สพร./PRD

พฤษภาคม 2569

มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัลอยู่ระหว่างการจัดทำ
ห้ามใช้หรือยึดร่างนี้เป็นมาตรฐาน

มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัลฉบับสมบูรณ์จะมีประกาศโดย
สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

ร่าง

มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

DGA Community Standard

ว่าด้วยแนวทางการแบ่งปันข้อมูลภาครัฐ

สำหรับเวียนขอข้อคิดเห็นจากหน่วยงานต่างๆ ที่เกี่ยวข้อง

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
เลขที่ 999 ชั้น 4 สถาบันเพื่อการยุติธรรมแห่งประเทศไทย
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210
หมายเลขโทรศัพท์: (+66) 0 2612 6000 โทรสาร: (+66) 0 2612 601

มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

DGA Community Standard

มสพร. x-xxxx

DGA x-xxxx

ว่าด้วยแนวทางการแบ่งปันข้อมูลภาครัฐ

เวอร์ชัน 1.0

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

สำนักนายกรัฐมนตรี

มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

ว่าด้วยแนวทางการแบ่งปันข้อมูลภาครัฐ

มสพร. X-XXXX

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
เลขที่ 999 ชั้น 4 สถาบันเพื่อการยุติธรรมแห่งประเทศไทย
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210
หมายเลขโทรศัพท์: (+66) 0 2612 6000 โทรสาร: (+66) 0 2612 601

ประกาศโดย
สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
สำนักนายกรัฐมนตรี
วันที่ ระบุวันที่ประกาศ

คณะกรรมการจัดทำร่างมาตรฐาน ข้อกำหนด และหลักเกณฑ์ ภายใต้พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562

ที่ปรึกษา

นางไอรดา เหลืองวิไล	รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล รักษาการแทนผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

ประธานกรรมการ

ผู้ช่วยศาสตราจารย์ณัฐวุฒิ หนูไพโรจน์	จุฬาลงกรณ์มหาวิทยาลัย

รองประธานกรรมการ

นายอาศิส อัญญะโพธิ์	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

กรรมการ

นายมารุต บูรณรัช	ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
นางสาวขนิษฐ์ ผาทอง	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
นายชลอ อินทพันธุ์	สำนักบริหารการทะเบียน กรมการปกครอง
นางสาวดารารัตน์ โฆษิตพิพัฒน์	สำนักงานคณะกรรมการพัฒนาระบบราชการ
นางสาวพรพิมล อุ่นไพร	สำนักงานคณะกรรมการกฤษฎีกา
นายสันติ สิทธิเลิศพิศาล	สำนักงานมาตรฐานผลิตภัณฑ์อุตสาหกรรม
นายวีระ วีระกุล	สภาดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ
รองศาสตราจารย์เกริก ภิรมย์โสภา	ประธานคณะทำงานเทคนิคด้านมาตรฐานกระบวนการและการดำเนินงานทางดิจิทัล
ศาสตราจารย์ธีรณี อจลากุล	ประธานคณะทำงานเทคนิคด้านมาตรฐานการบริหารจัดการข้อมูลภาครัฐ
ผู้ช่วยศาสตราจารย์มารอง ผดุงสิทธิ์	ประธานคณะทำงานเทคนิคด้านมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ

กรรมการและเลขานุการ

นางสาวอุรัชฎา เกตุพรหม	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

คณะทำงานเทคนิคด้านมาตรฐานการบริหารจัดการข้อมูลภาครัฐ

ที่ปรึกษา

นางไอรดา เหลืองวิไล	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ผู้ช่วยศาสตราจารย์ณัฐวุฒิ หนูไพโรจน์	จุฬาลงกรณ์มหาวิทยาลัย
นายอาศิส อัญญะโพธิ์	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ผู้ช่วยศาสตราจารย์ฐิติรัตน์ ทิพย์สัมฤทธิ์กุล	มหาวิทยาลัยธรรมศาสตร์

ประธานคณะทำงาน

ศาสตราจารย์ธีรณี อจลากุล	ผู้อำนวยการสถาบันข้อมูลขนาดใหญ่

รองประธานคณะทำงาน

ผู้ช่วยศาสตราจารย์โษฑศ์รัตต ธรรมบุษดี	มหาวิทยาลัยมหิดล

คณะทำงาน

นายโสภณ เอี่ยมศิริถาวร	กระทรวงสาธารณสุข
นายวันประชา เชาวลิตวงศ์	ธนาคารแห่งประเทศไทย
นายมารุต บูรณรัช	ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
นางสาวปริสุทธิ์ จิตต์ภักดี	สถาบันข้อมูลขนาดใหญ่ (องค์การมหาชน)
นายอธิพงศ์ สุวรรณรัตน์	สำนักข่าวกรองแห่งชาติ
นายอภิสิทธิ์ สุขสาคร	สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์
นางสาวปศิญา เชื้อดี	สำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ
นายสุวรรณโชติ ศิริมหาศาล	สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
นางสาวดารารัตน์ โฆษิตพิพัฒน์	สำนักงานคณะกรรมการพัฒนาระบบราชการ
นางสาวอัญญดา เพ็ญพร	สำนักงานเศรษฐกิจการเกษตร
นางกาญจนา ภู่มาลี	สำนักงานสถิติแห่งชาติ
นางสาวณัฐชยา ภาสสัทธา	สำนักงานสภาความมั่นคงแห่งชาติ
นายกฤษดา มาลีวงศ์	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
นายวริทธิ์ อยู่สบาย	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

คณะทำงานและเลขานุการ

นางสาวอุรัชฎา เกตุพรหม	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

ผู้ช่วยเลขานุการ

นางสาวสุภัทรา เรืองวานิช	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

วิเคราะห์และจัดทำมาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ว่าด้วยแนวทางการแบ่งปันข้อมูลภาครัฐ

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

นางสาวสุภัทรา เรืองวานิช สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

นางสาวศุภมาส พงษ์ภาคิน สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

นายธนัชกฤศ เรืองฉวี สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

(ร่าง) มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ว่าด้วยแนวทางการแบ่งปันข้อมูลภาครัฐ จัดทำขึ้นเพื่อเป็นข้อเสนอแนะ และเป็นแนวทางในการพิจารณาประเด็นต่างๆ ก่อนดำเนินการแบ่งปันข้อมูล โดยได้ประยุกต์หลักการสากลด้านการบริหารจัดการความเสี่ยง เพื่อสร้างความสมดุลระหว่างผลประโยชน์สาธารณะและความปลอดภัยของข้อมูล

โดยมาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ว่าด้วยแนวทางการแบ่งปันข้อมูลภาครัฐ ฉบับนี้ได้จัดทำตามมาตรฐานและแนวทาง

1 Australian Government, Best Practice Guide to Applying Data Sharing Principles

2 Tanvi D. , Felix R. , and Richard W. (2016). Five Safes: Designing data access for research. Bristol, England, UK: University of the West of England, Bristol Series: Economics Working Paper Series (1601)

3 United Nations Office for the Coordination of Humanitarian Affairs. (2017). Framework for data sharing in practice: Part I. Affairs, United Nations Office for the Coordination of Humanitarian.

และได้มีการจัดงานประชาพิจารณ์เพื่อเปิดรับฟังความคิดเห็นเป็นการทั่วไป และนำข้อมูล ข้อสังเกต ข้อคิดเห็นจากผู้ทรงคุณวุฒิและจากหน่วยงานที่เกี่ยวข้อง เพื่อให้ข้อเสนอแนะเกี่ยวกับมาตรฐานฉบับนี้มีความสมบูรณ์ครบถ้วน และสามารถนำไปปรับใช้ในทางปฏิบัติได้อย่างมีประสิทธิภาพ

มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ว่าด้วยแนวทางการแบ่งปันข้อมูลภาครัฐฉบับนี้จัดทำโดยฝ่ายมาตรฐานดิจิทัลภาครัฐ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) สำนักนายกรัฐมนตรี

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
เลขที่ 999 ชั้น 4 สถาบันเพื่อการยุติธรรมแห่งประเทศไทย
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210
หมายเลขโทรศัพท์: (+66) 0 2612 6000 โทรสาร: (+66) 0 2612 601
E-mail: sd-g2_division@dga.or.th
Website: www.dga.or.th

คำนำ

แผนพัฒนารัฐบาลดิจิทัล พ.ศ. 2566–2570 ได้กำหนดทิศทางสำคัญเพื่อยกระดับภาครัฐให้คล่องตัว โปร่งใส และมีประชาชนเป็นศูนย์กลาง โดยการบูรณาการข้อมูลระหว่างหน่วยงานถือเป็นหัวใจของการก้าวสู่รัฐบาลที่ขับเคลื่อนด้วยข้อมูล (Data-Driven Government) ซึ่งช่วยลดความซ้ำซ้อนและยกระดับคุณภาพการให้บริการภาครัฐ ประกอบกับพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 ได้กำหนดหน้าที่สำคัญของหน่วยงานรัฐไว้อย่างชัดเจน ในมาตรา 13 ซึ่งบังคับให้หน่วยงานต้องเชื่อมโยงและแลกเปลี่ยนข้อมูลเพื่อประโยชน์ในการบริหารราชการ และมาตรา 14 ที่ได้มีการกำหนดให้มีการคุ้มครองข้อมูลอย่างรัดกุม โดยการใช้ข้อมูลต้องมีการคุ้มครองข้อมูลให้มีความปลอดภัย ซึ่งเป็นกลไกในการสร้างความสมดุลระหว่างการใช้ประโยชน์และการคุ้มครองข้อมูล

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) หรือ สพร. มีบทบาทหลักในการสนับสนุนให้หน่วยงานรัฐสามารถปฏิบัติแบ่งปันข้อมูลระหว่างหน่วยงานได้ จึงได้จัดทำ (ร่าง) มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล ว่าด้วยแนวทางการแบ่งปันข้อมูลภาครัฐ เพื่อเป็นข้อเสนอแนะและเป็นแนวทางในการพิจารณาประเด็นต่างๆ ก่อนดำเนินการแบ่งปันข้อมูล โดยได้ประยุกต์หลักการสากลด้านการบริหารจัดการความเสี่ยงเพื่อสร้างความสมดุลระหว่างผลประโยชน์สาธารณะและความปลอดภัยของข้อมูล โดยข้อเสนอแนะนี้จะช่วยสร้างความมั่นใจให้แก่หน่วยงานในการแบ่งปันข้อมูลอย่างถูกต้องภายใต้หลักธรรมาภิบาลข้อมูล และผลักดันให้การเปลี่ยนผ่านสู่รัฐบาลดิจิทัลเป็นไปอย่างเป็นรูปธรรมและเกิดประโยชน์สูงสุดแก่ประชาชน

สารบัญ

สารบัญตาราง

สารบัญภาพ

มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ว่าด้วยแนวทางการแบ่งปันข้อมูลภาครัฐ

1. บทนำ

1.1. หลักการและความจำเป็น

มาตรฐานการแบ่งปันข้อมูลภาครัฐนี้มุ่งยกระดับการบริหารราชการตามแผนพัฒนารัฐบาลดิจิทัล พ.ศ. 2566 – 2570 โดยเปลี่ยนกระบวนทัศน์จากการทำงานแบบแยกส่วน (Silos) สู่การเป็นรัฐบาลที่ขับเคลื่อนด้วยข้อมูล (Data-Driven Government) ที่ยึดประชาชนเป็นศูนย์กลาง หัวใจสำคัญไม่ใช่เพียงการโอนย้ายไฟล์ทางเทคนิค แต่คือการสร้างระบบนิเวศการเชื่อมโยงข้อมูลที่มีมาตรฐานสากล (Interoperability) เพื่อลดความซ้ำซ้อนในกระบวนงานและส่งเสริมหลักการ "ให้ข้อมูลเพียงครั้งเดียว" (Once Only Principle) ซึ่งจะช่วยเพิ่มประสิทธิภาพในการให้บริการสาธารณะและสร้างความโปร่งใสในทุกระดับชั้นของรัฐบาลอย่างยั่งยืน

เพื่อให้การดำเนินงานเกิดขึ้นได้จริงและมั่นคงปลอดภัย มาตรฐานนี้จึงเป็นข้อเสนอแนะและแนวทางในการพิจารณามิติต่างๆ เพื่อให้การแบ่งปันข้อมูลมีความปลอดภัยตามกรอบธรรมาภิบาลข้อมูลภาครัฐ (Data Governance) ที่สอดคล้องกับกฎหมาย และมีการบริหารจัดการที่ระบุสิทธิและหน้าที่ของผู้เกี่ยวข้องที่ชัดเจน ซึ่งจะช่วยลดความกังวลของหน่วยงานต่อการดำเนินงานขัดต่อกฎหมาย พร้อมทั้งเปลี่ยนมุมมองต่อข้อมูลให้เป็น "ทรัพย์สินดิจิทัล" ที่ควรนำมาบูรณาการเพื่อสร้างประโยชน์สูงสุดแก่ประชาชน และส่งเสริมให้เกิดการใช้ประโยชน์จากข้อมูล ควบคู่ไปกับการคุ้มครองข้อมูลให้ปลอดภัยตามหลักธรรมาภิบาลข้อมูลภาครัฐ

1.2. วัตถุประสงค์

เอกสารฉบับนี้จัดทำขึ้นเพื่อแนวทางการแบ่งปันข้อมูลภาครัฐ โดยมีวัตถุประสงค์หลัก ดังนี้

1.2.1. เพื่อสร้างความเชื่อมั่นและความเข้าใจในการแบ่งปันข้อมูลภาครัฐทั้งในประเทศและต่างประเทศ เป็นการลดความคลุมเครือ รวมถึงสร้างแนวทางที่ชัดเจนสำหรับการตัดสินใจในแบ่งปันข้อมูล เพื่อให้หน่วยงานสามารถตัดสินใจการแบ่งปัน และยังสามารถใช้ประโยชน์จากข้อมูลที่มีอยู่ได้อย่างมีประสิทธิภาพ

1.2.2. เพื่อส่งเสริมการแบ่งปันข้อมูลที่มีความปลอดภัย โดยมีแนวทางและประเด็นสำคัญที่ต้องพิจารณา เช่น การปกป้องข้อมูลส่วนบุคคล การจัดการสิทธิการเข้าถึง และการใช้มาตรการควบคุมที่เหมาะสม เพื่อให้การแบ่งปันข้อมูลเป็นไปอย่างปลอดภัยและมีธรรมาภิบาล

1.2.3. เพื่อส่งเสริมการเป็นรัฐบาลดิจิทัล เนื่องจากการเป็นรัฐบาลดิจิทัลจำเป็นต้องขับเคลื่อนด้วยข้อมูลแบบบูรณาการระหว่างหน่วยงานรัฐ การแบ่งปันข้อมูลจึงเป็นรากฐานสำคัญที่ช่วยสร้าง

ความเชื่อมโยงข้อมูลระหว่างภาครัฐ ลดความซ้ำซ้อนในการทำงาน และเพิ่มความรวดเร็วในการให้บริการประชาชน

1.3. ขอบข่าย

แนวทางการแบ่งปันข้อมูลภาครัฐฉบับนี้จัดทำขึ้น เพื่อเป็นข้อเสนอแนะให้เจ้าของข้อมูล (Data Owner) ใช้เป็นหลักในการแบ่งปันข้อมูลให้มีความปลอดภัยตามกรอบธรรมาภิบาลข้อมูลภาครัฐ ซึ่งเป็นการเตรียมความพร้อมก่อนการแบ่งปันข้อมูลจริง โดยมุ่งเน้นไปที่ข้อมูลให้อยู่ในรูปแบบที่เครื่องสามารถอ่านได้ (Machine Readable) ภายใต้หลักการ Five Safes โดยแนวทางฉบับนี้ได้จัดทำตามมาตรฐานและแนวปฏิบัติที่ดีของ

3.3.1 Australian Government, Best Practice Guide to Applying Data Sharing Principles

3.3.2 Tanvi D. , Felix R. , and Richard W. (2016). Five Safes: Designing data access for research. Bristol, England, UK: University of the West of England, Bristol Series: Economics Working Paper Series (1601)

3.3.3 สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล. (2568). แนวปฏิบัติพื้นฐานด้านการคุ้มครองข้อมูลส่วนบุคคล (ภาคส่วนทั่วไป)

1.4. บทนิยาม

1.4.1. **การแบ่งปันข้อมูล (Data sharing)** หมายความว่า การทำให้ข้อมูลพร้อมใช้งานสำหรับหน่วยงาน องค์กร หรือบุคคลอื่นภายใต้เงื่อนไขที่ตกลงกันไว้ หรือ การอ้างอิงสำหรับใช้ในการแบ่งปันข้อมูล (Shared) แลกเปลี่ยนข้อมูล (Exchangeable) และนำข้อมูลไปต่อยอด (Extensible) เพื่อการสนับสนุนโครงสร้างพื้นฐานของกลุ่มผู้ใช้งานหรือผู้ใช้บริการแฟลตฟอร์ม (Community Infrastructure)

1.4.2. **ข้อมูลแบ่งปัน (Shared data)** หมายความว่า ข้อมูลอ่อนไหวที่ได้รับการจัดระดับชั้นข้อมูล ยกเว้นใน ระดับชั้นลับที่สุด ซึ่งสามารถแบ่งปันและแลกเปลี่ยนกันได้ระหว่างหน่วยงาน โดยจำเป็นต้องมีการกำหนดสิทธิ ในการเข้าถึงและใช้งาน รวมถึงการคุ้มครองข้อมูลให้มีความมั่นคงปลอดภัย

1.4.3. **เจ้าของข้อมูล (Data Owner)** หมายความว่า บุคคล/คณะบุคคลที่ทำหน้าที่รับผิดชอบดูแลข้อมูล โดยตรง เพื่อสร้างความมั่นใจได้ว่าการบริหารจัดการข้อมูลสอดคล้องกับนโยบาย มาตรฐาน กฎระเบียบ หรือกฎหมาย โดยเจ้าของข้อมูลทำการทบทวนและอนุมัติการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับข้อมูล เช่น การเปลี่ยนแปลงเมทาดาตาและเกณฑ์การทำข้อมูลให้ถูกต้องสมบูรณ์ (Data Cleansing) นอกจากนี้ยังมี หน้าที่ในการให้สิทธิในการเข้าถึงข้อมูลและการจัดระดับชั้นข้อมูล เจ้าของข้อมูลส่วนใหญ่อยู่ในตำแหน่งบริหาร เช่น ผู้อำนวยการฝ่ายหรือ

หัวหน้าส่วนงานบุคคลเป็นเจ้าของข้อมูลบุคคล ผู้อำนวยการฝ่ายหรือหัวหน้าส่วน งานการเงินเป็นเจ้าของข้อมูลการเงิน

1.4.4. **เจ้าหน้าที่ผู้รับผิดชอบดูแลข้อมูล (Data Agents)** หมายความว่า บุคคลที่มีหน้าที่จัดเก็บข้อมูลให้ มั่นคงปลอดภัย รวมทั้งทบทวน หรือเสนออนุมัติการดำเนินการต่างๆ ที่เกี่ยวข้องกับข้อมูล และรายงานบันทึก กิจกรรมการประมวลผลข้อมูล

1.4.5. **เจ้าของข้อมูลส่วนบุคคล (Data Subject)** หมายความว่า บุคคลธรรมดาที่ข้อมูลส่วนบุคคลเกี่ยวกับบุคคลนั้นระบุถึงได้ไม่ว่าทางตรงหรือทางอ้อม

1.5. กฎหมายและแนวทางที่เกี่ยวข้อง

1.5.1 พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540

1.5.2 พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 มาตรา 15

1.5.3 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

1.5.4 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

1.5.5 ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม

1.5.6 ระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. 2552 และที่แก้ไขเพิ่มเติม

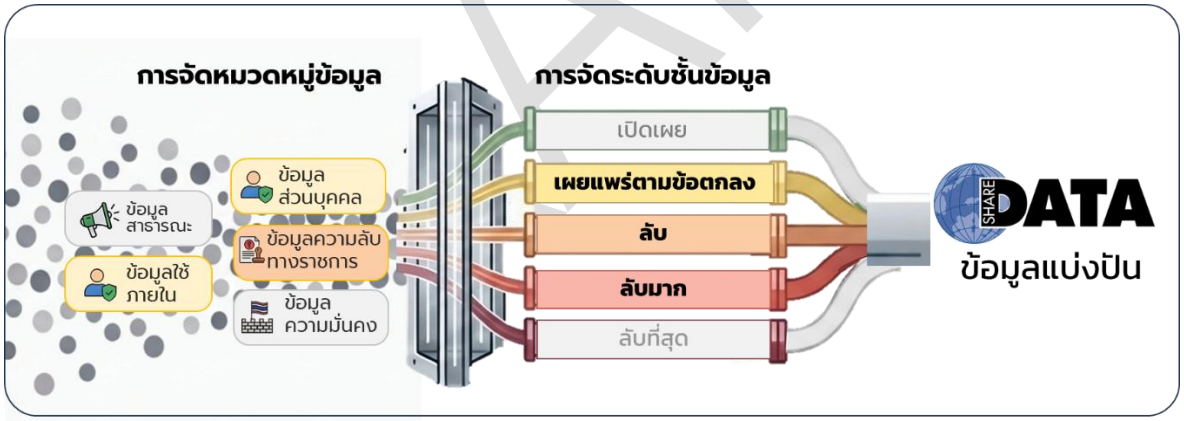
1.5.7 ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัลเรื่อง ธรรมาภิบาลข้อมูลภาครัฐ พ.ศ. 2563 และฉบับปรับปรุง พ.ศ. 2566

2. กรอบแนวคิดการแบ่งปันข้อมูลภาครัฐ

บทที่ 2 นี้จะมุ่งเน้นการศึกษาทั้งในเชิงกรอบแนวคิด ทฤษฎี และแนวปฏิบัติในระดับสากล เพื่อนำมาประยุกต์ใช้เป็นทิศทางสำหรับการแบ่งปันข้อมูลในประเทศไทย โดยในส่วนแรกจะกล่าวถึงแนวคิดเกี่ยวกับข้อมูลแบ่งปัน (Shared Data) ก่อนการนำเสนอกรณีศึกษาและหลักการที่เกี่ยวข้อง

