ประกาศกรมธนารักษ์
เรื่อง แนวปฏิบัติธรรมาภิบาลข้อมูลของกรมธนารักษ์

ตามพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ มาตรา ๑๒ กำหนดให้หน่วยงานของรัฐจัดให้มีการบริหารจัดการข้อมูลและการบูรณาการข้อมูลภาครัฐ กรมในฐานะหน่วยงานที่มีอำนาจหน้าที่เกี่ยวกับราชการของกระทรวงตามที่กำหนดในกฎกระทรวงแบ่งส่วนราชการของกรมหรือตามกฎหมายว่าด้วยอำนาจหน้าที่ของกรมนั้น ประกอบกับประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมมาภิบาลข้อมูลภาครัฐ ข้อ ๓ ให้หน่วยงานของรัฐดำเนินการให้เป็นไปตามธรรมาภิบาลข้อมูลภาครัฐ และจัดทำธรรมาภิบาลข้อมูลภาครัฐในระดับหน่วยงานให้สอดคล้องกับธรรมาภิบาลข้อมูลภาครัฐ รวมถึงสอดคล้องกับประกาศกรมธนารักษ์ เรื่อง นโยบายธรรมาภิบาลข้อมูลของกรมธนารักษ์

กรมธนารักษ์ในฐานะหน่วยงานที่มีภารกิจด้านที่ราชพัสดุ การประเมินราคาทรัพย์สินเพื่อประโยชน์แห่งรัฐ การผลิตเหรียญกษาปณ์และจัดสร้างเครื่องราชอิสริยยศ เครื่องราชอิสริยาภรณ์ ตลอดจนบริหารเงินตราและเก็บรักษาทรัพย์สินมีค่าของรัฐ ได้มีการรวบรวม จัดเก็บ ใช้ หรือเผยแพร่ข้อมูล เพื่อการบริหารงานตามหน้าที่และอำนาจ ดังนั้น เพื่อเป็นการกำหนดแนวปฏิบัติธรรมาภิบาลข้อมูล เกี่ยวกับการกำหนดสิทธิ์หน้าที่ ความรับผิดชอบในการบริหารจัดการข้อมูลของหน่วยงานของรัฐ กำหนดนโยบายหรือกฎเกณฑ์การเข้าถึงและใช้ประโยชน์จากข้อมูล จัดทำคำอธิบายชุดข้อมูลดิจิทัลของภาครัฐ และมีการบูรณาการ เชื่อมโยงและแลกเปลี่ยนข้อมูลการทำงานร่วมกันและระหว่างหน่วยงานของรัฐแห่งอื่น โดยไม่ต้องจัดทำข้อมูลขึ้นใหม่ทั้งหมด โดยข้อมูลจะต้องมีความปลอดภัย เชื่อถือได้ และมีผู้รับผิดชอบ จึงได้ออกประกาศเกี่ยวกับแนวปฏิบัติธรรมาภิบาลข้อมูลของกรมธนารักษ์ไว้ รายละเอียดปรากฏตามแนบท้ายประกาศนี้

ประกาศฉบับนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

ประกาศ ณ วันที่ ๑๙ พฤษภาคม พ.ศ. ๒๕๖๙

(นายอัครุตม์ สนธยานนท์)
อธิบดีกรมธนารักษ์

ประกาศกรมธนารักษ์ เรื่อง แนวปฏิบัติธรรมาภิบาลข้อมูลของกรมธนารักษ์

รหัสเอกสาร	DG-๐๑๐๒
ชื่อเอกสาร	แนวปฏิบัติธรรมาภิบาลข้อมูลของกรมธนารักษ์
หมายเลขปรับปรุงเอกสาร	๒.๐
วันที่เอกสารมีผลบังคับใช้	๑๙ พฤษภาคม ๒๕๖๙
เจ้าของเอกสาร :	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

การอนุมัติเอกสาร

ชื่อเอกสาร แนวปฏิบัติธรรมาภิบาลข้อมูลของกรมธนารักษ์			
หมายเลขปรับปรุงเอกสาร ๒.๐			
การอนุมัติ	**ชื่อ - สกุล**	**ตำแหน่ง**	**ลงนาม**
ผู้อนุมัติ	นายอัครุตม์ สนธยานนท์	อธิบดี	
ผู้ทบทวน	นายฤชา วราทร	รองอธิบดี	
ผู้ตรวจสอบ	นางสาวพิมพ์สราญ บำเพ็ญวิบูลย์กิจ	ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	
ผู้จัดทำ	นางสาวกรรณิการ์ นุชชมภู	นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ	
	นางสาวฐิลาพร เชตุราช	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	
วันที่อนุมัติ ๑๙ พฤษภาคม ๒๕๖๙		**วันที่บังคับใช้** ๑๙ พฤษภาคม ๒๕๖๙	

บันทึกประวัติการแก้ไขเอกสาร

ครั้งที่แก้ไข	**วันที่แก้ไข**	**รายการเปลี่ยนแปลง**	**ผู้จัดทำ**
๑	๘ พฤษภาคม ๒๕๖๙	๑. เพิ่มการอนุมัติเอกสาร ๒. เพิ่มบันทึกประวัติการแก้ไขเอกสาร ๓. เพิ่มคำนิยาม ๔. เพิ่ม/แก้ไขชื่อหมวด และรายละเอียด ๕. แก้ไขรายละเอียดให้สอดคล้องกับมาตรฐานรัฐบาลดิจิทัลว่าด้วยกรอบธรรมาภิบาลข้อมูลภาครัฐ ฉบับปรับปรุง (มรด ๖ : ๒๕๖๖)	นางสาวฐิลาพร เชตุราช

๑. คำนิยาม

๑) ธรรมาภิบาลข้อมูล (Data Governance) หมายถึง การกำหนดสิทธิ์ หน้าที่ และความรับผิดชอบของผู้มีส่วนได้ส่วนเสียในการบริหารจัดการข้อมูลของหน่วยงานทุกขั้นตอน เพื่อให้การได้มาและการนำข้อมูลของหน่วยงานไปใช้อย่างถูกต้อง ครบถ้วน เป็นปัจจุบัน รักษาความเป็นส่วนบุคคล และสามารถเชื่อมโยง แลกเปลี่ยน และบูรณาการระหว่างกันได้อย่างมีประสิทธิภาพและมั่นคงปลอดภัย โดยใช้ข้อมูลเป็นหลักในการบริหารงานและการบริการสาธารณะ

๒) ข้อมูล (Data) หมายถึง สิ่งที่สื่อความหมายให้รู้เรื่องราวข้อเท็จจริงหรือเรื่องอื่นใด ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเอง หรือโดยผ่านวิธีการใด ๆ และไม่ว่าจะได้จัดทำไว้ในรูปของเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ แบบแปลน ภาพวาด ภาพถ่าย ภาพถ่ายดาวเทียม ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ เครื่องมือตรวจวัด การสำรวจระยะไกล หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้

๓) ชุดข้อมูล (Dataset) หมายถึง การนำข้อมูลจากหลายแหล่งมารวบรวม เพื่อจัดเป็นชุดให้ตรงตามลักษณะโครงสร้างของข้อมูล

๔) บัญชีข้อมูล (Data Catalog) หมายถึง เอกสารแสดงบรรดารายการของชุดข้อมูล ที่จำแนกแยกแยะ โดยการจัดกลุ่มหรือจัดประเภทข้อมูลที่อยู่ในความครอบครองหรือควบคุมของหน่วยงานของรัฐ

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

๖) การจัดระดับชั้นของข้อมูล (Data Classification) หมายถึง ระดับชั้นข้อมูลเพื่อจัดการข้อมูลในกระบวนงานที่เกี่ยวข้องกับภารกิจ โดยข้อมูลที่มีความอ่อนไหวแบ่งระดับชั้นออกเป็น ชั้นเปิดเผย (Open) ชั้นเผยแพร่ภายในองค์กร (Private) ชั้นลับ (Confidential) ชั้นลับมาก (Secret) และชั้นลับที่สุด (Top Secret) ซึ่งข้อมูลที่มีระดับชั้น ลับ (Confidential) ลับมาก (Secret) และลับที่สุด (Top Secret) เป็นเพียงการจัดระดับชั้นของข้อมูล ไม่ใช่การกำหนดให้ข้อมูลนั้นเป็นข้อมูลความลับทางราชการตามระเบียบการรักษาความลับทางราชการ

๗) วงจรชีวิตของข้อมูล (Data Life Cycle) หมายถึง ลำดับขั้นตอนของข้อมูลตั้งแต่เริ่มสร้างข้อมูลไปจนถึงการทำลายข้อมูล ตามกรอบธรรมาภิบาลข้อมูลภาครัฐ

๘) คลังข้อมูล (Data Warehouse) หมายถึง ข้อมูลที่ได้จากการเชื่อมโยงข้อมูล (Data Integration) ซึ่งเกิดจากการรวบรวมข้อมูลจากแหล่งข้อมูลต่าง ๆ ที่มีหลากหลายรูปแบบมาเก็บในคลังข้อมูลโดยผ่านกระบวนการของ Extract Transform Load (ETL) ในรูปแบบข้อมูลที่มีโครงสร้าง และถูกจัดทำให้อยู่ในรูปแบบที่เหมาะสมสำหรับการนำไปวิเคราะห์ข้อมูล ทั้งในรูปแบบของรายงานอัจฉริยะ (Business Intelligence) และดาตาอนาไลติกส์ (Data Analytics)

๙) ทะเลสาบข้อมูล (Data Lake) หมายถึง แหล่งสำหรับเก็บรวบรวมข้อมูลที่มีหลากหลายรูปแบบ ข้อมูลที่จัดเก็บเป็นข้อมูลที่มีโครงสร้าง ข้อมูลกึ่งโครงสร้าง และข้อมูลที่ไม่มีโครงสร้าง โดยข้อมูลถูกเก็บรักษาไว้ในรูปแบบที่เหมือนหรือใกล้เคียงกับรูปแบบที่ได้รับมาจากแหล่งข้อมูลต้นฉบับ และสามารถใช้เป็นที่สำรองข้อมูลต้นฉบับได้

๑๐) เมทาดาตา (Metadata) หมายถึง ข้อมูลที่ใช้อธิบายข้อมูลหลักหรือกลุ่มข้อมูลอื่น ๆ ที่เกี่ยวข้องทั้งกระบวนการเชิงธุรกิจและเชิงเทคโนโลยีสารสนเทศ กฎและข้อจำกัดของข้อมูล และโครงสร้างของข้อมูลเมทาดาตาช่วยให้หน่วยงานสามารถเข้าใจข้อมูล ระบบ และขั้นตอนการทำงานได้ดียิ่งขึ้น

๑๑) เมทาดาตาทางธุรกิจ (Business Metadata) หมายถึง คำอธิบายชุดข้อมูลดิจิทัลที่ให้รายละเอียดชุดข้อมูล (Datasets) ในด้านธุรกิจ เหมาะสำหรับผู้ใช้งานข้อมูล (Data User) นักวิเคราะห์ข้อมูล (Data Analyst) และนักวิทยาการข้อมูล (Data Scientist) ตัวอย่างรายการเมทาดาตาเชิงธุรกิจ เช่น ชื่อข้อมูล ชื่อเจ้าของข้อมูล คำสำคัญ คำอธิบายอย่างย่อ วันที่เริ่มต้นใช้งาน วันที่ทำการเปลี่ยนแปลงข้อมูล ภาษาที่ใช้ ชื่อฟิลด์ข้อมูล (เช่น ชื่อพนักงาน นามสกุล เพศ) เป็นต้น

๑๒) เมทาดาตาทางเทคนิค (Technical Metadata) หมายถึง คำอธิบายชุดข้อมูลดิจิทัลที่ให้รายละเอียดชุดข้อมูล (Datasets) ในด้านเทคนิค (Technical) และปฏิบัติการ (Operational) เหมาะสำหรับผู้บริหารจัดการฐานข้อมูล (Database Administrator) ตัวอย่างรายการเมทาดาตาเชิงเทคนิค อาทิ ชื่อตารางข้อมูลในฐานข้อมูล ชื่อฟิลด์ข้อมูลในตารางข้อมูล ประเภทข้อมูล (เช่น ตัวเลข ตัวหนังสือ หรือวันที่) ความกว้างของฟิลด์ข้อมูล (เช่น ๑๐ ตัวอักษร ๕๐ ตัวอักษร หรือ ๑๐๐ ตัวอักษร) คีย์ข้อมูล (Primary Key หรือ Foreign Key) รวมไปถึงข้อมูลสำหรับการสำรองข้อมูล (Backup) และกู้คืนข้อมูล (Restore)

