองค์ประกอบของการบริหารจัดการข้อมูล

หมวดที่ ๑
หมวดทั่วไป

วัตถุประสงค์

เพื่อกำหนดแนวทางการดำเนินงานด้านธรรมาภิบาลข้อมูล เนื่องจากการกำหนดนโยบายข้อมูลจัดเป็นหนึ่งในองค์ประกอบตามกรอบการธรรมาภิบาลข้อมูล และให้การบริหารจัดการข้อมูลมีประสิทธิภาพ จึงต้องมีการกำหนดนโยบายที่ระบุอย่างชัดเจน สอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง หรือข้อกำหนดอื่น ๆ ที่เกี่ยวข้อง โดยผ่านการอนุมัติจากผู้บริหาร มีการเผยแพร่และสื่อสาร ให้กับเจ้าหน้าที่และผู้ที่เกี่ยวข้อง รวมถึงมีการทบทวนสม่ำเสมอ เพื่อให้นโยบายข้อมูลได้ถูกนำมาปฏิบัติอย่างมีประสิทธิภาพและต่อเนื่อง

นโยบาย

๑. กำหนดให้มีโครงสร้างกำกับดูแลข้อมูล และกำหนดบทบาทหน้าที่ความรับผิดชอบในการบริหารจัดการข้อมูล

๒. กำหนดกลุ่มบุคคลหรือหน่วยงานที่เป็นเจ้าของข้อมูลในการบริหารจัดการข้อมูล

๓. กำหนดขอบเขตข้อมูลที่อยู่ในความดูแลของผู้ครอบครองหรือควบคุมข้อมูล

๔. กำหนดนโยบาย มาตรการการรักษาความปลอดภัยของข้อมูล เพื่อป้องกันการเข้าถึงการสูญหาย การทำลาย หรือการเปลี่ยนแปลงข้อมูลโดยไม่ได้รับการอนุญาต

๕. กำหนดมาตรฐาน (Data Standard) และระเบียบปฏิบัติมาตรฐานและการบริหารจัดการเมทาดาตา (Metadata) หรือค่าอธิบายชุดข้อมูล ครอบคลุมถึงบทบาทหน้าที่ความรับผิดชอบ กระบวนการจัดทำเมทาดาตาการควบคุม ดูแลและสอบทานคำอธิบายชุดข้อมูล

๖. กำหนดให้มีการนำเครื่องมือและ/หรือเทคโนโลยีสารสนเทศเข้ามาช่วยในการบริหารจัดการข้อมูล

๗. กำหนดให้มีการสื่อสารและเผยแพร่นโยบายข้อมูลให้กับผู้ที่เกี่ยวข้องทั้งภายในองค์กรและภายนอกองค์กร

๘. กำหนดให้มีการฝึกอบรมเพื่อสร้างความตระหนักถึงการกำกับดูแลข้อมูล การบริหารจัดการข้อมูล โดยครอบคลุมกระบวนการของธรรมาภิบาลข้อมูล และวงจรชีวิตข้อมูล

๙. กำหนดให้มีการวัดผลการดำเนินการและความสำเร็จของธรรมาภิบาลข้อมูล และรายงานผลการดำเนินงาน อย่างน้อยปีละ ๓ ครั้ง เพื่อนำไปปรับปรุงกระบวนการธรรมาภิบาลข้อมูลให้มีประสิทธิภาพมากขึ้น

/๑๐. กำหนด...

๑๐. กำหนดให้มีการตรวจสอบความสอดคล้องระหว่างนโยบายข้อมูลกับการดำเนินการใด ๆ ของผู้มีส่วนได้ส่วนเสีย อย่างน้อยปีละ ๑ ครั้ง

๑๑. กำหนดให้มีการทบทวนนโยบายข้อมูลอย่างน้อยปีละ ๑ ครั้ง และให้ดำเนินการปรับปรุงอย่างต่อเนื่องหากพบว่านโยบายข้อมูลยังไม่มีประสิทธิภาพเพียงพอ

หมวดที่ ๒
การจัดเก็บข้อมูลและทำลายข้อมูล

วัตถุประสงค์

เพื่อให้การสร้าง การจัดเก็บรักษาข้อมูล และการทำลายข้อมูล เป็นไปอย่างมีคุณภาพ มีการควบคุมคุณภาพข้อมูล สำหรับการใช้ประโยชน์จากข้อมูลในการบริหารงานและการให้บริการของ อ.ต.ก. โดยเป็นไปตามอำนาจหน้าที่และวัตถุประสงค์ในการดำเนินงานของ อ.ต.ก. รวมถึงการกำหนดแนวทางในการบริหารจัดการความมั่นคงปลอดภัยของข้อมูลและความเป็นส่วนบุคคล ซึ่งจะต้องสอดคล้องกับนโยบายความมั่นคงปลอดภัยและความเป็นส่วนบุคคลของข้อมูล

นโยบาย

๑. กำหนดมาตรฐานข้อมูลให้เป็นแบบเดียวกัน และมีการควบคุมคุณภาพข้อมูลตลอดทั้งวงจรชีวิตข้อมูล (Data Lifecycle) ของข้อมูลที่ตนเองมีหน้าที่รับผิดชอบนั้น

๒. กำหนดให้มีการสร้างข้อมูลที่มีคุณภาพ ชุดข้อมูลทุกชุดต้องมีการวัดคุณภาพข้อมูลดังต่อไปนี้ ความถูกต้อง (Accuracy) ความครบถ้วน (Completeness) ความต้องกัน (Consistency) ความเป็นปัจจุบัน (Timeliness) ตรงตามความต้องการของผู้ใช้ (Relevancy) ความน่าเชื่อถือ (Data Integrity) และพร้อมใช้งาน (Availability)

๓. กำหนดตัวชี้วัดคุณภาพข้อมูล เช่น ความถูกต้อง ความครบถ้วน ความต้องกัน ความเป็นปัจจุบัน ตรงตามความต้องการของผู้ใช้ และพร้อมใช้งาน

๔. กำหนดสภาพแวดล้อมในการจัดเก็บข้อมูลที่เอื้อต่อการรักษาความมั่นคงปลอดภัยและคุณภาพของข้อมูล

๕. กำหนดให้มีการจัดเก็บข้อมูลที่สอดคล้องกับความต้องการและวัตถุประสงค์ในการดำเนินงาน

๖. กำหนดให้มีการแจ้งให้ผู้ใช้บริการทราบถึงเหตุผลในการจัดเก็บข้อมูล

๗. สร้างความรู้ความเข้าใจในการจัดเก็บข้อมูลแก่ผู้ที่เกี่ยวข้องภายในองค์กรและภายนอกองค์กร

๘. กำหนดชั้นความลับของข้อมูล (Data Classification) และจัดเก็บให้สอดคล้องกับแนวทาง หรือมาตรฐานการจัดการชั้นความลับของข้อมูลที่กำหนดไว้ เพื่อให้ข้อมูลมีความมั่นคงปลอดภัย และรักษาคุณภาพของข้อมูล

๙. กำหนดสิทธิการเข้าถึงข้อมูล วิธี และเครื่องมือที่ใช้ในการเข้าถึงข้อมูล

๑๐. กำหนดระยะเวลาในการทบทวนสิทธิและวิธีในการเข้าถึงข้อมูล

๑๑. กำหนดระยะเวลาในการจัดเก็บข้อมูลที่เหมาะสมกับข้อมูลแต่ละประเภท กำหนดเครื่องมือและกระบวนการที่จะใช้ในการจัดเก็บข้อมูลระหว่างระยะเวลาในการจัดเก็บข้อมูล

๑๒. กำหนดขั้นตอนและวิธีการทำลายข้อมูล

/๑๓. กำหนด...

๑๓. กำหนดอำนาจอนุมัติ สิทธิ และยืนยันตัวบุคคลในการทำลายข้อมูล

๑๔. กำหนดให้มีการกำหนดวิธีและแนวทางในการทำลายข้อมูล เมื่อข้อมูลนั้นไม่มีการใช้งาน หรือมีการเก็บข้อมูลไว้นานเกินกว่าระยะเวลาที่กำหนด

หมวดที่ ๓
การประมวลผลและการใช้ข้อมูล

วัตถุประสงค์

เพื่อให้การประมวลผลข้อมูลและการใช้ข้อมูลที่มีประสิทธิภาพ ถูกต้อง ตรงตามวัตถุประสงค์ของการใช้ข้อมูลให้เกิดประโยชน์ รวมถึงวิธีการและแนวทางในการขอข้อมูลจากหน่วยงานที่เกี่ยวข้องทั้งภายใน และภายนอก เพื่อนำมาใช้ในการประมวลผลและนำมาใช้ ทั้งนี้ การนำข้อมูลมาใช้ให้เป็นไปตามวัตถุประสงค์ตามที่แจ้ง หากนอกเหนือจากเหตุผลดังกล่าวข้างต้น จะต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อน

นโยบาย

๑. กำหนดแนวปฏิบัติและมาตรฐานของการประมวลผลข้อมูล และทำการสื่อสารให้แก่ผู้ที่เกี่ยวข้องรับทราบ

๒. บริกรข้อมูล เจ้าของข้อมูล และผู้มีส่วนได้ส่วนเสียกับข้อมูลที่เกี่ยวข้องต้องร่วมกัน จัดทำเมทาดาตา (Metadata) หรือคำอธิบายข้อมูลสำหรับข้อมูลที่จัดเก็บอยู่ในฐานข้อมูล (Database) ในทุกชุดข้อมูล

๓. ชุดข้อมูลต้องมีการจัดลำดับชั้นความลับของข้อมูล การกำหนดชั้นความลับของข้อมูล และการกำหนดสิทธิการเข้าถึง เพื่อให้สอดคล้องกับแนวทางการจัดชั้นความลับของข้อมูล

๔. การดำเนินการประมวลผลข้อมูลที่เป็นความลับ เช่น ข้อมูลส่วนบุคคล ให้เป็นไปตามขอบเขต เงื่อนไขหรือวัตถุประสงค์ในการยินยอมให้ดำเนินการกับข้อมูลส่วนบุคคลนั้น เป็นต้น

๕. การกำหนดข้อมูลมาใช้ให้เป็นไปตามวัตถุประสงค์ตามที่แจ้ง หากนอกเหนือจากเหตุผลดังกล่าวข้างต้น จะต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อน

๖. ต้องมีการบันทึกประวัติการประมวลผลและการใช้ข้อมูลใน Log files เพื่อให้สามารถตรวจสอบย้อนกลับได้

๗. ต้องมีการทบทวนระดับชั้นความลับข้อมูล อย่างน้อยปีละ ๑ ครั้ง และให้ดำเนินการปรับปรุงอย่างต่อเนื่อง

/หมวดที่ ๔...

หมวดที่ ๔
การแลกเปลี่ยนและการเชื่อมโยงข้อมูล

วัตถุประสงค์

เพื่อให้การแลกเปลี่ยนข้อมูลทั้งภายในและระหว่างหน่วยงานมีความมั่นคงปลอดภัยและข้อมูลมีคุณภาพ สามารถนำไปใช้ประโยชน์ได้อย่างมีประสิทธิภาพ โดยมีวิธีและแนวทางการนำข้อมูล ไปเชื่อมโยงและแลกเปลี่ยนกับหน่วยงานภายนอก ให้สอดคล้องกับระเบียบ หลักเกณฑ์ และกฎหมายที่กำหนดบนพื้นฐานของประโยชน์ส่วนรวมเป็นสำคัญ

นโยบาย

๑. กำหนดกระบวนการในการร้องขอ แลกเปลี่ยน เชื่อมโยงข้อมูลให้ชัดเจนเริ่มตั้งแต่ขั้นตอนการเตรียมการ การเริ่มดำเนินการ ระหว่างดำเนินการ และสิ้นสุดการดำเนินการ

๒. กำหนดเมทาดาตาของชุดข้อมูลที่ต้องการร้องขอ แลกเปลี่ยน เชื่อมโยงข้อมูลที่จำเป็นให้ครบถ้วน

๓. ทำสัญญาอนุญาต บันทึกข้อตกลง (Memorandum of Understanding : MOU) สัญญารักษาความลับ (Non-disclosure agreement : NDA) หรือข้อตกลงอื่นใดว่าด้วยการเชื่อมโยงข้อมูลขององค์กร หรือข้อตกลงในการแลกเปลี่ยนข้อมูลและการนำข้อมูลไปใช้

๔. กำหนดเทคโนโลยีและมาตรฐานทางเทคนิคที่ใช้ในการแลกเปลี่ยน เชื่อมโยงข้อมูล

๕. บันทึกรายละเอียดและจัดเก็บข้อมูลดำเนินงานที่เกิดขึ้นในแต่ละครั้งที่มีการ ร้องขอ แลกเปลี่ยน เชื่อมโยงข้อมูล ใน Log File ระหว่างหน่วยงาน เพื่อให้สามารถตรวจสอบย้อนกลับได้

๖. สามารถตรวจสอบได้ว่า การร้องขอ แลกเปลี่ยน เชื่อมโยงข้อมูล ได้ดำเนินการ อย่างเหมาะสมหรือเป็นไปตามแนวทางปฏิบัติของกระบวนการร้องขอ แลกเปลี่ยน เชื่อมโยงข้อมูล และมาตรฐานตามที่กำหนด

๗. กำหนดบุคคลหรือกลุ่มบุคคลในการดำเนินการเชื่อมโยงและแลกเปลี่ยนข้อมูล เช่น บุคคลที่ทำหน้าที่ออกแบบกระบวนการและเทคโนโลยีในการเชื่อมโยงและแลกเปลี่ยน ข้อมูล (Data Integration Architect) บุคคลที่ทำหน้าที่ดำเนินการเชื่อมโยงและแลกเปลี่ยนข้อมูลให้สอดคล้องกับที่ได้ออกแบบไว้ (Data Integration Specialist)

/หมวดที่ ๕...

หมวดที่ ๕
การเปิดเผยข้อมูล

วัตถุประสงค์

เพื่อกำหนดนโยบายในการเปิดเผยข้อมูล รวมถึงการแจกจ่ายข้อมูลที่สามารถแจกจ่ายได้ให้สามารถเปิดเผยข้อมูลได้อย่างถูกต้อง ตรงตามวัตถุประสงค์ของการให้นำข้อมูลไปใช้ประโยชน์ ซึ่งจะต้องกำหนดวิธีการและแนวทางการเปิดเผยข้อมูลสำหรับเอกชน และสำหรับหน่วยงานภาครัฐที่ร้องขอข้อมูล

นโยบาย

๑. กำหนดบทบาทหน้าที่ที่เกี่ยวข้องกับการเปิดเผยข้อมูล ได้แก่ กำหนดบุคคลหรือกลุ่มบุคคล ที่มีสิทธิตัดสินใจในการเปิดเผยข้อมูล กำหนดบุคคลหรือกลุ่มบุคคลในการดำเนินการและปรับปรุงการเปิดเผยข้อมูล และกำหนดบุคคลหรือกลุ่มบุคคลในการรับเรื่องและแก้ไขปัญหาเบื้องต้นในการเข้าถึงข้อมูลและการนำข้อมูลไปใช้

๒. ห้ามเปิดเผยข้อมูลที่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง หลักเกณฑ์ นโยบาย แนวปฏิบัติขององค์กรที่ประกาศใช้ ในปัจจุบัน ไม่ว่าข้อมูลจะอยู่ในรูปแบบใดหรือสถานที่ใดก็ตาม

๓. ต้องได้รับความยินยอม ได้รับอนุญาตจากเจ้าของข้อมูล (Data Owner) ก่อนการเปิดเผยข้อมูล

๔. ให้มีการคัดเลือกชุดข้อมูลที่ต้องการเผยแพร่ โดยหน่วยงานเจ้าของข้อมูลหรือผู้ที่ได้รับมอบหมาย

๕. ให้มีการจัดเตรียมข้อมูลที่อยู่ในรูปแบบที่ได้จัดทำไว้เป็นมาตรฐานตามกำหนด และง่ายต่อการนำไปใช้

๖. ให้มีการระบุช่องทางการเปิดเผยข้อมูลที่เข้าถึงและนำไปใช้ได้ง่าย

๗. ให้มีการเปิดเผยเมทาดาตา ควบคู่ไปกับข้อมูลที่เปิดเผย

๘. ให้สามารถตรวจสอบว่าการเปิดเผยข้อมูลได้ถูกดำเนินการอย่างเหมาะสม หรือเป็นไปตามแนวทางที่ได้กำหนดไว้ เพื่อให้ได้ข้อมูลที่มีคุณภาพ และเป็นการรักษาคุณภาพของข้อมูล

๙. ให้มีการกำหนดผู้รับผิดชอบหลัก ขั้นตอน และวิธีการนำชุดข้อมูลขึ้นเผยแพร่สู่สาธารณะ

๑๐. ต้องปฏิบัติตามอย่างเคร่งครัด และป้องกันมิให้มีการเปิดเผยข้อมูล โดยไม่ได้รับอนุญาต

ประกาศ ณ วันที่ ๒๗ กันยายน ๒๕๖๗

(นายพีรพันธ์ คอทอง)
อธิบดีกรมส่งเสริมการเกษตร
ประธานกรรมการองค์การตลาดเพื่อเกษตรกร

องค์การตลาดเพื่อเกษตรกร
WWW.ORTORKOR.COM

การบริหารจัดการข้อมูล (Data Management)

พ.ศ. 2567

องค์การตลาดเพื่อเกษตรกร
กองเทคโนโลยีและสารสนเทศ

คำนำ

ปัจจุบันโลกได้ก้าวเข้าสู่ยุคดิจิทัล (Digital Era) อย่างเต็มรูปแบบ ซึ่งได้ก่อให้เกิดเทคโนโลยีสมัยใหม่ที่ได้เข้ามาช่วยสนับสนุนการดำเนินงานในภาคส่วนต่าง ๆ เป็นจำนวนมาก ทั้งในด้านของเกษตรกรรม อุตสาหกรรม และการบริการต่าง ๆ รวมทั้งพฤติกรรมบุคคลลูกค้า และผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับการดำเนินงานขององค์กร โดยมีการนำเทคโนโลยีสมัยใหม่เข้ามาช่วยในการทำกิจกรรมต่าง ๆ มากขึ้น เช่น การสื่อสารผ่านสื่อสังคมออนไลน์ การสั่งซื้อสินค้าออนไลน์ หรือการทำธุรกรรมออนไลน์ เป็นต้น โดยพฤติกรรมต่าง ๆ เหล่านั้น ก็มีแนวโน้มที่สูงขึ้นเรื่อย ๆ เพราะช่วยเอื้ออำนวยความเกิดความสะดวก รวดเร็ว และประหยัดค่าใช้จ่ายได้มากกว่า ประกอบกับเทคโนโลยีที่ได้มีการพัฒนาขึ้นอย่างต่อเนื่องเพื่อที่จะสนับสนุนและรองรับความต้องการของทุกภาคส่วน ซึ่งผลที่เกิดขึ้นดังกล่าวทำให้ในปัจจุบันมีข้อมูลข่าวสารเกิดขึ้นเป็นจำนวนมาก ทั้งในรูปแบบมีโครงสร้าง กึ่งโครงสร้าง และไม่มีโครงสร้าง โดยในหลาย ๆ องค์กรสามารถใช้ประโยชน์จากการเกิดขึ้นของข้อมูลจำนวนมากมาช่วยสนับสนุนการดำเนินงานขององค์กรให้มีประสิทธิภาพมากขึ้น แต่ในขณะที่บางหน่วยงานกับขาดกลไกการตรวจสอบ และกำกับดูแลอย่างถูกวิธี ทำให้ส่งผลกระทบต่อการดำเนินงานขององค์กรตามมาในภายหลัง

