BIG DATA INSTITUTE

ประกาศสถาบันข้อมูลขนาดใหญ่ (องค์การมหาชน)
เรื่อง นโยบายธรรมาภิบาลข้อมูล (Data Governance Policy)

โดยที่เป็นการสมควรทบทวนนโยบายธรรมาภิบาลข้อมูลของสถาบันข้อมูลขนาดใหญ่ (องค์การมหาชน) ให้เป็นไปตามพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ และสอดคล้องกับประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ ลงวันที่ ๑๒ มีนาคม พ.ศ. ๒๕๖๓ และประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง มาตรฐานรัฐบาลดิจิทัล ว่าด้วยกรอบธรรมาภิบาลข้อมูลภาครัฐ ฉบับปรับปรุง : แนวปฏิบัติ ลงวันที่ ๒๔ กรกฎาคม พ.ศ. ๒๕๖๖ เพื่อให้การบริหารจัดการและการบูรณาการข้อมูลของสถาบันข้อมูลขนาดใหญ่ (องค์การมหาชน) มีความมั่นคงปลอดภัยและมีธรรมาภิบาล

อาศัยอำนาจตามความในมาตรา ๒๘ แห่งพระราชกฤษฎีกาจัดตั้งสถาบันข้อมูลขนาดใหญ่ (องค์การมหาชน) พ.ศ. ๒๕๖๖ ประกอบกับมติที่ประชุมคณะทำงานธรรมาภิบาลข้อมูล การคุ้มครองข้อมูลส่วนบุคคล และการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ครั้งที่ ๓/๒๕๖๘ เมื่อวันที่ ๑๓ มีนาคม ๒๕๖๘ จึงให้ยกเลิกประกาศสถาบันข้อมูลขนาดใหญ่ (องค์การมหาชน) เรื่อง นโยบายธรรมาภิบาลข้อมูล ลงวันที่ ๔ กรกฎาคม พ.ศ.๒๕๖๗ และให้ใช้นโยบายธรรมาภิบาลข้อมูล (Data Governance Policy) แนบท้ายประกาศนี้แทน

จึงประกาศให้ทราบและถือปฏิบัติอย่างเคร่งครัดโดยทั่วกัน ทั้งนี้ ให้มีผลนับตั้งแต่บัดนี้เป็นต้นไป จนกว่าจะมีประกาศเปลี่ยนแปลง

ประกาศ ณ วันที่ ๒๔ มีนาคม พ.ศ.๒๕๖๘

(รองศาสตราจารย์ธีรณี อจลากุล)
ผู้อำนวยการสถาบันข้อมูลขนาดใหญ่

นโยบายธรรมาภิบาลข้อมูล
(Data Governance Policy)

สถาบันข้อมูลขนาดใหญ่ (องค์การมหาชน)

เวอร์ชั่น ๒.๐

สารบัญ

นโยบายธรรมาภิบาลข้อมูล (Data Governance Policy)

๑. บทนำ

สถาบันข้อมูลขนาดใหญ่ (องค์การมหาชน) (สขญ.) จัดตั้งขึ้นเพื่อตอบสนองการดำเนินงานตามแนวทางการใช้ประโยชน์จากข้อมูลขนาดใหญ่ (Big Data) และรองรับการให้บริการด้านการพัฒนาเจ้าหน้าที่และการวิเคราะห์ข้อมูลขนาดใหญ่ (Big Data Analytics) ของภาครัฐ ตามยุทธศาสตร์ชาติยุทธศาสตร์ที่ ๖ ด้านการปรับสมดุลและการพัฒนาระบบบริหารจัดการภาครัฐ ที่กำหนดให้มีระบบการบริหารจัดการข้อมูลที่มีความเชื่อมโยงระหว่างหน่วยงาน และแหล่งข้อมูลต่าง ๆ ไปสู่การวิเคราะห์การจัดการข้อมูลขนาดใหญ่ โดยมีวัตถุประสงค์เพื่อส่งเสริมให้เกิดวัฒนธรรมการวิเคราะห์และใช้ประโยชน์ข้อมูลขนาดใหญ่ เพื่อประกอบการตัดสินใจ (Data-Driven Decision) สกัดข้อมูลเชิงลึกในการดำเนินงาน (Insight to Operation) และช่วยเหลือให้หน่วยงานภาครัฐสามารถให้บริการประชาชนได้อย่างเป็นรูปธรรม

การดำเนินงานของ สขญ. ได้มีส่วนเข้าไปเกี่ยวข้องกับข้อมูลจากหลากหลายหน่วยงาน ทั้งข้อมูลที่เปิดเผยได้ และไม่สามารถเปิดเผยได้ เป็นข้อมูลที่มีความอ่อนไหว หรือเป็นข้อมูลที่เป็นความลับของทางราชการ ที่ต้องมีการบริหารจัดการสิทธิการเข้าถึงข้อมูล ดังนั้น จึงจำเป็นต้องมีการวางกรอบนโยบายธรรมาภิบาล (Data Governance) ในการจัดเก็บ จัดการดูแล นำไปใช้ ประมวลผล แลกเปลี่ยนและเผยแพร่ข้อมูล ให้เป็นไปอย่างมีระบบ โดยมีการกำหนดนโยบายและแนวทางในการปฏิบัติที่ชัดเจน สอดคล้องตามมาตรฐานตามความถูกต้องเหมาะสม และตามกฎระเบียบ ข้อบังคับ หรือกฎหมายที่เกี่ยวข้องกับข้อมูลหรือกระบวนการต่างๆ กรอบนโยบายธรรมาภิบาลข้อมูลและแนวปฏิบัตินี้ ฝ่ายต่าง ๆ และผู้ปฏิบัติงานทุกคนของ สขญ. ต้องนำไปใช้ได้อย่างเหมาะสม โดยเข้าใจถึงสิทธิ หน้าที่ และความรับผิดชอบของการมีส่วนได้ส่วนเสียในข้อมูล รวมทั้งเป็นต้นแบบการดูแลข้อมูล และส่งเสริมความเชื่อมั่นของ สขญ.

๒. วัตถุประสงค์

(๑) เพื่อให้การบริหารจัดการข้อมูลของ สขญ. สอดคล้องกับกฎหมาย กรอบธรรมาภิบาลข้อมูลภาครัฐ และระเบียบปฏิบัติที่เกี่ยวข้อง

(๒) เพื่อใช้เป็นกรอบและแนวทางสำหรับผู้บริหาร ผู้ปฏิบัติงาน และผู้ที่เกี่ยวข้อง ในการบริหารจัดการข้อมูลของ สขญ.

๓. นิยาม

(๑) **BDI หรือ สขญ.** หมายถึง สถาบันข้อมูลขนาดใหญ่ (องค์การมหาชน)

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

(๓) **ชุดข้อมูล (Dataset)** หมายถึง การนำข้อมูลจากหลายแหล่งมารวบรวม เพื่อจัดเป็นชุดให้ตรงตามลักษณะโครงสร้างของข้อมูล หรือจากการใช้ประโยชน์ของข้อมูล

(๔) **บัญชีข้อมูล (Data Catalog)** หมายถึง เอกสารแสดงบรรดารายการของชุดข้อมูลที่จำแนกแยกแยะโดยการจัดกลุ่มหรือจัดประเภทข้อมูลที่อยู่ในความครอบครองหรือควบคุมของหน่วยงาน

(๕) **ธรรมาภิบาลข้อมูลภาครัฐ (Data Governance)** หมายถึง การกำหนดสิทธิ หน้าที่และความรับผิดชอบของผู้มีส่วนได้เสียในการบริหารจัดการข้อมูลทุกขั้นตอน เพื่อให้การได้มาและการนำไปใช้

ข้อมูลของหน่วยงานภาครัฐถูกต้อง ครบถ้วน เป็นปัจจุบัน รักษาความเป็นส่วนบุคคลและสามารถเชื่อมโยงกันได้อย่างมีประสิทธิภาพและมั่นคงปลอดภัย