๑๓) คุณภาพข้อมูล (Data Quality) หมายถึง ตัวชี้วัดเชิงปริมาณ (Quantitative Measurement) ของความพร้อมใช้ข้อมูลอย่างมีประโยชน์ โดยมี ๕ องค์ประกอบ ได้แก่ ความถูกต้องและสมบูรณ์ (Accuracy and Completeness) ความสอดคล้องกัน (Consistency) ตรงตามความต้องการของผู้ใช้ (Relevancy) ความเป็นปัจจุบัน (Timeliness) และความพร้อมใช้ (Availability)

๑๔) ข้อมูลหลัก (Master Data) หมายถึง ข้อมูลที่ถูกสร้างขึ้นเป็นข้อมูลพื้นฐานที่มีความสำคัญต่อการดำเนินงาน เพื่อใช้งานร่วมกันภายในหน่วยงานเป็นหลักและขับเคลื่อนองค์กรให้บรรลุเป้าหมาย เช่น ข้อมูลพนักงาน ข้อมูลโครงสร้างองค์กร ข้อมูลแผนปฏิบัติการและงบประมาณประจำปี และข้อมูลครุภัณฑ์ ทั้งนี้ หน่วยงานอาจแบ่งปันข้อมูลกับหน่วยงานอื่นตามวัตถุประสงค์ที่กำหนดขึ้น ไม่ได้จำกัดการใช้งานภายในองค์กรเท่านั้น เช่น ข้อมูลหลักของกรมการปกครองคือเลขประจำตัวประชาชน ๑๓ หลัก ที่กรมสรรพากรนำมาใช้เป็นเลขประจำตัวผู้เสียภาษีอากรได้

๑๕) ข้อมูลอ้างอิง (Reference Data) หมายถึง ข้อมูลที่ถูกสร้างขึ้นหรืออ้างอิงมาจากข้อมูลหลักเพื่อกำหนดให้เป็นมาตรฐานและใช้งานร่วมกันในวงกว้าง โดยมีการระบุแหล่งที่มาที่ใช้อ้างอิงได้ชัดเจน หรือมีหน่วยงานรับผิดชอบเป็นทางการ อาทิ ข้อมูลชื่อจังหวัด ข้อมูลรหัสไปรษณีย์ และข้อมูลรหัสประเทศ

หมวดที่ ๑ การสร้างข้อมูล (Data Creation)

๑) การสร้างข้อมูล (Data Creation) ทั้งข้อมูลที่เป็นกระดาษ และข้อมูลที่เป็นอิเล็กทรอนิกส์ทุกประเภท ให้ข้าราชการ เจ้าหน้าที่ ลูกจ้าง พนักงานราชการ รวมทั้งผู้ดูแลเครือข่าย ผู้ดูแลระบบในส่วนที่เกี่ยวข้องกับการสร้างข้อมูล (Data Creation) ต้องปฏิบัติตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ รวมทั้งกฎหมายอื่น ๆ ที่เกี่ยวข้อง การสร้างข้อมูลมีแนวปฏิบัติ ดังต่อไปนี้

๑.๑) เจ้าของข้อมูล กำหนดผู้มีสิทธิ์ในการสร้างข้อมูล (Create)

๑.๒) ผู้ดูแลระบบสารสนเทศ อนุมัติสิทธิ์การสร้างข้อมูล (Create) ในระบบตามสิทธิ์ที่เจ้าของข้อมูลได้มีการกำหนดไว้

๑.๓) ผู้สร้างข้อมูล สร้างข้อมูลตามสิทธิ์ที่ตนเองได้รับ และจะต้องไม่สร้างข้อมูลที่ขัดต่อมาตรฐานหรือข้อกฎหมายที่ได้มีการกำหนดไว้

๑.๔) ผู้สร้างข้อมูล จะต้องคำนึงถึงความมั่นคงปลอดภัยและความเป็นส่วนบุคคลของข้อมูล

๑.๕) ผู้สร้างข้อมูล สร้างข้อมูลจากแหล่งข้อมูลที่น่าเชื่อถือเท่านั้น

๑.๖) เจ้าของข้อมูล ตรวจสอบความถูกต้องของข้อมูลที่สร้างและห้ามสร้างข้อมูลลักษณะดังต่อไปนี้ อันได้แก่

๑.๖.๑) ห้ามสร้างข้อมูลที่บิดเบือน หรือปลอมแปลงไม่ว่าทั้งหมดหรือบางส่วน

๑.๖.๒) ห้ามสร้างข้อมูลอันเป็นเท็จ ที่น่าจะเกิดความเสียหายต่อการรักษาความมั่นคง ปลอดภัย ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจ หรือ โครงสร้างพื้นฐาน หรือก่อให้เกิดความตื่นตระหนก

๑.๖.๓) ห้ามสร้างข้อมูลอันเป็นความผิดเกี่ยวกับความมั่นคง หรือความผิดเกี่ยวกับการก่อการร้าย

๑.๖.๔) ห้ามสร้างข้อมูลที่มีลักษณะอันลามกอนาจาร

๑.๖.๕) ห้ามทำการตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ ที่จะทำให้ผู้อื่นเสียชื่อเสียง ถูกดูหมิ่นเกลียดชังหรือได้รับความอับอาย

๑.๖.๖) ห้ามสร้าง/ทำซ้ำ ข้อมูลที่ขัดต่อกฎหมายว่าด้วยลิขสิทธิ์หรือทรัพย์สินทางปัญญาของผู้อื่น

๑.๖.๗) ห้ามสร้างข้อมูลจากแหล่งข้อมูลที่ไม่น่าเชื่อถือ แต่ควรสร้างข้อมูลจากแหล่งข้อมูลต้นทางโดยตรงหรือแหล่งข้อมูลที่น่าเชื่อถือ

๑.๗) เจ้าของข้อมูลกำหนดหมวดหมู่และระดับชั้นข้อมูล

๑.๘) การกำหนดระดับชั้นของข้อมูล จะต้องดำเนินการพิจารณาลำดับชั้นที่เหมาะสมกับระดับความสำคัญของข้อมูล โดยพิจารณาจากการประเมินความเสี่ยง (Risk Assessment) ของข้อมูลดังกล่าว

๑.๙) การกำหนดหมวดหมู่ของข้อมูล จะต้องดำเนินการพิจารณาหมวดหมู่เลือกหมวดหมู่ที่เหมาะสม และสอดคล้องกับคุณลักษณะเฉพาะของข้อมูลหรือชุดข้อมูลดังกล่าว

๑.๑๐) ข้อมูลหรือชุดข้อมูลจะต้องมีการดำเนินการติดฉลาก (Data Label) หลังจากผ่านการพิจารณาระดับชั้นข้อมูลและการกำหนดหมวดหมู่ของข้อมูล โดยจะต้องดำเนินการให้เหมาะสมกับรูปแบบของข้อมูลที่ได้รับการดำเนินการ อาทิ ข้อมูลประเภทระเบียบสามารถดำเนินการฝังข้อมูลหมวดหมู่และระดับชั้นข้อมูลในเมทาดาตาของข้อมูลดังกล่าว

๑.๑๑) เจ้าของข้อมูล บริกรข้อมูลเชิงธุรกิจ บริกรข้อมูลเชิงเทคนิค และทีมบริหารจัดการข้อมูล ดำเนินการจัดทำคำอธิบายชุดข้อมูล (Metadata)

๑.๑๒) เจ้าของข้อมูล ทบทวนผู้มีสิทธิ์ในการสร้างข้อมูล (Create) อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงสำคัญ อาทิ การลาออก การโยกย้ายตำแหน่ง การปรับปรุงโครงสร้างองค์กร

หมวดที่ ๒ การจัดเก็บข้อมูล (Store)

๑) การจัดเก็บข้อมูลในส่วนนี้หมายความรวมถึงข้อมูลทั้งที่เป็นกระดาษและข้อมูลที่เป็นอิเล็กทรอนิกส์ทุกประเภท ไม่ว่าจะเป็นแฟ้มข้อมูลดิจิทัลทั่วไป (Digital Files) หรือแฟ้มข้อมูลที่มีการเข้ารหัสลับ (Encrypted Files) หรือแฟ้มข้อมูลที่ผ่านการประมวลผล (Information Files) หรือแฟ้มข้อมูลอื่น การจัดเก็บข้อมูลมีแนวปฏิบัติ ดังต่อไปนี้

๑.๑) ต้องจัดเก็บข้อมูลตามหมวดหมู่ โดยกรมธนารักษ์มีการกำหนดหมวดหมู่ของข้อมูลเป็น ๕ หมวดหมู่ มีนิยามและที่มา ดังนี้

๑.๑.๑) ข้อมูลส่วนบุคคล

(๑) ข้อมูลส่วนบุคคล (Personal Data) หมายถึง ข้อมูลเกี่ยวกับบุคคล ซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรม (ตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล)

(๒) ข้อมูลส่วนบุคคลอ่อนไหว (Sensitive Personal Data) หมายถึง ข้อมูลที่มีลักษณะเฉพาะและมีความอ่อนไหวสูง ซึ่งอาจส่งผลกระทบต่อเจ้าของข้อมูล หากถูกนำไปใช้โดยไม่ได้รับความยินยอมโดยชัดแจ้ง ทั้งนี้ ตามมาตรา ๒๖ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ข้อมูลดังกล่าวครอบคลุมถึงเชื้อชาติ เผ่าพันธุ์ ความคิดเห็น ทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใด

๑.๑.๒) ข้อมูลความมั่นคง (National Security Information) หมายถึง ข้อมูลข่าวสารเกี่ยวกับความมั่นคงของประเทศที่อยู่ในความครอบครอง หรือความควบคุมดูแลของหน่วยงานของรัฐที่ไม่สามารถรู้หรือไม่สามารถเข้าถึงได้โดยทั่วไป ซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะส่งผลให้ประเทศต้องเผชิญกับภัยคุกคามต่อเอกราช อธิปไตย บูรณภาพแห่งอาณาเขตการปกครองระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุข สถาบันศาสนา สถาบันพระมหากษัตริย์ ความสัมพันธ์ระหว่างประเทศ การทหารและการข่าวกรอง ความปลอดภัย และการดำรงชีวิตโดยปกติสุขของประชาชน

๑.๑.๓) ข้อมูลสาธารณะ (Public) หมายถึง ข้อมูลหรือข่าวสารสาธารณะที่หน่วยงานของรัฐจัดทำ และครอบครองในรูปแบบและช่องทางดิจิทัล เพื่อให้ประชาชนเข้าถึงได้โดยสะดวก มีส่วนร่วมและตรวจสอบการดำเนินงานของรัฐ และสามารถนำข้อมูลไปพัฒนาบริการและนวัตกรรมที่จะเป็นประโยชน์ต่อประเทศในด้านต่าง ๆ

๑.๑.๔) ข้อมูลใช้ภายใน (Internal Use Only) หมายความว่า ข้อมูลสำหรับใช้ในการดำเนินกิจการภายในของหน่วยงาน ซึ่งไม่อนุญาตให้นำไปใช้งานภายนอกก่อนได้รับอนุญาตจากเจ้าของข้อมูล เช่น ร่างนโยบาย ร่างมาตรฐาน และขั้นตอนการปฏิบัติงาน ประกาศ และบันทึกภายในหน่วยงานที่อยู่ระหว่างการขออนุมัติ เป็นต้น

๑.๑.๕) ข้อมูลความลับทางราชการ (Classified Information) หมายถึง ข้อมูลข่าวสารที่เป็นความลับ ตามกฎหมายว่าด้วยข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐ ที่มีคำสั่งไม่ให้เปิดเผยและอยู่ในความครอบครองหรือควบคุมดูแลของหน่วยงานของรัฐ ไม่ว่าจะเป็นเรื่องที่เกี่ยวกับการดำเนินงานของรัฐ หรือที่เกี่ยวกับเอกชน ซึ่งมีการกำหนดให้มีชั้นความลับเป็น ชั้นลับ ชั้นลับมาก หรือชั้นลับที่สุด ตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ และที่แก้ไขเพิ่มเติม โดยคำนึงถึงการปฏิบัติหน้าที่ของหน่วยงานของรัฐและประโยชน์แห่งรัฐประกอบกัน

๑.๒) ต้องจัดเก็บข้อมูลตามระดับชั้นของข้อมูล โดยกรมธนารักษ์มีการจัดระดับชั้นของข้อมูลแบ่งเป็น ๕ ระดับ ดังนี้

๑.๒.๑) ชั้นเปิดเผย (Open) หมายถึง ข้อมูลที่สามารถเปิดเผยต่อสาธารณะได้เท่าที่ไม่ส่งผลกระทบต่อการบังคับใช้กฎหมาย หรือทำให้การบังคับใช้กฎหมายเสื่อมประสิทธิภาพ รวมถึงเป็นข้อมูลข่าวสารของราชการที่หน่วยงานของรัฐต้องเปิดเผยให้ประชาชนได้รับรู้ รับทราบ หรือตรวจสอบได้โดยไม่จำเป็นต้องร้องขอ เช่น กฎ มติคณะรัฐมนตรี ข้อบังคับ รายงานผลการศึกษาทางวิชาการ และข้อมูลเปิดภาครัฐ เป็นต้น และไม่มีการจำกัดการเข้าถึงข้อมูลหรือเปิดเผยสู่สาธารณะ

