



สถาบันวิจัยแสงซินโครตรอน (องค์การมหาชน)

แนวทางปฏิบัติธรรมาภิบาลข้อมูล

สถาบันวิจัยแสงซินโครตรอน (องค์การมหาชน)

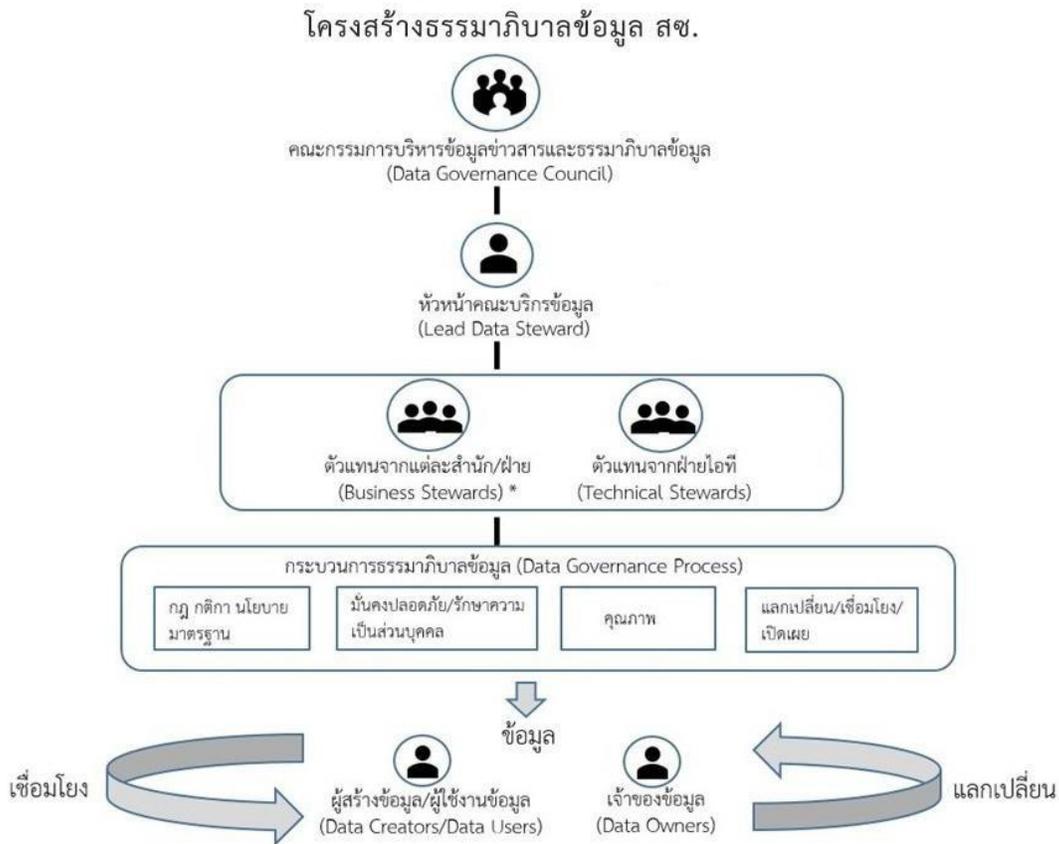
แนวปฏิบัติธรรมาภิบาลข้อมูล

ส่วนเทคโนโลยีสารสนเทศและสื่อสาร สถาบันวิจัยแสงซินโครตรอน (องค์การมหาชน) หรือ สช. ได้จัดทำแนวปฏิบัติธรรมาภิบาลข้อมูล เพื่ออธิบายการดำเนินงานของ สช. เกี่ยวกับธรรมาภิบาลข้อมูลและการบริหารจัดการข้อมูล รวมถึงแนวปฏิบัติต่าง ๆ นำไปสู่การบริหารจัดการข้อมูลที่มีประสิทธิภาพ มีคุณภาพ มีความปลอดภัย มีการเชื่อมโยง และสามารถดำเนินการได้อย่างต่อเนื่องและยั่งยืน

1. โครงสร้างธรรมาภิบาลข้อมูล

โครงสร้างธรรมาภิบาลข้อมูลเป็นการแสดงลำดับชั้นระหว่างกลุ่มบุคคลที่เกี่ยวข้องกับธรรมาภิบาลข้อมูลของ สช. และแสดงถึงสิทธิ์ในการสั่งการตามลำดับชั้น แบ่งเป็น 3 ส่วน ประกอบด้วย

- 1) คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council)
- 2) ทีมบริการข้อมูล (Data Steward Team)
- 3) ผู้มีส่วนได้เสียกับข้อมูล (Data Stakeholders)



รูปที่ 1. 1 โครงสร้างธรรมาภิบาลข้อมูล สช.

2. ระบบบริหารและกระบวนการจัดการข้อมูล (Data Life Cycle)

ระบบบริหารและกระบวนการจัดการข้อมูลหรือวงจรชีวิตของข้อมูล หมายถึง ลำดับขั้นตอนของข้อมูลตั้งแต่เริ่มสร้างข้อมูลไปจนถึงการทำลายข้อมูล ประกอบด้วย กระบวนการสร้างข้อมูล (Create) กระบวนการจัดเก็บข้อมูล (Store) กระบวนการใช้ข้อมูล (Use) กระบวนการเผยแพร่ข้อมูล (Publish) กระบวนการจัดเก็บข้อมูลถาวร (Archive) และกระบวนการทำลายข้อมูล (Destroy)

2.1 การสร้างข้อมูล

กระบวนการสร้างข้อมูล เป็นการสร้างข้อมูลขึ้นมาใหม่ โดยวิธีการบันทึกเข้าไปด้วยบุคคลหรือบันทึกอัตโนมัติ ด้วยอุปกรณ์อิเล็กทรอนิกส์ รวมถึงการซื้อข้อมูล หรือการรับข้อมูลมาจากหน่วยงานอื่น เพื่อนำมาจัดเก็บในภายหลัง

ตารางที่ 1.1 การดำเนินการและผู้มีส่วนร่วมในกระบวนการสร้างข้อมูล

กิจกรรม	เจ้าของข้อมูล	บริการข้อมูล	ผู้ดูแลระบบสารสนเทศ
กำหนดผู้มีสิทธิ์ในการสร้างข้อมูล	X		
กำหนดชั้นความลับข้อมูลของข้อมูลที่ถูกสร้างขึ้น	X		
กำหนดสิทธิ์ในการสร้างข้อมูลให้แก่ผู้สร้างข้อมูล			X
จัดทำคำอธิบายชุดข้อมูลดิจิทัล	X	X	
ประเมินคุณค่าของชุดข้อมูลดิจิทัล	X	X	
ตรวจสอบความถูกต้องของข้อมูล	X		

การดำเนินการ

1. เจ้าของข้อมูลเป็นผู้กำหนดผู้มีสิทธิ์ในการสร้างข้อมูลและจะต้องทบทวนสิทธิ์นั้นอย่างน้อยปี ละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ ได้แก่ การลาออก เปลี่ยนตำแหน่ง โอนย้าย สิ้นสุดการจ้าง การปรับ โครงสร้าง หรือเมื่อมีการปรับปรุงระบบสารสนเทศ เป็นต้น

2. เจ้าของข้อมูลเป็นผู้กำหนดชั้นความลับของข้อมูลที่ถูกสร้างขึ้นตามวิธีปฏิบัติกรจำแนกชั้น

3. เจ้าของข้อมูลกำหนดให้มีวิธีปฏิบัติกรจำแนกชั้นความลับของข้อมูลสำหรับข้อมูลที่ถูกสร้างขึ้นความลับของข้อมูล

4. ผู้ดูแลระบบสารสนเทศจะต้องกำหนดสิทธิ์ในการสร้างข้อมูลให้แก่ผู้สร้างข้อมูลตามที่เจ้าของข้อมูลกำหนด

5. เจ้าของข้อมูลร่วมกับบริการข้อมูล ร่วมจัดทำคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาทา (Metadata) เมื่อมีการสร้างชุดข้อมูล (Datasets) ตามมาตรฐานคำอธิบายชุดข้อมูลดิจิทัลที่ สข. กำหนด และ สอดคล้องกับมาตรฐานที่ภาครัฐได้กำหนดไว้

6. เจ้าของข้อมูลร่วมกับบริการข้อมูล ทำการประเมินคุณค่าของชุดข้อมูลดิจิทัลตามแบบฟอร์ม ประเมิน คุณค่าชุดข้อมูลที่ สพร. หรือ สข. กำหนด และเผยแพร่เป็นข้อมูลเปิดของหน่วยงานต่อสาธารณะตาม กฎหมายว่าด้วยข้อมูลข่าวสารของราชการในรูปแบบข้อมูลดิจิทัล

7.ห้ามมิให้ผู้สร้างข้อมูลนำข้อมูลที่มีลักษณะดังต่อไปนี้เข้าสู่ระบบคอมพิวเตอร์ที่ขัดต่อกฎหมาย ว่าด้วยการกระทำ ความผิดทางคอมพิวเตอร์

7.1. ข้อมูลที่บิดเบือน หรือปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลอันเป็นเท็จ น่าจะ เกิดความเสียหายแก่ ประชาชน

7.2. ข้อมูลอันเป็นเท็จที่น่าจะเกิดความเสียหายต่อการรักษาความมั่นคงปลอดภัย ความ ปลอดภัยสาธารณะ ความ มั่นคงทางเศรษฐกิจ หรือโครงสร้างพื้นฐาน หรือก่อให้เกิดความตื่นตระหนก

