ประกาศสำนักงานเศรษฐกิจการคลัง

เรื่อง นโยบายและแนวปฏิบัติการบริหารจัดการข้อมูล

ของสำนักงานเศรษฐกิจการคลัง พ.ศ. ๒๕๖๙

โดยที่สำนักงานเศรษฐกิจการคลังได้มีประกาศสำนักงานเศรษฐกิจการคลัง เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Policy) สำนักงานเศรษฐกิจการคลัง พ.ศ. ๒๕๖๘ เพื่อกำหนดมาตรฐานความปลอดภัยทางไซเบอร์ของสำนักงานเศรษฐกิจการคลังให้มีความชัดเจน เป็นไปในทิศทางเดียวกัน และสอดคล้องกับมาตรฐานสากล

เพื่อให้การบริหารจัดการข้อมูลของสำนักงานเศรษฐกิจการคลังมีมาตรฐานความปลอดภัยทางไซเบอร์สอดคล้องกับประกาศดังกล่าว จึงอาศัยอำนาจตามความในมาตรา ๓๒ แห่งพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน พ.ศ. ๒๕๓๔ ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน (ฉบับที่ ๕) พ.ศ. ๒๕๔๕ มาตรา ๓๖ และมาตรา ๓๗ แห่งพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน พ.ศ. ๒๕๓๔ ออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศสำนักงานเศรษฐกิจการคลัง เรื่อง นโยบายและแนวปฏิบัติการบริหารจัดการข้อมูลของสำนักงานเศรษฐกิจการคลัง พ.ศ. ๒๕๖๙”

ข้อ ๒ ให้ยกเลิก

(๑) ประกาศสำนักงานเศรษฐกิจการคลัง เรื่อง นโยบายและแนวปฏิบัติการบริหารจัดการข้อมูลของสำนักงานเศรษฐกิจการคลัง พ.ศ. ๒๕๖๘ ลงวันที่ ๓ เมษายน ๒๕๖๘

(๒) ประกาศสำนักงานเศรษฐกิจการคลัง เรื่อง แก้ไขเพิ่มเติมนโยบายและแนวปฏิบัติการบริหารจัดการข้อมูลของสำนักงานเศรษฐกิจการคลัง พ.ศ. ๒๕๖๘ ลงวันที่ ๒๒ พฤษภาคม ๒๕๖๘

ข้อ ๓ ให้ใช้นโยบายและแนวปฏิบัติการบริหารจัดการข้อมูลของสำนักงานเศรษฐกิจการคลัง พ.ศ. ๒๕๖๙ รายละเอียดตามแนบท้ายประกาศนี้

ข้อ ๔ ประกาศนี้ให้ใช้บังคับตั้งแต่วันที่ประกาศเป็นต้นไป

ประกาศ ณ วันที่ ๗ มีนาคม พ.ศ. ๒๕๖๙

(นายวินิจ วิเศษสุวรรณภูมิ)

ผู้อำนวยการสำนักงานเศรษฐกิจการคลัง

เอกสารแนบท้ายประกาศ

เรื่อง นโยบายและแนวปฏิบัติการบริหารจัดการข้อมูล ของสำนักงานเศรษฐกิจการคลัง พ.ศ. ๒๕๖๙

สารบัญ

บทนำ

ด้วยพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ กำหนดให้หน่วยงานของรัฐจัดให้มีการบริหารงานภาครัฐและการจัดทำบริการสาธารณะในรูปแบบและช่องทางดิจิทัลโดยมีการบริหารจัดการและการบูรณาการข้อมูลภาครัฐ เพื่อให้การทำงานมีความสอดคล้องและเชื่อมโยงเข้าด้วยกันอย่างมั่นคงปลอดภัยและมีธรรมาภิบาล ประกอบกับประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ ลงวันที่ ๑๒ มีนาคม ๒๕๖๓ กำหนดให้มีธรรมาภิบาลข้อมูลภาครัฐ เพื่อเป็นหลักการและแนวทางในการดำเนินงานให้เป็นไปตามพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ หน่วยงานของรัฐจึงต้องดำเนินการและจัดทำธรรมาภิบาลข้อมูลภาครัฐให้ระดับหน่วยงานให้สอดคล้องกับธรรมาภิบาลข้อมูลภาครัฐ

ดังนั้น สำนักงานเศรษฐกิจการคลังจึงได้จัดทำนโยบายและแนวปฏิบัติการบริหารจัดการข้อมูลของสำนักงานเศรษฐกิจการคลังขึ้น เพื่อให้การบริหารจัดการข้อมูลของสำนักงานเศรษฐกิจการคลังมีธรรมาภิบาล สามารถบูรณาการ เชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างกันได้ โดยมีการกำหนดสิทธิ หน้าที่ ความรับผิดชอบในการบริหารจัดการข้อมูลของสำนักงานเศรษฐกิจการคลัง ตั้งแต่การเก็บรวบรวม การใช้ การประมวลผล รวมถึงการเปิดเผยข้อมูลเป็นไปอย่างเหมาะสม มีประสิทธิภาพ คุณภาพ มั่นคงปลอดภัย สามารถป้องกันภัยคุกคามที่อาจจะเกิดขึ้นได้ เป็นไปตามพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒

วัตถุประสงค์

๑. เพื่อให้การบริหารจัดการข้อมูลของสำนักงานเศรษฐกิจการคลังสอดคล้องกับพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ รวมถึงกฎหมาย ประกาศ และระเบียบอื่น ๆ ที่เกี่ยวข้อง

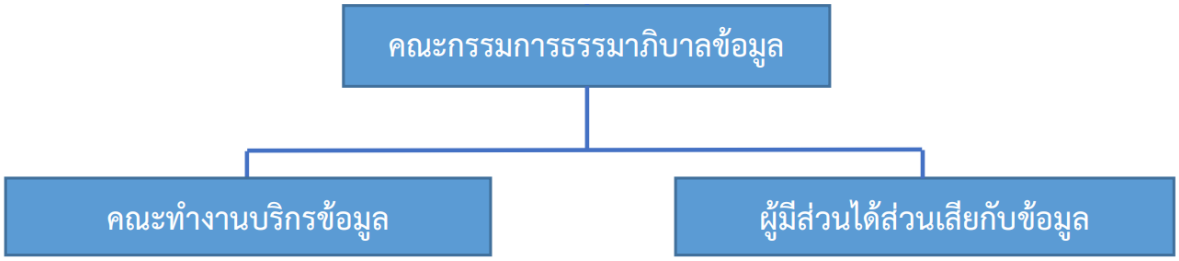
๒. เพื่อใช้เป็นกรอบและแนวปฏิบัติในการบริหารจัดการข้อมูลของสำนักงานเศรษฐกิจการคลังสำหรับผู้บริหาร บุคลากร และผู้ที่เกี่ยวข้อง

๓. เพื่อใช้เป็นแนวทางในการพัฒนาและปรับปรุงการบริหารจัดการข้อมูลให้เป็นไปตามกรอบธรรมาภิบาลข้อมูล รวมถึงการควบคุมคุณภาพของข้อมูลอย่างมีประสิทธิภาพ

หมวด ๑
ทั่วไป (General Domain)

๑. โครงสร้างธรรมาภิบาลข้อมูลของสำนักงานเศรษฐกิจการคลัง

สำนักงานเศรษฐกิจการคลังได้นำแนวทางตามกรอบธรรมาภิบาลข้อมูลภาครัฐที่ประกอบด้วยองค์ประกอบต่าง ๆ ทั้งในด้านของนิยามและกฎเกณฑ์ที่เกี่ยวข้องกับข้อมูล บุคคล และกระบวนการ ซึ่งองค์ประกอบเหล่านี้มีความสำคัญที่ก่อให้เกิดประสิทธิภาพและประสิทธิผลในการดำเนินงาน อันจะนำไปสู่การบรรลุเป้าหมายในการดำเนินงานตามที่กำหนดไว้ ซึ่งโครงสร้างการกำกับดูแลข้อมูล (Data Governance Structure) ของสำนักงานเศรษฐกิจการคลัง ประกอบด้วย ๑) คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance) ของสำนักงานเศรษฐกิจการคลัง ๒) คณะทำงานบริกรข้อมูล (Data Steward Team) ของสำนักงานเศรษฐกิจการคลัง ๓) ผู้มีส่วนได้ส่วนเสียกับข้อมูล (Data Stakeholders)



รูปที่ ๑ โครงสร้างธรรมาภิบาลข้อมูลของสำนักงานเศรษฐกิจการคลัง

๑.๑ คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance) ของสำนักงานเศรษฐกิจการคลัง

คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance) ของสำนักงานเศรษฐกิจการคลัง ประกอบด้วย ผู้อำนวยการสำนักงานเศรษฐกิจการคลัง ทำหน้าที่เป็นประธานกรรมการ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม (Department Chief Information Officer: DCIO) ประจำสำนักงานเศรษฐกิจการคลัง ทำหน้าที่เป็นรองประธานกรรมการ ผู้อำนวยการกอง/กลุ่ม ทำหน้าที่เป็นกรรมการ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ ทำหน้าที่เป็นกรรมการและเลขานุการ ผู้อำนวยการส่วนระบบข้อมูลและนวัตกรรมเทคโนโลยีสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศ ทำหน้าที่เป็นกรรมการและผู้ช่วยเลขานุการ ผู้อำนวยการส่วนโครงสร้างพื้นฐานและความมั่นคงปลอดภัย ศูนย์เทคโนโลยีสารสนเทศ ทำหน้าที่เป็นกรรมการและผู้ช่วยเลขานุการ ผู้อำนวยการส่วนกลยุทธ์เทคโนโลยีสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศ ทำหน้าที่เป็นกรรมการและผู้ช่วยเลขานุการ

มีหน้าที่และอำนาจ ดังนี้

(๑) กำหนดนโยบาย กรอบแนวทาง ทิศทางการดำเนินงาน มาตรฐานข้อมูล และจัดลำดับความสำคัญของข้อมูล เพื่อจัดทำธรรมาภิบาลข้อมูลภาครัฐของสำนักงานเศรษฐกิจการคลัง

(๒) กำกับ ดูแลการเปิดเผยข้อมูลเปิดภาครัฐ แนวทางปฏิบัติงาน เกณฑ์การวัดคุณภาพ ระเบียบ และข้อบังคับอื่น ๆ ที่เกี่ยวข้องกับข้อมูล เพื่อให้การดำเนินการธรรมาภิบาลข้อมูลภาครัฐเป็นไปอย่างมีประสิทธิภาพ

(๓) แต่งตั้งคณะอนุกรรมการ คณะทำงานบริกรข้อมูล (Data Steward Team) หรือคณะทำงานอื่น เพื่อดำเนินการให้เป็นไปตามกรอบธรรมาภิบาลข้อมูลภาครัฐ รวมถึงการดำเนินการให้เป็นไปตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

(๔) กำกับดูแล ให้ข้อเสนอแนะ และสนับสนุนการดำเนินงานของคณะทำงานบริกรข้อมูล (Data Steward Team) หรือคณะทำงานอื่นที่แต่งตั้ง

(๕) ปฏิบัติงานอื่น ๆ ที่เกี่ยวข้องกับการดำเนินงานด้านธรรมาภิบาลข้อมูลภาครัฐของสำนักงานเศรษฐกิจการคลัง ตามที่ผู้อำนวยการสำนักงานเศรษฐกิจการคลังมอบหมาย

๑.๒ คณะทำงานบริกรข้อมูล (Data Steward Team) ของสำนักงานเศรษฐกิจการคลัง

คณะทำงานบริกรข้อมูล (Data Steward Team) ของสำนักงานเศรษฐกิจการคลัง ประกอบด้วย ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ ทำหน้าที่เป็นหัวหน้าคณะทำงานบริกรข้อมูล ผู้แทนกอง/ศูนย์/กลุ่ม ที่ได้รับมอบหมายทำหน้าที่เป็นบริกรข้อมูล นักวิชาการคอมพิวเตอร์ ระดับชำนาญการหรือปฏิบัติการของศูนย์เทคโนโลยีสารสนเทศทำหน้าที่เป็นบริกรข้อมูลฝ่ายเลขานุการ

มีหน้าที่และอำนาจ ดังนี้

(๑) จัดทำร่างนโยบายข้อมูลและแนวปฏิบัติที่เกี่ยวข้องกับข้อมูล เพื่อให้ข้อมูลมีความถูกต้อง ครบถ้วน พร้อมใช้งาน เป็นปัจจุบัน และเป็นไปตามธรรมาภิบาลข้อมูลภาครัฐ

(๒) กำหนดนิยามของข้อมูล พร้อมจัดทำคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตา (Metadata) และบัญชีข้อมูล ให้ครบถ้วน และเป็นปัจจุบัน

(๓) กำหนดความต้องการด้านคุณภาพข้อมูลและความมั่นคงปลอดภัยของผู้ใช้ข้อมูลหรือผู้มีส่วนได้ส่วนเสียกับข้อมูล

(๔) ดำเนินงานให้สอดคล้องกับนโยบาย เป้าประสงค์ และความต้องการของผู้มีส่วนได้ส่วนเสียกับข้อมูล รวมทั้งติดตามการดำเนินงานตามแผนงานที่กำหนด

(๕) ทบทวนและปรับปรุงกระบวนการ เพื่อนำมาปรับปรุงกระบวนการทำงาน

(๖) รายงานการดำเนินการต่อคณะกรรมการธรรมาภิบาลข้อมูล

(๗) ปฏิบัติงานอื่น ๆ ตามที่คณะกรรมการธรรมาภิบาลข้อมูลมอบหมาย

๑.๓ ผู้มีส่วนได้ส่วนเสียกับข้อมูล (Data Stakeholders)

ผู้มีส่วนได้ส่วนเสียกับข้อมูล (Data Stakeholders) ประกอบด้วย

๑.๓.๑ เจ้าของข้อมูล (Data Owner) มีหน้าที่ความรับผิดชอบ คือ

๑) ตรวจสอบดูแลข้อมูลโดยตรง

๒) สร้างความมั่นใจว่าการบริหารจัดการข้อมูลสอดคล้องกับนโยบาย มาตรฐาน กฎระเบียบหรือกฎหมายที่เกี่ยวข้อง

๓) ทบทวนและร่วมกันอนุมัติการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับข้อมูล

๔) ทำการแก้ไข ลบ และปรับปรุงข้อมูล (Data Cleaning)