๑.๒.๒) ชั้นเผยแพร่ภายในหน่วยงาน (Private) หมายถึง ข้อมูลข่าวสารที่ใช้ภายในหน่วยงานของรัฐ เพื่อใช้ในภารกิจความมั่นคงทางการคลังของกรมธนารักษ์ เป็นข้อมูลสำหรับเปิดเผยสำหรับผู้ที่เกี่ยวข้อง เจ้าหน้าที่ในกรมธนารักษ์ หรือเปิดเผยเฉพาะข้าราชการที่มีอำนาจหน้าที่

๑.๒.๓) ชั้นลับ (Confidential) หมายถึง ข้อมูลลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐ และส่งผลให้เกิดความอับอายอย่างมากต่อบุคคลหรือหน่วยงาน เช่น ข้อมูลการฟ้องคดี และความเห็นภายในหน่วยงานที่ยังไม่ได้ข้อยุติ เป็นต้น และมีการจำกัดการเข้าถึงเฉพาะบุคคลที่จำเป็นต้องรู้หรือมีสิทธิ์รู้ และลงนามข้อตกลงไม่เปิดเผยข้อมูล (Non-Disclosure Agreements) สามารถตรวจสอบคำขอการเข้าถึงข้อมูล การทบทวน การอนุมัติ และกระบวนการยกเลิกได้

๑.๒.๔) ชั้นลับมาก (Secret) หมายถึง ข้อมูลลับซึ่งหากเปิดเผยทั้งหมด หรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรง อาจทำให้เสียชื่อเสียงและการสูญเสียทางการเงินหรือทรัพย์สิน เช่น รายงานการแพทย์ ข้อมูลความสัมพันธ์ระหว่างประเทศ และนโยบายสำคัญที่ใช้ปฏิบัติต่อรัฐต่างประเทศ เป็นต้น

๑.๒.๕) ชั้นลับที่สุด (Top Secret) หมายถึง ข้อมูลลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งภาครัฐอย่างร้ายแรงที่สุด อาจทำให้ชื่อเสียงและการสูญเสียทางการเงินหรือทรัพย์สิน ซึ่งในกรณีข้อมูลที่อยู่ในชั้น “ลับที่สุด” จะไม่สามารถนำเข้าในระบบสารสนเทศได้ ต้องดำเนินการในรูปแบบเอกสาร (Hard Copy) เท่านั้น เช่น ข้อมูลด้านการข่าวกรองยุทธศาสตร์ ข้อมูลความมั่นคงเชิงนโยบาย

๑.๓) เจ้าของข้อมูลกำหนดระยะเวลาในการจัดเก็บข้อมูล (Store) ที่ชัดเจน โดยจะต้องสอดคล้องกับข้อบังคับทางกฎหมายหรือข้อบังคับที่เกี่ยวข้อง อาทิ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ กำหนดให้ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่า ๙๐ วันนับตั้งแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์

๑.๔) เจ้าของข้อมูลจะต้องกำหนดประเภทของการดำเนินงานหลังข้อมูลหมดระยะเวลาจัดเก็บข้อมูล ได้แก่ การจัดเก็บถาวร หรือการทำลายข้อมูล โดยการกำหนดประเภทการดำเนินงานหลังข้อมูลหมดระยะเวลาจัดเก็บข้อมูล จะต้องคำนึงถึงบริบทของข้อมูลดังกล่าว ข้อบังคับของหน่วยงาน และกฎหมายที่เกี่ยวข้อง

๑.๕) กำหนดกระบวนการการสำรองข้อมูลที่จัดเก็บ (Backup) ให้มีความถูกต้องครบถ้วนและเป็นปัจจุบัน เพื่อป้องกันกรณีข้อมูลสูญหายโดยเหตุสุดวิสัย

๑.๖) ทีมบริหารจัดการข้อมูล และผู้ดูแลระบบสารสนเทศทำการย้ายข้อมูลที่มีการจัดเก็บเกินระยะเวลาที่กำหนดแล้วเพื่อนำข้อมูลเข้าสู่กระบวนการจัดเก็บถาวรหรือทำลายข้อมูลตามที่ได้มีการกำหนดไว้

๑.๗) กำหนดให้การจัดเก็บชุดข้อมูลจะต้องมีคำอธิบายชุดข้อมูล (Metadata) หากไม่มีหรือไม่ครบถ้วน ทีมบริหารจัดการข้อมูลจะต้องแจ้งผู้รับผิดชอบ ได้แก่ เจ้าของข้อมูล บริกรข้อมูลด้านเทคนิค และบริกรข้อมูลด้านธุรกิจ โดยทีมบริหารจัดการข้อมูลร่วมกันจัดทำและปรับปรุงให้เป็นปัจจุบัน

๑.๘) ผู้มีส่วนได้ส่วนเสียเกี่ยวข้องกับข้อมูล ทั้งเจ้าของข้อมูล ผู้สร้างข้อมูล ผู้ใช้ข้อมูล และทีมบริหารจัดการข้อมูล จะต้องจัดเก็บข้อมูลตามการจัดระดับชั้นข้อมูล โดยทำการเข้ารหัสข้อมูลเพื่อป้องกันการเข้าถึงหรือแก้ไขข้อมูลโดยไม่ได้รับอนุญาต ทั้งนี้ การเข้ารหัสข้อมูลให้ปฏิบัติตาม วิธีการเข้ารหัสข้อมูลแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

๑.๘.๑) ในกรณีที่ข้อมูลในตารางฐานข้อมูลเดียวกันมีฟิลด์ข้อมูลที่มีระดับชั้นความลับและไม่มีระดับชั้นความลับอยู่ร่วมกัน หากฐานข้อมูลสามารถดำเนินการเข้ารหัสเฉพาะคอลัมน์ (Column) ได้ให้ทำการเข้ารหัสข้อมูลเฉพาะฟิลด์ข้อมูลที่มีระดับชั้นความลับเท่านั้น

๑.๘.๒) ในกรณีข้อมูลดิจิทัลที่ไม่เป็นข้อมูลที่มีโครงสร้างสำหรับการดำเนินงานในหน่วยงานทั่วไป เช่น ลักษณะไฟล์ Word PowerPoint หรือ Excel กำหนดให้มีการเข้ารหัสข้อมูลไฟล์ดังกล่าว ตามระดับชั้นข้อมูล

๑.๘.๓) ในกรณีที่มีการจัดเก็บข้อมูลในรูปแบบเอกสาร ควรจัดเก็บในสถานที่ที่เหมาะสม และสามารถปิดล็อกได้เมื่อไม่ใช้งาน โดยต้องแยกเอกสารออกจากอุปกรณ์ประมวลผลต่าง ๆ เช่น เครื่องพิมพ์หรือเครื่องถ่ายเอกสารทันทีหลังใช้งาน เพื่อป้องกันไม่ให้ผู้ที่ไม่มีสิทธิ์สามารถเข้าถึงข้อมูลได้ นอกจากนี้ เอกสารดังกล่าวต้องอยู่ภายใต้การดูแลตลอดเวลา หรือจัดเก็บในสถานที่ที่มีมาตรการป้องกันการเข้าถึงจากบุคคลที่ไม่ได้รับอนุญาตอย่างเหมาะสม

๑.๙) กำหนดให้มีมาตรการรักษาความปลอดภัยในการจัดเก็บข้อมูล (Store) รวมทั้งกรณีที่มีการเคลื่อนย้าย อุปกรณ์ที่จัดเก็บข้อมูล เพื่อป้องกันมิให้มีการเข้าถึงโดยมิได้รับอนุญาต หรือลักลอบนำข้อมูลไปใช้ที่ก่อให้เกิดความเสียหายต่อหน่วยงาน

๑.๑๐) กำหนดให้มีมาตรการรักษาความปลอดภัยของการถ่ายโอนข้อมูลสำหรับกระบวนการจัดเก็บข้อมูลกับหน่วยงานภายนอกที่ผ่านช่องทางการสื่อสารทุกชนิด โดยต้องสอดคล้องตามนโยบายความมั่นคงปลอดภัยสารสนเทศ

๑.๑๑) กำหนดให้มีการทบทวนเกี่ยวกับช่วงระยะเวลาการจัดเก็บข้อมูล (Store) มาตรการและวิธีปฏิบัติที่เกี่ยวข้องกับการจัดเก็บข้อมูลถาวร (Archive) อย่างน้อยปีละ ๑ ครั้ง

๒) การจัดเก็บแฟ้มข้อมูลลับให้ปฏิบัติ ดังนี้

๒.๑) ผู้ที่เป็นเจ้าของแฟ้มข้อมูลลับต้องตรวจสอบความถูกต้องของแฟ้มข้อมูลลับก่อนนำไปใช้งาน

๒.๒) ต้องป้องกันแฟ้มข้อมูลลับที่มีการจัดเก็บไว้ในเครื่องคอมพิวเตอร์ที่ตนเองใช้งาน โดยเครื่องคอมพิวเตอร์ต้องมีการตั้งรหัสผ่านที่มีความมั่นคงปลอดภัย ต้องมีการเข้ารหัสลับ (Encryption) แฟ้มข้อมูลลับ และเมื่อมีการนำแฟ้มข้อมูลลับไปใช้งาน ให้ปฏิบัติตามกฎหมายว่าด้วยการรักษาความลับทางราชการอย่างเคร่งครัด

๒.๓) ต้องระมัดระวังการกระจาย หรือแจกจ่ายแฟ้มข้อมูลลับของกรมธนารักษ์ไปยังกลุ่มผู้รับที่มีความจำเป็นต้องรับรู้เท่านั้น

๒.๔) ห้ามเผยแพร่/แลกเปลี่ยน/แบ่งปัน แฟ้มข้อมูลลับบนเครือข่ายของกรมธนารักษ์ไม่ว่าบุคคลผู้นั้นจะได้รับอนุญาตให้เข้าถึงข้อมูลได้หรือไม่ก็ตาม เนื่องจากในระหว่างที่มีการเผยแพร่/แลกเปลี่ยน/แบ่งปัน แฟ้มข้อมูลลับ บุคคลอื่นอาจเข้าถึงแฟ้มข้อมูลลับนั้นได้

๒.๕) ต้องตรวจสอบการทำงานของระบบป้องกันไวรัสอย่างสม่ำเสมอในเครื่องคอมพิวเตอร์ที่ใช้จัดเก็บแฟ้มข้อมูลลับ ว่าระบบป้องกันไวรัสสามารถทำงานป้องกันไวรัสได้เป็นปกติ

๒.๖) ต้องตรวจสอบการทำงานของเครื่องคอมพิวเตอร์ที่ตนเองใช้งานอย่างสม่ำเสมอ ว่ามีการติดตั้งโปรแกรมแก้ไขช่องโหว่ของซอฟต์แวร์ (Patch) ที่ทันสมัยในเครื่องอย่างสม่ำเสมอหรือไม่

๒.๗) ต้องสำรองแฟ้มข้อมูลลับในเครื่องคอมพิวเตอร์ที่ตนเองใช้งานอย่างสม่ำเสมอ เอกสารที่เป็นความลับ หรือมีความสำคัญ ซึ่งพิมพ์ออกมาจากเครื่องพิมพ์ เจ้าหน้าที่ต้องปฏิบัติให้เป็นไปตามกฎหมายว่าด้วยการรักษาความลับทางราชการ ดังต่อไปนี้

๒.๗.๑) ต้องจัดหมวดหมู่เอกสารที่เป็นความลับ หรือมีความสำคัญไว้ต่างหาก

๒.๗.๒) ต้องมีกระบวนการจัดเก็บข้อมูล และกำหนดวิธีการป้องกันที่มีความปลอดภัยอย่างเพียงพอ

๒.๗.๓) สำเนาเอกสารที่เป็นความลับ หรือเอกสารที่มีความสำคัญ ต้องได้รับอนุญาตจากผู้เป็นเจ้าของ

๒.๗.๔) ให้ระมัดระวังการแจกจ่ายเอกสารที่เป็นความลับของกรมธนารักษ์ไปยังกลุ่มผู้รับที่มีความจำเป็นต้องรับรู้เท่านั้น

๒.๗.๕) ต้องตรวจสอบความถูกต้องของเอกสารก่อนนำไปใช้งาน

๒.๗.๖) ต้องทำลายเอกสารที่เป็นความลับ หรือมีความสำคัญ เมื่อหมดความจำเป็นในการใช้งาน

๓) การจัดเก็บข้อมูลส่วนบุคคลให้ปฏิบัติ ดังนี้

๓.๑) ให้เก็บรวบรวมได้เท่าที่จำเป็น ภายใต้อำนาจหน้าที่ และวัตถุประสงค์อันชอบตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลและไม่เก็บรวบรวมข้อมูลส่วนบุคคล ดังต่อไปนี้ เว้นแต่ได้รับการยินยอมจากเจ้าของข้อมูลส่วนบุคคล หรือพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล หรือกฎหมายอื่นบัญญัติให้กระทำได้ เชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสุขภาพจิต ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม หรือข้อมูลชีวภาพข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลในทำนองเดียวกันตามที่หน่วยงานกำหนด