การแบ่งปันข้อมูลของภาครัฐมุ่งเน้นการใช้ประโยชน์จากข้อมูล เพื่อเพิ่มประสิทธิภาพในการบริหารราชการและการให้บริการประชาชน ตามหลักการ Once-Only Principle ซึ่งส่งเสริมให้หน่วยงานภาครัฐสามารถนำข้อมูลที่มีอยู่มาใช้ประโยชน์ร่วมกันได้อย่างมีประสิทธิภาพ ในบริบทดังกล่าว การแบ่งปันข้อมูล (Data Sharing) จึงเป็นกลไกสำคัญที่ทำให้ข้อมูลสามารถนำไปใช้ประโยชน์ร่วมกันระหว่างหน่วยงานได้ โดยต้องมีการกำหนดประเภทของข้อมูลที่สามารถ ซึ่งเรียกว่า ข้อมูลแบ่งปัน (Shared Data) ที่มีระดับตั้งแต่ระดับชั้นเผยแพร่ตามข้อตกลงไปจนถึงระดับลับมากตามกรอบธรรมาภิบาลข้อมูลภาครัฐ เพื่อป้องกันผลกระทบจากการเข้าถึงหรือเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต และเพื่อให้การแลกเปลี่ยนข้อมูลเป็นไปอย่างปลอดภัย

ดังนั้น การดำเนินการแบ่งปันข้อมูลจึงมิใช่เพียงการส่งมอบข้อมูลระหว่างหน่วยงานเท่านั้น แต่ยังครอบคลุมถึงการบริหารจัดการสิทธิการเข้าถึง และการกำหนดวัตถุประสงค์การใช้งานที่ชัดเจน เพื่อสร้างความสมดุลระหว่างผลประโยชน์สาธารณะและความปลอดภัยของข้อมูลอย่างมีประสิทธิภาพ



รูปที่ 1 การจัดระดับชั้นข้อมูลและการแบ่งปันข้อมูล

ลักษณะสำคัญของการแบ่งปันข้อมูล สรุปได้ดังนี้ (Australian Government, 2019) (Tanvi Desai1, Felix Ritchie2 and Richard Welpton2, 2016)

- **การควบคุมการเข้าถึงข้อมูล (Controlled Access):** การแบ่งปันข้อมูลต้องดำเนินการภายใต้กลไกการควบคุมที่เหมาะสม โดยจำกัดสิทธิเฉพาะหน่วยงานหรือบุคคลที่ผ่านการพิสูจน์ตัวตนและได้รับอนุญาตเท่านั้น
- **รูปแบบการแบ่งปันและทางเทคนิค (Modes of Sharing & Technical Readiness):** สามารถดำเนินการได้ทั้งในรูปแบบการส่งมอบชุดข้อมูลโดยตรง หรือการให้สิทธิเข้าถึงข้อมูล

ผ่านระบบที่จัดเตรียมไว้ โดยข้อมูลควรอยู่ในรูปแบบที่คอมพิวเตอร์สามารถอ่านได้ (Machine Readable) เช่น .xls, .csv, .rdf เพื่อให้สามารถนำข้อมูลไปวิเคราะห์หรือเชื่อมโยงได้

- **วัตถุประสงค์เพื่อการใช้ข้อมูลซ้ำ (Re-use Purpose):** การแบ่งปันข้อมูลจะช่วยให้มีการนำข้อมูลที่มีอยู่มาสร้างมูลค่าเพิ่มให้เกิดประโยชน์สูงสุด และลดการเก็บข้อมูลทับซ้อนระหว่างหน่วยงาน ซึ่งจะช่วยลดภาระของประชาชนในการให้ข้อมูลซ้ำซ้อนตามหลักการ Once-only Principle[1] เพื่อให้ข้อมูลกลับมาใช้ซ้ำ (Re-use) เพื่อพัฒนาบริการเชิงรุกผ่านการบูรณาการร่วมกันได้

ทั้งนี้ จะเห็นได้ว่าลักษณะที่โดดเด่นของข้อมูลแบ่งปัน (Shared Data) คือการกำหนดสิทธิและการรับส่งผ่านส่งผ่านระบบแลกเปลี่ยนข้อมูลกลางที่มีมาตรการควบคุมความมั่นคงปลอดภัยอย่างเข้มงวด เช่น ศูนย์แลกเปลี่ยนข้อมูลกลาง (GDX) หรือแพลตฟอร์มกลางในการแลกเปลี่ยนข้อมูลที่มีมาตรฐาน เนื่องจากเป็นข้อมูลที่มีการจัดระดับชั้นความลับ ตั้งแต่ระดับที่ชั้นเผยแพร่ตามข้อตกลงไปจนถึงระดับลับที่สุด เพื่อป้องกันการเข้าถึงหรือการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต ซึ่งแตกต่างกับ ข้อมูลเปิด (Open Data) ที่เน้นการเข้าถึงได้โดยเสรีและในรูปแบบที่สามารถนำไปใช้งานได้ โดยข้อมูลเปิดจะถูกเผยแพร่ผ่านช่องทางสาธารณะ เช่น หน้าเว็บไซต์หน่วยงาน เพื่อให้ประชาชนหรือหน่วยงานอื่นสามารถขอเชื่อมโยงและใช้ประโยชน์ได้ทันที โดยไม่จำเป็นต้องมีการขออนุญาตอีกครั้ง ในขณะที่การแบ่งปันข้อมูลนั้นจะต้องผ่านกระบวนการตรวจสอบสิทธิ และพิจารณาวัตถุประสงค์ของการนำข้อมูลไปใช้งานอย่างละเอียดก่อนเริ่มดำเนินการทุกครั้ง

รูปที่ 2 การแบ่งปันข้อมูลภาครัฐและการเปิดเผยข้อมูล

[1] การข้อมูลจากประชาชนเพียงครั้งเดียว" (Once Only Principle) คือการที่ประชาชนให้ข้อมูลกับภาครัฐเพียงครั้งเดียวก็เข้าถึงบริการดิจิทัลภาครัฐได้อย่างครบวงจร จากแผนพัฒนารัฐบาลดิจิทัลของประเทศไทย พ.ศ. 2566 – 2570

ดังนั้น เพื่อให้เห็นภาพการแบ่งปันข้อมูลมากขึ้น ในบทที่ 2.1 จะกล่าวให้เห็นถึงความสำคัญของการแบ่งปันข้อมูลและตัวอย่างของต่างประเทศ เพื่อนำมาเป็นทิศทางและตัวอย่างในการแบ่งปันข้อมูล และบทที่ 2.2 หลักการในการแบ่งปันข้อมูล เพื่อพัฒนาแนวทางการแบ่งปันข้อมูลภาครัฐของประเทศไทยต่อไป

2.1. ความสำคัญของการแบ่งปันข้อมูลภาครัฐ

หัวข้อนี้จะพูดถึงความสำคัญในการแบ่งปันข้อมูลของต่างประเทศที่มีการนำ**หลักการความปลอดภัย 5 มิติ (Five Safes)** มาพิจารณาก่อนการแบ่งปันข้อมูล โดยเป็นการหาสมดุลระหว่างความเสี่ยงจากการเปิดเผยข้อมูลและประโยชน์ของข้อมูล โดยกรอบแนวคิด Five Safes ทำให้หน่วยงานรัฐสามารถที่จะจัดการความเสี่ยงจากการเปิดเผยข้อมูลอย่างมีระบบ ช่วยลดโอกาสของการเปิดเผยข้อมูลที่สามารถระบุตัวบุคคลได้ และสอดคล้องกับความต้องการใช้ข้อมูลจริง โดยไม่เพียงลดความละเอียดของข้อมูลเท่านั้น แต่ยังควบคุมที่มิติของด้านโครงการ (Safe Project) ด้านบุคคล (Safe People) ด้านสภาพแวดล้อม (Safe Settings) ด้านข้อมูล (Safe Data) และด้านผลลัพธ์ (Safe Output) ซึ่งการแบ่งปันข้อมูลช่วยให้สามารถนำข้อมูลจากหลายแหล่งมารวมกันเพื่อวิเคราะห์เชิงลึกและสร้างแบบจำลองเชิงนโยบายที่ครอบคลุม สร้างนวัตกรรมใหม่ ๆ หรือบริการที่ตอบโจทย์สังคมได้

<u>กรอบแนวคิดความปลอดภัย 5 มิติ (Five Safes) ในต่างประเทศ เพื่อการแบ่งปันข้อมูล 5 ประเทศ</u>

สำนักงานสถิติแห่งสหราชอาณาจักร (ONS) และ หน่วยงาน **UK Data Service (SecureLab)** ได้นำ Five Safes Framework มาใช้เพื่อบริหารจัดการข้อมูลสถิติและข้อมูลเชิงวิจัยที่มีความละเอียดสูงให้เป็นไปอย่าง **ปลอดภัย โปร่งใส และให้ประโยชน์เชิงสังคมอย่างแท้จริง** โดยไม่ละเมิดสิทธิพื้นฐานของเจ้าของข้อมูล ซึ่งแพลตฟอร์มวิจัย Trusted Research Environments (TREs) ที่พัฒนาโดย NHS England ร่วมกับ Bennett Institute for Applied Data Science รวมถึงHealth Data Research-UK (HDR-UK) และNational Institute for Health Research Design Service (NIHR) แพลตฟอร์มนี้ช่วยให้นักวิจัยสามารถวิเคราะห์ข้อมูลผู้ป่วยกว่า 58 ล้านคนโดยไม่ต้องดาวน์โหลดข้อมูลจริงออกมา ทำให้ข้อมูลคงอยู่ในสภาพแวดล้อมที่ปลอดภัย และเผยเฉพาะผลสรุปที่ไร้ความเสี่ยงต่อการระบุตัวบุคคลเท่านั้น ซึ่งช่วยให้งานวิจัยที่เป็นประโยชน์ต่อสาธารณะ และ การคุ้มครองข้อมูลส่วนบุคคล เกิดขึ้นควบคู่กัน

ตารางที่ 1 การเปรียบเทียบ Five Safes พร้อมตัวอย่างการนำไปใช้ใน (UK Data Service / ONS)

มิติ (Safe)	ตัวอย่างการควบคุมจริงจาก UK Data Service / ONS
Safe Projects โครงการที่ปลอดภัย	โครงการต้องได้รับอนุมัติจากเจ้าของข้อมูลว่าเป็นไปเพื่อประโยชน์สาธารณะ
Safe People บุคคลที่ปลอดภัย	นักวิจัยต้องผ่านการรับรองและฝึกอบรมก่อนเข้าถึงข้อมูลที่มีความละเอียดสูง

มิติ (Safe)	ตัวอย่างการควบคุมจริงจาก UK Data Service / ONS
Safe Settings สภาพแวดล้อมที่ปลอดภัย	ข้อมูลละเอียดไม่สามารถดาวน์โหลดได้ ต้องวิเคราะห์ภายใต้ SecureLab/Secure Research Service ที่ควบคุมเสมอ
Safe Data ข้อมูลที่ปลอดภัย	ข้อมูลถูกควบคุม ปรับแต่ง หรือ De-identified ก่อนให้ใช้งาน
Safe Outputs ผลลัพธ์ที่ปลอดภัย	ผลลัพธ์ของงานวิเคราะห์ต้องผ่านการตรวจสอบ เพื่อไม่ให้เสี่ยงต่อการเปิดเผยข้อมูลส่วนบุคคล

ที่มา: *(UK Data Service, 2026)*

📌 **ตัวอย่างบริการที่เกิดขึ้นจากการแบ่งปันข้อมูลภาครัฐ**

- **UK Data Service SecureLab** เป็นสภาพแวดล้อมที่ให้ *นักวิจัยที่ผ่านการรับรอง* เข้าถึงข้อมูลที่ละเอียดหรือมีความเสี่ยงสูงสำหรับการวิเคราะห์เชิงสถิติหรือวิจัย
- **ONS Secure Research Service (SRS)** การเข้าถึงข้อมูลสถิติที่ไม่ได้เผยแพร่ทั่วไป ภายใต้การควบคุมที่เข้มงวด เช่น ข้อมูลสุขภาพ การศึกษา หรือข้อมูลประชากรสำหรับงานวิจัยที่มีคุณค่าต่อสาธารณะ

บริการเหล่านี้เผยแพร่เป็นผลลัพธ์/รายงานวิจัยที่ ไม่มีข้อมูลส่วนบุคคล ก่อนที่จะเชื่อมโยงข้อมูลของแต่ละบุคคล ข้อมูลส่วนบุคคลของบุคคลนั้นจะถูกลบออกและแทนที่ด้วยรหัสเชื่อมโยง ซึ่งเป็นตัวระบุเฉพาะที่ช่วยให้สามารถเชื่อมโยงข้อมูลของบุคคลนั้นข้ามชุดข้อมูลต่างๆ ได้โดยไม่ประกอบด้วยข้อมูลที่สามารถใช้ระบุตัวตนของบุคคลนั้นได้ แต่ให้ภาพรวมที่เป็นประโยชน์ต่อการวางนโยบายด้านสาธารณสุขและบริการทางการแพทย์ได้อย่างปลอดภัย

 สำนักงานสถิติแห่งออสเตรเลีย ABS (Australian Bureau of Statistics) ได้นำกรอบแนวคิด Five Safes Framework มาช่วยให้โครงสร้างสำหรับการประเมินและจัดการความเสี่ยงจากการเปิดเผยข้อมูลอย่างมีระบบและสอดคล้องกับความต้องการใช้ข้อมูลจริง ซึ่งหน่วยงาน ABS ได้นำ Five Safes นี้มาใช้เป็นแนวทางในการให้บริการข้อมูลแก่ผู้ใช้หลายประเภท ทั้งในรูปของ Open Data (สถิติที่เข้าถึงได้ทั่วไป), Basic Microdata (ข้อมูลระดับจุลภาคพื้นฐาน) และ Detailed Microdata (ข้อมูลระดับจุลภาคแบบละเอียด) ที่ปลอดภัยและสอดคล้องกับผลประโยชน์สาธารณะ ซึ่งไม่เพียงแต่ลดความละเอียดของข้อมูลเท่านั้น แต่ยังควบคุมที่มิติของผู้ใช้ วัตถุประสงค์ สภาพแวดล้อม และผลลัพธ์ที่เผยแพร่อีกด้วย

1 **ตารางที่ 2 การเปรียบเทียบ Five Safes พร้อมตัวอย่างการนำไปใช้ใน ทั้ง 3 กรณี ในระบบ ABS**

มิติ (Safe)	Open Data สถิติที่เข้าถึงได้ทั่วไป	Basic Microdata ข้อมูลระดับจุลภาคพื้นฐาน (ดาวน์โหลดโดยตรง)	Detailed Microdata ข้อมูลระดับจุลภาคแบบละเอียด (ผ่าน ABS DataLab)
Safe Projects โครงการที่ปลอดภัย	ไม่ต้องมีการควบคุมใดๆ ใครๆ ก็สามารถใช้ข้อมูลเพื่อจุดประสงค์ของตนเองได้	ผู้ใช้ บางราย ต้องลงนามในเอกสารแสดงเจตนารมณ์ในการใช้ข้อมูล	ผู้ใช้งานที่มีการควบคุมสูงต้องระบุรายละเอียดวัตถุประสงค์ในการใช้ข้อมูลวัตถุประสงค์สามารถเปรียบเทียบกับผลลัพธ์ที่ได้จริง
Safe Pepple บุคคลที่ปลอดภัย	ไม่ต้องมีการควบคุมใดๆ ใครๆ ก็สามารถดูข้อมูลออนไลน์ได้	ผู้ใช้ บางรายต้องลงทะเบียนเพื่อใช้ข้อมูลและลงนามในข้อตกลงการใช้งานการฝ่าฝืนอาจมีบทลงโทษและ/หรือดำเนินคดีทางกฎหมาย	ผู้ใช้งานที่มีการควบคุมระดับสูงต้องเข้ารับการฝึกอบรม ผ่านกระบวนการอนุมัติ ลงนามในข้อตกลงรักษาความลับที่มีผลผูกพันทางกฎหมาย และลงนามในคำประกาศการปฏิบัติตามข้อกำหนด การฝ่าฝืนระเบียบหรือการเปิดเผยข้อมูลอาจส่งผลให้ถูกลงโทษและ/หรือดำเนินคดีทางกฎหมาย
Safe Settings สภาพแวดล้อมที่ปลอดภัย	ไม่จำเป็นต้องมีการควบคุมใดๆ	ผู้ใช้ บางรายจำเป็นต้องจัดเก็บข้อมูลอย่างปลอดภัย และสามารถทำงานกับข้อมูลได้ในสภาพแวดล้อมทางกายภาพและไอทีของตนเอง	การควบคุมระดับสูงข้อมูลรายละเอียดระดับจุลภาค (Detailed Microdata) สามารถเข้าถึงได้เฉพาะผ่าน ABS DataLab หรือภายในสภาพแวดล้อมที่มีการควบคุมการเข้าถึง พร้อมระบบบันทึกและตรวจสอบการใช้งานตามมาตรการความมั่นคงปลอดภัยที่กำหนด
Safe Data ข้อมูลที่ปลอดภัย	มีการควบคุมอย่างเข้มงวดข้อมูลถูกรวบรวมไว้ในระดับสูง	การควบคุมระดับสูงข้อมูลได้รับการประมวลผลโดย ABS เพื่อให้แน่ใจว่าไม่มีบุคคลใดสามารถระบุตัวตนได้	การควบคุมที่เหมาะสมข้อมูลระบุตัวตนโดยตรงจะถูกลบออก และข้อมูลจะได้รับการประมวลผลเพิ่มเติมตามความเหมาะสม การควบคุมข้อมูลอย่างเหมาะสมจะช่วยเพิ่มประโยชน์ของข้อมูล

มิติ (Safe)	Open Data สถิติที่เข้าถึงได้ทั่วไป	Basic Microdata ข้อมูลระดับจุลภาคพื้นฐาน (ดาวน์โหลดโดยตรง)	Detailed Microdata ข้อมูลระดับจุลภาคแบบละเอียด (ผ่าน ABS DataLab)
			สำหรับการวิเคราะห์ทางสถิติและการวิจัย
Safe Outputs ผลลัพธ์ที่ปลอดภัย	**การควบคุมระดับสูงมาก:** ตารางข้อมูลทุกชุดจะต้องผ่านการตรวจประเมินความเสี่ยงด้านการเปิดเผยข้อมูลก่อนอนุญาตให้เผยแพร่ (ในบริบทของข้อมูลเปิด ผลลัพธ์ของข้อมูลถือเป็นข้อมูลที่ผ่านการควบคุมเพื่อความปลอดภัยแล้ว)	**การควบคุมบางส่วน:**ผู้ใช้งานสามารถควบคุมการจัดทำผลลัพธ์ได้ในเชิงเทคนิค อย่างไรก็ตาม ABS กำหนดแนวทางหรือหลักเกณฑ์เกี่ยวกับสิ่งที่สามารถเผยแพร่หรือแบ่งปันได้	**การควบคุมระดับสูง:** ผลลัพธ์ทางสถิติทั้งหมดจะได้รับการตรวจประเมินโดย ABS เพื่อพิจารณาความเสี่ยงด้านการเปิดเผยข้อมูลก่อนอนุญาตให้เผยแพร่แก่ผู้ใช้ข้อมูลงาน และอาจมีการตรวจสอบความสอดคล้องกับข้อเสนอโครงการเดิมประกอบด้วย

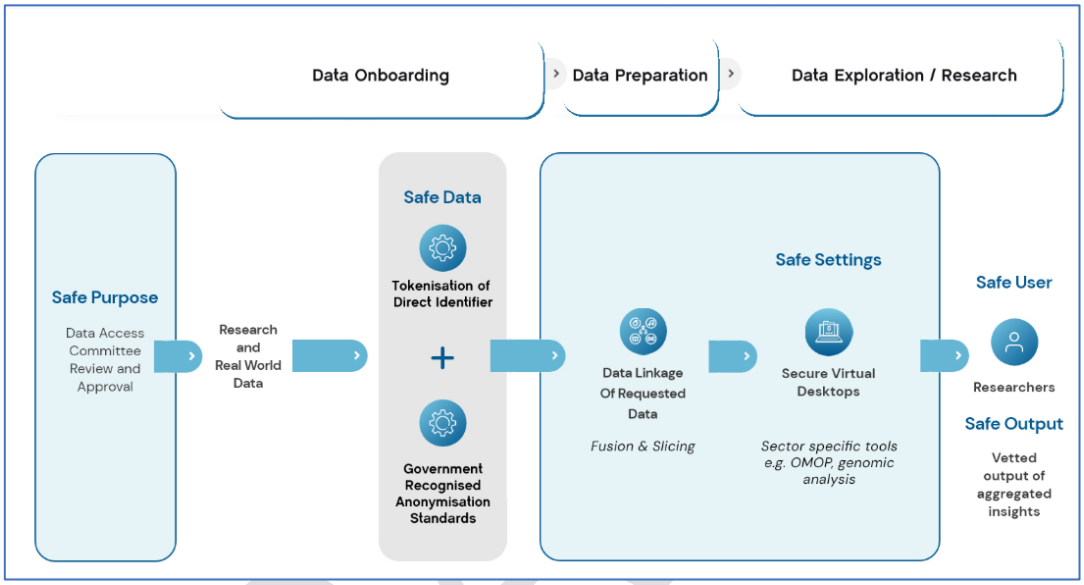
ที่มา: *(Australian Bureau of Statistics, 2021)*

📌 **ตัวอย่างบริการภาครัฐที่เกิดขึ้นจากการแบ่งปันข้อมูล**

หน่วยงาน ABS และหน่วยงานสถิติอื่นของรัฐ ได้สร้าง **บริการแบ่งปันข้อมูลภาครัฐ** ภายใต้การนำ Five Safes Framework มาใช้กับช่องทางการเข้าถึงข้อมูล 3 ช่องทางที่แตกต่างกัน ได้แก่