(๖) **หมวดหมู่ของข้อมูล** หมายถึง หมวดหมู่ของข้อมูลตามกรอบธรรมาภิบาลข้อมูลภาครัฐ แบ่งออกได้เป็น ๕ หมวดหมู่ ดังนี้ ข้อมูลส่วนบุคคล ข้อมูลความมั่นคง ข้อมูลความลับทางราชการ ข้อมูลใช้ภายใน และ ข้อมูลสาธารณะ

(๗) **การจัดชั้นความลับของข้อมูล** หมายถึง การกำหนดประเภทและข้อกำหนดของการจัดชั้นความลับของข้อมูล เพื่อป้องกันการเข้าถึงและสามารถนำข้อมูลไปใช้ได้อย่างเหมาะสม ชั้นความลับของข้อมูลมักถูกกำหนดให้สอดคล้องกับผลกระทบต่อหน่วยงานและความมั่นคงของประเทศ อาทิ ชื่อเสียง ความต่อเนื่องของการดำเนินงาน การเงิน และทรัพยากรบุคคล

(๘) **วงจรชีวิตของข้อมูล (Data Life Cycle)** หมายถึง ลำดับขั้นตอนของข้อมูลตั้งแต่เริ่มสร้างข้อมูลไปจนถึงการทำลายข้อมูล ตามกรอบธรรมาภิบาลข้อมูล

(๙) **ระบบคอมพิวเตอร์แม่ข่าย** หมายถึง เครื่องคอมพิวเตอร์ประมวลผลระดับสูง ที่มีเสถียรภาพทั้งในด้านการบริหารจัดการหน่วยจัดเก็บข้อมูล หน่วยความจำ การเชื่อมต่อระบบเครือข่าย และการใช้พลังงานไฟฟ้า โดยทำงานในการให้บริการระบบโปรแกรมประยุกต์ (Application) ระบบข้อมูลสารสนเทศ (Management Information System) และระบบฐานข้อมูล (Database) แก่ผู้ใช้งาน (User) ผ่านเว็บไซต์ (Website) หรือโปรแกรมคอมพิวเตอร์ลูกข่าย (Client Server Software) บนระบบเครือข่ายภายใน (Intranet) และระบบเครือข่ายอินเทอร์เน็ต (Internet)

(๑๐) **การสำรองข้อมูลสารสนเทศ (Backup)** หมายถึง กระบวนการจัดเก็บข้อมูลของเครื่องคอมพิวเตอร์ ทั้งระบบปฏิบัติการ (Operation System) ข้อมูลการตั้งค่า (Configuration Data) และข้อมูลอื่น ๆ (Data) โดยการคัดลอกข้อมูลของเครื่องคอมพิวเตอร์ที่ใช้งานอยู่ในปัจจุบันบนสื่อบันทึกข้อมูลภายนอกเครื่องคอมพิวเตอร์ เพื่อป้องกันข้อมูลเสียหาย (Data Corruption) และข้อมูลสูญหาย (Data Deletion / Data Loss) จากความตั้งใจ หรือความประมาทของผู้ใช้งาน รวมถึง การเกิดภัยพิบัติ (Disaster) ที่มีผลกระทบต่อเครื่องคอมพิวเตอร์ดังกล่าว

(๑๑) **การกู้คืนข้อมูลสารสนเทศ (Recovery)** หมายถึง กระบวนการแก้ไขปัญหาที่เกิดกับข้อมูลของเครื่องคอมพิวเตอร์ จากสื่อบันทึกข้อมูลที่สำรองข้อมูลสารสนเทศ

(๑๒) **เจ้าของข้อมูล (Data Owner)** หมายถึง ผู้ที่ได้รับมอบหมายในการปฏิบัติงานให้รับผิดชอบข้อมูลที่ระบุไว้ ซึ่งรวมถึงผู้บังคับบัญชาของเจ้าของข้อมูลนั้นด้วย โดยทำหน้าที่กำกับดูแลตามธรรมาภิบาลข้อมูลตลอดวงจรชีวิตของข้อมูลนั้นๆ รวมทั้งทำหน้าที่กำหนดสิทธิในการเข้าถึงข้อมูลและจัดชั้นความลับของข้อมูล

(๑๓) **ผู้รับผิดชอบข้อมูล** หมายถึง บุคคลที่ทำหน้าที่รับผิดชอบดูแลข้อมูลโดยตรง สร้างความมั่นใจได้ว่าการบริหารจัดการข้อมูลสอดคล้องกับนโยบาย มาตรฐาน กฎระเบียบ หรือกฎหมาย โดยผู้รับผิดชอบข้อมูลจะต้องทำการทบทวนและอนุมัติการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับข้อมูล เช่น การเปลี่ยนแปลงเมทาดาตาและเกณฑ์การทำความสะอาดข้อมูล (Data Cleansing)

(๑๔) **ผู้ใช้ข้อมูล (Data Users)** หมายถึง คณะกรรมการ ผู้อำนวยการ ผู้ปฏิบัติงาน รวมถึงผู้ที่เกี่ยวข้องอื่นๆ หรือหน่วยงานภายนอก ที่ได้รับอนุญาต (Authorized Users) ให้สามารถเข้ามาใช้ข้อมูลของ สขญ. ตามสิทธิและหน้าที่ความรับผิดชอบ พร้อมทั้งรายงานประเด็นปัญหาที่พบระหว่างการใช้ข้อมูล

(๑๕) **ข้อมูลส่วนบุคคล** หมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงการระบุเฉพาะชื่อ ตำแหน่ง สถานที่ทำงาน หรือ ที่อยู่ทางธุรกิจ และข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

(๑๖) **เจ้าของข้อมูลส่วนบุคคล (Data Subject)** หมายถึง บุคคลธรรมดาที่ข้อมูลส่วนบุคคลเกี่ยวกับบุคคลนั้นระบุถึง

(๑๗) **เจ้าของระบบงาน (System Owner)** หมายถึง ผู้ที่มีหน้าที่รับผิดชอบในการใช้งาน ดูแลและบำรุงรักษา หรือปรับปรุงระบบงานที่ใช้ในหน่วยงาน

(๑๘) **การประมวลผลข้อมูล** หมายถึง การปฏิบัติการหรือส่วนหนึ่งของการปฏิบัติการซึ่งได้กระทำต่อข้อมูลส่วนบุคคลไม่ว่าโดยวิธีการอัตโนมัติหรือไม่ เช่น การเก็บรวบรวม การบันทึก การจัดระเบียบ การจัดโครงสร้าง การจัดเก็บ การดัดแปลง ปรับเปลี่ยน การกู้คืน การให้คำปรึกษา การใช้ การเปิดเผยโดยการส่ง การแพร่กระจาย หรือทำให้มีอยู่ การจัดวางให้ถูกตำแหน่งหรือการรวม การจำกัด การลบ และการทำลาย

(๑๙) **ผู้ควบคุมข้อมูลส่วนบุคคล** หมายถึง บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

(๒๐) **ผู้ประมวลผลข้อมูลส่วนบุคคล** หมายถึง บุคคลหรือนิติบุคคลที่ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล “ตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล” โดยที่ผู้ประมวลผลข้อมูลส่วนบุคคลต้องไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

(๒๑) **ข้อมูลหลักและข้อมูลอ้างอิง (Master and Reference Data)** หมายถึง การบริหารจัดการข้อมูลเพื่อให้ทั้งหน่วยงานสามารถเข้าถึงและใช้ข้อมูลร่วมกันได้ โดยข้อมูลถูกจัดเก็บไว้แหล่งเดียว มีการกำหนดมาตรฐานของข้อมูล เพื่อช่วยลดความซ้ำซ้อนของข้อมูลและทำให้ข้อมูลมีคุณภาพ ซึ่ง Master data เป็นข้อมูลที่สร้างและถูกใช้งานอยู่ภายในหน่วยงาน มีโอกาสเปลี่ยนแปลงได้และมีรายละเอียดหรือจำนวนฟิลด์ข้อมูลที่มาก เช่น ข้อมูลพนักงาน ข้อมูลลูกค้า ข้อมูลผู้ขาย ข้อมูลสินค้าและบริการ ข้อมูลครุภัณฑ์ และข้อมูลสถานที่ ในขณะที่ Reference data มีความเป็นสากลถูกสร้างและใช้งานโดยทั่วไป โดยหลากหลายองค์กร หรือแม้กระทั่งใช้งานไปทั่วโลก เช่น รหัสไปรษณีย์ รหัสประเทศ หน่วยวัดระยะทาง

