แนวปฏิบัติธรรมาภิบาลข้อมูล
(Data governance guidelines)

กองทุนสนับสนุนการสร้างเสริมสุขภาพ (สสส.)

รายละเอียดเอกสาร

ชื่อเอกสาร	แนวปฏิบัติธรรมาภิบาลข้อมูล (Data governance guidelines)
เวอร์ชัน เอกสาร	1.0
ระดับชั้นเอกสาร	เอกสารใช้ภายใน
วันที่เผยแพร่ครั้งแรก	29 พฤศจิกายน 2565
วันที่ครบกำหนดปรับปรุงเอกสาร	

การเผยแพร่

สำนัก/ฝ่าย	ตำแหน่ง
ทุกสำนัก/ฝ่ายของ สสส.	ทุกตำแหน่งใน สสส.

ที่จัดเก็บ

ที่จัดเก็บ	ผู้รับผิดชอบ
ระบบจัดเก็บเอกสารของสำนักงาน	ฝ่ายเทคโนโลยีสารสนเทศ

ประวัติการปรับปรุงเอกสาร

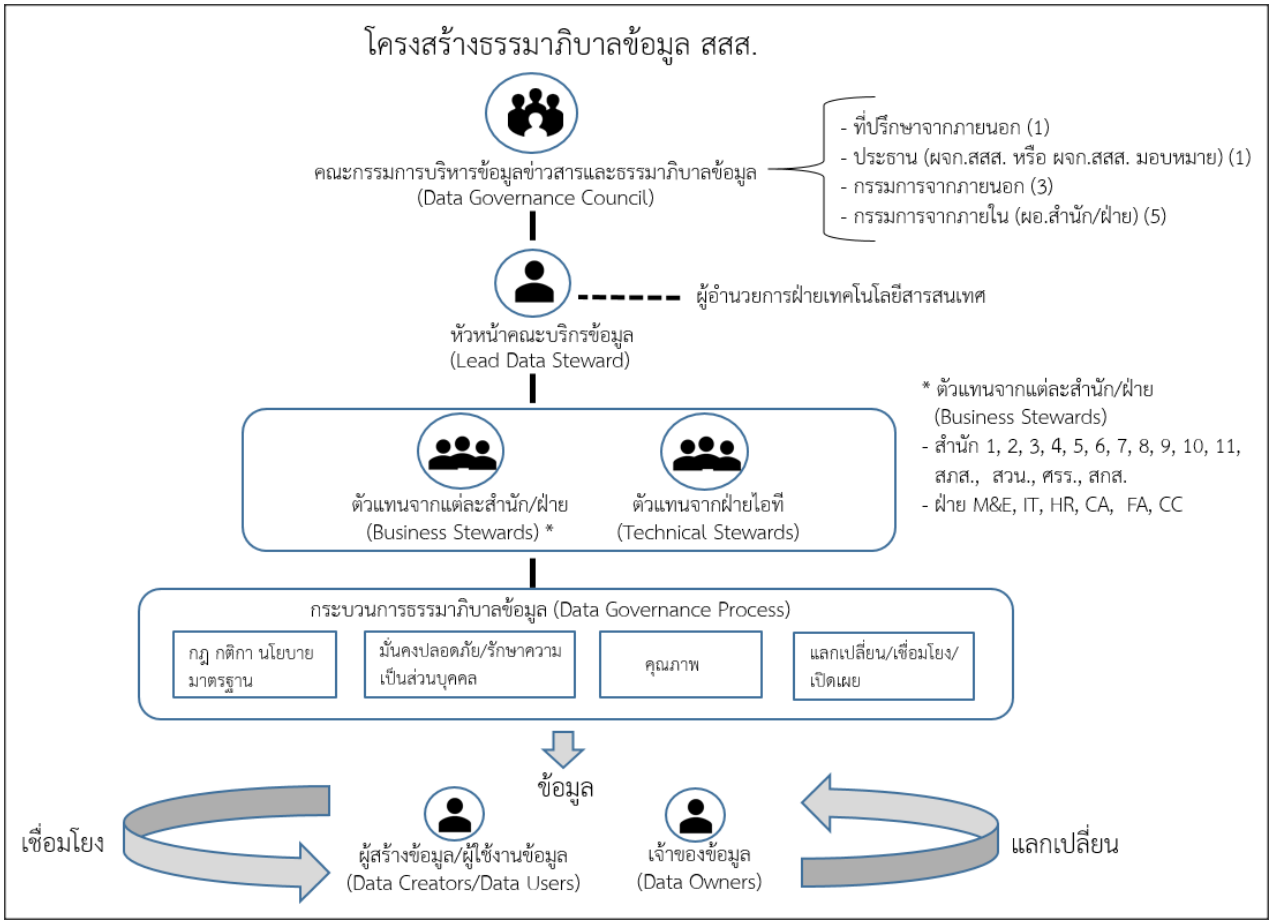
เวอร์ชัน	วันที่ปรับปรุง	ชื่อผู้จัดทำ	ชื่อผู้ตรวจทาน	รายละเอียดการเปลี่ยนแปลง
1.0	29 พ.ย. 65	ฝ่ายเทคโนโลยีสารสนเทศ	นายรวิศม์ วงษ์สมาน	เวอร์ชันใช้งาน

แนวปฏิบัติธรรมาภิบาลข้อมูล
ของสำนักงานกองทุนสนับสนุนการสร้างเสริมสุขภาพ

สำนักงานกองทุนสนับสนุนการสร้างเสริมสุขภาพ (สสส.) ได้จัดทำแนวปฏิบัติธรรมาภิบาลข้อมูล เพื่ออธิบายการดำเนินงานของ สสส. เกี่ยวกับธรรมาภิบาลข้อมูลและการบริหารจัดการข้อมูล รวมถึงแนวปฏิบัติต่าง ๆ นำไปสู่การบริหารจัดการข้อมูลที่มีประสิทธิภาพ มีคุณภาพ มีความปลอดภัย มีการเชื่อมโยง และสามารถดำเนินการได้อย่างต่อเนื่อง และยั่งยืน

1. โครงสร้างธรรมาภิบาลข้อมูล

โครงสร้างธรรมาภิบาลข้อมูล เป็นการแสดงลำดับขั้นระหว่างกลุ่มบุคคลที่เกี่ยวข้องกับธรรมาภิบาลข้อมูลของ สสส. และแสดงถึงสิทธิ์ในการสั่งการตามลำดับขั้น แบ่งเป็น 3 ส่วน ประกอบด้วย 1) คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council) ซึ่ง สสส. ได้กำหนดชื่อเป็น คณะกรรมการบริหารข้อมูลข่าวสารและธรรมาภิบาลข้อมูล 2) ทีมบริกรข้อมูล (Data Steward Team) และ 3) ผู้มีส่วนได้เสียกับข้อมูล (Data Stakeholders)



2. ระบบบริหารและกระบวนการจัดการข้อมูล (Data Life Cycle)

ระบบบริหารและกระบวนการจัดการข้อมูล หรือวงจรชีวิตของข้อมูล หมายถึงลำดับขั้นตอนของข้อมูลตั้งแต่เริ่มสร้างข้อมูลไปจนถึงการทำลายข้อมูล ประกอบด้วย กระบวนการสร้างข้อมูล (Create) กระบวนการจัดเก็บข้อมูล (Store) กระบวนการใช้ข้อมูล (Use) กระบวนการเผยแพร่ข้อมูล (Publish) กระบวนการจัดเก็บข้อมูลถาวร (Archive) และกระบวนการทำลายข้อมูล (Destroy)

2.1 การสร้างข้อมูล

กระบวนการสร้างข้อมูล เป็นการสร้างข้อมูลขึ้นมาใหม่ โดยวิธีการบันทึกเข้าไปด้วยบุคคลหรือบันทึกอัตโนมัติด้วยอุปกรณ์อิเล็กทรอนิกส์ รวมถึงการซื้อข้อมูล หรือการรับข้อมูลมาจากหน่วยงานอื่น เพื่อนำมาจัดเก็บในภายหลัง