7.3. ข้อมูลอันเป็นความผิดเกี่ยวกับความมั่นคง หรือความผิดเกี่ยวกับการก่อการร้าย

7.4. ข้อมูลที่มีลักษณะอันลามก และประชาชนทั่วไปอาจเข้าถึงได้

7.5. ข้อมูลที่ปรากฏภาพของผู้อื่น และเป็นภาพที่สร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใด ทำให้ผู้อื่นเสียชื่อเสียง ถูกดูหมิ่นถูกเกลียดชัง หรือได้รับความอับอาย

8.ห้ามมิให้ผู้สร้างข้อมูลทำการสร้าง ทำซ้ำหรือดัดแปลงต่อข้อมูลที่ขัดต่อกฎหมายว่าด้วยลิขสิทธิ์หรือทรัพย์สินทางปัญญา ของผู้อื่นเว้นแต่จะเป็นไปตามอำนาจที่กฎหมายรับรอง

9.กำหนดให้ผู้สร้างข้อมูลสร้างข้อมูลที่มาจากแหล่งข้อมูลที่เชื่อถือได้เท่านั้น

10.กำหนดให้เจ้าของข้อมูลตรวจสอบความถูกต้องของข้อมูลที่ถูกรสร้างขึ้น

11.กำหนดให้มีวิธีปฏิบัติเกี่ยวกับสร้างข้อมูลให้มีความปลอดภัย และเป็นประโยชน์ต่อผู้ใช้ข้อมูล

2.2 การจัดเก็บข้อมูล

กระบวนการจัดเก็บข้อมูล เป็นการจัดเก็บข้อมูลที่เกิดจากกระบวนการสร้าง หรือข้อมูลที่ได้จากการ แลกเปลี่ยนกับ หน่วยงานอื่น เพื่อให้มีระเบียบ ง่ายต่อการใช้งาน ไม่สูญหาย หรือถูกทำลาย และให้ผู้ใช้งานสามารถ ประมวลผลข้อมูลต่าง ๆ ตาม ความต้องการได้อย่างรวดเร็ว ไม่ว่าจะจัดเก็บลงแฟ้มข้อมูล (File) หรือระบบการจัดการ ฐานข้อมูล (Database Management System – DBMS)

ตารางที่ 1. 2 การดำเนินการและผู้มีส่วนร่วม ในกระบวนการจัดเก็บข้อมูล

กิจกรรม	เจ้าของข้อมูล	บริการข้อมูล	ผู้ดูแลระบบสารสนเทศ
กำหนดระยะเวลาในการจัดเก็บข้อมูล	X		
ตรวจสอบความครบถ้วนของชุดข้อมูลหรือเมทาดาดา ของการจัดเก็บชุดข้อมูล	X	X	
ทำการย้ายข้อมูลที่มีการจัดเก็บเกินระยะเวลาที่กำหนด เพื่อจัดเก็บเป็นข้อมูลถาวร		X	X
จัดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์			X

การดำเนินการ

1. เจ้าของข้อมูลจะต้องกำหนดระยะเวลาในการจัดเก็บข้อมูลที่ชัดเจน
2. กำหนดให้การจัดเก็บชุดข้อมูลจะต้องมีคำอธิบายชุดข้อมูลหรือเมทาดาทา หากไม่มีหรือไม่ครบถ้วน ทีมบริหารจัดการข้อมูลจะต้องแจ้งผู้รับผิดชอบ ได้แก่ เจ้าของข้อมูลและบริการข้อมูลร่วมกันจัดทำและปรับปรุงให้เป็นปัจจุบัน
3. บริการข้อมูลและผู้ดูแลระบบสารสนเทศ ทำการย้ายข้อมูลที่มีการจัดเก็บเกินระยะเวลาที่กำหนดแล้ว เพื่อจัดเก็บเป็นข้อมูลถาวร
4. การจัดเก็บข้อมูลที่มีชั้นความลับให้ทำการเข้ารหัสข้อมูล เพื่อป้องกันการเข้าถึงหรือแก้ไขข้อมูลโดยไม่ได้รับอนุญาต
5. กำหนดให้มีการจัดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่า 90 วัน นับแต่วันที่ข้อมูลเข้าสู่ระบบคอมพิวเตอร์ เพื่อให้สามารถระบุตัวผู้ใช้บริการนับแต่เริ่มใช้บริการให้สอดคล้องตามกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ ซึ่งประกอบด้วยข้อมูลอินเทอร์เน็ตที่เกิดจากการเข้าถึงระบบเครือข่าย และข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการจดหมายอิเล็กทรอนิกส์ (e-mail servers)
6. กำหนดให้การจัดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ให้สอดคล้องตามกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ ผู้ให้บริการจะต้องใช้วิธีการที่มั่นคงปลอดภัยอย่างน้อย ดังนี้
 - 6.1. เก็บในสื่อ (Media) ที่สามารถรักษาความครบถ้วน ถูกต้องแท้จริง (Integrity) และ ระบุตัวตน (Identification) ที่เข้าถึงสื่อดังกล่าวได้
 - 6.2. มีระบบการเก็บรักษาความลับของข้อมูลที่จัดเก็บ และกำหนดชั้นความลับในการ เข้าถึงข้อมูลดังกล่าว เพื่อรักษาความน่าเชื่อถือของข้อมูล และไม่อนุญาตให้ผู้ดูแลระบบสามารถแก้ไขข้อมูลที่เก็บรักษาไว้
 - 6.3. การจัดเก็บข้อมูลต้องสามารถระบุรายละเอียดผู้ใช้งานเป็นรายบุคคลได้ (Identification and Authentication)
7. กรณีข้อมูลที่จัดเก็บในรูปแบบเอกสารให้มีการจัดเก็บดังนี้
 - 7.1. เก็บในสถานที่เหมาะสม มีมาตรการป้องกันการเข้าถึงข้อมูล เช่น สามารถปิดล็อกได้เมื่อไม่ใช้งาน
 - 7.2. เก็บแยกออกจากอุปกรณ์ประมวลผลต่าง ๆ ได้แก่ เครื่องถ่ายเอกสาร เครื่องพิมพ์ เป็นต้น เพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิ์ในการเข้าถึงข้อมูลได้
8. กำหนดให้มีการจัดเก็บข้อมูลส่วนบุคคล โดยให้เก็บรวบรวมได้เท่าที่จำเป็นภายใต้อำนาจหน้าที่และวัตถุประสงค์อันชอบด้วยกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล
9. กำหนดให้มีมาตรการรักษาความปลอดภัยในการจัดเก็บข้อมูล รวมทั้งกรณีที่มีการเคลื่อนย้ายอุปกรณ์ที่จัดเก็บข้อมูล เพื่อป้องกันมิให้มีการเข้าถึงโดยไม่ได้รับอนุญาต หรือลักลอบนำข้อมูลไปใช้ที่ ก่อให้เกิดความเสียหายต่อหน่วยงาน
10. กำหนดให้มีมาตรการรักษาความปลอดภัยของการถ่ายโอนข้อมูลกับหน่วยงานภายนอกที่ผ่านช่องทางการสื่อสารทุกชนิด โดยต้องสอดคล้องตามนโยบายความมั่นคงปลอดภัยสารสนเทศ
11. ห้ามมิให้จัดเก็บข้อมูลส่วนตัวหรือข้อมูลที่ไม่เกี่ยวข้องกับการดำเนินงานของ สช. สำหรับการจัดเก็บข้อมูลถาวรบนเครื่องแม่ข่ายที่ สช. จัดสรรไว้

2.3 การใช้ข้อมูล

กระบวนการจัดเก็บข้อมูล เป็นการจัดเก็บข้อมูลที่เกิดจากกระบวนการสร้าง หรือข้อมูลที่ได้จากการ แลกเปลี่ยนกับหน่วยงานอื่น เพื่อให้มีระเบียบ ง่ายต่อการใช้งานไม่สูญหายหรือถูกทำลาย และให้ผู้ใช้งานสามารถประมวลผลข้อมูลต่าง ๆ ตามความต้องการได้อย่างรวดเร็ว ไม่ว่าจะจัดเก็บลงแฟ้มข้อมูล (File) หรือระบบการจัดการ ฐานข้อมูล (Database Management System – DBMS)

ตารางที่ 1. 3 การดำเนินการและผู้มีส่วนร่วม ในกระบวนการใช้ข้อมูล

กิจกรรม	เจ้าของข้อมูล	บริการข้อมูล	ผู้ดูแลระบบสารสนเทศ
กำหนดสิทธิ์ประมวลผลและเข้าใช้งานข้อมูลตามชั้นความลับ	X		
กำหนดสิทธิ์ในการประมวลผลและเข้าใช้งานข้อมูลให้แก่ผู้ใช้ข้อมูล			X
ทบทวนสิทธิ์การเข้าถึงและการใช้ข้อมูลของผู้ใช้งานอย่างน้อยปีละ 1 ครั้ง	X		