๔. โครงสร้างธรรมาภิบาลข้อมูล

โครงสร้างธรรมาภิบาลข้อมูลของ สขญ. แบ่งออกเป็น ๒ ส่วน ประกอบด้วย ส่วนที่ ๑ คณะทำงานธรรมาภิบาลข้อมูล การคุ้มครองข้อมูลส่วนบุคคล และการรักษาความมั่นคงปลอดภัยทางไซเบอร์ และส่วนที่ ๒ ผู้มีส่วนได้เสียกับข้อมูล (Data Stakeholders)

๔.๑ <u>คณะทำงานธรรมาภิบาลข้อมูล การคุ้มครองข้อมูลส่วนบุคคล และการรักษาความมั่นคงปลอดภัยทางไซเบอร์</u> ซึ่งต่อไปนี้จะเรียกว่า **<u>คณะทำงานฯ</u>** ประกอบไปด้วย ผู้บริหารระดับสูง และตัวแทนจากฝ่ายต่าง ๆ ของ สขญ.

มีหน้าที่รับผิดชอบธรรมาภิบาลข้อมูลและการบริหารจัดการด้านข้อมูล ของ สขญ. ดังนี้

(๑) กำหนดนโยบาย แนวปฏิบัติ และทิศทางการดำเนินงานด้านธรรมาภิบาลข้อมูล การคุ้มครองข้อมูลส่วนบุคคล และการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของ สขญ. ให้สอดคล้องกับกฎหมายว่าด้วยการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล กฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยทางไซเบอร์ และกฎหมายอื่นที่เกี่ยวข้องกับการบริหารจัดการข้อมูล

(๒) การกำหนดมาตรฐานข้อมูลและการวัดผลการบริหารจัดการข้อมูลของ สขญ. ให้สอดคล้องกับกฎหมายว่าด้วยการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล กฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยทางไซเบอร์ และกฎหมายอื่นที่เกี่ยวข้องกับการบริหารจัดการข้อมูล

(๓) กำกับ ติดตาม ประเมินผลการดำเนินงานด้านธรรมาภิบาลข้อมูล การคุ้มครองข้อมูลส่วนบุคคล และการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของ สขญ. ให้สอดคล้องกับนโยบาย แนวปฏิบัติมาตรฐานข้อมูลและการวัดผลการบริหารจัดการข้อมูลของ สขญ.

(๔) ปฏิบัติงานอื่นที่เกี่ยวข้องตามที่ได้รับมอบหมาย

เพื่อเป็นกรอบธรรมาภิบาลข้อมูลของ สขญ. คณะทำงานฯ เป็นผู้ให้ข้อเสนอแนะ กลั่นกรอง และอนุมัตินโยบายข้อมูล มาตรฐานข้อมูล แนวทางปฏิบัติงาน เกณฑ์การวัดคุณภาพ ที่เกี่ยวข้องกับข้อมูล รวมไปถึงการจัดลำดับความสำคัญและแก้ไขปัญหาที่เกี่ยวข้องกับข้อมูล

ผู้บริหารกลุ่มงานบูรณาการและวิเคราะห์ข้อมูล ทำหน้าที่เป็นผู้บริหารข้อมูลระดับสูง มีหน้าที่บริหารข้อมูลของ สขญ. เพื่อสร้างเทคโนโลยี เครื่องมือ แนวทาง และวิธีการในการทำให้ข้อมูลของ สขญ. มีคุณค่า และเกิดประโยชน์สูงสุด นอกจากนี้ ยังต้องวิเคราะห์และร่วมกับผู้บริหารส่วนอื่น ๆ เพื่อจัดทำยุทธศาสตร์และดำเนินการธรรมาภิบาลข้อมูลให้มีคุณภาพและการควบคุมอื่น ๆ เพื่อรักษาความสมบูรณ์ของข้อมูลของ สขญ. และผู้บริหารข้อมูลระดับสูง จะต้องทำหน้าที่เป็นตัวกลางระหว่างหน่วยงานในการแลกเปลี่ยน เชื่อมโยงข้อมูล รวมไปถึงการจัดการความเสี่ยงที่อาจเกิดจากข้อมูล รวมถึงส่งเสริมนวัตกรรมที่ใช้ประโยชน์จากข้อมูลในการวิเคราะห์ปัญหาเพื่อแก้ไข และลดความเสี่ยงของปัญหาที่อาจเกิดขึ้นในอนาคตได้

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Department Chief Information Officer : DCIO) มีหน้าที่ ส่งเสริมและผลักดันให้มีการปรับรูปแบบการบริการและทำงานของ สขญ. ให้มีความทันสมัย รวดเร็ว โปร่งใส เชื่อมโยงอย่างเป็นเครือข่ายทั้งภายในและภายนอกภาครัฐ พัฒนาและนำส่งนวัตกรรมบริการ บริหารจัดการทรัพยากรเพื่อการใช้ประโยชน์ร่วมกัน กำกับดูแลการพัฒนาเทคโนโลยี รวมทั้งเชื่อมโยงระบบงานและข้อมูลทั้งภายในและระหว่างหน่วยงาน ให้เกิดประโยชน์อย่างสร้างสรรค์ มีความเหมาะสมได้มาตรฐาน มั่นคงปลอดภัย และคำนึงถึงความเป็นส่วนบุคคล

ทีมบริกรข้อมูล (Data Steward Team) ประกอบไปด้วยตัวแทนจากฝ่ายต่าง ๆ รวมไปถึงบุคคลที่ทำหน้าที่เกี่ยวกับความมั่นคงปลอดภัย กฎหมาย และบุคคลที่ให้ความรู้เกี่ยวกับนโยบายข้อมูลและความรู้อื่น ๆ ที่จะสนับสนุนให้เกิดธรรมาภิบาลข้อมูลที่ดีภายใน สขญ. และสนับสนุนข้อมูลในการตัดสินใจต่อคณะทำงานฯ

บริกรข้อมูล (Data Stewards) คือ บุคคลที่ทำหน้าที่รับผิดชอบในการนิยามความต้องการด้านคุณภาพและความมั่นคงปลอดภัยซึ่งอาจจะได้รับมาจากผู้ใช้ข้อมูล (Data Users) หรือผู้มีส่วนได้เสียอื่น ๆ นิยามคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตาโดยการสนับสนุนจากผู้ใช้ข้อมูล สถาปนิกข้อมูล (Data Architects) และนักวิเคราะห์ระบบ (System Analyst) ร่างนโยบายข้อมูล ตรวจสอบการปฏิบัติตามนโยบายข้อมูล ตรวจสอบคุณภาพ ตรวจสอบความมั่นคงปลอดภัยของข้อมูล วิเคราะห์ผลจากการตรวจสอบแล้วรายงานผลลัพธ์ไปยังคณะทำงานฯ และผู้ที่เกี่ยวข้องอื่น ๆ ให้ทราบ

๔.๒ ผู้มีส่วนได้เสียกับข้อมูล (Data Stakeholders)

นอกจากคณะทำงานฯ และทีมบริกรข้อมูล ยังมีผู้มีส่วนได้เสียกับข้อมูล (Data Stakeholders) อื่น ๆ ซึ่งทำหน้าที่ให้การสนับสนุนธรรมาภิบาลข้อมูลต่อคณะทำงานฯ ประกอบไปด้วย ผู้รับผิดชอบข้อมูล (Data Owners) ทีมบริหารจัดการข้อมูล (Data Management Team) ผู้สร้างข้อมูล (Data Creators) และผู้ใช้ข้อมูล (Data Users)

