ข้อมูลใช้ภายใน
สพร./CDV
มกราคม 2569

มาตรฐานรัฐบาลดิจิทัลอยู่ระหว่างการจัดทำ
ห้ามใช้หรือยึดร่างนี้เป็นมาตรฐาน

มาตรฐานรัฐบาลดิจิทัลฉบับสมบูรณ์จะมีประกาศโดย
คณะกรรมการพัฒนารัฐบาลดิจิทัล

ร่าง
มาตรฐานรัฐบาลดิจิทัล
Digital Government Standard

ว่าด้วยหลักเกณฑ์การจัดระดับชั้นข้อมูลภาครัฐ
Government Data Classification Framework

สำหรับเวียนขอข้อคิดเห็นจากหน่วยงานต่างๆ ที่เกี่ยวข้อง

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
เลขที่ 999 ชั้น 4 สถาบันเพื่อการยุติธรรมแห่งประเทศไทย ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210
หมายเลขโทรศัพท์: 0 2612 6000 โทรสาร: 0 2612 6011

มาตรฐานรัฐบาลดิจิทัล

Digital Government Standard

มรด. X : 256X

DGS X : 256X

ว่าด้วยหลักเกณฑ์การจัดระดับชั้นข้อมูลภาครัฐ

GOVERNMENT DATA CLASSIFICATION FRAMEWORK

เวอร์ชัน 1.0

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

สำนักนายกรัฐมนตรี

มาตรฐานรัฐบาลดิจิทัล
ว่าด้วยหลักเกณฑ์การจัดระดับชั้นข้อมูลภาครัฐ

มรด. X : 256X

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

เลขที่ 999 ชั้น 4 สถาบันเพื่อการยุติธรรมแห่งประเทศไทย ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่กรุงเทพฯ 10210 23 หมายเลขโทรศัพท์: 0 2612 6000 โทรสาร: 0 2612 6011 0 2612 6012

ประกาศโดย

คณะกรรมการพัฒนารัฐบาลดิจิทัล

ประกาศในราชกิจจานุเบกษา เล่ม XX ตอนพิเศษ XX

วันที่ XX เดือน XXXX พ.ศ. 25XX

คณะกรรมการพัฒนารัฐบาลดิจิทัล

ตามมาตรา 6 แห่งพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 ให้มีคณะกรรมการพัฒนารัฐบาลดิจิทัล ประกอบด้วย

ประธาน

นายกรัฐมนตรี

กรรมการ

1. รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
2. ปลัดสำนักนายกรัฐมนตรี
3. ปลัดกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม
4. ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
5. ผู้อำนวยการสำนักงบประมาณ
6. เลขาธิการคณะกรรมการข้าราชการพลเรือน
7. เลขาธิการคณะกรรมการพัฒนาระบบราชการ
8. เลขาธิการสภาพัฒนาการเศรษฐกิจและสังคมแห่งชาติ
9. ผู้แทนจาก คณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ
10. ผู้แทนจาก คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
11. ผู้แทนจาก คณะกรรมการข้อมูลข่าวสารของราชการ
12. ผู้แทนจาก คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
13. ผู้แทนจาก คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

กรรมการและเลขานุการ

ผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

ผู้ช่วยเลขานุการ

1. รองผู้อำนวยการหรือผู้ช่วยผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล ที่ผู้อำนวยการมอบหมาย
2. เจ้าหน้าที่สำนักงานพัฒนารัฐบาลดิจิทัล

คณะกรรมการจัดทำร่างมาตรฐาน ข้อกำหนด และหลักเกณฑ์ ภายใต้พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562

ที่ปรึกษา

นางไอรดา เหลืองวิไล	รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล รักษาการแทนผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

ประธานกรรมการ

ผู้ช่วยศาสตราจารย์ณัฐวุฒิ หนูไพโรจน์	จุฬาลงกรณ์มหาวิทยาลัย

รองประธานกรรมการ

นายอาศิส อัญญะโพธิ์	ผู้ช่วยผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

กรรมการ

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

กรรมการและเลขานุการ

นางสาวอุรัชฎา เกตุพรหม	ผู้อำนวยการฝ่ายมาตรฐานดิจิทัลภาครัฐ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

คณะทำงานเทคนิคด้านมาตรฐานการบริหารจัดการข้อมูลภาครัฐ

ที่ปรึกษา

นางไอรดา เหลืองวิไล	รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล รักษาการแทนผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล
ผู้ช่วยศาสตราจารย์ณัฐวุฒิ หนูไพโรจน์	จุฬาลงกรณ์มหาวิทยาลัย
นายอาศิส อัญญะโพธิ์	รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล
นางสาวฐิติรัตน์ ทิพย์สัมฤทธิ์กุล	มหาวิทยาลัยธรรมศาสตร์

ประธานคณะทำงาน

ศาสตราจารย์ธีรณี อจลากุล	ผู้อำนวยการสถาบันข้อมูลขนาดใหญ่ (องค์การมหาชน)

รองประธานกรรมการ

ผู้ช่วยศาสตราจารย์โษฆศ์รัตต 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	ผู้อำนวยการฝ่ายมาตรฐานดิจิทัลภาครัฐ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

ผู้ช่วยเลขานุการ

นางสาวสุภัทรา เรืองวานิช	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

วิเคราะห์และจัดทำมาตรฐานรัฐบาลดิจิทัล

นางสาวสุภัทรา เรืองวานิช	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
นางสาวศุภมาส พงษ์ภาคิน	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
นายธนัชกฤศ เรืองฉวี	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

หลักเกณฑ์การจัดระดับชั้นข้อมูลภาครัฐ (Government Data Classification Framework) ฉบับนี้จัดทำขึ้น เพื่อใช้เป็นเกณฑ์พิจารณากำหนดระดับชั้นข้อมูลสำหรับทุกชุดข้อมูล (Dataset) ที่เป็นข้อมูลอิเล็กทรอนิกส์ของหน่วยงานภาครัฐ และใช้เป็นเครื่องมือประกอบการใช้ดุลพินิจของเจ้าของข้อมูล (Data Owner) ในการกำหนดสิทธิการเข้าถึงและการใช้งานข้อมูล รวมถึงการกำกับดูแลข้อมูลให้มีความมั่นคงปลอดภัยอย่างเหมาะสม ตลอดจนพิจารณาการเลือกใช้บริการคลาวด์ให้สอดคล้องกับการจำแนกประเภทข้อมูล ทั้งนี้ เพื่อสนับสนุนให้หน่วยงานของรัฐสามารถบริหารจัดการข้อมูลในกระบวนงานที่เกี่ยวข้องกับภารกิจของหน่วยงานได้อย่างมีประสิทธิภาพ โดยหลักเกณฑ์ฉบับนี้ได้จัดทำตามมาตรฐานและแนวทางแห่ง

1. มาตรฐาน NIST 800-60 Volume 1. and 2. : Guide for Mapping Types of Information and Information Systems to Security Categories
2. มาตรฐาน FIPS PUB 199 : Standards for Security Categorization of Federal Information and Information Systems
3. มาตรฐาน ISO/IEC 27001: 2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements

และได้รวบรวมความคิดเห็นและข้อเสนอแนะจากหน่วยงาน รวมทั้งมีการจัดประชุมกลุ่มย่อยร่วมกับหน่วยงานที่เกี่ยวข้อง และมีการจัดงานประชาพิจารณ์เพื่อเปิดรับฟังความคิดเห็นเป็นการทั่วไป และนำข้อมูลข้อสังเกต ข้อคิดเห็นจากผู้ทรงคุณวุฒิและจากหน่วยงานที่เกี่ยวข้อง เพื่อให้ข้อเสนอแนะเกี่ยวกับมาตรฐานฉบับนี้มีความสมบูรณ์ครบถ้วน และสามารถนำไปปรับใช้ในทางปฏิบัติได้อย่างมีประสิทธิภาพ โดยผ่านการพิจารณาความเห็นชอบจากคณะทำงานเทคนิคด้านมาตรฐานการบริหารจัดการข้อมูลภาครัฐ และคณะกรรมการจัดทำร่างมาตรฐาน ข้อกำหนด และหลักเกณฑ์ ภายใต้พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 เรียบร้อยแล้ว

หลักเกณฑ์การจัดระดับชั้นข้อมูลภาครัฐฉบับนี้จัดทำโดยฝ่ายมาตรฐานดิจิทัลภาครัฐ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) สำนักนายกรัฐมนตรี

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
เลขที่ 999 ชั้น 4 สถาบันเพื่อการยุติธรรมแห่งประเทศไทย
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210
E-mail: sd-g1_division@dga.or.th
Website: www.dga.or.th

คำนำ

องค์กรทั่วโลกทั้งภาครัฐและเอกชนให้ความสำคัญกับการจัดการและใช้ข้อมูลมากขึ้น เพื่อเพิ่มประสิทธิภาพการทำงาน วิเคราะห์ วางแผน และตัดสินใจเชิงนโยบาย พร้อมปฏิบัติตามกฎหมายและมาตรฐานกำกับดูแล เนื่องจากข้อมูลถือเป็นสินทรัพย์สำคัญ (Data as Asset) การบริหารข้อมูลต้องมีมาตรการรักษาความปลอดภัย โดยเฉพาะการพิจารณาหมวดหมู่และจัดระดับชั้นข้อมูล เพื่อลดความเสี่ยง กำหนดสิทธิการเข้าถึง และสนับสนุนการแบ่งปันข้อมูลอย่างถูกต้องตามกฎหมาย ขณะเดียวกันองค์กรต้องเข้าถึงข้อมูลได้รวดเร็วเพื่อรักษาประสิทธิภาพ และจัดการข้อมูลที่มีความอ่อนไหว (Sensitive Data) อย่างเหมาะสม เพื่อคุ้มครองความเป็นส่วนตัวและผลประโยชน์ขององค์กร

ประกอบกับหน่วยงานภาครัฐมีความจำเป็นต้องมีระบบบริหารและกระบวนการจัดการและคุ้มครองข้อมูลที่ครบถ้วน ตั้งแต่การจัดทำ การจัดเก็บ การพิจารณาหมวดหมู่ การประมวลผลหรือใช้ข้อมูล การปกปิดหรือเปิดเผยข้อมูล การตรวจสอบ และการทำลาย ซึ่งเป็นไปตามมาตรา 8 แห่งพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 และประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัลเรื่องธรรมาภิบาลข้อมูลภาครัฐ ข้อ 4 (5) จำแนกหมวดหมู่ของข้อมูล เพื่อกำหนดนโยบายข้อมูลหรือกฎเกณฑ์เกี่ยวกับผู้มีสิทธิเข้าถึงและใช้ประโยชน์จากข้อมูลต่างๆ ภายในหน่วยงาน สำหรับให้ผู้ซึ่งมีหน้าที่เกี่ยวข้องปฏิบัติตามนโยบายหรือกฎเกณฑ์ได้อย่างถูกต้อง และสอดคล้องตามกฎหมายที่เกี่ยวข้อง อันจะนำไปสู่การพัฒนาระบบข้อมูลสำคัญ เพื่อกำหนดหลักเกณฑ์และวิธีการเชื่อมโยง แลกเปลี่ยน และบูรณาการข้อมูลระหว่างหน่วยงานอย่างมีมาตรฐาน รวมถึงการพัฒนาศูนย์กลางข้อมูลเปิดภาครัฐ เพื่อให้ประชาชนเข้าถึงและใช้ประโยชน์ได้อย่างมีประสิทธิภาพ