๕) ให้สิทธิในการเข้าถึงข้อมูลและจัดชั้นความลับของข้อมูลของเจ้าของข้อมูลนั้น ๆ

๑.๓.๒ ผู้สร้างข้อมูล (Data Creator) มีหน้าที่ความรับผิดชอบ คือ

๑) สร้าง บันทึก แก้ไข ปรับปรุง หรือลบข้อมูลให้สอดคล้องกับโครงสร้างที่ถูกกำหนดไว้

๒) ทำงานร่วมกับคณะทำงานบริกรข้อมูล เพื่อตรวจสอบและแก้ไขปัญหาด้านคุณภาพข้อมูลและความมั่นคงปลอดภัย

๑.๓.๓ ผู้ใช้ข้อมูล (Data Users) มีหน้าที่ความรับผิดชอบ คือ

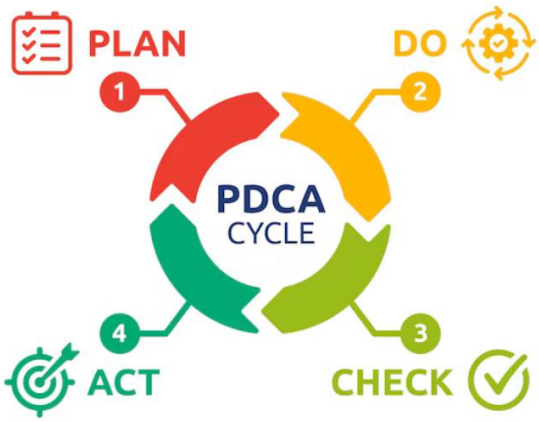
๑) นำข้อมูลไปใช้งานทั้งในระดับปฏิบัติงาน ระดับบริหารและการบริการ

๒) สนับสนุนการกำกับดูแลข้อมูลโดยการให้ข้อมูลเกี่ยวกับความต้องการในการใช้ข้อมูล

๓) รายงานประเด็นปัญหาที่พบระหว่างการใช้ข้อมูล ด้านคุณภาพและความปลอดภัยของข้อมูลไปยังคณะทำงานบริกรข้อมูล

๒. กระบวนการธรรมาภิบาลข้อมูล (Data Governance Processes)

กระบวนการธรรมาภิบาลข้อมูล เป็นขั้นตอนที่ใช้สำหรับกำกับดูแลการดำเนินการใด ๆ ต่อข้อมูลให้เป็นไปตามกฎ ระเบียบ ข้อบังคับ หรือนโยบายที่เกี่ยวข้องกับข้อมูล กระบวนการธรรมาภิบาลข้อมูล เริ่มตั้งแต่การวางแผนไปจนถึงการปรับปรุงอย่างต่อเนื่อง ดังนี้



รูปที่ ๒ กระบวนการธรรมาภิบาลข้อมูล

๒.๑ การวางแผน (Plan)

การวางแผนเริ่มตั้งแต่กำหนดวิสัยทัศน์และประเด็นปัญหา ซึ่งเป็นส่วนที่สำคัญเนื่องจากเป็นจุดเริ่มต้นที่จะกำหนดกฎระเบียบ นโยบาย มาตรฐาน หรือแนวทางปฏิบัติต่าง ๆ เพื่อใช้ในธรรมาภิบาลข้อมูลและการบริหารจัดการข้อมูล หลังจากที่ได้มีการกำหนดวิสัยทัศน์และประเด็นปัญหาอย่างชัดเจนแล้ว ขั้นตอนถัดไปคือ การกำหนดขอบเขตการดำเนินการ ระยะเวลาที่ดำเนินการ บุคคลที่เกี่ยวข้อง และต้นทุนที่ใช้ในการดำเนินงาน หลังจากนั้นนำแผนงาน กฎระเบียบ และนโยบายที่เกี่ยวข้องไปประกาศใช้อย่างเป็นทางการ

๒.๒ การปฏิบัติ (DO)

การดำเนินการใด ๆ ของบุคคลที่เกี่ยวข้องกับการบริหารจัดการข้อมูลและผู้ที่เกี่ยวข้องอื่น ๆ เช่น สถาปนิกข้อมูล นักออกแบบข้อมูล นักจัดการฐานข้อมูล วิศวกรข้อมูล นักวิเคราะห์ข้อมูล นักวิทยาการข้อมูล

เจ้าของข้อมูล เจ้าของข้อมูลส่วนบุคคล ผู้สร้างข้อมูล ผู้บริหาร ผู้ใช้ข้อมูล เป็นต้น ซึ่งต้องดำเนินการให้สอดคล้องกับกฎระเบียบ นโยบาย มาตรฐาน และแนวปฏิบัติที่ได้กำหนดไว้ ขณะที่บริกรข้อมูลจะให้ความรู้และสนับสนุนให้บุคคลที่เกี่ยวข้องสามารถปฏิบัติตามกฎระเบียบเหล่านั้น ทั้งนี้รายงานความก้าวหน้า ผลการปฏิบัติงานและประเด็นปัญหาที่พบระหว่างปฏิบัติงานจะถูกรายงานไปยังคณะกรรมการธรรมาภิบาลข้อมูล

๒.๓ การตรวจสอบ วัดผล และรายงาน (Check, Measure and Report)

คณะทำงานบริกรข้อมูลจะดำเนินการตรวจสอบความสอดคล้องกันระหว่างกฎระเบียบ นโยบายและมาตรฐานที่กำหนด กับการปฏิบัติงานของบุคคลที่เกี่ยวข้องกับการบริหารจัดการข้อมูลและผู้ที่เกี่ยวข้องอื่น ๆ พร้อมทั้งทำการวัดผลด้านคุณภาพข้อมูล หลังจากนั้นรายงานผลความสอดคล้อง คุณภาพข้อมูล ความมั่นคงปลอดภัย และความเสี่ยงที่เกี่ยวข้องกับข้อมูลไปยังคณะกรรมการธรรมาภิบาลข้อมูลและผู้ที่เกี่ยวข้องเพื่อให้ทราบถึงผลการดำเนินงานและประเด็นปัญหาที่พบ

๒.๔ การปรับปรุงอย่างต่อเนื่อง (Continual Improvement)

การดำเนินการด้านธรรมาภิบาลข้อมูลเป็นสิ่งที่ต้องดำเนินการอย่างต่อเนื่อง ทั้งนี้เมื่อสภาพแวดล้อมหรือกฎหมายที่เปลี่ยนแปลงไป การรายงานความต้องการจากผู้บริหารและผู้มีส่วนได้ส่วนเสีย รวมไปถึงผลการตรวจสอบ เช่น รายงานผลการตรวจสอบความสอดคล้องของการดำเนินงานต่อนโยบายข้อมูล รายงานคุณภาพข้อมูล รายงานความมั่นคงปลอดภัย รายงานความเสี่ยงต่อข้อมูล จะถูกใช้สำหรับการปรับปรุงกระบวนการธรรมาภิบาลข้อมูล นโยบาย กฎ ระเบียบ ข้อบังคับที่เกี่ยวข้องกับข้อมูล เกณฑ์การประเมินความพร้อมของธรรมาภิบาลข้อมูล เกณฑ์การวัดระดับคุณภาพข้อมูลและโครงสร้างธรรมาภิบาลข้อมูล เป็นต้น

๓. ขอบเขตและการนำไปใช้

นโยบายนี้จัดทำขึ้นโดยคณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council) ของสำนักงานเศรษฐกิจการคลัง เพื่อให้ผู้ทำหน้าที่ดูแลข้อมูล ผู้ใช้ข้อมูล คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council) คณะทำงานบริกรข้อมูล (Data Stewards Team) และบุคลากรอื่น ๆ ของหน่วยงานดำเนินการและปฏิบัติตามนโยบายอย่างเคร่งครัด

๔. คำนิยาม

“สำนักงาน” หมายถึง สำนักงานเศรษฐกิจการคลัง

“คณะกรรมการ” หมายถึง คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council) ของสำนักงานเศรษฐกิจการคลัง

“ทีมบริกรข้อมูล” หมายถึง คณะทำงานบริกรข้อมูล (Data Stewards Team) ของสำนักงานเศรษฐกิจการคลัง

“บริกรข้อมูล” หมายถึง ผู้แทนจากกอง/ศูนย์/กลุ่ม ให้ปฏิบัติหน้าที่ด้านธรรมาภิบาลข้อมูลและรายงานผลลัพธ์ต่อคณะกรรมการ

“บุคลากร” หมายถึง ข้าราชการ พนักงานราชการ ลูกจ้างและ/หรือ ผู้ปฏิบัติงานในสังกัดสำนักงานเศรษฐกิจการคลัง

“หัวหน้าหน่วยงาน” หมายถึง ผู้อำนวยการ รองผู้อำนวยการ ที่ปรึกษา และหัวหน้าส่วนราชการระดับกอง ศูนย์ กลุ่ม หรือผู้ที่ได้รับมอบหมาย

“ผู้รับผิดชอบที่เกี่ยวข้องกับข้อมูล” หมายถึง เจ้าหน้าที่ที่ทำหน้าที่ตรวจสอบดูแลข้อมูลโดยตรง ทำการทบทวนและอนุมัติการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับข้อมูลตามธรรมาภิบาลข้อมูลตลอดวงจรชีวิตของข้อมูล รวมถึงการให้สิทธิในการเข้าถึงข้อมูลและจัดชั้นความลับของข้อมูล

“ธรรมาภิบาลข้อมูลภาครัฐ” หมายถึง การกำหนดสิทธิ หน้าที่ และความรับผิดชอบของผู้มีส่วนได้เสียในการบริหารจัดการข้อมูลภาครัฐทุกขั้นตอน เพื่อให้การได้มาและการนำข้อมูลไปใช้ของหน่วยงานถูกต้อง ครบถ้วน เป็นปัจจุบัน รักษาความเป็นส่วนบุคคล สามารถเชื่อมโยงแลกเปลี่ยนและบูรณาการระหว่างกันได้อย่างมีประสิทธิภาพและมั่นคงปลอดภัย

“บูรณาการข้อมูล” หมายถึง การจัดทำและจัดเก็บข้อมูลตั้งแต่สองแหล่งขึ้นไป ด้วยวิธีการเชื่อมโยงหรือแลกเปลี่ยนโดยขึ้นกับลักษณะการใช้งานเป็นสำคัญ เพื่อลดความซ้ำซ้อนและใช้ประโยชน์ข้อมูลร่วมกัน ตามความพร้อมของเจ้าของข้อมูลและภารกิจขององค์กร

“การบริหารจัดการข้อมูล” หมายถึง ขั้นตอนการสร้างข้อมูล การรวบรวมข้อมูล การจัดเก็บ การจัดเก็บถาวร การทำลายข้อมูล การประมวลผลข้อมูล การใช้ข้อมูล การแลกเปลี่ยน การเชื่อมโยงข้อมูล และการเปิดเผยข้อมูลต่อสาธารณะ

“ข้อมูล” หมายถึง สิ่งที่สื่อความหมายให้รู้เรื่องราวข้อเท็จจริงหรือเรื่องอื่นใด ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใด ๆ และไม่ว่าจะได้จัดทำไว้ในรูปของเอกสาร แฟ้มรายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ภาพถ่ายดาวเทียม ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ เครื่องมือตรวจวัด การสำรวจระยะไกล หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้

“ชุดข้อมูล” หมายถึง การนำข้อมูลจากหลายแหล่งมารวบรวม เพื่อจัดเป็นชุดข้อมูลให้ตรงตามลักษณะโครงสร้างของข้อมูล

“บัญชีข้อมูล” หมายถึง เอกสารแสดงรายการของชุดข้อมูล ที่จำแนกแยกแยะโดยการจัดกลุ่มหรือจัดประเภทข้อมูลที่อยู่ในความครอบครองหรือควบคุมของหน่วยงาน

“สารสนเทศ” หมายถึง ข้อมูล ข่าวสาร ในรูปแบบต่าง ๆ เช่น ตัวอักษร ตัวเลข สัญลักษณ์ รูปภาพ เสียง ที่ผ่านกระบวนการประมวลผล และบันทึกไว้อย่างเป็นระบบตามหลักวิชาการ ในสื่อประเภทต่าง ๆ เช่น หนังสือ วารสาร หนังสือพิมพ์ วีดีโอ ซีดีรอม และฐานข้อมูลอิเล็กทรอนิกส์ เป็นต้น เพื่อนำออกเผยแพร่และใช้ประโยชน์

“วงจรชีวิตข้อมูล” หมายถึง ลำดับขั้นตอนของข้อมูล ตั้งแต่เริ่มสร้างข้อมูลไปจนถึงการทำลายข้อมูลตามกรอบธรรมาภิบาลข้อมูลภาครัฐ

“การกู้คืนข้อมูล (Restore)” หมายถึง กระบวนการที่ทำให้ข้อมูลที่สูญหาย หรือเสียหายและข้อมูลที่ไม่สามารถใช้งานได้จากสื่อบันทึกข้อมูลให้กลับมาใช้งานได้ตามปกติ ซึ่งผลสำเร็จในการกู้คืนข้อมูลจะมากหรือน้อยนั้นขึ้นอยู่กับสาเหตุที่ทำให้ข้อมูลนั้นใช้การไม่ได้ และการกระทำกับข้อมูลหลังจากที่เกิดความเสียหาย

“ข้อมูลเปิด (Open Data)” หมายถึง ข้อมูลที่สามารถเปิดเผยได้ สามารถนำไปใช้ได้อย่างอิสระ ไม่ว่าจะเป็นข้อมูลข่าวสาร ข้อมูลส่วนบุคคล ข้อมูลอิเล็กทรอนิกส์ เป็นต้น สามารถนำกลับมาใช้ใหม่และแจกจ่ายได้โดยใครก็ตาม แต่ต้องระบุแหล่งที่มาหรือเจ้าของงาน

“ข้อมูลส่วนบุคคล (Personal Data)” หมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