การกำกับดูแลข้อมูล หรือธรรมาภิบาลข้อมูล (Data Governance) จึงได้เข้ามามีบทบาทสำคัญในการส่งเสริม ใช้งาน และบริหารจัดการข้อมูลอย่างเหมาะสม ทั้งในด้านของการตัดสินใจ การกำหนดสิทธิ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน และการรักษาความมั่งคงปลอดภัยของข้อมูลทำให้ในหลาย ๆ หน่วยงานจึงได้มีการกำหนดหลักเกณฑ์เพื่อใช้เป็นแนวทางการดำเนินงานขององค์กรอย่างเหมาะสม เช่น ธรรมมาภิบาลข้อมูลภาครัฐของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) การกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร ของสำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ หรือการกำกับดูแลข้อมูลของสถาบันการกำกับดูแลข้อมูล (The Data Governance Institute)

ดังนั้น อ.ต.ก. ได้ตะหนักและเล็งเห็นถึงความสำคัญดังกล่าว จึงได้มีการจัดทำคู่มือการบริหารจัดการข้อมูล (Data Management Manual) ขึ้น เพื่อใช้เป็นแนวทางปฏิบัติในการบริหารจัดการข้อมูลให้กับบุคลากร ผู้บริหาร ตลอดจนผู้มีส่วนได้ส่วนเสียต่าง ๆ ที่เกี่ยวข้อง ให้สามารถมีวิธีการใช้ข้อมูลได้อย่างถูกต้องเหมาะสม และเกิดประโยชน์ในกระบวนงานของ อ.ต.ก. ต่อไป

ผู้จัดทำ

กองเทคโนโลยีและสารสนเทศ

สารบัญ

สารบัญ (ต่อ)

บทนำ
แนวทางการบริหารจัดการข้อมูล

วัตถุประสงค์

๑. เพื่อกำหนดนโยบายให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบ และบุคคลภายนอกที่ปฏิบัติงานให้กับองค์การตลาดเพื่อเกษตรกรตระหนักถึงความสำคัญของการธรรมาภิบาลข้อมูล

๒. เพื่อเป็นแนวทางในการควบคุม และตรวจสอบการดำเนินงานที่เกี่ยวข้องกับข้อมูล ตั้งแต่การสร้าง การจัดเก็บ การประมวลผล การใช้ การเผยแพร่ จนถึงการทำลาย

๓. เพื่อให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบ และบุคคลภายนอกที่ปฏิบัติงานให้กับ องค์การตลาดเพื่อเกษตรกรมีแนวทางในการดำเนินงานที่เกี่ยวข้องกับข้อมูล โดยครอบคลุมประเด็นต่อไปนี้

- คุณภาพข้อมูล (Data quality)
- ความพร้อมใช้งานของข้อมูล (Data availability)
- การใช้งานข้อมูล (Data usability)
- ความถูกต้องของข้อมูล (Data integrity)
- ความปลอดภัยของข้อมูล (Data security)

ขอบเขต

ใช้สำหรับการบริการจัดการข้อมูสำหรับองค์การตลาดเพื่อเกษตรกร และหน่วยงานที่เกี่ยวข้องให้ข้อมูลดังกล่าว พร้อมใช้งาน ถูกต้อง ปลอดภัย และเพื่อสามารถนำข้อมูลมาใช้งานได้อย่างมีประสิทธิภาพมากที่สุด ทั้งในแง่ของใช้ประโยชน์ภายในองค์กรและรองรับความต้องการของประชาชน

อ้างอิง

(References outside the company document system, such as the law, regulation, etc.)

- DAMA - DMBOK (หัวข้อ Data Management)
- ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ
- พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

คำจำกัดความและความหมาย

“อ.ต.ก.”	องค์การตลาดเพื่อเกษตรกร
การกำกับดูแลข้อมูล (Data Governance)	แนวคิดและกระบวนการสำหรับการจัดการข้อมูลในการทำให้มั่นใจว่าข้อมูลจะมีคุณภาพสูงตลอด Lifecycle
การบริหารจัดการข้อมูล (Data Management)	การควบคุมข้อมูล ไม่ว่าจะเป็นการเข้าถึง การเก็บรักษา ไปจนถึงการทำลายข้อมูลตามวงจรชีวิต (Data Life Cycle)
คำอธิบายชุดข้อมูล (Metadata)	ข้อมูลที่ใช้อธิบายข้อมูลหลักหรือกลุ่มข้อมูลอื่นๆ ที่เกี่ยวข้อง ทั้งกระบวนการเชิงธุรกิจและเชิงเทคโนโลยีสารสนเทศ ให้รายละเอียด ถึงกฎ ข้อจำกัดของข้อมูล และโครงสร้างของข้อมูล ช่วยให้องค์กรสามารถเข้าใจข้อมูล ระบบและขั้นตอนการทำงานได้ดียิ่งขึ้น
การบริหารจัดการคำอธิบายชุดข้อมูล (Metadata Management)	กระบวนการที่เกี่ยวข้องกับการบริหารจัดการหรือควบคุมคำอธิบาย ชุดข้อมูล เพื่อให้สามารถมั่นใจว่าคำอธิบายชุดข้อมูลสามารถมีการ เข้าถึง แบ่งปัน เชื่อมโยง วิเคราะห์ และบูรณาการ ให้เกิดประสิทธิผลทั่วทั้งองค์กร

คุณภาพข้อมูล (Data Quality)	ข้อมูลที่ดีได้มาตรฐานตามที่กำหนด กล่าวคือผลรวมของคุณลักษณะ และคุณสมบัติของผลิตผลข้อมูลที่พึงประสงค์ทุกประการของผล การปฏิบัติงานตามดัชนีตัวชี้วัดคุณภาพและองค์ประกอบที่กำหนดไว้ ข้อมูลที่เหมาะสมกับการใช้งาน ตอบสนองต่อความต้องการที่กำหนด และตรงตามวัตถุประสงค์
การบริหารจัดการคุณภาพข้อมูล (Data Quality Management)	กระบวนการที่เกี่ยวข้องกับการวางแผน การดำเนินการและการควบคุมกิจกรรมต่างๆ รวมถึงการปรับปรุงเพื่อให้ข้อมูลมีคุณภาพ มีความน่าเชื่อถือสามารถนำไปใช้ประกอบการวิเคราะห์และตัดสินใจทางธุรกิจได้อย่างถูกต้องเหมาะสม
การบริหารจัดการคุณภาพข้อมูล (Data Quality Management)	หมายถึงคำอธิบายชุดข้อมูลที่ให้รายละเอียดของชุดข้อมูลในด้านธุรกิจ เหมาะสำหรับผู้ใช้งานข้อมูลในการประกอบการดำเนินงานธุรกิจในองค์กร เช่น ชื่อข้อมูล ชื่อเจ้าของข้อมูล คำอธิบายอย่างย่อ วันที่เริ่มต้นใช้งาน วันที่ทำการเปลี่ยนแปลงข้อมูล ภาษาที่ใช้ชื่อฟิลด์ ข้อมูล (ชื่อพนักงาน นามสกุล เพศ) เป็นต้น
คำอธิบายข้อมูลเชิงธุรกิจ (Business Metadata)	คำอธิบายชุดข้อมูลที่ให้รายละเอียดของชุดข้อมูลในด้านธุรกิจเหมาะสำหรับผู้ใช้งานข้อมูลในการประกอบการดำเนินงานธุรกิจใน องค์กร เช่น ชื่อข้อมูล ชื่อเจ้าของข้อมูล คำอธิบายอย่างย่อ วันที่ เริ่มต้นใช้งาน วันที่ทำการเปลี่ยนแปลงข้อมูล ภาษาที่ใช้ชื่อฟิลด์ ข้อมูล (ชื่อพนักงาน นามสกุล เพศ) เป็นต้น
คำอธิบายข้อมูลเชิงเทคนิค (Technical Metadata)	คำอธิบายชุดข้อมูล ที่ให้รายละเอียดของชุดข้อมูลในด้านเทคนิค เหมาะสำหรับผู้บริหารจัดการข้อมูลในการประกอบการดำเนินงาน ด้านบริหารจัดการข้อมูลเช่น ชื่อตารางข้อมูลในฐาน ข้อมูล ชื่อฟิลด์ ข้อมูลในตารางข้อมูล ประเภทข้อมูล (เช่น ตัวเลข ตัวหนังสือ หรือ วันที่) ความกว้างของฟิลด์ข้อมูล (เช่น ๑๐ ตัวอักษร ๕๐ ตัวอักษร หรือ ๑๐๐ ตัวอักษร) คีย์ข้อมูล รวมไปถึงข้อมูลสำหรับการสำรอง ข้อมูล (Backup) และกู้คืนข้อมูล (Restore) เป็นต้น

บทที่ ๑
การกำกับดูแลข้อมูล

๑.๑ การจัดโครงสร้างองค์กรในการกำกับดูแลข้อมูล

อ.ต.ก. ควรกำหนดโครงสร้างองค์กร และบทบาทหน้าที่ความรับผิดชอบในกระบวนการกำกับดูแลข้อมูล อย่างชัดเจน เป็นลายลักษณ์อักษรโดยครอบคลุมอย่างน้อยในเรื่องดังต่อไป

๑.๑.๑ หน้าที่ความรับผิดชอบของคณะกรรมการ อ.ต.ก.

คณะกรรมการ อ.ต.ก. มีหน้าที่ในการกำกับดูแลให้ อ.ต.ก.ดำเนินการด้านที่เกี่ยวข้องกับการกำกับดูแล ข้อมูล ที่เหมาะสมกับขนาด ลักษณะการดำเนินธุรกิจ ความซับซ้อน และความเสี่ยงด้านข้อมูลของ อ.ต.ก. รวมทั้งสอดคล้องกับ กลยุทธ์ทางธุรกิจโดยควรกำหนดหน้าที่ความรับผิดชอบในการกำกับดูแลข้อมูลอย่างชัดเจน สอดคล้องตาม หลักการ line of defense และให้ดำเนินการอย่างน้อยในเรื่องดังต่อไปนี้

๑) กำกับดูแลให้ อ.ต.ก. มีการกำหนดนโยบายการกำกับดูแลข้อมูล โดยได้รับการพิจารณาอนุมัติจากคณะกรรมการ อ.ต.ก. หรือคณะกรรมการชุดย่อยที่ได้รับมอบหมาย และทบทวนอย่างน้อยปีละ ๑ ครั้ง หรือ ทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

๒) กำกับดูแลให้มีการนำนโยบายการกำกับดูแลข้อมูลที่ผ่านการอนุมัติจากคณะกรรมการ อ.ต.ก. หรือคณะกรรมการชุดย่อยที่ได้รับมอบหมายมาจัดทำระเบียบวิธีปฏิบัติและกระบวนการในการบริหารจัดการข้อมูลรวมถึงดูแลใหม่การนำไปปฏิบัติอย่างเหมาะสมและมีการทบทวนและประเมินประสิทธิภาพของนโยบายอย่างน้อยปีละ ๑ ครั้ง หรือ ทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

๓) กำกับดูแลให้มีผู้รับผิดชอบในการปฏิบัติหน้าที่ ครอบคลุมในเรื่องดังต่อไปนี้

- การกำกับ ดูแลข้อมูลและการบริหารจัดการข้อมูล
- การบริหารความเสี่ยงด้านข้อมูล
- การกำกับการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับข้อมูล
- การตรวจสอบการปฏิบัติงานที่เกี่ยวข้องกับข้อมูล

๔) จัดให้มีโครงสร้าง และกำหนดหน้าที่ความรับผิดชอบเกี่ยวกับการบริหารจัดการข้อมูล โดยเป็นไปตาม หลักการแบ่งแยกหน้าที่ความรับผิดชอบ ๓ ระดับ (Three Lines of Defense) เพื่อให้มีการกำหนดหน้าที่ความรับผิดชอบอย่างชัดเจน และมีการถ่วงดุลอำนาจในแต่ละระดับอย่างเหมาะสม

๕) กำกับดูแลให้มีการสร้างความรู้และความตระหนักด้านการกำกับดูแลข้อมูลในองค์กรแก่คณะกรรมการ อ.ต.ก. ผู้บริหาร และบุคลากรทุกระดับขององค์กร เพื่อสื่อสารให้เกิดความเข้ารู้ความเข้าใจถึงความสำคัญของการใช้ข้อมูลอย่างปลอดภัย

๖) จัดสรรทรัพยากรและงบประมาณ เพื่อรองรับการดำเนินการด้านการกำกับดูแลและบริหารจัดการข้อมูล แก่หน่วยงานที่เกี่ยวข้องทั้งในด้านบุคลากรและเครื่องมือให้เพียงพอที่จะสนับสนุนการปฏิบัติงานที่เกี่ยวข้องกับการกำกับดูแลข้อมูล

๑.๑.๒ การปฏิบัติหน้าที่เกี่ยวข้องกับการบริหารจัดการข้อมูล

๑.๑.๒.๑ การกำกับดูแลข้อมูล และการบริหารจัดการข้อมูล

อ.ต.ก. ควรจัดให้มีคณะกรรมการชุดย่อย (Data Governance Committee) เพื่อปฏิบัติหน้าที่ในการกำกับดูแลข้อมูลและบริหารจัดการข้อมูลโดยควรดำเนินการอย่างน้อยในเรื่องดังต่อไปนี้

๑) กำหนดนโยบายและระเบียบวิธีปฏิบัติที่เกี่ยวกับการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลรวมทั้งทบทวนหรือปรับปรุงให้เป็นปัจจุบันอยู่สมอ โดยควรทบทวนอย่างน้อยปีละ ๑ ครั้ง หรือ เมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ

๒) จัดให้มีการสื่อสารให้ความรู้เกี่ยวกับนโยบาย และระเบียบวิธีปฏิบัติที่เกี่ยวกับการกำกับดูแลข้อมูล และการบริหารจัดการข้อมูล ครอบคลุมทุกกระบวนการของการบริหารจัดการข้อมูล เพื่อให้บุคลากรทุกระดับ เกิดความตระหนักในการใช้ข้อมูลและสามารถนำไปปฏิบัติใดอย่างถูกต้องเหมาะสม

๓) ติดตามสถานะในเรื่องที่เกี่ยวข้องกับการกำกับดูแลข้อมูล และการบริหารจัดการข้อมูลรายงานผล ประเด็นปัญหา หรือความเสี่ยงที่พบต่อ ที่พบต่อคณะกรรมการ อ.ต.ก. หรือคณะกรรมการชุดย่อย หรือคณะกรรมการกำกับ ดูแลข้อมูล ตามระยะเวลาที่เหมาะสมเพียงพอ

๔) กำกับดูแลให้มั่นใจว่ามีการนำนโยบาย และระเบียบวิธีปฏิบัติที่เกี่ยวข้องกับการกำกับดูแลข้อมูล และการบริหารจัดการข้อมูลไปปฏิบัติ ในทุกระดับขององค์กรรวมถึงกำหนดบทบาทหน้าที่ ความรับผิดชอบในการอนุมัติหรือควบคุมดูแลการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับข้อมูล เช่น การอนุมัติการเข้าถึง การใช้และการเผยแพร่ข้อมูล เป็นต้น

๕) กำกับดูแลให้มีหน่วยงานหรือผู้รับผิดชอบบริหารจัดการคำอธิบายชุดข้อมูล (Metadata) เพื่อทำหน้าที่ในการจัดทำ ปรับปรุงแก้ไข และสอบทานคำอธิบายชุดข้อมูลให้เป็นปัจจุบัน

ทั้งนี้ เพื่อให้การดำเนินการด้านการกำกับดูแลข้อมูล และการบริหารจัดการข้อมูลมีประสิทธิภาพ อ.ต.ก. สามารถพิจารณากำหนดให้มีคณะทำงานหรือบุคลากรเพื่อดำเนินการในเรื่องดังต่อไปนี้

• คณะทำงานที่ปฏิบัติหน้าที่ด้านการบริกรข้อมูล (Data Steward) เพื่อดำเนินการอย่างน้อยในเรื่องดังต่อไปนี้

๑) สนับสนุนให้เกิดการกำกับดูแลข้อมูล และบริหารจัดการข้อมูลภายในองค์กร โดยรับคำสั่งโดยตรงจากคณะกรรมการชุดย่อยที่ปฏิบัติหน้าที่ในการกำกับดูแลข้อมูลและบริหารจัดการข้อมูลเพื่อสร้างความมั่นใจว่าการบริหารจัดการข้อมูลสอดคล้องกับนโยบาย และระเบียบวิธีปฏิบัติขององค์กร

๒) กำหนดให้มีหัวหน้าบริการข้อมูล (Lead Data Steward) โดยควรเป็นหนึ่งในคณะกรรมการชุดย่อยที่ปฏิบัติหน้าที่ในการกำกับดูแลข้อมูลและบริหารจัดการข้อมูล

แนวปฏิบัติ เรื่องการกำกับดูแลข้อมูล (Data Governance Guideline) ๗ กลุ่มงานมาตรฐานธรรมาภิบาลและการดำเนินธุรกิจ สายพัฒนามาตรฐานการกำกับ

๓) กำหนดให้มีบุคลากรที่บริการข้อมูลด้านธุรกิจ (Business Data Steward) ปฏิบัติหน้าที่ รับผิดชอบในการนิยามคุณลักษณะข้อมูลที่มีคุณภาพรวมถึงนิยามของคำอธิบายชุดข้อมูล (Metadata) ที่สำคัญภายในองค์กร ทั้งนี้ บริกรข้อมูลด้านธุรกิจควรประกอบด้วยบุคลากร จากหลายหน่วยงานที่มีชุดข้อมูลที่สำคัญของ อ.ต.ก. เพื่อสามารถนิยามข้อมูลที่มีคุณภาพ และคำอธิบายชุดข้อมูลได้อย่างชัดเจนที่สุด

๔) กำหนดให้มีบุคลากรที่บริการข้อมูลด้านเทคนิค (Technical Data Steward) ปฏิบัติหน้าที่ให้การสนับสนุนด้านเทคโนโลยีสารสนเทศ รวมถึงข้อเสนอแนะเชิงเทคนิคแก่บริกรข้อมูลด้านธุรกิจ เช่น การนิยาม คำอธิบายชุดข้อมูลเชิงเทคนิค (Technical Metadata) ทั้งนี้ บริกรข้อมูลด้านเทคนิคควรมาจากกองเทคโนโลยีสารสนเทศขององค์กร