ในการนี้ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.) จึงได้จัดทำเอกสาร **หลักเกณฑ์การจัดระดับชั้นข้อมูลภาครัฐ (Government Data Classification Framework)** ฉบับนี้ขึ้น **เพื่อใช้เป็นเกณฑ์พิจารณาประกอบการใช้ดุลพินิจของเจ้าของข้อมูล (Data Owner) ในการกำหนดระดับชั้นข้อมูลสำหรับทุกชุดข้อมูล (Dataset) ที่แลกเปลี่ยนกันได้ในรูปแบบอิเล็กทรอนิกส์ทุกประเภท ซึ่งรวมถึงข้อมูลข่าวสารลับ[1]ในรูปแบบอิเล็กทรอนิกส์ของหน่วยงานภาครัฐ โดยจะไม่ครอบคลุมเอกสารที่เป็นกระดาษทุกประเภท** เพื่อเป็นเครื่องมือประกอบการจัดระดับชั้นข้อมูล สามารถกำหนดการเข้าถึงและใช้งานข้อมูลและกำกับดูแลข้อมูลที่มีความอ่อนไหวหรือข้อมูลที่มีระดับชั้นความลับอย่างเหมาะสม ทั้งนี้ เพื่อใช้ประโยชน์จากข้อมูลร่วมกันในการพัฒนาบริการและนวัตกรรมที่จะเป็นประโยชน์ต่อประเทศในด้านต่างๆ ต่อไป

[1] ข้อมูลข่าวสารลับ หมายถึง ข้อมูลข่าวสารตามมาตรา 14 และมาตรา 15 แห่งพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540

สารบัญ

สารบัญภาพ

สารบัญตาราง

มาตรฐานรัฐบาลดิจิทัล
ว่าด้วยหลักเกณฑ์การจัดระดับชั้นข้อมูลภาครัฐ

1. บทนำ

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.) ได้จัดทำเอกสารหลักเกณฑ์การจัดระดับชั้นข้อมูลภาครัฐ **เหมาะสำหรับ 1) เจ้าของข้อมูล และ 2) ฝ่ายเทคโนโลยีสารสนเทศ เพื่อใช้เป็นเกณฑ์พิจารณาจัดระดับชั้นข้อมูล (Data Classification)** และส่งเสริมการกำกับดูแลข้อมูลที่มีคุณค่า และเพื่อให้สามารถบรรลุเป้าหมาย ด้านความเป็นส่วนตัว (Privacy) และความปลอดภัย (Security) ของข้อมูล รวมทั้งสามารถใช้งานข้อมูลได้อย่างถูกต้องเหมาะสม โดยไม่ขัดต่อข้อกฎหมายที่เกี่ยวข้อง ตลอดจนการทำข้อมูลสารสนเทศให้มีความพร้อม เพื่อการพิจารณาใช้คลาวด์ที่เหมาะสมกับการจำแนกประเภทข้อมูล

1.1 ความเป็นมา

องค์กรทั่วโลกทั้งภาครัฐและเอกชนให้ความสำคัญกับการจัดการและใช้ข้อมูลมากขึ้น เพื่อเพิ่มประสิทธิภาพการทำงาน วิเคราะห์ วางแผน และตัดสินใจเชิงนโยบาย พร้อมปฏิบัติตามกฎหมายและมาตรฐานกำกับดูแล เนื่องจากข้อมูลถือเป็นสินทรัพย์สำคัญ (Data as Asset) การบริหารข้อมูลต้องมีมาตรการรักษาความปลอดภัย **โดยมีขั้นตอนสำคัญคือ การพิจารณาหมวดหมู่ตามธรรมาภิบาลข้อมูลและจัดระดับชั้นข้อมูล** เพื่อลดความเสี่ยง กำหนดสิทธิการเข้าถึง และสนับสนุนการแบ่งปันข้อมูลอย่างถูกต้องตามกฎหมาย ขณะเดียวกันองค์กรต้องเข้าถึงข้อมูลได้รวดเร็วเพื่อรักษาประสิทธิภาพ และจัดการข้อมูลที่มีความอ่อนไหว (Sensitive Data) อย่างเหมาะสม เพื่อคุ้มครองความเป็นส่วนตัวและผลประโยชน์ขององค์กร

ด้วยพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 กำหนดให้หน่วยงานของรัฐจัดให้มีการบริหารจัดการ การบูรณาการข้อมูลภาครัฐ การทำงานให้มีความสอดคล้องกัน การเชื่อมโยงเข้าด้วยกันอย่างมั่นคงปลอดภัยและมีธรรมาภิบาล และตามมาตรา 8 ธรรมาภิบาลข้อมูลภาครัฐต้องประกอบด้วยอย่างน้อย ในมาตรา 8 (2) การมีระบบบริหารและกระบวนการจัดการและคุ้มครองข้อมูลที่ครบถ้วน ตั้งแต่การจัดทำ การจัดเก็บ การจำแนกหมวดหมู่ การประมวลผลหรือใช้ข้อมูล การปกปิดหรือเปิดเผยข้อมูล การตรวจสอบ และการทำลาย และประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ [1] ข้อ 4 (5) การจำแนกหมวดหมู่ของข้อมูล เพื่อกำหนดนโยบายข้อมูลหรือกฎเกณฑ์เกี่ยวกับผู้มีสิทธิเข้าถึงและใช้ประโยชน์จากข้อมูลต่างๆ ภายในหน่วยงาน สำหรับให้ผู้ซึ่งมีหน้าที่เกี่ยวข้องปฏิบัติตามนโยบายหรือกฎเกณฑ์ได้อย่างถูกต้อง และสอดคล้องตามกฎหมายที่เกี่ยวข้อง อันจะนำไปสู่การบริหารจัดการข้อมูลภาครัฐอย่างเป็นระบบ

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.) ได้ประกาศสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) เรื่อง มสพร. 8-2565 มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ว่าด้วยหลักเกณฑ์การจัดระดับชั้นและการแบ่งปันข้อมูลภาครัฐ เมื่อวันที่ 7 พฤศจิกายน 2565 เพื่อประกาศใช้สำหรับสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) และเพื่อเป็นข้อเสนอแนะให้แก่หน่วยงานรัฐอื่นๆ สามารถใช้เป็นเกณฑ์พิจารณาจัดระดับชั้นข้อมูล (Data Classification) เพื่อใช้ประโยชน์จากข้อมูลร่วมกันในการพัฒนา

บริการและนวัตกรรมที่จะเป็นประโยชน์ต่อประเทศในด้านต่างๆ รวมถึงช่วยให้หน่วยงานภาครัฐสามารถพิจารณาเลือกใช้คลาวด์ที่เหมาะสมกับการจำแนกประเภทข้อมูลนั้นได้ ซึ่งเป็นการส่งเสริมการขับเคลื่อนการทำงานของภาครัฐเพิ่มมากยิ่งขึ้น

จึงเป็นเหตุสมควรให้นำ มสพร. 8-2565 มาทบทวนและปรับปรุงเพื่อยกระดับมาตรฐานให้เป็นสากลมากยิ่งขึ้น มีความเป็นปัจจุบันและทันต่อสถานการณ์ รวมถึงสอดคล้องตามนโยบายการใช้คลาวด์ เพื่อสร้างความรู้ความเข้าใจให้กับหน่วยงานรัฐ และสามารถนำไปปฏิบัติใช้ ในการจัดระดับชั้นข้อมูลของหน่วยงานตลอดจนนำไปสู่การจัดระดับชั้นข้อมูลในรูปแบบภาพรวมของบริการ เพื่อรองรับต่อการก้าวเข้าสู่การเป็นรัฐบาลดิจิทัลต่อไป

1.2 วัตถุประสงค์

เอกสารฉบับนี้จัดทำขึ้นเพื่อเป็น หลักเกณฑ์นี้จะใช้เพื่อพิจารณากำหนดระดับชั้นข้อมูลภาครัฐ โดยมีวัตถุประสงค์หลัก ดังนี้

1) เพื่อเป็นเครื่องมือประกอบการใช้ดุลพินิจของผู้มีอำนาจในการตัดสินใจกำหนดระดับชั้นข้อมูล สามารถกำหนดการเข้าถึงและใช้งานข้อมูลและกำกับดูแลข้อมูลที่มีความอ่อนไหวหรือ ข้อมูลที่มีชั้นความลับอย่างเหมาะสม เพื่อรักษาความเป็นส่วนตัวและความปลอดภัยของข้อมูล

2) เพื่อให้หน่วยงานภาครัฐ สามารถให้บริการ ทำงานร่วมกันแ และนำไปสู่การแบ่งปันข้อมูลระหว่างหน่วยงานภาครัฐได้อย่างมีประสิทธิภาพมากยิ่งขึ้นด้วยการเข้าถึงข้อมูลจากทุกที่และทุกเวลา

3) เพื่อเพิ่มประสิทธิภาพการรักษาความปลอดภัยและคุ้มครองข้อมูล ลดความเสี่ยงจากการถูกละเมิดหรือการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต รวมถึงการสูญหายของข้อมูล โดยการเลือกใช้คลาวด์ที่เหมาะสม

ทั้งนี้ มาตรฐานฉบับนี้มุ่งเน้นไปที่การกำหนดระดับชั้นข้อมูลสำหรับทุกชุดข้อมูล (Dataset) ที่แลกเปลี่ยนกันได้ในรูปแบบอิเล็กทรอนิกส์ทุกประเภทของหน่วยงานภาครัฐ โดยจะไม่ครอบคลุมเอกสารที่เป็นกระดาษทุกประเภท

1.3 ขอบข่าย

หลักเกณฑ์การจัดระดับชั้นข้อมูลภาครัฐฉบับนี้จัดทำขึ้นเพื่อให้เจ้าของข้อมูล (Data Owner) และฝ่ายเทคโนโลยีสารสนเทศ ใช้เป็นเกณฑ์พิจารณาจัดระดับชั้นข้อมูล กำหนดการเข้าถึงและใช้งานข้อมูล กำกับดูแลข้อมูลของหน่วยงาน ตลอดจนพิจารณาการเลือกใช้บริการคลาวด์ให้เหมาะสมกับการจำแนกประเภทข้อมูล สอดคล้องตามแนวทางในประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัลเรื่อง ธรรมาภิบาลข้อมูลภาครัฐ โดยแนวทางฉบับนี้ได้จัดทำตามแนวมาตรฐานและแนวปฏิบัติที่ดีของ