ผู้รับผิดชอบข้อมูล (Data Owners) คือ บุคคลที่ทำหน้าที่รับผิดชอบดูแลข้อมูลโดยตรง สร้างความมั่นใจได้ว่าการบริหารจัดการข้อมูลสอดคล้องกับนโยบาย มาตรฐาน กฎระเบียบ หรือกฎหมาย โดยผู้รับผิดชอบข้อมูลต้องทำการทบทวนและอนุมัติการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับข้อมูล เช่น การเปลี่ยนแปลงเมทาดาตาและเกณฑ์การทำความสะอาดข้อมูล (Data Cleansing) นอกจากนี้ ยังมีหน้าที่

ในการให้สิทธิในการเข้าถึงข้อมูลและจัดชั้นความลับของข้อมูล รวมถึงสนับสนุนธรรมาภิบาลข้อมูลที่ดี เช่น จัดให้มีการสำรวจความต้องการในการใช้ข้อมูล พร้อมประเด็นปัญหาที่พบระหว่างการใช้ข้อมูล ทั้งด้านคุณภาพและความปลอดภัยของข้อมูลไปยังบริกรข้อมูล

ทีมบริหารจัดการข้อมูล (Data Management Team) ประกอบด้วย ผู้ปฏิบัติงานที่เกี่ยวข้องในการบริหารข้อมูล เช่น สถาปนิกข้อมูล (Data Architects) นักจัดการฐานข้อมูล (Database Administrators : DBA) นักวิเคราะห์ข้อมูล (Data Analysts) และนักวิทยาการข้อมูล (Data Scientists) มีหน้าที่หลักในการบริหารจัดการข้อมูล และสนับสนุนการดำเนินงานด้านธรรมาภิบาลข้อมูล เช่น ช่วยเหลือในการนิยามเมทาดาตา ร่างนโยบายข้อมูลและมาตรฐานข้อมูล และกำหนดสิทธิการเข้าถึงข้อมูล

ผู้สร้างข้อมูล (Data Creators) คือ บุคคลที่ทำหน้าที่ บันทึก แก้ไข ปรับปรุง หรือลบข้อมูลให้สอดคล้องกับโครงสร้างที่ถูกกำหนดไว้ นอกจากนี้ ยังมีหน้าที่ในการทำงานร่วมกับบริกรข้อมูล เพื่อตรวจสอบและแก้ไขปัญหาด้านคุณภาพข้อมูลและความมั่นคงปลอดภัย

ผู้ใช้ข้อมูล (Data Users) คือ บุคคลที่ทำหน้าที่นำข้อมูลไปใช้งาน ทั้งในระดับปฏิบัติงานและระดับบริหาร

๕. นโยบายธรรมาภิบาลข้อมูล

๕.๑ ข้อกำหนดทั่วไป

แนวทางการดำเนินงานที่เกี่ยวข้องกับการบริหารจัดการข้อมูลในภาพรวม ให้เป็นไปด้วยความเรียบร้อย ถูกต้อง รวมทั้งสอดคล้องกับกฎหมายและระเบียบต่าง ๆ ที่เกี่ยวข้อง ซึ่งประกอบไปด้วย

(๑) กำหนดบทบาท หน้าที่ และความรับผิดชอบของแต่ละบุคคล ตามโครงสร้างธรรมาภิบาลข้อมูล โดยต้องได้รับการมอบอำนาจและการอนุมัติจากผู้บริหาร พร้อมทั้งกำหนด ฝ่าย หรือ กลุ่มงาน หรือคณะทำงานหรือกลุ่มบุคคลภายใน สขญ. เป็นผู้รับผิดชอบข้อมูล เพื่อทำหน้าที่ในการบริหารจัดการข้อมูลนั้น ๆ

(๒) จัดทำนโยบายการบริหารจัดการข้อมูลเป็นลายลักษณ์อักษร อนุมัติเผยแพร่เพื่อประกาศใช้ และถือปฏิบัติ โดยให้มีผลบังคับใช้กับบุคลากรใน สขญ. ตลอดจนหน่วยงาน/บุคคลภายนอกที่เกี่ยวข้องกับการได้มาและการใช้ข้อมูลของ สขญ. พร้อมทั้งจัดทำแนวปฏิบัติและมาตรฐานที่เกี่ยวกับข้อมูลเพื่อสนับสนุนการปฏิบัติงานให้สอดคล้องตามนโยบายดังกล่าว

(๓) กำหนดมาตรการ วิธีการ และแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของข้อมูลเพื่อป้องกันการละเมิด การเข้าถึง การสูญหาย การทำลาย หรือการเปลี่ยนแปลงข้อมูล โดยปราศจากอำนาจโดยมิชอบหรือโดยมิได้รับอนุญาต (อ้างอิงตามนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy) ของ สขญ. และเป็นไปตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และมาตรฐาน ISO ๒๗๐๐๑)

(๔) กำหนดมาตรการ วิธีการ และแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลที่สอดคล้องกับกฎหมาย ระเบียบ และแนวปฏิบัติของ สขญ. (อ้างอิงตามนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) ของ สขญ. และเป็นไปตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล)

(๕) ตรวจสอบความมีอยู่และรายละเอียดของข้อมูลที่สำคัญ เช่น คำอธิบายข้อมูลหรือเมทาดาตา ชุดข้อมูล การจัดชั้นความลับข้อมูล และรายงานผลให้แก่ผู้รับผิดชอบตามโครงสร้างธรรมาภิบาลข้อมูลภาครัฐและดำเนินการตามกระบวนการธรรมาภิบาลข้อมูลภาครัฐ

(๖) ตรวจสอบ ติดตาม และประเมินผลการปฏิบัติตามนโยบายการบริหารจัดการข้อมูลโดยผู้ตรวจประเมิน พร้อมทั้งกำหนดให้มีการทบทวนนโยบาย รวมถึงมาตรการ วิธีการ และแนวปฏิบัติต่าง ๆ เกี่ยวกับข้อมูล อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญตามความเหมาะสม

(๗) ตรวจสอบ ติดตาม และประเมินผลการดำเนินงานธรรมาภิบาลข้อมูลของ สขญ. อย่างน้อยปีละ ๑ ครั้ง ในเรื่องการประเมินความพร้อมธรรมาภิบาลข้อมูล การประเมินคุณภาพข้อมูล และการประเมินความมั่นคงปลอดภัยของข้อมูลเป็นอย่างน้อย (อ้างอิงตามมาตรฐานและหลักเกณฑ์ที่สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.) กำหนด หรือเป็นไปตามมาตรฐานสากล)

(๘) จัดให้มีทรัพยากรด้านงบประมาณ ทรัพยากรบุคคล และเทคโนโลยีที่เพียงพอต่อการบริหารจัดการข้อมูล พร้อมทั้งสนับสนุนการฝึกอบรมธรรมาภิบาลข้อมูลภาครัฐและการบริหารจัดการข้อมูลให้ครอบคลุมทั้งวงจรชีวิตของข้อมูลแก่บุคลากรใน สขญ. อย่างน้อยปีละ ๑ ครั้ง

๕.๒ การจัดหมวดหมู่และชั้นความลับของข้อมูล

(๑) กำหนดบุคคลหรือกลุ่มบุคคลภายใน สขญ. ทำหน้าที่ในการจัดหมวดหมู่และชั้นความลับ เพื่อป้องกัน จัดการ และกำกับดูแลข้อมูลให้เหมาะสม

(๒) กำหนดหมวดหมู่และประเภทชั้นความลับของข้อมูลที่ใช้กับข้อมูลทุกรูปแบบของ สขญ. ทั้งเอกสารกระดาษและข้อมูลดิจิทัล ด้วยการประเมินผลกระทบของข้อมูล สขญ. เพื่อระบุหมวดหมู่และประเภทชั้นความลับของข้อมูล รวมทั้งกำหนดระดับความปลอดภัยที่เหมาะสมสำหรับการสร้าง การจัดเก็บ การใช้ และการเข้าถึงชุดข้อมูล และนำไปใช้กับบุคลากรรวมถึงตัวแทนบุคคลที่สามที่ได้รับอนุญาตให้เข้าถึงข้อมูลใน สขญ. ด้วย