ตารางที่ 1 การดำเนินการและผู้มีส่วนร่วม ในกระบวนการสร้างข้อมูล

กิจกรรม	เจ้าของข้อมูล	บริกรข้อมูล	ผู้ดูแลระบบสารสนเทศ
กำหนดผู้มีสิทธิ์ในการสร้างข้อมูล	x		
กำหนดชั้นความลับข้อมูลของข้อมูลที่ถูกสร้างขึ้น	x		
กำหนดสิทธิ์ในการสร้างข้อมูลให้แก่ผู้สร้างข้อมูล			x
จัดทำคำอธิบายชุดข้อมูลดิจิทัล	x	x	
ประเมินคุณค่าของชุดข้อมูลดิจิทัล	x	x	
ตรวจสอบความถูกต้องของข้อมูล	x		

การดำเนินการ

1. เจ้าของข้อมูลเป็นผู้กำหนดผู้มีสิทธิ์ในการสร้างข้อมูล และจะต้องทบทวนสิทธิ์นั้นอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ ได้แก่ การลาออก เปลี่ยนตำแหน่ง โอนย้าย สิ้นสุดการจ้าง การปรับโครงสร้าง หรือเมื่อมีการปรับปรุงระบบสารสนเทศ เป็นต้น
2. เจ้าของข้อมูลเป็นผู้กำหนดชั้นความลับของข้อมูลที่ถูกสร้างขึ้นตามวิธีปฏิบัติการจำแนกชั้นความลับของข้อมูล
3. เจ้าของข้อมูลกำหนดให้มีวิธีปฏิบัติการจำแนกชั้นความลับของข้อมูลสำหรับข้อมูลที่ถูกสร้างขึ้น
4. ผู้ดูแลระบบสารสนเทศจะต้องกำหนดสิทธิ์ในการสร้างข้อมูลให้แก่ผู้สร้างข้อมูลตามที่เจ้าของข้อมูลกำหนด
5. เจ้าของข้อมูลร่วมกับบริกรข้อมูล ร่วมจัดทำคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตา (Metadata) เมื่อมีการสร้างชุดข้อมูล (Datasets) ตามมาตรฐานคำอธิบายชุดข้อมูลดิจิทัลที่ สสส. กำหนด และสอดคล้องกับมาตรฐานที่ภาครัฐได้กำหนดไว้
6. เจ้าของข้อมูลร่วมกับบริกรข้อมูล ทำการประเมินคุณค่าของชุดข้อมูลดิจิทัลตามแบบฟอร์มประเมินคุณค่าชุดข้อมูลที่ สพร. หรือ สสส. กำหนด และเผยแพร่เป็นข้อมูลเปิดของหน่วยงานต่อสาธารณะตามกฎหมายว่าด้วยข้อมูลข่าวสารของราชการในรูปแบบข้อมูลดิจิทัล

7. ห้ามมิให้ผู้สร้างข้อมูลนำข้อมูลที่มีลักษณะดังต่อไปนี้ เข้าสู่ระบบคอมพิวเตอร์ที่ขัดต่อกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์
    - ข้อมูลที่บิดเบือน หรือปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลอันเป็นเท็จ น่าจะเกิดความเสียหายแก่ประชาชน
    - ข้อมูลอันเป็นเท็จที่น่าจะเกิดความเสียหายต่อการรักษาความมั่นคงปลอดภัย ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจ หรือโครงสร้างพื้นฐาน หรือก่อให้เกิดความตื่นตระหนก
    - ข้อมูลอันเป็นความผิดเกี่ยวกับความมั่นคง หรือความผิดเกี่ยวกับการก่อการร้าย
    - ข้อมูลที่มีลักษณะอันลามก และประชาชนทั่วไปอาจเข้าถึงได้
    - ข้อมูลที่ปรากฏภาพของผู้อื่น และเป็นภาพที่สร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทำให้ผู้อื่นเสียชื่อเสียง ถูกดูหมิ่นถูกเกลียดชัง หรือได้รับความอับอาย
8. ห้ามมิให้ผู้สร้างข้อมูล ทำการสร้าง ทำซ้ำหรือดัดแปลง ต่อข้อมูลที่ขัดต่อกฎหมายว่าด้วยลิขสิทธิ์หรือทรัพย์สินทางปัญญาของผู้อื่นเว้นแต่จะเป็นไปตามอำนาจที่กฎหมายรับรอง
9. กำหนดให้ผู้สร้างข้อมูลสร้างข้อมูลที่มาจากแหล่งข้อมูลที่เชื่อถือได้เท่านั้น
10. กำหนดให้เจ้าของข้อมูลตรวจสอบความถูกต้องของข้อมูลที่ถูกสร้างขึ้น
11. กำหนดให้มีวิธีปฏิบัติเกี่ยวกับสร้างข้อมูลให้มีความปลอดภัย และเป็นประโยชน์ต่อผู้ใช้ข้อมูล

2.2 การจัดเก็บข้อมูล

กระบวนการจัดเก็บข้อมูล เป็นการจัดเก็บข้อมูลที่เกิดจากกระบวนการสร้าง หรือข้อมูลที่ได้จากการแลกเปลี่ยนกับหน่วยงานอื่น เพื่อให้มีระเบียบ ง่ายต่อการใช้งาน ไม่สูญหาย หรือถูกทำลาย และให้ผู้ใช้งานสามารถประมวลผลข้อมูลต่าง ๆ ตามความต้องการได้อย่างรวดเร็ว ไม่ว่าจะจัดเก็บลงแฟ้มข้อมูล (File) หรือระบบการจัดการฐานข้อมูล (Database Management System – DBMS)

ตารางที่ 2 การดำเนินการและผู้มีส่วนร่วม ในกระบวนการจัดเก็บข้อมูล

กิจกรรม	เจ้าของข้อมูล	บริกรข้อมูล	ผู้ดูแลระบบสารสนเทศ
กำหนดระยะเวลาในการจัดเก็บข้อมูล	x		
ตรวจสอบความครบถ้วนของชุดข้อมูลหรือเมทาดาตา ของการจัดเก็บชุดข้อมูล	x	x	
ทำการย้ายข้อมูลที่มีการจัดเก็บเกินระยะเวลาที่กำหนดเพื่อจัดเก็บเป็นข้อมูลถาวร		x	x
จัดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์			x

การดำเนินการ

1. เจ้าของข้อมูลจะต้องกำหนดระยะเวลาในการจัดเก็บข้อมูลที่ชัดเจน
2. กำหนดให้การจัดเก็บชุดข้อมูลจะต้องมีคำอธิบายชุดข้อมูลหรือเมทาดาตา หากไม่มีหรือไม่ครบถ้วน ทีมบริหารจัดการข้อมูลจะต้องแจ้งผู้รับผิดชอบ ได้แก่ เจ้าของข้อมูลและบริกรข้อมูลร่วมกันจัดทำและปรับปรุงให้เป็นปัจจุบัน
3. บริกรข้อมูลและผู้ดูแลระบบสารสนเทศ ทำการย้ายข้อมูลที่มีการจัดเก็บเกินระยะเวลาที่กำหนดแล้ว เพื่อจัดเก็บเป็นข้อมูลถาวร
4. การจัดเก็บข้อมูลที่มีชั้นความลับให้ทำการเข้ารหัสข้อมูล เพื่อป้องกันการเข้าถึงหรือแก้ไขข้อมูลโดยไม่ได้รับอนุญาต
5. กำหนดให้มีการจัดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่า 90 วัน นับแต่วันที่ข้อมูลเข้าสู่ระบบคอมพิวเตอร์ เพื่อให้สามารถระบุตัวผู้ใช้บริการนับแต่เริ่มใช้บริการ ให้สอดคล้องตามกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ ซึ่งประกอบด้วยข้อมูลอินเทอร์เน็ตที่เกิดจากการเข้าถึงระบบเครือข่าย และข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการจดหมายอิเล็กทรอนิกส์ (e-mail servers)
6. กำหนดให้การจัดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ให้สอดคล้องตามกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ ผู้ให้บริการจะต้องใช้วิธีการที่มั่นคงปลอดภัยอย่างน้อย ดังนี้
    - เก็บในสื่อ (Media) ที่สามารถรักษาความครบถ้วน ถูกต้องแท้จริง (Integrity) และระบุตัวตน (Identification) ที่เข้าถึงสื่อดังกล่าวได้
    - มีระบบการเก็บรักษาความลับของข้อมูลที่จัดเก็บ และกำหนดชั้นความลับในการเข้าถึงข้อมูลดังกล่าว เพื่อรักษาความน่าเชื่อถือของข้อมูล และไม่อนุญาตให้ผู้ดูแลระบบสามารถแก้ไขข้อมูลที่เก็บรักษาไว้
    - การจัดเก็บข้อมูลต้องสามารถระบุรายละเอียดผู้ใช้งานเป็นรายบุคคลได้ (Identification and Authentication)
7. กรณีข้อมูลที่จัดเก็บในรูปแบบเอกสาร ให้มีการจัดเก็บดังนี้
    - เก็บในสถานที่เหมาะสม มีมาตรการป้องกันการเข้าถึงข้อมูล เช่น สามารถปิดล็อคได้เมื่อไม่ใช้งาน
    - เก็บแยกออกจากอุปกรณ์ประมวลผลต่าง ๆ ได้แก่ เครื่องถ่ายเอกสาร เครื่องพิมพ์ เป็นต้น เพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิ์ในการเข้าถึงข้อมูลได้
8. กำหนดให้มีการจัดเก็บข้อมูลส่วนบุคคล โดยให้เก็บรวบรวมได้เท่าที่จำเป็น ภายใต้อำนาจหน้าที่และวัตถุประสงค์อันชอบด้วยกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล
9. กำหนดให้มีมาตรการรักษาความปลอดภัยในการจัดเก็บข้อมูล รวมทั้งกรณีที่มีการเคลื่อนย้ายอุปกรณ์ที่จัดเก็บข้อมูล เพื่อป้องกันมิให้มีการเข้าถึงโดยมิได้รับอนุญาต หรือลักลอบนำข้อมูลไปใช้ที่ก่อให้เกิดความเสียหายต่อหน่วยงาน
10. กำหนดให้มีมาตรการรักษาความปลอดภัยของการถ่ายโอนข้อมูลกับหน่วยงานภายนอกที่ผ่านช่องทางการสื่อสารทุกชนิด โดยต้องสอดคล้องตามนโยบายความมั่นคงปลอดภัยสารสนเทศ