“เขตข้อมูล (Field)” หมายถึง กลุ่มของอักขระที่สัมพันธ์กัน ตั้งแต่ ๑ ตัวขึ้นไปที่นำมารวมกันแล้วแสดงลักษณะหรือความหมายอย่างใดอย่างหนึ่ง สามารถแยกประเภทของฟิลด์ได้เป็น ๓ ประเภท คือ ๑) ฟิลด์ตัวเลข (numeric field) ประกอบด้วย อักขระที่เป็นตัวเลขซึ่งอาจเป็นเลขจำนวนเต็มหรือทศนิยม และอาจมีเครื่องหมายลบหรือบวก เช่น ยอดคงเหลือในบัญชีเป็นกลุ่มของตัวเลข ๒) ฟิลด์ตัวอักษร (alphabetic field) ประกอบด้วยอักขระที่เป็นตัวอักษรหรือช่องว่าง (blank) เช่น ชื่อลูกค้าเป็นกลุ่มของตัวอักษร และ ๓) ฟิลด์อักขระ (character field หรือ alphanumeric field) ประกอบด้วยอักขระซึ่งอาจจะเป็นตัวเลขหรือตัวอักษรก็ได้ เช่น ที่อยู่ของลูกค้า

“คำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตา (Metadata)” หมายถึง ข้อมูลที่ใช้อธิบายข้อมูลหลักหรือกลุ่มข้อมูลอื่น ๆ ที่เกี่ยวข้องทั้งกระบวนการเชิงธุรกิจ (เมทาดาตาเชิงธุรกิจ) และเชิงเทคโนโลยีสารสนเทศ (เมทาดาตาเชิงเทคนิค) กฎและข้อจำกัดของข้อมูล และโครงสร้างของข้อมูล เมทาดาตาช่วยให้หน่วยงานสามารถเข้าใจข้อมูล ระบบ และขั้นตอนการทำงานที่เกิดขึ้นกับข้อมูลได้ดียิ่งขึ้น

“คุณภาพของข้อมูล (Data Quality)” หมายถึง เครื่องมือในการวัดความน่าเชื่อถือและประสิทธิภาพของการนำข้อมูลไปใช้ ประกอบด้วย การวางแผน การดำเนินการ และการควบคุมกิจกรรมต่าง ๆ รวมถึงการปรับปรุงเพื่อให้ข้อมูลมีคุณภาพ ประกอบด้วย ข้อมูลมีความถูกต้อง (accuracy) ความครบถ้วน (completeness) ความสอดคล้องกัน (consistency) ความเป็นปัจจุบัน (timeliness) ความตรงตามต้องการของผู้ใช้ (relevancy) และความพร้อมใช้ (availability)

“เจ้าของข้อมูล (Data Owners)” หมายถึง บุคคลที่ทำหน้าที่รับผิดชอบดูแลข้อมูลโดยตรงเพื่อสร้างความมั่นใจได้ว่าการบริหารจัดการข้อมูลสอดคล้องกับนโยบาย มาตรฐาน กฎระเบียบ หรือกฎหมาย ทำการทบทวนและอนุมัติการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับข้อมูล และให้สิทธิ์ในการเข้าถึงข้อมูลและจัดชั้นความลับของข้อมูล

“เจ้าของข้อมูลส่วนบุคคล (Personal Data Subject)” หมายถึง ตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคล แต่ไม่ใช่กรณีที่บุคคลที่ครอบครองข้อมูล หรือเป็นผู้สร้างหรือเก็บรวบรวมข้อมูลนั้นเอง โดยเจ้าของข้อมูลส่วนบุคคลจะหมายถึงบุคคลธรรมดาเท่านั้นและไม่รวมถึงนิติบุคคล

“ผู้ควบคุมข้อมูลส่วนบุคคล (Personal Data Controller)” หมายถึง บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

“ผู้ใช้ข้อมูล (Data Users)” หมายถึง บุคคลที่ทำหน้าที่นำข้อมูลไปใช้งานทั้งในระดับปฏิบัติงานและระดับบริหาร และสนับสนุนธรรมาภิบาลข้อมูลภาครัฐโดยการให้ความต้องการในการใช้ข้อมูล พร้อมทั้งรายงานประเด็นปัญหาที่พบระหว่างการใช้ข้อมูลทั้งด้านคุณภาพและความปลอดภัยของข้อมูลไปยังบริกรข้อมูล

“ผู้สร้างข้อมูล (Data Creators)” หมายถึง บุคคลที่ทำหน้าที่บันทึก แก้ไข ปรับปรุง หรือลบข้อมูลให้สอดคล้องกับโครงสร้างที่ถูกกำหนดไว้ นอกจากนี้ยังมีหน้าที่ในการทำงานร่วมกับบริกรข้อมูลเพื่อตรวจสอบและแก้ไขปัญหาด้านคุณภาพและความมั่นคงปลอดภัยของข้อมูล

“ผู้ทำลายข้อมูล (Data Disposer)” หมายถึง บุคคลที่ได้รับการกำหนดสิทธิจากเจ้าของข้อมูลให้มีสิทธิในการทำลายข้อมูล

“ผู้ดูแลระบบสารสนเทศ (System Administrators)” หมายถึง บุคคลที่ทำหน้าที่หรือได้รับมอบหมายให้ดูแลรับผิดชอบระบบสารสนเทศของหน่วยงาน

“ผู้ดูแลระบบแม่ข่าย (Server Administrators)” หมายถึง บุคคลที่ทำหน้าที่ดูแลรับผิดชอบระบบแม่ข่ายของหน่วยงาน

“หมวดหมู่ของข้อมูล (Data Category)” ตามกรอบธรรมาภิบาลข้อมูลภาครัฐแบ่งออกได้เป็น ๕ หมวดหมู่ ได้แก่ ข้อมูลสาธารณะ ข้อมูลใช้ภายใน ข้อมูลส่วนบุคคล ข้อมูลความลับทางราชการ และข้อมูลความมั่นคง

“การจัดชั้นความลับของข้อมูล (Data Classification)” หมายถึง การกำหนดประเภทและข้อกำหนดของการจัดชั้นความลับของข้อมูล เพื่อกำหนดสิทธิในการเข้าถึงและสามารถนำข้อมูลไปใช้ได้อย่างเหมาะสม ตามพระราชบัญญัติข้อมูลข่าวสารของราชการพ.ศ. ๒๕๔๐ และระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ รวมถึงระเบียบหรือแนวปฏิบัติที่เกี่ยวข้องในการกำหนดชั้นความลับของข้อมูล โดยคำนึงถึงการปฏิบัติหน้าที่ของหน่วยงานและประโยชน์แห่งรัฐประกอบกัน ดังนั้น ชั้นความลับของข้อมูลมักถูกกำหนดให้สอดคล้องกับผลกระทบต่อหน่วยงานและความมั่นคงของประเทศ อาทิ ชื่อเสียง ความต่อเนื่องของการดำเนินงาน การเงิน และทรัพยากรบุคคล

๕. กฎหมายและระเบียบต่าง ๆ ที่เกี่ยวข้อง

๕.๑ พระราชบัญญัติ/พระราชกำหนด

- พระราชบัญญัติข้อมูลข่าวสารราชการ พ.ศ. ๒๕๔๐
- พระราชบัญญัติลิขสิทธิ์ (ฉบับที่ ๒) พ.ศ. ๒๕๕๘
- พระราชบัญญัติการอำนวยความสะดวกในการพิจารณาอนุญาตของทางราชการ พ.ศ. ๒๕๕๘
- พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐
- พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒
- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒
- พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒
- พระราชกำหนดว่าด้วยการประชุมผ่านสื่ออิเล็กทรอนิกส์ พ.ศ. ๒๕๖๓
- พระราชบัญญัติการปฏิบัติราชการทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๖๕

๕.๒ ระเบียบ

- ระเบียบสำนักนายกรัฐมนตรีว่าด้วยงานสารบรรณ พ.ศ. ๒๕๒๖ และที่แก้ไขเพิ่มเติม
- ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ และที่แก้ไขเพิ่มเติม
- ระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. ๒๕๕๒ และที่แก้ไขเพิ่มเติม

๕.๓ ประกาศ

- ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๕๐

- ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓

- ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ พ.ศ. ๒๕๖๓

- ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง มาตรฐานและหลักเกณฑ์การเปิดเผยข้อมูลเปิดภาครัฐในรูปแบบข้อมูลดิจิทัลต่อสาธารณะ พ.ศ. ๒๕๖๓

- ประกาศสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ที่ ม ๑/๒๕๖๕ เรื่อง มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ว่าด้วยหลักเกณฑ์การจัดระดับชั้นและแบ่งปันข้อมูลภาครัฐ

- ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง มาตรฐานรัฐบาลดิจิทัลว่าด้วยหลักเกณฑ์การประเมินคุณภาพข้อมูลสำหรับหน่วยงานภาครัฐ พ.ศ. ๒๕๖๖

- ประกาศสำนักงานเศรษฐกิจการคลัง เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Policy) ของสำนักงานเศรษฐกิจการคลัง พ.ศ. ๒๕๖๘

- ประกาศสำนักงานเศรษฐกิจการคลัง เรื่อง นโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของสำนักงานเศรษฐกิจการคลัง พ.ศ. ๒๕๖๗

- ประกาศสำนักงานเศรษฐกิจการคลัง เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลของสำนักงานเศรษฐกิจการคลัง พ.ศ. ๒๕๖๘

๖. นโยบายการบริหารจัดการข้อมูล

๖.๑ ข้อกำหนดทั่วไป

๖.๑.๑ นโยบายบริหารจัดการข้อมูลของสำนักงานเศรษฐกิจการคลังต้องจัดทำเป็นลายลักษณ์อักษรและต้องได้รับการอนุมัติเพื่อประกาศใช้และถือปฏิบัติทั่วทั้งสำนักงาน โดยให้มีผลบังคับใช้กับบุคลากรในทุกระดับชั้นของสำนักงาน

๖.๑.๒ กำหนดให้มีแนวปฏิบัติเพื่อสนับสนุนการปฏิบัติงานให้สอดคล้องตามนโยบายข้อมูลและทบทวนแนวปฏิบัติให้เป็นตามพระราชบัญญัติและระเบียบที่บังคับใช้

๖.๑.๓ กำหนดให้มีมาตรฐานหรือวิธีปฏิบัติที่เกี่ยวกับข้อมูล ได้แก่ มาตรฐานการจัดชั้นความลับของข้อมูล เพื่อจัดลำดับความสำคัญของข้อมูลให้มีความมั่นคงปลอดภัยด้านสารสนเทศอย่างเหมาะสม

๖.๑.๔ ผู้อำนวยการสำนักงาน หรือผู้ที่ได้รับมอบอำนาจ มีอำนาจกำหนดบทบาทหน้าที่และความรับผิดชอบตามโครงสร้างธรรมาภิบาลข้อมูล

๖.๑.๕ กำหนดให้ผู้อำนวยการกอง/ศูนย์/กลุ่ม หรือผู้ที่ได้รับมอบหมาย เป็นผู้กำหนดสิทธิการบริหารจัดการข้อมูลที่อยู่ในขอบเขตความรับผิดชอบของตน ทั้งนี้ โดยให้เป็นไปตามการปฏิบัติและอำนาจหน้าที่ความรับผิดชอบของกอง/ศูนย์/กลุ่ม นั้น

๖.๑.๖ กำหนดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูล เพื่อป้องกันการละเมิด การเข้าถึง การสูญหาย การทำลาย หรือการเปลี่ยนแปลงข้อมูล โดยปราศจากอำนาจโดยมิชอบ หรือโดยมิได้รับอนุญาต

๖.๑.๗ กำหนดให้มีมาตรการ วิธีการ และแนวปฏิบัติในการคุ้มครองข้อมูลข่าวสารส่วนบุคคลข้อมูลส่วนบุคคล และข้อมูลในความรับผิดชอบของสำนักงาน

๖.๑.๘ กำหนดให้ตรวจสอบความมีอยู่และรายละเอียดของข้อมูลที่สำคัญ เช่น คำอธิบายข้อมูลหรือเมทาดาตา ชุดข้อมูล และการจัดชั้นความลับข้อมูล เป็นต้น ให้แก่ผู้รับผิดชอบตามโครงสร้างธรรมาภิบาลข้อมูลทราบ และดำเนินการตามกระบวนการธรรมาภิบาลข้อมูลภาครัฐ

๖.๑.๙ กำหนดให้มีการตรวจสอบการปฏิบัติตามนโยบายข้อมูล โดยผู้ตรวจประเมินของสำนักงาน และติดตามผลการประเมินเพื่อปรับปรุง ป้องกัน หรือแก้ไขปัญหาที่พบอย่างต่อเนื่อง

๖.๑.๑๐ กำหนดให้มีการทบทวนนโยบายบริหารจัดการข้อมูลในทุก ๓ ปี หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ และปรับปรุงอย่างต่อเนื่อง

๖.๑.๑๑ กำหนดให้มีการวัดผลการดำเนินการและความสำเร็จของธรรมาภิบาลข้อมูลอย่างน้อยปีละ ๑ ครั้ง โดยมีการวัดผลอย่างน้อยในเรื่องดังต่อไปนี้ (๑) การประเมินความพร้อมธรรมาภิบาลข้อมูล (๒) การประเมินคุณภาพข้อมูล และ (๓) การประเมินความมั่นคงปลอดภัยของข้อมูล

๖.๑.๑๒ กำหนดให้มีการจัดทำระบบบัญชีข้อมูลตามกรอบมาตรฐานการจัดทำบัญชีข้อมูลภาครัฐ

๖.๑.๑๓ กำหนดให้มีการเผยแพร่ประชาสัมพันธ์นโยบายข้อมูลให้แก่บุคคลหรือหน่วยงานที่เกี่ยวข้องทั้งภายในและภายนอก รวมทั้งผู้มีส่วนได้ส่วนเสีย เพื่อให้มีความรู้ความเข้าใจต่อการปฏิบัติตามนโยบายข้อมูล

๖.๑.๑๔ จัดให้มีทรัพยากรด้านงบประมาณ ทรัพยากรบุคคล และการบริหารจัดการเทคโนโลยีที่เพียงพอต่อการบริหารจัดการข้อมูล และส่งเสริมการนำระบบเทคโนโลยีสารสนเทศหรือระบบอัตโนมัติมาใช้เพื่อการเปิดเผยข้อมูลตามหลักการจัดทำธรรมาภิบาลข้อมูลภาครัฐ

๖.๑.๑๕ สนับสนุนให้มีการฝึกอบรมเพื่อสร้างความตระหนักถึงธรรมาภิบาลข้อมูลภาครัฐและการบริหารจัดการข้อมูล โดยให้ครอบคลุมทุกกระบวนการของการบริหารจัดการและวงจรชีวิตของข้อมูล