1.3.1 มาตรฐาน NIST 800-60 Volume 1. and 2. : Guide for Mapping Types of Information and Information Systems to Security Categories [2] เป็นมาตรฐานสำหรับการจัดหมวดหมู่ข้อมูลและระบบสารสนเทศตามระดับความสำคัญ เพื่อกำหนดมาตรการรักษาความปลอดภัยที่เหมาะสม

1.3.2 มาตรฐาน FIPS PUB 199 : Standards for Security Categorization of Federal Information and Information Systems [3] เป็นมาตรฐานการจัดหมวดหมู่ความปลอดภัยของข้อมูลและระบบสารสนเทศ เพื่อเป็นพื้นฐานในการเลือกมาตรการควบคุม

1.3.3 มาตรฐาน ISO/IEC 27001: 2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements [4] เป็นมาตรฐานสากลสำหรับการจัดการความปลอดภัยของข้อมูล (ISMS) ครอบคลุมการกำหนดนโยบาย กระบวนการ และการควบคุมความเสี่ยง

โดยหลักเกณฑ์ฯ ที่จัดทำขึ้นนี้เพื่อเป็นเกณฑ์พิจารณากำหนดระดับชั้นข้อมูลสำหรับทุกชุด**ข้อมูลที่แลกเปลี่ยนกันได้ในรูปแบบอิเล็กทรอนิกส์ทุกประเภท ซึ่งรวมถึงข้อมูลข่าวสารลับในรูปแบบอิเล็กทรอนิกส์ของหน่วยงานภาครัฐ โดยจะไม่ครอบคลุมเอกสารที่เป็นกระดาษทุกประเภท**[2] เพื่อเป็นเครื่องมือประกอบการใช้ดุลพินิจของผู้มีอำนาจในการตัดสินใจกำหนดระดับชั้นข้อมูล เพื่อให้หน่วยงานสามารถกำหนดการเข้าถึงและใช้งานข้อมูลและกำกับดูแลข้อมูลให้มีความปลอดภัย และสามารถพิจารณาเลือกใช้บริการคลาวด์ที่เหมาะสม **ซึ่งจะช่วยให้หน่วยงานของรัฐสามารถจัดการข้อมูลในกระบวนงานที่เกี่ยวข้องกับภารกิจของหน่วยงานได้อย่างมีประสิทธิภาพ**

ในกรณีของข้อมูลความมั่นคงที่ส่งผลกระทบอย่างร้ายแรงต่อผลประโยชน์แห่งชาติหรือการปกครองระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุข หรือความปลอดภัยของประเทศ ให้หน่วยงานดำเนินการตามกฎหมายเฉพาะที่เกี่ยวข้อง เช่น พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 ระเบียบสำนักนายกรัฐมนตรีว่าด้วยงานสารบรรณ (ฉบับที่ 4) พ.ศ. 2564 และระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. 2552

1.4 บทนิยาม

จากการทบทวนนิยามศัพท์ที่เกี่ยวข้องจากประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และนโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ รวมทั้งกรอบแนวคิดและมาตรฐานที่เกี่ยวข้องทั้งในและต่างประเทศ ได้ข้อสรุปความหมายของการจัดระดับชั้น และคำศัพท์อื่นๆ ที่เกี่ยวข้องดังนี้

1.4.1 **การจัดระดับชั้นข้อมูล (Data Classification)** หมายความว่า การจัดระดับชั้นของข้อมูลในบริบทของการรักษาความปลอดภัยข้อมูลตามระดับของความอ่อนไหวและผลกระทบต่อบุคคล องค์กร และประเทศ หากมีการเปิดเผย เปลี่ยนแปลง หรือทำลายข้อมูลโดยไม่ได้รับอนุญาต โดยการจัดระดับชั้นข้อมูลจะช่วยกำหนดการควบคุมความปลอดภัยพื้นฐานที่เหมาะสมสำหรับการปกป้องข้อมูลนั้นๆ ทั้งนี้ ข้อมูลสำคัญของบุคคล องค์กร และประเทศทั้งหมด ควรจัดชั้นตามระดับความอ่อนไหวของระดับชั้นข้อมูลหรือตามที่หน่วยงานกำหนด เพื่อให้หน่วยงานของรัฐสามารถจัดการข้อมูลในกระบวนงานที่เกี่ยวข้องกับภารกิจของหน่วยงานได้อย่างมีประสิทธิภาพ

1.4.2 **ข้อมูลอ่อนไหว (Sensitive Data)** หมายความว่า ข้อมูลอ่อนไหวเป็นข้อมูลที่มีระดับชั้นความลับหรือที่เป็นข้อมูลเกี่ยวข้องกับความมั่นคงที่ต้องได้รับการป้องกันจากการเข้าถึงโดยไม่ได้รับอนุญาต เพื่อคุ้มครองความเป็นส่วนตัว (Privacy) หรือความปลอดภัย (Security) ของบุคคลหรือองค์กร ซึ่งหากข้อมูลอ่อนไหวมีการเปิดเผยโดยไม่ได้รับอนุญาต จะมีแนวโน้มที่จะนำไปสู่ผลที่ไม่พึงประสงค์หรือส่งผลกระทบ

[2] สำหรับเอกสารในรูปกระดาษให้ดำเนินตามกฎหมายอื่นๆ ที่เกี่ยวข้อง

ต่อบุคคล หน่วยงาน องค์กร หรือ ประเทศ ตัวอย่างเช่น ข้อมูลส่วนบุคคลที่อ่อนไหว (Sensitive Personal Data) ข้อมูลที่เกี่ยวข้องกับด้านความมั่นคง กฎหมาย เศรษฐกิจ การพาณิชย์

1.4.3 **ระดับชั้นข้อมูล (Data Classification Level)** หมายความว่า ระดับชั้นข้อมูลเพื่อจัดการข้อมูลในกระบวนงานที่เกี่ยวข้องกับภารกิจ โดยข้อมูลที่มีความอ่อนไหวแบ่งระดับชั้นออกเป็น ชั้นเปิดเผย (Open) ชั้นเผยแพร่ภายในองค์กร (Private) ชั้นลับ (Confidential) ชั้นลับมาก (Secret) และชั้นลับที่สุด (Top Secret) **ซึ่งข้อมูลที่มีระดับชั้น ลับ (Confidential) ลับมาก (Secret) และ ลับที่สุด (Top Secret) เป็นเพียงการจัดระดับชั้นข้อมูล ไม่ใช่การกำหนดให้ข้อมูลนั้นเป็นข้อมูลข่าวสารลับตามระเบียบการรักษาความลับทางราชการ**

1.4.4 **นายทะเบียนข้อมูลข่าวสารลับ** หมายความว่า เจ้าหน้าที่ผู้ได้รับแต่งตั้งจากหัวหน้าหน่วยงานของรัฐ เพื่อทำหน้าที่ควบคุมและรับผิดชอบการดำเนินการเกี่ยวกับข้อมูลข่าวสารลับขึ้นภายในหน่วยงานที่ตนรับผิดชอบ ทั้งนี้ นิยามต่างๆ ให้อ้างอิงระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม

1.4.5 **นายทะเบียนบัญชีข้อมูลหน่วยงาน** หมายความว่า หัวหน้าหน่วยงานของรัฐ หรือผู้ที่ได้รับมอบหมาย ทำหน้าที่กำกับ ดูแล การลงทะเบียนบัญชีข้อมูลหน่วยงาน การตรวจสอบและแก้ไขบัญชีข้อมูลหน่วยงาน การเพิกถอนการลงทะเบียนบัญชีข้อมูลหน่วยงาน และอนุญาตใช้และเปิดเผยทะเบียนบัญชีข้อมูลของหน่วยงาน

1.5 กฎหมายและแนวทางที่เกี่ยวข้อง

1.5.1 พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540

1.5.2 ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม

1.5.3 ระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. 2552 และที่แก้ไขเพิ่มเติม

1.5.4 พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 มาตรา 7 และมาตรา 8 ธรรมาภิบาลข้อมูลภาครัฐ

1.5.5 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

1.5.6 นโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ (พ.ศ. 2566-2570)

1.5.7 ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัลเรื่อง ธรรมาภิบาลข้อมูลภาครัฐ พ.ศ. 2563 และ ฉบับปรับปรุง พ.ศ. 2566 ข้อ 4 ธรรมาภิบาลข้อมูลภาครัฐในระดับหน่วยงาน (5) การจำแนกหมวดหมู่ของข้อมูล เพื่อกำหนดนโยบายข้อมูลหรือกฎเกณฑ์เกี่ยวกับผู้มีสิทธิเข้าถึงและใช้ประโยชน์จากข้อมูลต่างๆ ภายในหน่วยงาน สำหรับให้ผู้ซึ่งมีหน้าที่เกี่ยวข้องปฏิบัติตามนโยบายหรือกฎเกณฑ์ได้อย่างถูกต้อง และสอดคล้องตามกฎหมายที่เกี่ยวข้อง อันจะนำไปสู่การบริหารจัดการข้อมูลภาครัฐอย่างเป็นระบบ

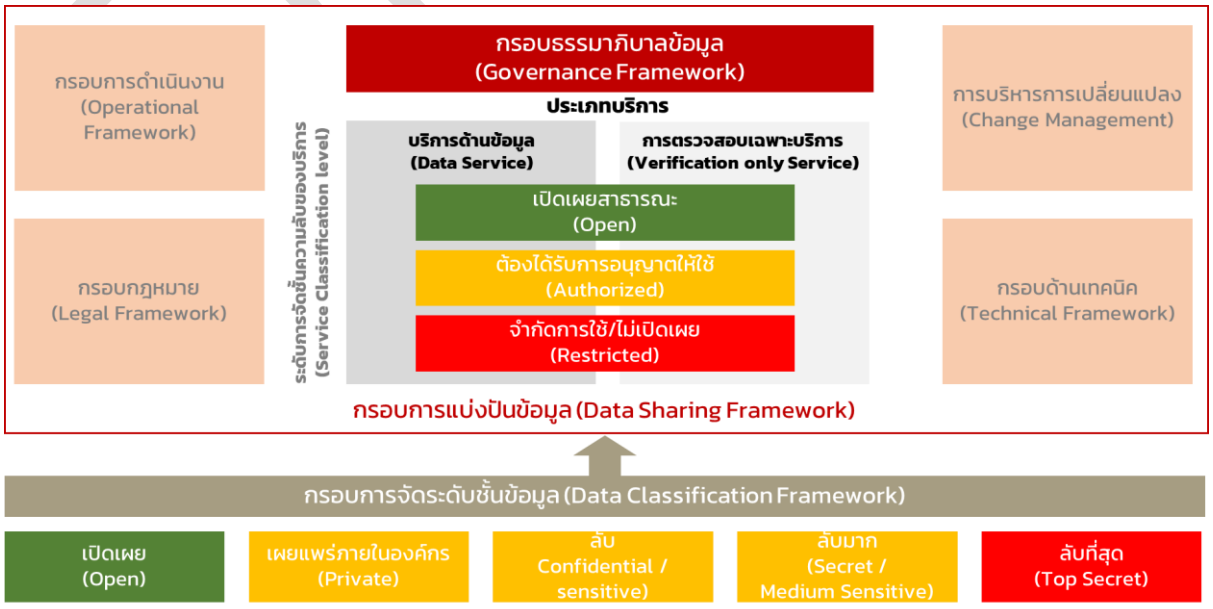
ทั้งนี้ หากมีกฎหมายอื่นๆ ที่เกี่ยวข้อง สามารถใช้ประกอบการพิจารณาได้