๓.๒) กำหนดให้มีการยกเลิกการจัดเก็บข้อมูลส่วนบุคคลกรณีเจ้าของข้อมูลส่วนบุคคลถอนความยินยอมตามที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลกำหนด

๔) ข้อมูลทุกประเภท ทั้งข้อมูลที่เป็นกระดาษ และข้อมูลที่เป็นอิเล็กทรอนิกส์ ต้องมีการบ่งชี้ระดับชั้นข้อมูล (Data Labeling) โดยข้อมูลที่เป็นกระดาษ ให้ปฏิบัติตามกฎหมายว่าด้วยการรักษาความลับทางราชการ และข้อมูลที่เป็นอิเล็กทรอนิกส์ ให้ดำเนินการระบุชั้นข้อมูลด้วยวิธีการ เช่น การทำลายน้ำ การใส่ชั้นระดับชั้นข้อมูลที่ตารางทำการ (Worksheet) หรือการใส่ชั้นความลับที่หัวท้ายกระดาษ (Header/Footer) เป็นต้น

หมวดที่ ๓ การประมวลผลข้อมูลและการใช้ข้อมูล (Data Processing and Use)

๑) การประมวลผลข้อมูลให้ปฏิบัติ ดังนี้

๑.๑) ข้าราชการ เจ้าหน้าที่ ลูกจ้าง พนักงานราชการ ผู้ดูแลระบบ ผู้รับจ้างตามสัญญา รวมถึง นิสิต นักศึกษาฝึกงาน ต้องปฏิบัติตามขั้นตอนการประมวลผลข้อมูลและการใช้ข้อมูลที่กรมธนารักษ์กำหนดขึ้น เพื่อให้มีสิทธิ์การใช้งานระบบสารสนเทศตามความจำเป็น

๑.๒) ผู้ประมวลผลข้อมูลต้องตรวจสอบความถูกต้องของข้อมูลก่อนนำไปประมวลผล

๑.๓) การประมวลผลข้อมูลที่เป็นความมั่นคงทางการคลัง เช่น ข้อมูลการปรับเงินเดือนบุคลากร ข้อมูลค่าเช่าที่ราชพัสดุ ข้อมูลการรับแลก-จ่ายแลกเหรียญกษาปณ์หมุนเวียน ให้เป็นไปตามขอบเขตเงื่อนไข หรือวัตถุประสงค์ในการใช้อำนาจรัฐที่ได้มอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคลตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลสามารถทำได้ โดยไม่ต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

๑.๔) การประมวลผลข้อมูลที่เป็นความลับ เช่น ข้อมูลส่วนบุคคล ให้เป็นไปตามขอบเขตเงื่อนไข หรือวัตถุประสงค์ในการยินยอมให้ดำเนินการกับข้อมูลส่วนบุคคลนั้น

๑.๕) กรณีข้อมูลมีการควบคุมโดยการเข้ารหัสลับ (Encryption) ในการประมวลผลข้อมูลต้องบันทึกหลักฐานไว้ทุกครั้ง เพื่อการตรวจสอบในภายหลัง และสามารถจัดพิมพ์เป็นรายงานเพื่อการตรวจสอบได้

๑.๖) ต้องมีการจัดทำเมทาดาตา (Metadata) สำหรับข้อมูลที่จัดเก็บอยู่ในคลังข้อมูล

๑.๗) การประมวลผลข้อมูล ให้คำนึงถึงความมั่นคงปลอดภัยด้านสารสนเทศ

๑.๘) การประมวลผลข้อมูลหรือใช้ข้อมูลส่วนบุคคล ต้องประมวลผล หรือใช้ข้อมูลเท่าที่จำเป็นภายใต้อำนาจหน้าที่ และวัตถุประสงค์อันชอบด้วยกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

๑.๙) ต้องมีมาตรการรักษาความมั่นคงปลอดภัยในการประมวลผลข้อมูลที่ได้กำหนดชั้นข้อมูลตั้งแต่ลับขึ้นไป อย่างเพียงพอและมีประสิทธิภาพ

๒) การใช้ข้อมูลให้ปฏิบัติ ดังนี้

๒.๑) ให้ใช้ข้อมูลสารสนเทศของกรมธนารักษ์ทั้งที่มีอยู่ภายในหน่วยงาน หรือได้รับข้อมูลจากภายนอกหน่วยงาน หรือข้อมูลที่อยู่บนระบบเครือข่ายรัษฎากร ระบบอินเทอร์เน็ต และระบบงานต่าง ๆ เพื่องานในราชการเท่านั้น กรณีข้อมูลที่มีความสำคัญหรือชั้นความลับ ต้องมีการกำหนดสิทธิ์ผู้ใช้งานและสิทธิ์ในการเข้าถึง ระยะเวลาที่นำข้อมูลไปใช้งาน วัตถุประสงค์ในการใช้งานข้อมูล

๒.๒) ห้ามมิให้ใช้ข้อมูลของกรมธนารักษ์เพื่อประโยชน์ในเชิงธุรกิจเป็นการส่วนตัว หรือใช้ข้อมูลอันอาจก่อให้เกิดความเสียหายต่อหน่วยงาน

๒.๓) การใช้งานข้อมูล ผู้ใช้งานจะใช้งานข้อมูลได้เฉพาะในส่วนที่ได้รับอนุญาต ตามการกำหนดสิทธิ์จากผู้ดูแลระบบคอมพิวเตอร์เท่านั้น

๒.๔) กรณีเป็นข้อมูลส่วนบุคคล และเข้าถึงบางส่วน หรือทุกรายการ หน่วยงานที่ถือครองข้อมูลต้องมีมาตรการในการปกปิดไม่ให้หน่วยงานที่ขอใช้ข้อมูล สามารถทราบได้ว่าข้อมูลแต่ละรายการเป็นของบุคคลใด โดยอ้างอิง “แนวปฏิบัติในการปกป้องข้อมูลที่ระบุตัวบุคคลได้ (Guideline to Protect The Personally Identifiable Information)”

๒.๕) กรณีเป็นข้อมูลส่วนบุคคล ที่มีการเข้าถึงเป็นรายบุคคล หากเป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล ตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลสามารถทำได้ตามอำนาจหน้าที่ โดยไม่ต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

หมวดที่ ๔ การเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน (Data Integration and Exchange)

๑) การเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน ต้องมีการตรวจสอบระดับชั้นของข้อมูล (Data Classification) ดังนี้

๑.๑) ตรวจสอบระดับชั้นของข้อมูล (Data Classification) ว่าอยู่ในชั้นความลับที่สามารถเปิดเผยได้หรือไม่ ทั้งนี้ ต้องไม่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ ความมั่นคงของประเทศ ความลับทางราชการและความเป็นส่วนตัว

๑.๒) กำหนดระดับชั้นของข้อมูล และจัดเก็บให้สอดคล้องกับแนวทางหรือมาตรฐานการจัดระดับชั้นของข้อมูล (Data Classification Standard) ที่กำหนดไว้ เพื่อให้มั่นใจได้ว่าข้อมูลมีความมั่นคงปลอดภัยและรักษาคุณภาพของข้อมูล

๑.๓) มาตรฐานระดับชั้นข้อมูล (Data Classification Standard) คือ การกำหนดรูปแบบและข้อกำหนดของการจัดชั้นความลับของข้อมูล เพื่อป้องกันการเข้าถึงและสามารถนำข้อมูลไปใช้ได้อย่างเหมาะสม

๑.๔) การบริหารจัดการข้อมูลตามระดับชั้นของข้อมูล ซึ่งมี ๕ ระดับ ดังนี้

๑.๔.๑) ชั้นเปิดเผย (Open) หมายถึง ข้อมูลข่าวสารตามมาตรา ๗ และมาตรา ๙ ตามพระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. ๒๕๔๐ เป็นข้อมูลข่าวสารที่สามารถเปิดเผยได้เป็นการทั่วไป รวมถึงเป็นข้อมูลข่าวสารของราชการที่หน่วยงานของรัฐต้องเปิดเผยให้ประชาชนได้รับรู้ รับทราบ หรือตรวจสอบได้ โดยไม่จำเป็นต้องร้องขอ เช่น กฎ มติคณะรัฐมนตรี ข้อบังคับ รายงานผลการศึกษาทางวิชาการ และข้อมูลเปิดภาครัฐ เป็นต้น และไม่มีการจำกัดการเข้าถึงข้อมูลหรือเปิดเผยสู่สาธารณะ

๑.๔.๒) ชั้นเผยแพร่ภายในหน่วยงาน (Private) หมายถึง ข้อมูลข่าวสารที่ใช้ภายในหน่วยงานของรัฐ เพื่อใช้ในภารกิจความมั่นคงทางการคลังของกรมธนารักษ์เป็นข้อมูลสำหรับเปิดเผยสำหรับผู้ที่เกี่ยวข้อง เจ้าหน้าที่ในกรมธนารักษ์ หรือเปิดเผยเฉพาะข้าราชการที่มีอำนาจหน้าที่

๑.๔.๓) ชั้นลับ (Confidential) คือ ข้อมูลซึ่งหากเปิดเผยทั้งหมดหรือบางส่วน จะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐ และส่งผลให้เกิดความอับอายอย่างมากต่อบุคคลหรือหน่วยงาน เช่น ข้อมูลการฟ้องคดี และความเห็นภายในหน่วยงานที่ยังไม่ได้ข้อยุติ เป็นต้น และมีการจำกัดการเข้าถึงเฉพาะบุคคลที่จำเป็นต้องรู้หรือมีสิทธิ์รู้ และลงนามข้อตกลงไม่เปิดเผยข้อมูล (Non-Disclosure Agreements) สามารถตรวจสอบคำขอการเข้าถึงข้อมูล การทบทวน การอนุมัติ และกระบวนการยกเลิกได้

๑.๔.๔) ชั้นลับมาก (Secret) คือ ข้อมูลซึ่งหากเปิดเผยทั้งหมดหรือบางส่วน จะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรง รวมถึงอาจทำให้เสียชื่อเสียงและการสูญเสียทางการเงินหรือทรัพย์สิน เช่น รายงานการแพทย์ ข้อมูลความสัมพันธ์ระหว่างประเทศ และนโยบายสำคัญที่ใช้ปฏิบัติต่อรัฐต่างประเทศ เป็นต้น

๑.๔.๕) ชั้นลับที่สุด (Top Secret) คือ ข้อมูลซึ่งหากเปิดเผยทั้งหมดหรือบางส่วน จะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งภาครัฐร้ายแรงที่สุด อาจทำให้ชื่อเสียงและการสูญเสียทางการเงินหรือทรัพย์สิน ซึ่งในกรณีข้อมูลที่อยู่ในชั้น “ลับที่สุด” จะไม่สามารถนำเข้าในระบบสารสนเทศได้ ต้องดำเนินการในรูปแบบเอกสาร (Hard Copy) เท่านั้น เช่น ข้อมูลด้านการข่าวกรองยุทธศาสตร์ ข้อมูลความมั่นคงเชิงนโยบาย

๒) ต้องมีการจัดทำเมทาดาตา (Metadata)

๒.๑) มาตรฐานเมทาดาตา (Metadata Standard) หมายถึง ข้อมูลเกี่ยวกับข้อมูล (Data about Data) เป็นข้อมูลที่ใช้กำกับเพื่ออธิบายข้อมูล หรือกลุ่มของข้อมูลอธิบายรายละเอียดของข้อมูลหรือสารสนเทศ ทำให้ทราบรายละเอียดและคุณลักษณะของข้อมูล เช่น เมทาดาตาต้องประกอบไปด้วยอย่างน้อย ๑๕ ส่วน ดังต่อไปนี้

๒.๑.๑) เลขที่เมทาดาตา คือ เลขทะเบียนคุมเมทาดาตาของหน่วยงาน

๒.๑.๒) ชื่อชุดข้อมูล เป็นการอธิบายข้อมูลในเมทาดาตานั้น เช่น ข้อมูลผู้ใช้งานระบบงาน ข้อมูลราคาประเมินที่ดิน ข้อมูลการเช่าที่ราชพัสดุ เป็นต้น

๒.๑.๓) เจ้าของข้อมูล เป็นการอธิบายว่าหน่วยงานใดเป็นเจ้าของเมทาดาตานี้ เช่น ข้อมูลทางทะเบียนที่ดิน กรมที่ดินเป็นเจ้าของข้อมูล เป็นต้น

๒.๑.๔) คำอธิบายข้อมูล เป็นคำอธิบายสั้น ๆ เพื่อให้รู้ว่าเมทาดาตาอันนี้คือข้อมูลอะไร