๖.๒ การจัดหมวดหมู่และชั้นความลับของข้อมูล

๖.๒.๑ กำหนดหมวดหมู่และประเภทชั้นความลับของข้อมูล ทั้งเอกสารกระดาษและข้อมูลดิจิทัล พร้อมทั้งกำหนดบทบาทหน้าที่ของบุคลากรในการสร้าง/จัดเก็บ การใช้ และการเข้าถึงชุดข้อมูลจัดหมวดหมู่และชั้นความลับ เพื่อป้องกันการเข้าถึงข้อมูลโดยผู้ที่ไม่ได้รับอนุญาต

๖.๒.๒ ติดป้ายกำกับชั้นความลับข้อมูล (ถ้ามี) เช่น ลับ ลับมาก ลับที่สุด เป็นต้น เพื่อจำแนกความแตกต่างของชุดข้อมูลภายในหน่วยงานหรือแนวปฏิบัติตามข้อกำหนดอื่น ๆ

๖.๒.๓ กำกับดูแลและติดตามอย่างต่อเนื่อง โดยตรวจสอบความปลอดภัยการใช้งานและรูปแบบการเข้าถึงของระบบและข้อมูล ทั้งผ่านกระบวนการอัตโนมัติหรือโดยบุคคล เพื่อระบุภัยคุกคามภายนอก การบำรุงรักษาการทำงานของระบบตามปกติ และการติดตั้งโปรแกรมเพื่อปรับปรุงและติดตามการเปลี่ยนแปลงของสภาพ แวดล้อมของระบบและข้อมูล

๖.๓ การบริหารจัดการข้อมูลตามวงจรชีวิตของข้อมูล

๖.๓.๑ กำหนดนโยบาย แนวปฏิบัติ และสภาพแวดล้อมการบริหารจัดการข้อมูลตามวงจรชีวิตของข้อมูล ที่เอื้อต่อการรักษาความมั่นคงปลอดภัย คุ้มครองความเป็นส่วนตัวของข้อมูล และเพื่อให้ได้ข้อมูลที่มีคุณภาพ

๖.๓.๒ จัดเก็บข้อมูลให้สอดคล้องกับแนวทางหรือมาตรฐานการจัดชั้นความลับของข้อมูลที่กำหนดไว้

๖.๔ คุณภาพข้อมูล

๖.๔.๑ กำหนดนโยบายการจัดการคุณภาพข้อมูล เพื่อใช้เป็นกรอบแนวทางในการจัดการข้อมูลของหน่วยงานให้มีคุณภาพเป็นตามเกณฑ์หรือคุณสมบัติที่กำหนด เช่น ความถูกต้องสมบูรณ์ ความสอดคล้องกัน (Consistency) ความเป็นปัจจุบัน ตรงตามความต้องการใช้งาน และความพร้อมใช้ เป็นต้น

๖.๔.๒ จัดทำเกณฑ์คุณภาพข้อมูลที่สามารถวัดผลได้

๖.๔.๓ ประเมินผลและจัดการคุณภาพข้อมูลอย่างสม่ำเสมอตลอดวงจรชีวิตของข้อมูล

หมวด ๒

แนวปฏิบัติการบริหารจัดการข้อมูล

๑. หลักการและขอบเขต

แนวปฏิบัติการบริหารจัดการข้อมูล ได้กำหนดขึ้นให้สอดคล้องตามนโยบายข้อมูล (Data Policy) ที่หน่วยงานประกาศ ซึ่งเป็นหนึ่งในองค์ประกอบตามกรอบธรรมาภิบาลข้อมูลภาครัฐ มีผลบังคับใช้กับผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับข้อมูลตามนโยบายและแนวปฏิบัติการบริหารจัดการข้อมูลที่สำนักงานเศรษฐกิจการคลังประกาศ ซึ่งมีหน้าที่โดยตรงที่จะต้องสนับสนุน ดำเนินการและปฏิบัติตามอย่างเคร่งครัด และผู้ใช้อื่นที่เกี่ยวข้องแต่ไม่มีหน้าที่ในการดูแลข้อมูลจะต้องให้ความร่วมมือในการดำเนินการตามแนวปฏิบัตินี้ ผู้ฝ่าฝืนมีความผิดและจะต้องได้รับการดำเนินการตามระเบียบของหน่วยงาน โดยแนวปฏิบัติจะต้องครอบคลุมระบบบริหารและกระบวนการจัดการข้อมูล หรือวงจรชีวิตของข้อมูลและองค์ประกอบในการบริหารจัดการข้อมูล

๒. วงจรชีวิตของข้อมูล

วงจรชีวิตของข้อมูล คือ ลำดับขั้นตอนของข้อมูลตั้งแต่เริ่มสร้างข้อมูลหรือการได้มาซึ่งข้อมูล การบริหารจัดการ การใช้ประโยชน์จากขั้นตอนไปจนถึงการเก็บข้อมูลถาวรหรือทำลายข้อมูล ประกอบด้วย ๖ ขั้นตอน ดังนี้

(๑) การสร้างข้อมูลและรวบรวมข้อมูล (Create) เป็นการสร้างข้อมูลขึ้นมาใหม่ หรือปรับปรุงข้อมูลขึ้นใหม่ โดยวิธีการบันทึกเข้าไปด้วยบุคคลหรือบันทึกอัตโนมัติด้วยอุปกรณ์อิเล็กทรอนิกส์ เช่น อุปกรณ์ตรวจจับสัญญาณ (Sensor) รวมถึงการซื้อข้อมูล หรือการรับข้อมูลจากหน่วยงานอื่น เพื่อนำมาจัดเก็บในภายหลัง

(๒) การจัดเก็บข้อมูล (Store) เป็นการจัดเก็บข้อมูลที่เกิดจากกระบวนการสร้างหรือข้อมูลที่ได้จากการเชื่อมโยงและ/หรือแลกเปลี่ยนกับหน่วยงานอื่น ไม่ว่าจะจัดเก็บลงแฟ้มข้อมูล (File) หรือระบบการจัดการฐานข้อมูล (Database Management System: DBMS) เพื่อให้เกิดความมีระเบียบ ง่ายต่อการใช้งาน ข้อมูลไม่สูญหายหรือถูกทำลาย และช่วยให้ผู้ใช้งานสามารถประมวลผลข้อมูลต่าง ๆ ตามความต้องการได้อย่างรวดเร็ว

(๓) การประมวลผลและใช้ข้อมูล (Processing and Use) เป็นการนำข้อมูลที่จัดเก็บมาประมวลผล เช่น การถ่ายโอนข้อมูล การเปลี่ยนรูปแบบการจัดเก็บข้อมูล การวิเคราะห์ข้อมูล การจัดทำรายงาน เพื่อนำข้อมูลเหล่านั้นมาใช้งานให้เกิดประโยชน์ตามวัตถุประสงค์ รวมถึงการสำรอง (Backup) ข้อมูล โดยการคัดลอกข้อมูลที่ใช้งานอยู่ในปัจจุบัน เพื่อทำสำเนา เช่น ใช้โปรแกรมในการสำรองข้อมูล เป็นการหลีกเลี่ยงความเสียหายที่จะเกิดขึ้นหากข้อมูลเกิดการเสียหายหรือสูญหาย ซึ่งสามารถนำข้อมูลที่สำรองไว้ในสื่อบันทึกข้อมูลกลับมาใช้งานได้ทันทีโดยการกู้คืน (Restore)

(๔) การเผยแพร่ข้อมูลหรือการเปิดเผยข้อมูล (Disclosure) เป็นการนำข้อมูลที่อยู่ในความครอบครองของหน่วยงาน เผยแพร่ตามช่องทางต่าง ๆ อย่างเหมาะสม อาทิ การเปิดเผยข้อมูล (Open data) การแชร์ข้อมูล (Sharing) การกระจายข้อมูล (Dissemination) การควบคุมการเข้าถึง (Access Control) และการกำหนดเงื่อนไขในการนำข้อมูลไปใช้ (Condition)

(๕) กระบวนการจัดเก็บข้อมูลถาวร (Archive) เป็นการย้ายข้อมูลที่มีช่วงอายุเกินช่วงใช้งานหรือไม่ได้ใช้งานแล้ว เพื่อเก็บรักษาถาวรโดยที่ข้อมูลนั้นไม่มีการลบ ปรับปรุง หรือแก้ไขอีก และสามารถนำกลับไปใช้งานได้ใหม่เมื่อต้องการ

(๖) การทำลายข้อมูล (Destroy) เป็นการทำลายข้อมูลที่มีการจัดเก็บถาวรเป็นระยะเวลานานหรือเกินกว่าระยะเวลาที่กำหนด

(๗) การเชื่อมโยงและแลกเปลี่ยนข้อมูล (Linkage and Exchange) การเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงานทั้งภายในและภายนอกให้มีความมั่นคงปลอดภัยและข้อมูลมีคุณภาพ สามารถนำไปใช้ประโยชน์ได้อย่างมีประสิทธิภาพ

๓. หมวดหมู่ของข้อมูล (Data Category)

การจำแนกหมวดหมู่ของข้อมูล เป็นการดำเนินการเพื่อกำหนดนโยบายข้อมูลหรือกฎเกณฑ์เกี่ยวกับผู้มีสิทธิเข้าถึงและใช้ประโยชน์จากข้อมูลต่าง ๆ ภายในหน่วยงาน รวมถึงเป็นการกำหนดให้ผู้ซึ่งมีหน้าที่เกี่ยวข้องปฏิบัติตามนโยบายหรือกฎเกณฑ์ได้อย่างถูกต้อง และสอดคล้องตามกฎหมายที่เกี่ยวข้อง อันจะนำไปสู่การบริหารจัดการข้อมูลภาครัฐอย่างเป็นระบบ

การจำแนกหมวดหมู่ของข้อมูลของสำนักงานเศรษฐกิจการคลังอ้างอิงตามเอกสารมาตรฐานรัฐบาลดิจิทัลว่าด้วยกรอบธรรมาภิบาลข้อมูลภาครัฐ ฉบับปรับปรุง: แนวปฏิบัติ เวอร์ชัน ๒.๐ เลขที่ มรด. ๖ : ๒๕๖๖ แนบท้ายประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง มาตรฐานรัฐบาลดิจิทัลว่าด้วยกรอบธรรมาภิบาลข้อมูลภาครัฐ ฉบับปรับปรุง: แนวปฏิบัติ สามารถแบ่งข้อมูลออกได้เป็น ๕ หมวดหมู่ ดังนี้

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

(๒) ข้อมูลใช้ภายใน (Internal Use Only) หมายความว่า ข้อมูลสำหรับใช้ในการดำเนินกิจการภายในของหน่วยงานซึ่งไม่อนุญาตให้นำไปใช้งานภายนอกก่อนได้รับอนุญาตจากเจ้าของข้อมูล เช่น ร่างนโยบาย ร่างมาตรฐาน และขั้นตอนการปฏิบัติงาน ประกาศ และบันทึกภายในหน่วยงานที่อยู่ระหว่างการขออนุมัติ เป็นต้น

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

(๔) ข้อมูลความลับทางราชการ (Classified Information) หมายความว่า ข้อมูลข่าวสารตามมาตรา ๑๔ หรือมาตรา ๑๕ แห่งพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐ ที่มีคำสั่งไม่ให้เปิดเผยและอยู่ในความครอบครองหรือควบคุมดูแลของหน่วยงานของรัฐ ไม่ว่าจะเป็นเรื่องที่เกี่ยวกับการดำเนินงานของรัฐหรือที่เกี่ยวกับเอกชน ซึ่งมีการกำหนดให้มีชั้นความลับเป็น ชั้นลับ ชั้นลับมาก หรือ ชั้นลับที่สุด ตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ และที่แก้ไขเพิ่มเติม โดยคำนึงถึงการปฏิบัติหน้าที่ของหน่วยงานของรัฐและประโยชน์แห่งรัฐประกอบกัน

(๕) ข้อมูลความมั่นคง (National Security Information) หมายความว่า ข้อมูลภายใต้กรอบความมั่นคงแห่งชาติ หรือภาวะที่ประเทศปลอดจากภัยคุกคามต่อเอกราช อธิปไตยบูรณภาพแห่งอาณาเขต สถาบันศาสนา สถาบันพระมหากษัตริย์ ความปลอดภัยของประชาชน การดำรงชีวิต โดยปกติสุขของประชาชน หรือที่กระทบต่อผลประโยชน์แห่งชาติหรือการปกครองระบอบประชาธิปไตย อันมีพระมหากษัตริย์ทรงเป็นประมุขรวมทั้งความพร้อมของประเทศที่จะเผชิญสถานการณ์ต่าง ๆ อันเกิดจากภัยคุกคามทุกรูปแบบและครอบคลุมด้านความมั่นคงปลอดภัยของประเทศ (National Security) ในมิติเศรษฐกิจ อาหาร สุขภาพ

สิ่งแวดล้อมและสิทธิมนุษยชน ส่วนบุคคล ชุมชน การเมือง และการต่างประเทศ ที่สอดคล้องตามเป้าหมายของนโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ

ทั้งนี้ กรณีที่ชุดข้อมูลประกอบด้วยข้อมูลมากกว่า ๑ ประเภทให้เลือกหมวดหมู่ธรรมาภิบาลข้อมูลภาครัฐที่ต้องให้ความคุ้มครองสูงสุด

๔. การจัดระดับชั้นข้อมูล

การจัดระดับชั้นข้อมูลจะช่วยให้สำนักงานเศรษฐกิจการคลังสามารถกำกับดูแลข้อมูลที่มีคุณค่าได้อย่างมีประสิทธิภาพ เพื่อให้สามารถบรรลุเป้าหมายด้านความเป็นส่วนตัว (Privacy) และความปลอดภัย (Security) ของข้อมูล รวมทั้งสามารถใช้งานข้อมูลได้อย่างถูกต้องเหมาะสม ตลอดจนสามารถแบ่งปันข้อมูล (Data Sharing) ระหว่างหน่วยงานภาครัฐโดยไม่ขัดต่อข้อกฎหมายที่เกี่ยวข้อง