11. ห้ามมิให้จัดเก็บข้อมูลส่วนตัวหรือข้อมูลที่ไม่เกี่ยวข้องกับการดำเนินงานของสำนักงาน สำหรับการจัดเก็บข้อมูลถาวรบนเครื่องแม่ข่ายที่สำนักงานจัดสรรไว้

2.3 การใช้ข้อมูล

กระบวนการใช้ข้อมูล (Use) เป็นการนำข้อมูลที่จัดเก็บมาประมวลผล เช่น การถ่ายโอนข้อมูล การเปลี่ยนรูปแบบการจัดเก็บข้อมูล การวิเคราะห์ข้อมูล การจัดทำรายงาน รวมถึงการสำรอง (Backup) ข้อมูล เพื่อเป็นการหลีกเลี่ยงความเสียหายที่จะเกิดขึ้นหากข้อมูลเกิดการเสียหายหรือสูญหาย ซึ่งสามารถนำข้อมูลที่สำรองไว้ในสื่อบันทึกข้อมูลกลับมาใช้งานได้ทันที โดยการกู้คืน (Restore)

ตารางที่ 3 การดำเนินการและผู้มีส่วนร่วม ในกระบวนการใช้ข้อมูล

กิจกรรม	เจ้าของข้อมูล	ผู้ดูแลระบบสารสนเทศ
กำหนดสิทธิ์ประมวลผลและเข้าใช้งานข้อมูลตามชั้นความลับ	x	
กำหนดสิทธิ์ในการประมวลผลและเข้าใช้งานข้อมูลให้แก่ผู้ใช้ข้อมูล		x
ทบทวนสิทธิ์การเข้าถึงและการใช้ข้อมูลของผู้ใช้งานอย่างน้อยปีละ 1 ครั้ง	x	

การดำเนินการ

1. เจ้าของข้อมูลจะต้องกำหนดผู้มีสิทธิ์เข้าถึงเพื่อประมวลผลและใช้ข้อมูลตามชั้นความลับ ดังนี้
    - ข้อมูลที่มีชั้นความลับ กำหนดให้ผู้ใช้งานที่ได้รับสิทธิ์ตามตำแหน่ง/บทบาท เท่านั้น
    - ข้อมูลใช้ภายใน กำหนดให้ผู้บริหาร เจ้าหน้าที่ ลูกจ้าง และเจ้าหน้าที่ของรัฐมาช่วยปฏิบัติงาน รวมถึงพนักงานจ้างเหมาบริการเท่านั้น ที่มีสิทธิ์เข้าถึงเพื่อประมวลผลและใช้งานข้อมูลได้ ทั้งนี้ต้องปกป้องข้อมูลจากการเข้าถึงโดยบุคคลภายนอก
    - ข้อมูลเปิดเผยได้ ไม่กำหนดสิทธิ์การเข้าถึงเพื่อประมวลผลและใช้งานข้อมูล
2. ผู้ดูแลระบบสารสนเทศจะต้องกำหนดสิทธิ์ในการเข้าถึงเพื่อประมวลผล และใช้ข้อมูลผู้ใช้งานตามที่เจ้าของข้อมูลกำหนด
3. เจ้าของข้อมูลจะต้องทบทวนสิทธิ์การเข้าถึงเพื่อประมวลผลและใช้ข้อมูลของผู้ใช้งานอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ ได้แก่ การลาออก เปลี่ยนตำแหน่ง โอนย้าย สิ้นสุดการจ้าง การปรับโครงสร้าง หรือเมื่อมีการปรับปรุงระบบสารสนเทศ
4. ผู้ที่มีสิทธิ์เข้าใช้งานข้อมูลที่มีชั้นความลับตามที่กำหนดโดยเจ้าของข้อมูลจะต้องใช้ข้อมูลอย่างระมัดระวัง โดยคำนึงถึงความปลอดภัยและต้องไม่ใช้งานข้อมูลที่มีชั้นความลับในพื้นที่สาธารณะ
5. ผู้ใช้ข้อมูลจะต้องไม่ใช้ข้อมูลในเครือข่ายของหน่วยงาน เพื่อประโยชน์ในเชิงธุรกิจเป็นการส่วนตัวหรือเพื่อเข้าสู่เว็บไซต์ที่ไม่เหมาะสม หรือใช้ข้อมูลอันก่อนให้เกิดความเสียหายต่อ สสส.

2.4 การเชื่อมโยงและการแลกเปลี่ยนข้อมูล

เพื่อกำหนดแนวปฏิบัติและมาตรฐานด้านเทคนิคในการเชื่อมโยงและการแลกเปลี่ยนข้อมูลดิจิทัลทั้งภายใน สสส. และระหว่างหน่วยงานอย่างมีประสิทธิภาพ และก่อให้เกิดประโยชน์ต่อภาครัฐ ภาคเอกชน และประชาชน โดยเป็นการเชื่อมโยงและแลกเปลี่ยนข้อมูล ให้มีความมั่นคงปลอดภัย น่าเชื่อถือ และข้อมูลมีคุณภาพ สามารถนำไปใช้ประโยชน์ได้อย่างมีประสิทธิภาพ

ตารางที่ 4 การดำเนินการและผู้มีส่วนร่วม ในกระบวนการเชื่อมโยงและการแลกเปลี่ยนข้อมูล

กิจกรรม	เจ้าของข้อมูล	บริกรข้อมูล	ผู้ดูแลระบบสารสนเทศ
กำหนดแนวทาง/กระบวนการ ในการเชื่อมโยงและแลกเปลี่ยนข้อมูล	x	x	
ตรวจสอบคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตา และตรวจสอบชั้นความลับของข้อมูล	x	x	
กำหนดเทคโนโลยีและมาตรฐานทางเทคนิคที่ใช้ในการแลกเปลี่ยนข้อมูล			x
กำหนดมาตรการรักษาความมั่นคงปลอดภัยเกี่ยวกับการเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัล		x	x
จัดเก็บบันทึกหลักฐานของการเชื่อมโยงและการแลกเปลี่ยนข้อมูลดิจิทัลที่เกิดขึ้นในแต่ละครั้งที่มีการแลกเปลี่ยนข้อมูล (Log File)			x
ทำสัญญาอนุญาตหรือข้อตกลงในการแลกเปลี่ยนข้อมูลและการนำไปใช้		x	x