(๔) ติดป้ายกำกับชุดข้อมูล (Labeling/Tagging Dataset) ตามผลประเมินและระบุหมวดหมู่และประเภทชั้นความลับอย่างเหมาะสม และป้ายกำกับสำรองชั้นความลับข้อมูล (ถ้ามี) เช่น ลับ ลับมาก ลับที่สุด เป็นต้น เพื่อจำแนกความแตกต่างของชุดข้อมูลภายใน สขญ. หรือแนวปฏิบัติตามข้อกำหนดอื่น ๆ

(๕) กำหนดให้มีการกำกับติดตามอย่างต่อเนื่อง และมีการวัดผลการดำเนินงานและความสำเร็จของการจำแนกข้อมูล โดยตรวจสอบความปลอดภัยและรูปแบบการเข้าถึงระบบและข้อมูล

๕.๓ การบริหารจัดการข้อมูลตามวงจรชีวิตของข้อมูล

(๑) กำหนดนโยบาย แนวปฏิบัติ และสภาพแวดล้อมการบริหารจัดการข้อมูลตามวงจรชีวิตของข้อมูล ที่เอื้อต่อการรักษาความมั่นคงปลอดภัย คุ้มครองความเป็นส่วนตัวของข้อมูล และเพื่อให้ได้ข้อมูลที่มีคุณภาพ

(๒) จัดทำแนวปฏิบัติการจัดการชุดข้อมูล รวมถึงการรักษาความปลอดภัยตามหมวดหมู่และประเภทชั้นความลับตามแนวทางที่เหมาะสม และปรับปรุงอย่างต่อเนื่องให้สอดคล้องกับสถานการณ์

(๓) จัดเก็บข้อมูลให้สอดคล้องกับแนวทางหรือมาตรฐานการจัดชั้นความลับของข้อมูลที่กำหนดไว้ โดยข้อมูลต้องมีความถูกต้อง สมบูรณ์ และเป็นปัจจุบัน พร้อมทั้งกำหนดสิทธิและจัดหาระบบเครื่องมือ ที่ใช้ในการเข้าถึงข้อมูลเพื่อรักษาความมั่นคงปลอดภัยและคุณภาพข้อมูล และทำลายข้อมูลตามแนวปฏิบัติและกฎหมายที่เกี่ยวข้อง

(๔) จัดทำแนวปฏิบัติและมาตรฐานการประมวลผลและใช้ข้อมูล เพื่อให้ผู้ใช้สามารถนำข้อมูลไปใช้ได้อย่างถูกต้องตามวัตถุประสงค์ที่ต้องการเพื่อให้เกิดประโยชน์สูงสุด

(๕) ห้ามเปิดเผยข้อมูลที่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง นโยบาย และแนวปฏิบัติ ไม่ว่าข้อมูลจะอยู่ในรูปแบบใดหรือสถานที่ใดก็ตาม และในการเปิดเผยข้อมูลต้องได้รับการอนุญาตจากตัวแทน สขญ. หรือเจ้าของข้อมูลก่อนการเปิดเผยข้อมูล รวมทั้งจัดให้มีช่องทางการเปิดเผยข้อมูลที่เข้าถึงและนำไปใช้ได้

(๖) กำหนดกระบวนการ เทคโนโลยี และมาตรฐานทางเทคนิคที่ใช้ในการแลกเปลี่ยนข้อมูล และจัดทำสัญญาอนุญาตหรือข้อตกลงในการแลกเปลี่ยนข้อมูลและการนำข้อมูลไปใช้

(๗) จัดทำแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยด้านคุณภาพข้อมูล และด้านคุ้มครองความเป็นส่วนตัวของข้อมูล และตรวจสอบให้แน่ใจว่าได้บริหารจัดการข้อมูลอย่างเหมาะสมตามแนวทางหรือแนวปฏิบัติที่กำหนดไว้

(๘) สร้างความรู้ความเข้าใจในการบริหารจัดการข้อมูลตามวงจรชีวิตของข้อมูล ให้แก่ผู้เกี่ยวข้องทั้งภายในและภายนอก สขญ.

๕.๔ คุณภาพข้อมูล

(๑) กำหนดแนวทางการจัดการคุณภาพข้อมูล เพื่อใช้เป็นกรอบแนวทางในการจัดการข้อมูลของ สขญ. ให้มีคุณภาพเป็นตามเกณฑ์หรือคุณสมบัติที่กำหนด เช่น ความถูกต้องสมบูรณ์ ความสอดคล้องกัน (Consistency) ความเป็นปัจจุบัน ตรงตามความต้องการใช้งาน และความพร้อมใช้ เป็นต้น โดยผู้ดูแลข้อมูลมีหน้าที่จัดการและกำกับดูแลข้อมูลให้มีคุณภาพเพื่อสร้างความมั่นใจให้กับผู้ใช้ข้อมูล ในขณะที่ผู้ใช้ข้อมูลมีบทบาทในการให้ข้อเสนอแนะแก่ผู้ดูแลข้อมูลเพื่อการปรับปรุงคุณภาพให้ดียิ่งขึ้น

(๒) จัดทำเกณฑ์คุณภาพข้อมูลที่สามารถวัดผลได้ และทำการประเมินผลตลอดวงจรชีวิตของข้อมูล อย่างน้อยปีละ ๑ ครั้ง

(๓) จัดทำแผนพัฒนาคุณภาพข้อมูลที่สามารถระบุตัวชี้วัดคุณภาพและแผนปฏิบัติการเพื่อจัดการคุณภาพข้อมูลได้อย่างมีประสิทธิภาพ โดยออกแบบการเก็บรวบรวมข้อมูลเพื่อให้ได้ข้อมูลสำหรับประเมินคุณภาพตามเกณฑ์ดังกล่าวให้รวมอยู่ในระบบเทคโนโลยีสารสนเทศและกระบวนการทำงาน (Quality by design) เพื่อลดข้อผิดพลาดและปรับปรุงคุณภาพตั้งแต่จุดการป้อนข้อมูลหรือการสร้างข้อมูลไปจนถึงการประมวลผลข้อมูล

๖. แนวปฏิบัติการบริหารจัดการข้อมูล

แนวปฏิบัติการบริหารจัดการข้อมูลตามวงจรชีวิตข้อมูล แบ่งออกเป็น ๖ หมวด ได้แก่ การสร้างข้อมูล การจัดเก็บข้อมูล การประมวลผลข้อมูลและการใช้ข้อมูล การเชื่อมโยงและการแลกเปลี่ยนข้อมูล การเปิดเผยข้อมูล และการทำลายข้อมูล ดังนี้

หมวด ๑ การสร้างข้อมูล

(๑) เจ้าของข้อมูล (ไม่ว่า เจ้าของข้อมูล จะอยู่ภายใน กลุ่มงาน/ฝ่าย/ส่วนงานเดียวหรือมากกว่าหลายกลุ่มงาน/ฝ่าย/ส่วนงาน ต้องมีการกำหนดชัดเจนถึงอำนาจหน้าที่ และขั้นตอนการทำงานร่วมกัน)

(๑.๑) มีหน้าที่จัดการสิทธิเกี่ยวกับการประมวลผลข้อมูล และจะต้องทบทวนสิทธินั้นอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ เช่น การลาออก เปลี่ยนตำแหน่ง โอนย้าย สิ้นสุดการจ้าง การปรับโครงสร้าง หรือเมื่อมีการปรับปรุงระบบสารสนเทศ เป็นต้น

(๑.๒) กำหนดหมวดหมู่และชั้นความลับของข้อมูล

(๒) ผู้ดูแลระบบสารสนเทศจะต้องกำหนดสิทธิในการสร้างข้อมูลในระบบให้แก่ผู้สร้างข้อมูลตามที่เจ้าของข้อมูลกำหนด