การจัดระดับชั้นข้อมูลของสำนักงานเศรษฐกิจการคลังอ้างอิงตามเอกสารมาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ว่าด้วยหลักเกณฑ์การจัดระดับชั้นข้อมูลและแบ่งปันข้อมูลภาครัฐ เลขที่ มสพร. ๘ - ๒๕๖๕ แนบท้ายประกาศสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ที่ ม ๑/๒๕๖๕ เรื่อง มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ว่าด้วยหลักเกณฑ์การจัดระดับชั้นและแบ่งปันข้อมูลภาครัฐ สามารถแบ่งระดับชั้นข้อมูลได้ ๕ ระดับ ดังนี้

(๑) ชั้นเปิดเผย (Open) สู่สาธารณะ เป็นข้อมูลข่าวสารของราชการที่หน่วยงานของรัฐต้องเปิดเผยให้ประชาชนได้รับรู้ รับทราบ หรือตรวจสอบได้โดยไม่จำเป็นต้องร้องขอ เช่น ข่าวประชาสัมพันธ์ รายงานเศรษฐกิจ ข้อมูลการจัดซื้อจัดจ้าง ข้อมูลการรับสมัครงาน ข้อมูลแถลงข่าว ข้อมูลกฎหมายที่อยู่ในความรับผิดชอบของ สศค. ที่ประกาศในราชกิจจานุเบกษาแล้ว รายงานผลการศึกษาทางวิชาการ และข้อมูลเปิดภาครัฐ เป็นต้น

(๒) ชั้นเผยแพร่ภายในองค์กร (Private) เปิดเผยเมื่อได้รับอนุญาต เป็นข้อมูลที่องค์กรไม่ได้เผยแพร่โดยอิสระ โดยทั่วไปจะเกี่ยวข้องกับข้อมูลที่มีลักษณะเป็นส่วนตัว (Private) ไม่ว่าจะเป็นข้อมูลบุคคลหรือองค์กร และแม้ว่าการสูญเสียข้อมูลหรือการเปิดเผยข้อมูลอาจไม่ส่งผลให้เกิดผลกระทบที่สำคัญ แต่ก็ไม่พึงประสงค์ที่ให้เปิดเผยโดยไม่ได้รับอนุญาต เช่น นโยบายและแนวปฏิบัติภายในหน่วยงาน เอกสารหรือคู่มือประกอบการปฏิบัติงาน และวิธีปฏิบัติภายในหน่วยงาน เป็นต้น

(๓) ชั้นลับ (Confidential) เปิดเผยเมื่อได้รับอนุญาต เป็นข้อมูลที่มีระดับ Confidential หรือ Sensitive จะก่อให้เกิดความสูญเสีย หากมีการเปิดเผยต่อบุคคล/องค์กรที่ไม่ได้รับอนุญาตและส่งผลให้เกิดความอับอายอย่างมากต่อบุคคล/องค์กร และอาจเป็นผลทางกฎหมาย หรือจะก่อให้เกิดความเสียหายแก่ผลประโยชน์แห่งรัฐ เช่น ข้อมูลการฟ้องคดี และความเห็นภายในหน่วยงานที่ยังไม่ได้ข้อยุติ เป็นต้น

(๔) ชั้นลับมาก (Secret) เปิดเผยเมื่อได้รับอนุญาต เป็นข้อมูลที่จัดระดับ Secret หรือ Medium Sensitive สงวนไว้สำหรับข้อมูลที่จะก่อให้เกิดความสูญเสีย/ผลกระทบร้ายแรง อาจทำให้เสียชื่อเสียง และการสูญเสียทางการเงิน/ทรัพย์สิน ต่อความมั่นคงและผลประโยชน์แห่งรัฐอย่างร้ายแรง หรือที่มีนัยสำคัญ (Importance) หากสูญหายหรือเปิดเผยอย่างไม่ถูกต้องเหมาะสม เช่น การเจรจาข้อตกลงที่สำคัญกับหน่วยงานอื่น รายงานการตรวจสอบที่เกี่ยวข้องกับผลประโยชน์แห่งรัฐ ข้อมูลความสัมพันธ์ระหว่างประเทศ และนโยบายสำคัญที่ใช้ปฏิบัติต่อรัฐต่างประเทศ เป็นต้น

(๕) ชั้นลับที่สุด (Top Secret) เปิดเผยไม่ได้ เป็นข้อมูลที่จัดระดับ Top Secret หรือ Highly Sensitive จำกัดการใช้/ไม่เปิดเผยสำหรับข้อมูลที่จะก่อให้เกิดความสูญเสีย/ผลกระทบ ร้ายแรงที่สุดอาจทำให้ชื่อเสียงและการสูญเสียทางการเงิน/ทรัพย์สิน ต่อความมั่นคงและผลประโยชน์แห่งรัฐอย่างร้ายแรงหรือที่สำคัญยิ่งยวด (Vital) หากสูญหายหรือเปิดเผยอย่างไม่ถูกต้องเหมาะสม เช่น ข้อมูลมาตรการหรือนโยบายที่สำคัญยิ่งของหน่วยงาน ซึ่งถ้าเปิดเผยก่อนเวลาอันสมควร อาจก่อให้เกิดผลเสียหายร้ายแรงต่อผลประโยชน์แห่งรัฐ เป็นต้น

๕. แนวปฏิบัติการบริหารจัดการข้อมูลตามวงจรชีวิตของข้อมูล

แนวปฏิบัติการบริหารจัดการข้อมูลตามวงจรชีวิตข้อมูล โดยแบ่งออกเป็น ๖ หมวด ได้แก่ การสร้างข้อมูล การจัดเก็บข้อมูล การประมวลผลข้อมูลและการใช้ข้อมูล การเชื่อมโยงและการแลกเปลี่ยนข้อมูล การเปิดเผยข้อมูล และการทำลายข้อมูล ในแต่ละหมวดจะระบุ วัตถุประสงค์ ผู้รับผิดชอบงาน ข้อปฏิบัติ และตารางแสดงความสัมพันธ์ระหว่างกระบวนการ/กิจกรรมและผู้มีส่วนได้ส่วนเสีย

๕.๑ การสร้างข้อมูล

วัตถุประสงค์

กำหนดแนวปฏิบัติสำหรับผู้ที่เกี่ยวข้องในการสร้างข้อมูลให้มีคุณภาพ มีความมั่นคงปลอดภัย และเป็นประโยชน์ต่อผู้ใช้ข้อมูล

ผู้รับผิดชอบงาน

๑. ผู้สร้างข้อมูล (Data Creators)

๒. คณะทำงานบริกรข้อมูล (Data Stewards Team)

๓. เจ้าของข้อมูล (Data Owners)

๔. บริกรข้อมูล (Data Stewards)

๕. ผู้ดูแลระบบสารสนเทศ (System Administrators)

ข้อปฏิบัติ

๑. เจ้าของข้อมูล *(ไม่ว่า เจ้าของข้อมูล จะอยู่ภายใน กอง/ศูนย์/กลุ่ม เดียว หรือ มากกว่าหลายกอง/กอง/ศูนย์/กลุ่ม ต้องมีการกำหนดชัดเจน ถึงอำนาจหน้าที่และขั้นตอนการทำงานร่วมกัน)*

๑.๑. กำหนดผู้มีสิทธิในการสร้างข้อมูล และจะต้องทบทวนสิทธินั้น อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ เช่น การลาออก เปลี่ยนตำแหน่ง โอนย้าย สิ้นสุดการจ้าง การปรับโครงสร้าง หรือเมื่อมีการปรับปรุงระบบสารสนเทศ เป็นต้น

๑.๒. กำหนดหมวดหมู่และชั้นความลับของข้อมูล

๒. ผู้ดูแลระบบสารสนเทศจะต้องกำหนดสิทธิในการสร้างข้อมูลในระบบให้แก่ผู้สร้างข้อมูลตามที่เจ้าของข้อมูลกำหนด

๓. เจ้าของข้อมูล บริกรข้อมูล และคณะทำงานบริกรข้อมูล ร่วมจัดทำคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตา (Metadata) ให้มีความถูกต้อง ครบถ้วนและเป็นปัจจุบัน ตามมาตรฐานขั้นต่ำคำอธิบายชุดข้อมูลดิจิทัลที่สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.) กำหนด

๔. ห้ามมิให้ผู้สร้างข้อมูลนำข้อมูลที่มีลักษณะดังต่อไปนี้เข้าสู่ระบบคอมพิวเตอร์ที่ขัดต่อกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์

- ข้อมูลที่บิดเบือน หรือปลอมไม่ว่าทั้งหมดหรือบางส่วน
- ข้อมูลอันเป็นเท็จ ที่น่าจะเกิดความเสียหายต่อการรักษาความมั่นคงปลอดภัย ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจ หรือ โครงสร้างพื้นฐาน หรือก่อให้เกิดความตื่นตระหนก
- ข้อมูลอันเป็นความผิดเกี่ยวกับความมั่นคง หรือความผิดเกี่ยวกับการก่อการร้าย
- ข้อมูลที่มีลักษณะอันลามก และคนทั่วไปอาจเข้าถึงได้
- ข้อมูลที่ปรากฏภาพของผู้อื่น และเป็นภาพที่สร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ ทำให้ผู้อื่นเสียชื่อเสียง ถูกดูหมิ่นถูกเกลียดชัง หรือได้รับความอับอาย

๕. ห้ามมิให้ผู้สร้างข้อมูล ทำการสร้าง/ทำซ้ำต่อข้อมูลที่ขัดต่อกฎหมายว่าด้วยลิขสิทธิ์หรือทรัพย์สินทางปัญญาของผู้อื่น เว้นแต่จะเป็นไปตามอำนาจที่กฎหมายรับรอง

๖. กำหนดให้ผู้สร้างข้อมูลสร้างข้อมูลที่มาจากแหล่งข้อมูลที่เชื่อถือได้เท่านั้น

๗. กำหนดให้เจ้าของข้อมูลตรวจสอบความถูกต้องของข้อมูลที่ถูกสร้างขึ้น

กิจกรรม	ผู้มีส่วนได้ส่วนเสีย				
	ผู้สร้างข้อมูล	คณะทำงานบริกรข้อมูล	เจ้าของข้อมูล	บริกรข้อมูล	ผู้ดูแลระบบสารสนเทศ
กำหนดผู้มีสิทธิในการสร้างข้อมูล และกำหนดหมวดหมู่และชั้นความลับ	I	I	R	C	S
กำหนดสิทธิในการสร้างข้อมูลในระบบให้แก่ผู้สร้างข้อมูล	I	I	S	I	R
สร้างข้อมูลที่ไม่ขัดต่อกฎหมายและจากแหล่งข้อมูลที่เชื่อถือได้เท่านั้น	R	I	C	C	S
จัดทำคำอธิบายชุดข้อมูลดิจิทัล	S	S	R	R	S
ประเมินคุณค่าของชุดข้อมูลดิจิทัล	I	I	R	R	I
ตรวจสอบความถูกต้องของข้อมูล	R	I	R	C	S

ตารางที่ ๑ ตัวอย่างผู้มีส่วนได้ส่วนเสียในการสร้างข้อมูล

หมายเหตุ

R (Responsible) หมายถึง ผู้มีหน้าที่ในการปฏิบัติงานตามกระบวนการหรือกิจกรรมที่กำหนดไว้
A (Accountable) หมายถึง ผู้มีหน้าที่ในการทบทวนและอนุมัติผลที่ได้รับจากการปฏิบัติงาน
S (Supportive) หมายถึง ผู้ที่มีหน้าที่ในการสนับสนุนหรือให้การช่วยเหลือต่อการปฏิบัติงาน
C (Consulted) หมายถึง ผู้ที่ทำหน้าที่ให้คำปรึกษาต่อผู้ปฏิบัติงาน
I (Informed) หมายถึง ผู้ที่ทำหน้าที่รับทราบผลการปฏิบัติงาน

๕.๒ การจัดเก็บข้อมูลและการจัดเก็บข้อมูลถาวร

วัตถุประสงค์

กำหนดแนวปฏิบัติสำหรับผู้ที่เกี่ยวข้องในการจัดเก็บข้อมูล ให้มีคุณภาพ เข้าถึงและใช้งานได้อย่างมั่นคงปลอดภัย

ผู้รับผิดชอบงาน

๑. เจ้าของข้อมูล (Data Owners)

๒. ผู้ดูแลระบบสารสนเทศ (System Administrators)

๓. ผู้สร้างข้อมูล (Data Creators)

๔. บริกรข้อมูล (Data Stewards)

๕. ผู้ใช้ข้อมูล (Data Users)

๖. คณะทำงานบริกรข้อมูล (Data Stewards Team)

ข้อปฏิบัติ

๑. การกำหนดชั้นความลับของข้อมูล ให้ดำเนินการตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ และที่แก้ไขเพิ่มเติม

๒. จัดเก็บให้สอดคล้องกับแนวทางหรือการจัดชั้นความลับของข้อมูลที่กำหนดไว้เพื่อให้ข้อมูลมีความมั่นคงปลอดภัย และรักษาคุณภาพของข้อมูล

๓. กำหนดสิทธิการเข้าถึงข้อมูลและเครื่องมือที่ใช้ในการเข้าถึงข้อมูล

๔. กำหนดให้เจ้าของข้อมูลจะต้องกำหนดระยะเวลาในการจัดเก็บข้อมูลที่ชัดเจน

๕. กำหนดให้บริกรข้อมูล และผู้ดูแลระบบสารสนเทศทำการย้ายข้อมูลที่มีการจัดเก็บเกินระยะเวลาที่กำหนดแล้วเพื่อจัดเก็บเป็นข้อมูลถาวร

๖. จัดเก็บข้อมูลให้สอดคล้องกับกระบวนงานและวัตถุประสงค์ในการดำเนินงาน โดยข้อมูลต้องมีความถูกต้อง สมบูรณ์ และเป็นปัจจุบัน โดยจัดทำเมทาดาตาสำหรับชุดข้อมูลที่มีการจัดเก็บ

๗. จัดเก็บข้อมูลตามการจัดชั้นความลับของหน่วยงาน โดยมีการกำหนดสิทธิผู้ที่สามารถเข้าถึงข้อมูลได้เพื่อเป็นการป้องกันไม่ให้ผู้ไม่มีสิทธิในการเข้าถึงข้อมูล เข้าถึงข้อมูลได้

๘. กำหนดให้มีวิธีปฏิบัติการกู้คืนข้อมูลที่จัดเก็บถาวร สำหรับข้อมูลที่มีความสำคัญมากต่อการดำเนินงานของหน่วยงาน เพื่อสอบทานความถูกต้อง ครบถ้วน ความพร้อมใช้งาน คุณภาพข้อมูล