การดำเนินการ

1. กำหนดให้เจ้าของข้อมูลหรือบริกรข้อมูล จัดทำแนวทาง/กระบวนการ ในการเชื่อมโยงและแลกเปลี่ยนข้อมูล โดยมีองค์ประกอบ ดังต่อไปนี้เป็นอย่างน้อย
    - วัตถุประสงค์ในการนำข้อมูลไปใช้งาน
    - ขอบเขตการนำข้อมูลไปใช้งาน
    - ช่วงเวลาและความถี่ในการเข้าถึงข้อมูลและการนำข้อมูลไปใช้
    - ชุดข้อมูล รายการข้อมูล ฟิลด์ข้อมูลที่สามารถเข้าถึง
    - กำหนดวิธีการ แนวทาง และรายละเอียดของการเชื่อมโยงและการแลกเปลี่ยนข้อมูลดิจิทัล
    - ในกรณีขอข้อมูลส่วนบุคคลเป็นรายคน ต้องจัดทำหนังสือแสดงความยินยอม เพื่อรับการยินยอมจากบุคคลนั้น ๆ หรือได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลดังกล่าวไว้ก่อนหน้านั้นแล้วตามวัตถุประสงค์ในแต่ละกิจกรรมไว้อย่างชัดเจน ยกเว้นหน่วยงานที่ขอใช้ข้อมูลมีอำนาจตามกฎหมายโดยชอบธรรม

2. กำหนดให้เจ้าของข้อมูล หรือบริกรข้อมูลตามที่ได้รับมอบหมายดำเนินการตรวจสอบคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตาของข้อมูลที่จะทำการเชื่อมโยงและแลกเปลี่ยนให้ครบถ้วน ดังนี้
    - ตรวจสอบเมทาดาตาของชุดข้อมูลดิจิทัลที่จัดเก็บให้มีฟิลด์ข้อมูลครบถ้วนสอดคล้องกับความต้องการของหน่วยงานที่ขอใช้ หากไม่ครบถ้วนต้องจัดทำเพิ่มเติมตามความต้องการของหน่วยงานที่ขอใช้
    - ตรวจสอบชั้นความลับของข้อมูลว่าอยู่ในชั้นความลับที่สามารถเปิดเผยได้หรือไม่ โดยต้องไม่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ ความมั่นคงของประเทศ ความลับทางราชการ และความเป็นส่วนบุคคล พร้อมทั้งตรวจสอบสิทธิ์ของหน่วยงานที่สามารถนำข้อมูลไปใช้ได้ตามบทบาทและภารกิจตามกฎหมายของหน่วยงานนั้น ๆ หากไม่ครบถ้วนหรือไม่เป็นปัจจุบัน ให้แจ้งเจ้าของข้อมูลและบริกรข้อมูลทำการจัดทำหรือปรับปรุงให้เป็นปัจจุบัน
3. กำหนดเทคโนโลยีและมาตรฐานทางเทคนิคที่ใช้ในการแลกเปลี่ยนข้อมูล
4. บริกรข้อมูลร่วมกับร่วมกับผู้ดูแลระบบสารสนเทศ กำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัยเกี่ยวกับการเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัล เพื่อป้องกันมิให้มีการรับส่งข้อมูลที่ไม่สมบูรณ์ หรือส่งข้อมูลไปผิดที่หรือมีการรั่วไหลของข้อมูล หรือข้อมูลถูกแก้ไขเปลี่ยนแปลง ถูกทำซ้ำใหม่ ถูกส่งซ้ำโดยมิได้รับอนุญาต
5. กำหนดให้ผู้ดูระบบสารสนเทศต้องจัดเก็บบันทึกหลักฐานของการเชื่อมโยง และการแลกเปลี่ยนข้อมูลดิจิทัล (Log File) เพื่อให้สามารถตรวจสอบย้อนกลับได้
6. บริกรข้อมูลร่วมกับร่วมกับผู้ดูแลระบบสารสนเทศ ทำสัญญาอนุญาตหรือข้อตกลงในการแลกเปลี่ยนข้อมูลและการนำไปใช้
7. ห้ามมิให้เชื่อมโยงและแลกเปลี่ยนเพื่อส่งต่อข้อมูล ที่เป็นการกระทำความผิดตามกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์

2.5 การเผยแพร่และการเปิดเผยข้อมูล

เพื่อกำหนดแนวปฏิบัติและมาตรฐานการเผยแพร่และการเปิดเผยข้อมูลต่อสาธารณะโดยอิงจากกฎหมาย กฎเกณฑ์และแนวปฏิบัติที่เกี่ยวข้อง ทั้งนี้ ข้อมูลที่เปิดเผยควรเป็นประโยชน์ สามารถนำไปประมวลผลและใช้ต่อยอดในการพัฒนาในรูปแบบต่าง ๆ ได้ โดยการเปิดเผยข้อมูลเป็นการนำข้อมูลที่อยู่ในครอบครองของ สสส. เผยแพร่ตามช่องทางต่าง ๆ อย่างเหมาะสม ทั้งการเปิดเผยตามนโยบายรัฐ และการแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน

ตารางที่ 5 การดำเนินการและผู้มีส่วนร่วม ในกระบวนการเปิดเผยข้อมูล

กิจกรรม	เจ้าของข้อมูล	บริกรข้อมูล
กำหนดช่องทางการเปิดเผยข้อมูลที่เข้าถึงและนำไปใช้ง่าย	x	x
คัดเลือกข้อมูลที่จะเปิดเผยในรูปแบบข้อมูลเปิด (Open Data)	x	x
ตรวจสอบคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตาของชุดข้อมูลที่จะทำการเปิดเผยให้มีความครบถ้วนเป็นปัจจุบัน	x	x
กำหนดรอบระยะเวลาในการตรวจสอบและปรับปรุงข้อมูลที่เปิดเผย	x	x

การดำเนินการ

1. เจ้าของข้อมูลร่วมกับบริกรข้อมูล กำหนดช่องทางการเปิดเผยข้อมูลที่เข้าถึงและนำไปใช้ง่าย
2. กำหนดให้เจ้าของข้อมูลร่วมกับบริกรข้อมูล คัดเลือกข้อมูลที่จะเปิดเผยในรูปแบบข้อมูลเปิดจากลำดับชั้นความสำคัญของชุดข้อมูล
3. เจ้าของข้อมูลร่วมกับบริกรข้อมูล คัดเลือกข้อมูลที่จะเปิดเผยในรูปแบบข้อมูลเปิด (Open Data) ในรูปแบบข้อมูลเปิดของ สสส. โดยดำเนินการ ดังนี้
    - กำหนดลักษณะของข้อมูลที่เผยแพร่กำหนดให้อยู่ในรูปแบบที่เครื่องสามารถประมวลผลได้
    - กำหนดให้มีคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตา และพจนานุกรมข้อมูล (Data Dictionary) สำหรับข้อมูลที่ต้องเปิดเผย และสอดคล้องกับมาตรฐานตามที่หน่วยงานของรัฐได้กำหนดไว้
    - ชุดข้อมูลและรายการชุดข้อมูลที่เผยแพร่ จะต้องมีการจัดรูปแบบที่กำหนดเป็นมาตรฐาน และกำหนดภายใต้หมวดหมู่เดียวกัน เพื่อให้ผู้ใช้ข้อมูลสามารค้นหาและเข้าถึงข้อมูลได้ง่าย
    - ข้อมูลที่เผยแพร่จะต้องมีการบันทึกเวลา (Timestamps) ที่ช่วยให้ผู้ใช้งานสามารถระบุได้ว่าข้อมูลนั้นเป็นปัจจุบัน
4. สนับสนุนการเผยแพร่ข้อมูลผ่านช่องทางที่ง่ายต่อการเข้าถึงข้อมูล และต้องเปิดเผยข้อมูลในรูปแบบดิจิทัลต่อสาธารณะที่ศูนย์กลางข้อมูลเปิดภาครัฐ (data.go.th) หรือระบบบัญชีภาครัฐ (gdcatalog.go.th) หรือเว็บไซต์หลัก สสส. หรือช่องทางที่หน่วยงานของรัฐได้กำหนดไว้ โดย
    - กำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัยในการเปิดเผยข้อมูลอย่างเพียงพอและมีประสิทธิภาพ
    - มีการตรวจสอบข้อมูลที่เผยแพร่จากหน่วยงานทั้งภายในและภายนอกหน่วยงาน เพื่อให้มั่นใจว่าหน่วยงานได้มีข้อมูลที่เผยแพร่ที่มีคุณค่า
    - การเผยแพร่ข้อมูล ต้องมีการตรวจสอบรูปแบบข้อมูลที่เผยแพร่ให้สอดคล้องกับมาตรฐานที่หน่วยงานกำหนด
    - หากการเปิดเผยข้อมูลไม่ครบถ้วน หรือไม่เป็นปัจจุบัน ให้แจ้งเจ้าของข้อมูลและบริกรข้อมูล ทำการจัดทำหรือปรับปรุงให้เป็นปัจจุบัน
    - ข้อมูลที่เผยแพร่ต้องไม่ขัดต่อกฎหมาย รวมถึงกฎหมายว่าด้วยทรัพย์สินทางปัญญา เว้นแต่การเปิดเผยข้อมูลจะเป็นไปตามอำนาจที่กฎหมายรับรอง
5. กำหนดให้เปิดเผยข้อมูลส่วนบุคคลตามข้อกำหนดของ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล หรือตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคล (สสส.) เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคลตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล
6. เจ้าของข้อมูลข้อมูลห้ามเปิดเผยข้อมูลความมั่นคง และข้อมูลความลับทางราชการที่อยู่ในความครอบครองของหน่วยงาน ยกเว้นได้รับการอนุมัติจาก สสส. รวมทั้งห้ามเปิดเผยข้อมูลที่เป็นการกระทำความผิดตามกฎหมาย นโยบาย และแนวปฏิบัติอันทำให้เกิดความเสียหายต่อหน่วยงานเจ้าของข้อมูลร่วมกับบริกรข้อมูล กำหนดรอบระยะเวลาในการตรวจสอบและปรับปรุงข้อมูลที่เปิดเผยเพื่อให้ข้อมูลถูกต้อง และเป็นปัจจุบัน