๒.๑.๕) คำสำคัญ

๒.๑.๖) วันที่ทำการเปลี่ยนแปลงข้อมูลล่าสุด

๒.๑.๗) แหล่งที่มาของข้อมูล เป็นการอธิบายว่าข้อมูลในเมทาดาตานี้ได้มาอย่างไร เช่น ข้อมูลนำเข้าจากกระทรวงมหาดไทย เป็นต้น

๒.๑.๘) รูปแบบการจัดเก็บข้อมูล เป็นการอธิบายเพื่อให้รู้ว่าข้อมูลดังกล่าวเก็บข้อมูลแบบไหน เช่น Database, CSV, XML, JSON, Text, VDO และกระดาษ เป็นต้น

๒.๑.๙) ขอบเขตที่เผยแพร่ข้อมูล เป็นการอธิบาย เพื่อให้รู้ว่าข้อมูลดังกล่าวสามารถเผยแพร่ข้อมูลได้ในระดับไหน เช่น ภายในหน่วยงาน ระหว่างหน่วยงาน ภายในขอบเขตความร่วมมือ ระหว่างประเทศ ไม่จำกัดขอบเขต (สาธารณะ)

๒.๑.๑๐) สิทธิ์ในการเข้าถึงข้อมูลหลังจากเผยแพร่ เป็นการอธิบายเพื่อให้รู้ว่าหลังจากเผยแพร่ข้อมูลแล้ว จะมีสิทธิ์อย่างไร เช่น View, Modify

๒.๑.๑๑) สิทธิ์ในการใช้ข้อมูล เป็นการอธิบายสิทธิ์ในการใช้ข้อมูล เช่น ใช้โดยอิสระ ให้เมื่อร้องขอสัญญาอนุญาต ขอบเขตความร่วมมือ

๒.๑.๑๒) การ Backup ข้อมูล เป็นการอธิบายถึงการ Backup เมทาดาตาว่ามีการ Backup แบบไหน เช่น Full, Differential, Incremental

๒.๑.๑๓) ระยะเวลาในการเก็บข้อมูล เป็นการอธิบายว่าข้อมูลในเมทาดาตานี้มีการเก็บข้อมูลโดยใช้หน่วยจัดเก็บอะไร เช่น ปี

๒.๑.๑๔) ข้อกำหนดในการล้างข้อมูล เป็นการอธิบายว่าข้อมูลในเมทาดาตานี้จะถูกล้างข้อมูลตามเงื่อนไขใด เช่น ตามกฎหมายกำหนด

๒.๑.๑๕) ภาษาที่ใช้ เป็นการอธิบายภาษาที่ใช้ในการเข้าถึงข้อมูลในเมทาดาตา เช่น SQL

๒.๒) จัดทำเมทาดาตา (Metadata) ของชุดข้อมูลที่ทำการแลกเปลี่ยน โดยต้องตรวจสอบให้แน่ใจได้ว่าเมทาดาตามีฟิลด์ข้อมูลครบถ้วน สอดคล้องกับความต้องการของหน่วยงานที่ขอใช้ข้อมูล

๓) กรณีข้อมูลที่เป็นความลับหากจำเป็นต้องแลกเปลี่ยนข้อมูล หน่วยงานปลายทางจะต้องมีการจัดทำธรรมาภิบาลข้อมูลในระดับเดียวกัน หากไม่มีการจัดทำธรรมาภิบาลข้อมูลต้องมีการทำสัญญาอนุญาตหรือเงื่อนไขในการแลกเปลี่ยนและการนำข้อมูลไปใช้ ตัวอย่างส่วนประกอบของสัญญา เช่น วัตถุประสงค์ในการนำไปใช้ ขอบเขตในการนำไปใช้ ช่วงวันที่ในการเข้าถึง ความถี่ในการเข้าถึง ช่วงเวลาในการนำไปใช้ ฟิลด์ที่สามารถเข้าถึง และรายการที่สามารถเข้าถึง โดยการแลกเปลี่ยนข้อมูลลับ ต้องดำเนินการอย่างน้อย ดังนี้

๓.๑) กำหนดแนวปฏิบัติและสัญญาอนุญาตในการแลกเปลี่ยนข้อมูลเพื่อให้มั่นใจได้ว่าข้อมูลจะยังคงความมั่นคงปลอดภัยและรักษาคุณภาพของข้อมูล เช่น การจัดการเรื่องความมั่นคงปลอดภัยและคุณภาพข้อมูล ผู้ประสานงาน หรือศูนย์ติดต่อ Contact Center

๓.๒) กำหนดกระบวนการในการแลกเปลี่ยนข้อมูลที่ชัดเจนตั้งแต่เตรียมการ เริ่มดำเนินการ ระหว่างดำเนินการ และสิ้นสุดการดำเนินการ

๓.๓) กำหนดรายการชุดข้อมูลมาตรฐานเมทาดาตา (Metadata) ของชุดข้อมูลมาตรฐานและข้อตกลงในการแลกเปลี่ยนข้อมูล

๓.๔) กำหนดเทคโนโลยีและมาตรฐานทางเทคนิคที่ใช้ในการแลกเปลี่ยนข้อมูล

๓.๕) ต้องมีการบันทึกการใช้งาน (Log File) เพื่อให้สามารถตรวจสอบย้อนกลับได้

๓.๖) ตรวจสอบให้แน่ใจว่าการแลกเปลี่ยนข้อมูลถูกดำเนินการได้อย่างเหมาะสมหรือเป็นไปตามแนวปฏิบัติ กระบวนการแลกเปลี่ยน และมาตรฐานที่กำหนด

๔) กำหนดสิทธิ์ของหน่วยงานที่สามารถนำข้อมูลไปใช้ได้ตามบทบาทและภารกิจตามกฎหมายของหน่วยงานนั้น ๆ

๕) กรณีที่หน่วยงานที่ขอข้อมูลเป็นหน่วยงานพิเศษที่มีอำนาจในการเข้าถึงข้อมูล เช่น กรมสอบสวนคดีพิเศษ สำนักงานป้องกันและปราบปรามการฟอกเงิน สำนักงานคณะกรรมการป้องกัน

และปราบปรามยาเสพติด สำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตแห่งชาติ หน่วยงานศาล หน่วยงานที่ขอข้อมูลจะต้องมีการจัดทำธรรมาภิบาลข้อมูลของหน่วยงานในระดับที่เทียบเท่า หรือสูงกว่า แต่หากหน่วยงานดังกล่าวยังไม่มีการจัดทำธรรมาภิบาลข้อมูล การนำข้อมูลที่ได้รับจากกรมธนารักษ์ให้นำไปใช้ตามอำนาจหน้าที่ของหน่วยงานเท่านั้น ห้ามนำไปเผยแพร่ต่อโดยเด็ดขาด

๖) การไม่แสดงตัวตน (Anonymization) กรณีที่หน่วยงานที่ขอข้อมูลไม่มีอำนาจในการเข้าถึงข้อมูลส่วนบุคคลแต่ต้องการใช้ข้อมูลเพื่อทำการศึกษาหรือวิจัย ต้องอ้างอิงแนวปฏิบัติในการปกป้องข้อมูลที่ระบุตัวบุคคลได้ พร้อมทั้งตรวจสอบและปรับปรุงคุณภาพของข้อมูล (Data Quality) ให้อยู่ในเกณฑ์มาตรฐานก่อนการเชื่อมโยงและแลกเปลี่ยน

๗) ต้องมีการเข้ารหัสลับ (Encryption) ข้อมูลก่อนการแลกเปลี่ยนข้อมูลบางประเภท เช่น ข้อมูลความมั่นคงประเทศ ข้อมูลส่วนบุคคล เป็นต้น

๘) ต้องดำเนินการแลกเปลี่ยนข้อมูลตามเงื่อนไขและมาตรฐานการแลกเปลี่ยนที่กำหนดไว้อย่างน้อย ดังนี้

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

๘.๒) กำหนดนโยบายและมาตรฐานเกี่ยวกับการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างอุปกรณ์

๘.๓) กำหนดกระบวนการที่ใช้ในการดำเนินการบูรณาการข้อมูล (Data Integration) คือ การมีระบบเชื่อมโยงข้อมูลกลางที่บูรณาการข้อมูลแบบครบวงจร มีการจัดทำข้อมูลหลัก (Master Data) คลังข้อมูล (Data Warehouse) ทะเลสาบข้อมูล (Data Lake) โดยมีมาตรฐานในการจัดเก็บและแลกเปลี่ยน

๙) ข้อตกลงในการแลกเปลี่ยนข้อมูลและการนำข้อมูลไปใช้ จะต้องบันทึกไว้ในแบบแผนมาตรฐานระดับชั้นข้อมูลเพื่อป้องกันไม่ให้บุคคลที่มีสิทธิ์ไม่ถึงระดับชั้นนั้นนำข้อมูลไปใช้ นอกจากนี้บุคคลที่จะแลกเปลี่ยนข้อมูลต้องมั่นใจว่าได้เลือกใช้ระบบเทคโนโลยีสารสนเทศที่มีความปลอดภัยในกระบวนการแลกเปลี่ยนข้อมูลที่เหมาะสมแล้ว ยกตัวอย่างเช่น การแลกเปลี่ยนข้อมูลผ่านจดหมายอิเล็กทรอนิกส์ ควรทำการเข้ารหัสลับข้อความอีเมลด้วย S/MIME หรือถ้าแลกเปลี่ยนข้อมูลผ่านระบบใช้ไฟล์ร่วมกัน (File Sharing) ควรใช้ช่องทางที่มีการเข้ารหัส เช่น SFTP หรือ SSH เป็นต้น และหากมีการส่งไฟล์ให้ดำเนินการเข้ารหัสไฟล์ โดยใช้รหัสผ่านที่ปลอดภัย และดำเนินการแจ้งรหัสผ่านไปยังช่องทางที่แตกต่างจากช่องทางที่ใช้ส่งไฟล์ หรือเข้ารหัสไฟล์ด้วยวิธีการอื่นที่มีความมั่นคงปลอดภัยที่ดีกว่า เช่น การใช้ลายมือชื่ออิเล็กทรอนิกส์ในการเข้ารหัสไฟล์ เป็นต้น

๑๐) มาตรการรักษาความมั่นคงปลอดภัยในการแลกเปลี่ยนและการเชื่อมโยงข้อมูล จำเป็นต้องบันทึกลงในข้อตกลง หรือสัญญาอย่างเป็นลายลักษณ์อักษร ซึ่งมาตรการรักษาความมั่นคงปลอดภัยจะต้องมีความชัดเจนครบถ้วน และบุคคลทั่วไปสามารถเข้าใจได้ โดยควรกำหนดหัวข้อต่อไปนี้

๑๐.๑) ประเภทของข้อมูลที่สามารถแลกเปลี่ยนได้

๑๐.๒) วิธีการแลกเปลี่ยนข้อมูล

๑๐.๓) วิธีการป้องกันข้อมูลที่มีความสำคัญ เช่น การเข้ารหัสลับ (Encryption) ควรต้องมีความยาวไม่น้อยกว่า ๑๒๘ บิต

๑๐.๔) ระบุผู้รับผิดชอบ หรือขอบเขตการรับผิดชอบหากข้อมูลสูญหาย หรือถูกทำลายระหว่างการแลกเปลี่ยน

นอกจากนี้ ก่อนทำการเชื่อมโยงข้อมูล ควรมีกระบวนการวิเคราะห์ความเสี่ยงและกำหนดมาตรการจัดการความเสี่ยงที่อาจเกิดขึ้นจากการใช้งานข้อมูลที่เชื่อมโยงกัน

๑๑) การนำเทคโนโลยีและมาตรฐานทางเทคนิคที่ใช้ในการแลกเปลี่ยนข้อมูล โดยมีแนวทางการปฏิบัติ ดังนี้

๑๑.๑) กำหนดอุปกรณ์หรือซอฟต์แวร์ที่สามารถนำมาใช้ในการแลกเปลี่ยนข้อมูล เช่น USB Drive ที่มีการเข้ารหัสลับ (Encryption), E-Mail แอปพลิเคชันที่มีการเข้ารหัสลับ PGP (Pretty Good Privacy) และการ Login ด้วยระบบเข้ารหัสลับ SSL เพื่อให้การสื่อสารข้อมูลเข้ารหัสลับตลอดเส้นทาง เป็นต้น

๑๑.๒) การแลกเปลี่ยนข้อมูลผ่านอุปกรณ์เครือข่าย ต้องใช้ซอฟต์แวร์หรือกระบวนการเข้ารหัสลับเพื่อดำเนินการป้องกันข้อมูลสารสนเทศให้ได้อย่างปลอดภัย และมีประสิทธิภาพ เช่น RSA, Blowfish, IDEA, DES, ๓DES เป็นต้น

๑๒) การบันทึกรายละเอียดในแต่ละครั้งที่มีการแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน โดยบันทึกเหตุการณ์จะต้องประกอบไปด้วยข้อมูลอย่างน้อย ดังนี้