๙. ในการจัดเก็บข้อมูลส่วนบุคคล**ให้เก็บรวบรวมได้เท่าที่จำเป็น** ภายใต้อำนาจหน้าที่และวัตถุประสงค์อันชอบด้วยกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล และ**ไม่เก็บรวบรวมข้อมูลส่วนบุคคล** ดังต่อไปนี้ เว้นแต่ได้รับการยินยอมจากเจ้าของข้อมูลส่วนบุคคล หรือพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล หรือกฎหมายอื่นบัญญัติให้กระทำได้

- เชื้อชาติ
- เผ่าพันธุ์
- ความคิดเห็นทางการเมือง
- ความเชื่อในลัทธิ ศาสนาหรือปรัชญา
- พฤติกรรมทางเพศ
- ประวัติอาชญากรรม
- ข้อมูลสุขภาพ ความพิการ หรือข้อมูลสุขภาพจิต
- ข้อมูลสหภาพแรงงาน
- ข้อมูลพันธุกรรม
- ข้อมูลชีวภาพ

- ข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลในทำนองเดียวกันตามที่หน่วยงานกำหนด

๑๐. กำหนดให้มีการยกเลิกการจัดเก็บข้อมูลส่วนบุคคลกรณีเจ้าของข้อมูลส่วนบุคคลถอนความยินยอมตามที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลกำหนด

๑๑. ในกรณีที่มีการประชุมหรือธุรกรรมออนไลน์ กำหนดให้มีการจัดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่า ๙๐ วัน นับแต่วันที่ข้อมูลเข้าสู่ระบบคอมพิวเตอร์ โดยจัดเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการนับแต่เริ่มใช้บริการให้สอดคล้องตามกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์และในการจัดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ให้สอดคล้องตามกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์

๑๒. กำหนดให้มีมาตรการรักษาความปลอดภัยในการจัดเก็บข้อมูล รวมทั้งกรณีที่มีการเคลื่อนย้ายอุปกรณ์ที่จัดเก็บข้อมูล เพื่อป้องกันมิให้มีการเข้าถึงโดยมิได้รับอนุญาต หรือลักลอบนำข้อมูลไปใช้ที่ก่อให้เกิดความเสียหายต่อหน่วยงาน

๑๓. กำหนดมาตรการรักษาความปลอดภัยของข้อมูลที่จัดเก็บถาวร เพื่อป้องกันข้อมูลไม่ให้มีการลบ ปรับปรุง แก้ไขได้ รวมทั้งป้องกันมิให้ข้อมูลที่จัดเก็บถาวรรั่วไหลไปยังบุคคลที่ไม่ได้รับอนุญาต

๑๔. กำหนดให้มีมาตรการรักษาความปลอดภัยของการถ่ายโอนข้อมูลกับหน่วยงานภายนอกที่ผ่านช่องทางการสื่อสารทุกชนิด โดยต้องสอดคล้องตามนโยบายและแนวปฏิบัติความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy) ของสำนักงานเศรษฐกิจการคลัง พ.ศ. ๒๕๖๘

๑๕. ห้ามมิให้จัดเก็บข้อมูลที่ไม่เกี่ยวข้องกับการดำเนินงานของหน่วยงานบนเครื่องแม่ข่ายที่หน่วยงานจัดสรรไว้

๑๖. กำหนดให้มีการทบทวนเกี่ยวกับช่วงระยะเวลาการจัดเก็บข้อมูล มาตรการ และวิธีปฏิบัติที่เกี่ยวข้องกับการจัดเก็บข้อมูลถาวร อย่างน้อยปีละ ๑ ครั้ง

กิจกรรม	**ผู้มีส่วนได้ส่วนเสีย**					
	เจ้าของข้อมูล	**ผู้ดูแลระบบสารสนเทศ**	**ผู้สร้างข้อมูล**	**ผู้ใช้ข้อมูล**	**บริกรข้อมูล**	**คณะทำงานบริกรข้อมูล**
กำหนดระยะเวลาในการจัดเก็บข้อมูล	R	S	S	I	I	S
ย้ายข้อมูลที่มีการจัดเก็บเกินระยะเวลาที่กำหนด	I/C	R	I	I	I	R
จัดทำคำอธิบายชุดข้อมูลดิจิทัลและปรับปรุงให้เป็นปัจจุบัน	A	S	R	I	R	R
จัดเก็บข้อมูลตามการจัดชั้นความลับของหน่วยงาน	R	S	R	I	C	S
จัดเก็บข้อมูลส่วนบุคคลเท่าที่จำเป็น	R	R/S	S	R	C	S
ยกเลิกการจัดเก็บข้อมูลส่วนบุคคลกรณีเจ้าของข้อมูลส่วนบุคคลถอนความยินยอม	R	R	I	I	I	I
จัดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์	I	R	I	I	I	I

ตารางที่ ๒ ตัวอย่างผู้มีส่วนได้ส่วนเสียในการจัดเก็บข้อมูล

หมายเหตุ R = Responsible A = Accountable S = Supportive C = Consulted และ I = Informed

๕.๓ การประมวลผลข้อมูลและการใช้ข้อมูล

วัตถุประสงค์

กำหนดแนวปฏิบัติในการประมวลผลข้อมูลและการใช้ข้อมูลที่มีประสิทธิภาพถูกต้อง ตรงตามวัตถุประสงค์ เพื่อให้เกิดประโยชน์สูงสุด

ผู้รับผิดชอบงาน

๑. เจ้าของข้อมูล (Data Owners)

๒. ผู้ใช้ข้อมูล (Data Users)

๓. ผู้ดูแลระบบสารสนเทศ (System Administrators)

ข้อปฏิบัติ

๑. เจ้าของข้อมูลจะต้องกำหนดผู้มีสิทธิเข้าถึงเพื่อประมวลผลและใช้ข้อมูลตามชั้นความลับ

๒. ผู้ดูแลระบบสารสนเทศจะต้องกำหนดสิทธิในการเข้าถึงข้อมูลในระบบเพื่อประมวลผลและใช้ข้อมูลของผู้ใช้งานตามที่เจ้าของข้อมูลกำหนด

๓. เจ้าของข้อมูลจะต้องทบทวนสิทธิการเข้าถึงเพื่อประมวลผลและใช้ข้อมูลของผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ เช่น การลาออก เปลี่ยนตำแหน่ง โอนย้าย สิ้นสุดการจ้าง การปรับโครงสร้าง หรือเมื่อมีการปรับปรุงระบบสารสนเทศ

๔. ผู้ที่มีสิทธิเข้าใช้งานข้อมูลที่มีชั้นความลับตามที่กำหนดโดยเจ้าของข้อมูลจะต้องใช้ข้อมูลอย่างระมัดระวัง โดยคำนึงถึงความปลอดภัยและต้องไม่ใช้งานข้อมูลที่มีชั้นความลับในพื้นที่สาธารณะ และผู้ใช้ข้อมูลต้องเป็นผู้รับผิดชอบ หากมีการประมวลผลข้อมูลและการใช้ข้อมูลที่ไม่เป็นไปตามกฎหมายกำหนด

๕. ผู้ใช้ข้อมูลจะประมวลผลข้อมูลหรือใช้ข้อมูลส่วนบุคคลเท่าที่จำเป็นภายใต้อำนาจหน้าที่และวัตถุประสงค์อันชอบด้วยกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล หรือตามคำสั่งที่ได้รับจากหน่วยงานเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคล

๖. หน่วยงานต้องยกเลิกการประมวลผลข้อมูลหรือการใช้ข้อมูลส่วนบุคคล กรณีที่เจ้าของข้อมูลส่วนบุคคลถอนความยินยอมตามที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลกำหนด

๗. ผู้ใช้ข้อมูลจะต้องไม่ใช้ข้อมูลในเครือข่ายของหน่วยงานเพื่อประโยชน์ในเชิงธุรกิจเป็นการส่วนตัว หรือเพื่อเข้าสู่เว็บไซต์ที่ไม่เหมาะสมหรือใช้ข้อมูลอันก่อให้เกิดความเสียหายต่อหน่วยงาน

๘. ต้องมีการบันทึกประวัติการประมวลผลและการใช้ข้อมูล เพื่อให้สามารถตรวจสอบย้อนหลังได้

กิจกรรม	ผู้มีส่วนได้ส่วนเสีย		
	เจ้าของข้อมูล	ผู้ใช้ข้อมูล	ผู้ดูแลระบบสารสนเทศ
กำหนดสิทธิในการประมวลผลและใช้งานข้อมูลตามชั้นความลับ	R	I	S
กำหนดสิทธิในการประมวลผลและเข้าใช้งานข้อมูลในระบบ	R	I	S
ไม่ใช้ข้อมูลในเครือข่ายของหน่วยงานเพื่อประโยชน์ในเชิงธุรกิจเป็นการส่วนตัว	I	R	S
ประมวลผลข้อมูลหรือใช้ข้อมูลส่วนบุคคลเท่าที่จำเป็น	C	R	S
ยกเลิกการประมวลผลข้อมูลหรือการใช้ข้อมูลส่วนบุคคล กรณีที่เจ้าของข้อมูลส่วนบุคคลถอนความยินยอม	A	R	S

ตารางที่ ๓ ตัวอย่างผู้มีส่วนได้ส่วนเสียในการประมวลผลและใช้ข้อมูล

หมายเหตุ R = Responsible A = Accountable S = Supportive C = Consulted และ I = Informed

๕.๔ การเผยแพร่ข้อมูลหรือการเปิดเผยข้อมูล

วัตถุประสงค์

กำหนดแนวปฏิบัติการเปิดเผยข้อมูลต่อสาธารณะโดยอิงจากกฎหมาย กฎเกณฑ์และแนวปฏิบัติที่เกี่ยวข้อง ทั้งนี้ข้อมูลที่เปิดเผยควรเป็นประโยชน์ สามารถนำไปประมวลผลและใช้ต่อยอดในการพัฒนาในรูปแบบต่าง ๆ ได้

ผู้รับผิดชอบงาน

๑. เจ้าของข้อมูล (Data Owners)

๒. ผู้ใช้ข้อมูล (Data Users)

๓. บริกรข้อมูล (Data Stewards)

๔. คณะทำงานบริกรข้อมูล (Data Stewards Team)

ข้อปฏิบัติ

๑. เจ้าของข้อมูลจะต้องเปิดเผยข้อมูลในความรับผิดชอบต่อสาธารณะตามกฎหมายว่าด้วยข้อมูลข่าวสารของราชการ และมาตรฐานและหลักเกณฑ์การเปิดเผยข้อมูลเปิดภาครัฐในรูปแบบข้อมูลดิจิทัลต่อสาธารณะ

๒. เจ้าของข้อมูลทำการเปิดเผยข้อมูลในความรับผิดชอบในรูปแบบข้อมูลเปิดของหน่วยงานโดยดำเนินการดังนี้

๒.๑ คัดเลือกข้อมูลที่ต้องการเผยแพร่ ให้ปฏิบัติ ดังนี้

๒.๑.๑ เจ้าของข้อมูลและหน่วยงานที่เกี่ยวข้องต้องพิจารณาข้อมูลที่จะเผยแพร่โดยข้อมูลที่สามารถเผยแพร่ได้จะต้องไม่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ คำสั่งของสำนักงาน

๒.๑.๒ ควรเป็นข้อมูลที่สามารถเปิดเผยได้ และไม่ละเมิดข้อมูลส่วนบุคคล เช่น ข้อมูลเชิงสถิติที่ไม่สามารถระบุตัวบุคคลได้ เป็นต้น แต่ในส่วนข้อมูลส่วนบุคคลที่ไม่เปิดเผย เช่น เลขประจำตัวประชาชน เป็นต้น

๒.๒ กำหนดให้เจ้าของข้อมูลคัดเลือกข้อมูลที่จะเปิดเผยในรูปแบบข้อมูลเปิดจากลำดับชั้นความสำคัญของชุดข้อมูลที่มีคุณค่าสูง (High Value Dataset) โดยต้องมีรายละเอียดที่อธิบายถึงความเป็นมาของข้อมูล เช่น ชื่อข้อมูล คำอธิบายข้อมูล คำสำคัญ วันที่ทำการเปลี่ยนแปลงข้อมูลล่าสุด ชื่อหน่วยงานเจ้าของข้อมูล

และฟิลด์ข้อมูล เป็นต้น ทั้งนี้ ต้องตรวจสอบฟิลด์ข้อมูลว่าครบถ้วนและสอดคล้องกับความต้องการของหน่วยงานที่ขอใช้ข้อมูล

๒.๓ การจัดเตรียมข้อมูลให้อยู่ในรูปแบบที่ง่ายต่อการนำไปใช้ ให้ปฏิบัติ ดังนี้

๒.๓.๑ ข้อมูลมีความพร้อมในการส่งต่อหรือเปิดเผยได้

๑) ต้องมีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย การเข้าถึง การใช้ การเปลี่ยนแปลง การแก้ไข หรือการเปิดเผยข้อมูลส่วนบุคคล โดยปราศจากอำนาจหรือโดยมิชอบ

๒) กรณีที่ต้องให้ข้อมูลส่วนบุคคลแก่บุคคลหรือหน่วยงานอื่นที่มิใช่เจ้าของข้อมูลส่วนบุคคล ต้องดำเนินการเพื่อป้องกันมิให้ผู้นั้นนำไปใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบด้วยประการใด ๆ

๒.๓.๒ การเชื่อมโยงข้อมูลที่มีการจัดเก็บและสามารถเข้าถึงได้เพื่อการตรวจสอบหรือเปิดเผยแก่ผู้ที่เกี่ยวข้อง

๒.๔ การนำชุดข้อมูลขึ้นเผยแพร่ ให้ดำเนินการ ดังนี้

๒.๔.๑ เก็บประวัติ (Log) การเปิดเผย เผยแพร่ข้อมูล เพื่อให้สามารถตรวจสอบได้ และเป็นไปตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

๒.๔.๒ มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหายการเข้าถึง การใช้ การเปลี่ยนแปลง การแก้ไข

๒.๔.๓ เจ้าของข้อมูลต้องกำหนดรอบระยะเวลาในการตรวจสอบและปรับปรุงข้อมูลที่เปิดเผยเพื่อให้ข้อมูลถูกต้อง และเป็นปัจจุบัน