2.6 การทำลายข้อมูล

เพื่อกำหนดแนวปฏิบัติการทำลายข้อมูล หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ เพื่อเป็นการรักษาความมั่นคงปลอดภัยของข้อมูล

ตารางที่ 6 การดำเนินการและผู้มีส่วนร่วม ในกระบวนการทำลายข้อมูล

กิจกรรม	เจ้าของข้อมูล	บริกรข้อมูล	ผู้ดูแลระบบสารสนเทศ	ผู้ทำลายข้อมูล
กำหนดผู้มีสิทธิ์ในการทำลายข้อมูล	x	x		
กำหนดสิทธิ์ในการทำลายข้อมูลให้แก่ผู้ทำลายข้อมูล			x	
ทำลายข้อมูลตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน				x
จัดเก็บคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตาที่ทำลายสำหรับตรวจสอบในภายหลัง	x	x		
จัดเก็บบันทึกรายละเอียดการทำลายข้อมูลไว้ในทะเบียนควบคุมและบันทึกการทำลายข้อมูล โดยให้เก็บรักษาไว้เป็นหลักฐานไม่น้อยกว่า 1 ปี				x
ทำลายข้อมูลส่วนบุคคลเมื่อเจ้าของข้อมูลส่วนบุคคลร้องขอหรือข้อมูลส่วนบุคคลที่พ้นระยะเวลาการเก็บรักษา ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล				x

การดำเนินการ

1. เจ้าของข้อมูลร่วมกับบริการข้อมูล กำหนดผู้มีสิทธิ์ในการทำลายข้อมูล หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ และจะต้องทบทวนสิทธิ์นั้นอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ ได้แก่ การลาออก เปลี่ยนตำแหน่ง โอนย้าย สิ้นสุดการจ้าง การปรับโครงสร้าง หรือเมื่อมีการปรับปรุงระบบสารสนเทศ เป็นต้น
2. ผู้ดูแลระบบสารสนเทศจะต้องกำหนดสิทธิ์ในการทำลายข้อมูลให้แก่ผู้ทำลายข้อมูลตามที่เจ้าของข้อมูลกำหนด
3. ผู้ทำลายข้อมูลต้องทำลายข้อมูลตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ สสส.
4. กำหนดให้เจ้าของข้อมูลร่วมกับบริกรข้อมูล จัดเก็บคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตาที่ทำลายสำหรับตรวจสอบในภายหลัง
5. กำหนดให้ผู้ทำลายข้อมูลจัดเก็บบันทึกรายละเอียดการทำลายข้อมูลไว้ในทะเบียนควบคุมและบันทึกการทำลายข้อมูล โดยให้เก็บรักษาไว้เป็นหลักฐานไม่น้อยกว่า 1 ปี

6. กำหนดให้ผู้ประมวลผลข้อมูลส่วนบุคคลทำลายข้อมูลส่วนบุคคลเมื่อเจ้าของข้อมูลส่วนบุคคลร้องขอตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยจะต้องผ่านการเห็นชอบจากผู้ควบคุมข้อมูลส่วนบุคคล และดำเนินการตามข้อกำหนดที่ผู้ควบคุมข้อมูลส่วนบุคคลกำหนดไว้อย่างเคร่งครัด

3. บทบาทและหน้าที่ของเจ้าของข้อมูล (Data Owner)

เพื่อให้การดำเนินงานด้านธรรมาภิบาลข้อมูล และการบริหารจัดการข้อมูลตามวงจรชีวิตของข้อมูล (Data Life Cycle) **ที่ได้กำหนดบทบาทหน้าที่ของเจ้าของข้อมูล (Data Owner)** ในการบริหารจัดการข้อมูลที่อยู่ในความรับผิดชอบ เพื่อให้ได้ข้อมูลที่มีคุณภาพ ประกอบด้วย กระบวนการสร้างข้อมูล (Create) กระบวนการจัดเก็บข้อมูล (Store) กระบวนการใช้ข้อมูล (Use) กระบวนการเผยแพร่ข้อมูล (Publish) กระบวนการจัดเก็บข้อมูลถาวร (Archive) และกระบวนการทำลายข้อมูล (Destroy) โดยบทบาทและหน้าที่ของเจ้าของข้อมูล ประกอบด้วย

1. เจ้าของข้อมูลเป็นผู้กำหนดผู้มีสิทธิ์ในการสร้างข้อมูล และจะต้องทบทวนสิทธิ์การเข้าถึงเพื่อประมวลผลและใช้ข้อมูลของผู้ใช้งานอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ ได้แก่ การลาออก เปลี่ยนตำแหน่ง โอนย้าย สิ้นสุดการจ้าง การปรับโครงสร้าง หรือเมื่อมีการปรับปรุงระบบสารสนเทศ
2. กำหนดให้เจ้าของข้อมูลตรวจสอบความถูกต้องของข้อมูลที่ถูกสร้างขึ้น
3. เจ้าของข้อมูลเป็นผู้กำหนดชั้นความลับของข้อมูลที่ถูกสร้างขึ้นตามวิธีปฏิบัติการจำแนกชั้นความลับของข้อมูล
4. เจ้าของข้อมูลจะต้องกำหนดผู้มีสิทธิ์เข้าถึงเพื่อประมวลผลและใช้ข้อมูลตามชั้นความลับ ดังนี้
    - ข้อมูลที่มีชั้นความลับ กำหนดให้ผู้ใช้งานที่ได้รับสิทธิ์ตามตำแหน่ง/บทบาท เท่านั้น
    - ข้อมูลใช้ภายใน กำหนดให้ผู้บริหาร เจ้าหน้าที่ ลูกจ้าง และเจ้าหน้าที่ของรัฐมาช่วยปฏิบัติงาน รวมถึงพนักงานจ้างเหมาบริการเท่านั้น ที่มีสิทธิ์เข้าถึงเพื่อประมวลผลและใช้งานข้อมูลได้ ทั้งนี้ต้องปกป้องข้อมูลจากการเข้าถึงโดยบุคคลภายนอก
    - ข้อมูลเปิดเผยได้ ไม่กำหนดสิทธิ์การเข้าถึงเพื่อประมวลผลและใช้งานข้อมูล
5. เจ้าของข้อมูลจะต้องกำหนดระยะเวลาในการจัดเก็บข้อมูลที่ชัดเจน
6. กรณีข้อมูลที่จัดเก็บในรูปแบบเอกสาร ให้มีการจัดเก็บดังนี้
    - เก็บในสถานที่เหมาะสม มีมาตรการป้องกันการเข้าถึงข้อมูล เช่น สามารถปิดล็อคได้เมื่อไม่ใช้งาน
    - เก็บแยกออกจากอุปกรณ์ประมวลผลต่าง ๆ ได้แก่ เครื่องถ่ายเอกสาร เครื่องพิมพ์ เป็นต้น เพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิ์ในการเข้าถึงข้อมูลได้
    - กำหนดให้มีการจัดเก็บข้อมูลส่วนบุคคล โดยให้เก็บรวบรวมได้เท่าที่จำเป็น ภายใต้อำนาจหน้าที่และวัตถุประสงค์อันชอบด้วยกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล
    - กำหนดให้มีมาตรการรักษาความปลอดภัยในการจัดเก็บข้อมูล รวมทั้งกรณีที่มีการเคลื่อนย้ายอุปกรณ์ที่จัดเก็บข้อมูล เพื่อป้องกันมิให้มีการเข้าถึงโดยมิได้รับอนุญาต หรือลักลอบนำข้อมูลไปใช้ที่ก่อให้เกิดความเสียหายต่อหน่วยงาน