๑๒.๑) Employee ID หรือ Official Email ของหน่วยงานของผู้รับและผู้ส่ง

๑๒.๒) วันที่และเวลาที่มีการแลกเปลี่ยนข้อมูล

๑๒.๓) ชื่อเครื่อง หมายเลข IP ซอฟต์แวร์หรืออุปกรณ์ที่ใช้ในการแลกเปลี่ยนข้อมูล

๑๒.๔) บันทึกรายละเอียดเกี่ยวกับข้อมูลที่ทำการแลกเปลี่ยน

๑๒.๕) บันทึกผลลัพธ์การแลกเปลี่ยนข้อมูลทั้งที่ประสบความสำเร็จ (Success) และที่ถูกปฏิเสธ (Failure)

๑๓) ต้องมีการติดตามและควบคุมประสิทธิภาพระหว่างการแลกเปลี่ยนข้อมูล เพื่อรักษาไว้ซึ่งความปลอดภัยและคุณภาพข้อมูล โดยมีการกำหนดระดับการให้บริการ (Service Level Agreement-SLA)

หมวดที่ ๕ การจัดเก็บข้อมูลถาวร (Archive)

การจัดเก็บข้อมูลถาวร (Archive) มีแนวปฏิบัติ ดังนี้

๑) เจ้าของข้อมูลเป็นผู้กำหนดผู้มีสิทธิ์ในการทำลายข้อมูล และจะต้องทบทวนสิทธิ์นั้นอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงทางโครงสร้างของหน่วยงานที่สำคัญ เช่น การลาออก เปลี่ยนตำแหน่ง โอนย้าย สิ้นสุดการจ้างการปรับโครงสร้าง หรือเมื่อมีการปรับปรุงระบบสารสนเทศ เป็นต้น

๒) ผู้ดูแลระบบสารสนเทศจะต้องกำหนดสิทธิ์ในการทำลายข้อมูลในระบบให้แก่ผู้ทำลายข้อมูลตามที่เจ้าของข้อมูลกำหนด

๓) ผู้ทำลายข้อมูลต้องทำลายข้อมูลตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

๔) กำหนดให้เจ้าของข้อมูลต้องจัดเก็บคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตาที่ทำลายสำหรับตรวจสอบในภายหลัง

๕) กำหนดให้ผู้ทำลายข้อมูลจัดเก็บบันทึกรายละเอียดการทำลายข้อมูลไว้ในทะเบียนควบคุมและบันทึกการทำลายข้อมูล โดยให้เก็บรักษาไว้เป็นหลักฐานไม่น้อยกว่า ๑ ปี

๖) กำหนดให้ผู้ใช้ข้อมูลส่วนบุคคลทำลายข้อมูลส่วนบุคคลเมื่อเจ้าของข้อมูลส่วนบุคคลร้องขอตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

หมวดที่ ๖ การทำลายข้อมูล (Destroy)

การทำลายข้อมูล (Destroy) มีแนวปฏิบัติ ดังต่อไปนี้

๑) เจ้าของข้อมูลเป็นผู้กำหนดผู้มีสิทธิ์ในการทำลายข้อมูล และจะต้องทบทวนสิทธิ์นั้นอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงทางโครงสร้างของหน่วยงานที่สำคัญ เช่น การลาออก เปลี่ยนตำแหน่ง โอนย้าย สิ้นสุดการจ้างการปรับโครงสร้าง หรือเมื่อมีการปรับปรุงระบบสารสนเทศ เป็นต้น

๒) ผู้ดูแลระบบสารสนเทศจะต้องกำหนดสิทธิ์ในการทำลายข้อมูลในระบบให้แก่ผู้ทำลายข้อมูลตามที่เจ้าของข้อมูลกำหนด

๓) ผู้ทำลายข้อมูลต้องทำลายข้อมูลตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

๔) การทำลายข้อมูลที่มีชั้นความลับบนสื่อบันทึกข้อมูลประเภทต่าง ๆ ที่มีชั้นความลับ ตั้งแต่ระดับลับขึ้นไป มีวิธีการทำลายข้อมูล ดังนี้

๔.๑) Flash Drive/SSD ให้ถอดแยกชิ้นส่วน และทำลายแผงวงจรภายในจนไม่สามารถประกอบใช้งานได้

๔.๒) Hard Disk ประเภทจานหมุน หรือ Tape Backup ต้องทำลายทางกายภาพให้แผ่นหรือสื่อเก็บข้อมูลภายในเป็นรอยขีดข่วนร้ายแรง อาทิเช่น ทุบ เจาะ บดทำลาย หรือใช้เครื่องทำลายแบบ Degaussing

๔.๓) ทั้งนี้ กรณีสื่อข้อมูลบันทึกข้อมูลแบบอิเล็กทรอนิกส์ที่ต้องการนำกลับมาใช้งานใหม่ให้ดำเนินการทำลายข้อมูลที่ไม่สามารถกู้คืนข้อมูลได้ เช่น การเขียนทับข้อมูลเดิมเป็นจำนวนหลายรอบ หรือเขียนข้อมูลทับด้วยวิธีเปลี่ยนโครงสร้างของไฟล์ เช่น De-identification, Masking, Scrambling, Blurring/Noising, Pseudonymization เป็นต้น

๔.๔) กระดาษ ใช้การทำลายด้วยเครื่องทำลายเอกสาร

๔.๕) แผ่น CD/DVD ใช้การหั่นด้วยเครื่องทำลายเอกสาร

๕) กำหนดให้ทำลายข้อมูลสำคัญในสื่อบันทึกข้อมูลก่อนที่จะมีการจำหน่ายอุปกรณ์ดังกล่าว

๖) กำหนดให้เจ้าของข้อมูลต้องจัดเก็บคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตาที่ทำลายสำหรับตรวจสอบในภายหลัง

๗) กำหนดให้ผู้ทำลายข้อมูลต้องจัดเก็บบันทึกรายละเอียดการทำลายข้อมูลไว้ในทะเบียนควบคุมและบันทึกการทำลายข้อมูล โดยให้เก็บรักษาไว้เป็นหลักฐานไม่น้อยกว่า ๑ ปี

๘) กำหนดให้ผู้ใช้ข้อมูลส่วนบุคคลทำลายข้อมูลส่วนบุคคลเมื่อเจ้าของข้อมูลส่วนบุคคล ร้องขอตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

หมวดที่ ๗ การจัดทำบัญชีข้อมูลของหน่วยงาน (Data Catalog)

๑) หัวหน้าหน่วยงานมีหน้าที่กำหนดให้มีผู้รับผิดชอบที่เกี่ยวข้องกับข้อมูลของหน่วยงาน

๒) ผู้รับผิดชอบที่เกี่ยวข้องกับข้อมูล มีหน้าที่กำหนดคำนิยามของชุดข้อมูล (List of Data) ดังนี้

๒.๑) ความสัมพันธ์ของข้อมูล

๒.๒) ชนิดข้อมูล (Reference/Master Data Definition) แบ่งเป็น

๒.๒.๑) ข้อมูลอ้างอิง (Reference Data) หมายถึง ข้อมูลที่มีลักษณะและโครงสร้างที่เป็นความจริงและถูกต้องทำให้ข้อมูลไม่ค่อยเปลี่ยนแปลง ส่งผลให้ข้อมูลอ้างอิงถูกเผยแพร่ไปยังแหล่งต่าง ๆ เพื่ออ้างอิงอยู่เสมอ เช่น ข้อมูลประเภทเหรียญกษาปณ์หมุนเวียน ข้อมูลประเภทการใช้ประโยชน์ที่ราชพัสดุ เป็นต้น

๒.๒.๒) ข้อมูลหลัก (Master Data) หมายถึง ข้อมูลที่ถูกสร้างขึ้นเป็นข้อมูลพื้นฐานที่มีความสำคัญต่อการดำเนินงาน เพื่อใช้งานร่วมกันภายในหน่วยงานเป็นหลักและขับเคลื่อนหน่วยงานให้บรรลุเป้าหมาย นอกจากนี้เป็นข้อมูลที่มีโอกาสเปลี่ยนแปลงได้มากกว่า มีรายละเอียดหรือจำนวนฟิลด์ข้อมูลที่มากกว่าข้อมูลอ้างอิงและใช้เป็นข้อมูลในการดำเนินงานภายในหน่วยงาน เช่น ข้อมูลสิ่งปลูกสร้าง ข้อมูลเหรียญกษาปณ์ หมุนเวียน ข้อมูลประเภททะเบียนที่ราชพัสดุ เป็นต้น

๒.๓) ขอบเขตที่ดำเนินการ

๒.๔) ชุดข้อมูลที่คาดว่าเกี่ยวข้อง

๒.๕) กระบวนงานหลักหรืองานหลักที่ได้รับมอบหมาย และกระบวนงานย่อย

๒.๖) ชุดข้อมูลที่เกี่ยวข้องกับกระบวนงานย่อย แบ่งเป็น ชุดข้อมูลที่มีอยู่แล้ว และชุดข้อมูลที่ต้องการเพิ่มเติม

๒.๗) รูปแบบของการเก็บข้อมูล

๒.๘) ความพร้อมของชุดข้อมูล

๒.๙) การเชื่อมโยงและแลกเปลี่ยนข้อมูลภายในหน่วยงาน

๓) ผู้รับผิดชอบที่เกี่ยวข้องกับข้อมูล มีหน้าที่กำหนดลักษณะหรือเงื่อนไขของข้อมูลให้สัมพันธ์กับคำนิยามจัดระดับชั้นของข้อมูล (Data Classification) อย่างน้อย ดังนี้

๓.๑) ข้อมูลที่มีการจัดระดับชั้นความลับของข้อมูล ในประเภทข้อมูลที่ใช้ภายในหน่วยงานหรือข้อมูลที่ใช้ระหว่างหน่วยงานภายในกรมธนารักษ์ ข้อมูลที่ใช้ระหว่างหน่วยงานภายนอก

๓.๒) ประเมินความเสี่ยงของอุปสรรคในการแลกเปลี่ยนข้อมูล

๓.๓) ข้อมูลเปิดเผยได้ต่อสาธารณะ

๓.๔) ชุดข้อมูลส่วนบุคคล

๓.๕) ชุดข้อมูลที่มีระดับชั้นความลับของข้อมูล

๓.๖) ความถี่ในการนำเข้าหรือจัดทำข้อมูล

๓.๗) ความพร้อมในการปรับปรุงข้อมูล

๓.๘) ผู้ที่มีความเกี่ยวข้องกับข้อมูล เช่น เจ้าของข้อมูล (Data Owner) ผู้ใช้ข้อมูล (Data User) เป็นต้น

๓.๙) หมวดหมู่ของข้อมูล

๔) ผู้รับผิดชอบที่เกี่ยวข้องกับข้อมูล มีหน้าที่กำหนดหัวข้อในการจัดกลุ่มหมวดหมู่ของข้อมูลให้สัมพันธ์กับคำนิยามข้อมูลเมทาดาตา (Metadata) อย่างน้อย ดังนี้

๔.๑) เลขที่เมทาดาตา (Metadata ID)

๔.๒) ชื่อชุดข้อมูล (Dataset Name)

๔.๓) เจ้าของข้อมูล (Data Owner)

๔.๔) คำสำคัญ (Keyword)

๔.๕) คำอธิบายอย่างย่อ (Description)

๔.๖) ผู้สนับสนุนหรือผู้ร่วมดำเนินการ (Data Support)

๔.๗) วันที่เริ่มต้นสร้าง (Created Date)

๔.๘) วันที่ทำการเปลี่ยนแปลงข้อมูลล่าสุด (Last Updated Date)

๔.๙) แหล่งที่มา (Data Source)

๔.๑๐) หน่วยที่ย่อยที่สุดของการจัดเก็บข้อมูล (Data Collect)

๔.๑๑) รูปแบบการเก็บข้อมูล (Data Format)

๔.๑๒) ภาษาที่ใช้ (Data Language)

๔.๑๓) เส้นทางการเข้าถึง (URL)

๔.๑๔) ขอบเขตที่เผยแพร่ข้อมูล (Area of Dissemination)

๔.๑๕) สิทธิ์ในการเข้าถึงข้อมูล หลังจากเผยแพร่ (Right of Access)

๔.๑๖) สิทธิ์ในการใช้ข้อมูล (Right of Usage)

๕) ผู้รับผิดชอบที่เกี่ยวข้องกับข้อมูล มีหน้าที่กำหนดพจนานุกรมข้อมูล (Data Dictionary) ดังนี้

๕.๑) เลขที่เมทาดาตา (Metadata ID)

๕.๒) ชื่อชุดข้อมูล (Dataset Name)

๕.๓) เลขที่ข้อมูล (Data ID)

๕.๔) ชื่อตารางข้อมูล (Table Name)