- **Open Data (สถิติที่เข้าถึงได้ทั่วไป) :** ข้อมูลสรุปหรือสถิติพื้นฐาน (เช่น ตัวเลข GDP, อัตราการว่างงาน) ที่เผยแพร่บนเว็บไซต์เพื่อให้ประชาชน หน่วยงาน และนักวิจัยใช้งานได้โดยไม่มีข้อจำกัดใน Safe People และ Safe Projects
- **Basic Microdata (ข้อมูลระดับจุลภาคพื้นฐาน) :** ไฟล์ข้อมูลระดับรายหน่วยที่ยังคงข้อมูลสำคัญ แต่ได้รับการปรับแต่ง เพื่อให้สามารถนำไปใช้วิเคราะห์ได้อย่างปลอดภัย โดยผู้ใช้ต้องสมัครและยอมรับเงื่อนไขการใช้งาน
- **Detailed Microdata (ข้อมูลระดับจุลภาคแบบละเอียด) เช่น ABS DataLab :** ข้อมูลละเอียดที่ผู้ใช้ต้องเข้าไปใช้งานในสภาพแวดล้อมที่ปลอดภัย และต้องมีการตรวจสอบก่อนเผยแพร่ผลลัพธ์

สิงคโปร์ ระบบ **TRUST (Trusted Research and Real-world-data Utilisation and Sharing Tech)** ถือเป็นแพลตฟอร์มแลกเปลี่ยนข้อมูลระดับชาติของสิงคโปร์ ซึ่งมีการใช้ Five Safes Framework เพื่อสนับสนุนการแลกเปลี่ยนข้อมูลสุขภาพระหว่างหน่วยงานรัฐ สถาบันวิจัย และภาคเอกชน โดยควบคุมการเข้าถึง และการวิเคราะห์ข้อมูลเพื่อป้องกันการละเมิดความเป็นส่วนตัวและความปลอดภัยของข้อมูลผู้ป่วย



รูปที่ 3 ระบบ TRUST *(ที่มา: (Singapore, 2026))*

ตารางที่ 3 การเปรียบเทียบ Five Safes พร้อมตัวอย่างการนำไปใช้ในบริบทของ TRUST

มิติ (Safe)	ตัวอย่างการควบคุมจริงจาก TRUST
Safe Projects โครงการที่ปลอดภัย	นักวิจัยและเจ้าหน้าที่ที่เข้าถึงข้อมูลต้องอยู่ภายใต้ข้อตกลงและปฏิบัติตาม Code of Conduct ของ TRUST
Safe People บุคคลที่ปลอดภัย	คณะกรรมการตรวจสอบคำขอ (DAC) พิจารณาความสอดคล้องกับผลประโยชน์สาธารณะก่อนให้ใช้
Safe Settings สภาพแวดล้อมที่ปลอดภัย	ใช้ Cloud ของรัฐบาลและห้องวิเคราะห์ที่ปลอดภัย เช่น Lab เฉพาะกิจสำหรับข้อมูลละเอียด
Safe Data ข้อมูลที่ปลอดภัย	ข้อมูลถูก Anonymise เช่น การลบตัวระบุเฉพาะบุคคลก่อนนำเข้า TRUST
Safe Outputs ผลลัพธ์ที่ปลอดภัย	อนุญาตให้ดาวน์โหลดหรือเผยแพร่เฉพาะข้อมูลเชิงสรุปที่ผ่านการตรวจสอบ

ที่มา: (Precision Health Research, 2026)

📌 **ตัวอย่างบริการที่เกิดขึ้นจากการแบ่งปันข้อมูล**

TRUST — Nation-wide Data Exchange Platform แพลตฟอร์มแลกเปลี่ยนข้อมูลสุขภาพที่รวบรวมข้อมูลจากหลายหน่วยงานสาธารณสุขและสถาบันวิจัย เพื่อสนับสนุนงานวิจัยและนวัตกรรมด้านการแพทย์ เช่น การวิเคราะห์โรคและการวางแผนบริการสุขภาพ โดยข้อมูลถูกจัดเก็บในสภาพแวดล้อมที่ปลอดภัยและวิเคราะห์ได้โดยไม่ต้องถ่ายโอนข้อมูลออกจากระบบ ทำให้การแบ่งปันข้อมูลสำคัญต่อการวิจัยเป็นไปอย่างมีประสิทธิภาพและปลอดภัย.

🍁 สถิติแห่งชาติของแคนาดา- Statistics Canada ใช้ Five Safes Framework เป็นแนวทางบริหารความเสี่ยงจากการเปิดเผยข้อมูล โดยเฉพาะใน Research Data Centre Program เพื่อควบคุมการเข้าถึงและวิเคราะห์ microdata (ข้อมูลระดับบุคคลที่ถูกทำให้ไม่ระบุตัวตนได้) โดยป้องกันการรั่วไหลและรักษาความลับของข้อมูลประชาชนอย่างเข้มงวด ซึ่งช่วยให้การแบ่งปันข้อมูลเชิงลึกเป็นไปอย่างปลอดภัยและเป็นประโยชน์ต่อสาธารณะ ทั้งในด้านงานวิจัย นโยบาย และบริการสาธารณะ โดยยังคงปกป้องความเป็นส่วนตัวของประชาชนอย่างเคร่งครัด

📋 **ตารางที่ 4: การเปรียบเทียบ Five Safes พร้อมตัวอย่างการนำไปใช้ในบริบทของ Statistics Canada**

มิติ (Safe)	ตัวอย่างการควบคุมจริงจาก Statistics Canada
Safe Projects โครงการที่ปลอดภัย	การเข้าถึงต้องได้รับอนุมัติจาก Statistics Canada หลังการประเมินโครงการวิจัยและ peer review ว่ามีคุณค่า
Safe People บุคคลที่ปลอดภัย	ผู้วิจัยต้องเป็นพนักงาน/ผู้ได้รับการแต่งตั้ง “deemed employee” ของรัฐ, ผ่านการคัดกรองความปลอดภัยและลงนามสัญญารักษาความลับก่อนเข้าถึง
Safe Settings สภาพแวดล้อมที่ปลอดภัย	ข้อมูลเข้าถึงได้ใน RDC (Research Data Centres) ซึ่งเป็นพื้นที่ปลอดภัยที่ควบคุมทางกายภาพและระบบเทคโนโลยี
Safe Data ข้อมูลที่ปลอดภัย	ข้อมูล microdata ถูกควบคุมและจัดเก็บอย่างปลอดภัย ก่อนให้ใช้ และการเข้าถึงเป็นไปภายในข้อจำกัดที่กำหนด
Safe Outputs ผลลัพธ์ที่ปลอดภัย	ผลลัพธ์จากการวิเคราะห์ต้องผ่านการตรวจสอบก่อนเผยแพร่ เพื่อให้แน่ใจว่าไม่สามารถระบุตัวบุคคลได้

ที่มา: (Canada, 2025)

ตัวอย่างบริการที่เกิดขึ้นจากการแบ่งปันข้อมูล

Research Data Centre (RDC) Program : เป็นระบบที่ให้ นักวิจัยที่ได้รับอนุมัติ เข้าถึง microdata ของรัฐบาลสำหรับการทำวิจัยสาธารณะ มีการจำกัดการเข้าถึงข้อมูลดิบจากภายนอก และอนุญาตให้เข้าถึงได้เฉพาะภายในสภาพแวดล้อมที่มีการควบคุมและรักษาความมั่นคงปลอดภัยตามที่กำหนดเท่านั้น **บริการที่นักวิจัยทำผ่าน RDC เช่น** วิเคราะห์ปัจจัยทางเศรษฐกิจและสังคม เช่น ผลกระทบของนโยบายสาธารณะ, วิจัยด้านสุขภาพประชากร,ตรวจสอบแนวโน้มการเปลี่ยนแปลงของแรงงาน, ศึกษาความเหลื่อมล้ำและกลุ่มประชากรที่เปราะบาง

นิวซีแลนด์ การบูรณาการข้อมูลของหน่วยงาน Stats NZ (Statistics New Zealand) โดยใช้ Five Safes Framework เป็นหลักในการบริหารความเสี่ยงและควบคุมการเข้าถึงชุดข้อมูลแบบ Integrated Data Infrastructure (IDI) ซึ่งรวมข้อมูลจากหลายหน่วยงานของรัฐเข้าด้วยกัน เพื่อช่วยในการบริหารการเข้าถึงและแบ่งปันข้อมูลแบบบูรณาการอย่างมีระบบ โดยสร้างสมดุลระหว่าง **การปกป้องความเป็นส่วนตัวและความปลอดภัยของข้อมูล** กับ **การใช้ข้อมูลเพื่อประโยชน์ต่อสาธารณะ** สนับสนุนการวิจัยและการตัดสินใจเชิงนโยบายที่เป็นประโยชน์ต่อสาธารณะ โดยยังคงความปลอดภัยและความเป็นส่วนตัวของข้อมูล เช่น การวิจัยนโยบายสาธารณะและการปรับปรุงบริการของรัฐ โดยทุกการเข้าถึงข้อมูลต้องผ่านการประเมินทั้ง 5 มิติอย่างเคร่งครัด

ตารางที่ 5: การเปรียบเทียบ Five Safes พร้อมตัวอย่างการนำไปใช้ในบริบทของ Stats NZ

มิติ (Safe)	ตัวอย่างการควบคุมจริงจาก Stats NZ
Safe Projects โครงการที่ปลอดภัย	ต้องแสดงวัตถุประสงค์ที่ เป็นประโยชน์ต่อสาธารณะ ให้เข้าถึงได้
Safe People บุคคลที่ปลอดภัย	นักวิจัยต้องผ่านการรับรอง ตรวจสอบประวัติ และฝึกอบรมก่อนเข้าถึงข้อมูล
Safe Settings สภาพแวดล้อมที่ปลอดภัย	เข้าถึงข้อมูลได้เฉพาะใน secure data lab หรือสภาพแวดล้อมปิดที่ไม่มีการเชื่อมต่อภายนอก
Safe Data ข้อมูลที่ปลอดภัย	ข้อมูลจะมีการ de-identification ลบตัวระบุ ก่อนอนุญาตใช้งาน
Safe Outputs ผลลัพธ์ที่ปลอดภัย	ผลลัพธ์/รายงาน ต้องผ่านการตรวจสอบว่าปลอดภัยก่อนเผยแพร่

ที่มา: (Stats NZ, 2017)

ตัวอย่างบริการที่เกิดขึ้นจากการแบ่งปันข้อมูล

Integrated Data Infrastructure (IDI) บริการวิจัยเชิงข้อมูลระดับชาติ ที่รวมข้อมูลสุขภาพ, การศึกษา, รายได้, การจ้างงานจากหลายหน่วยงานของรัฐเข้าด้วยกัน ข้อมูลเหล่านี้ถูกนำไปใช้เพื่อสนับสนุนการตัดสินใจด้านนโยบายและพัฒนาบริการของรัฐ *(ที่มา: (Stats NZ, 2020))*

- รายงานเกี่ยวกับผลลัพธ์เชิงสังคม เช่น ผลกระทบของโครงการสุขภาพต่อประชากร
- วิเคราะห์ภาวะรายได้และการจ้างงานของกลุ่มประชากร
- ศึกษาความเชื่อมโยงระหว่างข้อมูลการศึกษาและสุขภาพ

จากการประยุกต์หลักการ Five Safes กับกรณีศึกษาต่างประเทศ สามารถวิเคราะห์ได้ว่าหัวใจสำคัญของการแบ่งปันข้อมูลภาครัฐมีดังต่อไปนี้

หลักการความปลอดภัย 5 มิติ (Five Safes)
เพื่อเปลี่ยนจาก *"การเลี่ยงความเสี่ยง" สู่ "การบริหารจัดการความเสี่ยง"* เพื่อการแบ่งปันข้อมูล

ประเทศ / หัวข้อ	สหราชอาณาจักร	ออสเตรเลีย	สิงคโปร์	แคนาดา	นิวซีแลนด์
หน่วยงานที่เกี่ยวข้อง	Office for National Statistics (ONS)	Australian Bureau of Statistics (ABS)	Infocomm Media Development Authority (IMDA)	Statistics Canada	Statistics New Zealand (Stats NZ)
กรอบการแบ่งปันข้อมูล	The Five Safes Framework	Five Safes Framework	Five Safes, One TRUSTed Platform	Five Safes Model	The Five Safes framework
สถานะกรอบการทำงาน	กฎหมาย /มาตรฐาน (Digital Economy Act 2017	กฎหมาย (DATA Act 2022)	มาตรฐาน (MOH TRUST และ enTRUST)	มาตรฐาน (แนวทางปฏิบัติภายใต้ Statistics Act)	มาตรฐาน (Data and Statistics Act 2022)
ตัวอย่างการนำหลักการไปประยุกต์ใช้	• ระบบ Secure Research Service (SRS) เน้นมาตรฐานนักวิจัยระดับสูง • โครงการ Data First โดยกระทรวงยุติธรรม เพื่อวิเคราะห์ข้อมูลบุคคลในระบบยุติธรรม	• โครงการ MADIP (Multi-Agency Data Integration Project) เพื่อบูรณาการข้อมูลจากหน่วยงานรัฐ เช่น กรมสรรพากร กระทรวงบริการสังคม	• แพลตฟอร์ม TRUST (Trusted Research and Real-world-data Utilisation) เพื่อบูรณาการข้อมูลสุขภาพจาก กระทรวงสาธารณสุข (MOH) ร่วมกับหน่วยงานอื่นๆ	• โครงการ Statistics Canada เพื่อเชื่อมโยงข้อมูล การเข้ารับการรักษาในห้องฉุกเฉิน (Health) เข้ากับข้อมูลรายได้และสวัสดิการ และข้อมูล ประวัติอาชญากรรม	• โครงการ IDI เป็นคลังข้อมูลที่รวมข้อมูลดิบจากหน่วยงานมากกว่า 15 แห่ง เช่น ข้อมูลภาษี สวัสดิการ (MSD)

รูปที่ 4 กรอบแนวคิดการแบ่งปันข้อมูลภาครัฐ 5 ประเทศ

โดยสรุป กรอบแนวคิดการแบ่งปันข้อมูลภาครัฐที่ตั้งอยู่บนหลักการ Five Safes และมาตรฐานสากลจากสหราชอาณาจักร ออสเตรเลีย นิวซีแลนด์ แคนาดา และสิงคโปร์ เป็นเครื่องมือที่มีประสิทธิภาพในการขับเคลื่อนบูรณาการข้อมูลภาครัฐ ทั้งนี้ การประยุกต์ใช้ Five Safes อย่างเป็นระบบ จะช่วยให้หน่วยงานสามารถบริหารจัดการความเสี่ยงได้อย่างครอบคลุมทุกมิติ ทั้งในด้านวัตถุประสงค์โครงการ คุณสมบัติบุคคล ความมั่นคงของสภาพแวดล้อม ความละเอียดของข้อมูล และความปลอดภัยของผลลัพธ์ที่เผยแพร่ข้อมูล

2.2. หลักการแบ่งปันข้อมูลภาครัฐ (Data Sharing Criteria)

ในหัวข้อนี้จะเป็นผลการศึกษาหลักการแบ่งปันข้อมูลภาครัฐ โดย สพร. ได้อ้างอิงหลักการตาม Best Practice Guide to Applying Data Sharing Principles จัดทำโดยรัฐบาลประเทศออสเตรเลีย (Australian Government, 2019) ที่มีการนำ Five Safes มาใช้เป็นหลักการแบ่งปันข้อมูลเป็นกรอบในการปรับปรุง

การเข้าถึงและการนำข้อมูลภาครัฐที่แลกเปลี่ยนกันได้ในรูปแบบอิเล็กทรอนิกส์ เพื่อรักษาความเป็นส่วนตัวและความปลอดภัยของข้อมูล ซึ่งหลักการฯ นี้ เป็นหลักการให้หน่วยงานนำไปพิจารณาก่อนการแบ่งปันข้อมูลของหน่วยงานภาครัฐ โดยการแบ่งปันข้อมูลควรคำนึงถึงกฎหมายที่เกี่ยวข้อง เช่น พระราชบัญญัติข้อมูลข่าวสารของราชการฯ ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 ระเบียบสำนักนายกรัฐมนตรีว่าด้วยงานสารบรรณ (ฉบับที่ 4) พ.ศ. 2564 และระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. 2552 หรือกฎหมายอื่นๆ ที่เกี่ยวข้อง ทั้งนี้ การแบ่งปันข้อมูลจะช่วยจัดเตรียมการเข้าถึงข้อมูลในลักษณะที่มีการควบคุมการเปิดเผยข้อมูล ซึ่งการแบ่งปันข้อมูลช่วยให้นำข้อมูลที่มีอยู่กลับมาใช้ใหม่เพื่อก่อให้เกิดประโยชน์ต่อสาธารณะและการสร้างชุดข้อมูลใหม่เพื่อให้ข้อมูลเชิงลึกเกี่ยวกับภาคประชาสังคม (ชุมชน ครอบครัว และประชาชน) ระบบเศรษฐกิจและภาคการผลิต (ภาคอุตสาหกรรม การค้าและบริการ) ตลอดจนทรัพยากรและสิ่งแวดล้อม อย่างไรก็ตาม การแบ่งปันข้อมูลจะต้องได้รับการจัดการอย่างระมัดระวังและปลอดภัย เพื่อให้ประชาชนไว้วางใจว่าหน่วยงานของรัฐมีการจัดการกับข้อมูลที่ถือครองอย่างเหมาะสม ซึ่งมีหลักการและเงื่อนไขการแบ่งปันข้อมูลภาครัฐดังต่อไปนี้

1) หลักการแบ่งปันข้อมูลภาครัฐ สามารถแบ่งออกเป็น 3 หลักการสำคัญ ดังนี้

- หลักการแบ่งปันข้อมูล

(1) **การจัดทำคำขอแบ่งปันข้อมูล (Data Sharing Request)** เป็นการจัดทำคำขอแบ่งปันข้อมูลไปยังหน่วยงานเจ้าของข้อมูล ซึ่งอาจมาจากหน่วยงานของรัฐอื่น ภาคเอกชน หรือภาคการศึกษา เพื่อเริ่มต้นการพิจารณาโครงการ/แผนงาน/กิจกรรมที่จะแบ่งปันข้อมูล ซึ่งควรมีเนื้อหาระบุอย่างชัดเจนถึงข้อตกลง ข้อกำหนดและเงื่อนไขของโครงการ/แผนงาน/กิจกรรม วัตถุประสงค์ในการใช้ข้อมูล และการนำไปใช้ประโยชน์ รวมถึงระยะเวลาในการเผยแพร่ข้อมูลและความคุ้มครองการนำข้อมูลไปใช้ประโยชน์ เพื่อประเมินความเหมาะสมของการแบ่งปันข้อมูลในเบื้องต้นได้ โดยมีเกณฑ์พิจารณาดังนี้

- **ข้อมูลเป็นข้อมูลที่มีอยู่และเหมาะสมหรือไม่** เจ้าของข้อมูลควรดำเนินการประเมินคำขอและระบุแหล่งที่มาหลักของข้อมูลที่สามารถแบ่งปันตามคำขอ โดยเจ้าของข้อมูลจะต้องมีความเข้าใจที่ดีที่สุดเกี่ยวกับขอบเขตการใช้ข้อมูลว่า เป็นข้อมูลของหน่วยงานหรือไม่ สามารถแบ่งปันหรือเปิดเผยข้อมูลได้มากน้อยเพียงใด

- **ข้อมูลสามารถแบ่งปันได้ตามกฎหมายหรือไม่** เจ้าของข้อมูลควรรับรองว่า การแบ่งปันข้อมูลเป็นไปตามที่กฎหมายกำหนด ซึ่งเจ้าของข้อมูลจำเป็นต้องตระหนักถึงข้อจำกัดทางกฎหมายและมีการสื่อสารไปยังผู้ร้องขอได้อย่างชัดเจน ทั้งนี้ สำหรับหน่วยงานภาครัฐ การเปิดเผยข้อมูลที่มีระดับชั้นความลับควรพิจารณาพระราชบัญญัติข้อมูลข่าวสารของราชการฯ ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 ระเบียบสำนักนายกรัฐมนตรี ว่าด้วยงานสารบรรณ (ฉบับที่ 4) พ.ศ. 2564 และระเบียบสำนักนายกรัฐมนตรี ว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. 2552 และที่แก้ไขเพิ่มเติม

- **ข้อมูลมีความอ่อนไหวหรือไม่** เจ้าของข้อมูลควรพิจารณาว่า ข้อมูลมีความอ่อนไหว และมีระดับอ่อนไหวเป็นอย่างไร เช่น ข้อมูลส่วนบุคคล ข้อมูลความมั่นคงของประเทศ สิ่งที่สำคัญคือต้องพิจารณาว่าความอ่อนไหวของข้อมูลอาจเปลี่ยนแปลงไปตามสถานการณ์ หากต้องการเข้าถึงข้อมูลอ่อนไหวสามารถทำได้โดยการจำกัดการเข้าถึงเฉพาะผู้ใช้ที่ได้รับอนุญาต แต่ข้อมูลเดียวกันนี้จำเป็นต้องลบข้อมูลที่สามารถระบุตัวตนได้หากเปิดเผยต่อสาธารณะ

(2) **การพิจารณาความต้องการของผู้ใช้ข้อมูล** หน่วยงานเจ้าของข้อมูลต้องพิจารณาความต้องการเฉพาะของบุคคลหรือหน่วยงานที่ร้องขอ เพื่อพิจารณาแนวทางการสนับสนุนการแบ่งปันข้อมูลและช่วยให้เกิดประโยชน์สูงสุดจากการใช้ข้อมูล ทั้งนี้ เมื่อได้รับคำขอแล้วเจ้าของข้อมูลจะต้องกำหนดข้อตกลงการแบ่งปันที่เหมาะสม อาทิ การแบ่งปันข้อมูลให้แก่ผู้ร้องขอ หรือให้ผู้ร้องขอเข้าถึงข้อมูล โดยเจ้าของข้อมูลมีหน้าที่ตรวจสอบความเหมาะสมเพื่อให้การแบ่งปันข้อมูลเป็นไปตามที่กฎหมายกำหนดและมีความปลอดภัยของข้อมูลแบ่งปัน