7. เจ้าของข้อมูลร่วมกับบริกรข้อมูล ร่วมจัดทำคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตา (Metadata) เมื่อมีการสร้างชุดข้อมูล (Datasets) ตามมาตรฐานคำอธิบายชุดข้อมูลดิจิทัลที่ สสส. กำหนด และสอดคล้องกับมาตรฐานที่ภาครัฐได้กำหนดไว้
8. กำหนดให้เจ้าของข้อมูล หรือบริกรข้อมูลตามที่ได้รับมอบหมายดำเนินการตรวจสอบคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตาของข้อมูลที่จะทำการเชื่อมโยงและแลกเปลี่ยนให้ครบถ้วน ดังนี้
    - ตรวจสอบเมทาดาตาของชุดข้อมูลดิจิทัลที่จัดเก็บให้มีฟิลด์ข้อมูลครบถ้วนสอดคล้องกับความต้องการของหน่วยงานที่ขอใช้ หากไม่ครบถ้วนต้องจัดทำเพิ่มเติมตามความต้องการของหน่วยงานที่ขอใช้
    - ตรวจสอบชั้นความลับของข้อมูลว่าอยู่ในชั้นความลับที่สามารถเปิดเผยได้หรือไม่ โดยต้องไม่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ ความมั่นคงของประเทศ ความลับทางราชการ และความเป็นส่วนบุคคล พร้อมทั้งตรวจสอบสิทธิ์ของหน่วยงานที่สามารถนำข้อมูลไปใช้ได้ตามบทบาทและภารกิจตามกฎหมายของหน่วยงานนั้น ๆ หากไม่ครบถ้วนหรือไม่เป็นปัจจุบัน ให้แจ้งเจ้าของข้อมูลและบริกรข้อมูลทำการจัดทำหรือปรับปรุงให้เป็นปัจจุบัน
9. กำหนดให้เจ้าของข้อมูลหรือบริกรข้อมูล จัดทำแนวทาง/กระบวนการ ในการเชื่อมโยงและแลกเปลี่ยนข้อมูล โดยมีองค์ประกอบ ดังต่อไปนี้เป็นอย่างน้อย
    - วัตถุประสงค์ในการนำข้อมูลไปใช้งาน
    - ขอบเขตการนำข้อมูลไปใช้งาน
    - ช่วงเวลาและความถี่ในการเข้าถึงข้อมูลและการนำข้อมูลไปใช้
    - ชุดข้อมูล รายการข้อมูล ฟิลด์ข้อมูลที่สามารถเข้าถึง
    - กำหนดวิธีการ แนวทาง และรายละเอียดของการเชื่อมโยงและการแลกเปลี่ยนข้อมูลดิจิทัล
    - ในกรณีขอข้อมูลส่วนบุคคลเป็นรายคน ต้องจัดทำหนังสือแสดงความยินยอม เพื่อรับการยินยอมจากบุคคลนั้น ๆ หรือได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลดังกล่าวไว้ก่อนหน้านั้นแล้วตามวัตถุประสงค์ในแต่ละกิจกรรมไว้อย่างชัดเจน ยกเว้นหน่วยงานที่ขอใช้ข้อมูลมีอำนาจตามกฎหมายโดยชอบธรรม
10. เจ้าของข้อมูลร่วมกับบริกรข้อมูล กำหนดช่องทางการเปิดเผยข้อมูลที่เข้าถึงและนำไปใช้ง่าย
11. กำหนดให้เจ้าของข้อมูลร่วมกับบริกรข้อมูล คัดเลือกข้อมูลที่จะเปิดเผยในรูปแบบข้อมูลเปิดจากลำดับชั้นความสำคัญของชุดข้อมูล
12. เจ้าของข้อมูลร่วมกับบริกรข้อมูล คัดเลือกข้อมูลที่จะเปิดเผยในรูปแบบข้อมูลเปิด (Open Data) ในรูปแบบข้อมูลเปิดของ สสส. โดยดำเนินการ ดังนี้
    - กำหนดลักษณะของข้อมูลที่เผยแพร่กำหนดให้อยู่ในรูปแบบที่เครื่องสามารถประมวลผลได้
    - กำหนดให้มีคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตา และพจนานุกรมข้อมูล (Data Dictionary) สำหรับข้อมูลที่ต้องเปิดเผย และสอดคล้องกับมาตรฐานตามที่หน่วยงานของรัฐได้กำหนดไว้
    - ชุดข้อมูลและรายการชุดข้อมูลที่เผยแพร่ จะต้องมีการจัดรูปแบบที่กำหนดเป็นมาตรฐาน และกำหนดภายใต้หมวดหมู่เดียวกัน เพื่อให้ผู้ใช้ข้อมูลสามารค้นหาและเข้าถึงข้อมูลได้ง่าย
    - ข้อมูลที่เผยแพร่จะต้องมีการบันทึกเวลา (Timestamps) ที่ช่วยให้ผู้ใช้งานสามารถระบุได้ว่าข้อมูลนั้นเป็นปัจจุบัน

13. สนับสนุนการเผยแพร่ข้อมูลผ่านช่องทางที่ง่ายต่อการเข้าถึงข้อมูล และต้องเปิดเผยข้อมูลในรูปแบบดิจิทัลต่อสาธารณะที่ศูนย์กลางข้อมูลเปิดภาครัฐ (data.go.th) หรือระบบบัญชีภาครัฐ (gdcatalog.go.th) หรือเว็บไซต์หลัก สสส. หรือช่องทางที่หน่วยงานของรัฐได้กำหนดไว้ โดย
    - กำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัยในการเปิดเผยข้อมูลอย่างเพียงพอและมีประสิทธิภาพ
    - มีการตรวจสอบข้อมูลที่เผยแพร่จากหน่วยงานทั้งภายในและภายนอกหน่วยงาน เพื่อให้มั่นใจว่าหน่วยงานได้มีข้อมูลที่เผยแพร่ที่มีคุณค่า
    - การเผยแพร่ข้อมูล ต้องมีการตรวจสอบรูปแบบข้อมูลที่เผยแพร่ให้สอดคล้องกับมาตรฐานที่หน่วยงานกำหนด
    - หากการเปิดเผยข้อมูลไม่ครบถ้วน หรือไม่เป็นปัจจุบัน ให้แจ้งเจ้าของข้อมูลและบริกรข้อมูล ทำการจัดทำหรือปรับปรุงให้เป็นปัจจุบัน
    - ข้อมูลที่เผยแพร่ต้องไม่ขัดต่อกฎหมาย รวมถึงกฎหมายว่าด้วยทรัพย์สินทางปัญญา เว้นแต่การเปิดเผยข้อมูลจะเป็นไปตามอำนาจที่กฎหมายรับรอง
14. กำหนดให้เจ้าของข้อมูลร่วมกับบริกรข้อมูล คัดเลือกข้อมูลที่จะเปิดเผยในรูปแบบข้อมูลเปิดจากลำดับชั้นความสำคัญของชุดข้อมูล
15. กำหนดให้เปิดเผยข้อมูลส่วนบุคคลตามข้อกำหนดของ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล หรือตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคล (สสส.) เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคล ตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล
16. เจ้าของข้อมูลข้อมูลห้ามเปิดเผยข้อมูลความมั่นคง และข้อมูลความลับทางราชการที่อยู่ในความครอบครองของหน่วยงาน ยกเว้นได้รับการอนุมัติจาก สสส. รวมทั้งห้ามเปิดเผยข้อมูลที่เป็นการกระทำความผิดตามกฎหมาย นโยบาย และแนวปฏิบัติอันทำให้เกิดความเสียหายต่อหน่วยงาน
17. เจ้าของข้อมูลร่วมกับบริกรข้อมูล กำหนดรอบระยะเวลาในการตรวจสอบและปรับปรุงข้อมูลที่เปิดเผยเพื่อให้ข้อมูลถูกต้องและเป็นปัจจุบัน
18. เจ้าของข้อมูลร่วมกับบริกรข้อมูล กำหนดผู้มีสิทธิ์ในการทำลายข้อมูล หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ และจะต้องทบทวนสิทธิ์นั้นอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ ได้แก่ การลาออก เปลี่ยนตำแหน่ง โอนย้าย สิ้นสุดการจ้าง การปรับโครงสร้าง หรือเมื่อมีการปรับปรุงระบบสารสนเทศ เป็นต้น
19. กำหนดให้เจ้าของข้อมูลร่วมกับบริกรข้อมูล จัดเก็บคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตาที่ทำลายสำหรับตรวจสอบในภายหลัง
20. เจ้าของข้อมูลร่วมกับบริกรข้อมูล ทำการประเมินคุณค่าของชุดข้อมูลดิจิทัลตามแบบฟอร์มประเมินคุณค่าชุดข้อมูลที่ สพร. หรือ สสส. กำหนด และเผยแพร่เป็นข้อมูลเปิดของหน่วยงานต่อสาธารณะตามกฎหมายว่าด้วยข้อมูลข่าวสารของราชการในรูปแบบข้อมูลดิจิทัล