๕.๕) ชื่อฟิลด์ข้อมูล (Field)

๕.๖) คำอธิบายฟิลด์ (Description)

๕.๗) ระดับชั้นข้อมูล (Classification)

๕.๘) ประเภทข้อมูล (Data Type)

๕.๙) ขนาดข้อมูล (Data Size)

๕.๑๐) คุณลักษณะข้อมูล (Characteristic Type)

๕.๑๑) แหล่งที่มาของค่าที่ระบุในฟิลด์ (Data Source)

๕.๑๒) รูปแบบ (Data Format)

๕.๑๓) เงื่อนไข (Condition)

หมวดที่ ๘ การประเมินผลการกำกับดูแลข้อมูล (Data Governance Assessment)

๑) หน่วยงานที่เป็นเจ้าของข้อมูลต้องมีการประเมินผลการกำกับดูแลข้อมูล อย่างน้อยปีละ ๑ ครั้ง โดยให้ส่งรายงานอย่างเป็นทางการให้กับคณะกรรมการธรรมาภิบาลข้อมูล

๒) การวัดผลการดำเนินการและผลสัมฤทธิ์ (Metric and Key Success Measurement) มีจุดประสงค์เพื่อทราบผลลัพธ์จากความก้าวหน้าในการปฏิบัติงานของหน่วยงาน และเพื่อให้ได้ข้อมูลที่จำเป็นแก่ผู้บริหาร ผู้ปฏิบัติ และผู้รับบริการในการตัดสินใจเพื่อปรับปรุงเปลี่ยนแปลง หรือแก้ไขปัญหาในด้านต่าง ๆ ของหน่วยงานให้สามารถบรรลุวัตถุประสงค์ที่กำหนดไว้

๓) การประเมินความพร้อมของธรรมาภิบาลข้อมูล (MDM Maturity Levels and Model-Driven) เป็นเครื่องมือชี้วัดว่าหน่วยงานบริหารจัดการธรรมาภิบาลข้อมูลระดับใด โดยเกณฑ์ในการประเมินความพร้อมของธรรมาภิบาลข้อมูลที่ดี ควรประกอบด้วยการประเมินดังต่อไปนี้ คือ ประสิทธิผล (Effectiveness) ประสิทธิภาพ (Efficiency) การตอบสนอง (Responsiveness) ภาระรับผิดชอบ (Accountability) ความโปร่งใส (Transparency) การมีส่วนร่วม (Participation) การกระจายอำนาจ (Decentralization) นิติธรรม (Rule of Law) ความเสมอภาค (Equity) และมุ่งเน้นฉันทามติ (Consensus Oriented) คู่มือการจัดระดับการกำกับดูแลองค์การภาครัฐตามหลักธรรมาภิบาลของการบริหารกิจการบ้านเมืองที่ดี (Good Governance Rating)

๔) ต้องมีการปรับปรุงการดำเนินการจัดทำธรรมาภิบาลข้อมูลอย่างสม่ำเสมอ การกำกับดูแลข้อมูล นอกจากจำเป็นต้องมีการดำเนินการที่เกิดประสิทธิภาพแล้ว การวัดระดับของการดำเนินงานเป็นอีกปัจจัยสำคัญ ซึ่งจะทำให้หน่วยงานได้ทราบถึงสิ่งที่ได้ดำเนินการแล้ว และสิ่งใดบ้างที่ควรจะดำเนินการต่อไป เพื่อปรับปรุงการดำเนินงานให้เกิดประสิทธิภาพสูงสุด ระดับความพร้อมของการกำกับดูแลข้อมูล ถูกใช้เป็นเครื่องมือในการวัดระดับการดำเนินงานและการกำกับดูแลข้อมูล ซึ่งประกอบด้วย ๖ ระดับ ดังนี้

๔.๑) ระดับ ๐ : None หมายถึง ไม่มีการกำกับดูแลข้อมูล หรือมีแต่ไม่ได้ดำเนินการอย่างเป็นทางการ เช่น มีการดำเนินงานบางส่วนและไม่มีการประกาศให้ทราบอย่างเป็นทางการ

๔.๒) ระดับ ๑ : Initial หมายถึง ไม่มีการกำหนดมาตรฐานของกระบวนการ หรือกระบวนการถูกกำหนดขึ้นมาเฉพาะกิจ ทำให้แต่ละโครงการมีรูปแบบของกระบวนการที่แตกต่างกัน และอำนาจในการจัดการและกำกับดูแลข้อมูลที่มีอยู่ในเทคโนโลยีสารสนเทศ แต่มีข้อจำกัดต่อกระบวนการทางธุรกิจ การทำงานร่วมกันระหว่างธุรกิจและเทคโนโลยีสารสนเทศไม่สอดคล้องกัน

๔.๓) ระดับ ๒ : Managed หมายถึง เริ่มมีการกำหนดมาตรฐานของกระบวนการเฉพาะแต่ละส่วนงานหรือบริการ และมีการกำหนดบุคคลที่เกี่ยวข้องกับการกำกับติดตาม เช่น บริกรข้อมูล และผู้รับผิดชอบข้อมูล เป็นต้น โดยกระบวนการดังกล่าวต้องนำไปใช้กับโครงการสำคัญ ๆ ภายในส่วนงาน

๔.๔) ระดับ ๓ : Standardized หมายถึง กระบวนการถูกกำหนดเป็นมาตรฐานของหน่วยงาน มีการกำหนดส่วนงานกลางในการกำกับและติดตามข้อมูล ซึ่งมาจากบุคคลด้านธุรกิจและเทคโนโลยีสารสนเทศ มีการบังคับใช้นโยบายข้อมูลครอบคลุมทั้งหน่วยงาน มีการติดตาม วิเคราะห์และรายงานคุณภาพข้อมูล

๔.๕) ระดับ ๔ : Advanced หมายถึง กระบวนการกำกับดูแลและคุณภาพข้อมูลมีการวัดผลและรายงานผลต่อเนื่อง

๔.๖) ระดับ ๕ : Optimized หมายถึง มีการดำเนินการการวิเคราะห์ความคุ้มทุนในการดำเนินการกำกับดูแล วัตถุประสงค์ของการปรับปรุงกระบวนการกำกับข้อมูลถูกกำหนดขึ้น ให้สอดคล้องกับการเปลี่ยนแปลงของวัตถุประสงค์ของหน่วยงาน และวัตถุประสงค์ของการปรับปรุงได้นำไปใช้เป็นเกณฑ์สำหรับการปรับปรุงกระบวนการกำกับและติดตาม

หมวดที่ ๙ การประเมินคุณภาพข้อมูล (Data Quality)

๑) การประเมินคุณภาพข้อมูลมีแนวทางปฏิบัติดังต่อไปนี้

๑.๑) ผู้ประเมินคุณภาพข้อมูลตรวจสอบความรู้ความเข้าใจของตนเองเกี่ยวกับคำจำกัดความ/คำนิยามของตัวชี้วัด และชี้แจงประเด็นที่ยังมีความไม่ชัดเจนหรือคลุมเครือกับบริกรข้อมูลด้านคุณภาพข้อมูลก่อนที่จะดำเนินการประเมินคุณภาพข้อมูล

๑.๒) เจ้าของข้อมูลดำเนินการประเมินคุณภาพข้อมูลตามเกณฑ์การประเมินที่ได้มีการกำหนดไว้ โดยใช้เครื่องมือหรือแพลตฟอร์มที่เหมาะสม เช่น ซอฟต์แวร์ตรวจสอบความถูกต้องของข้อมูล (Data Profiling Tools) หรือการวิเคราะห์ด้วยตารางข้อมูล เพื่อตรวจสอบตามมิติ ความถูกต้อง (Accuracy) ความครบถ้วน (Completeness) ความสอดคล้อง (Consistency) ความเป็นปัจจุบัน (Timeliness) ความพร้อมใช้งาน (Availability)

๑.๓) ผู้ประเมินคุณภาพข้อมูลจัดทำเอกสารรวบรวมการประเมินคุณภาพข้อมูล อาทิ ชุดข้อมูลที่ได้รับการประเมิน กระบวนการในการประเมิน ผลการประเมินแต่ละตัวชี้วัด ข้อจำกัดที่พบ เพื่อเป็นหลักฐานที่อธิบายได้ว่ามีการตรวจสอบความถูกต้องของข้อมูลที่นำมารายงาน

๑.๔) คณะบริกรข้อมูล (Data Steward Team) วิเคราะห์ผลการตรวจสอบด้วยคะแนนตามเกณฑ์ในแต่ละมิติ และระบุข้อบกพร่องที่ควรได้รับการปรับปรุง เช่น ความไม่ถูกต้อง ความไม่สอดคล้องกันของข้อมูล หรือการขาดข้อมูลที่สำคัญ

๑.๕) คณะบริกรข้อมูล (Data Steward Team) ตรวจสอบความถูกต้องของกระบวนการประเมินคุณภาพข้อมูล

๑.๖) เจ้าของข้อมูล (Data Owner) พิจารณาและอนุมัติรายงานผลการประเมินจากคณะบริกรข้อมูล จัดทำแผนงานปรับปรุงข้อมูล โดยพิจารณาผลกระทบและลำดับความสำคัญ

๑.๗) คณะบริกรข้อมูล (Data Steward Team) ตรวจสอบการปรับปรุงข้อมูลตามแผนที่กำหนด เช่น การทำความสะอาดข้อมูล (Data Cleansing) หรือการปรับปรุงระบบจัดเก็บข้อมูล และประเมินคุณภาพข้อมูลใหม่เพื่อยืนยันว่าแก้ไขแล้ว

๑.๘) กำหนดให้มีการทบทวนเกณฑ์การประเมินคุณภาพข้อมูล และกระบวนการในการประเมินคุณภาพข้อมูล อย่างน้อยปีละ ๑ ครั้ง

๒) เครื่องมือการประเมินคุณภาพข้อมูล เพื่อให้หน่วยงานภาครัฐใช้ในการตรวจสอบและควบคุมการบริหารจัดการข้อมูลเพื่อให้ได้ข้อมูลที่มีคุณภาพ น่าเชื่อถือ สามารถนำไปใช้ประกอบการวิเคราะห์และตัดสินใจในเชิงนโยบายและการดำเนินงานได้อย่างถูกต้องเหมาะสม รวมทั้งสามารถนำไปใช้ประโยชน์เพื่อเพิ่มประสิทธิภาพในการทำงาน เพิ่มคุณค่าในการให้บริการภาครัฐ และต่อยอดการพัฒนาของประเทศในมิติต่าง ๆ ได้ ตลอดจนสร้างความเชื่อมั่นให้กับผู้ใช้ข้อมูลภาครัฐ

๒.๑) แบบประเมินคุณภาพข้อมูล (DQA Checklist) เป็นเครื่องมือในรูปแบบของแบบฟอร์มที่มีลักษณะเป็นรายการคำถามที่ต้องกรอกคำตอบ และให้คะแนนตามเกณฑ์ที่กำหนด เพื่อประเมินว่าข้อมูลมีคุณภาพตามมาตรฐานหรือไม่ กระบวนการประเมินเริ่มจากการกำหนดชุดข้อมูลที่ต้องการประเมิน จากนั้นผู้ประเมินจะต้องตอบคำถามตามรายการที่กำหนดไว้ในแบบฟอร์ม หลังจากตอบคำถามทั้งหมดแล้ว เครื่องมือจะทำการคำนวณคะแนนรวม และแสดงผลการประเมินในรูปแบบร้อยละ การประเมินด้วย DQA Checklist ครอบคลุมมิติคุณภาพข้อมูลตามมาตรฐาน มรด. ๕ : ๒๕๖๕ ทั้ง ๕ มิติ ได้แก่ ความถูกต้องและสมบูรณ์ (Accuracy and Completeness) ความสอดคล้องกัน (Consistency) ความเป็นปัจจุบัน (Timeliness) ความตรงตามความต้องการของผู้ใช้งาน (Relevancy) และความพร้อมใช้ (Availability) ทำให้หน่วยงานสามารถประเมินคุณภาพข้อมูลได้อย่างรอบด้านและมีมาตรฐาน