๓. กำหนดให้เงื่อนไขและข้อกำหนดของข้อมูลที่นำมาเปิดเผยภายในเครือข่ายของหน่วยงาน ข้อมูลที่เผยแพร่ต้องไม่ขัดต่อกฎหมายว่าด้วยทรัพย์สินทางปัญญา เว้นแต่การเปิดเผยข้อมูลจะเป็นไปตามอำนาจที่กฎหมายรับรอง

๔. สนับสนุนการจัดทำบัญชีข้อมูลหน่วยงานและการลงทะเบียนบัญชีข้อมูลภาครัฐ โดยบริหารจัดการข้อมูลสำคัญ จัดทำบัญชีข้อมูลของหน่วยงาน และทำการลงทะเบียนบัญชีข้อมูลของหน่วยงานและชุดข้อมูลสำคัญเข้าสู่ระบบบัญชีข้อมูลภาครัฐ (Government Data Catalog หรือ GD Catalog) เพื่อการเปิดเผยข้อมูลภาครัฐที่เป็นระบบ และมีเอกภาพ สามารถสืบค้นชุดข้อมูล คำอธิบายชุดข้อมูล รวมไปถึงแหล่งต้นทางของชุดข้อมูลภาครัฐที่สำคัญ สนับสนุนการใช้ประโยชน์ข้อมูลภาครัฐร่วมกัน

๕. กำหนดให้เปิดเผยข้อมูลส่วนบุคคลตามข้อกำหนดของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ หรือตามคำสั่งที่ได้รับจากหน่วยงานเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติในกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

๖. เจ้าของข้อมูลห้ามเปิดเผยข้อมูลความมั่นคงและข้อมูลความลับทางราชการที่อยู่ในความครอบครองของหน่วยงาน รวมทั้งห้ามเปิดเผยข้อมูลที่เป็นการกระทำความผิดตามกฎหมาย นโยบาย และแนวปฏิบัติอันทำให้เกิดความเสียหายต่อหน่วยงาน

กิจกรรม	ผู้มีส่วนได้ส่วนเสีย			
	เจ้าของข้อมูล	ผู้ใช้ข้อมูล	บริกรข้อมูล	คณะทำงานบริกรข้อมูล
จะต้องเปิดเผยข้อมูลในความรับผิดชอบต่อสาธารณะตามกฎหมาย/มาตรฐานที่เกี่ยวข้อง	R	I	C	S
คัดเลือกข้อมูลที่จะเปิดเผยในรูปแบบข้อมูลเปิดจากลำดับชั้นความสำคัญของ High Value Dataset	R	I	C	S
ตรวจสอบคำอธิบายชุดข้อมูลดิจิทัลที่จะทำการเปิดเผยให้มีความครบถ้วนเป็นปัจจุบัน	A	I	R	R
เปิดเผยข้อมูลส่วนบุคคลตามข้อกำหนดของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และห้ามเปิดเผยข้อมูลความมั่นคงและข้อมูลความลับทางราชการ รวมถึงข้อมูลที่เป็นการกระทำความผิดตามกฎหมาย	R	R	C	S
กำหนดรอบระยะเวลาในการตรวจสอบและปรับปรุงข้อมูลที่เปิดเผย	R	I	I	I

ตารางที่ ๔ ตัวอย่างผู้มีส่วนได้ส่วนเสียในการเปิดเผยข้อมูล

หมายเหตุ R = Responsible A = Accountable S = Supportive C = Consulted และ I = Informed

๕.๕ การทำลายข้อมูล

วัตถุประสงค์

กำหนดแนวปฏิบัติการทำลายข้อมูล และการพิจารณาอนุมัติทำลายโดยเจ้าของข้อมูลเพื่อเป็นการรักษาความมั่นคงปลอดภัยของข้อมูล

ผู้รับผิดชอบงาน

๑. เจ้าของข้อมูล (Data Owners)

๒. ผู้ทำลายข้อมูล (Data Disposer)

๓. ผู้ดูแลระบบสารสนเทศ (Systems Administrators)

ข้อปฏิบัติ

๑. กำหนดแนวปฏิบัติและผู้ทำลายข้อมูลของหน่วยงานในการทำลายข้อมูลเมื่อข้อมูลไม่มีการใช้งานหรือมีการจัดเก็บเกินระยะเวลาที่กำหนดโดยให้เป็นไปตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยงานสารบรรณ พ.ศ. ๒๕๒๖ และที่แก้ไขเพิ่มเติม แต่ควรมีการเก็บรักษาเมทาดาตาของข้อมูลที่ทำลายไว้เพื่อใช้สำหรับการตรวจสอบ

๒. ผู้ทำลายข้อมูลต้องทำลายข้อมูลตามนโยบายและแนวปฏิบัติความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy) ของสำนักงานเศรษฐกิจการคลัง พ.ศ. ๒๕๖๘

๓. กำหนดให้ผู้ทำลายข้อมูลจัดเก็บบันทึกรายละเอียดการทำลายข้อมูลไว้ในทะเบียนควบคุมและบันทึกการทำลายข้อมูล โดยให้เก็บรักษาไว้เป็นหลักฐานไม่น้อยกว่า ๑ ปี

๔. ในกรณีที่มีการร้องขอให้ทำลายข้อมูลส่วนบุคคลจากเจ้าของข้อมูล ผู้ควบคุมข้อมูลส่วนบุคคลหรือหน่วยงานที่จัดเก็บต้องทำลายให้เร็วที่สุด โดยต้องไม่ขัดต่อข้อตกลง หรือไม่ขัดต่อข้อกฎหมายใด ๆ

๕. สร้างความรู้ความเข้าใจในการจัดเก็บและทำลายข้อมูลให้แก่ผู้เกี่ยวข้องทั้งภายในและภายนอกสำนักงาน

กิจกรรม	ผู้มีส่วนได้ส่วนเสีย			
	เจ้าของข้อมูล	ผู้ดูแลระบบสารสนเทศ	ผู้ทำลายข้อมูล	ผู้ใช้ข้อมูล
กำหนดผู้มีสิทธิในการทำลายข้อมูล	R	R	I	I
ทำลายข้อมูลตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน	C	S	R	I
จัดเก็บคำอธิบายข้อมูลที่ทำลายสำหรับตรวจสอบในภายหลัง	R	S	R	I
จัดเก็บบันทึกรายละเอียดการทำลายข้อมูล	I	S	R	I
ทำลายข้อมูลส่วนบุคคลเมื่อเจ้าของข้อมูลส่วนบุคคลร้องขอ ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒	I	S	R	I

ตารางที่ ๕ ตัวอย่างผู้มีส่วนได้ส่วนเสียในการทำลายข้อมูล

หมายเหตุ R = Responsible A = Accountable S = Supportive C = Consulted และ I = Informed

๕.๖ การเชื่อมโยงและการแลกเปลี่ยนข้อมูล

วัตถุประสงค์

เพื่อกำหนดแนวปฏิบัติและมาตรฐานด้านเทคนิคในการเชื่อมโยงและการแลกเปลี่ยนข้อมูลดิจิทัลทั้งภายในหน่วยงานและระหว่างหน่วยงาน อย่างมีประสิทธิภาพและก่อให้เกิดประโยชน์ต่อภาคประชาชน ภาครัฐ และภาคเอกชน

ผู้รับผิดชอบงาน

๑. เจ้าของข้อมูล (Data Owners)

๒. บริกรข้อมูล (Data Stewards)

๓. คณะทำงานบริกรข้อมูล (Data Stewards Team)

๔. ผู้ดูแลระบบแม่ข่าย (Server Administrators)

๕. ผู้ดูแลระบบสารสนเทศ (System Administrators)

ข้อปฏิบัติ

๑. กำหนดกระบวนการในการแลกเปลี่ยนข้อมูล กระบวนการเชื่อมโยงข้อมูล การรวบรวมข้อมูลส่วนบุคคล โดยนำมาตรฐานสากลมาประยุกต์ใช้งาน

๒. กำหนดเมทาดาตาของชุดข้อมูลที่ต้องการแลกเปลี่ยนและเชื่อมโยงข้อมูลให้ครบถ้วน

๓. จัดทำสัญญาอนุญาตหรือข้อตกลงในการแลกเปลี่ยนและเชื่อมโยงข้อมูล และ/หรือการนำข้อมูลไปใช้

๔. กำหนดเทคโนโลยีและมาตรฐานทางเทคนิคที่ใช้ในการแลกเปลี่ยนและเชื่อมโยงข้อมูล และการรวบรวมข้อมูลส่วนบุคคล

๕. ต้องบันทึกรายละเอียดและจัดเก็บข้อมูลการดำเนินงานที่เกิดขึ้นในแต่ละครั้งที่มีการแลกเปลี่ยนและเชื่อมโยงข้อมูล การรวบรวมข้อมูลส่วนบุคคล (Log File) ระหว่างหน่วยงาน เพื่อการตรวจสอบย้อนกลับ

๖. ต้องตรวจสอบได้ว่าการแลกเปลี่ยนและเชื่อมโยงข้อมูล และการรวบรวมข้อมูลส่วนบุคคลได้ดำเนินการอย่างเหมาะสมหรือเป็นไปตามแนวปฏิบัติและมาตรฐานที่กำหนด

๗. ห้ามมิให้เชื่อมโยงและแลกเปลี่ยนเพื่อส่งต่อข้อมูลคอมพิวเตอร์ที่เป็นการกระทำความผิดตามกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์

กิจกรรม	**ผู้มีส่วนได้ส่วนเสีย**				
	เจ้าของข้อมูล	**บริกรข้อมูล**	**คณะทำงานบริกรข้อมูล**	**ผู้ดูแลระบบแม่ข่าย**	**ผู้ดูแลระบบสารสนเทศ**
กำหนดวิธีปฏิบัติและมาตรฐานทางด้านเทคนิคที่จำเป็นในการเชื่อมโยงและแลกเปลี่ยนข้อมูล	I	I	I	S/R	S/R
ตรวจสอบคำอธิบายชุดข้อมูลดิจิทัล และชั้นความลับของข้อมูล	S/R	C	S	S	S/R
จัดทำแนวทางการทำงานร่วมกันทั้งระหว่างหน่วยงานภายในและหน่วยงานภายนอกในการเชื่อมโยงและแลกเปลี่ยนข้อมูล	S	S	S	S/R	S/R
จัดเก็บบันทึกหลักฐานของการเชื่อมโยงและการแลกเปลี่ยนข้อมูลดิจิทัล	I	I	I	R	R

ตารางที่ ๖ ตัวอย่างผู้มีส่วนได้ส่วนเสียในการเชื่อมโยงและแลกเปลี่ยนข้อมูล

หมายเหตุ R = Responsible A = Accountable S = Supportive C = Consulted และ I = Informed

ตารางแสดงความสัมพันธ์ระหว่างกระบวนการ/กิจกรรมและผู้มีส่วนได้ส่วนเสีย

(อ้างอิง: เอกสารมาตรฐานรัฐบาลดิจิทัลว่าด้วยข้อเสนอแนะสำหรับการจัดทำแนวปฏิบัติการบริหารจัดการข้อมูล เลขที่ มรด. ๔-๒ : ๒๕๖๕)

โดยกำหนดให้

R (Responsible) หมายถึง ผู้มีหน้าที่ในการปฏิบัติงานตามกระบวนการหรือกิจกรรมที่กำหนดไว้
A (Accountable) หมายถึง ผู้มีหน้าที่ในการทบทวนและอนุมัติผลที่ได้รับจากการปฏิบัติงาน
S (Supportive) หมายถึง ผู้ที่มีหน้าที่ในการสนับสนุนหรือให้การช่วยเหลือต่อการปฏิบัติงาน
C (Consulted) หมายถึง ผู้ที่ทำหน้าที่ให้คำปรึกษาต่อผู้ปฏิบัติงาน
I (Informed) หมายถึง ผู้ที่ทำหน้าที่รับทราบผลการปฏิบัติงาน

วงจรชีวิตข้อมูล	กิจกรรม	ผู้มีส่วนได้ส่วนเสีย							
		เจ้าของข้อมูล	ผู้ดูแลระบบสารสนเทศ	ผู้สร้างข้อมูล	ผู้ใช้ข้อมูล	บริกรข้อมูล	คณะทำงานบริกรข้อมูล	ผู้ทำลายข้อมูล	ผู้ดูแลระบบแม่ข่าย
การสร้างข้อมูล	๑. กำหนดผู้มีสิทธิในการสร้างข้อมูล และกำหนดหมวดหมู่และชั้นความลับ	R	S	I		C	I		
	๒. กำหนดสิทธิในการสร้างข้อมูลในระบบให้แก่ผู้สร้างข้อมูล	S	R	I		I	I		
	๓. สร้างข้อมูลที่ไม่ขัดต่อกฎหมายและจากแหล่งข้อมูลที่เชื่อถือได้เท่านั้น	C	S	R		C	I		
	๔. จัดทำคำอธิบายชุดข้อมูลดิจิทัล	R	S	S		R	S		
	๕. ประเมินคุณค่าของชุดข้อมูลดิจิทัล	R	I	I		R	I		
	๖. ตรวจสอบความถูกต้องของข้อมูล	R	S	R		C	I		
การจัดเก็บข้อมูล	๑. กำหนดระยะเวลาในการจัดเก็บข้อมูล	R	S	S	I	I	S		
	๒. ย้ายข้อมูลที่มีการจัดเก็บเกินระยะเวลาที่กำหนด	I/C	R	I	I	I	R		
	๓. จัดทำคำอธิบายชุดข้อมูลดิจิทัลและปรับปรุงให้เป็นปัจจุบัน	A	S	R	I	R	R		
	๔. จัดเก็บข้อมูลตามการจัดชั้นความลับของหน่วยงาน	R	S	R	I	C	S		