4. บทบาทและหน้าที่ของบริกรข้อมูล (Data Steward)

เพื่อให้การดำเนินงานด้านธรรมาภิบาลข้อมูล และการบริหารจัดการข้อมูลตามวงจรชีวิตของข้อมูล (Data Life Cycle) **ที่ได้กำหนดบทบาทหน้าที่ของบริกรข้อมูล (Data Steward)** ในการบริหารจัดการข้อมูลที่อยู่ในความรับผิดชอบ เพื่อให้ได้ข้อมูลที่มีคุณภาพ ประกอบด้วย กระบวนการสร้างข้อมูล (Create) กระบวนการจัดเก็บข้อมูล (Store) กระบวนการใช้ข้อมูล (Use) กระบวนการเผยแพร่ข้อมูล (Publish) กระบวนการจัดเก็บข้อมูลถาวร (Archive) และกระบวนการทำลายข้อมูล (Destroy) โดยบทบาทและหน้าที่ของบริกรข้อมูล

1. เจ้าของข้อมูลร่วมกับบริกรข้อมูล ร่วมจัดทำคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตา (Metadata) เมื่อมีการสร้างชุดข้อมูล (Datasets) ตามมาตรฐานคำอธิบายชุดข้อมูลดิจิทัลที่ สสส. กำหนด และสอดคล้องกับมาตรฐานที่ภาครัฐได้กำหนดไว้
2. กำหนดให้เจ้าของข้อมูล หรือบริกรข้อมูลตามที่ได้รับมอบหมายดำเนินการตรวจสอบคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตาของข้อมูลที่จะทำการเชื่อมโยงและแลกเปลี่ยนให้ครบถ้วน ดังนี้
    - ตรวจสอบเมทาดาตาของชุดข้อมูลดิจิทัลที่จัดเก็บให้มีฟิลด์ข้อมูลครบถ้วนสอดคล้องกับความต้องการของหน่วยงานที่ขอใช้ หากไม่ครบถ้วนต้องจัดทำเพิ่มเติมตามความต้องการของหน่วยงานที่ขอใช้
    - ตรวจสอบชั้นความลับของข้อมูลว่าอยู่ในชั้นความลับที่สามารถเปิดเผยได้หรือไม่ โดยต้องไม่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ ความมั่นคงของประเทศ ความลับทางราชการ และความเป็นส่วนบุคคล พร้อมทั้งตรวจสอบสิทธิ์ของหน่วยงานที่สามารถนำข้อมูลไปใช้ได้ตามบทบาทและภารกิจตามกฎหมายของหน่วยงานนั้น ๆ หากไม่ครบถ้วนหรือไม่เป็นปัจจุบัน ให้แจ้งเจ้าของข้อมูลและบริกรข้อมูลทำการจัดทำหรือปรับปรุงให้เป็นปัจจุบัน
3. กำหนดให้เจ้าของข้อมูลหรือบริกรข้อมูล จัดทำแนวทาง/กระบวนการ ในการเชื่อมโยงและแลกเปลี่ยนข้อมูล โดยมีองค์ประกอบ ดังต่อไปนี้เป็นอย่างน้อย
    - วัตถุประสงค์ในการนำข้อมูลไปใช้งาน
    - ขอบเขตการนำข้อมูลไปใช้งาน
    - ช่วงเวลาและความถี่ในการเข้าถึงข้อมูลและการนำข้อมูลไปใช้
    - ชุดข้อมูล รายการข้อมูล ฟิลด์ข้อมูลที่สามารถเข้าถึง
    - กำหนดวิธีการ แนวทาง และรายละเอียดของการเชื่อมโยงและการแลกเปลี่ยนข้อมูลดิจิทัล
    - ในกรณีขอข้อมูลส่วนบุคคลเป็นรายคน ต้องจัดทำหนังสือแสดงความยินยอม เพื่อรับการยินยอมจากบุคคลนั้น ๆ หรือได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลดังกล่าวไว้ก่อนหน้านั้นแล้วตามวัตถุประสงค์ในแต่ละกิจกรรมไว้อย่างชัดเจน ยกเว้นหน่วยงานที่ขอใช้ข้อมูลมีอำนาจตามกฎหมายโดยชอบธรรม
4. เจ้าของข้อมูลร่วมกับบริกรข้อมูล กำหนดช่องทางการเปิดเผยข้อมูลที่เข้าถึงและนำไปใช้ง่าย
5. กำหนดให้เจ้าของข้อมูลร่วมกับบริกรข้อมูล คัดเลือกข้อมูลที่จะเปิดเผยในรูปแบบข้อมูลเปิดจากลำดับชั้นความสำคัญของชุดข้อมูล