• อ.ต.ก. ควรกำหนดบุคลากรหรือหน่วยงานที่เป็นเจ้าของข้อมูล (Data Owners) เพื่อดำเนินการอย่างน้อยในเรื่องดังต่อไปนี้

๑) กำหนดให้มีบุคลากรหรือหน่วยงานที่เป็นเจ้าของข้อมูลซึ่งปฏิบัติหน้าที่รับผิดชอบดูแลชุดข้อมูลโดยตรงในแต่ละชุดข้อมูลที่สำคัญ โดยทั่วไปควรเป็นผู้บริหารจากหน่วยงานที่ รับผิดชอบชุดข้อมูลที่สำคัญภายในองค์กร

๒) ปฏิบัติหน้าที่ทบทวนและอนุมัติการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับข้อมูลที่รับผิดชอบดูแลอยู่รวมถึงให้สิทธิในการเข้าถึงข้อมูลและจัดชั้นความลับของข้อมูล

• อ.ต.ก. ควรจัดให้มีคณะทำงานที่ปฏิบัติหน้าที่บริหารจัดการข้อมูล (Data Management Team) เพื่อดำเนินการอย่างน้อยในเรื่องดังต่อไปนี้

๑) ปฏิบัติหน้าที่สนับสนุนการดำเนินการบริหารจัดการข้อมูลในด้านเทคโนโลยีสารสนเทศ เช่น การจัดทำสถาปัตยกรรมข้อมูล การจัดการฐานข้อมูล การวิเคราะห์ข้อมูล การตรวจสอบคุณภาพข้อมูล รวมถึงการดำเนินการอื่นที่สนับสนุนให้กิจกรรมที่ใช้ข้อมูลภายในองค์กรมีประสิทธิภาพมากยิ่งขึ้น

๑.๑.๒.๒ การบริหารความเสี่ยงด้านข้อมูล

ติดตามและบริหารจัดการความเสี่ยงด้านข้อมูลตลอดวงจรชีวิตให้เหมาะสมและ เป็นไปตามแนวทางการบริหารจัดการความเสี่ยงขององค์กร เพื่อหลีกเลี่ยงโอกาสเกิดความเสี่ยงที่อาจส่งผลกระทบต่อการดำเนินงานขององค์กรโดย มีการดำเนินการดังต่อไปนี้

• จัดทำกรอบและกระบวนการบริหารความเสี่ยงขององค์กรให้ครอบคลุมความเสี่ยงด้านข้อมูลรวมทั้งสนับสนุนให้หน่วยงานต่าง ๆ ให้มีการประเมินความเสี่ยงด้านข้อมูล

• หน่วยงานกลางที่มีหน้าที่ในการกำกับดูแลและมีความเข้าใจในการบริหารจัดการข้อมูลดำเนินการให้คำปรึกษา ติดตาม และทบทวนความเสี่ยงด้านข้อมูลให้อยู่ในระดับที่ยอมรับได้ รวมทั้งรวบรวม และเชื่อมโยงความเสี่ยงด้านข้อมูลกับความเสี่ยงด้านอื่นขององค์กร และนำเสนอผลการบริหารจัดการความเสี่ยงต่อคณะกรรมการที่เกี่ยวข้อง และผู้บริหารองค์กร

๑.๑.๒.๓ การกำกับการปฏิบัติตามกฎหมายและหลักเกณฑ์เกี่ยวข้องกับข้อมูล

องค์กรควรรักษาความมั่นคงปลอดภัยของข้อมูลและการรักษาความเป็นส่วนบุคคล ของข้อมูลตลอด วงจรชีวิตให้สอดคล้องกับระดับความเสี่ยงของข้อมูล ให้เป็นไปตามกฎเกณฑ์และกฎหมายที่เกี่ยวข้อง โดยดำเนินการกำกับดูแลให้เป็นไปตามกฎหมายและหลักเกณฑ์เกี่ยวข้องกับข้อมูลดังต่อไปนี้

• มีการรักษาความมั่นคงปลอดภัยของข้อมูลที่ครอบคลุมการรับส่งข้อมูลผ่านเครือข่ายการสื่อสาร การจัดเก็บหรือใช้ข้อมูลบนระบบงานและสื่อบันทึกข้อมูลต่าง ๆ การเก็บรักษา และการทำลายข้อมูล รวมถึงกรณีที่องค์กรมีการใช้บริการการเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอกให้สอดคล้องกับระดับความเสี่ยงของข้อมูล ทั้งนี้องค์กรสามารถอ้างถึงแนวทางการรักษาความมั่นคงปลอดภัย ร่างนโยบายที่เกี่ยวข้องต่อการบริหารจัดการธรรมาภิบาลข้อมูลว่าด้วยหลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ขององค์กร รวมถึงแนวปฏิบัติอื่นที่เกี่ยวข้อง

• มีการรักษาความเป็นส่วนบุคคลของข้อมูล ให้สอดคล้องกับกฎเกณฑ์และกฎหมายที่เกี่ยวข้อง เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ โดยต้องมีการเก็บ รวบรวม ใช้งาน หรือเปิดเผยข้อมูลส่วนบุคคลเท่าที่จำเป็น ภายใต้วัตถุประสงค์ที่กำหนดไว้ และคำนึงถึงสิทธิของเจ้าของข้อมูล

• มีการดูแลข้อมูลของผู้ใช้บริการให้เป็นไปตามมาตรฐานขั้นตอนสำหรับการดูแลข้อมูลของผู้ใช้บริการตามที่กำหนดในคู่มือบริหารจัดการข้อมูล

๑.๑.๒.๔ การตรวจสอบการปฏิบัติงานที่เกี่ยวข้องกับข้อมูล

องค์กรควรเตรียมความพร้อมในการบริหารจัดการประเด็นปัญหาด้านข้อมูลเพื่อป้องกันไม่ให้เกิดเหตุการณ์ที่อำนาจไปสู่ความเสียหาย หรือเพื่อลดผลกระทบกรณีมีความเสียหายเกิดขึ้นแล้ว

• มีกระบวนการติดตามและบริหารจัดการประเด็นปัญหาด้านข้อมูล ทั้งการตรวจจับการระบุการยับยั้งปัญหา การวิเคราะห์หาสาเหตุ การรวบรวมหลักฐานหรือเอกสาร การแก้ไขปัญหาการบริหารจัดการให้สามารถกลับมาดำเนินธุรกิจได้ตามปกติ รวมถึง การปรับปรุงกระบวนการควบคุม เพื่อลดโอกาสที่จะเกิดปัญหาที่คล้ายกันในอนาคต ในกรณีที่ประเด็นปัญหาที่เกิดขึ้นส่งผลกระทบต่อ

• ตรวจสอบการปฏิบัติงานและการบริหารความเสี่ยงที่เกี่ยวข้องกับข้อมูล เพื่อสอบทานให้มั่นใจว่าเป็นไปตามนโยบาย มาตรฐาน และระเบียบวิธีปฏิบัติที่เกี่ยวข้องกับการกำกับดูแลข้อมูล

๑.๒ นโยบายการกำกับดูแลข้อมูล

การกำหนดนโยบายข้อมูลจัดเป็นหนึ่งในองค์ประกอบตามกรอบการธรรมาภิบาลข้อมูลภาครัฐ เพื่อให้การบริหารจัดข้อมูลของ อ.ต.ก. เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีคุณภาพ มีความมั่นคงปลอดภัย รวมทั้งการป้องกันภัยคุกคามหรือปัญหาที่อาจจะเกิดขึ้นจากการบริหารจัดการและการใช้ข้อมูล และสอดคล้องตามกรอบธรรมาภิบาลข้อมูลภาครัฐ จึงต้องมีการกำหนดให้มีแนวนโยบายการกำกับดูแลข้อมูล

๑.๒.๑ โดเมนข้อมูล และโดเมนย่อยของข้อมูล

ในส่วนนี้เป็นการสรุปแนวคิดของโดเมนข้อมูลและโดเมนย่อยของข้อมูลเมื่อรวมกันแล้ว Data Domains และ Data Subdomains จะเป็นหน่วยงานกำกับดูแลข้อมูลใน อ.ต.ก.

๑.๒.๒ ประเภทของโดเมนข้อมูล

โดเมนข้อมูลหมายถึงชุดข้อมูลที่ครอบคลุมแขนงของข้อมูลทั้งหมด (เช่น ข้อมูลพนักงาน) มีการกำหนดขอบเขตของโดเมนข้อมูลเพื่อให้แน่ใจว่าไม่มีข้อมูลที่ไม่มีการอ้างสิทธิ์หรือทับซ้อนกันระหว่างโดเมนข้อมูลสองโดเมน โดเมนข้อมูลได้รับการจัดการโดย บริกรข้อมูล (Data Stewards) ซึ่งมีบทบาทและความรับผิดชอบอธิบายไว้ในส่วนถัดไป เมื่อข้อมูลสำหรับแขนง ข้อมูลหนึ่งมีการกระจายการดำเนินงานระหว่างธุรกิจหลายแห่ง โดเมนย่อยของข้อมูลเหล่านี้จะจัดแนวเป็นโดเมนข้อมูลเดียว

อ.ต.ก. จะมีรูปแบบการดำเนินงานแบบรวมศูนย์ซึ่งมีความสมดุลระหว่างส่วนกลาง การควบคุมทั่วทั้งกลุ่ม และหน่วยงานระดับโดเมนข้อมูลหรือโดเมนย่อยข้อมูล (เช่น บริกรข้อมูล) สำหรับการกำกับดูแลข้อมูล โมเดลการดำเนินงานแบบรวมศูนย์ให้ประโยชน์ในด้านขนาดและความสม่ำเสมอจากการรวมศูนย์ในขณะที่ช่วยให้ธุรกิจมีความยืดหยุ่นในการตอบสนองความต้องการด้านการกำกับดูแลข้อมูลเฉพาะของตน

รูปแบบการดำเนินงานแบบรวมศูนย์ต้องการบทบาททั้งในสำนักงานกลางที่สอดคล้องกับหัวหน้าฝ่ายจัดการข้อมูลและในธุรกิจ (เช่น บริกรข้อมูล) เพื่อนำมาตรฐานทั่วไปไปใช้ใน อ.ต.ก. อย่างมีประสิทธิภาพ และรับประกันคุณภาพและความสอดคล้องของข้อมูล ด้วยเหตุนี้ โดเมนข้อมูลและโดเมนย่อยของข้อมูลจึงเป็นรากฐานที่สำคัญของรูปแบบการดำเนินงานแบบรวมศูนย์

อ.ต.ก. จะมีโดเมนข้อมูล ๔ ประเภท ได้แก่

๑) โดเมนข้อมูลธุรกรรม (Transactional Data Domains): โดเมนข้อมูลเหล่านี้ประกอบด้วยข้อมูลที่สร้างขึ้นโดยแอปพลิเคชั่นที่จัดการกระบวนการทางธุรกิจ เช่นเดียวกับข้อมูลการดำเนินงานที่ข้อมูลถูกเก็บไว้ชั่วคราว หรือถาวร (เช่น ธุรกรรมบัตรเครดิต) ซึ่งข้อมูลที่ลูกค้าพบส่วนใหญ่เป็นข้อมูลธุรกรรม

๒) โดเมนข้อมูลอ้างอิง (Reference Data Domains): โดเมนข้อมูลเหล่านี้ประกอบด้วยข้อมูลทั้งองค์กรที่ค่อนข้างคงที่เมื่อเวลาผ่านไป และจำเป็นสำหรับสายธุรกิจหลายสาย (เช่น ข้อมูลลูกค้า ข้อมูลผลิตภัณฑ์) ข้อมูลส่วนใหญ่มีการแลกเปลี่ยนกับบุคคลที่สามสอดคล้องกับข้อมูลอ้างถึง

๓) โดเมนข้อมูลที่ได้รับมา (Derived Data Domains): โดเมนข้อมูลเหล่านี้ประกอบด้วยข้อมูลที่ได้รับการจัดการ และรวบรวมตามธุรกรรมและข้อมูลอ้างอิงเพื่อตอบคำถามเฉพาะ โดยทั่วไปจะรวมถึงการวิเคราะห์รายงานความเสี่ยง และกิจกรรมการประมวลผลข้อมูลที่คล้ายคลึงกัน

๔) โดเมนข้อมูลที่ค้นพบ (Discovered Data Domains): โดเมนข้อมูลเหล่านี้ประกอบด้วยข้อมูลที่ได้รับการจัดการและรวบรวมตามธุรกรรมและข้อมูลอ้างอิงเพื่อค้นหาข้อมูลเชิงลึกที่ไม่รู้จักมาก่อน โดยทั่วไปจะรวมถึงการวิเคราะห์ การทดสอบผลิตภัณฑ์ และกิจกรรมการค้นหาข้อมูลที่คล้ายคลึงกัน

๑.๒.๓ บทบาทหน้าที่ และความรับผิดชอบ

ส่วนนี้อธิบายถึงบทบาทและความรับผิดชอบหลักในการดำเนินการตามนโยบายและมาตรฐานสนับสนุนทั่วทั้ง อ.ต.ก. บทบาทการกำกับดูแลข้อมูลที่กำหนดซึ่งกำหนดไว้ในนโยบายนั้นมีอำนาจโดยคณะกรรมการบริหารองค์การตลาดเพื่อเกษตรกร เพื่อใช้และดำเนินการตามวิจารณญาณของตนเองเพื่อปฏิบัติตามความรับผิดชอบที่กำหนดไว้ในเอกสารนี้

๑.๒.๔ บทบาทระดับโดเมนข้อมูลและระดับโดเมนย่อยของข้อมูล

โดเมนข้อมูลและโดเมนย่อยของข้อมูลประกอบด้วยกลุ่มอิสระที่สร้างและจัดการข้อมูล และมีโอกาสแรกในการระบุความเสี่ยงระหว่างกิจกรรมทางธุรกิจในแต่ละวัน พนักงานที่ได้รับมอบหมายบทบาทเหล่านี้จะต้องมีวุฒิภาวะและความอาวุโสในการดำเนินการตามคำสั่งในนโยบายและมาตรฐานสนับสนุนอย่างมีประสิทธิภาพ ควรสร้างบทบาทการกำกับดูแลข้อมูล ต่อไปนี้สำหรับแต่ละโดเมนข้อมูลและโดเมนย่อยข้อมูลใน อ.ต.ก.

• เจ้าของข้อมูล (Data Owner): กรรมการหรือผู้จัดการที่เป็นเจ้าของการกำกับดูแลข้อมูลในโดเมนข้อมูลหรือ โดเมนย่อยของข้อมูล ความรับผิดชอบรวมถึง

- กำหนดกลยุทธ์ข้อมูล ลำดับความสำคัญ และเป้าหมายสำหรับข้อมูลภายในโดเมนข้อมูลหรือโดเมนย่อยข้อมูล
- สนับสนุนและอนุญาตการเริ่มข้อมูลใหม่ภายในขอบเขตของโดเมนข้อมูลหรือโดเมนย่อยข้อมูล
- ทำงานร่วมกับหัวหน้าฝ่ายการจัดการข้อมูลในการพัฒนาความคิดริเริ่มระดับโดเมนข้อมูลหรือโดเมนย่อยของข้อมูลในระดับกลุ่มที่ต้องการการลงทุนจำนวนมาก
- ทำหน้าที่เป็นบุคคลติดต่อในการยกระดับสำหรับปัญหาโดเมนข้อมูลหรือโดเมนย่อยข้อมูล

• บริกรข้อมูล (Data Steward), ผู้เชี่ยวชาญเฉพาะเรื่องของข้อมูลในโดเมนข้อมูลหรือโดเมนย่อยข้อมูล ซึ่งมีหน้าที่รับผิดชอบในการรับรองว่าข้อมูลได้รับการจัดการตามนโยบายและมาตรฐานที่สนับสนุนความรับผิดชอบรวมถึง :

- แปลกลยุทธ์ข้อมูลสำหรับโดเมนข้อมูลหรือโดเมนย่อยข้อมูลเป็นความคิดริเริ่มที่ดำเนินการได้
- พัฒนากรณีธุรกิจโดยละเอียดสำหรับกรณีการใช้งานที่เสนอ

- จัดการการควบคุมการเข้าถึง ตรวจสอบการกระจายของข้อมูล อนุมัติการจัดเตรียมข้อมูลให้กับผู้ใช้ที่ ได้รับอนุญาต และสนับสนุนผู้ใช้ที่ได้รับอนุญาตในฐานะผู้เชี่ยวชาญเฉพาะเรื่องสำหรับข้อมูลในโดเมน ข้อมูลหรือโดเมนย่อยข้อมูล

- ทำงานร่วมกับหัวหน้าฝ่ายจัดการข้อมูลเพื่อใช้กรอบงานและจัดประเภทข้อมูลตามผลกระทบ

- กำหนดแหล่งที่มาอย่างเป็นทางการของข้อมูล ตรวจสอบสายข้อมูล และจัดการข้อมูลเมทาดาตา

- กำหนดกฎทางธุรกิจที่เกี่ยวข้องกับการวัดและเมตริกคุณภาพของข้อมูล

- อนุมัติและจัดลำดับความสำคัญของแผนการแก้ไขคุณภาพข้อมูล

• บริกรแพลตฟอร์ม (Platform Steward) : รับผิดชอบในการพัฒนาหรือจัดการระบบประมวลผลข้อมูลและ โครงสร้างพื้นฐานที่สนับสนุนการกำกับดูแลข้อมูล ความรับผิดชอบรวมถึง

- ดำเนินการความคิดริเริ่มด้านข้อมูลใหม่และให้ข้อมูลตามเวลาและประมาณการค่าใช้จ่าย

- กำหนดและใช้การควบคุมทางเทคนิค และพัฒนาหลักฐานการปฏิบัติตามนโยบายและมาตรฐานสนับสนุน

- ใช้การควบคุมการเข้าถึงเพื่อให้ข้อมูลแก่พนักงานหรือระบบที่ได้รับอนุญาต การติดตามและควบคุมการเคลื่อนย้ายข้อมูล และทำให้มั่นใจว่ามีการแบ่งปันข้อมูลจากแหล่งข้อมูลที่เป็นทางการอย่างมีประสิทธิภาพ

- รักษาแบบจำลองข้อมูลเชิงตรรกะและกำหนดสายเลือดทางเทคนิค

- ตรวจสอบให้แน่ใจว่าข้อมูลได้รับการจัดเตรียมในระบบบันทึกที่เหมาะสม

- แปลกฎทางธุรกิจเป็นกฎคุณภาพข้อมูลและสร้างการควบคุมคุณภาพข้อมูล

- วิเคราะห์ต้นตอของปัญหาคุณภาพของข้อมูล และออกแบบและดำเนินกิจกรรมการแก้ไขโดยร่วมมือกับหัวหน้าฝ่ายจัดการข้อมูล

๑.๒.๕ บทบาทระดับองค์กร

หัวหน้าฝ่ายจัดการข้อมูลมีโอกาสครั้งที่สองในการระบุความเสี่ยงและรับผิดชอบในการกำกับดูแลที่เป็นอิสระ บทบาท ระดับกลุ่มจากส่วนกลางประกอบด้วย

๑) หัวหน้าฝ่ายการจัดการข้อมูล : รับผิดชอบในการกำกับดูแลข้อมูลทั้งองค์กร และกลยุทธ์

๒) หัวหน้าฝ่ายกำกับดูแลข้อมูล : สร้างและรักษานโยบายและมาตรฐานสนับสนุน จัดลำดับความสำคัญของความคิดเริ่มด้านข้อมูลทั่วทั้งกลุ่ม และกำหนดวาระสำหรับการประชุมคณะกรรมการด้านข้อมูลที่เกี่ยวข้อง

๓) ผู้นำด้านคุณภาพข้อมูล : ตรวจสอบและนำมาตรฐานคุณภาพข้อมูล มาตรการ และเมตริกไปใช้ในโดเมนข้อมูล และโดเมนย่อยข้อมูล ติดตามแผนการแก้ไขคุณภาพข้อมูล

๔) ผู้นำด้านเมทาดาตา : ให้การกำกับดูแลแหล่งข้อมูลที่เป็นทองและจัดการการเลือกองค์ประกอบข้อมูลทางเทคนิคเพื่อเปิดใช้งานสายข้อมูล

๕) ผู้นำด้านสถาปัตยกรรมข้อมูล : กำหนดสถาปัตยกรรมข้อมูลและออกแบบความคิดริเริ่มด้านข้อมูลใหม่ร่วมกับ ทีมสถาปัตยกรรมด้านเทคโนโลยีสารสนเทศ และทีมกำหนดกลยุทธ์ขององค์กร

๑.๒.๖ ความรับผิดชอบของคณะกรรมการ

คณะกรรมการ ๓ ระดับจะมีส่วนร่วมในการกำกับดูแลข้อมูล อ.ต.ก.