(3) **ขีดความสามารถและวัฒนธรรมองค์กร** เจ้าของข้อมูลจำเป็นต้องมีการประเมินทักษะและขีดความสามารถที่มีอยู่ภายในหน่วยงานก่อนการแบ่งปันข้อมูล และพัฒนาความเชี่ยวชาญของตนเอง เพื่อให้จัดการเตรียมการแบ่งปันข้อมูลเป็นไปอย่างมีประสิทธิภาพ นอกจากนี้ ควรปรับทัศนคติด้านวัฒนธรรมภายในองค์กร โดยเจ้าของข้อมูลต้องเปลี่ยนจาก *“การหลีกเลี่ยงความเสี่ยง”* ไปเป็น *“การจัดการความเสี่ยง”* ที่เกี่ยวข้องเพื่อให้เกิดการแบ่งปันข้อมูลและใช้ประโยชน์จากข้อมูลร่วมกัน

(4) **เตรียมจัดทำข้อตกลงการแบ่งปันข้อมูล** (Data Sharing Agreement) ซึ่งข้อตกลงการแบ่งปันข้อมูล จัดทำขึ้นระหว่างเจ้าของข้อมูลและหน่วยงานที่ได้รับหรือเข้าถึงข้อมูล เช่น หน่วยงานภาครัฐอื่นๆ สถาบัน การศึกษาและวิจัย องค์กรภาคเอกชน เป็นต้น โดยเนื้อหาในข้อตกลงอาจรวมถึงวัตถุประสงค์เงื่อนไขและรายละเอียดของโครงการ/แผนงาน/กิจกรรมที่จะแบ่งปันข้อมูล ทั้งนี้ เจ้าหน้าที่ที่รับผิดชอบของหน่วยงานที่ได้รับหรือเข้าถึงข้อมูลจะยินยอมให้ผู้ใช้งานข้อมูลทั้งหมดภายในหน่วยงานต้องปฏิบัติตามข้อกำหนดและเงื่อนไขการเข้าถึงข้อมูลภายในข้อตกลง ทั้งนี้ ในกรณีของข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล โดยมีการแบ่งปันเมื่อต้นทางกับปลายทางมีสถานะเป็นผู้ควบคุมข้อมูล (Data Controller) ทั้ง 2 ฝ่าย โดยเฉพาะในกรณีที่มีการแบ่งปันข้อมูลส่วนบุคคล หน่วยงานควรพิจารณาจัดทำข้อตกลงเป็นลายลักษณ์อักษรเพื่อกำหนดขอบเขตการใช้ข้อมูลให้ชัดเจน โดยข้อกำหนดขั้นที่ต้องระบุในข้อตกลง ต้องสอดคล้องกับกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

- **หลักการพิจารณาความเสี่ยงในการเปิดเผยข้อมูล**

หลักการแบ่งปันข้อมูลจะต้องพิจารณาการจัดการความเสี่ยงในการเปิดเผยข้อมูลและประโยชน์สาธารณะ เพื่อให้มีการควบคุมความเสี่ยงที่จะเกิดขึ้นในการแบ่งปันข้อมูล ประกอบด้วย 5 หลักการดังนี้

(1) **หลักการด้านโครงการ (Project Principle) : ข้อมูลจะถูกแบ่งปันเพื่อวัตถุประสงค์ที่เหมาะสมอันก่อให้เกิดประโยชน์สาธารณะ** เจ้าของข้อมูลต้องพิจารณาวัตถุประสงค์ของโครงการ/แผนงาน/กิจกรรม หรือการใช้ข้อมูลในคำขอข้อมูลว่ามีความเหมาะสมหรือไม่ และตอบสนองวัตถุประสงค์ในการแบ่งปันข้อมูลของหน่วยงาน ซึ่งหน่วยงานของรัฐหลายแห่งจะมีนโยบายหรือข้อกำหนดทางกฎหมายให้แบ่งปันข้อมูลได้หากเป็นไปตามวัตถุประสงค์ เช่น นโยบายของรัฐบาล การวิจัยและพัฒนาโดยสาธารณประโยชน์ การออกแบบโปรแกรม การนำไปปฏิบัติ และการประเมินผล หรือ การส่งมอบบริการภาครัฐ เป็นต้น และควรมีการประเมินโครงการที่จะแบ่งปันข้อมูลทั้งด้านกฎหมาย ด้านจริยธรรม/หลักจรรยาบรรณ และสาธารณประโยชน์ ทั้งนี้ขอให้คำนึงถึงประโยชน์ต่อสาธารณะเป็นสำคัญ ซึ่งโครงการเหล่านั้นควรได้รับการจัดการผ่านกระบวนการกำกับดูแลอย่างเป็นทางการ โดยอาจให้คณะกรรมการ/คณะทำงานด้านธรรมาภิบาลข้อมูลพิจารณาประเมินข้อเสนอโครงการทั้งหมดเพื่อการแบ่งปันข้อมูล และเจ้าของข้อมูลสามารถขอรวมประเด็นสำคัญบางประการไว้ในข้อเสนอโครงการ เช่น ข้อกำหนดสำหรับการอนุมัติจริยธรรมหรือความยินยอมจากต้นฉบับ ซึ่งกระบวนการอนุมัติของคณะกรรมการจะแสดงให้ทั้งผู้ใช้ข้อมูลและเจ้าของข้อมูลทราบว่าโครงการไม่มีอุปสรรคทางจริยธรรมที่สำคัญ ในทำนองเดียวกัน หากมีการแจ้งความยินยอมจากผู้ให้บริการด้านข้อมูลอาจลดความกังวลของเจ้าของข้อมูลเกี่ยวกับข้อพิจารณาอื่นๆ ที่อาจส่งผลต่อกระบวนการประเมินโครงการ เช่น ต้นทุนของการแบ่งปันข้อมูล หรือ การแบ่งปันข้อมูลอาจส่งผลกระทบต่อองค์กร เป็นต้น

(2) **หลักการด้านบุคคล (People Principle) : ผู้มีสิทธิที่เหมาะสมในการเข้าถึงข้อมูล** โดยผู้ใช้งานข้อมูลอาจต้องผ่านกระบวนการอนุมัติเพื่อประเมินความรู้ ความสามารถ ทักษะ และวัตถุประสงค์ในการใช้งาน เพื่อพิจารณาว่าสามารถใช้หรือจัดเก็บข้อมูลที่มีการแบ่งปันได้อย่างเหมาะสมและปลอดภัย สำหรับการให้สิทธิ์ผู้ใช้งานข้อมูล เกณฑ์การอนุญาตแก่ผู้ใช้อาจมีพื้นฐานทางกฎหมาย เช่น กฎหมายอาจอนุญาตให้ผู้ใช้งานเฉพาะในการเข้าถึงข้อมูล หรืออาจตอบสนองต่อเจ้าของข้อมูลซึ่งผู้ใช้เข้าใจความคาดหวังเมื่อเข้าถึงข้อมูลที่แบ่งปัน ในบางกรณี เจ้าของข้อมูลอาจใช้งานข้อมูลทั้งหมดหรือบางส่วนของกระบวนการที่ได้รับอนุญาตโดยหน่วยงานอื่นที่สร้างข้อมูลเพื่อจำกัดการทำซ้ำ ทั้งนี้ ผู้ใช้งานข้อมูลอาจได้รับอนุญาตให้เข้าถึงข้อมูลที่แบ่งปันสำหรับโครงการใดโครงการหนึ่ง หรือได้รับสิทธิ์ในการเข้าถึงข้อมูลสำหรับหลายโครงการเพิ่มเติม อาจรวมถึงสิทธิในการเข้าถึงข้อมูลอย่างต่อเนื่อง อาทิ การเข้าถึงชุดข้อมูลที่มีการอัปเดตเป็นระยะโดยเจ้าของข้อมูล ซึ่งเจ้าของข้อมูลจะต้องพิจารณาขอบเขตของการอนุญาตในบริบทของการร้องขอเพื่อการเข้าถึงในแต่ละครั้ง

(3) **หลักการด้านสภาพแวดล้อม (Setting Principle) : สภาพแวดล้อมที่มีการแบ่งปันข้อมูลช่วยลดความเสี่ยงของการใช้หรือการเปิดเผยโดยไม่ได้รับอนุญาต** เจ้าของข้อมูลจำเป็นต้องพิจารณาความเสี่ยงที่จะเกิดขึ้นทั้งในสภาพแวดล้อมทางกายภาพและระบบเทคโนโลยีสารสนเทศเพื่อควบคุมวิธีการจัดเก็บ ถ่ายโอน และเข้าถึงข้อมูลได้ รวมไปถึงการพิจารณาว่าทุกฝ่ายที่เกี่ยวข้องได้ดำเนินการตามขั้นตอนที่เหมาะสมหรือไม่ เพื่อลดการใช้งานและเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต หรือการสูญหายของข้อมูล เพื่อให้มั่นใจได้ว่าข้อมูลจะถูกใช้ใน

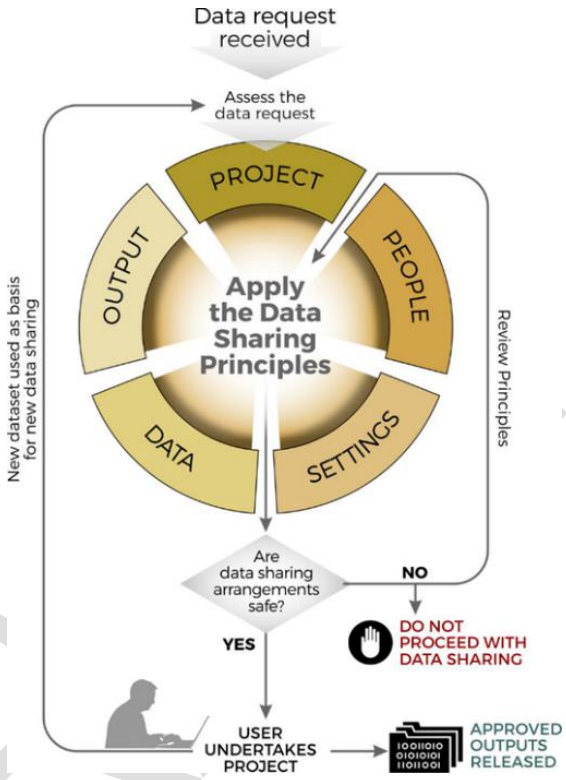
สภาพแวดล้อมที่ปลอดภัยและมีเสถียรภาพ นอกจากนี้ ลักษณะสำคัญของหลักการนี้เกี่ยวข้องกับการฝึกอบรม (มักเป็นส่วนหนึ่งของการให้สิทธิ์ผู้ใช้งานข้อมูล) เพื่อช่วยให้ผู้ใช้งานข้อมูลหลีกเลี่ยงข้อผิดพลาดและเพื่อตอบสนองเจ้าของข้อมูลที่ผู้ใช้สามารถคาดหวังได้อย่างสมเหตุสมผลว่าจะใช้และจัดเก็บข้อมูลอย่างเหมาะสม

(4) **หลักการด้านข้อมูล (Data Principle) : มีการปกป้องคุ้มครองข้อมูลที่นำไปใช้งานอย่างเหมาะสม** เจ้าของข้อมูลต้องควบคุมข้อมูลที่แบ่งปันให้แก่ผู้ใช้งานข้อมูล โดยมุ่งเน้นไปที่การจัดการข้อมูล อาทิ การลดขนาดข้อมูล การรวมข้อมูล การลบข้อมูลที่ระบุตัวตนโดยตรง หรือการระงับการบันทึกข้อมูลส่วนบุคคล ซึ่งเป็นสิ่งจำเป็นในการควบคุมความเสี่ยงที่ไม่สามารถแก้ไขได้ด้วยหลักการด้านโครงการ บุคลากร และสภาพแวดล้อม ทั้งนี้ เจ้าของข้อมูลอาจจำกัดการเข้าถึงข้อมูลโดยเฉพาะผู้ใช้ที่ได้รับอนุญาตเท่านั้นที่จะสามารถเข้าถึงและเห็นรายละเอียดของข้อมูลนั้น อย่างไรก็ตาม หลักการนี้มีข้อจำกัดคือต้องเข้าใจความแตกต่างระหว่างหลักการด้านข้อมูล และหลักการด้านผลลัพธ์ โดยหลักการด้านข้อมูลใช้ในการควบคุม เช่น การลบข้อมูลที่ระบุตัวตนโดยตรง และการรักษาความลับอื่นๆ กับชุดข้อมูลทั้งหมดที่มีให้กับผู้ใช้ ในขณะที่หลักการด้านผลลัพธ์จะใช้ควบคุมผลลัพธ์ที่จะเปิดเผยต่อสาธารณะหรือพร้อมสำหรับการแบ่งปันเพิ่มเติมโดยผู้ใช้ที่ได้รับอนุญาต กล่าวคือ หลักการด้านข้อมูลจะปกป้องข้อมูลที่ไปจากเจ้าของข้อมูลไปยังผู้ใช้ข้อมูล และหลักการด้านผลลัพธ์จะปกป้องข้อมูลภายหลังออกจากผู้ใช้งานข้อมูล

(5) **หลักการด้านผลลัพธ์ (Output Principle) : การจัดเตรียมการแบ่งปันข้อมูลได้รับการคุ้มครองอย่างเหมาะสมก่อนที่จะแบ่งปันหรือเผยแพร่ต่อไป** หากผู้ใช้งานข้อมูลต้องการแบ่งปันข้อมูลที่ผ่านการวิเคราะห์แล้ว ผู้ใช้ข้อมูลต้องดำเนินการประเมินตามหลักการแบ่งปันข้อมูลใหม่อีกครั้ง ก่อนจะแบ่งปันชุดข้อมูลใหม่ เพื่อสร้างสมดุลระหว่างความเสี่ยงในการเปิดเผยข้อมูลกับผลประโยชน์ หลักการนี้เกี่ยวข้องกับสิ่งที่จะเกิดขึ้นกับข้อมูลหรือข้อมูลที่ถูกสร้างขึ้นตามมาจากการแบ่งปันข้อมูล ในหลายกรณี ผลลัพธ์นี้จะเป็นสิ่งพิมพ์ รายงาน หรืออื่นๆ ที่เผยแพร่สู่สาธารณะ หรือแม้ว่าผลงานจะไม่ถูกเปิดเผยต่อสาธารณะ อาทิ โครงการของรัฐบาล รายงานการประเมิน จำเป็นต้องได้รับการคุ้มครอง ในการแบ่งปันข้อมูลอาจส่งผลให้เกิดการสร้างชุดข้อมูลใหม่ซึ่งอาจถูกแบ่งปันต่อ ตัวอย่างเช่น เจ้าของข้อมูลจัดเตรียมชุดข้อมูลให้กับหน่วยงานข้อมูลที่ความเชี่ยวชาญซึ่งปรับปรุงหรือแก้ไขข้อมูลและให้ผู้ใช้งานที่ได้รับอนุญาตเข้าถึงข้อมูลเพื่อการวิเคราะห์นั้น หน่วยงานข้อมูลที่ความเชี่ยวชาญจำเป็นต้องดำเนินการประเมินตามหลักการแบ่งปันข้อมูลใหม่อีกครั้งร่วมกับเจ้าของข้อมูลเดิม ก่อนที่ชุดข้อมูลใหม่จะถูกแบ่งปันต่อไป

โดยมีกระบวนการประยุกต์ใช้หลักการแบ่งปันข้อมูล เริ่มจากหน่วยงานรับคำร้องขอข้อมูล และประเมินคำร้องขอข้อมูลด้วยการประยุกต์ใช้หลักการแบ่งปันข้อมูล 5 ประการ (โครงการ บุคคล สภาพแวดล้อม ข้อมูล และผลลัพธ์) เพื่อให้มีการควบคุมความเสี่ยงที่จะเกิดขึ้นในการแบ่งปันข้อมูลและสร้างความมั่นใจได้ว่ามีการจัดเตรียมการแบ่งปันข้อมูลได้อย่างปลอดภัย กรณีที่การแบ่งปันข้อมูลมีความปลอดภัย สามารถแบ่งปันข้อมูลให้ผู้ใช้ดำเนินการโครงการต่อไป ทั้งนี้ **ในกรณีที่มีการแบ่งปันข้อมูลส่วนบุคคล หน่วยงานควรพิจารณา**

จัดทำข้อตกลงเป็นลายลักษณ์อักษร (Data Sharing Agreement) ทั้ง 2 ฝ่าย เพื่อกำหนดขอบเขตการใช้ข้อมูลให้ชัดเจน โดยข้อกำหนดขั้นที่ต้องระบุในข้อตกลง ต้องสอดคล้องกับกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล เมื่อดำเนินโครงการจะเกิดชุดข้อมูลใหม่ที่ถูกใช้งานและจำเป็นต้องทำการร้องขอข้อมูลตามกระบวนการประยุกต์ใช้หลักการแบ่งปันข้อมูลใหม่ และในกรณีที่การแบ่งปันข้อมูลไม่มีความปลอดภัยจะไม่อนุญาตให้แบ่งปันข้อมูลและกลับไปทบทวนตามหลักการใหม่อีกครั้ง



รูปที่ 5 การประยุกต์ใช้หลักการแบ่งปันข้อมูล

ที่มา: Best Practice Guide to Applying Data Sharing Principles Version 15 March 2019, Department of the Prime Miniter and Cabinet, Australian Government.

- **หลักการดูแลควบคุมการใช้ข้อมูล**

หน่วยงานสามารถยึดหลักการแบ่งปันข้อมูลและหลักการพิจารณาความเสี่ยงในการเปิดเผยข้อมูล โดยเจ้าของข้อมูลจะต้องพิจารณาและตรวจสอบว่าการควบคุมนั้นสามารถปกป้องข้อมูลที่จะแบ่งปันอย่างเหมาะสม เจ้าของข้อมูลต้องถามว่า หลังจากมีการนำข้อมูลไปใช้งาน “มีหลักการลดความเสี่ยงของการแบ่งปันให้อยู่ในระดับที่ยอมรับได้หรือไม่” และ “สามารถแบ่งปันข้อมูลอย่างปลอดภัยได้หรือไม่” หากคำตอบคือ “ไม่” เจ้าของข้อมูลสามารถกลับไปพิจารณาหลักการแต่ละข้อซ้ำเพื่อปรับระดับการควบคุมและการเข้าถึงข้อมูลใหม่อีกครั้ง หากไม่สามารถลดความเสี่ยงของการแบ่งปันให้อยู่ในระดับที่ยอมรับได้ ข้อมูลนั้นก็ไม่ควรแบ่งปัน ทั้งนี้ เจ้าของข้อมูลควรมีการกำหนดกระบวนการตรวจสอบในการกำกับดูแล การรายงาน และการประกันเพื่อให้เกิดการควบคุมความเสี่ยงที่เหมาะสมกับข้อมูลแบ่งปัน (Shared data) และมั่นใจได้ว่าผู้ใช้งานข้อมูลปฏิบัติตามเงื่อนไขที่กำหนดภายในข้อตกลงการแบ่งปันข้อมูล เพื่อให้การแบ่งปันข้อมูลมีความเหมาะสมกับการใช้งานและมีความปลอดภัย

จากทั้ง 3 หลักการข้างต้น จึงสามารถสรุปเพื่อนำไปประยุกต์ใช้ในการแบ่งปันข้อมูลภาครัฐโดยสามารถแบ่งออกเป็น 3 ระยะ ได้แก่

ระยะที่ 1 ก่อนการประยุกต์ใช้หลักการแบ่งปันข้อมูล

ระยะที่ 2 การประยุกต์ใช้หลักการแบ่งปันข้อมูล

ระยะที่ 3 ภายหลังการประยุกต์หลักการแบ่งปันข้อมูล

โดยสามารถศึกษาแนวทางการนำไปปฏิบัติ รายละเอียด และขั้นตอน เพิ่มเติมได้ที่ บทที่ 3 แนวปฏิบัติการแบ่งปันข้อมูลภาครัฐ ต่อไป

รูปที่ 6 หลักการและการประยุกต์ใช้แบ่งปันข้อมูลภาครัฐ

2) การแบ่งปันข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคล เป็นหนึ่งในหมวดหมู่ข้อมูลตามกรอบธรรมาภิบาลข้อมูลภาครัฐ โดยเป็นหมวดหมู่ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม โดยมีพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นกฎหมายที่ทำหน้าที่คุ้มครองสิทธิข้อมูลในส่วนนี้ ส่งผลให้หลายหน่วยงานภาครัฐและเอกชนยังมีข้อกังวลด้านกฎหมายส่งผลให้ขาดความเชื่อมั่นในการแบ่งปันข้อมูลระหว่างหน่วยงาน ถึงแม้เป็นการสร้างประโยชน์เพื่อสาธารณะและประชาชน ทำให้ขาดโอกาสและลดทอนการพัฒนาขีดความสามารถของการให้บริการของหน่วยงาน โดยแผนพัฒนารัฐบาลดิจิทัลของประเทศไทย พ.ศ. 2566 - 2570 ระบุว่าในกรณีของประเทศไทย หน่วยงานภาครัฐได้มีความพยายามที่จะพัฒนาฐานข้อมูลและเชื่อมโยงข้อมูลระหว่างหน่วยงาน เพื่อให้สามารถแบ่งปันข้อมูลและบริการกันระหว่างหน่วยงานภาครัฐได้อย่างมีประสิทธิภาพ ผ่านการใช้เทคโนโลยี เช่น API เป็นต้น อย่างไรก็ตามการดำเนินการดังกล่าวต้องใช้เวลานาน