(๓) เจ้าของข้อมูล บริกรข้อมูล คณะทำงานฯ ร่วมจัดทำคำอธิบาย ชุดข้อมูลดิจิทัลหรือเมทาดาตา (Metadata) เมื่อมีการสร้างชุดข้อมูล (Datasets) ตามมาตรฐานขั้นต่ำคำอธิบายชุดข้อมูลดิจิทัลที่สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.) กำหนด และกำหนดชุดข้อมูลเปิดเพื่อสนับสนุนการเผยแพร่ของชุดข้อมูลที่มีคุณค่าสูง (High Value Dataset) ต่อสาธารณะตามกฎหมายว่าด้วยข้อมูลข่าวสารของราชการในรูปแบบข้อมูลดิจิทัล

(๔) ห้ามมิให้ผู้สร้างข้อมูลนำข้อมูลที่มีลักษณะ ดังต่อไปนี้ ซึ่งขัดต่อกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์เข้าสู่ระบบคอมพิวเตอร์

- ข้อมูลที่บิดเบือน หรือปลอมไม่ว่าทั้งหมดหรือบางส่วน
- ข้อมูลอันเป็นเท็จ ที่น่าจะเกิดความเสียหายต่อการรักษาความมั่นคงปลอดภัย ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจ หรือ โครงสร้างพื้นฐาน หรือ ก่อให้เกิดความตื่นตระหนก
- ข้อมูลอันเป็นความผิดเกี่ยวกับความมั่นคง หรือ ความผิดเกี่ยวกับการก่อการร้าย
- ข้อมูลที่มีลักษณะอันลามก และคนทั่วไปอาจเข้าถึงได้
- ข้อมูลที่ปรากฏภาพของผู้อื่น และเป็นภาพที่สร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ ทำให้ผู้อื่นเสียชื่อเสียง ถูกดูหมิ่นถูกเกลียดชัง หรือ ได้รับความอับอาย

(๕) ห้ามมิให้ผู้สร้างข้อมูล ทำการสร้าง/ทำซ้ำต่อข้อมูลที่ขัดต่อกฎหมายว่าด้วยลิขสิทธิ์หรือทรัพย์สินทางปัญญาของผู้อื่น เว้นแต่จะเป็นไปตามอำนาจที่กฎหมายรับรอง

(๖) กำหนดให้ผู้สร้างข้อมูลสร้างข้อมูลที่มาจากแหล่งข้อมูลที่เชื่อถือได้เท่านั้น

(๗) กำหนดให้เจ้าของข้อมูลตรวจสอบความถูกต้องของข้อมูลที่ถูกสร้างขึ้น

หมวด ๒ การจัดเก็บข้อมูล

(๑) กำหนดให้เจ้าของข้อมูลจะต้องกำหนดระยะเวลาในการจัดเก็บข้อมูลที่ชัดเจน

(๒) กำหนดให้คณะทำงานฯ และผู้ดูแลระบบสารสนเทศทำการย้ายข้อมูลที่มีการจัดเก็บเกินระยะเวลาที่กำหนดแล้วเพื่อจัดเก็บเป็นข้อมูลถาวร

(๓) กำหนดให้การจัดเก็บชุดข้อมูลจะต้องมีคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตา หากไม่มีหรือไม่ครบถ้วน คณะทำงานฯ จะต้องแจ้งผู้รับผิดชอบ ได้แก่ เจ้าของข้อมูล บริกรข้อมูล ทราบ โดยให้คณะทำงานฯ ร่วมกันจัดทำและปรับปรุงให้เป็นปัจจุบัน

(๔) ผู้มีส่วนได้ส่วนเสียเกี่ยวข้องกับข้อมูล ทั้งเจ้าของข้อมูล ผู้สร้างข้อมูล ผู้ใช้ข้อมูล และคณะทำงานฯ จะต้องจัดเก็บข้อมูลตามการจัดชั้นความลับของ สขญ. โดยทำการเข้ารหัสข้อมูล เพื่อป้องกันการเข้าถึงหรือแก้ไขข้อมูลโดยไม่ได้รับอนุญาต ทั้งนี้ การเข้ารหัสข้อมูลให้ปฏิบัติตามวิธีการเข้ารหัสข้อมูลแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ สขญ.

(๕) กำหนดให้มีวิธีปฏิบัติการกู้คืนข้อมูลที่จัดเก็บถาวร สำหรับข้อมูลที่มีความสำคัญมากต่อการดำเนินงานของ สขญ. เพื่อสอบทานความถูกต้อง ครบถ้วน ความพร้อมใช้งาน คุณภาพข้อมูล

(๖) ในการจัดเก็บข้อมูลส่วนบุคคลให้เก็บรวบรวมได้เท่าที่จำเป็น ภายใต้อำนาจหน้าที่และวัตถุประสงค์อันชอบด้วยกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล และไม่เก็บรวบรวมข้อมูลส่วนบุคคล ดังต่อไปนี้ เว้นแต่ได้รับการยินยอมจากเจ้าของข้อมูลส่วนบุคคล หรือกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล หรือกฎหมายอื่นบัญญัติให้กระทำได้

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

- ข้อมูลชีวภาพ

- ข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลในทำนองเดียวกันตามที่ สขญ. กำหนด

(๗) กำหนดให้มีการยกเลิกการจัดเก็บข้อมูลส่วนบุคคลกรณีเจ้าของข้อมูลส่วนบุคคลถอนความยินยอม ตามที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลกำหนด

(๘) ในกรณีที่มีการประชุมหรือธุรกรรมออนไลน์ กำหนดให้มีการจัดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่า ๙๐ วัน นับแต่วันที่ข้อมูลเข้าสู่ระบบคอมพิวเตอร์ โดยจัดเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการนับแต่เริ่มใช้บริการให้สอดคล้องตามกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์และในการจัดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ให้สอดคล้องตามกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ ผู้ให้บริการจะต้องใช้วิธีการที่มั่นคงปลอดภัยอย่างน้อย ดังนี้

- เก็บลงในสื่อที่รักษาความครบถ้วนถูกต้องแท้จริง (Integrity) และระบุตัวตน (Identification) ที่เข้าถึงสื่อได้

- มีการรักษาความลับของข้อมูล และกำหนดชั้นความลับในการเข้าถึงและจัดเก็บข้อมูล เพื่อรักษาความน่าเชื่อถือของข้อมูล และไม่อนุญาตให้ผู้ดูแลระบบแก้ไขข้อมูลที่จัดเก็บไว้ได้

- การจัดเก็บข้อมูลระบุรายละเอียดผู้ใช้บริการเป็นรายบุคคลได้ (Identification and Authentication) เช่น Proxy Server NAT และอื่น ๆ

(๙) กำหนดให้มีมาตรการรักษาความปลอดภัยในการจัดเก็บข้อมูล รวมทั้งกรณีที่มีการเคลื่อนย้ายอุปกรณ์ที่จัดเก็บข้อมูล เพื่อป้องกันมิให้มีการเข้าถึงโดยมิได้รับอนุญาต หรือลักลอบนำข้อมูลไปใช้ที่ก่อให้เกิดความเสียหายต่อ สขญ.