6. เจ้าของข้อมูลร่วมกับบริกรข้อมูล คัดเลือกข้อมูลที่จะเปิดเผยในรูปแบบข้อมูลเปิด (Open Data) ในรูปแบบข้อมูลเปิดของ สสส. โดยดำเนินการ ดังนี้
    - กำหนดลักษณะของข้อมูลที่เผยแพร่กำหนดให้อยู่ในรูปแบบที่เครื่องสามารถประมวลผลได้
    - กำหนดให้มีคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตา และพจนานุกรมข้อมูล (Data Dictionary) สำหรับข้อมูลที่ต้องเปิดเผย และสอดคล้องกับมาตรฐานตามที่หน่วยงานของรัฐได้กำหนดไว้
    - ชุดข้อมูลและรายการชุดข้อมูลที่เผยแพร่ จะต้องมีการจัดรูปแบบที่กำหนดเป็นมาตรฐาน และกำหนดภายใต้หมวดหมู่เดียวกัน เพื่อให้ผู้ใช้ข้อมูลสามารค้นหาและเข้าถึงข้อมูลได้ง่าย
    - ข้อมูลที่เผยแพร่จะต้องมีการบันทึกเวลา (Timestamps) ที่ช่วยให้ผู้ใช้งานสามารถระบุได้ว่าข้อมูลนั้นเป็นปัจจุบัน
7. สนับสนุนการเผยแพร่ข้อมูลผ่านช่องทางที่ง่ายต่อการเข้าถึงข้อมูล และต้องเปิดเผยข้อมูลในรูปแบบดิจิทัลต่อสาธารณะที่ศูนย์กลางข้อมูลเปิดภาครัฐ (data.go.th) หรือระบบบัญชีภาครัฐ (gdcatalog.go.th) หรือเว็บไซต์หลัก สสส. หรือช่องทางที่หน่วยงานของรัฐได้กำหนดไว้ โดย
    - กำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัยในการเปิดเผยข้อมูลอย่างเพียงพอและมีประสิทธิภาพ
    - มีการตรวจสอบข้อมูลที่เผยแพร่จากหน่วยงานทั้งภายในและภายนอกหน่วยงาน เพื่อให้มั่นใจว่าหน่วยงานได้มีข้อมูลที่เผยแพร่ที่มีคุณค่า
    - การเผยแพร่ข้อมูล ต้องมีการตรวจสอบรูปแบบข้อมูลที่เผยแพร่ให้สอดคล้องกับมาตรฐานที่หน่วยงานกำหนด
    - หากการเปิดเผยข้อมูลไม่ครบถ้วน หรือไม่เป็นปัจจุบัน ให้แจ้งเจ้าของข้อมูลและบริกรข้อมูล ทำการจัดทำหรือปรับปรุงให้เป็นปัจจุบัน
    - ข้อมูลที่เผยแพร่ต้องไม่ขัดต่อกฎหมาย รวมถึงกฎหมายว่าด้วยทรัพย์สินทางปัญญา เว้นแต่การเปิดเผยข้อมูลจะเป็นไปตามอำนาจที่กฎหมายรับรอง
8. กำหนดให้เปิดเผยข้อมูลส่วนบุคคลตามข้อกำหนดของ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล หรือตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคล (สสส.) เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคลตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล
9. เจ้าของข้อมูลร่วมกับบริกรข้อมูล กำหนดรอบระยะเวลาในการตรวจสอบและปรับปรุงข้อมูลที่เปิดเผยเพื่อให้ข้อมูลถูกต้อง และเป็นปัจจุบัน
10. บริกรข้อมูลร่วมกับร่วมกับผู้ดูแลระบบสารสนเทศ กำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัยเกี่ยวกับการเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัล เพื่อป้องกันมิให้มีการรับส่งข้อมูลที่ไม่สมบูรณ์ หรือส่งข้อมูลไปผิดที่หรือมีการรั่วไหลของข้อมูล หรือข้อมูลถูกแก้ไขเปลี่ยนแปลง ถูกทำซ้ำใหม่ ถูกส่งซ้ำโดยมิได้รับอนุญาต
11. บริกรข้อมูลร่วมกับร่วมกับผู้ดูแลระบบสารสนเทศ ทำสัญญาอนุญาตหรือข้อตกลงในการแลกเปลี่ยนข้อมูลและการนำไปใช้
12. เจ้าของข้อมูลร่วมกับบริกรข้อมูล กำหนดผู้มีสิทธิ์ในการทำลายข้อมูล หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ และจะต้องทบทวนสิทธิ์นั้นอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ ได้แก่ การลาออก เปลี่ยนตำแหน่ง โอนย้าย สิ้นสุดการจ้าง การปรับโครงสร้าง หรือเมื่อมีการปรับปรุงระบบสารสนเทศ เป็นต้น

13. กำหนดให้เจ้าของข้อมูลร่วมกับบริกรข้อมูล จัดเก็บคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตาที่ทำลายสำหรับตรวจสอบในภายหลัง
14. เจ้าของข้อมูลร่วมกับบริกรข้อมูล ทำการประเมินคุณค่าของชุดข้อมูลดิจิทัลตามแบบฟอร์มประเมินคุณค่าชุดข้อมูลที่ สพร. หรือ สสส. กำหนด และเผยแพร่เป็นข้อมูลเปิดของหน่วยงานต่อสาธารณะตามกฎหมายว่าด้วยข้อมูลข่าวสารของราชการในรูปแบบข้อมูลดิจิทัล

5. บทบาทและหน้าที่ของผู้ดูแลระบบสารสนเทศ (Technical Stewards)

เพื่อให้การดำเนินงานด้านธรรมาภิบาลข้อมูล และการบริหารจัดการข้อมูลตามวงจรชีวิตของข้อมูล (Data Life Cycle) **ที่ได้กำหนดบทบาทหน้าที่ของผู้ดูแลระบบสารสนเทศ (Technical Stewards)** ในการบริหารจัดการข้อมูลที่อยู่ในความรับผิดชอบ เพื่อให้ได้ข้อมูลที่มีคุณภาพ ประกอบด้วย กระบวนการสร้างข้อมูล (Create) กระบวนการจัดเก็บข้อมูล (Store) กระบวนการใช้ข้อมูล (Use) กระบวนการเผยแพร่ข้อมูล (Publish) กระบวนการจัดเก็บข้อมูลถาวร (Archive) และกระบวนการทำลายข้อมูล (Destroy) โดยบทบาทและหน้าที่ของผู้ดูแลระบบสารสนเทศ

1. ผู้ดูแลระบบสารสนเทศจะต้องกำหนดสิทธิ์ในการสร้างข้อมูลให้แก่ผู้สร้างข้อมูลตามที่เจ้าของข้อมูลกำหนด
2. ผู้ดูแลระบบสารสนเทศจะต้องกำหนดสิทธิ์ในการเข้าถึงเพื่อประมวลผล และใช้ข้อมูลผู้ใช้งานตามที่เจ้าของข้อมูลกำหนด
3. ผู้ดูแลระบบสารสนเทศจะต้องกำหนดสิทธิ์ในการทำลายข้อมูลให้แก่ผู้ทำลายข้อมูลตามที่เจ้าของข้อมูลกำหนด
4. บริกรข้อมูลและผู้ดูแลระบบสารสนเทศ ทำการย้ายข้อมูลที่มีการจัดเก็บเกินระยะเวลาที่กำหนดแล้ว เพื่อจัดเก็บเป็นข้อมูลถาวร
5. การจัดเก็บข้อมูลที่มีชั้นความลับให้ทำการเข้ารหัสข้อมูล เพื่อป้องกันการเข้าถึงหรือแก้ไขข้อมูลโดยไม่ได้รับอนุญาต
6. กำหนดให้ผู้ดูระบบสารสนเทศต้องจัดเก็บบันทึกหลักฐานของการเชื่อมโยง และการแลกเปลี่ยนข้อมูลดิจิทัล (Log File) เพื่อให้สามารถตรวจสอบย้อนกลับได้
7. กำหนดให้มีการจัดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่า 90 วัน นับแต่วันที่ข้อมูลเข้าสู่ระบบคอมพิวเตอร์ เพื่อให้สามารถระบุตัวผู้ใช้บริการนับแต่เริ่มใช้บริการ ให้สอดคล้องตามกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ ซึ่งประกอบด้วยข้อมูลอินเทอร์เน็ตที่เกิดจากการเข้าถึงระบบเครือข่าย และข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการจดหมายอิเล็กทรอนิกส์ (e-mail servers)
8. กำหนดให้การจัดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ให้สอดคล้องตามกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ ผู้ให้บริการจะต้องใช้วิธีการที่มั่นคงปลอดภัยอย่างน้อย ดังนี้
    - เก็บในสื่อ (Media) ที่สามารถรักษาความครบถ้วน ถูกต้องแท้จริง (Integrity) และระบุตัวตน (Identification) ที่เข้าถึงสื่อดังกล่าวได้

- มีระบบการเก็บรักษาความลับของข้อมูลที่จัดเก็บ และกำหนดชั้นความลับในการเข้าถึงข้อมูลดังกล่าว เพื่อรักษาความน่าเชื่อถือของข้อมูล และไม่อนุญาตให้ผู้ดูแลระบบสามารถแก้ไขข้อมูลที่เก็บรักษาไว้
- การจัดเก็บข้อมูลต้องสามารถระบุรายละเอียดผู้ใช้งานเป็นรายบุคคลได้ (Identification and Authentication)

9. กำหนดให้มีมาตรการรักษาความปลอดภัยของการถ่ายโอนข้อมูลกับหน่วยงานภายนอกที่ผ่านช่องทางการสื่อสารทุกชนิด โดยต้องสอดคล้องตามนโยบายความมั่นคงปลอดภัยสารสนเทศ
10. กำหนดเทคโนโลยีและมาตรฐานทางเทคนิคที่ใช้ในการแลกเปลี่ยนข้อมูล
11. บริกรข้อมูลร่วมกับร่วมกับผู้ดูแลระบบสารสนเทศ กำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัยเกี่ยวกับการเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัล เพื่อป้องกันมิให้มีการรับส่งข้อมูลที่ไม่สมบูรณ์ หรือส่งข้อมูลไปผิดที่หรือมีการรั่วไหลของข้อมูล หรือข้อมูลถูกแก้ไขเปลี่ยนแปลง ถูกทำซ้ำใหม่ ถูกส่งซ้ำโดยมิได้รับอนุญาต
12. บริกรข้อมูลร่วมกับร่วมกับผู้ดูแลระบบสารสนเทศ ทำสัญญาอนุญาตหรือข้อตกลงในการแลกเปลี่ยนข้อมูลและการนำไปใช้