2. กรอบแนวคิด

2.1 กรอบหลักการจัดระดับชั้นข้อมูล

การจัดระดับชั้นข้อมูลเป็นส่วนพื้นฐานในการรักษาความปลอดภัยข้อมูลขององค์กรและบุคคลที่สามารถเข้าถึงได้ เป็นกระบวนการในการระบุและกำหนดระดับความอ่อนไหวหรือการรักษาความลับที่กำหนดไว้ล่วงหน้าให้กับข้อมูลประเภทต่างๆ โดยการวิเคราะห์ข้อมูลที่มีโครงสร้างหรือไม่มีโครงสร้าง และการจัดระดับชั้นข้อมูลขึ้นอยู่กับประเภทไฟล์และเนื้อหา ซึ่งช่วยให้องค์กรสามารถกำหนดและให้คุณค่ากับข้อมูลและเป็นจุดเริ่มต้นพื้นฐานสำหรับการกำกับดูแลหรือจัดทำธรรมาภิบาลข้อมูล กระบวนการจัดระดับชั้นข้อมูลจะจำแนกข้อมูลตามความอ่อนไหวและผลกระทบทางธุรกิจ/ในการดำเนินภารกิจของหน่วยงานเพื่อระบุความเสี่ยง เมื่อข้อมูลถูกจัดระดับชั้นแล้วจะสามารถจัดการเพื่อปกป้องข้อมูลที่มีความอ่อนไหวหรือสำคัญจากการโจรกรรมหรือการสูญหายได้ ทั้งนี้ **การจัดระดับชั้นข้อมูลจะแตกต่างกันไปตามบริบทหรือกฎหมายที่เกี่ยวข้องของหน่วยงานนั้นๆ**

ข้อมูลที่มีการจัดระดับชั้นข้อมูลไม่ควรเข้าถึงได้โดยทุกคน เพราะจะแสดงให้เห็นว่าขาดความน่าเชื่อถืออันเนื่องมาจากความไม่ซื่อสัตย์ ขาดความถูกต้อง (Integrity) หรือผู้ที่อาจได้รับผลกระทบที่ไม่เหมาะสมอันเนื่องมาจากสถานการณ์ด้านข้อมูลส่วนบุคคล สำหรับข้อกังวลด้านการคุ้มครองข้อมูลส่วนบุคคลต้องกำหนดให้ผู้ประมวลผลข้อมูลดำเนินการตามข้อกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล สำหรับข้อมูลใช้ภายในองค์กรอาจกำหนดให้ฝ่ายบุคลากรดำเนินการตรวจสอบเพิ่มเติมเกี่ยวกับพนักงาน/เจ้าหน้าที่ อาทิ การตรวจสอบประวัติอาชญากรรม เพื่อการควบคุมการเข้าถึงข้อมูล โดยผู้ใช้จะต้องได้รับการระบุตรวจสอบสิทธิและได้รับอนุญาต ซึ่งจุดอ่อนที่สำคัญที่สุดในปัจจุบันของการพิสูจน์ตัวตนผู้ใช้คือการใช้รหัสผ่านอย่างต่อเนื่อง เนื่องจากรหัสผ่านมีความปลอดภัยไม่เพียงพอ ผู้ใช้มักเลือกสิ่งที่เดาหรือถอดรหัสได้ง่าย ดังนั้นการเข้าถึงข้อมูลที่เป็นความลับจำเป็นต้องควบคุมโดยใช้การพิสูจน์ตัวตนที่รัดกุมหรือแบบสองปัจจัย (Two Factor Authentication) โดยมีปัจจัยที่สองคือสิ่งที่ผู้ใช้มีหรือสิ่งที่ผู้ใช้เป็น และเป็นสิ่งจำเป็นนอกเหนือจากสิ่งที่ผู้ใช้รู้ อาทิ การเข้ารหัสผ่าน



ภาพที่ 1 กรอบการจัดระดับชั้นและการแบ่งปันข้อมูล

การจัดประเภทข้อมูลช่วยให้มั่นใจได้ว่าทั้งข้อกำหนดเกี่ยวกับข้อมูลและการปฏิบัติตามข้อกำหนดจะบรรลุผลอย่างมีประสิทธิภาพและประสิทธิผล การจัดประเภทข้อมูลควรเป็นรากฐานที่สำคัญของกิจกรรมการจัดการข้อมูลและนโยบายการจัดการวงจรข้อมูล นำไปสู่การแบ่งปันข้อมูลมีความสำคัญ เพื่อให้มั่นใจว่ามีการจัดเก็บและใช้งานอย่างเหมาะสมและปลอดภัย ซึ่งกรอบการจัดระดับชั้นข้อมูลและการแบ่งปันข้อมูลโดยทั่วไปมีองค์ประกอบที่หลากหลาย [6] อาทิ กรอบการดำเนินงาน (Operational Framework) กรอบกฎหมาย (Legal Framework) การบริหารการเปลี่ยนแปลง (Change Management) กรอบด้านเทคนิค (Technical Framework) และประเภทบริการ ที่ตอบสนองต่อข้อมูลที่มีความอ่อนไหว และมีการจัดระดับชั้นข้อมูลเป็นรากฐานที่มั่นคงสำหรับกลยุทธ์ด้านความปลอดภัยของข้อมูล โดยกำหนดแนวทางและเงื่อนไขในการแบ่งปันข้อมูล ทั้งนี้ ข้อมูลที่ต้องได้รับอนุญาตให้ใช้นั้นจะต้องยอมรับข้อตกลงการใช้งานข้อมูล ใช้ข้อมูลตามวัตถุประสงค์และระยะเวลาที่ได้รับอนุญาตเท่านั้น และการทำลายข้อมูลหลังจากใช้งานแล้ว นอกจากนี้ ควรมีระบบรองรับในอนาคต เช่น กลไกการเข้ารหัสข้อมูลเพื่อความปลอดภัยในการจัดเก็บ การจัดการสิทธิการเข้าถึงข้อมูล การเก็บประวัติการเข้าถึงข้อมูล การยืนยันตัวตน (Authentication) การปรับปรุงข้อมูลที่จัดเก็บให้เป็นปัจจุบัน และการประเมินคุณภาพข้อมูลอย่างกึ่งอัตโนมัติ อาทิ ความปรับปรุงให้เป็นปัจจุบัน ความครบถ้วน ปริมาณข้อมูล ประเภท และ Machine-readable เพื่อให้การจัดระดับชั้นเป็นไปอย่างมีประสิทธิภาพและสร้างความมั่นใจในการแบ่งปันข้อมูล

2.1.1. หลักการจัดระดับชั้นข้อมูล (Principle of data and information classification)

การดำเนินการจัดการข้อมูลโดยทั่วไปและการจัดระดับชั้นข้อมูลโดยเฉพาะที่มีความแตกต่างกันไปตามประเภทองค์กรและอาจแตกต่างกันไปขึ้นอยู่กับแต่ละองค์กร อย่างไรก็ตาม มีหลักการพื้นฐานร่วมกันระหว่างองค์กรภาครัฐและภาคเอกชน 6 ประการ [7] ซึ่งแสดงโดยแหล่งข้อมูลทางกฎหมายระดับชาติ (และระดับภูมิภาค) และเป็นเครื่องมือขององค์กรระหว่างประเทศสำหรับการจัดการข้อมูลข่าวสาร โดยหลักการดังต่อไปนี้ควรใช้เป็นแนวทางมากกว่าเป็นเกณฑ์เทียบเคียง (Benchmark) อย่างเดียวในการสร้างและ/หรือการปรับปรุงการจัดการข้อมูลและกลยุทธ์การจัดระดับชั้นข้อมูล

1) การเปิดกว้าง ความโปร่งใส และค่านิยมทางสังคม (Openness, Transparency, and Societal values) การจัดระดับชั้นข้อมูลควรใช้อย่างระมัดระวังและสอดคล้องกับความอ่อนไหว ค่านิยม และความสำคัญของข้อมูล การจำกัดการเข้าถึงควรเลือกพิจารณาเฉพาะในกรณีที่การเปิดเผยข้อมูลอาจเป็นอันตรายต่อผลประโยชน์ที่ชอบด้วยกฎหมายและภาระผูกพันทางกฎหมายขององค์กร เจ้าหน้าที่ หรือบุคคลที่สาม ซึ่งในกรณีดังกล่าวควรปฏิบัติตามขั้นตอนที่ระบุอย่างเคร่งครัดเพื่อให้แน่ใจว่าข้อมูลจะไม่ถูกรุกล้ำไม่ว่าจะโดยเจตนาหรือไม่เจตนาก็ตาม ความท้าทายคือการไม่จัดให้ข้อมูลอยู่ในระดับชั้นข้อมูลที่เป็นความลับมากเกินไปเพื่อความสะดวกหรือเพื่อความได้เปรียบอันจะเป็นการทำลายความโปร่งใสและความไว้วางใจจากสาธารณชนและกีดกันผู้มีส่วนได้ส่วนเสียในความเป็นเจ้าของสำหรับการตัดสินใจในการจัดการความเสี่ยงของตนเอง

2) แนวทางการขับเคลื่อนด้วยเนื้อหาและเป็นกลางทางเทคโนโลยี (Content driven, technology neutral approach) ข้อมูลควรได้รับการจัดระดับชั้นตามเนื้อหาและความเสี่ยงที่เกี่ยวข้องกับความสอดคล้องของเนื้อหาในรูปแบบอิเล็กทรอนิกส์ โดยไม่คำนึงถึงรูปแบบ สื่อ หรือแหล่งที่มาของข้อมูล ไม่ควรมีการเลือกปฏิบัติตามรูปแบบหรือสื่อของข้อมูล ที่ถูกจัดเก็บไว้ในระบบข้อมูล บนสื่อบันทึกข้อมูล บนอุปกรณ์พกพาหรือในระบบคลาวด์ ในทำนองเดียวกันการตัดสินใจจัดระดับชั้นข้อมูลควรขึ้นอยู่กับตัวเนื้อหาของข้อมูล