(๑๐) กำหนดมาตรการรักษาความปลอดภัยของข้อมูลที่จัดเก็บถาวร เพื่อป้องกันข้อมูลไม่ให้มีการลบ ปรับปรุง แก้ไขได้ รวมทั้งป้องกันมิให้ข้อมูลที่จัดเก็บถาวรรั่วไหลไปยังบุคคลที่ไม่ได้รับอนุญาต

(๑๑) กำหนดให้มีมาตรการรักษาความปลอดภัยของการถ่ายโอนข้อมูลกับหน่วยงานภายนอกที่ผ่านช่องทางการสื่อสารทุกชนิด โดยต้องสอดคล้องตามนโยบายความมั่นคงปลอดภัยสารสนเทศ

(๑๒) กำหนดให้มีการทบทวนเกี่ยวกับช่วงระยะเวลาการจัดเก็บข้อมูล มาตรการ และวิธีปฏิบัติที่เกี่ยวข้องกับการจัดเก็บข้อมูลถาวร อย่างน้อยปีละ ๑ ครั้ง

หมวด ๓ การประมวลผลข้อมูลและการใช้ข้อมูล

(๑) เจ้าของข้อมูลจะต้องกำหนดผู้มีสิทธิเข้าถึงเพื่อประมวลผลและใช้ข้อมูลตามชั้นความลับ ดังนี้

- ข้อมูลเปิดเผยได้ ไม่กำหนดสิทธิการเข้าถึงเพื่อประมวลผลและใช้งานข้อมูล

- ข้อมูลใช้ภายใน กำหนดให้บุคลากรของ สขญ. เท่านั้นที่มีสิทธิเข้าถึงเพื่อประมวลผลและใช้งานข้อมูลได้

- ข้อมูลที่มีชั้นความลับ กำหนดให้ผู้ใช้งานที่ได้รับสิทธิเข้าถึงและใช้ข้อมูลตามอำนาจหน้าที่เท่านั้น

(๒) ผู้ดูแลระบบสารสนเทศจะต้องกำหนดสิทธิในการเข้าถึงข้อมูลในระบบเพื่อประมวลผลและใช้ข้อมูลของผู้ใช้งานตามที่เจ้าของข้อมูลกำหนด

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

(๔) ผู้ที่มีสิทธิเข้าใช้งานข้อมูลที่มีชั้นความลับตามที่กำหนดโดยเจ้าของข้อมูลจะต้องใช้ข้อมูลอย่างระมัดระวัง โดยคำนึงถึงความปลอดภัยและต้องไม่ใช้งานข้อมูลที่มีชั้นความลับในพื้นที่สาธารณะ

(๕) ผู้ใช้ข้อมูลจะประมวลผลข้อมูลหรือใช้ข้อมูลส่วนบุคคลเท่าที่จำเป็นภายใต้อำนาจหน้าที่และวัตถุประสงค์อันชอบด้วยกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล หรือตามคำสั่งที่ได้รับจาก สขญ. เท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคล

(๖) กรณีที่เจ้าของข้อมูลส่วนบุคคลถอนความยินยอม หน่วยงานต้องยกเลิกการประมวลผลข้อมูลหรือการใช้ข้อมูลส่วนบุคคลตามที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลกำหนด

(๗) ผู้ใช้ข้อมูลจะต้องไม่ใช้ข้อมูลในเครือข่ายของหน่วยงานเพื่อประโยชน์ในเชิงธุรกิจเป็นการส่วนตัว หรือเพื่อเข้าสู่เว็บไซต์ที่ไม่เหมาะสม หรือใช้ข้อมูลอันก่อให้เกิดความเสียหายต่อ สขญ.

หมวด ๔ การเปิดเผยข้อมูล

(๑) เจ้าของข้อมูลจะต้องเปิดเผยข้อมูลในความรับผิดชอบต่อสาธารณะตามกฎหมายว่าด้วยข้อมูลข่าวสารของราชการและมาตรฐานและหลักเกณฑ์การเปิดเผยข้อมูลเปิดภาครัฐในรูปแบบข้อมูลดิจิทัลต่อสาธารณะ

(๒) เจ้าของข้อมูลทำการเปิดเผยข้อมูลในความรับผิดชอบในรูปแบบข้อมูลเปิดของ สขญ. โดยดำเนินการดังนี้

- กำหนดลักษณะของข้อมูลที่เผยแพร่กำหนดให้อยู่ในรูปแบบที่เครื่องสามารถประมวลผลได้
- กำหนดให้มีคำอธิบายข้อมูลหรือเมทาดาตาสำหรับข้อมูลที่ต้องเปิดเผย
- ข้อมูลที่เผยแพร่จะต้องมีการบันทึกเวลา (Timestamps) ที่ช่วยให้ผู้ใช้งานสามารถระบุได้ว่าข้อมูลนั้นเป็นปัจจุบัน
- ข้อมูลที่เผยแพร่ต้องมาจากแหล่งที่เก็บข้อมูลโดยตรง ด้วยระดับความละเอียดสูงโดยไม่มีการปรับแต่งหรือเป็นข้อมูลรูปแบบสรุป (Summary data)
- ชุดข้อมูลและรายการชุดข้อมูลที่เผยแพร่จะต้องมีการจัดรูปแบบที่กำหนดเป็นมาตรฐาน และกำหนดภายใต้หมวดหมู่เดียวกัน เพื่อให้ผู้ใช้ข้อมูลสามารถค้นหาและเข้าถึงข้อมูลได้ง่าย

(๓) กำหนดให้เงื่อนไขและข้อกำหนดของข้อมูลที่นำมาเปิดเผยภายในเครือข่ายของ สขญ. ข้อมูลที่เผยแพร่ต้องไม่ขัดต่อกฎหมายว่าด้วยทรัพย์สินทางปัญญา เว้นแต่การเปิดเผยข้อมูลจะเป็นไปตามอำนาจที่กฎหมายรับรอง

(๔) จัดทำบัญชีข้อมูลของ สขญ. และลงทะเบียนบัญชีข้อมูลภาครัฐ โดยบริหารจัดการข้อมูลสำคัญ จัดทำบัญชีข้อมูล และทำการลงทะเบียนบัญชีข้อมูล และชุดข้อมูลสำคัญ เข้าสู่ระบบบัญชีข้อมูลภาครัฐ (Government Data Catalog หรือ GD Catalog) เพื่อการเปิดเผยข้อมูลภาครัฐที่เป็นระบบ และสามารถสืบค้นชุดข้อมูล คำอธิบายชุดข้อมูล รวมไปถึงแหล่งต้นทางของชุดข้อมูลภาครัฐที่สำคัญ สนับสนุนการใช้ประโยชน์ข้อมูลภาครัฐร่วมกัน

(๕) ในการเปิดเผยข้อมูลส่วนบุคคลต้องปฏิบัติตามข้อกำหนดของกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล หรือตามคำสั่งที่ได้รับจาก สขญ. เท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติในกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

(๖) ห้ามเปิดเผยข้อมูลความมั่นคงและข้อมูลความลับทางราชการที่อยู่ในความครอบครองของ สขญ. รวมทั้งห้ามเปิดเผยข้อมูลที่เป็นการกระทำความผิดตามกฎหมาย นโยบาย และแนวปฏิบัติอันทำให้เกิดความเสียหายต่อ สขญ.

(๗) เจ้าของข้อมูลต้องคัดเลือกข้อมูลที่จะเปิดเผยในรูปแบบข้อมูลเปิดจากลำดับชั้นความสำคัญของชุดข้อมูลที่มีคุณค่าสูง (High Value Dataset)

(๘) เจ้าของข้อมูลต้องกำหนดรอบระยะเวลาในการตรวจสอบและปรับปรุงข้อมูลที่เปิดเผยเพื่อให้ข้อมูลถูกต้อง และเป็นปัจจุบัน

การจัดทำบัญชีข้อมูล (Data Catalog)

(๑) เจ้าของข้อมูลหรือผู้ครอบครองข้อมูลมีหน้าที่กำหนดให้มีผู้รับผิดชอบที่เกี่ยวข้องกับข้อมูลของ สขญ.