หลายปี เพราะการเก็บข้อมูลของแต่ละหน่วยงานอยู่ในรูปแบบต่างกัน กฎระเบียบที่จำกัดการแบ่งปันข้อมูลของหน่วยงาน ข้อจำกัดด้านกฎหมายในการแบ่งปันข้อมูลส่วนบุคคล รวมถึงการขาดแนวทางการบูรณาการที่เป็นมาตรฐานกลางที่มีการบังคับใช้อย่างเคร่งครัดและการขาดงบประมาณในการดำเนินการ ดังนั้น เพื่อให้การเชื่อมโยงและการบูรณาการข้อมูลระหว่างภาครัฐเป็นไปอย่างมีประสิทธิภาพ จึงจำเป็นอย่างยิ่งที่ต้องส่งเสริมให้มีการบูรณาการข้อมูลระหว่างภาครัฐอย่างต่อเนื่อง ประกอบกับผลการสำรวจระดับความพร้อมรัฐบาลดิจิทัลของหน่วยงานภาครัฐ ปี 2568 พบว่า หน่วยงานระดับกรมหรือเทียบเท่ามีความพร้อมในการดำเนินการด้านกระบวนการพัฒนาด้วยข้อมูล (Data-driven Practices) โดยเฉพาะในด้าน Data Privacy สะท้อนให้เห็นถึงการคุ้มครองข้อมูลส่วนบุคคลตาม PDPA อย่างมีประสิทธิภาพ ในขณะที่การแบ่งปันข้อมูลยังคงเป็นจุดที่หน่วยงานระดับกรมมีความพร้อมน้อยที่สุด โดยมีสัดส่วนความพร้อมในระดับเริ่มต้นสูงถึงร้อยละ 36.95 ซึ่งแสดงให้เห็นว่าต้องการการส่งเสริมในการแบ่งปันและแลกเปลี่ยนข้อมูลระหว่างหน่วยงานภาครัฐให้มากขึ้น

การสร้างความมั่นใจในการแบ่งปันข้อมูลภาครัฐ รวมถึงข้อมูลส่วนบุคคล เป็นสิ่งสำคัญที่สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ตระหนักถึงการดำเนินงานของบุคลากรภาครัฐเป็นอย่างยิ่ง โดยมุ่งเน้นการขับเคลื่อนข้อมูลภายใต้กรอบธรรมาภิบาลข้อมูลภาครัฐ *(สามารถศึกษาเพิ่มเติมได้ที่ มรด. 6 : 2566 ว่าด้วยกรอบธรรมาภิบาลข้อมูลภาครัฐ ฉบับปรับปรุง: แนวปฏิบัติ)* ส่งเสริมให้หน่วยงานภาครัฐมีการขับเคลื่อนด้วยข้อมูลตามยุทธศาสตร์ด้านข้อมูลของหน่วยงานเป็นหลัก และเสนอแนวทางเพื่อสร้างความเชื่อมั่นในการแบ่งปันข้อมูล โดยผ่านกระบวนการและเครื่องมือ เช่น การจัดระดับชั้นข้อมูลภาครัฐ *(สามารถศึกษาเพิ่มเติมได้ที่ ร่าง มรด. X : 256X ว่าด้วยหลักเกณฑ์การจัดระดับชั้นข้อมูลภาครัฐ)* เพื่อให้หน่วยงานภาครัฐใช้เป็นหลักเกณฑ์ประกอบการใช้ดุลพินิจของผู้มีอำนาจในการตัดสินใจกำหนดระดับชั้นข้อมูล สามารถกำหนดการเข้าถึงและใช้งานข้อมูลและกำกับดูแลข้อมูลที่มีความอ่อนไหวหรือข้อมูลที่มีชั้นความลับอย่างเหมาะสม เพื่อรักษาความเป็นส่วนตัวและความปลอดภัยของข้อมูล ลดความเสี่ยงจากการถูกละเมิดหรือการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต รวมถึงการสูญหายของข้อมูล และเพื่อการเลือกใช้ประเภทคลาวด์ที่เหมาะสม โดยมีเครื่องมือในการประเมินระดับชั้นข้อมูลโดยพิจารณาตามกฎหมายที่เกี่ยวข้อง ประเมินด้านความปลอดภัยของข้อมูล (CIA) และการประเมินความเสี่ยงและผลกระทบ ตามลำดับ นอกจากนี้เพื่อสร้างความมั่นใจให้หน่วยงานภาครัฐมากยิ่งขึ้น อีกทั้งยังมีแนวทางการจัดทำข้อมูลนิรนาม ซึ่งเป็นแนวทางสำคัญในการสร้างความไว้วางใจและความน่าเชื่อถือต่อข้อมูลเพื่อการขับเคลื่อนองค์กรให้ดำเนินไปยังเป้าหมายได้อย่างมีประสิทธิภาพ โดยการทำข้อมูลให้เป็นนิรนาม เป็นกระบวนการจัดทำให้ข้อมูลส่วนบุคคลหรือข้อมูลที่สามารถระบุ ตัวตนได้มาอยู่ในรูปแบบที่ไม่สามารถระบุตัวตนได้ เพื่อลดความเสี่ยงการระบุตัวตนของเจ้าของ ข้อมูลส่วนบุคคล และเพื่อสร้างความมั่นใจให้แก่หน่วยงานภาครัฐในการสามารถนำข้อมูลไปใช้ประโยชน์ ทั้งยังเป็นการสร้างความเชื่อมั่นให้แก่ประชาชนถึงแนวทางการใช้ข้อมูลของภาครัฐ *(สามารถศึกษาเพิ่มเติมได้ที่ มสพร. 14-2567 ว่าด้วยแนวทางการจัดทำข้อมูลนิรนาม)* โดยหน่วยงานสามารถใช้เพื่อเป็นกรอบหลักการในการทำงานเพื่อสร้างความเชื่อมั่นในการแบ่งปันข้อมูลเพิ่มเติมได้

ในขณะที่หลายหน่วยงานขาดความมั่นใจหรือมีข้อกังวลด้านกฎหมาย พบว่ามีบางหน่วยงานเริ่มมีการขับเคลื่อนและผลักดันในการแบ่งปันข้อมูลระหว่างหน่วยงาน โดยดำเนินการตามภารกิจหลักของหน่วยงาน โดยยึดประโยชน์ของประชาชนและสาธารณะเป็นหลัก รวมไปถึงหน่วยงานที่มีความพร้อมด้านดิจิทัล สามารถดำเนินการตามมาตรา 15 แห่งพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 ให้มีศูนย์แลกเปลี่ยนข้อมูลกลางทำหน้าที่เป็นศูนย์กลางในการแลกเปลี่ยนข้อมูลดิจิทัลและทะเบียนดิจิทัลระหว่างหน่วยงานของรัฐ เพื่อสนับสนุนการดำเนินการของหน่วยงานของรัฐในการให้บริการประชาชนผ่านระบบดิจิทัล จึงก่อให้เกิดการแลกเปลี่ยนข้อมูลโดยการใช้บริการผ่านศูนย์แลกเปลี่ยนข้อมูลกลางภาครัฐ (GDX) หรือแพลตฟอร์มกลางในการแลกเปลี่ยนข้อมูลที่มีมาตรฐาน เพื่อยกระดับการให้บริการต่อประชาชน ดังตัวอย่างเช่น

- **กรมที่ดิน โครงการบูรณาการระบบทะเบียนทรัพย์สิน ตามมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูล ภาครัฐหน่วยงาน ด้านความหมายข้อมูล**

โครงการบูรณาการระบบทะเบียนทรัพย์สิน โดยเป็นความร่วมมือระหว่าง กรมที่ดิน, กรมธนารักษ์, กรมส่งเสริมการปกครองท้องถิ่น, กรมโยธาธิการและผังเมือง และองค์กรปกครองท้องถิ่น เป็นที่นำมาตรฐาน ด้านการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ไปปรับใช้ผ่านการพัฒนาระบบการแลกเปลี่ยนข้อมูลของแพลตฟอร์มกลาง (Platform) เพื่อการบูรณาการระบบทะเบียนทรัพย์สิน (PIPR: Central Platform for The Integration of Registration) และระบบอื่น ๆ ของหน่วยงานที่เกี่ยวข้อง โดยชุดข้อมูลที่สำคัญเช่น ข้อมูลประเมินภาษีที่ดินและสิ่งปลูกสร้าง ข้อมูลภาษีที่ดินและสิ่งปลูกสร้าง ข้อมูลผู้ถือกรรมสิทธิ์ ข้อมูลการชำระภาษี ข้อมูลภาษีห้องชุด ข้อมูลหน้าสำรวจของเอกสารสิทธิ ซึ่งจะนำไปใช้สำหรับการแลกเปลี่ยนข้อมูลดิจิทัลระหว่างหน่วยงานของรัฐ อีกทั้งเพื่อให้กรมที่ดินสามารถขยายผลแพลตฟอร์มให้ครอบคลุมหน่วยงานที่เกี่ยวข้องอื่น ๆ ได้มากขึ้น เช่น กทม., พัทยา, สำนักงบประมาณ และกระทรวงเกษตรและสหกรณ์ เป็นต้น โดยแต่ละหน่วยงานมีข้อมูลหลักของหน่วยงานในการดำเนินการด้านภาษีที่ดินและสิ่งปลูกสร้าง หรือห้องชุด ทั้งนี้หน่วยงานดำเนินการภายใต้อำนาจและหน้าที่ซึ่งสอดคล้องตามกฎหมายที่กำหนด และดำเนินการผ่านแพลตฟอร์มของระบบการรับส่งข้อมูล เอกสารและทะเบียนดิจิทัลภาครัฐ ที่เป็นไปตามธรรมาภิบาลข้อมูล โดยอ้างอิงมาตรฐานกรอบแนวทางการพัฒนามาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ (Thailand Government Information eXchange :TGIX Semantic ด้านความหมายข้อมูล) ปัจจุบันมี API ให้บริการผ่านศูนย์แลกเปลี่ยนข้อมูลกลางภาครัฐ (Government Data Exchange: GDX) จำนวน 5 รายการ ได้แก่ ข้อมูลแปลงที่ดิน ข้อมูลการครอบครองกรรมสิทธิ์ที่ดินและห้องชุด (อช.2), (นส.3), (นส.3ก) และ (นส.4) เพื่อให้หน่วยงานของรัฐสามารถมีศูนย์กลางแลกเปลี่ยนข้อมูลกลางที่มีมาตรฐาน ทำงานร่วมกันได้ มีความมั่นคงปลอดภัย เป็นไปตามหลักธรรมาภิบาลข้อมูล และประหยัดงบประมาณ

ปัจจุบันหน่วยงานมีการปรับใช้ในส่วนของ API ที่ดำเนินการแลกเปลี่ยนข้อมูลระหว่างหน่วยงานผ่านศูนย์แลกเปลี่ยนข้อมูลกลางภาครัฐ (Government Data Exchange: GDX) ซึ่งเป็นแพลตฟอร์มดิจิทัลเพื่อการเชื่อมโยงและแลกเปลี่ยนข้อมูล เป็นศูนย์กลางในการแลกเปลี่ยนข้อมูล และเอกสารทะเบียนดิจิทัลระหว่างหน่วยงานภาครัฐ เพื่ออำนวยความสะดวกแก่ประชาชนและภาคเอกชนเมื่อต้องการใช้บริการจากหน่วยงานภาครัฐ มีการออกแบบโดยคำนึงถึงมาตรฐาน ความมั่นคงปลอดภัย สามารถให้บริการได้อย่างต่อเนื่อง รองรับการขยายหรือเพิ่มเติมการเชื่อมโยงจากหน่วยงานภาครัฐต่างๆ และที่สำคัญคือการดำเนินงานของผู้ที่เกี่ยวข้องทั้งหมดจะเป็นไปตามธรรมาภิบาลข้อมูล โดยแต่ละหน่วยงานเจ้าของข้อมูลยังคงทำหน้าที่จัดเก็บและดูแลข้อมูล เอกสารทะเบียนดิจิทัลซึ่งมีบทบาทเป็นผู้ควบคุมข้อมูล และประมวลผลข้อมูลในด้านที่เกี่ยวข้องโดยดำเนินงานตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่จะต้องมีการคำนึงถึงความเป็นส่วนตัวของเจ้าของข้อมูลก่อนนำไปใช้งาน จึงช่วยให้หน่วยงานภาครัฐสามารถแลกเปลี่ยนเชื่อมโยงข้อมูลในรูปแบบดิจิทัลตามประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัลเรื่อง มาตรฐานและหลักเกณฑ์การเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัลว่าด้วยเรื่อง กรอบแนวทางการพัฒนามาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ โดยไม่จำเป็นต้องจัดทำบันทึกข้อตกลง (Memorandum of Understanding : MOU) กับหน่วยงานเจ้าของข้อมูลอีกครั้ง ปัจจุบันหน่วยงานบริการข้อมูล 27 หน่วยงาน และมี API บริการข้อมูล 106 รายการ สามารถดูรายละเอียดเพิ่มเติมได้ที่ https://gdx.dga.or.th/Account/Login?Index=Show

- **สำนักงานกิจการยุติธรรม กระทรวงยุติธรรม ศูนย์แลกเปลี่ยนข้อมูลกระบวนการยุติธรรม (Data Exchange Center : DXC)**

เป็นศูนย์บริการและเชื่อมข้อมูลข้อมูลกระบวนการยุติธรรมสนับสนุนการให้บริการของเจ้าหน้าที่ในการให้บริการกับประชาชน ลดระยะเวลาในการสืบค้นข้อมูล โดยหน่วยงานที่มีความพร้อมสามารถแลกเปลี่ยนและให้บริการข้อมูลได้อย่างมีประสิทธิภาพ สอดคล้องตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และกรอบธรรมาภิบาลข้อมูลภาครัฐ รวมถึงกฎหมาย ระเบียบ ข้อบังคับ คำสั่งหรือข้อกำหนดอื่นๆ ที่เกี่ยวข้อง มีการประกาศสำนักงานกิจการยุติธรรม เรื่อง นโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) เพื่อกำหนดแนวทางในการควบคุมดูแลข้อมูลส่วนบุคคลภายใต้การดำเนินงานของศูนย์แลกเปลี่ยนข้อมูลกระบวนการยุติธรรม สำหรับ DXC มีฐานข้อมูลที่เชื่อมโยงและให้บริการมากกว่า 60 ฐานข้อมูล เช่น ฐานข้อมูลเด็กหรือเยาวชนผู้กระทำผิด ฐานข้อมูลผู้ต้องขัง ฐานข้อมูลประวัติคดียาเสพติด ฐานข้อมูลหมายจับคดีพิเศษ เป็นต้น และระบบบัญชีข้อมูล DXC แสดงรายการกว่า 96 ชุดข้อมูล ซึ่งมีการเชื่อมโยงผ่านระบบเครือข่ายสื่อสารข้อมูลภาครัฐ (Government Information Network : GIN) ทำให้สามารถค้นหาและรายงานผลได้อย่างสะดวกรวดเร็วมากยิ่งขึ้น โดยขั้นตอนการเข้าร่วมเครือข่ายเพื่อใช้ระบบงานเริ่มต้นจาก หน่วยงานแจ้งความประสงค์มายัง สำนักงานกิจการยุติธรรม โดยเสนอพิจารณาเหตุผลความจำเป็น อำนาจหน้าที่และความต้องการ ในคณะทำงานพัฒนาระบบเทคโนโลยีสารสนเทศ กระบวนการยุติธรรม และรายงานต่อคณะอนุกรรมการพัฒนา ระบบเทคโนโลยีสารสนเทศกระบวนการยุติธรรม หน่วยงานจึงสามารถแต่งตั้ง ผู้ดูแล

ระบบ เพื่อบริหารจัดการผู้ใช้งานในหน่วยงาน ทั้งนี้ผู้ที่สามารถเข้าถึงข้อมูลต้องได้รับมอบสิทธิการเข้าถึงข้อมูลจากหน่วยงานที่มีการลง MOU ซึ่งมีทั้งสิ้น 27 หน่วยงาน โดยสามารถเข้าใช้งานเพื่อค้นหาข้อมูลได้ที่ https://www.dxc.go.th/

ทั้งนี้ในการเข้าถึงฐานข้อมูลมีการกำหนดรายชื่อหน่วยงานที่มีสิทธิ์เข้าใช้งานและกฎหมายกำหนดให้ใช้หรือวัตถุประสงค์การใช้งานรวมถึงตำแหน่งหรือกลุ่มบุคคลที่จำเป็นต้องใช้ข้อมูลไว้ชัดเจน เช่น ฐานข้อมูลหมายจับศาล มี สำนักงานอัยการสูงสุด ใช้เพื่อนำไปตรวจสอบเพื่อยืนยันความถูกต้องของข้อมูลหมายจับที่ปรากฏในสำนวนการสอบสวนของพนักงานสอบสวน เพื่อนำมาใช้ประกอบการพิจารณาทำความเห็นของพนักงานอัยการว่าจะอุทธรณ์คัดค้านคำพิพากษาของศาลหรือไม่ โดยตำแหน่งหรือกลุ่มบุคคลที่จำเป็นต้องใช้ คือ พนักงานอัยการ นอกจากนี้ยังมี กรมราชทัณฑ์ ใช้ข้อมูลเพื่อสนับสนุนการจำแนกลักษณะผู้ต้องขังเป็นรายบุคคล และสนับสนุนการพิจารณานักโทษเด็ดขาดที่จะได้รับพักการลงโทษ จะต้องพิจารณาคุณสมบัติตามกฎหมายที่เกี่ยวข้อง โดยตำแหน่งหรือกลุ่มบุคคลที่จำเป็นต้องใช้ คือ กองทัณฑปฏิบัติ (ส่วนกลาง) / ฝ่ายทัณฑปฏิบัติ (เรือนจำ) / งานจำแนกลักษณะผู้ต้องขัง (เรือนจำ) เป็นต้น นอกจากเพื่อให้การปฏิบัติงานด้านการตรวจสอบข้อมูลผู้กระทำผิดในภารกิจด้านพฤตินิสัยเป็นไปอย่างมีประสิทธิภาพมากยิ่งขึ้น จึงมีระเบียบกระทรวงยุติธรรมว่าด้วยการใช้ประโยชน์จากข้อมูลผู้กระทำผิดผ่านระบบศูนย์แลกเปลี่ยนข้อมูลกระบวนการยุติธรรม (Data Exchange Center : DXC) พ.ศ. 2558 ในการกำหนดบทบาทหน้าที่ของหน่วยงานที่เกี่ยวข้องเพื่อเป็นแนวทางในการปฏิบัติไว้อย่างชัดเจน *(ที่มา : (สำนักงานปลัดกระทรวงยุติธรรม, 2021)๗*

- **กรมสุขภาพจิต ขอหารือเกี่ยวกับการแลกเปลี่ยนข้อมูลผู้ป่วยจิตเวชและยาเสพติดที่มีความเสี่ยงสูงต่อการก่อความรุนแรง เพื่อความปลอดภัยของผู้ป่วย ผู้อื่น และสาธารณชน**

เมื่อวันที่ 10 กุมภาพันธ์ 2569 สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ได้เผยแพร่ข้อหารือตามกฎหมาย PDPA เกี่ยวกับการแลกเปลี่ยนข้อมูลผู้ป่วยจิตเวชและยาเสพติดที่มีความเสี่ยงสูงต่อการก่อความรุนแรง เพื่อความปลอดภัยของผู้ป่วย ผู้อื่น และสาธารณชน โดยมีกรมสุขภาพจิตซึ่งมีบทบาทหน้าที่ ในการประสานงานและร่วมมือกับหน่วยงานของรัฐ และเอกชนที่เกี่ยวข้องในการดำเนินงานด้านสุขภาพจิตเพื่อดำเนินการตามนโยบาย ยุทธศาสตร์และแผนสุขภาพจิตระดับชาตินั้น พบว่ามีผู้ป่วยจิตเวชที่ก่อความรุนแรงถึงขั้นมีคดีความและได้รับโทษแล้ว และเมื่อพ้นโทษหรือได้รับการปล่อยตัวจากกรมราชทัณฑ์ หรือกรมคุมประพฤติ ยังคงมีความเสี่ยงที่จะก่อความรุนแรงซ้ำ โดยที่ผู้ป่วยยังสามารถอยู่ร่วมกับคนในสังคมได้ หากแต่ต้องมีมาตรการ เฝ้าระวังที่เข้มข้น ได้แก่ การติดตามเฝ้าระวังอย่างใกล้ชิด การดูแลรักษาอย่างต่อเนื่องในชุมชน หากมีอาการกำเริบต้องรีบนำส่งสถานพยาบาลอย่างรวดเร็ว โดยอาศัยความร่วมมือของสำนักงานตำรวจแห่งชาติ ในการเข้าระงับความคลุ้มคลั่งของผู้ป่วยหากอาการกำเริบ และการนำส่งโดยสถาบันการแพทย์ฉุกเฉินแห่งชาติ จึงจะสามารถป้องกันการก่อความรุนแรงได้ การแลกเปลี่ยนข้อมูลผู้ป่วยจิตเวชที่พ้นโทษและปล่อยตัวแล้ว แต่มีความเสี่ยงสูงต่อการก่อความรุนแรงร่วมกันระหว่างหน่วยงานที่เกี่ยวข้องดังกล่าวจึงมีความจำเป็น

อย่างยิ่งสำหรับการติดตามเฝ้าระวัง เพื่อลดการก่อความรุนแรงซ้ำ และเพื่อความปลอดภัยของผู้ป่วย ผู้อื่น และสาธารณชน โดยหน่วยงานสามารถดำเนินการตามระบบ V-care ที่เป็นระบบเฝ้าระวังผู้ป่วยจิตเวชและยาเสพติดที่มีความเสี่ยงสูงต่อการก่อความรุนแรง (Serious Mental Illness with High Risk to Violence: SMI-V) โดยการเข้าใช้งานที่ https://vcare.jvkorat.go.th/