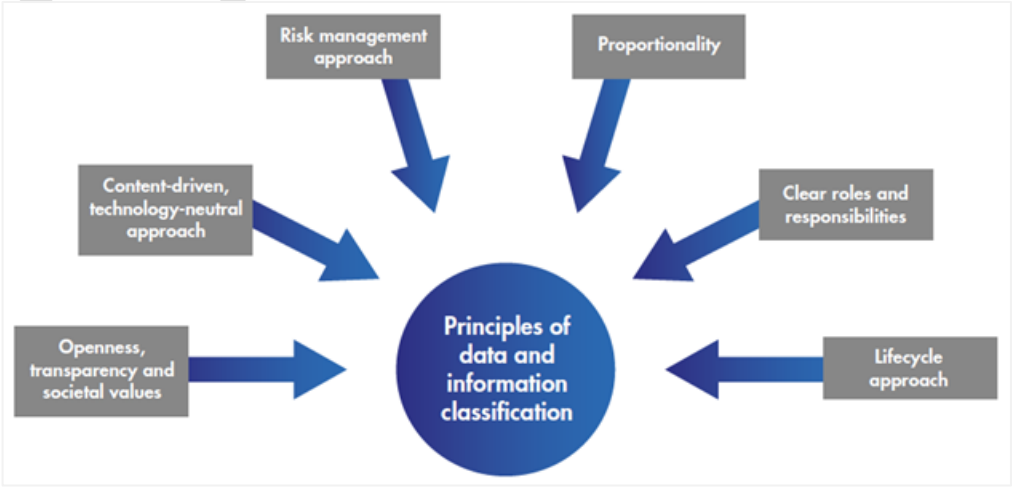
และไม่จำเป็นต้องได้รับมาโดยอัตโนมัติจากแหล่งข้อมูลที่อ้างอิง ตอบสนอง หรืออ้างถึง ตัวอย่างเช่น การอ้างอิงแหล่งข้อมูลสาธารณะไม่ควรตัดสินใจโดยอัตโนมัติว่าการประมวลข้อมูลโดยรวมสามารถเปิดเผยต่อสาธารณะได้

3) แนวทางการบริหารความเสี่ยง (Risk management approach) ข้อมูลควรได้รับการคุ้มครองตามระดับของความอ่อนไหว คุณค่า และความสำคัญของข้อมูล ตามแนวทางนี้จะให้ค่าคะแนนขึ้นอยู่กับระดับที่สอดคล้องกับคุณค่าและความเสี่ยงของข้อมูล ระดับการป้องกันควรกำหนดขอบเขตของมาตรการเพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ อาทิ ความรุนแรงและความเป็นไปได้ที่ข้อมูลจะถูกรุกล้ำหรือทำลาย ในการกำหนดระดับความอ่อนไหวและคุณค่าของข้อมูล ควรพิจารณาทั้งระดับของความเสียหายที่อาจเกิดขึ้นจากการถูกรุกล้ำหรือทำลาย (การเปิดเผยโดยไม่ได้รับอนุญาต การแก้ไข หรือการสูญเสีย) ตลอดจนคุณค่าที่เป็นไปได้ของข้อมูลที่ถูกจัดชั้น

4) สัดส่วนการจัดระดับชั้น (Proportionality) ข้อมูลต้องได้รับการจัดระดับชั้นที่เหมาะสมและควรจะให้มีระดับต่ำที่สุด เพื่อส่งเสริมให้เกิดการใช้ประโยชน์จากข้อมูลให้ได้มากที่สุด ทั้งนี้ ควรมีแต่ข้อมูลที่สำคัญและจำเป็นต้องได้รับการปกป้องเท่านั้นจึงจะจัดให้อยู่ในระดับสูงเพื่อรักษาความปลอดภัยของข้อมูล

5) บทบาทและความรับผิดชอบที่ชัดเจน (Clear roles and responsibilities) ควรมีการกำหนดบทบาทหน้าที่ของผู้ที่มีส่วนเกี่ยวข้องกับข้อมูลที่ชัดเจน โดยคำนึงถึงการจัดระดับชั้นข้อมูล นโยบายและกระบวนการควรได้รับการออกแบบสำหรับการรักษาความปลอดภัยข้อมูลภายในองค์กรและกฎหมายที่เกี่ยวข้อง [8] [9] และถือปฏิบัติด้วยการตระหนักรู้ในการบริหารจัดการและมุ่งมั่นในการรักษาความปลอดภัยของข้อมูล

6) แนวทางวงจรชีวิตของข้อมูล (Lifecycle approach) ในฐานะที่เป็นส่วนหนึ่งของระบบการจัดการข้อมูล การจัดระดับชั้นข้อมูลควรมีการพิจารณาตลอดวงจรชีวิตของข้อมูล ตั้งแต่การสร้าง การจัดเก็บ การเรียกดูข้อมูล การประมวลผลและใช้ข้อมูล การเผยแพร่ การจัดเก็บข้อมูลถาวร จนถึงการทำลาย นอกจากนี้ นโยบายการจัดการข้อมูลและประมวลผลข้อมูลขององค์กรไม่ควรเขียนไว้เป็นเป้าหมายเพียงอย่างเดียว นโยบายการจัดการและประมวลผลข้อมูลขององค์กรไม่ควรเป็นเพียงกรอบแนวทางที่กำหนดไว้เท่านั้น แต่ควรประเมินผลการดำเนินงานตามนโยบายอย่างสม่ำเสมอเพื่อให้มั่นใจว่าสอดคล้องกับความต้องการและความคาดหวังที่มีต่อองค์กร



ภาพที่ 2 หลักการจัดระดับชั้นข้อมูล

2.1.2. การตัดสินใจจัดระดับชั้นข้อมูลที่ถูกต้อง

การตัดสินใจว่าข้อมูลอยู่ในระดับชั้นใด ควรทำการประเมินเพื่อพิจารณาผลกระทบที่อาจเกิดขึ้นหากข้อมูลถูกเปิดเผย/นำไปใช้โดยไม่ได้รับอนุญาต การจัดระดับชั้นข้อมูลที่ถูกต้องจะช่วยให้มั่นใจได้ว่าข้อมูลโดยเฉพาะข้อมูลที่มีความอ่อนไหวจะได้รับการควบคุมและดูแลเพิ่มเติม **โดยในการประเมินเพื่อจัดระดับชั้นข้อมูลควรพิจารณา/คำนึงถึงประเด็นต่อไปนี้**

- การจัดระดับชั้นข้อมูลที่มีระดับชั้นความลับที่สูงเกินไปสามารถขัดขวางการเข้าถึงข้อมูล นำไปสู่การควบคุมเพื่อคุ้มครองที่ไม่จำเป็นและมีราคาแพง และทำให้ประสิทธิภาพในการดำเนินการขององค์กรลดลง
- การจัดระดับชั้นข้อมูลที่ต่ำเกินไปอาจนำไปสู่ผลเสียหายและเป็นอันตรายต่อผลประโยชน์ของข้อมูล
- การยอมให้ชุดข้อมูลมีความเสี่ยงเพื่อการใช้ประโยชน์จากข้อมูลที่มากขึ้น ในการจัดระดับชั้นข้อมูลที่มีระดับชั้นข้อมูลเดียวมีแนวโน้มที่จะส่งผลกระทบ (โดยเฉพาะอย่างยิ่งในส่วนที่เกี่ยวข้องกับข้อมูลส่วนบุคคล) มากกว่ากรณีเดียว โดยทั่วไปจะไม่ส่งผลให้มีการจัดระดับชั้นข้อมูลในระดับที่สูงขึ้น แต่อาจต้องมีการจัดการเพิ่มเติม อย่างไรก็ตาม หากการเก็บรวบรวมข้อมูลส่งผลให้มีการสร้างข้อมูลที่มีความอ่อนไหวมากขึ้นควรพิจารณาจัดระดับชั้นข้อมูลที่มีระดับชั้นความลับที่สูงที่สุด
- ระดับความเสี่ยงของข้อมูลอาจเปลี่ยนแปลงเมื่อเวลาผ่านไปตามวงรอบ และอาจจำเป็นต้องจัดระดับชั้นข้อมูลใหม่ (Declassification) ตัวอย่างเช่น หากเอกสารถูกยกเลิกการจัดระดับชั้นข้อมูล หรือเปลี่ยนการติดป้าย หรือแท็ก ไฟล์ข้อมูลควรปรับเปลี่ยนเพื่อแสดงระดับชั้นข้อมูลใหม่ภายในเอกสารด้วย
- ทั้งนี้ ตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม กำหนดไว้ว่า “การปรับชั้นความลับ” หมายความว่า การลดหรือเพิ่มชั้นความลับของข้อมูลข่าวสารลับและให้หมายความรวมถึงการยกเลิกชั้นความลับของข้อมูลข่าวสารลับนั้นด้วย โดยผู้บังคับบัญชาตามสายงานมีอำนาจปรับชั้นความลับได้เมื่อพิจารณาเห็นว่าการกำหนดชั้นความลับไม่เหมาะสม แต่ต้องแจ้งให้ผู้กำหนดชั้นความลับเดิมทราบ

การศึกษาเปรียบเทียบการจัดระดับชั้นข้อมูล

จากการเปรียบเทียบการจัดระดับชั้นข้อมูลของประเทศไทยและต่างประเทศทั้งหน่วยงานภาครัฐและภาคเอกชน [10] – [13] พบว่า จัดระดับชั้นข้อมูลสามารถแบ่งได้ 5 ระดับ ได้แก่ 1) ชั้นเปิดเผย (Open) 2) ชั้นเผยแพร่ภายในองค์กร (Private) 3) ชั้นลับ (Confidential / Sensitive) 4) ชั้นลับมาก (Secret / Medium Sensitive) และ 5) ชั้นลับที่สุด (Top secret / Highly Sensitive) โดยประเทศไทยและหน่วยงานในต่างประเทศมีระดับชั้นข้อมูลที่สอดคล้องและเป็นไปในทิศทางเดียวกัน แต่อาจมีความแตกต่างกันตามลักษณะการใช้งานของประเภทหน่วยงานดังภาพ

Case Study / Data Class. Level	Thailand	Public Sector		Private Sector		Education Domain		
		US	UK	AWS	Netwrix	Clark	UNSW	Harvard
Public / Open	✓			✓	✓	✓	✓	✓
Private / Restrict / Internal Use			✓	✓		✓	✓	✓
Confidential / Sensitive	✓	✓		✓	✓	✓	✓	✓
Secret / Medium Sensitive	✓	✓	✓	✓				✓
Top secret / Highly Sensitive	✓	✓	✓	✓	✓	✓	✓	✓

ภาพที่ 3 การศึกษาเปรียบเทียบ Data Classification Schemes

2.2 วิธีการจัดระดับชั้นข้อมูล

วิธีการจัดระดับชั้นข้อมูลมักเกี่ยวข้องกับแท็กและป้ายกำกับจำนวนมากที่กำหนดประเภทของข้อมูล การรักษาความลับ ความสมบูรณ์ของข้อมูล และความพร้อมใช้งานอาจถูกนำมาพิจารณาในกระบวนการจัดชั้นของข้อมูล ระดับความอ่อนไหวของข้อมูลมักถูกจัดระดับชั้นตามระดับความสำคัญหรือการรักษาความลับที่แตกต่างกัน ซึ่งสัมพันธ์กับมาตรการรักษาความปลอดภัยที่ใช้เพื่อปกป้องแต่ละระดับการ จัดระดับชั้นข้อมูลโดยพิจารณาตามมาตรฐานอุตสาหกรรม/สากลทั่วไปสามารถจัดระดับชั้นข้อมูลเป็น 3 ประเภทหลักตาม