การดำเนินการ

1. เจ้าของข้อมูลจะต้องกำหนดผู้มีสิทธิ์เข้าถึงเพื่อประมวลผลและใช้ข้อมูลตามชั้นความลับ ดังนี้
 - 1.1. ข้อมูลที่มีชั้นความลับ กำหนดให้ผู้ใช้งานที่ได้รับสิทธิ์ตามตำแหน่ง/บทบาท เท่านั้น
 - 1.2. ข้อมูลใช้ภายใน กำหนดให้ผู้บริหาร เจ้าหน้าที่ ลูกจ้าง และเจ้าหน้าที่ของรัฐมาช่วยปฏิบัติงาน รวมถึงพนักงานจ้างเหมาบริการเท่านั้น ที่มีสิทธิ์เข้าถึงเพื่อประมวลผลและใช้งานข้อมูลได้ ทั้งนี้ ต้องปกป้อง ข้อมูลจากการเข้าถึงโดยบุคคลภายนอก
 - 1.3. ข้อมูลเปิดเผยได้ ไม่กำหนดสิทธิ์การเข้าถึงเพื่อประมวลผลและใช้งานข้อมูล
2. ผู้ดูแลระบบสารสนเทศจะต้องกำหนดสิทธิ์ในการเข้าถึงเพื่อประมวลผล และใช้ข้อมูลผู้ใช้งานตามที่เจ้าของข้อมูลกำหนด
3. เจ้าของข้อมูลจะต้องทบทวนสิทธิ์การเข้าถึงเพื่อประมวลผลและใช้ข้อมูลของผู้ใช้งานอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ ได้แก่ การลาออก เปลี่ยนตำแหน่ง โอนย้าย สิ้นสุดการจ้าง การ ปรับโครงสร้าง หรือเมื่อมีการปรับปรุงระบบสารสนเทศ
4. ผู้ที่มีสิทธิ์เข้าใช้งานข้อมูลที่มีชั้นความลับตามที่กำหนดโดยเจ้าของข้อมูลจะต้องใช้ข้อมูลอย่าง ระมัดระวัง โดยคำนึงถึงความปลอดภัยและต้องไม่ใช้งานข้อมูลที่มีชั้นความลับในพื้นที่สาธารณะ
5. ผู้ใช้ข้อมูลจะต้องไม่ใช้ข้อมูลในเครือข่ายของหน่วยงาน เพื่อประโยชน์ในเชิงธุรกิจเป็นการ ส่วนตัวหรือเพื่อเข้าสู่เว็บไซต์ที่ไม่เหมาะสม หรือใช้ข้อมูลอันก่อให้เกิดความเสียหายต่อ สช.

2.4 การเชื่อมโยงและการแลกเปลี่ยนข้อมูล

เพื่อกำหนดแนวปฏิบัติและมาตรฐานด้านเทคนิคในการเชื่อมโยงและการแลกเปลี่ยนข้อมูลดิจิทัลทั้ง ภายใน สช. และระหว่างหน่วยงานอย่างมีประสิทธิภาพ และก่อให้เกิดประโยชน์ต่อภาครัฐ ภาคเอกชน และประชาชน โดย เป็นการเชื่อมโยงและแลกเปลี่ยนข้อมูล ให้มีความมั่นคงปลอดภัย น่าเชื่อถือ และข้อมูลมีคุณภาพ สามารถนำไปใช้ ประโยชน์ได้อย่างมีประสิทธิภาพ

ตารางที่ 1. 4 การดำเนินการและผู้มีส่วนร่วม ในกระบวนการเชื่อมโยงและการแลกเปลี่ยนข้อมูล

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

การดำเนินการ

1. กำหนดให้เจ้าของข้อมูล หรือบริการข้อมูล จัดทำแนวทาง/กระบวนการ ในการเชื่อมโยงและ แลกเปลี่ยนข้อมูล โดยมีองค์ประกอบ ดังต่อไปนี้เป็นอย่างน้อย

- 1.1. วัตถุประสงค์ในการนำข้อมูลไปใช้งาน
- 1.2. ขอบเขตการนำข้อมูลไปใช้งาน
- 1.3. ช่วงเวลาและความถี่ในการเข้าถึงข้อมูลและการนำข้อมูลไปใช้
- 1.4. ชุดข้อมูล รายการข้อมูล ฟิลด์ข้อมูลที่สามารถเข้าถึง
- 1.5. กำหนดวิธีการ แนวทาง และรายละเอียดของการเชื่อมโยงและการแลกเปลี่ยนข้อมูลดิจิทัล

1.6. ในกรณีขอข้อมูลส่วนบุคคลเป็นรายคน ต้องจัดทำหนังสือแสดงความยินยอม เพื่อรับการยินยอมจากบุคคลนั้น ๆ หรือได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลดังกล่าวไว้ก่อน หน้านั้นแล้วตาม วัตถุประสงค์ในแต่ละกิจกรรมไว้อย่างชัดเจน ยกเว้นหน่วยงานที่ขอใช้ข้อมูลมีอำนาจตามกฎหมายโดยชอบธรรม

2. กำหนดให้เจ้าของข้อมูล หรือบริการข้อมูลตามที่ได้รับมอบหมายดำเนินการตรวจสอบ คำอธิบายชุดข้อมูลดิจิทัลหรือเมทาตาตาของข้อมูลที่จะทำการเชื่อมโยงและแลกเปลี่ยนให้ครบถ้วน ดังนี้

2.1. ตรวจสอบเมทาตาตาของชุดข้อมูลดิจิทัลที่จัดเก็บให้มีฟิลด์ข้อมูลครบถ้วนสอดคล้องกับความต้องการของหน่วยงานที่ขอใช้ หากไม่ครบถ้วนต้องจัดทำเพิ่มเติมตามความต้องการของหน่วยงานที่ขอใช้

2.2. ตรวจสอบชั้นความลับของข้อมูลว่าอยู่ในชั้นความลับที่สามารถเปิดเผยได้หรือไม่ โดยต้องไม่ขัดต่อกฎหมายระเบียบ ข้อบังคับ ความมั่นคงของประเทศ ความลับทางราชการ และความเป็นส่วนบุคคล พร้อมทั้งตรวจสอบสิทธิ์ของหน่วยงานที่สามารถนำข้อมูลไปใช้ได้ตามบทบาทและภารกิจตามกฎหมายของหน่วยงานนั้น ๆ หากไม่ครบถ้วนหรือไม่เป็นปัจจุบัน ให้แจ้งเจ้าของข้อมูลและบริการข้อมูลทำการจัดทำหรือปรับปรุงให้เป็นปัจจุบัน

3. กำหนดเทคโนโลยีและมาตรฐานทางเทคนิคที่ใช้ในการแลกเปลี่ยนข้อมูล

4. บริการข้อมูลร่วมกับผู้ดูแลระบบสารสนเทศ กำหนดให้มีมาตรการรักษาความมั่นคง ปลอดภัยเกี่ยวกับการเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัล เพื่อป้องกันมิให้มีการรับส่งข้อมูลที่ไม่สมบูรณ์ หรือส่ง ข้อมูลไปผิดที่หรือมีการรั่วไหลของข้อมูล หรือข้อมูลถูกแก้ไขเปลี่ยนแปลง ถูกทำซ้ำใหม่ ถูกส่งซ้ำโดยมิได้รับอนุญาต

5. กำหนดให้ผู้ดูแลระบบสารสนเทศต้องจัดเก็บบันทึกหลักฐานของการเชื่อมโยง และการแลกเปลี่ยนข้อมูลดิจิทัล (Log File) เพื่อให้สามารถตรวจสอบย้อนกลับได้

6. บริการข้อมูลร่วมกับผู้ดูแลระบบสารสนเทศ ทำสัญญาอนุญาตหรือข้อตกลงในการ แลกเปลี่ยนข้อมูลและการนำไปใช้

7. ห้ามมิให้เชื่อมโยงและแลกเปลี่ยนเพื่อส่งต่อข้อมูลที่เป็นการกระทำความผิดตามกฎหมายว่า ด้วยการกระทำความผิดทางคอมพิวเตอร์

2.5 การเผยแพร่และการเปิดเผยข้อมูลต่อสาธารณะ

เพื่อกำหนดแนวปฏิบัติและมาตรฐานการเผยแพร่และการเปิดเผยข้อมูลต่อสาธารณะโดยอิงจาก กฎหมาย กฎเกณฑ์และแนวปฏิบัติที่เกี่ยวข้อง ทั้งนี้ ข้อมูลที่เปิดเผยควรเป็นประโยชน์ สามารถนำไปประมวลผลและใช้ ต่อยอด ในการพัฒนาในรูปแบบต่าง ๆ ได้ โดยการเปิดเผยข้อมูลเป็นการนำข้อมูลที่อยู่ในครอบครองของ สช. เผยแพร่ ตามช่องทางต่าง ๆ อย่างเหมาะสม ทั้งการเปิดเผยตามนโยบายรัฐ และการแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน

ตารางที่ 1. 5 การดำเนินการและผู้มีส่วนร่วมในกระบวนการเปิดเผยข้อมูล

กิจกรรม	เจ้าของข้อมูล	บริการข้อมูล	ผู้ดูแลระบบสารสนเทศ
กำหนดช่องทางการเปิดเผยข้อมูลที่เข้าถึงและนำไปใช้ ง่าย	x	x	
คัดเลือกข้อมูลที่จะเปิดเผยในรูปแบบข้อมูลเปิด (Open Data)	x	x	

กิจกรรม	เจ้าของข้อมูล	บริการข้อมูล	ผู้ดูแลระบบสารสนเทศ
ตรวจสอบคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตาของชุดข้อมูลที่จะทำการเปิดเผย ให้มีความครบถ้วนเป็นปัจจุบัน	x	x	
กำหนดรอบระยะเวลาในการตรวจสอบและปรับปรุงข้อมูลที่เปิดเผย	x	x	