การแบ่งปันและการแลกเปลี่ยนข้อมูลผู้ป่วยจิตเวชระหว่างหน่วยงานจึงมีความสำคัญอย่างมาก ในการจัดทำฐานข้อมูล โดยการแลกเปลี่ยนข้อมูลผู้ป่วยจิตเวชที่มีความเสี่ยงสูงต่อการก่อความรุนแรง จากกรมสุขภาพจิต ข้อมูลผู้ต้องขังที่กำลังจะพ้นโทษ จากกรมราชทัณฑ์ ข้อมูลผู้ที่ได้รับคำสั่งศาล ในการคุมประพฤติ และข้อมูลผู้ที่พ้นโทษที่มีความผิดตามพระราชบัญญัติมาตรการป้องกันการกระทำความผิดซ้ำ ในความผิดเกี่ยวกับเพศหรือใช้ความรุนแรง พ.ศ. 2565 จากกรมคุมประพฤติ ข้อมูลเด็กและเยาวชน ผู้ที่จะได้รับการปล่อยตัวจากกรมพินิจและคุ้มครองเด็กและเยาวชน เพื่อส่งต่อข้อมูลให้สำนักงานตำรวจแห่งชาติ และสถาบันการแพทย์ฉุกเฉินแห่งชาติ ในการดำเนินมาตรการเฝ้าระวังต่อไป ทั้งนี้กรมสุขภาพจิตมีแนวทางการจัดทำฐานข้อมูลผู้ป่วยและเป็นผู้ควบคุมข้อมูลและออกแบบให้มีการบันทึกข้อมูล และมีกรมราชทัณฑ์ กรมคุมประพฤติ และกรมพินิจและคุ้มครองเด็กและเยาวชน เป็นผู้บันทึกข้อมูลและสามารถเข้าถึงข้อมูลได้ตามเงื่อนไขที่กำหนดเท่านั้น

คณะอนุกรรมการพัฒนาและขับเคลื่อนการดำเนินงานตามกฎหมายว่าด้วยสุขภาพจิต ได้มีการหารือร่วมกันโดยมีความเห็นว่า การเชื่อมโยงข้อมูลดังกล่าวน่าจะสามารถกระทำได้ตามข้อยกเว้นในบทบัญญัติตามมาตรา 16 แห่งพระราชบัญญัติสุขภาพจิต พ.ศ. 2551 ซึ่งบัญญัติห้ามมิให้ผู้ใดเปิดเผยข้อมูลด้านสุขภาพของผู้ป่วยในประการที่น่าจะทำให้เกิดความเสียหายแก่ผู้ป่วย เว้นแต่ (1) ในกรณีที่อาจเกิดอันตรายต่อผู้ป่วยหรือผู้อื่น (2) เพื่อความปลอดภัยของสาธารณชน (3) มีกฎหมายเฉพาะบัญญัติให้ต้องเปิดเผย และตามข้อยกเว้นในมาตรา 24 (2) และ (4) แห่งพระราชบัญญัติ คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จึงได้จัดตั้งคณะทำงานอันประกอบด้วยตัวแทนของส่วนราชการและหน่วยงานของรัฐที่เกี่ยวข้อง ได้แก่ กรมสุขภาพจิต กรมราชทัณฑ์ กรมคุมประพฤติ กรมพินิจและคุ้มครองเด็กและเยาวชน สำนักงานตำรวจแห่งชาติ และสถาบันการแพทย์ฉุกเฉินแห่งชาติ สำหรับการดำเนินการเชื่อมโยงข้อมูลเพื่อติดตามผู้ป่วยและหารือกับหน่วยงานที่เกี่ยวข้องสามารถเชื่อมโยงข้อมูลและแลกเปลี่ยนข้อมูลระหว่างกันได้หรือไม่ หากดำเนินการได้ มีเงื่อนไข ขั้นตอน ข้อพึงปฏิบัติ และข้อสังเกตในการดำเนินการอย่างไร เพื่อให้ถูกต้องตามบทบัญญัติแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เช่น การจัดทำข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล (Data Sharing Agreement: DSA) ซึ่งถือเป็นมาตรการเชิงองค์กรอย่างหนึ่งเพื่อกำหนดวัตถุประสงค์ วิธีการ เงื่อนไข และหน้าที่ความรับผิดชอบของแต่ละฝ่ายในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ไม่ว่าจะเป็นการรับและส่งข้อมูลที่เป็นเอกสารหรือเป็นการแลกเปลี่ยนข้อมูลโดยวิธีการอิเล็กทรอนิกส์ก็ตาม อันจะเป็นการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่จะเปิดเผยให้กับหน่วยงานที่เกี่ยวข้อง และควบคุมดูแลให้การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลระหว่างกันสอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

รวมทั้งยังเป็นมาตรการเพื่อป้องกันมิให้หน่วยงานที่ได้รับข้อมูลส่วนบุคคลใช้หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์อื่นนอกเหนือจากวัตถุประสงค์ ที่ได้แจ้งไว้ตามมาตรา 27 วรรคสอง หรือเพื่อป้องกันมิให้หน่วยงานดังกล่าวใช้หรือเปิดเผยโดยปราศจากอำนาจ หรือโดยมิชอบ ตามมาตรา 37 (2) อีกด้วย นอกจากนี้ต้องคำนึงถึงมาตรการรักษาความมั่นคงปลอดภัยดังกล่าว อย่างน้อยต้องประกอบด้วย การควบคุมการเข้าถึงข้อมูลส่วนบุคคล (Access control) ที่มีการพิสูจน์และยืนยันตัวตน และการอนุญาตหรือการกำหนดสิทธิในการเข้าถึงและใช้งานที่เหมาะสม โดยคำนึงถึงหลักการให้สิทธิเท่าที่จำเป็นตามหลักการให้สิทธิที่น้อยที่สุดเท่าที่จำเป็น การบริหารจัดการการเข้าถึงของผู้ใช้งาน รวมถึงการลงทะเบียนและการถอนสิทธิผู้ใช้งาน และการทบทวนสิทธิการเข้าถึงของผู้ใช้งาน ที่เหมาะสม การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งานที่ชัดเจน และการจัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง แก้ไข หรือลบข้อมูลส่วนบุคคลอย่างเหมาะสมตามระดับความเสี่ยง โดยคำนึงถึงความจำเป็นในการเข้าถึงและใช้งานตามลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล การรักษาความมั่นคงปลอดภัยตามระดับความเสี่ยง ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการประกอบกัน ทั้งนี้ ตามข้อ 4 (6) (ก) ถึง (ง) ของประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 รวมถึงการสร้างเสริมความตระหนักรู้ด้านความสำคัญของการคุ้มครองข้อมูล ส่วนบุคคลและการรักษาความมั่นคงปลอดภัยและการแจ้งนโยบาย แนวปฏิบัติ และมาตรการด้านการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัยอย่างเหมาะสม ให้ผู้ใช้งาน (User) หรือผู้ที่เกี่ยวข้องกับการเข้าถึง เก็บรวบรวม ใช้ เปลี่ยนแปลง แก้ไข ลบ หรือเปิดเผยข้อมูลส่วนบุคคล ทราบและถือปฏิบัติ ตามข้อ 4 (7) ของประกาศดังกล่าวด้วย *(ที่มา (สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล, 2026) : https://www.pdpc.or.th/wp-content/uploads/2026/02/consultation-65.pdf)*

3) ข้อเสนอแนะแนวทางการแบ่งปันข้อมูลภาครัฐ

(1) กำหนดนโยบายและหลักการการแบ่งปันข้อมูล (Data Sharing Policy & Principle) ด้วยการกำหนดเงื่อนไขให้สอดคล้องตาม “5 Data Sharing Principles” พร้อมระบุเหตุผลที่ยอมรับได้ในการไม่แบ่งปันข้อมูล ข้อมูลจะพร้อมใช้งานหรือเปิดเผยข้อมูลเมื่อใด หน่วยงานอื่นจะเข้าถึงข้อมูลได้อย่างไร มีข้อจำกัดใดๆ เกี่ยวกับข้อมูลหรือไม่ ข้อมูลมีเอกสารเพียงพอที่จะเป็นประโยชน์หรือไม่

(2) กำหนดข้อมูลแบ่งปัน และ คำขอการแบ่งปันข้อมูล (Shared Data and Data Sharing Request) โดย

- ข้อมูลแบ่งปัน (Shared Data) ในที่นี้ได้แก่ ข้อมูลสำคัญที่สอดคล้องกับยุทธศาสตร์ข้อมูล (Data Strategy) ภารกิจหลักและเป้าหมายของหน่วยงานและประเทศ รวมถึงข้อมูลอ่อนไหวที่ได้รับการจัดระดับชั้น เผยแพร่ตามข้อตกลง ลับ และลับมาก ซึ่งสามารถแบ่งปันและแลกเปลี่ยนกันได้ระหว่างหน่วยงาน โดยจำเป็นต้องมีการกำหนดสิทธิในการเข้าถึงและใช้งาน รวมถึงการคุ้มครองข้อมูลให้มีความมั่นคงปลอดภัย ไม่รวมถึงข้อมูลที่มีระดับชั้นลับที่สุด

ข้อควรคำนึงถึงในการแบ่งปันข้อมูล :

- ✓ ข้อมูล**ไม่สามารถเปิดเผย**ต่อสาธารณะได้ เนื่องจากเป็นข้อมูลข่าวสารที่ไม่ต้องเปิดเผย ตาม พ.ร.บ. ข้อมูลข่าวสารฯ มาตรา 14 และ มาตรา 15 ที่อาจมีคำสั่งมิให้เปิดเผยก็ได้ และเป็นข้อมูลที่สามารถระบุตัวตนของบุคคลได้ ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ[1]
- ✓ **ข้อมูลประกอบด้วยตำแหน่งที่สามารถถูกคุกคาม หรือสิ่งประดิษฐ์ที่มีคุณค่า** และจะ**ถูกแบ่งปันกับหน่วยงาน/ฝ่ายที่เชื่อถือได้เท่านั้นที่ตกลงตามเงื่อนไข**หรือเกณฑ์ในการใช้ซ้ำ (Reuse Criteria)
- ✓ **ไม่สามารถเปิดเผยข้อมูล**ได้จนกว่าจะมีการออกสิทธิบัตร (Patents) ที่เกี่ยวข้องกับการวิจัยและนวัตกรรมนั้น

(3) คำขอการแบ่งปันข้อมูล (Data Sharing Request) ควรต้อง

- แสดงให้เห็น*จุดมุ่งหมาย/เป้าหมายที่เหมาะสม* สอดคล้องกับการตรวจสอบเป้าประสงค์เกี่ยวข้อง (หากมี)
- แสดงให้เห็นถึงประโยชน์ต่อสาธารณะ หรือ ผลประโยชน์แห่งชาติ รวมทั้งความสอดคล้องกับข้อกฎหมายที่กำหนด เพื่อนำไปสู่การเปิดเผยข้อมูลภาครัฐ
- ระบุถึงข้อมูลที่ต้องการร้องขอ/เหตุผลที่ร้องขอ กรอบเวลาที่ต้องการใช้ข้อมูลและผลลัพธ์ที่คาดหวัง
- ระบุถึงตัวบุคคล/หน่วยงานจะร่วมงานในโครงการ/ข้อตกลงในการแบ่งปันข้อมูล

แสดงให้เห็นถึงความเป็นไปได้ในการแบ่งปันข้อมูล อาทิ ข้อมูลการให้บริการ (ข้อมูลระเบียน) เหมาะสมสำหรับการตอบสนองคำขอข้อมูลแบ่งปัน

กำหนดข้อตกลงการแบ่งปันข้อมูล (Data Sharing Agreement)

- ทำขึ้นระหว่างหน่วยงานเจ้าของข้อมูลและหน่วยงานที่ได้รับชุดข้อมูลที่ร้องขอหรือข้อมูลแบ่งปัน
- อาจรวมถึงผลการตรวจสอบตามเป้าประสงค์และรายละเอียดของโครงการที่ครอบคลุมโดยข้อตกลง
- ควรระบุถึงข้อมูลใดบ้างที่ใช้ได้และใช้ไม่ได้ภายใต้ข้อตกลง
- ควรให้ข้อมูลเกี่ยวกับบทลงโทษใดๆ ที่อาจถูกกำหนดไว้หากไม่ปฏิบัติตามข้อกำหนดและเงื่อนไขในข้อตกลง (ซึ่งอาจรวมถึงการอ้างอิงถึงบทลงโทษที่มีการบังคับใช้ตามกฎหมายที่เกี่ยวข้อง)

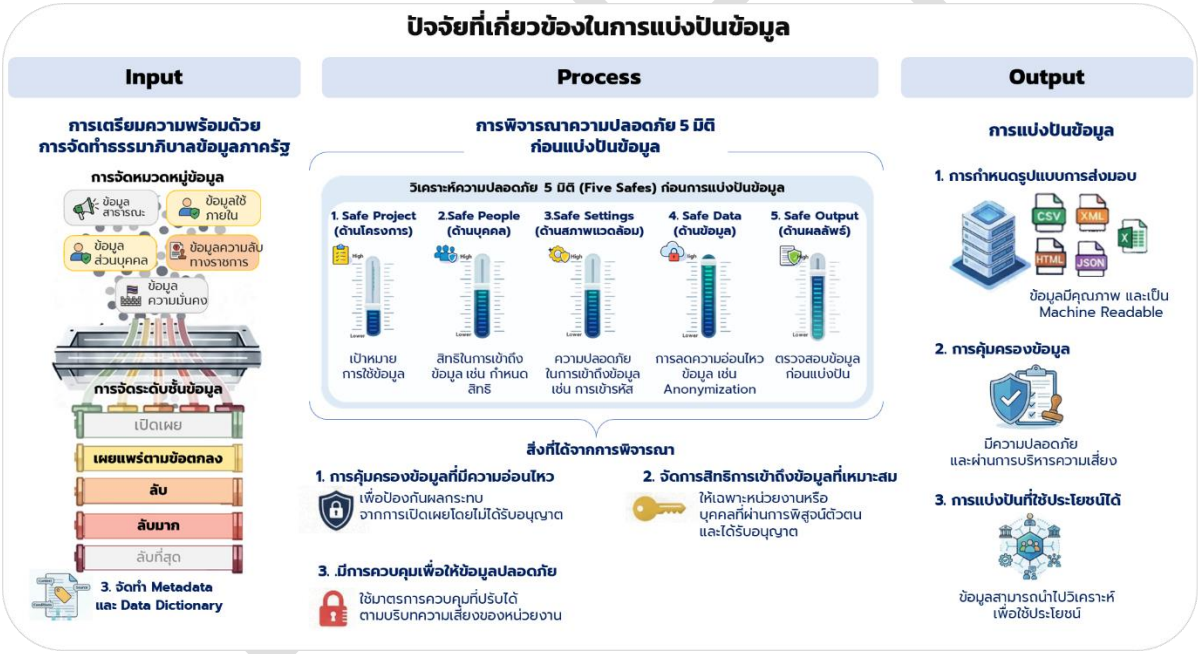
3. แนวปฏิบัติการแบ่งปันข้อมูลภาครัฐ

ในบทที่ 3 จะนำหลักการในหัวข้อที่ 2.2 มาประยุกต์สู่การปฏิบัติจริง โดยกระบวนการแบ่งปันข้อมูลที่ประสบความสำเร็จเป็นผลมาจากการบริหารที่เป็นระบบ ซึ่งประกอบด้วย 3 องค์ประกอบ ได้แก่ ปัจจัยนำเข้า (Input) การเตรียมข้อมูลที่ผ่านการทำธรรมาภิบาลข้อมูลภาครัฐ กระบวนการ (Process) เพื่อจัดการความเสี่ยง และผลผลิต (Output) เพื่อการใช้ประโยชน์จากข้อมูล ดังนี้

ปัจจัยนำเข้า (Input): การจัดทำธรรมาภิบาลข้อมูลภาครัฐ โดยการจัดหมวดหมู่ข้อมูลตามระดับชั้นข้อมูล และการเตรียม Metadata เพื่อให้เข้าใจบริบท แหล่งที่มา และเงื่อนไขการใช้งานข้อมูลได้อย่างถูกต้อง

กระบวนการแบ่งปันข้อมูล (Process - Five Safes): การวิเคราะห์ความเหมาะสมผ่านเกณฑ์ความปลอดภัย 5 ด้าน เพื่อบริหารจัดการความเสี่ยงในทุกมิติก่อนการส่งมอบ เพื่อสร้างความมั่นใจในการแบ่งปัน

ผลลัพธ์ (Output): การส่งมอบข้อมูลที่มีคุณภาพในรูปแบบมาตรฐานที่ตกลงกัน เช่น การส่งข้อมูลในรูปแบบ Machine Readable Data เพื่อให้สามารถนำไปบูรณาการต่อได้ทันที พร้อมทั้งมีกลไกการบริหารจัดการข้อมูลให้เป็นไปตามข้อกำหนด



รูปที่ 7 ปัจจัยที่เกี่ยวข้องในการแบ่งปันข้อมูล

3.1. ประยุกต์ใช้หลักการแบ่งปันข้อมูล

ในหัวข้อนี้จะเป็นแนวทางการประยุกต์หลักการแบ่งปันข้อมูลจากบทที่ 2.2 สู่การปฏิบัติจริงอย่างไร โดยการดำเนินการแบ่งเป็น 2 ส่วนหลัก คือ กิจกรรมภายในหน่วยงานของเจ้าของข้อมูล และกิจกรรมที่เชื่อมโยงกับหน่วยงานภายนอก (ผู้ใช้ข้อมูลที่ต้องการขอใช้ข้อมูล) โดยแบ่งออกเป็น 3 ระยะ ดังนี้

ระยะที่ 1: การเตรียมการก่อนแบ่งปันข้อมูล (Before Sharing) แบ่งได้ 2 กิจกรรม ดังนี้

- **การยื่นคำขอและการประเมินเบื้องต้น:** กระบวนการเริ่มต้นเมื่อผู้ใช้ข้อมูล (Data User) ยื่น "คำขอแบ่งปันข้อมูล" **รายละเอียดสามารถดูได้ที่หัวข้อ 3.2.1** เพื่อใช้เป็นหลักฐานประกอบการพิจารณาของเจ้าของข้อมูลว่าจะอนุมัติการแบ่งปันข้อมูลหรือไม่ โดยครอบคลุมทั้งการขอข้อมูลเพื่อดำเนินโครงการเฉพาะกิจ หรือการขอข้อมูลตามภารกิจหลักของหน่วยงาน *ทั้งนี้ ในระยะเริ่มต้นเพื่อความสะดวกในการประสานงาน ผู้ขอใช้ข้อมูลสามารถดำเนินการกรอกรายละเอียดใน ส่วนที่ 1 และส่วนที่ 2 เพื่อให้เจ้าของข้อมูลพิจารณาในหลักการ ก่อนดำเนินการในขั้นตอนถัดไป*
- **การเตรียมลงนามในเอกสารที่เกี่ยวข้อง:** เมื่อเจ้าของข้อมูลพิจารณาว่า คำขอใช้ข้อมูลนั้นเป็นการขอใช้ข้อมูลที่หน่วยงานมีอยู่ ซึ่งมีความสอดคล้องกับกฎหมายและจำเป็นต่อการปฏิบัติภารกิจตามวัตถุประสงค์ที่ระบุไว้จริง ก็จะพิจารณาเพื่อเตรียมการจัดทำข้อตกลงหรือข้อกำหนดที่เกี่ยวข้องกับการแบ่งปันข้อมูล โดยในทางปฏิบัติ แม้กฎหมายจะไม่ได้กำหนดบังคับให้การแบ่งปันข้อมูลในทุกกรณีต้องจัดทำสัญญาหรือข้อตกลงประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement: DPA) หรือข้อตกลงการแบ่งปันข้อมูล (Data Sharing Agreement: DSA) โดยเสมอไป เพื่อพิจารณาว่าควรมีการทำสัญญาหรือข้อตกลงอย่างไร แต่ในกรณีที่มีการแบ่งปันข้อมูลส่วนบุคคล หน่วยงานควรพิจารณาจัดทำข้อตกลงเป็นลายลักษณ์อักษรเพื่อกำหนดขอบเขตการใช้ข้อมูลให้ชัดเจน พร้อมทั้งกำหนดมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมกับระดับความเสี่ยง ตามบทบัญญัติมาตรา 37(1) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เพื่อป้องกันการนำข้อมูลไปใช้ผิดวัตถุประสงค์ ตัวอย่างข้อตกลงการแบ่งปันข้อมูล **รายละเอียดสามารถดูได้ที่หัวข้อ 3.2.3**

ตารางที่ 6 รูปแบบลักษณะการแบ่งปันข้อมูลและประเภทสัญญา

รูปแบบ	ลักษณะการแบ่งปันข้อมูล	ประเภทสัญญา
หน่วยงานรัฐ กับ **หน่วยงานรัฐ** (เจ้าของข้อมูล/ผู้ควบคุมข้อมูลร่วม)	เป็นการแบ่งปันข้อมูลตามอำนาจหน้าที่ที่กฎหมายกำหนดหรือเพื่อบรรลุเป้าหมายภาระกิจองค์กร	DSA
หน่วยงานรัฐ (เจ้าของข้อมูล/ผู้ควบคุมข้อมูล) กับ **บริษัทเอกชน** (ผู้ประมวลผลข้อมูล)	เป็นการจัดซื้อจัดจ้าง จ้างทำระบบ (Outsource) เพื่อดำเนินการตามคำสั่งของหน่วยงาน	DPA (กฎหมายบังคับ)
หน่วยงานรัฐ กับ **บริษัทเอกชน** (ในฐานะเจ้าของข้อมูล/ผู้ควบคุมข้อมูลร่วม)	เป็นการตกลงร่วมกันในการแบ่งปันและใช้ประโยชน์จากข้อมูลภายใต้วัตถุประสงค์ร่วมกัน	DSA
บริษัทเอกชน (ผู้ใช้ข้อมูล) กับ **หน่วยงานรัฐ** (เจ้าของข้อมูล/ผู้ควบคุมข้อมูลร)	เป็นการส่งข้อมูลตามที่กฎหมายบังคับ หรือตามที่หน่วยงานมีอำนาจเรียกตรวจ	**ไม่มี/MoU**