• คณะกรรมการบริหารองค์การตลาดเพื่อเกษตรกร : กำหนดกลยุทธ์การกำกับดูแลข้อมูลสำหรับ อ.ต.ก.นอกจากนี้ยังอนุมัติและประสานงานกิจกรรมการกำกับดูแลข้อมูลทั่วทั้งกลุ่มและทำหน้าที่เป็นผู้ประเมินเมื่อปัญหามีการยกระดับความรับผิดชอบรวมถึง :

- อนุมัติกลยุทธ์ด้านข้อมูลและแผนงานของ อ.ต.ก. เพื่อให้สอดคล้องกับกลยุทธ์ทางธุรกิจ
- อนุมัตินโยบายและมาตรฐานสนับสนุน
- อนุมัติความคิดริเริ่มที่เกี่ยวข้องกับข้อมูลที่สำคัญ
- ติดตามและตรวจสอบความคืบหน้ากับความคิดริเริ่มด้านการกำกับดูแลข้อมูลที่สำคัญ
- ตรวจสอบคุณภาพข้อมูลระดับสูงและมาตรวัดและตัวบ่งชี้การกำกับดูแลข้อมูล

• คณะกรรมการควบคุมการกำกับดูแลข้อมูล : หัวหน้าฝ่ายการจัดการข้อมูลเป็นประธานและตรวจสอบ อนุมัติประเด็นการกำกับดูแลข้อมูลและการแก้ปัญหาตามลำดับ ความรับผิดชอบรวมถึง :

- ทบทวนและสรุปนโยบายและมาตรฐานสนับสนุน
- กำหนดโดเมนข้อมูล โดเมนย่อยข้อมูล และขอบเขต
- ทำหน้าที่เป็นผู้ตัดสินใจในการยกระดับสำหรับปัญหาที่เจ้าของข้อมูล บริกรข้อมูลแพลตฟอร์ม ไม่ได้รับการแก้ไข
- ตรวจสอบและอนุมัติมาตรวัดคุณภาพข้อมูลและมาตรวัด
- ตรวจสอบปัญหาคุณภาพของข้อมูลและบริกร

• คณะทำงาน : ประกอบด้วยหน่วยงานกำกับดูแลตามหน้าที่ (เช่น การปกป้องข้อมูล คุณภาพของข้อมูล) โดยมี ส่วนร่วมจากเจ้าของข้อมูล บวกข้อมูล และบริกรแพลตฟอร์ม ประชุมกันเพื่อตอบสนองความต้องการใน การดำเนินงานเฉพาะ ความรับผิดชอบรวมถึง :

- พัฒนาแผนการแก้ไขสำหรับปัญหาการกำกับดูแลข้อมูล (เช่น คุณภาพของข้อมูล)
- ข้อมูลเมทาของเอกสาร (เช่น การตรวจสอบย้อนกลับ)
- พัฒนากรณีธุรกิจสำหรับการได้มาซึ่งข้อมูลจากบุคคลที่สาม
- ตรวจสอบและอนุมัติคำขอแบ่งปันข้อมูลที่เป็นความลับ

๑.๒.๗ นโยบาย

<u>ภาพรวมของนโยบาย</u>

นโยบายกำหนดให้ปฏิบัติตามกฎระเบียบที่เกี่ยวข้องทั้งหมด ปัจจัยอื่นๆ เช่น ภาวะผูกพันตามสัญญา อาจต้องใช้ข้อกำหนดทางธุรกิจที่เข้มงวดมากขึ้นบริกรข้อมูลต้องระบุระบบการประมวลผลข้อมูลและกระบวนการที่ต้องการการควบคุมที่เข้มงวดมากขึ้น และปฏิบัติตามข้อกำหนดทางกฎหมายหรือข้อบังคับของธุรกิจเฉพาะเหล่านี้ ความคาดหวังทางกฎหมายหรือ ข้อบังคับใด ๆ ที่กำหนดและจัดทำเป็นเอกสารโดยกฎหมายซึ่งแตกต่างจากนโยบายและมาตรฐานสนับสนุนจะมีผลเหนือกว่า

<u>การธรรมาภิบาลข้อมูล</u>

ต้องกำหนดเจ้าของข้อมูล บริการข้อมูลและ บริกรแพลตฟอร์ม สำหรับแต่ละโดเมนข้อมูลและโดเมนย่อยของข้อมูล เจ้าของข้อมูลต้องเป็นกรรมการหรือสูงกว่า และต้องรับผิดชอบในการจัดทำโปรแกรมการกำกับดูแลข้อมูลเพื่อให้มั่นใจว่าเป็นไป ตามนโยบายและมาตรฐานสนับสนุน เจ้าของข้อมูลมีความรับผิดชอบสูงสุดต่อการปฏิบัติตามโดเมนข้อมูลและโดเมนย่อยข้อมูล ของตน เจ้าของข้อมูลต้อง :

• สร้างโครงสร้างโปรแกรมการกำกับดูแลข้อมูลที่ยั่งยืนและรูปแบบการดำเนินงานสำหรับโดเมนข้อมูลและโดเมนย่อยของข้อมูล

• กำหนด บริกรข้อมูล ซึ่งเป็นผู้เชี่ยวชาญเฉพาะเรื่องของข้อมูลในโดเมนข้อมูล หรือโดเมนย่อยของข้อมูล และเป็นผู้รับผิดชอบในการรับรองว่าข้อมูลได้รับการจัดการตามนโยบายและมาตรฐานสนับสนุน

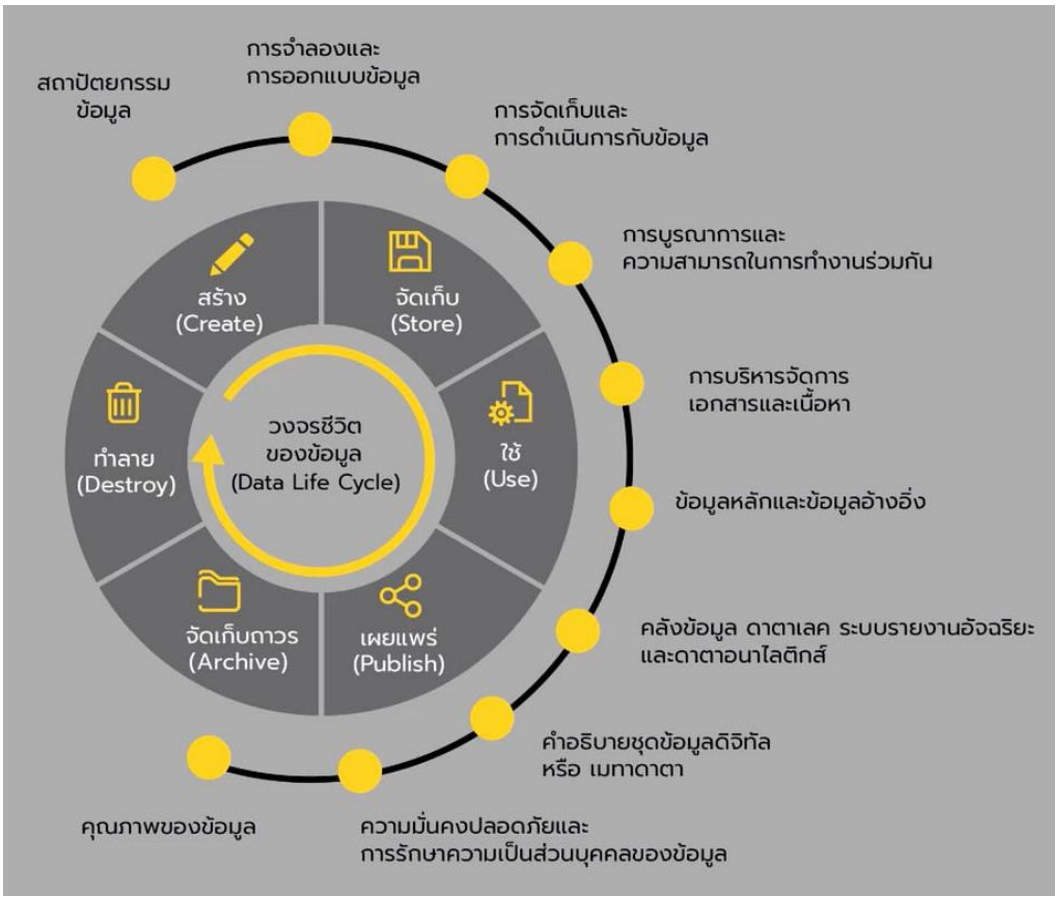
• ตรวจสอบให้แน่ใจว่าได้มอบหมาย ผู้นำด้านคุณภาพข้อมูล จาก หัวหน้าฝ่ายการจัดการข้อมูล และรับผิดชอบในการวัดคุณภาพข้อมูล แก้ไขปัญหา และดำเนินกิจกรรมการดำเนินงานเพื่อรักษาข้อมูลในโดเมนข้อมูล หรือ โดเมนย่อยของข้อมูล

• ตรวจสอบให้แน่ใจว่า บริกรแพลตฟอร์ม ได้รับมอบหมายให้เป็นผู้รับผิดชอบในการพัฒนาหรือดูแลระบบการประมวลผลข้อมูลและโครงสร้างพื้นฐาน

บทที่ ๒
การบริหารจัดการข้อมูล (Data Management)

๒.๑ วงจรชีวิตของข้อมูล (Data Life Cycle)

วงจรชีวิตของข้อมูล หรือที่เรียกว่า “Data Life Cycle” หมายถึงช่วงเวลาทั้งหมดที่มีข้อมูลอยู่ในระบบขององค์กร ซึ่งวงจรชีวิตนี้จะครอบคลุมทุกขั้นตอนที่ข้อมูลของคุณต้องผ่าน ตั้งแต่การสร้างข้อมูลไปจนถึงทำลายข้อมูล ในวิชาวิทยาศาสตร์ สิ่งมีชีวิตทุกชนิดจะต้องผ่านช่วงต่างๆ ได้แก่ วัยทารก ช่วงเวลาของการเติบโต และการพัฒนา วัยเจริญพันธุ์ที่มีประสิทธิผล และ วัยชรา ซึ่งขั้นตอนเหล่านี้แตกต่างกันไป เช่น ปลาแซลมอนจะตายทันทีหลังจากวางไข่ ในขณะที่มนุษย์มีชีวิตอยู่จนเป็นปู่ย่าตายาย แม้ว่าสิ่งมีชีวิตจะอาศัยอยู่ในสภาพแวดล้อมเดียวกัน แต่ต่างก็มีวงจรชีวิตที่ไม่เหมือนกัน



วงจรชีวิตของข้อมูล (Data Life Cycle)

ในทำนองเดียวกันข้อมูล หรือ Data ก็จะผ่านช่วงเวลาต่าง ๆ ของชีวิตตามจังหวะของมันเอง ซึ่งโดยทั่วไปแล้ววงจรชีวิตข้อมูล หรือ data life cycle จะแบ่งออกได้เป็น ๖ ขั้นตอนดังนี้

๒.๒.๑ สร้างข้อมูล (Create)

ในการเริ่มต้นของวงจรชีวิตข้อมูล หรือ data life cycle ขั้นตอนลำดับแรกต้องเป็นการสร้างข้อมูล ถ้าไม่มีขั้นตอนนี้ก็ จะไม่มีขั้นตอนอื่น ๆ ตามมา ทุกวันนี้ทั่วทั้งโลกมีการสร้างข้อมูลกว่า ๒.๕ quintillion bytes หรือ ๒,๕๐๐ ล้าน GB ต่อวัน หรือ ถ้าจะอธิบายให้เห็นภาพคือ “เราแต่ละคนผลิตข้อมูลกันเฉลี่ยวินาทีละ ๑.๗ MB เลยทีเดียว และมีการประมาณการอีกด้วย ว่า ในปี ๒๐๒๕ เราอาจผลิตข้อมูลเพิ่มขึ้นเป็นคนละ ๔๕๓ Exabytes ต่อวัน โดยข้อมูลเหล่านี้ส่วนใหญ่ก็มาจากการใช้งานอินเตอร์เน็ตและอุปกรณ์ต่างๆ ข้อมูล Big data จากหลายๆองค์กร, อุปกรณ์ lot และข้อมูล transaction ต่างๆในสกุล เงินดิจิตอล ที่มีแนวโน้มเพิ่มขึ้นเรื่อย ๆ อย่างไม่มีที่สิ้นสุด

๒.๒.๒ จัดเก็บข้อมูล (Store)

หลังจากที่มีการสร้างข้อมูลแล้ว ขั้นตอนถัดไปของวงจรชีวิตข้อมูล หรือ data life cycle คือการจัดเก็บข้อมูล (Store) เพื่อให้มีระเบียบ ง่ายต่อการใช้งาน ไม่สูญหาย หรือถูกทำลาย และให้ผู้ใช้งานสามารถประมวลผลข้อมูลต่าง ๆ ตาม ความต้องการได้อย่างรวดเร็ว

ซึ่งเราสามารถจัดเก็บข้อมูลได้โดยสร้างฐานข้อมูล (databases) หรือชุดข้อมูล (datasets) จากนั้นชุดข้อมูลเหล่านี้ อาจจะถูกจัดเก็บไว้ในระบบคลาวด์ บนเซิร์ฟเวอร์ หรือใช้อุปกรณ์จัดเก็บข้อมูลทางกายภาพรูปแบบอื่น เช่น ฮาร์ดไดรฟ์ ซีดี เทป คาสเซ็ตต์ หรือฟลอปปีดิสก์ โดยวิธีการจัดเก็บข้อมูลที่ดีที่สุดจะพิจารณาตามการใช้งานและบริบทของแต่ละองค์กร

๒.๒.๓ ใช้ข้อมูล (Use)

การใช้ข้อมูล (Use) ในวงจรชีวิตข้อมูล หรือ data life cycle เป็นการนำข้อมูลที่จัดเก็บมาประมวลผล เช่น การถ่าย โอนข้อมูล การเปลี่ยนรูปแบบการจัดเก็บข้อมูล การวิเคราะห์ข้อมูล การจัดทำรายงาน เพื่อนำข้อมูลเหล่านั้นมาใช้งานให้เกิดประโยชน์ตามวัตถุประสงค์และสนับสนุนกิจกรรมขององค์กร รวมถึงการสำรอง (Backup) ข้อมูล โดยการคัดลอกข้อมูลที่ใช้งานอยู่ในปัจจุบัน เพื่อทำสำเนา เช่น ใช้โปรแกรมในการสำรองข้อมูล เป็นการหลีกเลี่ยงความเสียหายที่จะเกิดขึ้นหากข้อมูลเกิดการเสียหายหรือสูญหาย ซึ่งสามารถนำข้อมูลที่สำรองไว้ในสื่อบันทึกข้อมูลกลับมาใช้งานได้ทันที โดยการกู้คืน (Restore)

๒.๒.๔ เผยแพร่ข้อมูล (Publish)

ขั้นตอนเผยแพร่ข้อมูลในวงจรชีวิตข้อมูล หรือ data life cycle นี้ จะเป็นการแชร์ข้อมูล (Sharing) การกระจายข้อมูล (Dissemination) การควบคุมการเข้าถึง (Access Control) การแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน (Exchange) และการกำหนดเงื่อนไขในการนำข้อมูลไปใช้ (Condition) เพื่อที่ข้อมูลเหล่านี้จะถูกเปลี่ยนไปเป็นกิจกรรมและการตัดสินใจขององค์กร ซึ่งจะเป็นการเพิ่มคุณค่าสูงสุดให้กับข้อมูลนั้น ๆ

๒.๒.๕ จัดเก็บข้อมูลถาวร (Archive)

หลังจากที่ข้อมูลได้ถูกใช้ และเผยแพร่แล้ว ข้อมูลนั้นๆจะเข้าสู่ขั้นตอน จัดเก็บข้อมูลถาวรในวงจรชีวิตข้อมูล หรือ data life cycle ซึ่งจะเป็นการคัดลอกเอาข้อมูลที่มีช่วงอายุเป็นช่วงใช้งาน หรือไม่ได้ใช้งานแล้วมาทำสำเนาสำหรับการเก็บรักษา โดยที่ข้อมูลนั้นไม่มีการลบ ปรับปรุง หรือแก้ไขอีก และสามารถนำกลับไปใช้งานได้ใหม่เมื่อต้องการ

๒.๒.๖ ทำลายข้อมูล (Destroy)

เมื่อข้อมูลในกระบวนการจัดเก็บข้อมูลถาวรมีปริมาณเพิ่มขึ้นมาก จนไม่สามารถจัดเก็บไว้ได้ เนื่องจากปัญหา หรือจัดเก็บถาวรเป็นระยะเวลานานหรือเกินกว่าระยะเวลาที่กำหนด ข้อมูลเหล่านั้นจะเข้าสู่ด้านต้นทุนในการจัดเก็บข้อมูลขั้นตอนทำลายข้อมูล ในวงจรชีวิตข้อมูล หรือ data life cycle

ความท้าทายของวงจรชีวิตข้อมูลระยะนี้ก็คือ การทำให้แน่ใจว่า ข้อมูลถูกทำลายอย่างเหมาะสม สิ่งสำคัญคือต้องตรวจสอบให้แน่ใจ ก่อนที่จะทำลายข้อมูลว่ารายการข้อมูลนั้นเป็นระยะเวลาการเก็บรักษาตามข้อบังคับที่กำหนดหรือไม่

๒.๒ การบริหารจัดการค่าอธิบายชุดข้อมูล (Metadata Management)