(๒) ผู้รับผิดชอบที่เกี่ยวข้องกับข้อมูล มีหน้าที่กำหนดคำนิยามของชุดข้อมูล (List of Data) โดยอย่างน้อยต้องมีในเรื่อง ดังต่อไปนี้

(๒.๑) ความสัมพันธ์ของข้อมูล ได้แก่ หน่วยงานใดเป็นเจ้าของข้อมูล หน่วยงานใดเป็นผู้ใช้ข้อมูล

(๒.๒) รูปแบบการจัดเก็บไฟล์ข้อมูล เช่น ไฟล์เอกสาร หรือแฟ้มกระดาษ

(๒.๓) ความพร้อมของชุดข้อมูล เช่น ชั้นข้อมูล ความครบถ้วนถูกต้อง สมบูรณ์พร้อมใช้ ความถี่ในการนำเข้าหรือจัดทำข้อมูล

(๒.๔) ความพร้อมในการเชื่อมโยงและแลกเปลี่ยนข้อมูล เช่น เปิดให้ใช้งานสาธารณะหรือใช้งานเฉพาะภายในหน่วยงาน ชุดข้อมูลอยู่ในรูปแบบมาตรฐานพร้อมเชื่อมโยงหรือแลกเปลี่ยนหรือไม่

(๓) ผู้รับผิดชอบที่เกี่ยวข้องกับข้อมูล มีหน้าที่กำหนดพจนานุกรมข้อมูล (Data Dictionary) ตามมาตรฐานเมทาดาตา ของการจัดทำบัญชีข้อมูลภาครัฐ

หมวด ๕ การทำลายข้อมูล

(๑) เจ้าของข้อมูลเป็นผู้กำหนดผู้มีสิทธิในการทำลายข้อมูล และจะต้องทบทวนสิทธินั้นอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ เช่น การลาออก เปลี่ยนตำแหน่ง โอนย้าย สิ้นสุดการจ้าง การปรับโครงสร้าง หรือเมื่อมีการปรับปรุงระบบสารสนเทศ เป็นต้น

(๒) ผู้ดูแลระบบสารสนเทศจะต้องกำหนดสิทธิในการทำลายข้อมูลในระบบให้แก่ผู้ทำลายข้อมูลตามที่เจ้าของข้อมูลกำหนด

(๓) ผู้ทำลายข้อมูลต้องทำลายข้อมูลตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ สขญ.

(๔) เจ้าของข้อมูลต้องจัดเก็บคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตาที่ทำลายสำหรับตรวจสอบในภายหลัง

(๕) ผู้ทำลายข้อมูลต้องจัดเก็บบันทึกรายละเอียดการทำลายข้อมูลไว้ในทะเบียนควบคุม และบันทึกการทำลายข้อมูล โดยให้เก็บรักษาไว้เป็นหลักฐานไม่น้อยกว่า ๑ ปี

(๖) เมื่อเจ้าของข้อมูลส่วนบุคคลร้องขอ ผู้ใช้ข้อมูลส่วนบุคคลจะทำลายข้อมูลส่วนบุคคลตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

หมวด ๖ การเชื่อมโยงและการแลกเปลี่ยนข้อมูล

(๑) ผู้จัดการโครงการต้องกำหนดวิธีปฏิบัติและมาตรฐานทางด้านเทคนิคที่จำเป็นต้องใช้เกี่ยวกับการเชื่อมโยงและแลกเปลี่ยนข้อมูลของโครงการในความรับผิดชอบ ดังนี้

- การเชื่อมโยงและแลกเปลี่ยนข้อมูลภายในหน่วยงาน กำหนดให้ใช้รูปแบบที่เป็นมาตรฐานเปิด (Open Format) ทั้งในส่วนมาตรฐานข้อมูล เช่น XML และ JSON เป็นต้น มาตรฐานโปรโตคอลสื่อสาร เช่น SOAP REST หรืออื่น ๆ ที่ได้รับการยอมรับจากมาตรฐานสากล

- การเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน ให้ดำเนินการตามมาตรฐานกลางของหน่วยงานหลักที่เป็นผู้รับผิดชอบ

(๒) ผู้จัดการโครงการต้องดำเนินการตรวจสอบคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตาที่จะทำการเชื่อมโยงและแลกเปลี่ยนให้ครบถ้วน ดังนี้

- ตรวจสอบเมทาดาตาของชุดข้อมูลดิจิทัลที่จัดเก็บให้มีฟิลด์ข้อมูลครบถ้วนสอดคล้องกับความต้องการของหน่วยงานที่ขอใช้ หากไม่ครบถ้วนต้องจัดทำเพิ่มเติมตามความต้องการของหน่วยงานที่ขอใช้

- ตรวจสอบชั้นความลับของข้อมูลว่าอยู่ในชั้นความลับที่สามารถเปิดเผยได้หรือไม่ กล่าวคือ ต้องไม่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ ความมั่นคงของประเทศ ความลับทางราชการ และความเป็นส่วนตัว พร้อมทั้งตรวจสอบสิทธิของหน่วยงานที่สามารถนำข้อมูลไปใช้ได้ตามบทบาทและภารกิจตามกฎหมายของหน่วยงานนั้น ๆ

- หากไม่ครบถ้วน หรือไม่เป็นปัจจุบัน ให้แจ้งเจ้าของข้อมูลเพื่อดำเนินการจัดทำ/ปรับปรุงให้เป็นปัจจุบัน

(๓) ในกรณีที่มีหน่วยงานอื่นต้องการใช้ข้อมูลส่วนบุคคล ซึ่งในการครอบครองของ สขญ. เพื่อทำการศึกษาหรือวิจัย ซึ่งเป็นข้อยกเว้นตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล สขญ. อาจอนุญาตให้หน่วยงานนั้นเชื่อมโยงข้อมูลได้ โดยจะต้องดำเนินการจัดทำข้อมูลนั้นให้เป็นข้อมูลนิรนาม (Anonymization) ก่อน

(๔) กำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัยเกี่ยวกับการเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัลเพื่อป้องกันมิให้มีการรับส่งข้อมูลที่ไม่สมบูรณ์ หรือส่งข้อมูลไปผิดที่หรือมีการรั่วไหลของข้อมูล หรือข้อมูลถูกแก้ไขเปลี่ยนแปลง ถูกทำซ้ำใหม่ ถูกส่งซ้ำโดยมิได้รับอนุญาต

(๕) ห้ามมิให้เชื่อมโยงและแลกเปลี่ยนเพื่อส่งต่อข้อมูลคอมพิวเตอร์ที่เป็นการกระทำความผิดตามกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์

(๖) ผู้ดูระบบแม่ข่ายต้องจัดเก็บบันทึกหลักฐานของการเชื่อมโยงและการแลกเปลี่ยนข้อมูลดิจิทัล เพื่อใช้ตรวจสอบสิ่งผิดปกติต่าง ๆ ที่เกิดขึ้นในการเชื่อมโยงและแลกเปลี่ยนข้อมูล

๗. เอกสารอ้างอิง

(๑) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

(๒) พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

(๓) พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒

(๔) ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ

(๕) ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง มาตรฐานและหลักเกณฑ์การเปิดเผยข้อมูลเปิดภาครัฐในรูปแบบข้อมูลดิจิทัลต่อสาธารณะ (มรด.-๑๒๐๐๑ : ๒๕๖๓)

(๖) ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง มาตรฐานและหลักเกณฑ์การเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัล ว่าด้วยเรื่อง กรอบแนวทางการพัฒนามาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ (มรด. ๒-๑ : ๒๕๖๕)

(๗) ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง มาตรฐานรัฐบาลดิจิทัลว่าด้วยข้อเสนอแนะสำหรับการจัดทำนโยบายและแนวปฏิบัติการบริหารจัดการข้อมูล (มรด. ๔-๑ : ๒๕๖๕ และ มรด. ๔-๒ : ๒๕๖๕)

(๘) ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง มาตรฐานรัฐบาลดิจิทัลว่าด้วยกรอบธรรมาภิบาลข้อมูลภาครัฐ ฉบับปรับปรุง: แนวปฏิบัติ (มรด. ๖ : ๒๕๖๖)

(๙) ประกาศสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ที่ ๓/๒๕๖๔ เรื่อง มาตรฐานของสำนักงานพัฒนารัฐบาลดิจิทัล ว่าด้วยแนวทางการจัดทำบัญชีข้อมูลภาครัฐ (มสพร. ๑-๒๕๖๔)

(๑๐) ประกาศสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ที่ ๔/๒๕๖๔ เรื่อง นโยบายความมั่นคงปลอดภัยสารสนเทศของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

(๑๑) ประกาศสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ที่ ม ๑/๒๕๖๕ เรื่อง มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ว่าด้วยหลักเกณฑ์การจัดระดับชั้นและแบ่งปันข้อมูลภาครัฐ (มสพร. ๘-๒๕๖๕)

(๑๒) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

(๑๓) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐

(๑๔) พระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. ๒๕๔๐

(๑๕) ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔

(๑๖) ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๕๐

(๑๗) ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