การดำเนินการ

1. เจ้าของข้อมูลร่วมกับบริการข้อมูล กำหนดช่องทางการเปิดเผยข้อมูลที่เข้าถึงและนำไปใช้งาน
2. กำหนดให้เจ้าของข้อมูลร่วมกับบริการข้อมูล คัดเลือกข้อมูลที่จะเปิดเผยในรูปแบบข้อมูลเปิด จากลำดับชั้นความสำคัญของชุดข้อมูล
3. เจ้าของข้อมูลร่วมกับบริการข้อมูล คัดเลือกข้อมูลที่จะเปิดเผยในรูปแบบข้อมูลเปิด (Open Data) ใน รูปแบบข้อมูลเปิดของ สช. โดยดำเนินการ ดังนี้
 - 3.1. กำหนดลักษณะของข้อมูลที่เผยแพร่กำหนดให้อยู่ในรูปแบบที่เครื่องสามารถประมวลผลได้
 - 3.2. กำหนดให้มีคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตา และพจนานุกรมข้อมูล (Data Dictionary) สำหรับข้อมูลที่ต้องเปิดเผยและสอดคล้องกับมาตรฐานตามที่หน่วยงานของรัฐได้กำหนดไว้
 - 3.3. ชุดข้อมูลและรายการชุดข้อมูลที่เผยแพร่จะต้องมีการจัดรูปแบบที่กำหนดเป็น มาตรฐานและกำหนดภายใต้หมวดหมู่เดียวกัน เพื่อให้ผู้ใช้ข้อมูลสามารถค้นหาและเข้าถึงข้อมูลได้ง่าย
 - 3.4. ข้อมูลที่เผยแพร่จะต้องมีการบันทึกเวลา (Timestamps) ที่ช่วยให้ผู้ใช้งานสามารถ ระบุได้ว่า ข้อมูลนั้นเป็นปัจจุบัน
4. สนับสนุนการเผยแพร่ข้อมูลผ่านช่องทางที่ง่ายต่อการเข้าถึงข้อมูล และต้องเปิดเผยข้อมูลใน รูปแบบดิจิทัลต่อสาธารณะที่ศูนย์กลางข้อมูลเปิดภาครัฐ (data.go.th) หรือระบบบัญชีภาครัฐ (gdcatalog.go.th) หรือ เว็บไซต์หลัก สช. หรือช่องทางที่หน่วยงานของรัฐได้กำหนดไว้ โดย
 - 4.1. กำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัยในการเปิดเผยข้อมูลอย่างเพียงพอและมีประสิทธิภาพ
 - 4.2. มีการตรวจสอบข้อมูลที่เผยแพร่จากหน่วยงานทั้งภายในและภายนอกหน่วยงาน เพื่อให้มั่นใจว่าหน่วยงานได้มีข้อมูลที่เผยแพร่ที่มีคุณค่า
 - 4.3. การเผยแพร่ข้อมูล ต้องมีการตรวจสอบรูปแบบข้อมูลที่เผยแพร่ให้สอดคล้องกับ มาตรฐานที่หน่วยงานกำหนด
 - 4.4. หากการเปิดเผยข้อมูลไม่ครบถ้วนหรือไม่เป็นปัจจุบัน ให้แจ้งเจ้าของข้อมูลและบริการ ข้อมูลทำการจัดทำหรือปรับปรุงให้เป็นปัจจุบัน
 - 4.5. ข้อมูลที่เผยแพร่ต้องไม่ขัดต่อกฎหมาย รวมถึงกฎหมายว่าด้วยทรัพย์สินทางปัญญา เว้นแต่การเปิดเผยข้อมูลจะเป็นไปตามอำนาจที่กฎหมายรับรอง

5. กำหนดให้เปิดเผยข้อมูลส่วนบุคคลตามข้อกำหนดของ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล หรือ ตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคล (สช.) เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติในการคุ้มครอง ข้อมูลส่วนบุคคลตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล

6. เจ้าของข้อมูลห้ามเปิดเผยข้อมูลความมั่นคงและข้อมูลความลับทางราชการที่อยู่ใน ความครอบครองของหน่วยงาน ยกเว้นได้รับการอนุมัติจาก สช. รวมทั้งห้ามเปิดเผยข้อมูลที่เป็นการกระทำความผิด ตามกฎหมาย นโยบาย และแนวปฏิบัติอันทำให้เกิดความเสียหายต่อหน่วยงาน เจ้าของข้อมูลร่วมกับบริการข้อมูล กำหนดกรอบระยะเวลาในการตรวจสอบและปรับปรุงข้อมูลที่เปิดเผยเพื่อให้ข้อมูลถูกต้อง และเป็นปัจจุบัน

2.6 การทำลายข้อมูล

เพื่อกำหนดแนวปฏิบัติการทำลายข้อมูล หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัว บุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ เพื่อเป็นการรักษาความมั่นคงปลอดภัยของข้อมูล

ตารางที่ 1. 6 การดำเนินการและผู้มีส่วนร่วมในกระบวนการทำลายข้อมูล

กิจกรรม	เจ้าของข้อมูล	บริการข้อมูล	ผู้ดูแลระบบสารสนเทศ	ผู้ทำลายข้อมูล
กำหนดผู้มีสิทธิ์ในการทำลายข้อมูล	X	X		
กำหนดสิทธิ์ในการทำลายข้อมูลให้แก่ผู้ทำลายข้อมูล			X	
ทำลายข้อมูลตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน				X
จัดเก็บคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาทาที่ทำลายสำหรับตรวจสอบในภายหลัง	X	X		
จัดเก็บบันทึกรายละเอียดการทำลายข้อมูลไว้ในทะเบียนควบคุมและบันทึกการทำลายข้อมูล โดยให้เก็บรักษาไว้เป็น หลักฐานไม่น้อยกว่า 1 ปี				X
ทำลายข้อมูลส่วนบุคคลเมื่อเจ้าของข้อมูลส่วนบุคคลร้องขอ หรือข้อมูลส่วนบุคคลที่พ้นระยะเวลาการเก็บรักษาตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล				X

การดำเนินการ

1. เจ้าของข้อมูลร่วมกับบริการข้อมูล กำหนดผู้มีสิทธิ์ในการทำลายข้อมูล หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ และจะต้องทบทวนสิทธิ์นี้อย่างน้อยปี ละ 1 ครั้ง หรือเมื่อมีการ

เปลี่ยนแปลงที่สำคัญ ได้แก่ การลาออก เปลี่ยนตำแหน่ง โอนย้าย สิ้นสุดการจ้าง การปรับโครงสร้าง หรือเมื่อมีการปรับปรุงระบบสารสนเทศ เป็นต้น

2. ผู้ดูแลระบบสารสนเทศจะต้องกำหนดสิทธิ์ในการทำลายข้อมูลให้แก่ผู้ทำลายข้อมูลตามที่ เจ้าของข้อมูลกำหนด
3. ผู้ทำลายข้อมูลต้องทำลายข้อมูลตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ สช.
4. กำหนดให้เจ้าของข้อมูลร่วมกับบริการข้อมูล จัดเก็บคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตา ที่ทำลาย สำหรับตรวจสอบในภายหลัง
5. กำหนดให้ผู้ทำลายข้อมูลจัดเก็บบันทึกรายละเอียดการทำลายข้อมูลไว้ในทะเบียนควบคุม และบันทึกการทำลายข้อมูล โดยให้เก็บรักษาไว้เป็นหลักฐานไม่น้อยกว่า 1 ปี
6. กำหนดให้ผู้ประมวลผลข้อมูลส่วนบุคคลทำลายข้อมูลส่วนบุคคลเมื่อเจ้าของข้อมูลส่วนบุคคล ร้องขอตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยจะต้องผ่านการเห็นชอบจากผู้ควบคุมข้อมูลส่วนบุคคล และ ดำเนินการตามข้อกำหนดที่ผู้ควบคุมข้อมูลส่วนบุคคลกำหนดไว้อย่างเคร่งครัด

3. บทบาทและหน้าที่ของเจ้าของข้อมูล (Data Owner)

เพื่อให้การดำเนินงานด้านธรรมาภิบาลข้อมูล และการบริหารจัดการข้อมูลตามวงจรชีวิตของข้อมูล (Data Life Cycle) ที่ได้กำหนดบทบาทหน้าที่ของเจ้าของข้อมูล (Data Owner) ในการบริหารจัดการข้อมูลที่อยู่ในความรับผิดชอบ เพื่อให้ได้ข้อมูลที่มีคุณภาพประกอบด้วย กระบวนการสร้างข้อมูล (Create) กระบวนการจัดเก็บข้อมูล (Store) กระบวนการใช้ข้อมูล (Use) กระบวนการเผยแพร่ข้อมูล (Publish) กระบวนการจัดเก็บข้อมูลถาวร (Archive) และ กระบวนการทำลายข้อมูล (Destroy) โดยบทบาทและหน้าที่ของเจ้าของข้อมูล ประกอบด้วย