เมทาดาตา คือข้อมูลที่อธิบายข้อมูล (เช่น ข้อมูลเกี่ยวกับข้อมูล) และรวมถึงลักษณะต่างๆ เช่น คำจำกัดความ เจ้าของ แหล่งข้อมูลที่เป็นทางการ เชื้อสายของข้อมูล และมาตรวัดและเมตริกคุณภาพของข้อมูล ข้อมูลเมทาเป็นสิ่งสำคัญสำหรับพนักงานในการทำความเข้าใจข้อมูลและรายงานที่พวกเขาใช้ขจัดความกำกวม และทำให้สามารถกระทบยอดผลการรายงานได้ นอกจากนี้ยังเป็นสิ่งสำคัญสำหรับวิศวกรที่สนับสนุนระบบการประมวลผลข้อมูลและโครงสร้างพื้นฐานการจัดการข้อมูลเมทา เป็นวิธีปฏิบัติในการรวบรวมและ

กำหนดมาตรฐานข้อมูลในพจนานุกรมข้อมูลกลุ่ม ผู้นำด้านเมทาดาตา ซึ่งเป็นตัวแทนของหัวหน้าฝ่ายจัดการข้อมูล จะต้อง :

• กำหนดมาตรฐานสำหรับข้อมูลเมทาตามแนวทางปฏิบัติที่ดีที่สุดระหว่างประเทศ และรับรองว่าสอดคล้องกับมาตรฐานเหล่านี้

• คิดค้นและแก้ไขอนุกรมวิธานข้อมูล รวมถึงการระบุและจัดการรายการมาตรฐานของโดเมนข้อมูลและโดเมนย่อย

• ตรวจสอบให้แน่ใจว่าไม่มีการซ้ำซ้อนสำหรับอนุกรมวิธานข้อมูลกลุ่ม

• สร้างเทมเพลตสำหรับทั้งกลุ่มสำหรับบันทึกทั้งข้อมูลเมทาของธุรกิจ (เช่น คำจำกัดความของธุรกิจ กฎด้านคุณภาพข้อมูล) และข้อมูลเมทาทางเทคนิค (เช่น สายข้อมูล)

บริกรข้อมูลร่วมกับบริกรแพลตฟอร์ม จะต้อง :

• ดูแลรักษาพจนานุกรมข้อมูลและสายข้อมูลสำหรับโดเมนข้อมูลและโดเมนของข้อมูลที่กำหนด

• ส่งเสริมการใช้พจนานุกรมข้อมูลสำหรับโดเมนข้อมูลและโดเมนย่อยข้อมูลที่กำหนด

• รายงานการสร้างคำจำกัดความใหม่หรือการเบี่ยงเบนใด ๆ จากพจนานุกรมข้อมูลที่มีอยู่ไปยังเจ้าของข้อมูล

๒.๓ การบริหารจัดการคุณภาพข้อมูล (Data Quality Management)

เพื่อให้การควบคุมคุณภาพข้อมูล สำหรับการนำไปใช้ประโยชน์ในการบริหารงานและการให้บริการประชาชนของ อ.ต.ก. โดยให้เป็นไปตามอำนาจหน้าที่และวัตถุประสงค์ในการดำเนินงานตามที่กฎหมายกำหนด โดยข้อมูลที่ได้รับ การจัดเก็บนั้น อ.ต.ก. จะคำนึงถึงคุณภาพข้อมูล (Data Quality) ในทุกชุดข้อมูล (Dataset) โดยมีการกำหนดมาตรฐานดังนี้

๒.๓.๑ กำหนดมาตรฐานข้อมูลให้เป็นแบบเดียวกัน และมีการควบคุมคุณภาพข้อมูลตลอดทั้งวงจรชีวิตข้อมูล (Data Life Cycle) ของข้อมูลที่ตนเองมีหน้าที่รับผิดชอบเท่านั้น

๒.๓.๒ กำหนดให้มีข้อกำหนดพื้นฐานของการบริหารจัดการคุณภาพข้อมูล (Data Quality Management) รวมถึงแนวทางการควบคุมและการปรับปรุงอย่างต่อเนื่อง

๒.๓.๓ ทุกข้อมูลทุกชุดต้องมีการวัดคุณภาพข้อมูล (Data Quality) ดังนี้

• ความถูกต้อง (Accuracy)

ข้อมูลจะมีความถูกต้องและเชื่อถือได้ขึ้นกับวิธีการที่ใช้ในการควบคุมข้อมูลนำเข้า และการควบคุมการประมวลผล การควบคุมข้อมูลนำเข้าเป็นการกระทำเพื่อให้เกิดความมั่นใจว่าข้อมูลนำเข้ามีความถูกต้องเชื่อถือได้ เพราะถ้าข้อมูลนำเข้าไม่มีความถูกต้องแล้ว ถึงแม้จะใช้วิธีการวิเคราะห์และ ประมวลผลข้อมูลที่ดีเพียงใด ผลลัพธ์ที่ได้ก็จะไม่มีความถูกต้อง หรือนำไปใช้ไม่ได้ข้อมูลนำเข้าจะต้องเป็นข้อมูลที่ผ่านการตรวจสอบว่าถูกต้องแล้ว ข้อมูลบางประเภทอาจต้องแปลงให้อยู่ในรูปแบบที่เครื่องคอมพิวเตอร์สามารถเข้าใจได้อย่างถูกต้อง ซึ่งอาจต้องพิมพ์ข้อมูลมาตรวจสอบก่อนการประมวลผล ถึงแม้ว่าจะมีการตรวจสอบข้อมูลนำเข้าแล้วก็ตาม ก็อาจทำให้ได้ข้อมูลที่ผิดพลาดได้ เช่น การเขียน โปรแกรมหรือใช้สูตรคำนวณผิดพลาด ดังนั้นจึงควรกำหนดวิธีการควบคุมการประมวลผล ได้แก่การตรวจสอบยอดรวมที่ได้จากการประมวลผลแต่ละครั้งหรือการตรวจสอบผลลัพธ์ที่ได้จากการประมวลผลด้วย เครื่องคอมพิวเตอร์กับข้อมูลสมบัติที่มีการคำนวณด้วยว่ามีความถูกต้องตรงกันหรือไม่

• ความครบถ้วน (Completeness)

ข้อมูลบางประเภทหากไม่ครบถ้วน จัดเป็นข้อมูลที่ด้อยคุณภาพได้เช่นกัน เช่น ข้อมูลประวัติคนไข้ หากไม่มีหมู่เลือดของคนไข้ จะไม่สามารถใช้ได้ในกรณีที่ผู้ร้องขอข้อมูลต้องการข้อมูลหมู่เลือดของคนไข้

หรือข้อมูลที่อยู่ของลูกค้าที่กรอกผ่านแบบฟอร์ม ถ้ามีชื่อและนามสกุลโดยไม่มีข้อมูลบ้านเลขที่ ถนน แขวง/ตำบล เขต/อำเภอ หรือ จังหวัด ข้อมูลเหล่านั้นก็ไม่สามารถนำมาใช้ได้เช่นกัน

• ตรงตามความต้องการของผู้ใช้ (Relevancy)

ระดับของข้อมูลที่บริหารจัดการต้องการนำเสนอโดยตรงและมีประสิทธิภาพ โดยสามารถใช้งานได้ตามวัตถุประสงค์ ตัวอย่างเช่น ข้อมูลทางสถิติที่จะเป็นการนำเสนอในรูปแบบตารางเข้าใจง่าย และข้อความอยู่ในหลาย ๆ ย่อหน้า ซึ่งสามารถใช้งานได้ตามความต้องการ

• ความน่าเชื่อถือ (Data Integrity}

การรักษาความถูกต้องของข้อมูล ความสามารถที่จะตรวจสอบได้ว่าข้อมูลที่ได้รับมีความถูกต้อง ครบถ้วน สมบูรณ์ และไม่ถูกเปลี่ยนแปลงแก้ไขใดๆ ไปจากเดิม โดยผู้ที่ไม่ได้รับอนุญาต หากมีการเปลี่ยนแปลงโดยผู้ได้รับอนุญาตจะต้องมีการบันทึกทุกการเปลี่ยนแปลง เพื่อการตรวจสอบกลับการเปลี่ยนแปลงนั้น

• ความพร้อมใช้งาน (Availability)

ข้อมูลควรเข้าถึงได้ง่าย สามารถใช้งานได้จริง และสามารถใช้งานได้ตลอดเวลา ตัวอย่างเช่น นักวิเคราะห์ แผนงานต้องการข้อมูลบัญชีของการประกันภัยต่อเขตต่าง ๆ แต่ข้อมูลไม่พร้อมใช้งานจนกระทั่งต้องใช้คนเขียนโปรแกรมเพื่อดึงข้อมูลนั้นออกมา ในกรณีนี้หากข้อมูลมีความพร้อมกับความต้องการใช้ ผู้ใช้สามารถใช้ข้อมูลดังกล่าวได้ทันที

โดยทุกเกณฑ์ เป็นเกณฑ์เชิงปริมาณ (Quantitative measurement)

๒.๓.๔ การกำหนดตัวชี้วัดคุณภาพข้อมูล เช่น ความถูกต้อง ความครบถ้วน ความต้องกัน ความเป็นปัจจุบัน ตรงความต้องการของผู้ใช้ และพร้อมใช้งาน

๒.๓.๕ รายงานคุณภาพข้อมูล ประกอบด้วย การกำหนดระดับมิติตัวชี้วัดและค่าเป้าหมายในการประเมินคุณภาพข้อมูล จะต้องแนบไปกับการใช้ชุดข้อมูล (Dataset) และชุดคำอธิบายข้อมูล หรือเมทาดาดา

๒.๓.๖ การฝึกอบรมเพื่อสร้างความตระหนักถึงคุณภาพของข้อมูล

๒.๔ การบริหารจัดการความเสี่ยงด้านข้อมูล (Data Risk Management)

ขอบเขตการบริหารความเสี่ยง สามารถอ้างอิงจาก นโยบาย หรือมาตรฐานการจัดการความเสี่ยงด้านเทคโนโลยี สารสนเทศขององค์กร โดยครอบคลุมความเสี่ยงดังต่อไปนี้

• ความเสี่ยงด้านปฏิบัติการงานเทคโนโลยีสารสนเทศ (IT operation risks) คือความเสี่ยงที่เกิดขึ้นจากความผิดพลาดในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ เช่น ความผิดพลาด หรือความไม่เหมาะสมในการควบคุม ติดตามการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ เช่น การสำรองข้อมูล การพิมพ์รายงานประจำวัน การควบคุมสภาพแวดล้อมการปฏิบัติงานในศูนย์คอมพิวเตอร์ และการบริหารจัดการการเปลี่ยนแปลงเทคโนโลยีสารสนเทศ การจัดการทรัพย์สินเทคโนโลยีสารสนเทศ การตั้งค่าสิทธิการเข้าถึงบน cloud เป็นต้น

• ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ (IT hardware risks) คือความเสี่ยงที่เกิดจากการทำงานผิดพลาด หรือการไม่ทำงานของอุปกรณ์เทคโนโลยีสารสนเทศ เช่น เครื่องคอมพิวเตอร์แม่ข่าย เครื่องคอมพิวเตอร์ อุปกรณ์เครือข่าย อุปกรณ์สนับสนุนการประมวลผลสารสนเทศ อุปกรณ์ในศูนย์คอมพิวเตอร์ สื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ เป็นต้น

• ความเสี่ยงด้านโปรแกรมเทคโนโลยีสารสนเทศ (IT software risks) คือความเสี่ยงที่เกิดขึ้นจากการทำงานผิดพลาด การหยุดชะงัก หรือความไม่พร้อมใช้งานโปรแกรมเทคโนโลยีสารสนเทศ เช่น โปรแกรมประยุกต์ โปรแกรมระบบ เครื่องมือสำหรับพัฒนา และโปรแกรมประเภทยูทีดีที่สำหรับระบบ รวมถึงความเสี่ยงจากการพัฒนาโปรแกรมหรือระบบงานที่ไม่ตรงตามความต้องการของหน่วยงานธุรกิจ

• ความเสี่ยงด้านข้อมูลสารสนเทศ (Digital data risks) คือความเสี่ยงที่เกิดขึ้นจากข้อมูลในระบบสารสนเทศที่สำคัญ หรือเป็นความลับ เสียหาย หาย รั่วไหล จารกรรม ถูกปลอมแปลง หรือถูกทำลาย เช่น ฐานข้อมูล ไฟล์ข้อมูล ซอร์สโค้ด สัญญา เอกสาร/คู่มือระบบ ข้อมูลการวิจัย คู่มือผู้ใช้งาน ขั้นตอนการปฏิบัติงาน ข้อมูลการตรวจสอบ ประวัติการตรวจสอบ ข้อมูลสำรองของระบบงาน

• ความเสี่ยงด้านผู้ขายและผู้ให้บริการงานเทคโนโลยีสารสนเทศ (IT vendor/supplier risks) คือความเสี่ยงที่เกิดขึ้นจากการคัดเลือกและการบริหารจัดการผู้ขาย ผู้ให้บริการ คู่ค้า คู่สัญญา ผู้ส่งมอบงานตามข้อกำหนดในสัญญา การใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศทั้งในประเทศและต่างประเทศ ซึ่งรวมถึงการใช้บริการ cloud services ที่ไม่เหมาะสมหรือไม่มีประสิทธิภาพ และความเสี่ยงจากผู้ให้บริการ คู่ค้า หรือคู่สัญญาไม่สามารถให้บริการใต้ซึ่งส่งผลกระทบต่อการดำเนินงานขององค์กร

• ความเสี่ยงด้านการบริหารโครงการเทคโนโลยีสารสนเทศ (IT project management risks) คือความเสี่ยงจากการบริหารโครงการเทคโนโลยีสารสนเทศ ล่าช้า หรือไม่สำเร็จ อันเนื่องมาจากการกำกับดูแลการบริหารจัดการโครงการ การมอบหมายและกำหนดขอบเขต การจัดสรรทรัพยากร เวลา เงินทุน การประสานงาน เป็นต้น

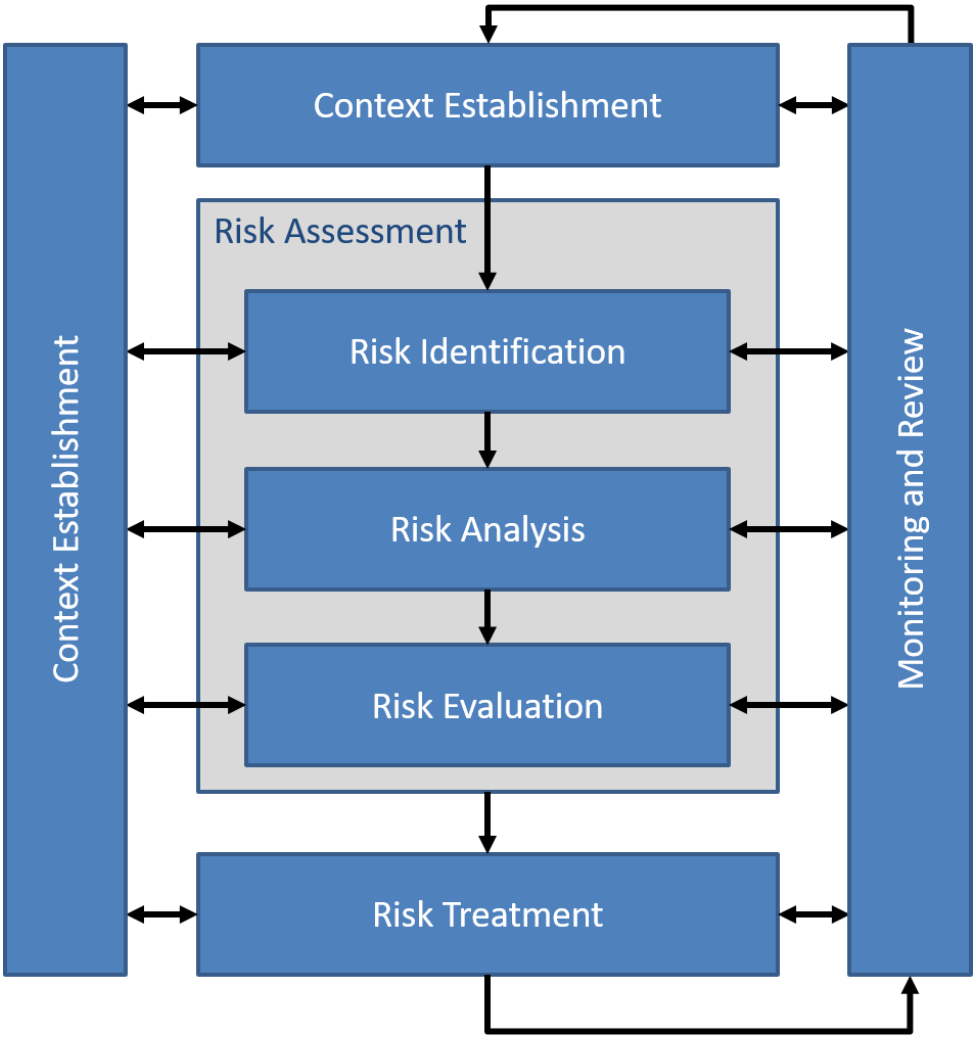
• ความเสี่ยงด้านบุคลากร (Personal risks) คือความเสี่ยงที่เกิดจากบุคลากรขาดความรู้ ทักษะที่เพียงพอต่อการดำเนินงาน การจัดสรรบุคลากรที่ไม่เหมาะสมกับลักษณะงานที่มอบหมาย ความเสี่ยงที่เกิดจากการทุจริต ของบุคลากร เป็นต้น

• ความเสี่ยงด้านการกู้ระบบจากเหตุการณ์ฉุกเฉิน และการบริหารความต่อเนื่องของการให้บริการงานเทคโนโลยีสารสนเทศ (Disaster recovery and IT continuity risks) คือความเสี่ยงที่เกิดขึ้นจากภัยพิบัติหรือเหตุการณ์ ฉุกเฉินต่าง ๆ ซึ่งอาจส่งผลให้ธุรกิจเกิดความเสียหาย หยุดชะงัก หรือไม่สามารถให้บริการแก่ลูกค้าตามระยะเวลาที่กำหนดได้ เป็นต้น

• ความเสี่ยงด้านการปฏิบัติตามกฎ ระเบียบ ข้อบังคับ และกฎหมายด้านเทคโนโลยีสารสนเทศ (IT compliance risks) คือความเสี่ยงที่เกิดขึ้นที่เกิดขึ้นจากการไม่ปฏิบัติตามกฎ ระเบียบ ข้อบังคับและกฎหมาย ซึ่งอาจส่งผลใน ด้านลบต่อบริบทองค์กร เช่น สูญเสียภาพลักษณ์ ถูกปรับหรือฟ้องร้อง เป็นต้น