- **เนื้อหา (Content-based)** จะตรวจสอบและตีความไฟล์ของข้อมูลที่มีความอ่อนไหว
- **บริบท (Context-based)** จะพิจารณาแอปพลิเคชัน สถานที่ หรือผู้สร้างท่ามกลางตัวแปรอื่นๆ เป็นตัวบ่งชี้ทางอ้อมของข้อมูลที่มีความอ่อนไหว
- **ผู้ใช้ (User-based)** ขึ้นอยู่กับคู่มือการเลือกผู้ใช้ปลายทางของแต่ละเอกสาร การจัดระดับชั้นข้อมูลตามผู้ใช้ขึ้นอยู่กับความรู้ของผู้ใช้และดุลยพินิจในการสร้าง แก้ไข ตรวจสอบ หรือเผยแพร่เพื่อตั้งค่าสถานะเอกสารที่มีความอ่อนไหว

ภาพที่ 4 CIA Triad Model

ทั้งนี้ วิธีการจัดระดับชั้นข้อมูลเพื่อจัดการข้อมูลในกระบวนงานที่เกี่ยวข้องกับภารกิจสามารถพิจารณาจากเนื้อหา บริบท และผู้ใช้อาจเป็นได้ทั้งถูกหรือผิด ขึ้นอยู่กับพันธกิจของหน่วยงาน และประเภทข้อมูล โดยข้อมูลข่าวสารลับอาจมีการปรับจัดระดับชั้นข้อมูลได้ตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม โดยสามารถจัดระดับชั้นข้อมูลเป็นระดับ ลับ (Confidential / Sensitive) ลับมาก (Secret / Medium Sensitive) ลับที่สุด (Top secret / Highly Sensitive) ในตัวอย่างนี้ ข้อมูลสาธารณะแสดงถึงข้อมูลที่มีความอ่อนไหวน้อยที่สุดโดยมีข้อกำหนดด้านความปลอดภัยต่ำสุด ในขณะที่ข้อมูลที่ถูกจำกัดการใช้อยู่ในประเภทความปลอดภัยสูงสุดและแสดงถึงข้อมูลที่มีความอ่อนไหวมากที่สุด การจัดระดับชั้นข้อมูลนี้มักเป็นจุดเริ่มต้นสำหรับองค์กรหลายแห่ง ตามด้วยขั้นตอนการระบุและติดแท็กเพิ่มเติมโดยติดป้ายกำกับข้อมูลตามความเกี่ยวข้องกับองค์กร คุณภาพ และระดับชั้นข้อมูลอื่นๆ ซึ่ง

กระบวนการจัดชั้นของข้อมูลที่ประสบความสำเร็จมากที่สุดถูกใช้ตามกระบวนการติดตามผลการดำเนินงานและกรอบแผนงานเพื่อจัดเก็บข้อมูลสำคัญไว้ในที่ที่เหมาะสม

โดยการจัดระดับชั้นข้อมูลถือเป็นส่วนพื้นฐานในการรักษาความปลอดภัยข้อมูลขององค์กรและบุคคลที่สามารถเข้าถึงได้ เป็นกระบวนการในการระบุและกำหนดระดับความอ่อนไหวหรือการรักษาความลับที่กำหนดไว้ล่วงหน้าให้กับข้อมูลประเภทต่างๆ หากองค์กรไม่ได้จัดระดับชั้นข้อมูลอย่างเหมาะสม จะไม่สามารถปกป้องข้อมูลได้อย่างถูกต้องหรือป้องกันไม่ให้มีการเข้าถึง การใช้ การหยุดชะงัก การแก้ไข หรือการทำลายโดยไม่ได้รับอนุญาตขณะอยู่ในที่จัดเก็บ ซึ่งจากมุมมองของความปลอดภัยของข้อมูล CIA Triad Model ถูกใช้เพื่อเป็นแนวทางในนโยบายการรักษาความปลอดภัยข้อมูลและการจัดระดับชั้นข้อมูลภายในองค์กร

- **ด้านความลับ (Confidentiality)** การรักษาความลับนั้นเทียบเท่ากับความเป็นส่วนตัวโดยประมาณ ต้องจำกัดการเข้าถึงเฉพาะผู้ที่ได้รับอนุญาตเท่านั้นเพื่อดูข้อมูลที่มีความอ่อนไหว

- **ด้านความถูกต้อง ครบถ้วนสมบูรณ์ ความคงสภาพ (Integrity)** ความสมบูรณ์เกี่ยวข้องกับการรักษาความสอดคล้องของข้อมูล ข้อมูลต้องไม่เปลี่ยนแปลงในระหว่างการส่ง และควรสอดคล้องกันตลอดวงจรชีวิตทั้งหมด

- **ด้านความพร้อมใช้งาน (Availability)** ความพร้อมใช้งานทำให้แน่ใจได้ว่าระบบทำงานและใช้งานได้ และไม่มีการสึกหรอเนื่องจากความล้มเหลวของฮาร์ดแวร์หรือซอฟต์แวร์

ดังนั้น การจัดระดับชั้นข้อมูลจะพิจารณาร่วมกับวัตถุประสงค์ด้านความมั่นคงปลอดภัย (Security) ของระบบเทคโนโลยีสารสนเทศ และความเสี่ยง (Risks) ที่คาดว่าจะส่งผลกระทบ เช่น ข้อมูลสาธารณะก็มีความเสี่ยงหรือความอ่อนไหวในระดับต่ำ ส่วนข้อมูลที่ต้องการความคุ้มครองสูงก็จะมีระดับความเสี่ยงสูง ซึ่งภาครัฐหลายประเทศได้มีการจัดระดับชั้นข้อมูลเป็น สาธารณะ เผยแพร่ภายในองค์กร ลับ ลับมาก และลับที่สุด

3. หลักเกณฑ์การจัดระดับชั้นข้อมูล

3.1 เป้าประสงค์

หลักเกณฑ์การจัดระดับชั้นข้อมูลภาครัฐจัดทำขึ้นเพื่อใช้ ซึ่งหลักเกณฑ์นี้จะช่วยให้หน่วยงานของรัฐสามารถจัดการข้อมูลในกระบวนงานที่เกี่ยวข้องกับภารกิจของหน่วยงานได้อย่างมีประสิทธิภาพ โดยในการพิจารณาว่าจะปกป้องคุ้มครองและจัดการข้อมูลอย่างไรนั้นขึ้นอยู่กับการพิจารณาประเภท ความสำคัญ และการใช้งานของข้อมูล โดยเป็นการระบุระดับการคุ้มครองข้อมูลขั้นต่ำที่จำเป็นเมื่อดำเนินภารกิจขององค์กรและแบ่งปันข้อมูลระหว่างหน่วยงานภาครัฐโดยอ้างอิงจากการจัดระดับชั้นข้อมูลที่ได้รับการจัดการ (Handled)

โดย**หลักเกณฑ์นี้จะใช้เพื่อพิจารณากำหนดระดับชั้นข้อมูลภาครัฐ** และเพื่อเป็นเครื่องมือประกอบการใช้ดุลพินิจของผู้มีอำนาจในการตัดสินใจกำหนดระดับชั้นข้อมูล สามารถกำหนดการเข้าถึงและใช้งานข้อมูลและกำกับดูแลข้อมูลที่มีความอ่อนไหวหรือที่มีชั้นความลับอย่างเหมาะสมเพื่อรักษาความเป็นส่วนตัวและความปลอดภัยของข้อมูล รวมทั้งกำหนดนโยบายการแบ่งปันข้อมูลระหว่างหน่วยงานภาครัฐโดยไม่ขัดต่อข้อกฎหมายที่เกี่ยวข้อง

3.2 หลักเกณฑ์การจัดระดับชั้นข้อมูลภาครัฐ

ตามมาตรฐาน NIST SP 800-60 การจัดหมวดหมู่ความปลอดภัยของข้อมูลและระบบสารสนเทศ ได้กำหนดว่า ข้อมูลควรมี**การพิจารณาหมวดหมู่ก่อนการจัดระดับชั้นข้อมูล** โดยการจัดหมวดหมู่ข้อมูลสามารถ

พิจารณาได้จากกฎหมายที่เกี่ยวข้อง หรือภารกิจของหน่วยงาน เพื่อใช้เป็นพื้นฐานในการประเมินผลกระทบและกำหนดมาตรการควบคุมที่เหมาะสม เพราะทำให้เจ้าของข้อมูลหรือผู้ที่มีส่วนเกี่ยวข้องเข้าใจบริบทของข้อมูลมากขึ้น ซึ่งสอดคล้องกับกรอบธรรมาภิบาลข้อมูลภาครัฐตามประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ พ.ศ. 2563 และ ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง มาตรฐานรัฐบาลดิจิทัลว่าด้วยว่าด้วยกรอบธรรมาภิบาลข้อมูลภาครัฐ ฉบับปรับปรุง: แนวปฏิบัติ พ.ศ. 2566 ซึ่งมีการกำหนดการพิจารณาหมวดหมู่ข้อมูลและการจัดระดับชั้นข้อมูล

ตามกรอบธรรมาภิบาลข้อมูลภาครัฐได้มีการแบ่งระดับชั้นข้อมูลออกเป็น ชั้นเปิดเผย (Open) สู่สาธารณะ เปิดเผยเมื่อได้รับอนุญาต ได้แก่ ชั้นเผยแพร่ภายในองค์กร (Private) ชั้นลับ (Confidential) และ ชั้นลับมาก (Secret) และเปิดเผยไม่ได้/ปกปิด ได้แก่ ชั้นลับที่สุด (Top Secret) ทั้งนี้ ข้อมูลใช้ภายในควรมีการพิจารณาหมวดหมู่ตามธรรมาภิบาลข้อมูลภาครัฐ ก่อนจัดแบ่งระดับชั้นข้อมูลภาครัฐ ดังแสดงตามภาพที่ 5