1. เจ้าของข้อมูลเป็นผู้กำหนดผู้มีสิทธิ์ในการสร้างข้อมูล และจะต้องทบทวนสิทธิ์การเข้าถึงเพื่อ ประมวลผลและใช้ข้อมูลของผู้ใช้งานอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ ได้แก่ การลาออก เปลี่ยน ตำแหน่ง โอนย้าย สิ้นสุดการจ้าง การปรับโครงสร้าง หรือเมื่อมีการปรับปรุงระบบสารสนเทศ
2. กำหนดให้เจ้าของข้อมูลตรวจสอบความถูกต้องของข้อมูลที่ถูกสร้างขึ้น
3. เจ้าของข้อมูลเป็นผู้กำหนดชั้นความลับของข้อมูลที่ถูกสร้างขึ้นตามวิธีปฏิบัติการจำแนกชั้นความลับ ของข้อมูล
4. เจ้าของข้อมูลจะต้องกำหนดผู้มีสิทธิ์เข้าถึงเพื่อประมวลผลและใช้ข้อมูลตามชั้นความลับ ดังนี้
 - 4.1. ข้อมูลที่มีชั้นความลับ กำหนดให้ผู้ใช้งานที่ได้รับสิทธิ์ตามตำแหน่ง/บทบาท เท่านั้น
 - 4.2. ข้อมูลใช้ภายใน กำหนดให้ผู้บริหาร เจ้าหน้าที่ ลูกจ้าง และเจ้าหน้าที่ของรัฐมาช่วยปฏิบัติงาน รวมถึง พนักงานจ้างเหมาบริการเท่านั้น ที่มีสิทธิ์เข้าถึงเพื่อประมวลผลและใช้งานข้อมูลได้ ทั้งนี้ต้องปกป้องข้อมูล จาก การเข้าถึงโดยบุคคลภายนอก
 - 4.3. ข้อมูลเปิดเผยได้ ไม่กำหนดสิทธิ์การเข้าถึงเพื่อประมวลผลและใช้งานข้อมูล
5. เจ้าของข้อมูลจะต้องกำหนดระยะเวลาในการจัดเก็บข้อมูลที่ชัดเจน
6. กรณีข้อมูลที่จัดเก็บในรูปแบบเอกสาร ให้มีการจัดเก็บดังนี้
 - 6.1. เก็บในสถานที่เหมาะสม มีมาตรการป้องกันการเข้าถึงข้อมูล เช่น สามารถปิดล็อกได้เมื่อไม่ใช้งาน

6.2. เก็บแยกออกจากอุปกรณ์ประมวลผลต่าง ๆ ได้แก่ เครื่องถ่ายเอกสาร เครื่องพิมพ์ เป็นต้น เพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิ์ในการเข้าถึงข้อมูลได้

6.3. กำหนดให้มีการจัดเก็บข้อมูลส่วนบุคคลโดยให้เก็บรวบรวมได้เท่าที่จำเป็น ภายใต้อำนาจหน้าที่และวัตถุประสงค์อันชอบด้วยกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

6.4. กำหนดให้มีมาตรการรักษาความปลอดภัยในการจัดเก็บข้อมูล รวมทั้งกรณีที่มีการเคลื่อนย้าย อุปกรณ์ที่ จัดเก็บข้อมูล เพื่อป้องกันมิให้มีการเข้าถึงโดยมิได้รับอนุญาต หรือลักลอบนำข้อมูลไปใช้ที่ก่อให้เกิดความเสียหายต่อหน่วยงาน

7. เจ้าของข้อมูลร่วมกับบริการข้อมูล ร่วมจัดทำคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตา (Metadata) เมื่อ มีการสร้างชุดข้อมูล (Datasets) ตามมาตรฐานคำอธิบายชุดข้อมูลดิจิทัลที่ สข. กำหนดและสอดคล้องกับมาตรฐานที่ ภาครัฐได้กำหนดไว้

8. กำหนดให้เจ้าของข้อมูลหรือบริการข้อมูลตามที่ได้รับมอบหมายดำเนินการตรวจสอบคำอธิบายชุด ข้อมูลดิจิทัลหรือเมทาดาตาของข้อมูลที่จะทำการเชื่อมโยงและแลกเปลี่ยนให้ครบถ้วน ดังนี้

8.1. ตรวจสอบเมทาดาตาของชุดข้อมูลดิจิทัลที่จัดเก็บให้มีฟิลด์ข้อมูลครบถ้วนสอดคล้องกับความ ต้องการของหน่วยงานที่ขอใช้ หากไม่ครบถ้วนต้องจัดทำเพิ่มเติมตามความต้องการของหน่วยงานที่ขอใช้

8.2. ตรวจสอบชั้นความลับของข้อมูลว่าอยู่ในชั้นความลับที่สามารถเปิดเผยได้หรือไม่ โดยต้องไม่ ขัดต่อกฎหมายระเบียบ ข้อบังคับ ความมั่นคงของประเทศ ความลับทางราชการ และความเป็นส่วนบุคคล พร้อมทั้ง ตรวจสอบสิทธิ์ของหน่วยงานที่สามารถนำข้อมูลไปใช้ได้ตามบทบาทและภารกิจตามกฎหมาย ของหน่วยงานนั้น ๆ หาก ไม่ครบถ้วนหรือไม่เป็นปัจจุบัน ให้แจ้งเจ้าของข้อมูลและบริการข้อมูลทำการจัดทำหรือปรับปรุงให้เป็นปัจจุบัน

9. กำหนดให้เจ้าของข้อมูลหรือบริการข้อมูล จัดทำแนวทาง/กระบวนการ ในการเชื่อมโยงและแลกเปลี่ยน ข้อมูล โดยมีองค์ประกอบ ดังต่อไปนี้เป็นอย่างน้อย

9.1. วัตถุประสงค์ในการนำข้อมูลไปใช้งาน

9.2. ขอบเขตการนำข้อมูลไปใช้งาน

9.3. ช่วงเวลาและความถี่ในการเข้าถึงข้อมูลและการนำข้อมูลไปใช้

9.4. ชุดข้อมูล รายการข้อมูล ฟิลด์ข้อมูลที่สามารถเข้าถึง

9.5. กำหนดวิธีการ แนวทาง และรายละเอียดของการเชื่อมโยงและการแลกเปลี่ยนข้อมูลดิจิทัล

9.6. ในกรณีขอข้อมูลส่วนบุคคลเป็นรายคน ต้องจัดทำหนังสือแสดงความยินยอมเพื่อรับการ ยินยอมจากบุคคลนั้น ๆ หรือได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลดังกล่าวไว้ก่อนหน้านั้น แล้วตาม วัตถุประสงค์ในแต่ละกิจกรรมไว้อย่างชัดเจน ยกเว้นหน่วยงานที่ขอใช้ข้อมูลมีอำนาจตามกฎหมายโดยชอบธรรม

10. เจ้าของข้อมูลร่วมกับบริการข้อมูล กำหนดช่องทางการเปิดเผยข้อมูลที่เข้าถึงและนำไปใช้งาน

11. กำหนดให้เจ้าของข้อมูลร่วมกับบริการข้อมูล คัดเลือกข้อมูลที่จะเปิดเผยในรูปแบบข้อมูลเปิดจากลำดับ ชั้น ความสำคัญของชุดข้อมูล

12. เจ้าของข้อมูลร่วมกับบริการข้อมูล คัดเลือกข้อมูลที่จะเปิดเผยในรูปแบบข้อมูลเปิด (Open Data) ใน รูปแบบข้อมูลเปิดของ สข. โดยดำเนินการ ดังนี้

12.1. กำหนดลักษณะของข้อมูลที่เผยแพร่ กำหนดให้อยู่ในรูปแบบที่เครื่องสามารถประมวลผลได้

12.2. กำหนดให้มีคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาทา และพจนานุกรมข้อมูล (Data Dictionary) สำหรับข้อมูลที่ต้องเปิดเผย และสอดคล้องกับมาตรฐานตามที่หน่วยงานของรัฐได้กำหนดไว้

12.3. ชุดข้อมูลและรายการชุดข้อมูลที่เผยแพร่ จะต้องมีการจัดรูปแบบที่กำหนดเป็นมาตรฐาน และกำหนดภายใต้หมวดหมู่เดียวกัน เพื่อให้ผู้ใช้ข้อมูลสามารถค้นหาและเข้าถึงข้อมูลได้ง่าย

12.4. ข้อมูลที่เผยแพร่จะต้องมีการบันทึกเวลา (Timestamps) ที่ช่วยให้ผู้ใช้งานสามารถระบุได้ว่า ข้อมูลนั้นเป็นปัจจุบัน

13. สนับสนุนการเผยแพร่ข้อมูลผ่านช่องทางที่ง่ายต่อการเข้าถึงข้อมูล และต้องเปิดเผยข้อมูลในรูปแบบ ดิจิทัลต่อสาธารณะที่ศูนย์กลางข้อมูลเปิดภาครัฐ (data.go.th) หรือระบบบัญชีภาครัฐ (gdcatalog.go.th) หรือเว็บไซต์ หลัก สช. หรือช่องทางที่หน่วยงานของรัฐได้กำหนดไว้โดย

13.1. กำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัยในการเปิดเผยข้อมูลอย่างเพียงพอและมีประสิทธิภาพ

13.2. มีการตรวจสอบข้อมูลที่เผยแพร่จากหน่วยงานทั้งภายในและภายนอกหน่วยงาน เพื่อให้มั่นใจว่าหน่วยงานได้มีข้อมูลที่เผยแพร่ที่มีคุณค่า

13.3. การเผยแพร่ข้อมูล ต้องมีการตรวจสอบรูปแบบข้อมูลที่เผยแพร่ให้สอดคล้องกับมาตรฐานที่ หน่วยงานกำหนด