• ความเสี่ยงด้านความปลอดภัยเทคโนโลยีสารสนเทศ (IT security/cyber security risks) คือความเสี่ยงที่เกิดขึ้นจากความไม่ปลอดภัยของเทคโนโลยีสารสนเทศ ระบบความปลอดภัยด้านโครงสร้างพื้นฐานสารสนเทศและการใช้งานด้านไซเบอร์ สอดคล้องกับความเสี่ยงที่อาจเกิดขึ้นภายใต้หลักการสำคัญด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ ๓ ประการคือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้อง (Integrity) และความพร้อมใช้งาน (Availability) ของระบบเทคโนโลยีสารสนเทศ เช่น การถูกโจมตีระบบเทคโนโลยี สารสนเทศ และ/หรือ โครงสร้างพื้นฐานสารสนเทศโดยผู้ไม่ประสงค์ดีผ่านทางระบบเครือข่าย การแพร่กระจาย ไวรัส ขาดการควบคุมการเข้าถึงทางกายภาพ การปลอมแปลง การแชร์ใช้งานรหัสผ่าน เป็นต้น

โดยการประเมินความเสี่ยงดังกล่าว สามารถอ้างอิงได้จากมาตรฐานสากล ISO ๓๑๐๐๐ Risk Management



มาตรฐานสากล ISO ๓๑๐๐๐ Risk Management

๒.๕ การรักษาความมั่นคงปลอดภัยของข้อมูล (Data security)

การรักษาความมั่นคงปลอดภัยของข้อมูล เป็นส่วนหนึ่งของความพยายามในวงกว้างเพื่อลดความเสี่ยงด้านความปลอดภัยในโลกไซเบอร์ โดยเฉพาะอย่างยิ่ง การคุ้มครองข้อมูลมุ่งเน้นไปที่ความเสี่ยงที่เกี่ยวข้องกับความเป็นส่วนตัวที่เกี่ยวข้องกับการละเมิดความลับ ความสมบูรณ์ หรือความพร้อมใช้งานของข้อมูลส่วนบุคคล ข้อกำหนดและการควบคุม การปกป้องข้อมูลควรได้รับการบังคับใช้และตรวจสอบเป็นระยะ โดยการกระทำข้างต้นดังกล่าวเป็นส่วนหนึ่งของความพยายามในการจัดการความเสี่ยงด้านความปลอดภัยทางไซเบอร์ที่กว้างขึ้น

• หัวหน้าฝ่ายกำกับดูแลความปลอดภัยจะต้องสร้างและบังคับใช้กระบวนการเพื่อประเมินและตัดสินการปฏิบัติตามมาตรฐานอย่างน้อยปีละ ๒ ครั้ง

• หัวหน้าฝ่ายกำกับดูแลความปลอดภัยจะต้องประสานงานกับบริกรข้อมูล และ บริกรแพลตฟอร์มเพื่อออกแบบและนำแผนการแก้ไขไปปฏิบัติเมื่อมีการระบุช่องว่างการควบคุมเทียบกับมาตรฐานในระบบการประมวลผลข้อมูล

๒.๕.๑ การจัดระดับชั้นความลับของข้อมูล

การจัดระดับชั้นความลับของข้อมูลช่วยให้ อ.ต.ก. สามารถจัดหมวดหมู่ข้อมูลออกเป็นระดับต่าง ๆ ตามผลกระทบของข้อมูลที่ถูกบุกรุกข้อมูล อาจถูกบุกรุกในแง่ของการรักษาความลับ ความสมบูรณ์ หรือความพร้อมใช้งาน ไม่ว่าจะโดยตั้งใจหรือโดยบังเอิญ การจัดระดับชั้นความลับของข้อมูลเป็นพื้นฐานสำหรับ อ.ต.ก. ในการตัดสินใจว่าข้อมูลต่าง ๆ ควรได้รับการคุ้มครองอย่างไรเมื่อมีการรวบรวม ประมวลผล หรือเปิดเผย :

• บริกรข้อมูลต้องประสานงานกับ หัวหน้าฝ่ายกำกับดูแลข้อมูล และหัวหน้าฝ่ายกำกับดูแลความปลอดภัย เพื่อประเมินผลกระทบของความเสียหายต่อข้อมูลสำหรับแต่ละโดเมนย่อยของข้อมูลที่ดำเนินการจัดการ

• บริกรข้อมูลต้องใช้กรอบผลกระทบของข้อมูลเพื่อประเมินผลกระทบของการประนีประนอมของโดเมนย่อยข้อมูลแต่ละรายการ

• บริกรข้อมูลต้องประสานงานกับ หัวหน้าฝ่ายกำกับดูแลข้อมูล และ หัวหน้าฝ่ายกำกับดูแลความปลอดภัย เพื่อกำหนดระดับการจัดประเภทให้กับแต่ละโดเมนย่อยของข้อมูล

• บริกรข้อมูลต้องใช้กรอบการจัดประเภทข้อมูลเพื่อจำแนกแต่ละโดเมนย่อยของข้อมูล

๒.๕.๒ การติดฉลากข้อมูล

อ.ต.ก. ต้องติดฉลากข้อมูลตามระดับชั้นความลับเพื่อใช้ประโยชน์จากข้อมูล กิจกรรมการติดฉลากข้อมูลนี้ ดำเนินการโดยใช้แอดทริบิวต์ของเมทาดาตาสำหรับข้อมูลที่จัดเก็บอย่างมีเหตุผล และใช้ป้ายกำกับทางกายภาพสำหรับข้อมูลที่จัดเก็บทางกายภาพ :

• หัวหน้าฝ่ายกำกับดูแลข้อมูลจะต้องจัดหาฉลากที่จับต้องได้ซึ่งแสดงถึงข้อมูลที่เป็นความลับและทำให้พร้อมใช้ งานสำหรับธุรกิจ (เอกสารที่ไม่มีป้ายกำกับถือเป็นเอกสารที่ใช้ภายใน)

• บริกรข้อมูลต้องสร้างและบังคับใช้กระบวนการเพื่อติดฉลากข้อมูลทางกายภาพ (เช่น งานพิมพ์) โดยใช้ฉลาก เมื่อข้อมูลดังกล่าวถูกถ่ายโอนภายใน อ.ต.ก. หรือจาก อ.ต.ก. ไปยังบุคคลที่สาม

• บริกรแพลตฟอร์มต้องสร้างและบังคับใช้การควบคุมทางเทคนิคเพื่อบันทึกการจัดประเภทของข้อมูลดิจิทัลโดยใช้แอดทริบิวต์เมทาดาตาทางเทคนิค การรักษาความลับ เมื่อข้อมูลดังกล่าวถูกสร้างขึ้นหรือถ่ายโอนไปยัง อ.ต.ก.

๒.๕.๓ การเข้ารหัสข้อมูล

การเข้ารหัสข้อมูลใช้กับทั้งการขนส่งข้อมูลและการจัดเก็บข้อมูล เป็นวิธีการหนึ่งในการรับรอง ว่าข้อมูลได้รับการปกป้องจากการละเมิดความลับหรือความสมบูรณ์ อ.ต.ก. ควรใช้แนวทางปฏิบัติที่ดีที่สุดระดับสากลสำหรับการเข้ารหัสข้อมูล :

• ทีมกำกับดูแลข้อมูลต้องประสานงานกับทีมรักษาความมั่นคงความปลอดภัยด้านเทคโนโลยีสารสนเทศเพื่อให้แน่ใจว่า อัลกอริทึมการเข้ารหัสที่ได้รับการพิสูจน์แล้วและความยาวของคีย์ที่เลือกเท่านั้นที่ใช้สำหรับการเข้ารหัส

๒.๖ การรักษาความเป็นส่วนบุคคลของข้อมูล (Data Privacy)

เพื่อลดความเสี่ยงในการแบ่งปันข้อมูลและรองรับการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลของไทย (PDPA) อ.ต.ก. ต้องมีการพัฒนานโยบายความยินยอมของลูกค้าแบบรวมและข้อตกลงมาตรฐานในการแบ่งปันข้อมูล เอกสารเหล่านี้จะเป็นรากฐานทางกฎหมายร่วมกันสำหรับ อ.ต.ก. ในการรวบรวม ประมวลผล และเปิดเผย ข้อมูลส่วนบุคคลระหว่างกัน และเพื่อเจรจาแบ่งปันข้อมูลกับบุคคลที่สามโดยใช้ข้อกำหนดและเงื่อนไขมาตรฐาน นอกเหนือจากนโยบายความยินยอมของลูกค้าแบบรวมและข้อตกลงมาตรฐานการแบ่งปันข้อมูลแล้ว ยังมีข้อกำหนดในการจัดเก็บและขนส่งข้อมูลที่เฉพาะเจาะจงอีกด้วย เพื่อให้มั่นใจว่า อ.ต.ก. ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล และ ปกป้องข้อมูลส่วนบุคคลจากการเปิดเผยโดยไม่ตั้งใจ

• บริกรข้อมูลต้องสร้างและบังคับใช้กระบวนการเพื่อให้มั่นใจว่าข้อมูลส่วนบุคคลตามที่กำหนดไว้ในกรอบข้อมูลส่วนบุคคลจะถูกแบ่งปันระหว่าง อ.ต.ก. และบุคคลอื่น ๆ ในลักษณะที่มีการเข้ารหัส หรือรักษาความมั่นคงปลอดภัย (เช่น การแอช เป็นต้น)

• บริกรแพลตฟอร์มต้องสร้างและบังคับใช้การควบคุมทางเทคนิคเพื่อให้แน่ใจว่าข้อมูลส่วนบุคคลตามที่กำหนดไว้ในกรอบข้อมูลส่วนบุคคลจะถูกแบ่งปันระหว่าง อ.ต.ก.และบุคคลอื่น ๆ ในลักษณะที่มีการเข้ารหัส หรือรักษาความมั่นคงปลอดภัย (เช่น การแอช เป็นต้น)

• ผู้นำด้านสถาปัตยกรรมคอมพิวเตอร์จะต้องประสานงานกับทีมรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ เพื่อให้แน่ใจว่ามีการป้องกันข้อมูลเมื่อมีการขนส่งโดยใช้การควบคุม เช่น การเข้ารหัส

บทที่ ๓
แนวทางการประเมินระดับการกำกับดูแลข้อมูล
(Data Governance Maturity Assessment)

๓.๑ องค์ประกอบและมิติของการประเมินระดับความพร้อมของการกำกับดูแลข้อมูล

การประเมินความพร้อมของการกำกับดูแลข้อมูลจะทำให้องค์กรได้ทราบถึงสิ่งที่ได้ดำเนินการแล้วและสิ่งใดบ้างที่ควรจะดำเนินการต่อไป เพื่อปรับปรุงการดำเนินงานให้เกิดประสิทธิภาพสูงสุด ระดับความพร้อมของการกำกับดูแลข้อมูลถูกใช้ เป็นเครื่องมือในการประเมินความพร้อมของการกำกับดูแลข้อมูลโดยกรอบการกำกับดูแลข้อมูล เวอร์ชัน ๑.๐ ที่จัดทำโดย สำนักงานพัฒนารัฐบาลดิจิทัล (๒๕๖๑) ได้เสนอระดับความพร้อมและวุฒิภาวะ ๕ ระดับ ดังภาพต่อไปนี้

แนวทางการประเมินระดับการกำกับดูแลข้อมูล (Data Savemance Maturity Assessment)

Level ๑ - Initial หมายถึง ไม่มีการกำหนดมาตรฐานของกระบวนการ นั่นคือ กระบวนการถูกกำหนดขึ้นมาเฉพาะกิจ (Adhoc) ทำให้แต่ละโครงการหรือบริการมีรูปแบบของกระบวนการที่แตกต่างกัน และอำนาจในการจัดการและ กำกับดูแลข้อมูลส่วนใหญ่ถูกดำเนินการโดยฝ่ายเทคโนโลยีสารสนเทศทำให้การทำงานร่วมกันระหว่างฝ่ายธุรกิจและฝ่ายเทคโนโลยีสารสนเทศไม่สอดคล้องกัน

Level ๒ - Managed หมายถึง เริ่มมีการกำหนดมาตรฐานของกระบวนการเฉพาะแต่ละส่วนงานหรือบริการ และมีการกำหนดบุคคลที่เกี่ยวข้องกับการกำกับติดตาม เช่น บริกรข้อมูล (Data Steward) และเจ้าของข้อมูล (Data Owner)

Level ๓ - Defined หมายถึง กระบวนการถูกกำหนดเป็นมาตรฐานของหน่วยงาน มีการกำหนดส่วนงานกลางใน การกำกับและติดตามข้อมูล ซึ่งมาจากบุคคลด้านธุรกิจและเทคโนโลยีสารสนเทศมีการบังคับใช้นโยบายข้อมูลครอบคลุมทั้งหน่วยงาน มีการติดตาม วิเคราะห์ และรายงานคุณภาพข้อมูลหรือความมั่นคงปลอดภัย

Level ๔ - Quantitatively Managed หมายถึง กระบวนการถูกกำหนดเป็นมาตรฐานของหน่วยงาน มีการกำหนดส่วนงานกลางในการกำกับและติดตามข้อมูล ซึ่งมาจากบุคคลด้านธุรกิจและเทคโนโลยีสารสนเทศมีการบังคับใช้นโยบายข้อมูล ครอบคลุมทั้งหน่วยงาน มีการติดตาม วิเคราะห์ และรายงานคุณภาพข้อมูลและความมั่นคงปลอดภัย

Level ๕ - Optimized หมายถึง มีการดำเนินการสอดคล้องกับระดับ ๔ วิเคราะห์สาเหตุของปัญหา (Root Cause) ประกอบไปด้วย ความไม่สอดคล้องในการปฏิบัติงานกับนโยบายข้อมูล (Non-Conformation) คุณภาพข้อมูลที่ต่ำ และความไม่คุ้มทุนในการบริหารจัดการข้อมูล ดำเนินการปรับปรุงกระบวนการ กฎเกณฑ์ และนโยบายข้อมูล หรือโครงสร้างการกำกับดูแล ข้อมูลเพื่อแก้ไขปัญหาที่พบจากผลการวิเคราะห์ และให้สอดคล้องกับความต้องการของผู้ที่เกี่ยวข้องและวัตถุประสงค์ที่เปลี่ยนไปของหน่วยงาน

๓.๒ องค์ประกอบและมิติของการประเมินระดับความพร้อมของการกำกับดูแลข้อมูล

ตัวชี้วัดที่ระบุในกรอบการกำกับดูแลข้อมูล เป็นเพียงเกณฑ์กว้างๆ ที่ยังไม่สามารถสืบเสาะไปจนถึงความพร้อมในองค์ประกอบย่อย ๆ ของการกำกับดูแลข้อมูล จึงได้เสนอแบบประเมินความพร้อมของการกำกับดูแลข้อมูลที่พัฒนา โดย Stanford University (๒๐๑๑) โดยองค์ประกอบด้านการเชื่อมโยงข้อมูล ดังนั้น องค์ประกอบของการประเมินสถานะมี ๘ องค์ประกอบ ได้แก่

๑) ความตระหนักรู้ (Awareness)
๒) การจัดระเบียบ (Formalization)
๓) เมทาดาตา (Metadata)
๔) การให้บริการข้อมูล (Stewardship)
๕) คุณภาพข้อมูล (Data Quality)
๖) ข้อมูลหลัก (Master Data)

โดยทั้ง ๘ องค์ประกอบจะทำการวัดใน ๓ มิติ ได้แก่

๗) บุคลากร (People)
๘) นโยบาย (Policies)
๙) ประสิทธิภาพ (Capabilities)

องค์ประกอบที่ ๑ ความตระหนักรู้ (Awareness)

มิติด้านบุคลากร (People) :	ความตระหนักทำให้บุคลากรมีความรู้เกี่ยวกับหน้าที่ของการกำกับดูแลข้อมูล
มิติด้านนโยบาย (Policies) :	นโยบายการกำกับข้อมูลมาตรฐานและแนวปฏิบัติที่ดีที่สุดของการกำกับดูแลข้อมูล
มิติด้านประสิทธิภาพ (Capabilities) :	การรู้ถึงสิทธิการเข้าถึงข้อมูลประเภทความสามารถในการควบคุมและพัฒนาให้เกิดคุณค่าต่อ

องค์ประกอบที่ ๒ การจัดระเบียบ (Formalization)

มิติด้านบุคลากร (People) :	องค์กรการกำกับดูแลข้อมูลได้รับการพัฒนาอย่างไรและมีบทบาทใดบ้างที่จะสนับสนุนกิจกรรมการกำกับดูแลข้อมูล
มิติด้านนโยบาย (Policies) :	นโยบายการกำกับดูแลข้อมูลมีการกำหนดปฏิบัติและบังคับใช้อย่างเป็นทางการในระดับใด
มิติด้านประสิทธิภาพ (Capabilities) :	การพัฒนาเตรียมพร้อมที่จะทำบางอย่างเพื่อสนับสนุนกิจกรรมการกำกับดูแลข้อมูลและชุดเครื่องมือที่ใช้งานตรวจสอบอย่างสม่ำเสมอ

องค์ประกอบที่ ๓ เมทาดาตา (Metadata)

มิติด้านบุคลากร (People) : การมีส่วนร่วมในการพัฒนาและบำรุงเมทาดาดา ในระดับใด

มิติด้านนโยบาย (Policies) : นโยบายการสร้างและบำรุงรักษาเมทาดาดา โดยต้องกำหนดไว้อย่างเป็นทางการ

มิติด้านประสิทธิภาพ (Capabilities) : การเตรียมจัดการเมทาดาตาที่มีความหลากหลายระดับของการกำกับดูแลข้อมูล

องค์ประกอบที่ ๔ การให้บริการข้อมูล (Stewardship)

มิติด้านบุคลากร (People) : การทราบถึงข้อมูลที่มีอยู่ที่เกี่ยวกับบทบาทของ Stewardship ในการกำกับดูแลข้อมูล

มิติด้านนโยบาย (Policies) : นโยบายการกำกับดูแลข้อมูลที่ดีที่สุดต้องทำให้เกิดมาตรฐานและแนวทางปฏิบัติที่ดีที่สุด

มิติด้านประสิทธิภาพ (Capabilities) : การทราบถึงข้อมูลที่มีความสามารถในการควบคุมข้อมูลที่สามารถสร้างและพัฒนาต่อได้

องค์ประกอบที่ ๕ คุณภาพข้อมูล (Data Quality)

มิติด้านบุคลากร (People) : องค์กรที่กำกับดูแลข้อมูลควรได้รับการพัฒนาอย่างไรและมีบทบาทใด ที่ตอบสนองและสนับสนุนกิจกรรมของการกำกับดูแลข้อมูล

มิติด้านนโยบาย (Policies) : นโยบายการกำกับดูแลข้อมูลมีกำหนดนำไปปฏิบัติและบังคับใช้อย่างเป็นทางการได้ถึงในระดับใด

มิติด้านประสิทธิภาพ (Capabilities) : ชุดเครื่องมือที่พัฒนาขึ้นนั้นสนับสนุนกิจกรรมการกำกับดูแลข้อมูลอย่างไรและชุดเครื่องมือนั้นจะทำอย่างไรให้เกิดความสม่ำเสมอในการกำกับดูแลข้อมูล

องค์ประกอบที่ ๖ ข้อมูลหลัก (Master Data)