วงจรชีวิตข้อมูล	กิจกรรม	ผู้มีส่วนได้ส่วนเสีย							
		เจ้าของข้อมูล	ผู้ดูแลระบบสารสนเทศ	ผู้สร้างข้อมูล	ผู้ใช้ข้อมูล	บริกรข้อมูล	คณะทำงานบริกรข้อมูล	ผู้ทำลายข้อมูล	ผู้ดูแลระบบแม่ข่าย
	๕. จัดเก็บข้อมูลส่วนบุคคลเท่าที่จำเป็น	R	R/S	S	R	C	S		
	๖. ยกเลิกการจัดเก็บข้อมูลส่วนบุคคลกรณีเจ้าของข้อมูลส่วนบุคคลถอนความยินยอม	R	R	I	I	I	I		
	๗. จัดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์	I	R	I	I	I	I		
การประมวลผลและใช้ข้อมูล	๑. กำหนดสิทธิในการประมวลผลและใช้งานข้อมูลตามชั้นความลับ	R	S		I				
	๒. กำหนดสิทธิในการประมวลผลและเข้าใช้งานข้อมูลในระบบ	R	S		I				
	๓. ไม่ใช้ข้อมูลในเครือข่ายของหน่วยงานเพื่อประโยชน์ในเชิงธุรกิจเป็นการส่วนตัว	I	S		R				
	๔.ประมวลผลข้อมูลหรือใช้ข้อมูลส่วนบุคคลเท่าที่จำเป็น	C	S		R				
	๕. ยกเลิกการประมวลผลข้อมูลหรือการใช้ข้อมูลส่วนบุคคล กรณีที่เจ้าของข้อมูลส่วนบุคคลถอนความยินยอม	A	S		R				
การเปิดเผยข้อมูล	๑. จะต้องเปิดเผยข้อมูลในความรับผิดชอบต่อสาธารณะตามกฎหมาย/มาตรฐานที่เกี่ยวข้อง	R			I	C	S		
	๒. คัดเลือกข้อมูลที่จะเปิดเผยในรูปแบบข้อมูลเปิดจากลำดับชั้นความสำคัญของ High Value Dataset	R			I	C	S		
	๓. ตรวจสอบคำอธิบายชุดข้อมูลดิจิทัลที่จะทำการเปิดเผยให้มีความครบถ้วนเป็นปัจจุบัน	A			I	R	R		

วงจรชีวิตข้อมูล	กิจกรรม	ผู้มีส่วนได้ส่วนเสีย							
		เจ้าของข้อมูล	ผู้ดูแลระบบสารสนเทศ	ผู้สร้างข้อมูล	ผู้ใช้ข้อมูล	บริกรข้อมูล	คณะทำงานบริกรข้อมูล	ผู้ทำลายข้อมูล	ผู้ดูแลระบบแม่ข่าย
	๔. เปิดเผยข้อมูลส่วนบุคคลตามข้อกำหนดของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และห้ามเปิดเผยข้อมูลความมั่นคงและข้อมูลความลับทางราชการ รวมถึงข้อมูลที่เป็นการกระทำความผิดตามกฎหมาย	R			R	C	S		
	๕. กำหนดรอบระยะเวลาในการตรวจสอบและปรับปรุงข้อมูลที่เปิดเผย	R			I	I	I		
การทำลายข้อมูล	๑. กำหนดผู้มีสิทธิในการทำลายข้อมูล	R	R		I			I	
	๒. ทำลายข้อมูลตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน	C	S		I			R	
	๓. จัดเก็บคำอธิบายข้อมูลที่ทำลายสำหรับตรวจสอบในภายหลัง	R	S		I			R	
	๔. จัดเก็บบันทึกรายละเอียดการทำลายข้อมูล	I	S		I			R	
	๕. ทำลายข้อมูลส่วนบุคคลเมื่อเจ้าของข้อมูลส่วนบุคคลร้องขอ ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒	I	S		I			R	
การเชื่อมโยงและแลกเปลี่ยนข้อมูล	๑. กำหนดวิธีปฏิบัติและมาตรฐานทางด้านเทคนิคที่จำเป็นในการเชื่อมโยงและแลกเปลี่ยนข้อมูล	I	S/R			I	I		S/R
	๒. ตรวจสอบคำอธิบายชุดข้อมูลดิจิทัล และชั้นความลับของข้อมูล	S/R	S/R			C	S		S
	๓. จัดทำแนวทางการทำงานร่วมกันทั้งระหว่างหน่วยงานภายในและหน่วยงาน	S	S/R			S	S		S/R

วงจรชีวิตข้อมูล	กิจกรรม	ผู้มีส่วนได้ส่วนเสีย							
		เจ้าของข้อมูล	ผู้ดูแลระบบสารสนเทศ	ผู้สร้างข้อมูล	ผู้ใช้ข้อมูล	บริกรข้อมูล	คณะทำงานบริกรข้อมูล	ผู้ทำลายข้อมูล	ผู้ดูแลระบบแม่ข่าย
	ภายนอกในการเชื่อมโยงและแลกเปลี่ยนข้อมูล								
	๔. จัดเก็บบันทึกหลักฐานของการเชื่อมโยงและการแลกเปลี่ยนข้อมูลดิจิทัล	I	R			I	I		R

หมวด ๓
การประเมินคุณภาพข้อมูล (Data Quality Management)

วัตถุประสงค์

เพื่อใช้เป็นกรอบและเครื่องมือสำหรับตรวจสอบคุณภาพข้อมูลเบื้องต้นให้เป็นไปตามกรอบธรรมาภิบาลข้อมูลภาครัฐ โดยจัดทำเกณฑ์ตัวชี้วัดตามมิติคุณภาพข้อมูล ดังนี้

เกณฑ์การประเมินคุณภาพข้อมูล

เกณฑ์การประเมินคุณภาพข้อมูลอ้างอิงตามเอกสารมาตรฐานรัฐบาลดิจิทัลว่าด้วยหลักเกณฑ์การประเมินคุณภาพข้อมูลสำหรับหน่วยงานภาครัฐ เลขที่ มรด. ๕ : ๒๕๖๕ แนบท้ายประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง มาตรฐานรัฐบาลดิจิทัลว่าด้วยหลักเกณฑ์การประเมินคุณภาพข้อมูลสำหรับหน่วยงานภาครัฐ ได้มีการกำหนดเกณฑ์การประเมินคุณภาพข้อมูลตามมิติคุณภาพข้อมูล ๕ มิติ ได้แก่ (๑) ความถูกต้อง (๒) ความสอดคล้องกัน (๓) ตรงตามความต้องการของผู้ใช้ (๔) ความเป็นปัจจุบัน และ (๕) ความพร้อมใช้ที่สอดคล้องตามองค์ประกอบในการประเมินคุณภาพข้อมูลตามกรอบธรรมาภิบาลข้อมูลภาครัฐ โดยแต่ละมิติมีรายละเอียดและตัวชี้วัด (indicators) ดังต่อไปนี้

มิติคุณภาพข้อมูล	รายละเอียด	รายการตัวชี้วัด
ความถูกต้อง และสมบูรณ์ (Accuracy and Completeness)	ประเมินเรื่องความถูกต้องแม่นยำ แหล่งข้อมูลที่น่าเชื่อถือ และมีกระบวนการตรวจสอบ	▪ มีแหล่งข้อมูลที่น่าเชื่อถือ ▪ มีกระบวนการหรือเครื่องมือตรวจสอบจุดผิดพลาดของข้อมูล ▪ มีการตรวจสอบความครบถ้วนของข้อมูล ▪ มีวิธีเก็บข้อมูลที่มีความเป็นกลาง น่าเชื่อถือ และไม่สร้างข้อมูลที่มีอคติ ▪ มีการระบุคำนิยามและลักษณะข้อมูลที่ต้องการ
ความสอดคล้องกัน (Consistency)	ประเมินเรื่องรูปแบบของข้อมูล ความสอดคล้องกัน และมาตรฐานในการจัดทำข้อมูลของหน่วยงาน	▪ มีการเก็บข้อมูลภายใต้มาตรฐานข้อมูลเดียวกันหรือมาตรฐานข้อมูลที่สอดคล้องกัน ทำให้สามารถใช้ประโยชน์ข้อมูลร่วมกันได้ ▪ มีการตรวจสอบรูปแบบข้อมูลภายในชุดข้อมูลเดียวกัน ▪ ข้อมูลมีความเชื่อมโยงและไม่ขัดแย้งกัน ▪ มีการใช้กฎ วิธีการตรวจวัดที่สอดคล้องกันทั้งหน่วยงาน รวมถึงหน่วยงานภายนอก ▪ มีการกำหนดบทบาทและผู้รับผิดชอบข้อมูล

มิติคุณภาพข้อมูล	รายละเอียด	รายการตัวชี้วัด
ตรงตามความต้องการของผู้ใช้ (Relevancy)	ประเมินว่า เป็นข้อมูลที่ผู้ใช้ต้องการ หรือเป็นข้อมูลที่จำเป็นต้องทราบ มีความละเอียดเพียงพอต่อการนำไปใช้งาน	▪ ข้อมูลตรงตามความต้องการและวัตถุประสงค์ของการใช้งาน ▪ มีผลประเมินความพึงพอใจของผู้ใช้และมีการปรับปรุงคุณภาพให้ตรงตามความต้องการของผู้ใช้
ความเป็นปัจจุบัน (Timeliness)	ประเมินเรื่องการเผยแพร่ข้อมูล การปรับปรุงข้อมูล และแผนเรื่องระยะเวลา	▪ ข้อมูลมีการเผยแพร่ ส่งต่อตรงเวลา ▪ ข้อมูลมีความเป็นปัจจุบัน ▪ ข้อมูลมีการเผยแพร่ในเวลาที่เหมาะสม ▪ มีการจัดทำปฏิทินเผยแพร่ข้อมูล
ความพร้อมใช้ (Availability)	ประเมินความพร้อมใช้ของข้อมูล รวมไปถึงช่องทางในการขอ หรือใช้ข้อมูล	▪ ข้อมูลถูกจัดในรูปแบบที่พร้อมนำไปใช้งาน และเหมาะสมกับผู้ใช้งาน ▪ มีการเผยแพร่ข้อมูลที่เหมาะสมและสามารถเข้าถึงได้ โดยผู้ใช้สามารถเข้าถึงข้อมูลได้สะดวกตามสิทธิที่เหมาะสม ▪ ข้อมูลสามารถอ่านด้วยโปรแกรมคอมพิวเตอร์ได้ ▪ มีคำอธิบายข้อมูลที่ชัดเจน ▪ มีคำอธิบายขั้นตอนการขอข้อมูลที่ไม่เผยแพร่เป็นสาธารณะสำหรับหน่วยงานภายนอก

เครื่องมือการประเมินคุณภาพข้อมูล

ในการประเมินคุณภาพข้อมูล เจ้าของข้อมูลหรือผู้ครอบครองข้อมูลสามารถใช้เครื่องมือการประเมินคุณภาพข้อมูล เพื่อตรวจสอบและควบคุมการบริหารจัดการข้อมูล เพื่อให้ได้ข้อมูลที่มีคุณภาพ น่าเชื่อถือ รวมทั้งสามารถนำไปใช้ประโยชน์เพื่อเพิ่มประสิทธิภาพในการทำงาน เพิ่มคุณค่าในการให้บริการภาครัฐ โดยเครื่องมือการประเมินคุณภาพข้อมูล มี ๓ รูปแบบ ดังนี้

๑. แบบตรวจประเมินคุณภาพ (DQA Checklist) เพื่อประเมินกระบวนการเตรียมข้อมูลให้มีคุณภาพตามมิติคุณภาพข้อมูล ๕ มิติ

๒. แบบประเมินคุณภาพข้อมูลด้วยตนเอง (DQA Self-Assessment) เพื่อประเมินชุดข้อมูลตามมิติคุณภาพข้อมูล ๕ มิติ เพื่อให้ทราบว่าข้อมูลภายในหน่วยงานมีคุณภาพมากน้อยเพียงใด และควรปรับปรุงหรือพัฒนาในมิติใด

๓. แบบตรวจประเมินการควบคุมและติดตามคุณภาพข้อมูล (Data Quality Monitoring and Control Checklist) เพื่อตรวจสอบหลักฐานในการสนับสนุนกระบวนการเผยแพร่ข้อมูลที่มีคุณภาพ ตั้งแต่การจัดเตรียมข้อมูล การเผยแพร่ข้อมูล และการรายงานผลข้อมูล เพื่อกำหนดเป็นมาตรฐานในการดำเนินงานในหน่วยงาน

แนวทางปฏิบัติและความรับผิดชอบ

๑. ชุดข้อมูลทุกชุดต้องมีคุณภาพข้อมูลอย่างน้อยครอบคลุมถึงความถูกต้อง (Accuracy) ความครบถ้วน (Completeness) ความต้องกัน (Consistency) และความเป็นปัจจุบัน (Timeliness)

๑.๑ ความถูกต้องของข้อมูลต้องมีการตรวจสอบโดยบริกรข้อมูล และแก้ไขโดยเจ้าของข้อมูล

๑.๒ ความครบถ้วนของข้อมูลสามารถตรวจสอบได้

๑.๓ ความต้องกันของข้อมูลสามารถตรวจสอบได้กับมาตรฐานข้อมูลที่ตั้งไว้ในแต่ละชุดข้อมูล

๑.๔ ความเป็นปัจจุบันต้องมีการเปรียบเทียบกับฟิลด์อ้างอิงที่เป็นเกณฑ์เวลาตามมาตรฐาน

๒. คุณภาพข้อมูลต้องดำเนินการโดยเจ้าของข้อมูล ผู้ใช้ข้อมูล และบริกรข้อมูลในกอง/ศูนย์/กลุ่ม และเห็นชอบโดยคณะกรรมการธรรมาภิบาลข้อมูลของสำนักงานเศรษฐกิจการคลัง

๓. สอบทานคุณภาพคุณภาพข้อมูลให้เป็นไปตามหลักเกณฑ์ที่กำหนดอย่างสม่ำเสมอ

๔. ติดตามและปรับปรุงผลการประเมินคุณภาพข้อมูลอย่างต่อเนื่อง

๕. เมื่อมีการนำเข้าข้อมูล จะต้องมีหน้าที่ตรวจสอบคุณภาพข้อมูลก่อนนำเข้า

๖. เมื่อข้อมูลถูกนำเข้าไปแล้ว ถ้ามีความผิดพลาด ผู้สร้างข้อมูลหรือเจ้าของข้อมูลจะต้องดำเนินการแก้ไข

๗. จัดทำรายงานผลการติดตามคุณภาพข้อมูล สรุปความคืบหน้าการแก้ไขปรับปรุงชุดข้อมูลที่ไม่ผ่านเกณฑ์การประเมินคุณภาพ รวมทั้ง รายงานประเด็นปัญหาหรือความเสี่ยงที่พบ ภาพรวมปัญหาและสาเหตุที่ทำให้ชุดข้อมูลไม่มีคุณภาพ นำเสนอคณะกรรมการธรรมาภิบาลข้อมูลของสำนักงานเศรษฐกิจการคลัง