13.4. หากการเปิดเผยข้อมูลไม่ครบถ้วน หรือไม่ในปัจจุบัน ให้แจ้งเจ้าของข้อมูลและบริการข้อมูล ทำการจัดทำหรือปรับปรุงให้เป็นปัจจุบัน

13.5. ข้อมูลที่เผยแพร่ต้องไม่ขัดต่อกฎหมาย รวมถึงกฎหมายว่าด้วยทรัพย์สินทางปัญญา เว้นแต่การเปิดเผยข้อมูลจะเป็นไปตามอำนาจที่กฎหมายรับรอง

14. กำหนดให้เจ้าของข้อมูลร่วมกับบริการข้อมูล คัดเลือกข้อมูลที่จะเปิดเผยในรูปแบบข้อมูลเปิดจากลำดับ ชั้น ความสำคัญของชุดข้อมูล

15. กำหนดให้เปิดเผยข้อมูลส่วนบุคคลตามข้อกำหนดของ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล หรือตามคำสั่ง ที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคล (สช.) เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคล ตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล

16. เจ้าของข้อมูลห้ามเปิดเผยข้อมูลความมั่นคง และข้อมูลความลับทางราชการที่อยู่ในความ ครอบครองของหน่วยงาน ยกเว้นได้รับการอนุมัติจาก สช. รวมทั้งห้ามเปิดเผยข้อมูลที่เป็นการกระทำความผิดตาม กฎหมาย นโยบาย และแนวปฏิบัติอันทำให้เกิดความเสียหายต่อหน่วยงาน

17. เจ้าของข้อมูลร่วมกับบริการข้อมูล กำหนดกรอบระยะเวลาในการตรวจสอบและปรับปรุงข้อมูลที่เปิดเผย เพื่อให้ข้อมูลถูกต้องและเป็นปัจจุบัน

18. เจ้าของข้อมูลร่วมกับบริการข้อมูล กำหนดผู้มีสิทธิในการทำลายข้อมูล หรือทำให้ข้อมูลส่วนบุคคลเป็น ข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ และจะต้องทบทวนสิทธินี้อย่างน้อยปีละ 1 ครั้ง หรือ เมื่อมีการเปลี่ยนแปลงที่สำคัญ ได้แก่ การลาออก เปลี่ยนตำแหน่ง โอนย้าย ลีนสุดการจ้าง การปรับโครงสร้าง หรือเมื่อมี การปรับปรุงระบบสารสนเทศ เป็นต้น

19. กำหนดให้เจ้าของข้อมูลร่วมกับบริการข้อมูล จัดเก็บคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาทาที่ทำลาย สำหรับตรวจสอบในภายหลัง

20. เจ้าของข้อมูลร่วมกับบริการข้อมูล ทำการประเมินคุณค่าของชุดข้อมูลดิจิทัลตามแบบฟอร์มประเมิน คุณค่าชุดข้อมูลที่ สพร. หรือ สช. กำหนดและเผยแพร่เป็นข้อมูลเปิดของหน่วยงานต่อสาธารณะตามกฎหมายว่าด้วย ข้อมูลข่าวสารของราชการใน รูปแบบข้อมูลดิจิทัล

4. บทบาทและหน้าที่ของบริการข้อมูล (Data Steward)

เพื่อให้การดำเนินงานด้านธรรมาภิบาลข้อมูล และการบริหารจัดการข้อมูลตามวงจรชีวิตของข้อมูล (Data Life Cycle) ที่ได้กำหนดบทบาทหน้าที่ของเจ้าของข้อมูล (Data Owner) ในการบริหารจัดการข้อมูลที่อยู่ในความรับผิดชอบ เพื่อให้ได้ข้อมูล ที่มีคุณภาพประกอบด้วย กระบวนการสร้างข้อมูล (Create) กระบวนการจัดเก็บข้อมูล (Store) กระบวนการใช้ข้อมูล (Use) กระบวนการเผยแพร่ข้อมูล (Publish) กระบวนการจัดเก็บข้อมูลถาวร (Archive) และ กระบวนการทำลายข้อมูล (Destroy) โดยบทบาทและหน้าที่ของเจ้าของข้อมูล ประกอบด้วย

1. เจ้าของข้อมูลร่วมกับบริการข้อมูล ร่วมจัดทำคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตา (Metadata) เมื่อมีการสร้าง ชุดข้อมูล (Datasets) ตามมาตรฐานคำอธิบายชุดข้อมูลดิจิทัลที่ สช. กำหนด และสอดคล้องกับมาตรฐานที่ภาครัฐได้กำหนดไว้

2. กำหนดให้เจ้าของข้อมูล หรือบริการข้อมูลตามที่ได้รับมอบหมายดำเนินการตรวจสอบคำอธิบายชุดข้อมูลดิจิทัลหรือ เมทาดาตาของข้อมูลที่จะทำการเชื่อมโยงและแลกเปลี่ยนให้ครบถ้วน ดังนี้

2.1. ตรวจสอบเมทาดาตาของชุดข้อมูลดิจิทัลที่จัดเก็บให้มีฟิลด์ข้อมูลครบถ้วนสอดคล้องกับความต้องการของ หน่วยงานที่ขอใช้ หากไม่ครบถ้วนต้องจัดทำเพิ่มเติมตามความต้องการของหน่วยงานที่ขอใช้

2.2. ตรวจสอบชั้นความลับของข้อมูลว่าอยู่ในชั้นความลับที่สามารถเปิดเผยได้หรือไม่ โดยต้องไม่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ ความมั่นคงของประเทศ ความลับทางราชการ และความเป็นส่วนบุคคล พร้อมทั้งตรวจสอบสิทธิ์ของหน่วยงานที่ สามารถนำข้อมูลไปใช้ได้ตามบทบาทและภารกิจตามกฎหมาย ของหน่วยงานนั้น ๆ หาก ไม่ครบถ้วนหรือไม่เป็นปัจจุบัน ให้แจ้ง เจ้าของข้อมูลและบริการข้อมูลทำการจัดทำหรือปรับปรุงให้เป็นปัจจุบัน

3. กำหนดให้เจ้าของข้อมูลหรือบริการข้อมูล จัดทำแนวทาง/กระบวนการ ในการเชื่อมโยงและแลกเปลี่ยนข้อมูล โดยมี องค์ประกอบ ดังต่อไปนี้เป็นอย่างน้อย

3.1. วัตถุประสงค์ในการนำข้อมูลไปใช้งาน

3.2. ขอบเขตการนำข้อมูลไปใช้งาน

3.3. ช่วงเวลาและความถี่ในการเข้าถึงข้อมูลและการนำข้อมูลไปใช้

3.4. ชุดข้อมูล รายการข้อมูล ฟิลด์ข้อมูลที่สามารถเข้าถึง

3.5. กำหนดวิธีการ แนวทาง และรายละเอียดของการเชื่อมโยงและการแลกเปลี่ยนข้อมูลดิจิทัล

3.6. ในกรณีขอข้อมูลส่วนบุคคลเป็นรายคน ต้องจัดทำหนังสือแสดงความยินยอม เพื่อรับการยินยอมจากบุคคล นั้น ๆ หรือได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลดังกล่าวไว้ก่อนหน้านั้นแล้ว ตามวัตถุประสงค์ในแต่ละกิจกรรมไว้อย่าง ชัดเจน ยกเว้นหน่วยงานที่ขอใช้ข้อมูลมีอำนาจตามกฎหมายโดยชอบธรรม

4. เจ้าของข้อมูลร่วมกับบริการข้อมูล กำหนดช่องทางการเปิดเผยข้อมูลที่เข้าถึงและนำไปใช้งาน

5. กำหนดให้เจ้าของข้อมูลร่วมกับบริการข้อมูล คัดเลือกข้อมูลที่จะเปิดเผยในรูปแบบข้อมูลเปิดจากลำดับ ชั้น ความสำคัญของชุดข้อมูล

6. เจ้าของข้อมูลร่วมกับบริการข้อมูล คัดเลือกข้อมูลที่จะเปิดเผยในรูปแบบข้อมูลเปิด (Open Data) ในรูปแบบข้อมูลเปิดของ สช. โดยดำเนินการ ดังนี้

6.1. กำหนดลักษณะของข้อมูลที่เผยแพร่กำหนดให้อยู่ในรูปแบบที่เครื่องสามารถประมวลผลได้

6.2. กำหนดให้มีคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตา และพจนานุกรมข้อมูล (Data Dictionary) สำหรับข้อมูลที่ต้องเปิดเผย และสอดคล้องกับมาตรฐานตามที่หน่วยงานของรัฐได้กำหนดไว้

6.3. ชุดข้อมูลและรายการชุดข้อมูลที่เผยแพร่ จะต้องมีการจัดรูปแบบที่กำหนดเป็นมาตรฐาน และ กำหนดภายใต้หมวดหมู่เดียวกัน เพื่อให้ผู้ใช้ข้อมูลสามารถค้นหาและเข้าถึงข้อมูลได้ง่าย

6.4. ข้อมูลที่เผยแพร่จะต้องมีการบันทึกเวลา (Timestamps) ที่ช่วยให้ผู้ใช้งานสามารถระบุได้ว่า ข้อมูลนั้นเป็นปัจจุบัน