มิติด้านบุคลากร (People) : การบริหารจัดการข้อมูลหลักอย่างเป็นทางการนั้นได้รับการพัฒนาได้ถึง ระดับใดและได้รับมอบหมายหน้าที่ความรับผิดชอบให้สอดคล้องกันระหว่างข้อมูล

มิติด้านนโยบาย (Policies) : นโยบายในการสร้างข้อมูลหลักและการบำรุงรักษาต้องปฏิบัติถึงระดับ โดเพื่อการนำไปปฏิบัติและบังคับใช้อย่างเป็นทางการ

มิติด้านประสิทธิภาพ (Capabilities) : กำหนดความสามารถในการจัดการเมทาดาตา ในระดับความหลากหลายระดับข้อมูลความเป็นการกำกับดูแลข้อมูล

บทที่ ๔
การสร้าง การจัดเก็บรักษา การทำลาย และการควบคุมคุณภาพข้อมูล

๔.๑ แนวปฏิบัติการสร้างข้อมูล

๑) ต้องปฏิบัติตามกฎหมาย ระเบียบ ประกาศ และหลักเกณฑ์ที่เกี่ยวข้อง และให้ปฏิบัติโดยเคร่งครัดในประเด็น ดังต่อไปนี้

• สร้างข้อมูลจากแหล่งข้อมูลต้นทางโดยตรงหรือแหล่งข้อมูลที่น่าเชื่อถือ และอ้างอิง แหล่งที่มาตามรูปแบบที่ถูกต้อง

• ห้ามสร้างข้อมูลที่บิดเบือน หรือปลอมแปลงไม่ว่าทั้งหมดหรือบางส่วน แนวปฏิบัติการจัดเก็บข้อมูล

๒) แนวปฏิบัตินี้หมายความรวมถึงการจัดเก็บข้อมูลทั้งที่เป็นกระดาษ และข้อมูลที่เป็นอิเล็กทรอนิกส์ทุกประเภท ไม่ว่าจะเป็นไฟล์ข้อมูลธรรมดา (Plain Files) ไฟล์ข้อมูลที่มีการเข้ารหัส (Encryption Files) ไฟล์ข้อมูลที่ผ่านการประมวลผล (Information Files) หรือไฟล์ข้อมูล รูปแบบอื่น ๆ

๓) ต้องปฏิบัติตามกฎหมาย ระเบียบ ประกาศ และหลักเกณฑ์ที่เกี่ยวข้อง และให้ปฏิบัติโดยเคร่งครัดในประเด็น ดังต่อไปนี้

• ต้องจัดเก็บข้อมูล ให้ถูกต้องเหมาะสมตามระดับการเปิดเผยข้อมูลของ อ.ต.ก. โดยกำหนดระดับการเปิดข้อมูล ไว้ดังนี้

- ข้อมูลสาธารณะ
- ข้อมูลเปิดภายใน อ.ต.ก.
- ข้อมูลที่ต้องได้รับอนุญาตจากคณะทำงานบริกรข้อมูลของ อ.ต.ก.
- ข้อมูลที่ต้องได้รับอนุญาตจากหน่วยงานภายนอก
- ข้อมูลปกปิด

• การจัดเก็บไฟล์ข้อมูลลับ ให้ปฏิบัติดังนี้

- เจ้าของข้อมูล ผู้สร้างข้อมูลต้องตรวจสอบความถูกต้องของข้อมูลก่อนจัดเก็บ
- ต้องแจกแจงประเภทของข้อมูลตามลำดับชั้นความลับ รวมถึงกำหนดผู้มีสิทธิในการเข้าถึงหรือควบคุมการใช้งานอย่างเหมาะสม และในกรณีจำเป็นที่ต้องมีการจำกัดการเข้าถึงข้อมูลลับให้แก่บุคคลผู้ที่มีหน้าที่เกี่ยวข้อง ให้จัดทำรายชื่อผู้ได้รับอนุญาตให้เข้าถึงดังกล่าวอย่างรอบคอบ
- เอกสารต้นฉบับต้องได้รับการเก็บรักษาอย่างดีไม่ให้เกิดความเสียหาย
- ต้องป้องกันไฟล์ข้อมูลที่เป็นความลับที่มีการจัดเก็บไว้ในเครื่องคอมพิวเตอร์ที่ตนเองใช้งานโดยเครื่องคอมพิวเตอร์ต้องมีการตั้งรหัสผ่านที่มีความมั่นคงปลอดภัย ต้องมีการเข้ารหัสลับ (Encryption) ไฟล์ข้อมูลที่เป็นความสั้น
- รหัสผ่านถือเป็นข้อมูลลับและเป็นหน้าที่ของผู้ใช้งานทุกคนที่ต้องเก็บรักษารหัสผ่านให้มีความมั่นคงปลอดภัย

๔.๒ แนวปฏิบัติการทำลายข้อมูล (Data Destruction)

๑) ต้องมีการตรวจสอบความสอดคล้องของวิธีปฏิบัติการทำลายข้อมูลให้สอดคล้องต่อกฎหมาย นโยบาย และแนวปฏิบัติ ที่เกี่ยวข้องกับข้อมูลต้องทำลาย โดยเฉพาะมาตรฐานการรักษาความมั่นคงปลอดภัยสารสนเทศ หรือมั่นใจได้ว่า สารสนเทศที่ตนดูแลรักษาอยู่นั้น ได้ถูกลบทำลายอย่างมั่นคงปลอดภัย เพื่อป้องกันข้อมูลรั่วไหลจากการลักลอบกู้คืนข้อมูล

๒) การลบทำลายข้อมูลอย่างมั่นคงปลอดภัย ให้ดำเนินการด้วยวิธีการใดวิธีการหนึ่งดังต่อไปนี้

- ลบทำลายข้อมูลในระดับไฟล์ด้วยวิธีการ Secure delete
- ลบ ลายไฟล์สำหรับสารสนเทศที่มีการเข้ารหัสลับ (Encrypted data)
- ทำลายข้อมูลแบบ Secure delete Secure erase ด้วยวิธีการที่ผู้ผลิตกำหนด
- ใช้ซอฟต์แวร์ หรือฮาร์ดแวร์สำหรับการลบข้อมูลโดยเฉพาะ (Sanitization)
- กรณีครุภัณฑ์ หรือส่วนใดส่วนหนึ่งของครุภัณฑ์ของสำนักงานให้ทำลายทิ้งในเชิงกายภาพ เช่น การทำให้ เสื่อมภาพของจานแม่เหล็ก Degauss) บททำลาย เผาทำลาย โดยต้องผ่านกระบวนการทางพัสดุก่อน

๓) เมื่อสิ้นสุดการเป็นพนักงานหรือพนักงานโครงการ หรือสิ้นสุดการใช้เครื่องคอมพิวเตอร์ส่วนบุคคล พนักงานหรือ พนักงานโครงการมีหน้าที่จะต้องสำรองข้อมูล หรือจะต้องรับผิดชอบข้อมูลด้วย ตนเอง พร้อมทั้งดำเนินการส่งเครื่อง คอมพิวเตอร์คืนให้แก่หน่วยบริการเทคโนโลยีสารสนเทศเพื่อ ดำเนินการทำลายข้อมูลต่อไป

๔) มีการจัดเก็บคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาดา (Metadata) ของข้อมูลที่ทำลาย เพื่อการตรวจสอบในภายหลัง

๕) ต้องมีการจัดเก็บบันทึกรายละเอียดการทำลายข้อมูลไว้ในทะเบียนคุม และบันทึก การทำลายข้อมูล โดยให้เก็บรักษา ไว้เป็นหลักฐานไม่น้อยกว่า ๑ ปี

๔.๓ แนวปฏิบัติการควบคุมคุณภาพข้อมูล (Data Quality)

๔.๓.๑ หลักการการจัดการคุณภาพของข้อมูล (Data Quality Principles)

คุณภาพของข้อมูล (Data Quality) คือ ข้อมูลที่ดี ได้มาตรฐานตามที่กำหนด กล่าวคือผลรวมของคุณลักษณะและ คุณสมบัติของผลิตผลข้อมูลที่พึงประสงค์ทุกประการของผลการปฏิบัติงานตามดัชนีตัวชี้วัดคุณภาพและองค์ประกอบที่กำหนดไว้ข้อมูลที่เหมาะสมกับการใช้งาน ตอบสนองต่อความต้องการที่กำหนด และตรงตามวัตถุประสงค์

การกำหนดแกนหลักในการขับเคลื่อนแนวทางในการกำกับดูแลคุณภาพของข้อมูล ประกอบด้วยหลักการ ๗ ประการดังนี้

- **หลักการที่ ๑ :** การกำกับดูแลข้อมูลที่มีประสิทธิภาพกำหนดให้ต้องวัดผล และทำความเข้าใจข้อมูลขององค์กร โดย อ.ต.ก. จะกำหนดมาตรการและมาตรวัดเพื่อประเมินประสิทธิภาพการจัดการข้อมูล
- **หลักการที่ ๒ :** ระบบอัตโนมัติจำเป็นอย่างยิ่งในการขยายคุณภาพข้อมูลทั่วทั้ง อ.ต.ก. หากเป็นไปได้ อ.ต.ก. ควรลงทุนในกระบวนการและเครื่องมือเพื่อช่วยให้กิจกรรมด้านคุณภาพข้อมูลเป็นไปโดยอัตโนมัติ
- **หลักการที่ ๓ :** อ.ต.ก. ต้องลดความซับซ้อนของสภาพแวดล้อมข้อมูล โดย อ.ต.ก. จะต้องพยายามใช้แหล่งข้อมูลที่เป็นทางการเท่านั้น และในขณะเดียวกันต้องทำการพิจารณาการยกเลิกการใช้แหล่งข้อมูลที่ไม่เป็นทางการ
- **หลักการที่ ๔ :** ความเข้าใจเรื่องคุณภาพของข้อมูลที่ อ.ต.ก. ได้รับ มีความจำเป็นต่อการใช้ข้อมูลอย่างมีประสิทธิภาพ ไม่ว่าข้อมูลจะมีคุณภาพสูงหรือต่ำ อ.ต.ก. ต้องประเมินและรับทราบผลกระทบอาจมีต่อภารกิจขององค์กร
- **หลักการที่ ๕ :** ความซับซ้อนในการออกแบบเป็นอุปสรรคต่อความสามารถในการรักษาข้อมูลคุณภาพสูง อ.ต.ก. จำเป็นต้องดำเนินการวางแผนผังข้อมูล (Data Map) และการจำแนก Data Domains เพื่อจัดโครงสร้างวิธีการจำลองข้อมูล

- **หลักการที่ ๖ :** การดำเนินการด้านคุณภาพข้อมูลจะมุ่งเน้นไปที่วิธีเปิดใช้งานข้อมูลที่จำเป็นของ อ.ต.ก. กฎคุณภาพข้อมูลควรซับซ้อนเท่าที่จำเป็น
- **หลักการที่ ๗ :** การเก็บรักษาและการทำซ้ำข้อมูลทำให้รักษาข้อมูลคุณภาพสูงได้ยากขึ้น อ.ต.ก. ควรเก็บรักษาและทำซ้ำข้อมูลเมื่อจำเป็นต้องใช้ข้อมูลดังกล่าว เพื่อเปิดใช้งานกรณีการใช้งานเฉพาะ

๔.๓.๒ มาตรฐานด้านคุณภาพของข้อมูล (Data Quality Standard)

มิติของแบบจำลองคุณภาพข้อมูล

อ.ต.ก. ต้องตกลงร่วมกันในคำจำกัดความของคุณภาพของข้อมูล โดยการสร้างแบบจำลองคุณภาพของข้อมูลในหลายมิติ แต่ละมิติควรระบุลักษณะความต้องการของแต่ละหน่วยงาน และความตั้งใจที่จะใช้ข้อมูลในกรณีการใช้งานจากมุมมองเชิงปฏิบัติ กรอบผลลัพธ์ต้องสนับสนุนการประเมิน คุณภาพข้อมูล โดยอ้างถึงกรอบคุณภาพข้อมูลดังต่อไปนี้

- อ.ต.ก. จะใช้มิติและมาตรการในกรอบคุณภาพข้อมูลเพื่อสร้างแบบจำลองของคุณภาพของข้อมูล
- Data Quality Lead จะต้องประสานงานกับ Data Stewards เพื่อระบุเป้าหมายด้านคุณภาพข้อมูลสำหรับแต่ละมิติในระดับโดเมนย่อยของข้อมูลและโดยรวม

Data Quality Framework

การประเมินคุณภาพข้อมูล

อ.ต.ก. ควรประเมินระดับคุณภาพข้อมูลเป็นระยะและเพื่อตอบสนองต่อเหตุการณ์ต่าง ๆ การประเมินเป็นระยะจะให้ข้อมูลที่จำเป็นในการปรับปรุงคุณภาพข้อมูลเมื่อเวลาผ่านไป และช่วยให้มั่นใจได้ว่าข้อมูลจะสามารถนำไปใช้กับกรณีการใช้งานต่าง ๆ ได้อย่างง่ายดาย การประเมินตามเหตุการณ์จะช่วยให้ อ.ต.ก. สามารถวัดคุณภาพของข้อมูลที่ได้มาใหม่ หรือสร้างขึ้นได้ ซึ่งการประเมินคุณภาพของข้อมูลต้องได้รับการสนับสนุนจากผู้บริหารจัดการข้อมูลเพื่อบังคับใช้การตรวจสอบคุณภาพของข้อมูล

- Data Quality Lead ต้องบังคับใช้กระบวนการเพื่อให้แน่ใจว่าหน่วยงานจัดทำโปรไฟล์โดเมนย่อยข้อมูลใหม่ รวมถึงการประเมินคุณภาพข้อมูล เมื่อมีการกำหนดเนื่องจากการสร้างข้อมูลใหม่หรือการนำเข้าข้อมูลใหม่จากบุคคลที่สาม

• Data Quality Lead ต้องบังคับใช้กระบวนการเพื่อให้แน่ใจว่าหน่วยงานต่าง ๆ จะประเมินคุณภาพข้อมูลของ Data Subdomain ผ่านการสุ่มตัวอย่าง อย่างน้อยปีละ ๒ ครั้ง

• เจ้าของข้อมูลต้องตรวจสอบให้แน่ใจว่าข้อมูลส่วนบุคคลนั้นถูกต้อง เป็นปัจจุบัน ครบถ้วน และไม่ก่อให้เกิดความเข้าใจผิดตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDPA)

อ.ต.ก. ควรใช้มีข้อมูลตามกรอบคุณภาพข้อมูล (Data Quality Framework) เพื่อประเมินระดับคุณภาพข้อมูลสำหรับแต่ละ Data Subdomain :

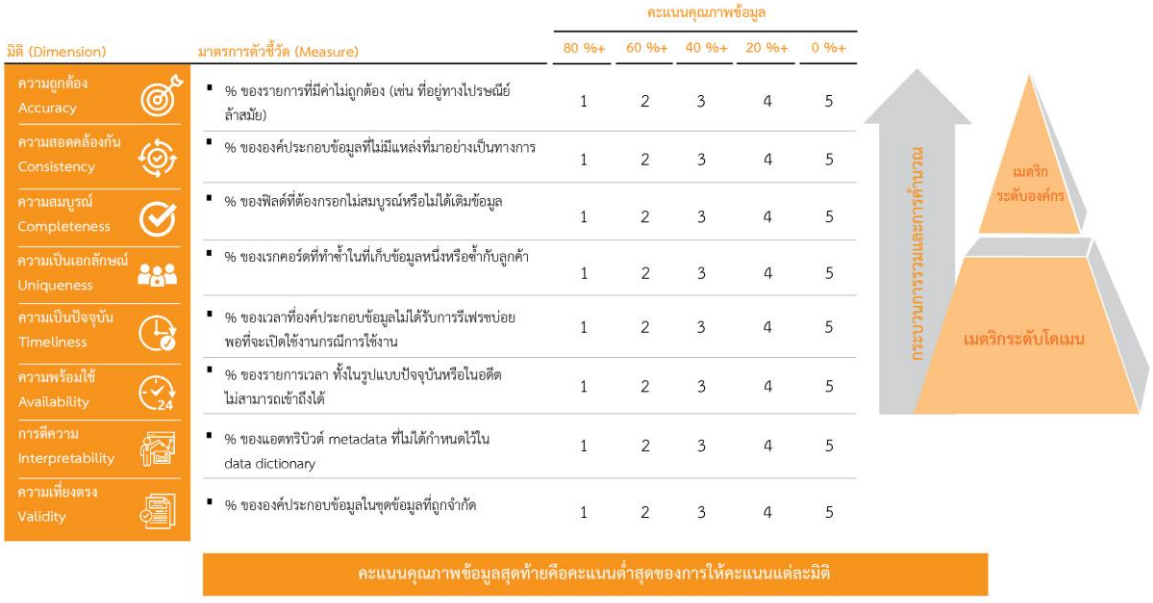
• Data Quality Lead จะใช้เกณฑ์คุณภาพข้อมูลเพื่อให้คะแนนคุณภาพข้อมูลสำหรับแต่ละ Data Subdomain และคำนวณคะแนนคุณภาพข้อมูลขั้นสุดท้าย

• Data Quality Lead จะต้องตกลงน้ำหนัก (Weight) สำหรับแต่ละมิติของกรอบคุณภาพข้อมูลกับ Data Steward สำหรับแต่ละ Data Subdomain เพื่อสะท้อนให้เห็นว่าข้อมูลนั้นถูกใช้โดยหน่วยงาน

• Data Quality Lead จะใช้วิธีการสุ่มตัวอย่างเพื่อตรวจสอบองค์ประกอบข้อมูลและประเมินคุณภาพข้อมูล าหรับแต่ละ Data Subdomain

• Data Quality Lead จะต้องประสานงานกับเจ้าของข้อมูลเพื่อทำให้กระบวนการประเมินคุณภาพข้อมูลเป็นแบบอัตโนมัติในขอบเขตที่เป็นไปได้

• Data Quality Lead จะต้องประสานงานกับ Platform Stewards เพื่อยกระดับ Data Subdomains ด้วยคะแนนคุณภาพข้อมูลขั้นสุดท้ายเท่ากับสอง (๒) หรือต่ำกว่าData Stewards จะประสานงานกับ Data Quality Lead เพื่อทำความเข้าใจบริบททางธุรกิจของข้อมูล ระบุองค์ประกอบข้อมูลที่สำคัญ และอุปกรณ์การวัดที่เหมาะสมสำหรับมีข้อมูลคุณภาพ (เช่น กำหนดสิ่งที่ประกอบขึ้นเป็นชุดข้อมูล)



Data Quality Thresholds

การแก้ไขปัญหาคุณภาพข้อมูล

คะแนนคุณภาพข้อมูลหมายความว่าข้อมูลที่หน่วยงานนั้นยังบกพร่องในกรอบคุณภาพข้อมูล ตั้งแต่หนึ่งมีดีขึ้นไป ซึ่งส่งผลเสียต่อความสามารถในการใช้งานของข้อมูล และลดทอนความสามารถของหน่วยงานในการประมวลผลหรือแบ่งปันข้อมูล เพื่อแก้ไขปัญหานี้และจึงควรทำให้แน่ใจว่าข้อมูลได้รับการจัดการในลักษณะที่ปรับการใช้งานให้เหมาะสม อ.ต.ก. ควรแก้ไขโดเมนย่อยข้อมูลที่มีคะแนนคุณภาพข้อมูลค่า ในทำนองเดียวกันควรประเมินและแก้ไขรายงานปัญหาคุณภาพข้อมูล