ระยะที่ 2 การบริหารความเสี่ยงโดยใช้ Five Safes พิจารณาก่อนการแบ่งปันข้อมูล

การแบ่งปันข้อมูลอย่างปลอดภัยจำเป็นต้องอาศัยการตัดสินใจที่เป็นระบบ ดังนั้น ในการพิจารณาเพื่อแบ่งปันข้อมูล เจ้าของข้อมูลจึงต้องพิจารณาความเหมาะสมผ่านการประเมินตามหลักการความปลอดภัย 5 มิติ (Five Safes) ซึ่งประกอบด้วย 1) ด้านโครงการ (Safe Project) 2) ด้านบุคคล (Safe People) 3) ด้านสภาพแวดล้อม (Safe Settings) 4) ด้านข้อมูล (Safe Data) 5) ผลลัพธ์ (Safe Output) *(ที่มา: (Australian Government, 2019))* โดยเจ้าของข้อมูลสามารถใช้ผลการประเมินเป็นตัวช่วยในการตัดสินใจว่า จะดำเนินการแบ่งปันข้อมูลตามกรอบงาน (Standard Approval) หรือควรมีการกำหนดมาตรการควบคุมเพิ่มเติม (Enhanced Controls) ในแต่ละมิติให้สอดคล้องกับบริบทการใช้งานจริง **โดยสามารถดูได้ที่หัวข้อ 3.2.2 รายการตรวจสอบตามมิติ Five Safes ก่อนการแบ่งปันข้อมูล**

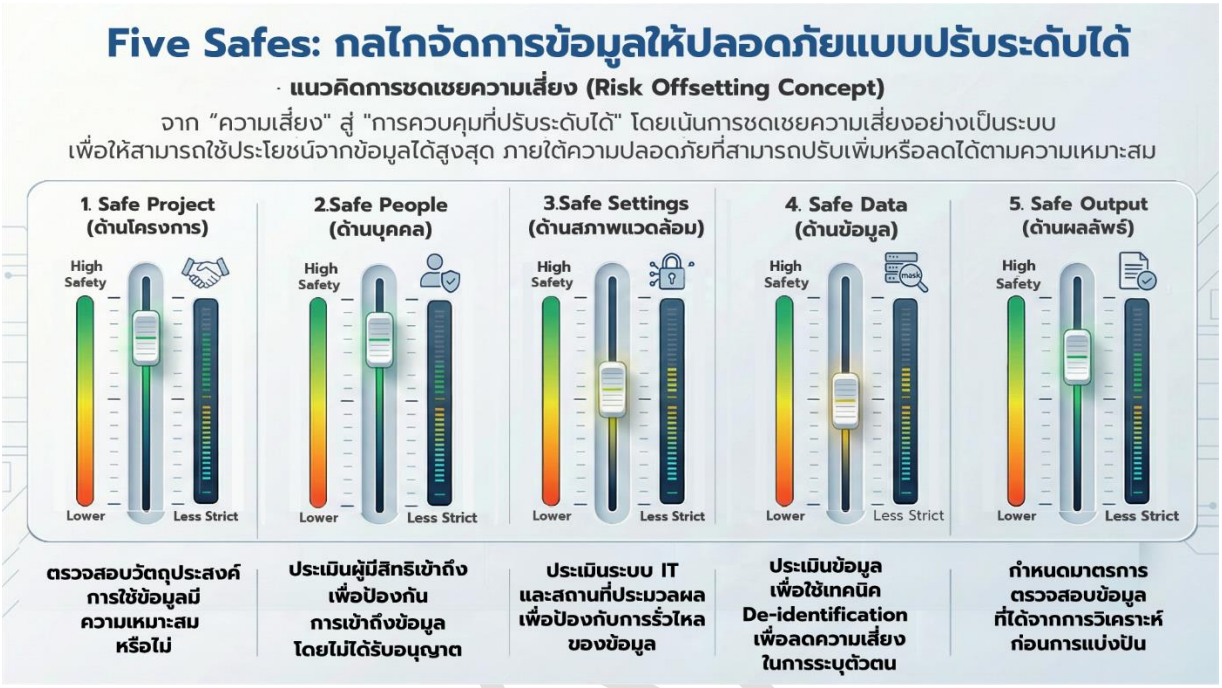
ในเชิงปฏิบัติ ข้อมูลที่สำคัญต่อการวิเคราะห์เชิงลึกมักมีความอ่อนไหวและความเสี่ยงสูงควบคู่กัน หน่วยงานจึงมีการใช้กลไกการบริหารความเสี่ยงที่สามารถปรับระดับได้ตามความเหมาะสม เพื่อสร้างสมดุลระหว่าง "ประโยชน์ที่ได้รับ" และ "ความเสี่ยงที่ยอมรับได้"

รูปที่ 8 การปรับระดับมาตรการควบคุมตามความเหมาะสม

การใช้หลักการ Five Safes ซึ่งเปลี่ยนมิติด้านความปลอดภัยทั้งห้าด้านให้กลายเป็น “กลไกการควบคุมที่ปรับระดับได้” (Adjustable Control Mechanism)แทนที่จะเป็นข้อห้ามในการแบ่งปันข้อมูล โดยให้ความสำคัญกับ “การชดเชยความเสี่ยง” (Risk Offsetting) แทนที่ เข้ามาจัดการอย่างเป็นระบบ เช่น เมื่อหน่วยงานมีความจำเป็นต้องใช้ข้อมูลที่มีความละเอียดสูงและมีความเสี่ยงต่อหน่วยงานหากข้อมูลถูกเปิดเผยโดยไม่ได้รับอนุญาต หน่วยงานจะต้องทำการชดเชยความเสี่ยงด้วยการยกระดับการควบคุมในมิติอื่นให้เข้มงวดขึ้นในระดับสูงสุด ไม่ว่าจะเป็นมิติด้านบุคคล (Safe People) ที่ต้องผ่านการคัดกรองอย่างเข้มงวด หรือมิติด้านสถานที่และระบบจัดเก็บ (Safe Settings) ที่ต้องมีความปลอดภัยสูง เพื่อให้ภาพรวมความเสี่ยงขององค์กรยังคงอยู่ในระดับที่ปลอดภัยตามมาตรฐาน *(ที่มา:* (Stats NZ, 2020; Australian Bureau of Statistics, 2021; UK Data Service, 2026)*)*

ดังนั้น ความสำเร็จของการแบ่งปันข้อมูลจึงไม่ได้ขึ้นอยู่กับการจำกัดสิทธิการเข้าถึงให้เหลือน้อยที่สุด แต่ขึ้นอยู่กับการบริหารความสมดุล (Trade-off) ที่มี ทั้งนี้ การปรับระดับมาตรการควบคุมตามความเหมาะสม

จะช่วยส่งเสริมการแบ่งปันข้อมูล โดยไม่สร้างภาระความเสี่ยงเกินจำเป็น เจ้าของข้อมูลจึงต้องพิจารณาความอ่อนไหวของข้อมูล (Safe Data) และการควบคุมสภาพแวดล้อม (Safe Setting) เพื่อช่วยให้มีการแบ่งปันข้อมูลได้อย่างเหมาะสม *(ที่มา: (Tanvi Desai1, Felix Ritchie2 and Richard Welpton2, 2016))*



รูปที่ 9 การปรับระดับมิติคงวามปลอดภัยตาม Five Safes

ตัวอย่างการทำมาตรการควบคุมตาม Five Safes

เพื่อสนับสนุนการตัดสินใจในการแบ่งปันข้อมูล เจ้าของข้อมูลสามารถเลือกใช้ กลไกการควบคุมที่ปรับระดับได้ (Adjustable Controls) ในแต่ละมิติของ Five Safes ตามบริบทของหน่วยงาน ดังตัวอย่างดังนี้

ตารางที่ 7 ตัวอย่างมาตรการควบคุมตาม Five Safes

มิติ Five Safes	มาตรการควบคุมระดับต่ำ	มาตรการควบคุมระดับระดับปานกลาง	มาตรการควบคุมระดับระดับสูง
โครงการที่ปลอดภัย (Safe Projects)	ไม่จำกัดวัตถุประสงค์ในการใช้งาน สามารถนำไปใช้เพื่อประโยชน์ใดก็ได้	อนุญาตให้ใช้ในโครงการวิเคราะห์ทั่วไปภายในหน่วยงาน หรือโครงการที่มีความเสี่ยงต่ำ	ต้องเป็นโครงการเฉพาะทางที่ได้รับอนุมัติผ่านกระบวนการธรรมาภิบาลที่ตรวจสอบได้ มีเป้าหมายเพื่อประโยชน์สาธารณะที่ชัดเจน หรือเป็นโครงการสำคัญระดับชาติที่มีกฎหมายรองรับ
บุคคลที่ปลอดภัย (Safe People)	สาธารณชนทั่วไปสามารถเข้าถึงได้ทุกคนโดยไม่ต้องลงทะเบียน	จำกัดสิทธิ์เฉพาะเจ้าหน้าที่ภายในหน่วยงานที่เกี่ยวข้องตามบทบาทหน้าที่	จำกัดสิทธิเฉพาะเจ้าหน้าที่ที่ได้รับอนุมัติเป็นกรณีพิเศษ

มิติ Five Safes	มาตรการควบคุมระดับต่ำ	มาตรการควบคุมระดับ ระดับปานกลาง	มาตรการควบคุมระดับ ระดับสูง
			(Approved Government Staff)
สภาพแวดล้อมที่ปลอดภัย (Safe Settings)	เข้าถึงได้จากอินเทอร์เน็ตสาธารณะ หรือจากทุกที่ (Public Cloud/Web)	เข้าถึงได้เฉพาะผ่านเครือข่ายภายใน (Intranet) หรือ VPN ของหน่วยงาน	ข้อมูลจะถูกประมวลผลภายในระบบปิดที่มีความมั่นคงปลอดภัยสูง (Secure Environment/Air-gapped) มีการจำกัดการเข้าถึงทั้งทางกายภาพและไอที รวมถึงมีระบบบันทึกความเคลื่อนไหว (Audit Log) อย่างละเอียด
ข้อมูลที่ปลอดภัย (Safe Data)	ข้อมูลมีความละเอียดสูงหรือเป็นข้อมูลดิบ (Raw Data)[2] เพื่อรักษาคุณค่าสำหรับการวิเคราะห์ที่แม่นยำที่สุด	ข้อมูลที่ไม่มีการใช้ประโยชน์หรือข้อมูลที่มีความอ่อนไหวจะถูกทำเป็นข้อมูลนิรนามบางส่วน (Data Masking) หรือแทนที่ค่าจริงด้วยรหัส (Pseudonymization) เพื่อลดความเสี่ยง	ข้อมูลถูกลดความอ่อนไหวจนไม่สามารถระบุตัวตนได้ (Anonymization) หรือเป็นข้อมูลสถิติภาพรวม (Aggregated) โดยไม่มีข้อมูลส่วนบุคคลหรือข้อมูลอ่อนไหว
ผลลัพธ์ที่ปลอดภัย (Safe Outputs)	ผลลัพธ์สามารถนำไปเผยแพร่ได้ทันทีโดยไม่ต้องผ่านการคัดกรอง	มีกระบวนการตรวจสอบความถูกต้องและตรวจสอบผลลัพธ์เบื้องต้นก่อนนำไปใช้งาน	ใช้แนวทางการตรวจสอบข้อมูลเพื่อรักษาความปลอดภัยในระดับหน่วยข้อมูล ไม่ให้ข้อมูลมีการเชื่อมโยงกลับไปที่ข้อมูลส่วนบุคคล

จากตารางมาตรการข้างต้น เจ้าของข้อมูลสามารถนำเกณฑ์การควบคุมในแต่ละมิติมาประยุกต์ใช้และปรับให้สอดคล้องกับบริบทความเสี่ยงและความอ่อนไหวของข้อมูลแต่ละประเภท โดยยึดหลักการว่า **“ความปลอดภัยที่สมบูรณ์ไม่ได้เกิดจากการกำหนดระดับการควบคุมสูงสุดในทุกมิติ แต่เกิดจากการจัดระดับการควบคุมความเสี่ยงให้มีความสมดุลและเหมาะสม”** ตามหลักธรรมาภิบาลข้อมูลภาครัฐ โดยหน่วยงานควรพิจารณาเลือกใช้เฉพาะมาตรการที่สอดคล้องและเหมาะสมตามบริบทของหน่วยงาน (*ที่มา: (UK Data Service, 2026)*) ซึ่งมีตัวอย่างดังนี้

- **ข้อมูลระดับชั้นเผยแพร่ตามข้อตกลง:** มุ่งเน้นการลดความเสี่ยงที่ข้อมูลโดยตรง โดยยกระดับมาตรการด้านข้อมูล (Safe Data) และด้านผลลัพธ์ (Safe Outputs) ให้มีความปลอดภัยสูง เช่น การทำข้อมูลนิรนาม (Anonymization) ที่มีการตรวจสอบ โดยควบคุมที่เข้มงวดในมิติ

[2] ข้อมูลในรูปแบบที่ได้รับมาโดยตรงจากที่แหล่งกำเนิด ก่อนที่จะผ่านกระบวนการจัดการหรือการประมวลผลใดๆ ในลำดับถัดมา จาก ISO 5127:2017 - Information and documentation

ดังกล่าว ช่วยให้สามารถผ่อนปรนมาตรการด้านโครงการ (Safe Project) เป็นระดับต่ำ โดยด้านบุคคล (Safe People) และด้านสภาพแวดล้อม (Safe Settings) เป็นระดับปานกลาง ได้ เนื่องจากข้อมูลมีความเสี่ยงที่ลดต่ำแล้ว

- **ข้อมูลระดับชั้นลับ:** มุ่งเน้นการสร้างความสมดุลระหว่างการเข้าถึงข้อมูลและความมั่นคงปลอดภัย ในกรณีที่มีการใช้ข้อมูลที่มีความละเอียดมากขึ้น มาตรการด้านข้อมูล (Safe Data) และด้านสภาพแวดล้อม (Safe Settings) จะถูกกำหนดไว้ในระดับปานกลาง โดยต้องชดเชยความเสี่ยงด้วยการยกระดับมาตรการด้านโครงการ (Safe Project) ด้านบุคคล (Safe People) และด้านผลลัพธ์ (Safe Outputs) ให้เป็นระดับสูง เพื่อควบคุมขอบเขตการใช้งานและตัวบุคคลผู้เข้าถึงข้อมูลอย่างเคร่งครัด
- **ข้อมูลระดับชั้นลับมาก:** ในกรณีที่มีความจำเป็นต้องใช้ข้อมูลดิบหรือข้อมูลที่มีความอ่อนไหวสูงมาก ซึ่งส่งผลให้มาตรการด้านข้อมูล (Safe Data) อยู่ในระดับต่ำ (ข้อมูลมีความเสี่ยงสูง) และด้านผลลัพธ์ (Safe Outputs) อยู่ในระดับปานกลาง จึงควรชดเชยความเสี่ยงด้วยการยกระดับมาตรการในมิติอื่นสู่ระดับสูงสุด (High Control) เช่น ด้านโครงการ (Safe Project) ที่ต้องกำหนดระยะเวลาและขอบเขตที่ชัดเจน ด้านบุคคล (Safe People) ที่ต้องผ่านการคัดกรองขั้นสูงสุด และด้านสภาพแวดล้อม (Safe Settings) ที่ต้องใช้เทคโนโลยีการเข้ารหัสข้อมูล (Encryption) พร้อมช่องทางส่งมอบที่ปิดสนิท เพื่อรักษามาตรฐานความปลอดภัยในภาพรวม

มิติ five Safes / ระดับชั้นข้อมูล	SafeProjects	Safe People	Safe Settings	Safe Data	Safe Outputs
เผยแพร่ตามข้อตกลง	ต่ำ	ปานกลาง	ปานกลาง	สูง	สูง
ลับ	สูง	สูง	ปานกลาง	ปานกลาง	ปานกลาง
ลับมาก	สูง	สูง	สูง	ต่ำ	ปานกลาง

รูปที่ 10 ตัวอย่างการปรับมาตรการการควบคุมความปลอดภัย Five Safes ตามระดับชั้นข้อมูล

โดยสามารถปรับเลือก Five Safes ให้เหมาะสมกับชุดข้อมูลได้ดังรูปดังต่อไปนี้

รูปที่ 11 ตัวอย่างการปรับมาตรการการควบคุม Five Safes

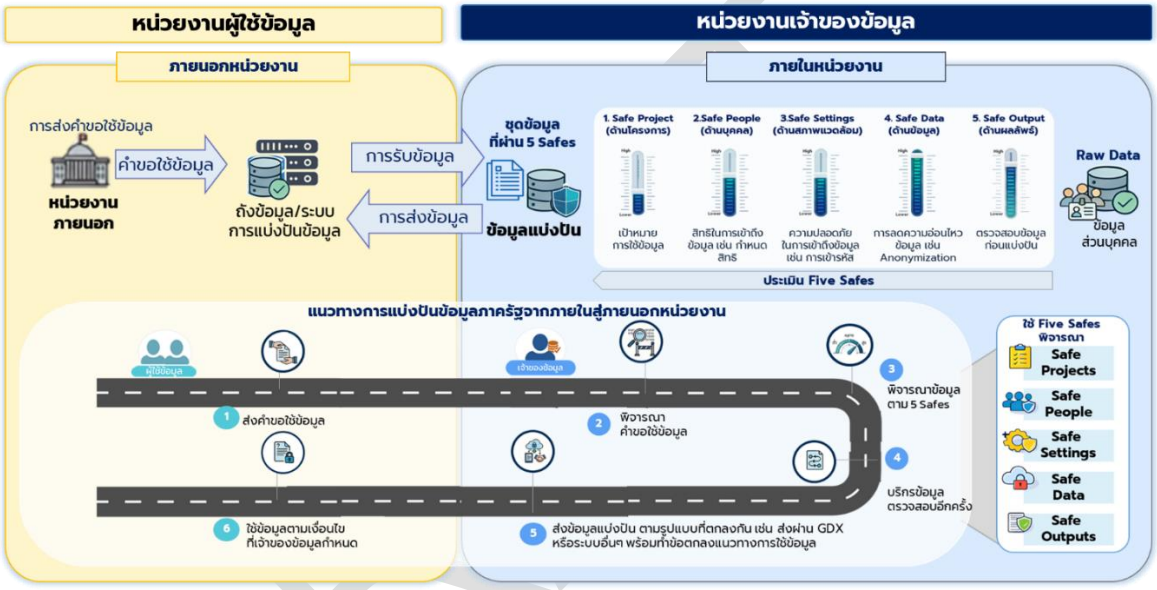
ทั้งนี้ หลังจากที่ข้อมูลได้ถูกแบ่งปันและนำไปใช้ภายใต้กรอบของหลักการทั้งห้าแล้วกระบวนการยังไม่สิ้นสุด แต่ต้องมีการกำกับดูแลอย่างต่อเนื่องตามวงจรชีวิตข้อมูล และควรมีการทบทวนหลักการ Five Safes ตามรอบการทบทวน หรือเมื่อมีการเปลี่ยนแปลงต่อการดำเนินการที่เกี่ยวข้องกับข้อมูลอย่างมีนัยสำคัญ

ระยะที่ 3 การแบ่งปันข้อมูล

หลังจากเจ้าของข้อมูล (Data Owner) ได้นำหลักการ Five Safes มาพิจารณาแล้ว ประกอบกับทีมบริกรได้มีการตรวจสอบว่าข้อมูลมีความปลอดภัยเพียงพอที่จะแบ่งปันได้ เจ้าของข้อมูลจะทำการ:

- **การแบ่งปันข้อมูล:** เมื่อข้อมูลดังกล่าวผ่านการพิจารณาทั้ง 5 ด้านตาม**รายการตรวจสอบตามมิติ Five Safes ที่กำหนดในหัวข้อ 3.2.2 เรียบร้อยแล้ว** ให้มีการดำเนินการดังนี้
  - เจ้าของข้อมูลนำผลที่ได้จากการนำผล**รายการตรวจสอบตามมิติ Five Safes** เพื่อกำหนดแนวทางและเงื่อนไขการแบ่งปันข้อมูล ซึ่งอาจเป็นข้อกำหนดแนวทางการใช้ข้อมูล หรือข้อตกลงหรือสัญญาที่จะใช้เพื่อแบ่งปันข้อมูล เพื่อให้หน่วยงานผู้ใช้ข้อมูลมีหลักเกณฑ์การปฏิบัติที่ชัดเจนและสอดคล้องกับมาตรฐานความมั่นคงปลอดภัยที่กำหนดไว้รูปธรรม
  - **กำหนดการปฏิบัติตามเงื่อนไข:** การทำข้อตกลงหรือสัญญาการแบ่งปันข้อมูลโดยผู้ใช้ข้อมูลมีหน้าที่รับผิดชอบในการปฏิบัติหน้าที่ตามเงื่อนไขการใช้งาน รักษาความลับ และดูแลความปลอดภัยของข้อมูล,กำหนดไว้ในข้อตกลง รวมถึงการทำลายข้อมูลเมื่อสิ้นสุดการแบ่งปันข้อมูล

- **การส่งมอบข้อมูลและช่องทางการเข้าถึง (Data Delivery & Access):** เมื่อผ่านการตรวจสอบทุกขั้นตอน ข้อมูลจะถูกส่งมอบให้แก่หน่วยงานผู้ใช้ข้อมูล (Data User) ผ่านช่องทางที่เหมาะสม ดังนี้
  - **กำหนดช่องทางการแบ่งปันข้อมูล:** การกำหนดแพลตฟอร์มเพื่อแบ่งปันข้อมูล เช่น ศูนย์แลกเปลี่ยนข้อมูลกลาง (GDX) หรือแพลตฟอร์มกลางในการแลกเปลี่ยนข้อมูลที่มีมาตรฐาน
  - **ส่งมอบในรูปแบบที่ตกลงกัน:** เช่น รูปแบบ Machine Readable Data เพื่อให้ผู้ใช้สามารถนำไปบูรณาการต่อได้



รูปที่ 12 แนวทางการแบ่งปันข้อมูลภาครัฐจากภายในสู่ภายนอกหน่วยงาน

3.2. เครื่องมือที่ช่วยในการแบ่งปันข้อมูล

ในหัวข้อ 3.2 จะกล่าวถึงเครื่องมือเพื่อช่วยในการแบ่งปันข้อมูลภาครัฐ หน่วยงานสามารถนำเครื่องมือไปประยุกต์สู่การแบ่งปันข้อมูลได้ดังนี้

3.2.1. ตัวอย่างคำขอแบ่งปันข้อมูล (Data Request Form)

แบบฟอร์มนี้จัดทำขึ้นสำหรับผู้ขอใช้ข้อมูล เพื่อใช้เป็นเอกสารแสดงความประสงค์ในการเข้าถึงและใช้ประโยชน์จากชุดข้อมูลอย่างเป็นทางการ โดยประยุกต์จาก Australian Capital Territory Government ซึ่งมีวัตถุประสงค์หลักเพื่อจัดเก็บข้อมูลพื้นฐานของผู้ใช้ข้อมูล ตลอดจนรายละเอียดเชิงลึกเกี่ยวกับวัตถุประสงค์และลักษณะของข้อมูลที่ต้องการ ข้อมูลดังกล่าวจะถูกใช้เป็นฐานข้อมูลสำคัญสำหรับเจ้าของข้อมูล (Data Owner) ในการประเมินความพร้อมและความเหมาะสมก่อนการแบ่งปันข้อมูลต่อไป

ทั้งนี้ เพื่อความสะดวกในระยะเริ่มต้น ผู้ขอใช้ข้อมูลสามารถดำเนินการกรอกรายละเอียดในส่วนที่ 1 และส่วนที่ 2 เพื่อให้เจ้าของข้อมูลพิจารณาในหลักการเบื้องต้น หากผลการพิจารณาเห็นสมควรให้มีการแบ่งปันข้อมูล ผู้ขอใช้ข้อมูลจึงดำเนินการกรอกรายละเอียดเพิ่มเติมใน ส่วนที่ 3 และส่วนที่ 4 เพื่อใช้เป็นหลักฐานประกอบการดำเนินการตามขั้นตอนต่อไป

ส่วนที่ 1: ข้อมูลผู้ขอใช้ข้อมูล (Applicant Information)
ชื่อ-นามสกุล: ..... ตำแหน่ง/บทบาท: ..... องค์กร/หน่วยงาน: .....ข้อมูลติดต่อ: .....
ส่วนที่ 2: วัตถุประสงค์การใช้ข้อมูล
2.1) รายละเอียดด้านโครงการ (Project) - เพื่อประเมินวัตถุประสงค์และความเหมาะสมของการนำข้อมูลไปใช้ • ชื่อโครงการที่นำข้อมูลไปใช้ประโยชน์: ..... • ชุดข้อมูลที่ต้องการ (Data Requested): (โปรดระบุชื่อชุดข้อมูล ตัวแปร (Variables) หรือรายละเอียดให้เฉพาะเจาะจงที่สุด) o ..... o ..... o ..... • รายละเอียดโครงการโดยสังเขป (Project Summary): o ..... o ..... o ..... • วัตถุประสงค์การใช้ข้อมูล (Purpose): o การวางแผน/กำหนดนโยบาย (Policy/Planning) o การวิจัยทางวิชาการ (Academic Research) o การใช้ประโยชน์เพื่อบริการประชาชน (โปรดระบุรายละเอียดเพิ่มเติม)อื่นๆ: ....