๒.๒) แบบตรวจประเมินการควบคุมและติดตามคุณภาพข้อมูล (Data Quality Monitoring and Control Checklist) เป็นเครื่องมือที่ใช้ในการตรวจสอบคุณภาพข้อมูลในระดับรายละเอียด การใช้งานเริ่มต้นจากการตั้งค่ากฎเกณฑ์ (Rules) ให้เหมาะสมกับลักษณะข้อมูลและความต้องการของหน่วยงาน ซึ่งกฎเกณฑ์เหล่านี้จะถูกกำหนดในรูปแบบของสูตรและเงื่อนไขใน Excel ที่สอดคล้องกับมิติคุณภาพข้อมูลที่ต้องการประเมิน เช่น การกำหนดรูปแบบข้อมูลที่ถูกต้อง ช่วงของค่าที่ยอมรับได้ ความสัมพันธ์ระหว่างข้อมูล หรือเงื่อนไขเฉพาะที่ข้อมูลต้องเป็นไปตาม หลังจากตั้งค่ากฎเกณฑ์เรียบร้อยแล้ว ผู้ใช้นำชุดข้อมูลที่ต้องการตรวจสอบมาใส่ในไฟล์ Excel เมื่อนำเข้าข้อมูลแล้ว เครื่องมือจะทำการประมวลผลโดยอัตโนมัติและระบุจุดบกพร่องของข้อมูลที่ไม่เป็นไปตามกฎเกณฑ์ที่กำหนดด้วยการ highlight เซลล์ที่มีปัญหา ทำให้ผู้ใช้สามารถเห็นข้อมูลที่ต้องแก้ไขได้อย่างชัดเจนและรวดเร็ว ผลการตรวจสอบนี้จะถูกสรุปและคำนวณเป็นค่าร้อยละของข้อมูลที่เป็นไปตามกฎเกณฑ์ในแต่ละข้อ ซึ่งจะส่งต่อไปยังแบบประเมินคุณภาพข้อมูลด้วยตนเอง (DQA Self Assessment) เพื่อวิเคราะห์และประเมินคุณภาพข้อมูลในภาพรวมต่อไป

๒.๓) แบบประเมินคุณภาพข้อมูลด้วยตนเอง (DQA Self Assessment) เป็นเครื่องมือที่ใช้ในการประเมินผลลัพธ์ของคุณภาพข้อมูลโดยเปรียบเทียบกับเป้าหมายที่หน่วยงานกำหนด การใช้งานเครื่องมือนี้เชื่อมโยงโดยตรงกับผลลัพธ์จากแบบตรวจประเมินการควบคุม และติดตามคุณภาพข้อมูล (Data Quality Monitoring and Control Checklist) โดยค่าร้อยละความถูกต้องของข้อมูลที่เป็นไปตามกฎเกณฑ์ที่ตั้งไว้ในแต่ละมิติคุณภาพจะถูกส่งมาที่แบบประเมินนี้โดยอัตโนมัติ ผู้ใช้งานจะต้องกำหนดเกณฑ์เป้าหมายคุณภาพข้อมูล (Data Quality KPI) ในแต่ละมิติคุณภาพ ซึ่งอาจแตกต่างกันไปตามความสำคัญและความต้องการเฉพาะของแต่ละประเภทข้อมูลหรือแต่ละหน่วยงาน เช่น อาจกำหนดเป้าหมายความถูกต้องไว้ที่ร้อยละ ๙๕ ความครบถ้วนที่ร้อยละ ๙๘ หรือความเป็นปัจจุบันที่ร้อยละ ๙๐ เป็นต้น เมื่อกำหนดเป้าหมายเรียบร้อยแล้ว ระบบจะทำการเปรียบเทียบค่าร้อยละที่ได้จากการตรวจสอบจริงกับเกณฑ์เป้าหมายในแต่ละมิติ และแสดงผลการประเมินว่าผ่านเกณฑ์หรือไม่ผ่านเกณฑ์ พร้อมทั้งแสดงผลต่างระหว่างค่าจริงกับค่าเป้าหมาย ทำให้ผู้ใช้งานสามารถเห็นภาพรวมของคุณภาพข้อมูลในทุกมิติ และทราบว่ามิติใดที่ยังต้องปรับปรุงเพื่อให้บรรลุเป้าหมายที่กำหนดไว้ ผลการประเมินนี้จะช่วยให้หน่วยงานสามารถวางแผนปรับปรุงคุณภาพข้อมูลได้อย่างตรงจุดและมีประสิทธิภาพ

หมวดที่ ๑๐ การประเมินความมั่นคงปลอดภัยของข้อมูล (Data Security)

การประเมินความมั่นคงปลอดภัยของข้อมูล ควรประกอบด้วยการประเมิน ดังต่อไปนี้

๑) ด้านการจัดทำและทบทวนนโยบายด้านความมั่นคงปลอดภัยของข้อมูลที่รวมถึงการป้องกันข้อมูลในบริบทของการรักษาความลับ ความถูกต้องของข้อมูล ความพร้อมใช้งานของข้อมูล

๒) ด้านการจัดระดับชั้นข้อมูล (Data Classification) ข้อมูลควรมีการจัดระดับชั้นให้สอดคล้องกับกฎหมาย เงื่อนไข และข้อกำหนดต่าง ๆ

๓) ด้านการกำหนดมาตรการควบคุมและป้องกันการเข้าถึงข้อมูล (Data Protection) โดยต้องมีการคำนึงถึงระดับชั้นความลับของข้อมูล เช่น ข้อมูลที่มีความอ่อนไหวต้องมีการกำหนดมาตรการควบคุมและป้องกันการเข้าถึงข้อมูลแบบพิเศษ เพื่อป้องกันการเข้าถึงเพื่อเปิดเผยข้อมูลที่อ่อนไหวนั้น รวมถึงเพื่อป้องกันการดัดแปลง แก้ไข แต่งเติมข้อมูลโดยไม่ได้รับอนุญาต

๔) ด้านการใช้ข้อมูล โดยข้อมูลต้องถูกใช้งานอย่างเหมาะสม การนำข้อมูลไปใช้ ควรดำเนินการให้สอดคล้องกับสัญญาอนุญาต และไม่ขัดต่อกฎหมาย

๕) ด้านความพร้อมใช้ของข้อมูล ต้องมีการดำเนินการเตรียมความพร้อมไม่ว่าข้อมูลจะอยู่ในรูปแบบใดก็ตาม เช่น ข้อมูลในรูปแบบกระดาษต้องมีสถานที่จัดเก็บดูแล และสามารถเข้าถึงโดยผู้มีสิทธิ์ได้อย่างสม่ำเสมอ ข้อมูลในรูปแบบอิเล็กทรอนิกส์ต้องมีการเตรียมความพร้อมเรื่องระบบงาน การสำรองข้อมูล รวมถึงมีแผนการดำเนินการในกรณีฉุกเฉินใด ๆ ที่อาจมีผลต่อการใช้ข้อมูลด้วย

หมวดที่ ๑๑ การเปิดเผยข้อมูลและการขอใช้ข้อมูล (Data Disclosure)

๑) กำหนดแนวปฏิบัติการเปิดเผยข้อมูลต่อสาธารณะโดยอิงจากกฎหมายกฎเกณฑ์และแนวปฏิบัติที่เกี่ยวข้อง ทั้งนี้ข้อมูลที่เปิดเผยควรเป็นประโยชน์ สามารถนำไปประมวลผล และใช้ต่อยอดในการพัฒนา

๒) คัดเลือกชุดข้อมูลที่ต้องการเผยแพร่ให้ปฏิบัติ ดังนี้

๒.๑) ข้อมูลในการเปิดเผยควรเป็น Open by Default และ Closed by Exception โดย Open by Default จะเป็นลักษณะของข้อมูลที่สามารถเปิดเผยได้ และไม่ละเมิดข้อมูลส่วนบุคคล เช่น ข้อมูลเชิงสถิติที่ไม่สามารถระบุตัวบุคคลได้ ข้อมูลที่สามารถเปิดเผยได้ตามกฎหมาย ข้อมูลที่กฎหมายกำหนดให้ต้องเปิดเผย ข้อมูลที่เกี่ยวข้องกับหน้าที่หรือภารกิจของหน่วยงาน ข้อมูลที่มีศักยภาพในการนำไปใช้

ประโยชน์ต่อการพัฒนาในด้านต่าง ๆ ข้อมูลที่ตอบโจทย์หรือเป็นประโยชน์ต่อกลุ่มผู้ใช้งาน รวมถึงข้อมูลที่ช่วยเสริมสร้างความโปร่งใสและความน่าเชื่อถือของหน่วยงาน ในส่วน Closed by Exception ซึ่งเป็นลักษณะข้อมูลส่วนบุคคลที่ไม่เปิดเผย เช่น ข้อมูลของเชิงรายการของผู้เช่าที่ราชพัสดุ หมายเลขบัตรประจำตัวประชาชน หมายเลขบัตรเครดิต รหัสผ่านที่ใช้เข้าระบบ เป็นต้น ถ้าจำเป็นต้องมีการเปิดเผยให้ดำเนินการปกปิดข้อมูล (Data Masking) หรือการเข้ารหัสข้อมูล (Data Encryption) ตามลักษณะของการนำข้อมูลไปใช้งาน

๒.๒) กรณีเป็นข้อมูลส่วนบุคคล และเข้าถึงเป็นรายบุคคล หน่วยงานที่ขอใช้จะต้องได้รับการยินยอมจากเจ้าของข้อมูลก่อน พร้อมทั้งแจ้งผลการตอบรับการยินยอมไปยังหน่วยงานที่ถือครองข้อมูล ในกรณีเป็นข้อมูลส่วนบุคคลและเข้าถึงบางส่วนหรือทุกรายการ หน่วยงานที่ถือครองข้อมูลต้องมีมาตรการปกปิดไม่ให้หน่วยงานที่ขอใช้ข้อมูลสามารถทราบได้ว่าข้อมูลแต่ละรายการเป็นของบุคคลใด

๓) การพิจารณาชุดข้อมูลที่คัดเลือก ข้อมูลต้องมีรายละเอียดที่อธิบายถึงความเป็นมาของข้อมูล เช่น ชื่อข้อมูล คำอธิบายข้อมูล คำสำคัญ วันที่ทำการเปลี่ยนแปลงข้อมูลล่าสุด ชื่อหน่วยงาน เจ้าของข้อมูล และฟิลด์ข้อมูล ทั้งนี้ ต้องตรวจสอบฟิลด์ข้อมูลว่าครบถ้วนสอดคล้องกับความต้องการของหน่วยงานที่ขอใช้ข้อมูล

๔) การจัดเตรียมข้อมูลให้อยู่ในรูปแบบที่ง่ายต่อการนำไปใช้ให้ปฏิบัติ ดังนี้

๔.๑) ข้อมูลมีความพร้อมในการส่งต่อหรือเปิดเผยได้

๔.๑.๑) ต้องมีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย การเข้าถึง การใช้ การเปลี่ยนแปลง การแก้ไข หรือการเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

๔.๑.๒) กรณีที่ต้องให้ข้อมูลส่วนบุคคลแก่บุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล ต้องดำเนินการเพื่อป้องกันมิให้ผู้นั้นนำไปใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

๔.๑.๓) ต้องมีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น หรือตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ

๔.๑.๔) ปรับปรุงชุดข้อมูลให้เหมาะสมและพร้อมสำหรับการเปิดเผย อาทิ การทำความสะอาดข้อมูล (Data Cleansing) กำจัดข้อมูลซ้ำ (Duplicate) หรือค่าว่าง (Null) สอดคล้องกับมาตรฐานสากล

๔.๑.๕) ดำเนินการจัดทำคำอธิบายชุดข้อมูลให้ครบถ้วนก่อนทำการเปิดเผย

๔.๒) การเชื่อมโยงของข้อมูลมีการจัดเก็บและสามารถเข้าถึงได้ เพื่อตรวจสอบหรือเปิดเผยแก่ผู้ที่เกี่ยวข้อง

๕) นำชุดข้อมูลขึ้นเผยแพร่ให้ปฏิบัติ ดังนี้

๕.๑) ช่องทางการเปิดเผยข้อมูลช่องทางการเปิดเผยข้อมูล สามารถเปิดเผยข้อมูลโดยจัดส่งเชื่อมโยงข้อมูลผ่านศูนย์กลางข้อมูลเปิดภาครัฐ ได้ที่เว็บไซต์ https://data.go.th หรือผ่านเว็บไซต์ของกรมธนารักษ์

๕.๒) ภายหลังจากการเปิดเผยข้อมูลแล้ว จะต้องมีการดำเนินการกำหนดความถี่ในการปรับปรุงชุดข้อมูล โดยความถี่อย่างน้อยปีละ ๑ ครั้ง

๕.๓) ผู้มีส่วนเกี่ยวข้องดำเนินการติดตามผลการดำเนินการโดยเปรียบเทียบกับแผนที่ได้มีการวางไว้

๕.๔) ผู้มีส่วนเกี่ยวข้องประเมินผลการดำเนินการ รวมถึงความต้องการหรือความคาดหวังของผู้ใช้ข้อมูล เพื่อนำมาวางแผน พัฒนา และปรับปรุงอย่างต่อเนื่อง

๕.๕) ต้องดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น

๕.๖) ต้องเก็บประวัติ (Log) การเปิดเผยและเผยแพร่ข้อมูล เพื่อให้สามารถตรวจสอบได้และเป็นไปตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

๕.๗) ต้องมีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย การเข้าถึง การใช้ การเปลี่ยนแปลง การแก้ไข หรือการเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ รวมทั้งแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น

๕.๘) ต้องจัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลไว้ตามหลักเกณฑ์และวิธีการที่กำหนด