• Data Stewards ยกระดับโดเมนย่อยของข้อมูลที่ควรได้รับการแก้ไขไปยังผู้บริหารฝ่ายจัดการข้อมูลโดเมนย่อยข้อมูลที่มีคะแนนคุณภาพข้อมูลสอง (๒) หรือต่ำกว่าควรได้รับการแก้ไขใหม่

• Platform Stewards วิเคราะห์โดเมนย่อยข้อมูลที่ได้รับการเลื่อนระดับเพื่อระบุปัญหาด้านคุณภาพข้อมูลที่ส่งผลให้คะแนนคุณภาพข้อมูลเป็นสอง (๒) หรือต่ำกว่า

• Data Quality Lead จะต้องประเมินปัญหาคุณภาพข้อมูลที่ระบุและปัญหาที่พนักงานรายงานสำหรับความรุนแรงตามตัวเลขความรุนแรงของปัญหาคุณภาพข้อมูล และจัดลำดับความสำคัญของปัญหาคุณภาพข้อมูลที่จะวิเคราะห์

Date Quality issue Severity

• Platform Stewards จะประสานงานกับผู้บริหารฝ่ายจัดการข้อมูลเพื่อทำการวิเคราะห์สาเหตุของปัญหาด้านคุณภาพของข้อมูลที่จัดลำดับความสำคัญ และระบุสาเหตุที่เกิดปัญหาด้านคุณภาพของข้อมูล

• Data Quality Lead จะต้องจัดหมวดหมู่ปัญหาด้านคุณภาพข้อมูลตามสาเหตุที่แท้จริงโดยใช้การจำแนกของปัญหาด้านคุณภาพข้อมูล

Data entry & conversion causes	Data conversion	ข้อมูลถูกปฏิเสธหรือข้อมูลผิดประเภทหลังจากการแปลงข้อมูล เนื่องจากข้อมูลไม่เพียงพอเกี่ยวกับการตีความแหล่งข้อมูล ข้อมูลต้นฉบับอาจผิดพลาดได้
	System consolidation	ข้อมูลใหม่มักไม่เข้ากับโครงสร้างที่มีอยู่ การทับซ้อนของข้อมูล ความขัดแย้งของข้อมูล
	Manual data entry	ข้อผิดพลาดเกิดขึ้นเนื่องจากขาดสมาธิหรือแรงจูงใจ พิมพ์ผิด มีการเว้นช่องว่าง กรอกข้อมูลค่าเริ่มต้น
	Batch/ETL feeds	การเปลี่ยนแปลงโครงสร้างของโครงสร้างต้นทาง มักไม่สะท้อนให้เห็นในโปรแกรม
	Real-time interfaces	ข้อมูลที่มาถึงผ่านช่องทางเรียลไทม์จะต้องได้รับการยอมรับหรือปฏิเสธจากฐานข้อมูลทันที ข้อมูลที่ถูกต้องและเป็นข้อมูลที่ดีอาจสูญหาย ข้อมูลที่ไม่ถูกต้องอาจแพร่กระจายด้วยวิธีนี้
Direct causes	Data processing	การเปลี่ยนแปลงโปรแกรมเล็กน้อยอาจส่งผลให้เกิดความไม่สอดคล้องกัน ข้อมูลถูกแปลงและไม่พอดีกับโครงสร้างฐานข้อมูล (DB)
	Data Cleansing	ปัญหาด้านคุณภาพของข้อมูลมีความซับซ้อนและเกี่ยวเนื่องกัน การแก้ไขปัญหาหนึ่งอาจสร้างปัญหาอื่นๆ อีกมากมายในองค์ประกอบข้อมูลเดียวกันหรืออื่น ๆ ที่เกี่ยวข้องกัน
	Data purging	โครงสร้างข้อมูลเปลี่ยนแปลงและเมื่อข้อมูลถูกกำจัด มีความเสี่ยงที่ข้อมูลที่เกี่ยวข้องบางอย่างจะถูกลบโดยไม่ตั้งใจ
Indirect Causes	Changes not captured	ข้อมูลวัตถุ หรือข้อมูลส่วนบุคคลจริงอาจมีการเปลี่ยนแปลงข้อมูล (เช่น เจ้าของข้อมูลเสียชีวิต) ดังนั้นข้อมูลดังกล่าวจึงเกิดความผิดพลาด
	Systems upgrades	ฟิลด์ข้อมูลถูกใช้เพื่อวัตถุประสงค์ที่ไม่ถูกต้อง และข้อมูลบางส่วนหายไป ในขณะที่ข้อมูลอื่น ๆ ถูกทำให้อยู่ในรูปแบบที่โปรแกรมเวอร์ชันก่อนหน้ายอมรับได้
	New data uses	ข้อมูลอาจดีเพียงพอสำหรับวัตถุประสงค์หนึ่ง แต่ไม่เพียงพอสำหรับอีกวัตถุประสงค์หนึ่ง การใช้งานใหม่อาจเช่น ให้ความสำคัญกับความถูกต้องของข้อมูลมากขึ้น แม้จะไม่ได้เปลี่ยนคำจำกัดความของคุณภาพก็ตาม
	Loss of expertise	ความรู้ด้านข้อมูลส่วนใหญ่อยู่ในสกิล หรือความรู้ของพนักงาน เจ้าหน้าที่ มากกว่าเอกสาร Metadata เมื่อพนักงาน เจ้าหน้าที่เหล่านี้มีการโยกย้าย ลาออก เกษียณอายุ ข้อมูลจะไม่ถูกใช้งานอีกต่อไป
	Process automation	พนักงาน เจ้าหน้าที่ ที่การตรวจสอบข้อมูลโดยอัตโนมัติก่อนใช้งาน ส่วนโปรแกรมคอมพิวเตอร์ใช้ข้อมูลจริงที่ไม่ผ่านการตรวจสอบ และไม่สามารถตัดสินใจอย่างเหมาะสมเกี่ยวกับความเป็นไปได้ที่ข้อมูลนั้นจะถูกต้อง

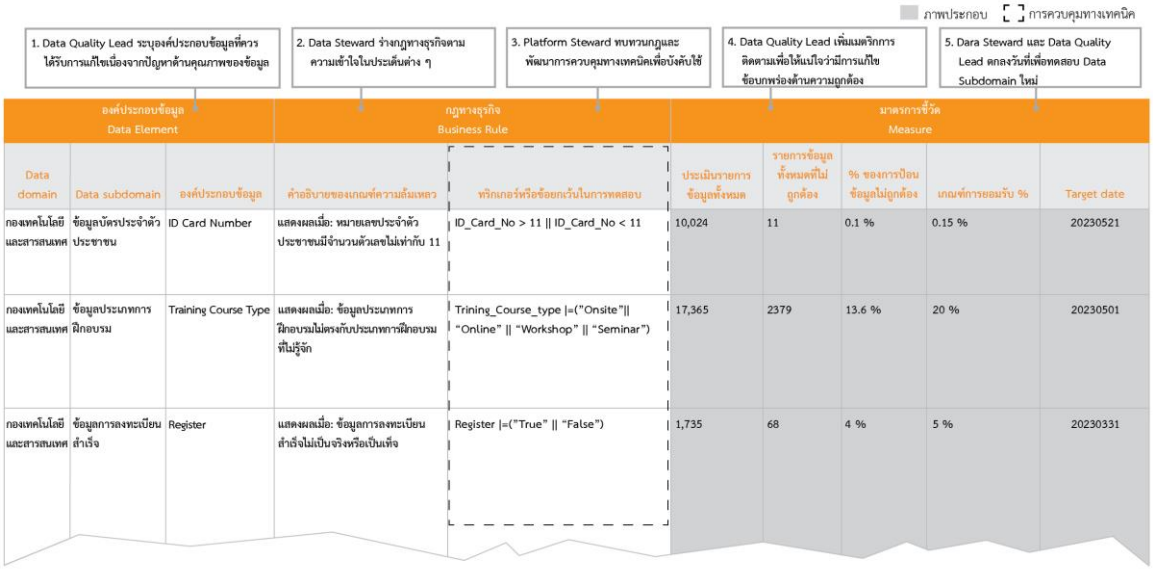
Data Quality Issue Category

• ปัญหาด้านคุณภาพข้อมูลที่เกิดจากข้อผิดพลาดในการป้อนข้อมูลหรือการแปลง Data Stewards จะต้องบังคับใช้กฎด้านคุณภาพข้อมูลสำหรับฟิลด์ข้อมูลที่ได้รับผลกระทบเพื่อให้แน่ใจว่าข้อผิดพลาดนี้จะไม่เกิดขึ้นอีกในอนาคต

• คุณภาพของข้อมูลที่เกิดจากการป้อนข้อมูลหรือข้อผิดพลาดในการแปลงข้อมูล Platform Stewards ต้องออกแบบและใช้การควบคุมทางเทคนิคเพื่อบังคับใช้กฎคุณภาพข้อมูลที่กำหนด โดย Data Stewards

• กฎคุณภาพข้อมูลจะใช้ข้อกำหนดทางธุรกิจเพื่อจำกัดองค์ประกอบข้อมูลให้อยู่ในชุดของค่าที่คาดไว้

• ปัญหาด้านคุณภาพข้อมูลที่เกิดจากการป้อนข้อมูลหรือข้อผิดพลาดในการแปลงข้อมูล Data Quality Lead จะต้องจัดทำเอกสารกฎคุณภาพข้อมูลที่สร้างขึ้นสำหรับแต่ละโดเมนย่อยของข้อมูล และยอมรับเงื่อนไขการทดสอบโดยใช้รูปแบบ เช่น เทมเพลตกฎคุณภาพข้อมูลดังต่อไปนี้



Data Quality Rules Template

• Platform Stewards จะต้องพัฒนาแผนการแก้ไขระดับสูงสำหรับปัญหาด้านคุณภาพข้อมูลแต่ละรายการ โดยอธิบายขั้นตอนที่จำเป็นในการแก้ไขปัญหาด้านคุณภาพข้อมูลด้วยเวลาและความพยายามโดยประมาณ

• Data Stewards ประสานงานกับหน่วยงานเพื่อจัดลำดับความสำคัญของปัญหาด้านคุณภาพข้อมูลที่ต้องแก้ไขตามแผนการแก้ไข

• Platform Stewards ประสานงานกับผู้บริหารฝ่ายจัดการข้อมูลเพื่อออกแบบและใช้การควบคุมทางเทคนิคเพื่อดำเนินการตามแผนการแก้ไขและป้องกันสาเหตุไม่ให้เกิดขึ้นอีกในอนาคต

การรายงานคุณภาพข้อมูล

การวัดคุณภาพข้อมูลที่รวบรวมจากโดเมนย่อยของข้อมูลควรได้รับการรวบรวมและรายงานทั่วทั้งองค์กร นอกจากนี้ควรรายงานการเปลี่ยนแปลงของเวลา (เช่น เมตริก) ทั่วทั้งองค์กรด้วย ข้อมูลเหล่านี้จะช่วยให้องค์กรเข้าใจถึงข้อมูลต่าง ๆ ที่มีอยู่ใน อ.ต.ก. นอกจากนี้ยังช่วยให้เจ้าของข้อมูล (Data Owner) Data Stewards และ Platform Stewards ประเมินกำลังที่จำเป็นในการใช้ข้อมูลต่าง ๆ

• Data Quality Lead จะรวบรวมผลการประเมินคุณภาพข้อมูลทั่วทั้งองค์กร และเผยแพร่การวิเคราะห์คะแนนคุณภาพข้อมูลขั้นสุดท้าย การเปลี่ยนแปลงเมื่อเวลาผ่านไป และกำหนดเป้าหมายโดยใช้รูปแบบ เช่น เทมเพลตรายงานคุณภาพข้อมูล

• Data Quality Lead ต้องส่งต่อผลการประเมินคุณภาพข้อมูลไปยังคณะกรรมการกำกับดูแลข้อมูลอย่างน้อยทุกไตรมาสจัดสรรทรัพยากรเพื่อแก้ไขแหล่งที่มาที่ใหญ่ที่สุดของปัญหาคุณภาพข้อมูล

Data Quality Report Template

การจัดการแหล่งข้อมูลอย่างเป็นทางการ

ปัญหาด้านคุณภาพของข้อมูลจำนวนมากเกิดขึ้นเนื่องจากการใช้ข้อมูลจากแหล่งข้อมูลที่ไม่เป็นทางการในฐานะส่วนหนึ่งของการรับประกันคุณภาพของข้อมูลใน อ.ต.ก. ผู้บริหารฝ่ายการจัดการข้อมูลควรสนับสนุนให้ธุรกิจใช้ข้อมูลจากแหล่งข้อมูลที่เป็นทางการซึ่งดูแลโดย Platform Stewards ที่ได้รับการยอมรับเท่านั้น

• เจ้าของข้อมูล (Data Owner) ต้องประสานงานกับผู้บริหารฝ่ายจัดการข้อมูลเพื่อกำหนดแผนการยกเลิกการใช้แหล่งข้อมูลที่ไม่เป็นทางการ และลดความซับซ้อนของสภาพแวดล้อม ข้อมูลใน อ.ต.ก. อย่างต่อเนื่อง

• Platform Stewards ต้องประสานงานกับผู้บริหารฝ่ายจัดการข้อมูลเพื่อให้แน่ใจว่าระบบประมวลผลข้อมูลที่ใช้ในการจัดเก็บและประมวลผลข้อมูลได้รับการออกแบบมาเพื่อรองรับมิติของคุณภาพข้อมูล

บทที่ ๕
การประมวลผลและการใช้ข้อมูล

๕.๑ แนวปฏิบัติการประมวลผลข้อมูล

• ต้องปฏิบัติตามกฎหมาย ระเบียบ ประกาศ และหลักเกณฑ์ที่เกี่ยวข้อง และให้ปฏิบัติโดยเคร่งครัดในประเด็น ดังต่อไปนี้

- ต้องปฏิบัติตามขั้นตอนการประมวลผลข้อมูลและการใช้ข้อมูลที่กำหนดขึ้น เพื่อให้มีสิทธิ์ การใช้งานระบบสารสนเทศตามความจำเป็น
- ต้องตรวจสอบความถูกต้องของข้อมูลก่อนนำไปประมวลผล
- กรณีข้อมูลมีการควบคุมโดยการเข้ารหัส (Encryption) ในการประมวลผลข้อมูลต้องบันทึกหลักฐานไว้ทุกครั้งเพื่อการตรวจสอบในภายหลัง และสามารถจัดพิมพ์เป็นรายงานเพื่อการตรวจสอบได้
- ต้องมีมาตรการรักษาความมั่นคงปลอดภัยในการประมวลผลข้อมูลที่ได้กำหนดชั้นข้อมูลตั้งแต่ลับขึ้นไปอย่างเพียงพอและมีประสิทธิภาพ

๕.๒ แนวปฏิบัติการใช้ข้อมูล

• ต้องปฏิบัติตามกฎหมาย ระเบียบ ประกาศ และหลักเกณฑ์ที่เกี่ยวข้อง และให้ปฏิบัติโดยเคร่งครัดในประเด็น ดังต่อไปนี้

- ให้ใช้ข้อมูลทั้งที่มีอยู่ภายในหน่วยงาน หรือได้รับข้อมูลจากภายนอกหน่วยงานเพื่องานในราชการเท่านั้น
- ใช้ข้อมูลเฉพาะในส่วนที่ได้รับอนุญาตตามการกำหนดสิทธิ์จากผู้ดูแลระบบคอมพิวเตอร์เท่านั้น
- กรณีข้อมูลที่มีความสำคัญหรือชั้นความลับ ต้องมีการกำหนดสิทธิ์ผู้ใช้งานและสิทธิในการเข้าถึงระยะเวลาที่นำข้อมูลไปใช้งาน วัตถุประสงค์ในการใช้งานข้อมูล
- ห้ามมิให้ใช้ข้อมูลเพื่อประโยชน์ในเชิงธุรกิจเป็นการส่วนตัว หรือใช้ข้อมูลอันอาจก่อให้เกิดความเสียหายต่อองค์กร

บทที่ ๖
การเปิดเผยข้อมูล/การเชื่อโยงข้อมูลและการรักษาความลับ

• ต้องปฏิบัติตามกฎหมาย ระเบียบ ประกาศ และหลักเกณฑ์ที่เกี่ยวข้อง และให้ปฏิบัติโดยเคร่งครัดในประเด็น ดังต่อไปนี้

- ข้อมูลมีความพร้อมในการส่งต่อหรือเปิดเผยได้ข้อมูลที่เปิดเผยควรเป็น Open by Default และ Closed by Exception โดย Open by Default จะเป็นลักษณะของ ข้อมูลที่สามารถเปิดเผยได้และไม่ละเมิดข้อมูลส่วนบุคคล เช่น ข้อมูลเชิงสถิติที่ไม่มีตัวบุคคล ในส่วน Closed by Exception เป็นลักษณะข้อมูล ส่วนบุคคลที่ไม่ควรเปิดเผย เช่น หมายเลขบัตรประจำตัวประชาชน หมายเลขบัตรเครดิต รหัสผ่านที่ใช้เข้าระบบ เป็นต้น

- ต้องมีการตรวจสอบชั้นความลับของข้อมูล (Data Classification) ว่าอยู่ในชั้นความลับ ที่สามารถเปิดเผยได้หรือไม่

- กรณีข้อมูลที่เป็นความลับ หากจำเป็นต้องแลกเปลี่ยนข้อมูล หน่วยงานปลายทางจะต้องมีการจัดทำธรรมาภิบาลข้อมูลในระดับเดียวกัน หากไม่มีการจัดทำธรรมาภิบาลข้อมูล ต้องมีการทำสัญญาอนุญาตหรือเงื่อนไขในการแลกเปลี่ยน และการนำข้อมูลไปใช้ที่ยอมรับได้ ห้ามนำไปเผยแพร่ต่อโดยเด็ดขาด

- ต้องมีการเข้ารหัสลับ (Encryption) ข้อมูลก่อนการแลกเปลี่ยนข้อมูลบางประเภท เช่น ข้อมูลความมั่นคงประเทศ

- ข้อมูลส่วนบุคคลบางรายการต้องไม่แสดงตัวตน (Anonymization) กรณีที่หน่วยงานที่ขอข้อมูลไม่มีอำนาจในการเข้าถึงข้อมูลส่วนบุคคลแต่ต้องการใช้ข้อมูลเพื่อทำการศึกษาหรือวิจัย

- มีกลไกตรวจสอบให้แน่ใจว่าการแลกเปลี่ยนข้อมูลถูกดำเนินการได้อย่างเหมาะสมหรือ เป็นไปตามแนวปฏิบัติ กระบวนการแลกเปลี่ยน และมาตรฐานที่กำหนด