- การดำเนินการตามโครงการมีกฎหมายกำหนดไว้หรือไม่
  - มี (โปรดระบุ)
  - ไม่มี
- การเชื่อมโยงข้อมูล: มีการนำไปเชื่อมโยงกับชุดข้อมูลอื่นหรือไม่? (หากมี โปรดระบุรายละเอียด)
  - มี (โปรดระบุ) .....
  - ไม่มี
- การเผยแพร่: ข้อมูลจะถูกทำซ้ำ เผยแพร่ หรือเปิดเผยต่อบุคคลที่สามหรือไม่?
  - มี (โปรดระบุ) .....
  - ไม่มี
- รูปแบบการแบ่งปันข้อมูลเป็นอย่างไร
  - การแบ่งปันข้อมูลอย่างเป็นระบบ (Systematic Data Sharing)
  - การแบ่งปันข้อมูลเพียงครั้งเดียว (One-off Disclosures)
- การรับรองและการอนุมัติ (Approvals): โครงการของท่านได้รับการอนุมัติจากหน่วยงานหรือไม่ (โปรดแนบหลักฐาน): .....

ส่วนที่ 3: รายละเอียดการใช้ข้อมูล

3.1) รายละเอียดด้านบุคลากร (People) - เพื่อประเมินว่าผู้ที่จะเข้าถึงข้อมูลมีทักษะและความน่าเชื่อถือเพียงพอ

- รายชื่อผู้มีสิทธิเข้าถึงข้อมูล (Authorized Users) (โปรดระบุรายชื่อทุกคนที่จะมีส่วนร่วมในการประมวลผลข้อมูลชุดนี้)
- ผู้เข้าถึงข้อมูลมีความรู้ความเข้าใจต่อการจัดการข้อมูลใช่หรือไม่
  - ใช่
  - ไม่ใช่

3.2) รายละเอียดสภาพแวดล้อม (Settings) - เพื่อยืนยันว่าผู้ขอใช้ข้อมูลมีระบบการจัดเก็บข้อมูลที่ปลอดภัยเพียงพอ

- **วิธีการจัดเก็บและป้องกันข้อมูล (Data Storage & Security):** ***(เลือกได้มากกว่า 1 ข้อ)***
  - การเข้ารหัสข้อมูล (Encryption)
  - การยืนยันตัวตนหลายขั้นตอน (Multi-factor authentication)
  - การจำกัดสิทธิ์เข้าถึงเฉพาะบุคคลที่ระบุชื่อ (Access Control)
  - เก็บในเครื่องคอมพิวเตอร์ที่ไม่มีการเชื่อมต่อเครือข่าย (Standalone PC)
- สถานที่ประมวลผลข้อมูล:
  - Cloud ของหน่วยงาน, Server ภายใน
  - Laptop ส่วนตัว
  - ระบบปิดที่มีความมั่นคงปลอดภัยสูง
- ช่องทางการรับส่งข้อมูล:
  - Secure FTP / SFTP
  - Hand-carry (Encrypted Drive / External Hard Drive)
  - API (โปรดระบุชื่อระบบ): .....

- Cloud Storage (เช่น Government Cloud, OneDrive หน่วยงาน)
- อื่นๆ (โปรดระบุ): .....

- **การบริหารจัดการข้อมูลหลังจบโครงการ (Retention & Disposal): เมื่อสิ้นสุดโครงการ ท่านจะดำเนินการกับข้อมูลอย่างไร:**
  - ทำลายข้อมูลทันที (Destroy) พร้อมส่งหนังสือยืนยันการทำลาย
  - ขอเก็บรักษาต่อ (Retain) เป็นเวลา ..... ปี (โปรดระบุเหตุผลความจำเป็น) .....

3.3) ข้อมูลที่ขอ - เพื่อระบุขอบเขตข้อมูลให้ชัดเจนและลดความเสี่ยงในการเปิดเผยข้อมูลเกินความจำเป็น

- **รูปแบบข้อมูลที่ต้องการ**
  - ข้อมูลส่วนบุคคลที่ระบุตัวตนได้ (Identifiable Data) (ต้องมีเหตุผลความจำเป็นทางกฎหมายรองรับ) *(ควรทำข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล (Personal Data Sharing Agreement) รายยละเอียดดูได้ที่หัวข้อ 3.2.3)*
  - ข้อมูลระดับบุคคลที่ปิดบังตัวตนแล้ว (De-identified Individual-level Data) *(ควรทำข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล (Personal Data Sharing Agreement) รายยละเอียดดูได้ที่หัวข้อ 3.2.3)*
  - ข้อมูลสรุป/สถิติภาพรวม (Aggregate/Summary Data)
- **ช่วงเวลาของข้อมูล (Time Period):** ตั้งแต่ (วว/ดด/ปปปป): ..... ถึง (วว/ดด/ปปปป): .....
- **การเชื่อมโยงข้อมูล (Data Linkage):** ท่านมีความประสงค์จะนำข้อมูลนี้ไปเชื่อมโยงกับฐานข้อมูลอื่นภายนอกหรือไม่? ☐ ไม่ต้องการ ☐ ต้องการ (โปรดระบุฐานข้อมูลที่จะนำไปเชื่อมโยง): .....

3.4) ผลลัพธ์และการเผยแพร่ (Outputs) - เพื่อควบคุมการนำเสนอผลงานสู่สาธารณะ

- **รูปแบบผลลัพธ์ที่จะเกิดขึ้น (Project Outputs):**
  - รายงานวิจัย/บทความตีพิมพ์ (Research Paper)
  - รายงานภายในองค์กร (Internal Report)
  - เว็บไซต์/Dashboard สาธารณะ
  - บริการภาครัฐ
- **การตรวจสอบก่อนเผยแพร่ (Output Review / No Surprises Period):**
  ท่านยินยอมที่จะส่งร่างผลงานให้หน่วยงานเจ้าของข้อมูลตรวจสอบความเสี่ยงในการระบุตัวตน (Re-identification Risk) ก่อนการเผยแพร่หรือไม่?
  - ยินยอม (ยอมรับเงื่อนไขการส่งตรวจสอบล่วงหน้า เช่น 30 วัน)
  - ไม่ยินยอม

ส่วนที่ 4: เงื่อนไขการขอใช้ข้อมูล

- ผู้ขอใช้ข้อมูลตกลงที่จะปฏิบัติตามข้อกำหนดของหน่วยงานเจ้าของข้อมูล และจะไม่ส่งต่อข้อมูลให้บุคคลที่สามที่ไม่ได้ระบุไว้ในแบบคำขอนี้ โดยจะปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลและระเบียบที่เกี่ยวข้องอย่างเคร่งครัด และยินยอมรับบทลงโทษหากมีการละเมิดข้อกำหนดของหน่วยงานเจ้าของข้อมูล
  - ตกลง

1

3.2.2. รายการตรวจสอบตามหลักการความปลอดภัย 5 มิติ (Five Safes) ก่อนการแบ่งปันข้อมูล

เครื่องมือนี้สำหรับเจ้าของข้อมูล เพื่อประเมินความพร้อมและระดับความมั่นคงปลอดภัยก่อนดำเนินการแบ่งปันข้อมูล โดยแบบตรวจสอบจะครอบคลุมมิติด้านความปลอดภัยทั้ง 5 ด้าน (Five Safes) ซึ่งประยุกต์จาก Australian Government, 2019 และ Australian Capital Territory Government เพื่อช่วยให้เจ้าของข้อมูล (Data Owner) สามารถวิเคราะห์ระดับมาตรการควบคุมที่จำเป็นได้ และสามารถใช้เป็นข้อกำหนดสำคัญเพื่อให้แบ่งปันข้อมูลมีความปลอดภัย รายละเอียดมีดังนี้

รายการคำถาม		จำเป็นต้องมีหรือไม่ (ตอบ มี / ไม่มี)
1. Safe Projects (โครงการปลอดภัย)		
1.1	มีวัตถุประสงค์ในการใช้ข้อมูลที่ชัดเจนและเป็นลายลักษณ์อักษรหรือไม่?	
1.2	โครงการที่ต้องการนำข้อมูลไปใช้งานมีกฎหมายรองรับการดำเนินการหรือไม่?	
1.3	โครงการนี้สอดคล้องกับภารกิจของหน่วยงาน และมุ่งพัฒนาระบบการให้บริการภาครัฐให้มีประสิทธิภาพยิ่งขึ้นหรือไม่?	
1.4	ต้องมีกระบวนการเพื่อประเมิน ติดตาม และควบคุมดูแลโครงการหรือไม่?	
2. Safe People (บุคคลปลอดภัย)		
2.1	มีการคัดกรองและพิจารณาอนุญาตผู้เข้าถึงข้อมูลตามลำดับชั้นความลับและหน้าที่ (Need-to-know basis) ที่ชัดเจนหรือไม่?	
2.2	ต้องมีการจัดทำข้อตกลงหรือพันธสัญญาที่มีผลผูกพันทางกฎหมายกับผู้ใช้ข้อมูล เพื่อควบคุมการใช้ข้อมูลหรือไม่?	
2.3	ผู้ใช้ข้อมูลต้องผ่านการฝึกอบรมด้านการใช้งานข้อมูลอย่างปลอดภัย หรือต้องมีทักษะทางเทคนิคที่จำเป็นหรือไม่?	
2.4	มีการกำหนดบทลงโทษทั้งทางกฎหมายและวินัย/ปกครอง สำหรับการใช้งานข้อมูลผิดวัตถุประสงค์หรือไม่?	
3. Safe Settings (สภาพแวดล้อมปลอดภัย)		
3.1	มีการกำหนดวิธีการแบ่งปันข้อมูลหรือรูปแบบไฟล์หรือไม่? เช่น ข้อมูลจะถูกส่งในรูปแบบไฟล์รูปแบบที่อ่านได้ด้วยเครื่อง เช่น .xls, .csv, .rdf เป็นต้น หรือจะมีการให้สิทธิ์เข้าถึงข้อมูลโดยตรง (Direct access) หรือไม่?	
3.2	มีการกำหนดสถานที่ทางกายภาพและระบบดิจิทัลที่ใช้จัดเก็บและเข้าถึงข้อมูลอย่างปลอดภัยและมีการควบคุมหรือไม่?	
3.3	มีระบบบันทึกเหตุการณ์ (Audit Logs) เพื่อติดตามการเข้าถึงและการเคลื่อนย้ายข้อมูลเข้า-ออกสภาพแวดล้อมที่ได้รับอนุญาตอย่างต่อเนื่องหรือไม่?	
3.4	สภาพแวดล้อมการทำงานสอดคล้องกับมาตรฐานความมั่นคงปลอดภัยสารสนเทศ (เช่น ISO 27001 หรือ ISMS) หรือไม่?	

	รายการคำถาม	จำเป็นต้องมีหรือไม่ (ตอบ มี / ไม่มี)
4. Safe Data (ข้อมูลปลอดภัย)		
4.1	ข้อมูลที่จะแบ่งปันมีการคัดเลือกเฉพาะข้อมูลที่จำเป็นและสอดคล้องกับวัตถุประสงค์การดำเนินงานเท่านั้นหรือไม่?	
4.2	มีการคัดแยกหรือจัดการข้อมูลที่มีความละเอียดอ่อนสูง (เช่น ตำแหน่งทรัพยากรธรรมชาติที่สำคัญ) เพื่อป้องกันความเสี่ยงที่เจาะจงหรือไม่?	
4.3	มีการดำเนินการทำข้อมูลนิรนาม (Anonymization) หรือการใช้นามแฝง (Pseudonymization) กับข้อมูลส่วนบุคคลหรือข้อมูลอ่อนไหวในส่วนที่ไม่ได้ใช้งานหรือไม่?	
4.4	มีการประเมินและมาตรการป้องกันความเสี่ยงในการเชื่อมโยงข้อมูล (Data Linkage) กับฐานข้อมูลอื่นในระบบ เพื่อป้องกันการระบุตัวตนย้อนกลับ (Re-identification) หรือไม่?	
5. Safe Outputs (ผลลัพธ์ปลอดภัย)		
5.1	การควบคุมช่วยลดความเสี่ยงในการแบ่งปันข้อมูลส่วนบุคคลหรือไม่?	
5.2	มีการตรวจสอบเพื่อพิจารณาความอ่อนไหวของข้อมูล เช่น ข้อมูลไม่สามารถย้อนกลับตัวตนได้หรือไม่?	
5.3	จำเป็นต้องตรวจสอบและอนุมัติผลลัพธ์ก่อนที่จะเปิดเผยต่อกลุ่มเป้าหมายที่กว้างขึ้นหรือไม่?	
5.4	หากผลลัพธ์ที่ได้จะมีการแบ่งปันให้บุคคลที่สาม จะต้องมีการทำข้อตกลงฉบับใหม่หรือไม่?	

1

3.2.3. ตัวอย่างข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล (Personal Data Sharing Agreement)

ในกรณีที่มี**การแบ่งปันข้อมูลส่วนบุคคล** หน่วยงานควรพิจารณาจัดทำข้อตกลงเป็นลายลักษณ์อักษรเพื่อกำหนดขอบเขตการใช้ข้อมูลให้ชัดเจน พร้อมทั้งกำหนดมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมกับระดับความเสี่ยง ตามบทบัญญัติมาตรา 37(1) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เพื่อป้องกันการนำข้อมูลไปใช้ผิดวัตถุประสงค์

โดยการจัดทำข้อตกลงการแบ่งปันข้อมูล (DSA) ไม่ใช่ข้อบังคับทางกฎหมายในทุกกรณี แต่ควรพิจารณาตามความเหมาะสมโดยอ้างอิงจาก **"แนวปฏิบัติพื้นฐานด้านการคุ้มครองข้อมูลส่วนบุคคล (ภาคส่วนทั่วไป)"** ของสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ซึ่งสรุปได้ว่า

1. **กรณีการแบ่งปันข้อมูลตามอำนาจหน้าที่** ให้ใช้ข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล (DSA) โดยใช้เมื่อหน่วยงานต่างฝ่ายต่างต้องการแบ่งปันข้อมูล เพื่อปฏิบัติงานตามภารกิจของตนเอง ทั้งนี้ การจัดทำ DSA ไม่ใช่ข้อบังคับทางกฎหมายในทุกกรณี แต่ควรพิจารณาทำเมื่อข้อมูลส่วนบุคคลที่มีความเสี่ยงสูงหรือมีปริมาณมากเพื่อบริหารจัดการความเสี่ยงตามมาตรา 37(1)
2. **กรณีการมอบหมายให้ประมวลผลข้อมูล** ให้ใช้สัญญาการประมวลผลข้อมูล โดยใช้เมื่อส่งมอบข้อมูลให้หน่วยงานอื่นหรือเอกชนดำเนินการแทนตามคำสั่ง ซึ่งตามมาตรา 40 บังคับว่าต้องจัดทำข้อตกลงเป็นลายลักษณ์อักษร เพื่อควบคุมขอบเขตการใช้งานให้มีมาตรฐานและปลอดภัย

รูปที่ 13 รูปแบบลักษณะการแบ่งปันข้อมูลและประเภทสัญญา

ทั้งนี้ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลได้ระบุโครงสร้างและหัวข้อมาตรฐานที่ควรมีในข้อตกลงเหล่านี้ไว้ในแนวปฏิบัติฯ โดยท่านสามารถดูตัวอย่างรายละเอียดได้ที่ https://dg.th/v7xrkubh84 หรือ แสกน QR Code

https://dg.th/v7xrkubh84

บรรณานุกรม

Australian Bureau of Statistics. (2021). *Five Safes Framework*. Retrieved from https://www.abs.gov.au/about/data-services/data-confidentiality-guide/five-safes-framework

Australian Capital Territory Government. (n.d.). *Data sharing agreement* .

Australian Government. (2019). *Best Practice Guide to Applying Data Sharing Principles* . Australian.

Canada, S. (2025). *Access to microdata: Application process and guidelines*. Retrieved from https://www.statcan.gc.ca/en/microdata/data-centres/access.

Precision Health Research, S. (2026). *National precision medicine strategy: Transforming healthcare through data and genomics*. Retrieved from https://www.npm.sg.

Singapore, M. o. (2026). *Improving health outcomes through trusted data exchange*. Retrieved from https://trustplatform.sg.

Stats NZ. (2017). *Integrated Data Infrastructure: A guide to the IDI*. Retrieved from https://www.stats.govt.nz/integrated-data/integrated-data-infrastructure/.

Stats NZ. (2020). *Integrated Data Infrastructure: Overarching privacy impact assessment (6th ed.)*. Retrieved from https://www.stats.govt.nz/privacy-impact-assessments/integrated-data-infrastructure-overarching-privacy-impact-assessment-6th-edition.

Tanvi Desai1, Felix Ritchie2 and Richard Welpton2. (2016). *Five Safes: Designing data access for research.* Bristol, England, UK: University of the West of England, Bristol Series: Economics Working Paper Series (1601). Retrieved from https://www2.uwe.ac.uk/faculties/BBS/Documents/1601.pdf

UK Data Service. (2026). *The Five Safes Framework: A guide to data privacy and secure access*. Retrieved from https://ukdataservice.ac.uk/help/secure-lab/five-safes/.

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล. (2026, 2 10). *ขอหารือเกี่ยวกับการแลกเปลี่ยนข้อมูลผู้ป่วยจิตเวชและยาเสพติดที่มีความเสี่ยงสูงต่อการก่อความรุนแรง เพื่อความปลอดภัยของผู้ป่วย ผู้อื่นและสาธารณชน*. Retrieved from https://www.pdpc.or.th/wp-content/uploads/2026/02/consultation-65.pdf.

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล. (2568). *แนวปฏิบัติพื้นฐานด้านการคุ้มครองข้อมูลส่วนบุคคล (ภาคส่วนทั่วไป)*. Retrieved from https://www.pdpc.or.th/pdpc-book/%e0%b9%81%e0%b8%99%e0%b8%a7%e0%b8%9b%e0%b8%8f%e0%b8%b4

%e0%b8%9a%e0%b8%b1%e0%b8%95%e0%b8%b4%e0%b8%9e%e0%b8%b7%e0%b9%89%e0%b8%99%e0%b8%90%e0%b8%b2%e0%b8%99%e0%b8%94%e0%b9%89%e0%b8%b2%e0%b8%99%e0%b8%81/.

สำนักงานปลัดกระทรวงยุติธรรม. (2021). *ศูนย์แลกเปลี่ยนข้อมูลกระบวนการยุติธรรม (Data Exchange Center: DXC).* Retrieved from https://www.dxc.go.th/wp-content/uploads/2021/09/DXC-E-book-Final.pdf.

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน). (2021). *แผนพัฒนารัฐบาลดิจิทัลของประเทศไทย พ.ศ. 2566 – 2570.* 2566. Retrieved from https://satoricyber.com/data-masking/data-anonymization-use-cases-and-6-common-techniques/.