7. สนับสนุนการเผยแพร่ข้อมูลผ่านช่องทางที่ง่ายต่อการเข้าถึงข้อมูล และต้องเปิดเผยข้อมูลในรูปแบบดิจิทัลต่อสาธารณะที่ศูนย์กลางข้อมูลเปิดภาครัฐ (data.go.th) หรือระบบบัญชีภาครัฐ (gdcatalog.go.th) หรือเว็บไซต์ หลัก สช. หรือช่องทางที่หน่วยงานของรัฐได้กำหนดไว้ โดย

7.1. กำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัยในการเปิดเผยข้อมูลอย่างเพียงพอและมีประสิทธิภาพ

7.2. มีการตรวจสอบข้อมูลที่เผยแพร่จากหน่วยงานทั้งภายในและภายนอกหน่วยงาน เพื่อให้มั่นใจว่าหน่วยงาน ได้มีข้อมูลที่เผยแพร่ที่มีคุณค่า

7.3. การเผยแพร่ข้อมูล ต้องมีการตรวจสอบรูปแบบข้อมูลที่เผยแพร่ให้สอดคล้องกับมาตรฐานที่หน่วยงานกำหนด

7.4. หากการเปิดเผยข้อมูลไม่ครบถ้วนหรือไม่เป็นปัจจุบัน ให้แจ้งเจ้าของข้อมูลและบริการข้อมูล ทำการจัดทำหรือปรับปรุงให้เป็นปัจจุบัน

7.5. ข้อมูลที่เผยแพร่ต้องไม่ขัดต่อกฎหมาย รวมถึงกฎหมายว่าด้วยทรัพย์สินทางปัญญา เว้นแต่การเปิดเผยข้อมูลจะเป็นไปตามอำนาจที่กฎหมายรับรอง

8. กำหนดให้เปิดเผยข้อมูลส่วนบุคคลตามข้อกำหนดของ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล หรือตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคล (สช.) เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคล ตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล

9. เจ้าของข้อมูลร่วมกับบริการข้อมูล กำหนดระยะเวลาในการตรวจสอบและปรับปรุงข้อมูลที่เปิดเผย เพื่อให้ข้อมูลถูกต้อง และเป็นปัจจุบัน

10. บริการข้อมูลร่วมกับผู้ดูแลระบบสารสนเทศ กำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัยเกี่ยวกับการเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัล เพื่อป้องกันมิให้มีการรับส่งข้อมูลที่ไม่สมบูรณ์ หรือส่งข้อมูลไปผิดที่ หรือมีการรั่วไหลของข้อมูล หรือข้อมูลถูกแก้ไขเปลี่ยนแปลง ถูกทำซ้ำใหม่ ถูกส่งซ้ำโดยมิได้รับอนุญาต

11. บริการข้อมูลร่วมกับผู้ดูแลระบบสารสนเทศ ทำสัญญาอนุญาตหรือข้อตกลงในการแลกเปลี่ยนข้อมูล และการนำไปใช้

12. เจ้าของข้อมูลร่วมกับบริการข้อมูล กำหนดผู้มีสิทธิ์ในการทำลายข้อมูล หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ และจะต้องทบทวนสิทธิ์นั้นอย่างน้อยปีละ 1 ครั้ง หรือ เมื่อมีการเปลี่ยนแปลงที่สำคัญ ได้แก่ การลาออก เปลี่ยนตำแหน่ง โอนย้าย สิ้นสุดการจ้าง การปรับโครงสร้าง หรือเมื่อมีการปรับปรุงระบบสารสนเทศ เป็นต้น

13. กำหนดให้เจ้าของข้อมูลร่วมกับบริการข้อมูล จัดเก็บคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตาที่ทำลาย สำหรับตรวจสอบในภายหลัง

14. เจ้าของข้อมูลร่วมกับบริการข้อมูล ทำการประเมินคุณค่าของชุดข้อมูลดิจิทัลตามแบบฟอร์มประเมิน คุณค่าชุด ข้อมูลที่ สพร. หรือ สช. กำหนด และเผยแพร่เป็นข้อมูลเปิดของหน่วยงานต่อสาธารณะตามกฎหมายว่าด้วย ข้อมูลข่าวสารของราชการในรูปแบบข้อมูลดิจิทัล

5. บทบาทและหน้าที่ของผู้ดูแลระบบสารสนเทศ (Technical Stewards)

เพื่อให้การดำเนินงานด้านธรรมาภิบาลข้อมูล และการบริหารจัดการข้อมูลตามวงจรชีวิตของข้อมูล (Data Life Cycle) ที่ได้กำหนดบทบาทหน้าที่ของผู้ดูแลระบบสารสนเทศ (Technical Stewards) ในการบริหารจัดการ ข้อมูลที่อยู่ใน ความรับผิดชอบ เพื่อให้ได้ข้อมูลที่มีคุณภาพ ประกอบด้วย กระบวนการสร้างข้อมูล (Create) กระบวนการจัดเก็บข้อมูล (Store) กระบวนการใช้ข้อมูล (Use) กระบวนการเผยแพร่ข้อมูล (Publish) กระบวนการ จัดเก็บข้อมูลถาวร (Archive) และ กระบวนการทำลายข้อมูล (Destroy) โดยบทบาทและหน้าที่ของผู้ดูแลระบบ สารสนเทศ

1. ผู้ดูแลระบบสารสนเทศจะต้องกำหนดสิทธิ์ในการสร้างข้อมูลให้แก่ผู้สร้างข้อมูลตามที่เจ้าของข้อมูลกำหนด
2. ผู้ดูแลระบบสารสนเทศจะต้องกำหนดสิทธิ์ในการเข้าถึง เพื่อประมวลผลและใช้ข้อมูลผู้ใช้งานตามที่เจ้าของข้อมูลกำหนด
3. ผู้ดูแลระบบสารสนเทศจะต้องกำหนดสิทธิ์ในการทำลายข้อมูลให้แก่ผู้ทำลายข้อมูลตามที่เจ้าของข้อมูลกำหนด
4. บริการข้อมูลและผู้ดูแลระบบสารสนเทศทำการย้ายข้อมูลที่มีการจัดเก็บเกินระยะเวลาที่กำหนดแล้ว เพื่อจัดเก็บเป็นข้อมูลถาวร
5. การจัดเก็บข้อมูลที่มีชั้นความลับให้ทำการเข้ารหัสข้อมูล เพื่อป้องกันการเข้าถึงหรือแก้ไขข้อมูลโดยไม่ได้รับอนุญาต
6. กำหนดให้ผู้ดูแลระบบสารสนเทศต้องจัดเก็บบันทึกหลักฐานของการเชื่อมโยง และการแลกเปลี่ยนข้อมูลดิจิทัล (Log File) เพื่อให้สามารถตรวจสอบย้อนกลับได้
7. กำหนดให้มีการจัดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่า 90 วัน นับแต่วันที่ข้อมูลเข้าสู่ระบบคอมพิวเตอร์ เพื่อให้สามารถระบุตัวผู้ใช้บริการนับแต่เริ่มใช้บริการ ให้สอดคล้องตามกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ ซึ่งประกอบด้วยข้อมูลอินเทอร์เน็ตที่เกิดจากการเข้าถึงระบบเครือข่าย และข้อมูล อินเทอร์เน็ตบนเครื่องผู้ให้บริการจดหมายอิเล็กทรอนิกส์ (e-mail Servers)

8. กำหนดให้การจัดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ให้สอดคล้องตามกฎหมายว่าด้วยการกระทำ ความผิดทางคอมพิวเตอร์ ผู้ให้บริการจะต้องใช้วิธีการที่มั่นคงปลอดภัยอย่างน้อย ดังนี้

8.1. เก็บในสื่อ (Media) ที่สามารถรักษาความครบถ้วน ถูกต้องแท้จริง (Integrity) และระบุตัวตน (Identification) ที่เข้าถึงสื่อดังกล่าวได้

8.2. มีระบบการเก็บรักษาความลับของข้อมูลที่จัดเก็บ และกำหนดชั้นความลับในการเข้าถึงข้อมูลดังกล่าว เพื่อรักษาความน่าเชื่อถือของข้อมูล และไม่อนุญาตให้ผู้ดูแลระบบสามารถแก้ไขข้อมูลที่เก็บรักษาไว้

8.3. การจัดเก็บข้อมูลต้องสามารถระบุรายละเอียดผู้ใช้งานเป็นรายบุคคลได้ (Identification and Authentication)

9. กำหนดให้มีมาตรการรักษาความปลอดภัยของการถ่ายโอนข้อมูลกับหน่วยงานภายนอกที่ผ่านช่องทางการสื่อสารทุกชนิด โดยต้องสอดคล้องตามนโยบายความมั่นคงปลอดภัยสารสนเทศ

10. กำหนดเทคโนโลยีและมาตรฐานทางเทคนิคที่ใช้ในการแลกเปลี่ยนข้อมูล

11. บริการข้อมูลร่วมกับผู้ดูแลระบบสารสนเทศ กำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัย เกี่ยวกับการเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัล เพื่อป้องกันมิให้มีการรับส่งข้อมูลที่ไม่สมบูรณ์ หรือส่งข้อมูลไปผิดที่ หรือมีการรั่วไหลของข้อมูล หรือข้อมูลถูกแก้ไขเปลี่ยนแปลง ถูกทำซ้ำใหม่ ถูกส่งซ้ำโดยมิได้รับอนุญาต

12. บริการข้อมูลร่วมกับผู้ดูแลระบบสารสนเทศ ทำสัญญาอนุญาตหรือข้อตกลงในการแลกเปลี่ยนข้อมูล และการนำไปใช้