หมวดหมู่ข้อมูล \ ระดับชั้นข้อมูล	เปิดเผย (Open)	เผยแพร่ภายในองค์กร (Private)	ลับ (Confidential)	ลับมาก (Secret)	ลับที่สุด (Top Secret)
ข้อมูลสาธารณะ	พ.ร.บ ข้อมูลข่าวสารของทางราชการ พ.ศ. 2540 (มาตรา 7 และมาตรา 9 มรด. 8 : 2567 ว่าด้วย แนวทางการเปิดเผยข้อมูลเปิดภาครัฐ				
ข้อมูลใช้ภายใน		• มาตรฐาน ISO/IEC 27001: 2022			
ข้อมูลส่วนบุคคล		• พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (มาตรา 24- 27)	• พ.ร.บ ข้อมูลข่าวสารของทางราชการ พ.ศ. 2540 (มาตรา 9 และมาตรา 15 ที่เปิดเผยได้)		
ข้อมูลความลับทางราชการ	สามารถทบทวนหมวดหมู่และระดับชั้นข้อมูลได้ตามระยะเวลาและเทคโนโลยีที่เปลี่ยนแปลง		• ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.2544 และที่แก้ไขเพิ่มเติม		• พ.ร.บ ข้อมูลข่าวสารของทางราชการ มาตรา 15
ข้อมูลความมั่นคง					• พ.ร.บ ข้อมูลข่าวสารของทางราชการ มาตรา 14 • นโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ

ภาพที่ 5 การพิจารณาหมวดหมู่และการจัดระดับชั้นข้อมูลภาครัฐ

โดยมีแนวทางการพิจารณาหมวดหมู่และการจัดระดับชั้นข้อมูลภาครัฐดังนี้

1) จัดทำกรอบนโยบายการบริหารจัดการข้อมูลและการพิจารณาหมวดหมู่และจัดระดับชั้นข้อมูลตามที่ สพร. แนะนำ หรือที่หน่วยงานประกาศ

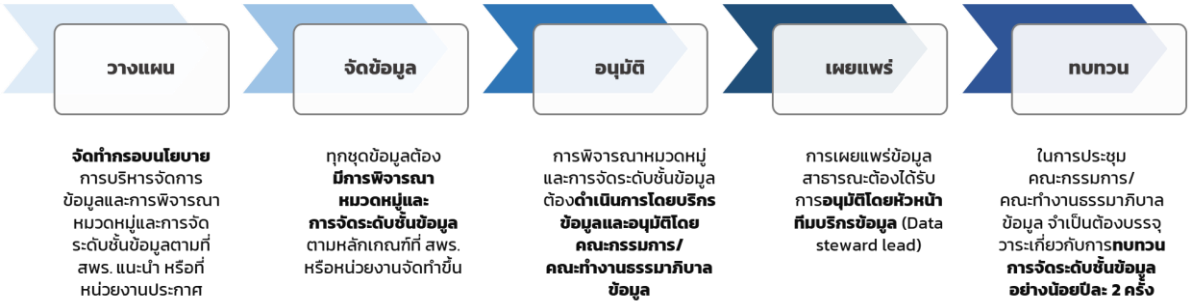
2) หากหน่วยงานมีกฎหมายหรือกฎระเบียบที่เกี่ยวข้องกับการพิจารณาหมวดหมู่และจัดระดับชั้นข้อมูลของตนเอง ให้หน่วยงานพิจารณากฎหมายหรือกฎระเบียบที่เกี่ยวข้องกับภาระกิจตนเองก่อน

3) ทุกชุดข้อมูลต้องมีการพิจารณาหมวดหมู่และจัดระดับชั้นข้อมูลตามหลักเกณฑ์ที่ สพร. หรือหน่วยงานจัดทำขึ้น

4) การพิจารณาจัดหมวดหมู่และจัดระดับชั้นข้อมูลต้องดำเนินการโดยบริกรข้อมูลและอนุมัติ โดยคณะกรรมการ/คณะทำงานธรรมาภิบาลข้อมูล

5) การเผยแพร่ข้อมูลสาธารณะต้องได้รับการอนุมัติโดยหัวหน้าทีมบริกรข้อมูล (Data steward lead)

6) ในการประชุมคณะกรรมการ/คณะทำงานธรรมาภิบาลข้อมูล จำเป็นต้องบรรจุวาระเกี่ยวกับการทบทวนการจัดระดับชั้นข้อมูลอย่างน้อยปีละ 2 ครั้ง



ภาพที่ 6 แนวทางการพิจารณาหมวดหมู่และการจัดระดับชั้นข้อมูลภาครัฐ

สำหรับคำแนะนำในการดำเนินการพิจารณาหมวดหมู่และจัดระดับชั้นข้อมูลของหน่วยงานภาครัฐ เพื่อให้เป็นมาตรฐานเดียวกัน มีดังต่อไปนี้

✓ การควบคุมและการดำเนินการเกี่ยวกับข้อมูลข่าวสารลับให้เป็นดุลพินิจของหัวหน้าหน่วยงานของรัฐนั้นๆ ที่จะกำหนดแนวทางที่เหมาะสม ทั้งการมอบหมายหน้าที่หรือ แต่งตั้งเจ้าหน้าที่รับผิดชอบ โดยต้องคำนึงถึงการปฏิบัติในการเปิดเผยข้อมูลให้เป็นไปตามพระราชบัญญัติข้อมูลข่าวสารของราชการฯ ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม ระเบียบสำนักนายกรัฐมนตรีว่าด้วยงานสารบรรณ (ฉบับที่ 4) พ.ศ. 2564 และระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. 2552 หรือกฎหมาย กฎระเบียบที่เกี่ยวข้อง

ทั้งนี้ ในกรณีของการลงทะเบียนบัญชีข้อมูลหน่วยงานที่เป็นข้อมูลข่าวสารลับ หัวหน้าหน่วยงานของรัฐสามารถแต่งตั้งให้นายทะเบียนข้อมูลข่าวสารลับเป็นนายทะเบียนบัญชีข้อมูลหน่วยงาน หรืออาจกำหนดให้นายทะเบียนบัญชีข้อมูลหน่วยงานให้เข้าถึงข้อมูลข่าวสารลับได้เฉพาะเรื่องที่ได้รับมอบหมายเท่านั้น ตามข้อ 8 ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม ตามที่ระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. 2552 และประกาศที่เกี่ยวข้อง กำหนดไว้

✓ ทุกฟิลด์ในแต่ละชุดข้อมูลถือว่ามีระดับชั้นเท่ากัน

✓ ในกรณีชุดข้อมูลที่มีผลกระทบในเชิงพื้นที่ เช่น ประเทศ จังหวัด ท้องถิ่น เป็นต้น หน่วยงานสามารถกำหนดเกณฑ์ประกอบการพิจารณาเพิ่มเติมได้

✓ หากหน่วยงานมีการอ้างอิงหลักเกณฑ์และ/หรือมาตรฐานของต่างประเทศอยู่แล้วให้ดำเนินการตามมาตรฐานดังกล่าว

✓ สำหรับชุดข้อมูลที่มีการจัดระดับความลับในหมวดหมู่ข้อมูลส่วนบุคคล ข้อมูลความลับทางราชการ และข้อมูลความมั่นคง รวมถึงข้อมูลใช้ภายในองค์กร จำเป็นต้องระบุสิทธิ์ในการเข้าถึงและใช้งานข้อมูล

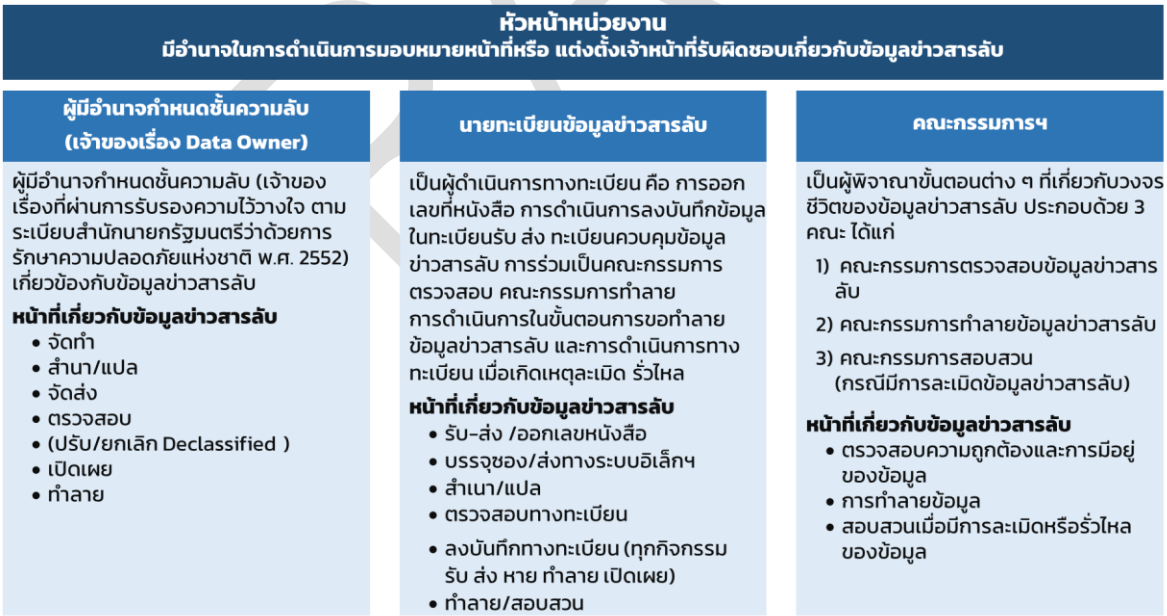
✓ หากชุดข้อมูลมีความอ่อนไหวทั้งด้านความเป็นส่วนตัว และความมั่นคง หน่วยงานสามารถพิจารณาแยกชุดข้อมูลและตัดสินใจเผยแพร่หรือไม่เผยแพร่ข้อมูลให้สอดคล้องกับข้อกฎหมายที่เกี่ยวข้องและเกณฑ์การจัดระดับชั้นข้อมูลตามที่หน่วยงานกำหนด

✓ ข้อมูลอ่อนไหวที่ได้รับการจัดระดับชั้นข้อมูลจะต้องมีกระบวนการในการเข้าถึงข้อมูลตามกระบวนการและปฏิบัติตามข้อกฎหมายที่เกี่ยวข้องหรือตามข้อกำหนดของหน่วยงาน

✓ ข้อมูลระดับชั้น “ลับที่สุด” อ้างอิงตามข้อมูลข่าวสารตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม รวมถึงร่างระเบียบว่าด้วยการรักษาความลับของทาง