6. เกณฑ์การประเมินคุณภาพข้อมูล ให้ดำเนินการตามมิติคุณภาพข้อมูล 5 มิติ ได้แก่

1. ความถูกต้อง
2. ความสอดคล้องกัน
3. ตรงตามความต้องการของผู้ใช้
4. ความเป็นปัจจุบัน
5. ความพร้อมใช้ที่สอดคล้องตามองค์ประกอบในการประเมินคุณภาพข้อมูลตามกรอบธรรมาภิบาลข้อมูลภาครัฐโดยแต่ละมิติ มีรายละเอียดและตัวชี้วัด (Indicators) ดังนี้

มิติคุณภาพข้อมูล	รายละเอียด	รายการตัวชี้วัด
<p>ความถูกต้องและสมบูรณ์</p> <p>Accuracy and Completeness</p>	<p>ประเมินเรื่องความถูกต้อง แม่นยำ แหล่งข้อมูลที่น่าเชื่อถือ และมีกระบวนการตรวจสอบ</p>	<ul style="list-style-type: none"> - มีแหล่งข้อมูลที่น่าเชื่อถือ - มีกระบวนการหรือเครื่องมือตรวจสอบจุดผิดพลาด บกพร่อง - มีการตรวจสอบความครบถ้วนของข้อมูล - มีวิธีเก็บข้อมูลมีความเป็นกลาง น่าเชื่อถือและไม่สร้างข้อมูลที่มีอคติ - มีการระบุค่านิยามและลักษณะข้อมูลที่ต้องการ
<p>ความสอดคล้องกัน</p> <p>(Consistency)</p>	<p>ประเมินเรื่องรูปแบบ ของข้อมูล ความสอดคล้องกัน และมาตรฐานในการจัดทำข้อมูลของหน่วยงาน</p>	<ul style="list-style-type: none"> - มีการเก็บข้อมูลได้มาตรฐานข้อมูลเดียวกัน หรือมาตรฐานข้อมูลที่สอดคล้องกัน - มีการตรวจสอบรูปแบบข้อมูลภายในชุดข้อมูลเดียวกัน - ข้อมูลมีความเชื่อมโยงและไม่ขัดแย้งกัน - มีการใช้กฎ วิธีการตรวจวัดที่สอดคล้องกันทั้งหน่วยงาน รวมถึงหน่วยงานภายนอก - มีการกำหนดบทบาทและผู้รับผิดชอบข้อมูล
<p>ตรงตามความต้องการของผู้ใช้ (Relevancy)</p>	<p>ประเมินว่า เป็นข้อมูลที่ใช้ของผู้ใช้ ต้องการ หรือเป็นข้อมูลที่จำเป็นต่อทราบ มีความละเอียดเพียงพอต่อนำไปใช้งาน</p>	<ul style="list-style-type: none"> - ข้อมูลตรงตามความต้องการ และวัตถุประสงค์ของการใช้งาน - มีการปรับปรุงคุณภาพให้ตรงตามความต้องการของผู้ใช้
<p>ความเป็นปัจจุบัน</p> <p>(Timeliness)</p>	<p>ประเมินเรื่องการเผยแพร่ข้อมูล การปรับปรุงข้อมูลและแผนเรื่องระยะเวลา</p>	<ul style="list-style-type: none"> - ข้อมูลมีการเผยแพร่ ส่งต่อตรงเวลา - ข้อมูลมีความเป็นปัจจุบัน ข้อมูลมีการเผยแพร่ข้อมูลในเวลาที่เหมาะสม
<p>ความพร้อมใช้</p> <p>(Availability)</p>	<p>ประเมินความพร้อมใช้ของข้อมูล รวมถึงไปถึงช่องทางในการขอ หรือ ใช้ข้อมูล</p>	<ul style="list-style-type: none"> - ข้อมูลถูกจัดในรูปแบบที่พร้อมนำไปใช้งาน และเหมาะกับผู้ใช้งาน - มีการเผยแพร่ข้อมูลที่เหมาะสม และสามารถเข้าถึงได้ โดยผู้ใช้สามารถเข้าถึงข้อมูลได้สะดวกตามสิทธิที่เหมาะสม - ข้อมูลสามารถอ่านด้วยโปรแกรมคอมพิวเตอร์ได้ - มีคำอธิบายข้อมูลที่ชัดเจน

7. หมวดหมู่ของข้อมูล (Data Category)



รูปที่ 1. 2 หมวดหมู่ของข้อมูล

ข้อมูลแบ่งออกได้เป็น 5 หมวดหมู่ ดังนี้

1. ข้อมูลสาธารณะ (Public Data) หมายความว่า ข้อมูลที่สามารถเปิดเผยได้ สามารถนำไปใช้ได้อย่างอิสระ ไม่ว่าจะเป็นข้อมูลข่าวสาร ข้อมูลส่วนบุคคล ข้อมูลอิเล็กทรอนิกส์ เป็นต้น
2. ข้อมูลใช้ภายใน (Internal Use Only) หมายความว่า ข้อมูลสำหรับการดำเนินการภายในของหน่วยงานซึ่งไม่อนุญาตให้นำไปใช้งานภายนอกก่อนได้รับอนุญาต เช่น นโยบาย มาตรฐาน และขั้นตอนการปฏิบัติงาน ประกาศ และบันทึกภายในหน่วยงาน เป็นต้น
3. ข้อมูลส่วนบุคคล คือ ข้อมูลเกี่ยวกับสิ่งเฉพาะตัวของบุคคลที่ทำให้สามารถระบุตัวหรือรู้ตัวของบุคคลนั้น ๆ ได้ ไม่ว่าจะเป็นข้อมูลการศึกษา ประวัติสุขภาพ ลายพิมพ์นิ้วมือ เป็นต้น
4. ข้อมูลความลับทางราชการ คือ ข้อมูลที่อยู่ในความครอบครองหรือควบคุมดูแลของหน่วยงานของรัฐที่มีคำสั่งไม่ให้มีการเปิดเผย และมีการกำหนดชั้นความลับของข้อมูล
5. ข้อมูลความมั่นคง คือ ข้อมูลเกี่ยวกับความมั่นคงของรัฐที่ทำให้เกิดความสงบเรียบร้อย การมีเสถียรภาพความเป็นปึกแผ่น ปลอดภัยจากภัยคุกคาม เป็นต้น

8. การจัดทำบัญชีข้อมูล

การจัดทำบัญชีข้อมูลประกอบด้วยรายละเอียด ดังนี้

1. เจ้าของข้อมูลหรือผู้ครอบครองข้อมูลมีหน้าที่กำหนดให้มีผู้รับผิดชอบที่เกี่ยวข้องกับข้อมูลหน่วยงาน
2. ผู้รับผิดชอบที่เกี่ยวข้องกับข้อมูล มีหน้าที่กำหนดคำนิยามของชุดข้อมูล (List of Data) ดังนี้
 - 2.1 ความสัมพันธ์ของข้อมูล
 - 2.2 ชนิดข้อมูล (Reference/Master Data Definition) แบ่งเป็น

2.2.1 Reference Data หรือ ข้อมูลที่มีลักษณะและโครงสร้างที่เป็นความจริงและถูกต้อง ทำให้ข้อมูลไม่ค่อยเปลี่ยนแปลง ส่งผลให้ข้อมูล Reference Data ถูกเผยแพร่ไปยังแหล่งต่าง ๆ เพื่ออ้างอิงอยู่เสมอ

2.2.1 Master Data หรือ ข้อมูลที่มีโอกาสเปลี่ยนแปลงได้มากกว่า มีรายละเอียดหรือจำนวนฟิลด์ ข้อมูลที่มากกว่า Reference Data และใช้เป็นข้อมูลในการดำเนินงานภายในหน่วยงาน

2.3 ขอบเขตที่ดำเนินการ

2.4 ชุดข้อมูลที่คาดว่าจะเกี่ยวข้อง

2.5 กระบวนการหลักหรืองานหลักที่ได้รับมอบหมาย และกระบวนการย่อย

2.6 ชุดข้อมูลที่เกี่ยวข้องกับกระบวนการย่อย แบ่งเป็น ชุดข้อมูลที่มีอยู่แล้ว และชุดข้อมูล

2.7 รูปแบบของการเก็บข้อมูล

2.8 ความพร้อมของชุดข้อมูล

2.9 การเชื่อมโยงและแลกเปลี่ยนข้อมูลภายในหน่วยงาน

3. ผู้รับผิดชอบที่เกี่ยวข้องกับข้อมูล มีหน้าที่กำหนดพจนานุกรมข้อมูล (Data Dictionary) ดังนี้

3.1 เลขที่เมทาดาทา (Metadata ID)

3.2 ชื่อชุดข้อมูล (Dataset Name)

3.3 เลขที่ข้อมูล (Data ID)

3.4 ชื่อตารางข้อมูล (Table Name)

3.5 ชื่อฟิลด์ข้อมูล (Field)

3.6 คำอธิบายฟิลด์ (Description)

3.7 ระดับชั้นความลับ (Classification)

3.8 ประเภทข้อมูล (Data Type)

3.9 ขนาดข้อมูล (Data Size)

3.10 คุณลักษณะข้อมูล (Characteristic Type)

3.11 แหล่งที่มาของค่าที่ระบุในฟิลด์ (Data Source)

3.12 รูปแบบ (Data Format)

3.13 เงื่อนไข (Condition)