ราชการ (ฉบับที่ ..) พ.ศ. .... ตามที่ประชุมคณะรัฐมนตรี (ครม.) มีมติเห็นชอบร่างระเบียบ โดยมีการกำหนดให้เพิ่มเติมหมวด 5 ข้อมูลข่าวสารลับอิเล็กทรอนิกส์ จำนวน 26 ข้อ อาทิ ส่วนที่ 6 การส่งและการรับ ข้อ 50/16 การส่งและการรับข้อมูลข่าวสารลับอิเล็กทรอนิกส์โดยปกติให้ดำเนินการเฉพาะข้อมูลข่าวสารลับอิเล็กทรอนิกส์ชั้น “ลับ” และ “ลับมาก” ข้อมูลข่าวสารอิเล็กทรอนิกส์ชั้น “ลับที่สุด” ห้ามหน่วยงานของรัฐดำเนินการส่งและรับผ่านระบบอิเล็กทรอนิกส์ เว้นแต่หน่วยงานของรัฐมีความจำเป็นต้องดำเนินการส่งและรับผ่านระบบอิเล็กทรอนิกส์ให้ทำความตกลงกับองค์การรักษาความปลอดภัยเพื่อจัดทำข้อตกลงในการส่งและรับข้อมูลเป็นกรณีพิเศษ ข้อ 50/19 เมื่อนายทะเบียนข้อมูลข่าวสารลับอิเล็กทรอนิกส์ได้รับข้อมูลข่าวสารลับอิเล็กทรอนิกส์จากหน่วยงานอื่นทั้งในประเทศและต่างประเทศที่กำหนดชั้นความลับ ชั้น “ลับ” หรือ “ลับมาก” ให้นายทะเบียนข้อมูลข่าวสารลับอิเล็กทรอนิกส์บันทึกการรับข้อมูลข่าวสารลับอิเล็กทรอนิกส์ในทะเบียนข้อมูลข่าวสารลับอิเล็กทรอนิกส์ และแจ้งเลขทะเบียนรับไปยังผู้ส่ง และจัดส่งข้อมูลข่าวสารลับอิเล็กทรอนิกส์ที่ได้รับนั้นไปยังผู้รับที่มีสิทธิเข้าถึงข้อมูลข่าวสารลับอิเล็กทรอนิกส์นั้น ตามหลักเกณฑ์และวิธีการที่หัวหน้าหน่วยงานของรัฐหรือองค์การรักษาความปลอดภัยกำหนด เป็นต้น

✓ ข้อมูลระดับชั้น “ลับที่สุด” ตามที่ระเบียบสำนักนายกรัฐมนตรีว่าด้วยงานสารบรรณ (ฉบับที่ 4) พ.ศ. 2564 ข้อ 29 กำหนดว่าการติดต่อราชการให้ดำเนินการด้วยระบบสารบรรณอิเล็กทรอนิกส์เป็นหลัก เว้นแต่กรณีที่เป็นข้อมูลข่าวสารลับชั้นลับที่สุดตามระเบียบว่าด้วยการรักษาความลับของทางราชการหรือเป็นสิ่งที่เป็นความลับของทางราชการชั้นลับที่สุดตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความลับของทางราชการ



ภาพที่ 7 ผู้ที่เกี่ยวข้องกับข้อมูลข่าวสารลับ

✓ ในกรณีที่ผู้ร้องขอข้อมูลไม่ได้มีสิทธิ์ตามสิทธิ์การเข้าถึงข้อมูลจำเป็นต้องดำเนินการตามกระบวนการดังต่อไปนี้

- ข้อมูลส่วนบุคคล เจ้าของข้อมูลส่วนบุคคล (Data subject) จะต้องทำการร้องขอผ่านส่วนงานที่ถือครองข้อมูล และส่วนงานที่เป็นเจ้าของข้อมูล (Data owner) โดยแจ้งวัตถุประสงค์ให้ชัดเจน โดยส่วนงานที่เป็นเจ้าของข้อมูล และ ผู้ควบคุมข้อมูลส่วนบุคคล (Data controller) ต้องรับทราบและ

มีสิทธิ์ที่จะปฏิเสธการร้องขอนั้นเว้นแต่จะมีระเบียบหรือประกาศของหน่วยงานรองรับ และต้องเป็นไปตามแนวปฏิบัติตามข้อกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล[3]

- ข้อมูลความลับทางราชการ และ ข้อมูลความมั่นคง ต้องมีการร้องขอผ่านส่วนงานที่เป็นเจ้าของข้อมูล โดยหัวหน้าส่วนงานและบริกรข้อมูลต้องพิจารณาร่วมกัน หากเป็นข้อมูลที่มีความอ่อนไหวหรือมีความเสี่ยงต้องได้รับการอนุมัติ หัวหน้าหน่วยงานของรัฐหรือเจ้าหน้าที่รัฐที่ได้รับมอบหมายเป็นผู้มีอำนาจหน้าที่เปิดเผยข้อมูล โดยการเปิดเผยมีข้อยกเว้นความผิดทางละเมิดตามข้อ 49 และข้อ 50 ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม

- ข้อมูลใช้ภายใน ต้องมีการร้องขอผ่านส่วนงานที่เป็นเจ้าของข้อมูล โดยต้องได้รับอนุญาตจากหัวหน้าส่วนงานและหัวหน้าทีมบริกรข้อมูล

7) เทคโนโลยีการจัดระดับชั้นข้อมูล

- ระดับชั้นข้อมูลจะต้องถูกระบุไว้ในเมทาดาตา ดังนั้นจึงจำเป็นต้องมีระบบในการจัดการเมทาดาตา (Metadata Management System) เพื่อกำหนดสิทธิการเข้าถึงและการนำข้อมูลไปใช้ได้อย่างเหมาะสม รักษาความปลอดภัยของข้อมูล และสอดคล้องกับกฎหมาย กฎระเบียบของหน่วยงาน เพื่อส่งเสริมให้เกิดการแลกเปลี่ยนหรือเปิดเผยข้อมูลของหน่วยงานรัฐได้

- การร้องขอข้อมูลต้องทำผ่านระบบและมีการเก็บบันทึก (Logging System)

3.2.1. เกณฑ์การแบ่งระดับชั้นข้อมูลภาครัฐ (Data Classification Level)

การพิจารณาจัดระดับชั้นข้อมูลภาครัฐตามผลกระทบที่จะเกิดขึ้น ตามแนวมาตรฐานสากลและเป็นไปตามข้อกฎหมายที่เกี่ยวข้อง ซึ่งระดับชั้นข้อมูลสามารถแบ่งได้ 5 ระดับ ได้แก่

1) ชั้นเปิดเผย (Open) สู่สาธารณะ เป็นข้อมูลข่าวสารของราชการที่หน่วยงานของรัฐต้องเปิดเผยให้ประชาชนได้รับรู้ รับทราบ หรือตรวจสอบได้โดยไม่จำเป็นต้องร้องขอ เช่น กฎ มติคณะรัฐมนตรี ข้อบังคับ รายงานผลการ ศึกษาทางวิชาการ และข้อมูลเปิดภาครัฐ ฯลฯ

2) ชั้นเผยแพร่ภายในองค์กร (Private) เปิดเผยเมื่อได้รับอนุญาต เป็นข้อมูลที่องค์กรไม่ได้เผยแพร่โดยอิสระ โดยทั่วไปจะเกี่ยวข้องกับข้อมูลที่มีลักษณะเป็นส่วนตัว (Private) ไม่ว่าจะเป็นข้อมูลบุคคลหรือองค์กร **และแม้ว่าการสูญเสียข้อมูลหรือการเปิดเผยข้อมูลอาจไม่ส่งผลให้เกิดผลกระทบที่สำคัญแต่ก็ไม่พึงประสงค์ที่ให้เปิดเผยโดยไม่ได้รับอนุญาต** เช่น ข้อมูลระเบียน ข้อมูลพนักงาน เอกสารประกอบการปฏิบัติงาน และ วิธีปฏิบัติภายในหน่วยงาน ฯลฯ

3) ชั้นลับ (Confidential) เปิดเผยเมื่อได้รับอนุญาต เป็นข้อมูลที่มีระดับ Confidential หรือ Sensitive จะก่อให้เกิดความสูญเสีย หากมีการเปิดเผยต่อบุคคล/องค์กรที่ไม่ได้รับอนุญาตและส่งผลให้เกิดความอับอายอย่างมากต่อบุคคล/องค์กร และอาจเป็นผลทางกฎหมาย หรือจะก่อให้เกิดความเสียหายแก่**ผลประโยชน์แห่งรัฐ** เช่น ข้อมูลการฟ้องคดี และความเห็นภายในหน่วยงานที่ยังไม่ได้ข้อยุติ ฯลฯ

4) ชั้นลับมาก (Secret) เปิดเผยเมื่อได้รับอนุญาต เป็นข้อมูลที่จัดระดับ Secret หรือ Medium Sensitive สงวนไว้สำหรับข้อมูลที่จะก่อให้เกิดความสูญเสีย/ผลกระทบร้ายแรง อาจทำให้เสีย

[3] ตัวอย่าง เช่น การเปิดเผยข้อมูลส่วนบุคคลสู่สาธารณะต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล (Data subject)

ชื่อเสียงและการสูญเสียทางการเงิน/ทรัพย์สิน ต่อความมั่นคงและ**ผลประโยชน์แห่งรัฐอย่างร้ายแรง หรือที่มีนัยสำคัญ (Importance)** หากสูญหายหรือเปิดเผยอย่างไม่ถูกต้องเหมาะสม เช่น รายงานการแพทย์ ข้อมูลความสัมพันธ์ระหว่างประเทศ และนโยบายสำคัญที่ใช้ปฏิบัติต่อรัฐต่างประเทศ ฯลฯ

5) ชั้นลับที่สุด (Top Secret) เปิดเผยไม่ได้ เป็นข้อมูลที่จัดระดับ Top Secret หรือ Highly Sensitive จำกัดการใช้/ไม่เปิดเผยสำหรับข้อมูลที่จะ**ก่อให้เกิดความสูญเสีย/ผลกระทบ ร้ายแรงที่สุด** อาจทำให้ชื่อเสียงและการสูญเสียทางการเงิน/ทรัพย์สิน ต่อความมั่นคงและ**ผลประโยชน์แห่งรัฐอย่างร้ายแรงหรือที่สำคัญยิ่งยวด (Vital)** หากสูญหายหรือเปิดเผยอย่างไม่ถูกต้องเหมาะสม **ซึ่งในกรณีข้อมูลข่าวสารลับที่สุดให้เป็นไปตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยงานสารบรรณ (ฉบับที่ 4) พ.ศ. 2564 ซึ่งกำหนดว่า "ข้อ 29 การติดต่อราชการให้ดำเนินการด้วยระบบสารบรรณอิเล็กทรอนิกส์เป็นหลัก เว้นแต่กรณีที่เป็นข้อมูลข่าวสารลับชั้นลับที่สุด" และให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544** เช่น ข้อมูลกำลังรบ ข้อมูลด้านการข่าวกรองยุทธศาสตร์ ข้อมูลความมั่นคงเชิงนโยบาย

ทั้งนี้ นิยามการกำหนดข้อมูลข่าวสารลับ ให้อ้างอิงตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม

หน่วยงานสามารถพิจารณาการจัดระดับชั้นข้อมูล โดยใช้เกณฑ์ดังต่อไปนี้

Open	Private *(กระทบระดับบุคคล/องค์กร)*	Confidential / sensitive *(กระทบระดับบุคคล/องค์กร)*	Secret / Medium Sensitive *(กระทบระดับองค์กร/ประเทศ)*	Top secret / Highly Sensitive *(กระทบระดับองค์กร/ประเทศ)*
เกณฑ์การพิจารณาแบ่งระดับชั้นข้อมูล (Classification Criteria)*				
ตาม พ.ร.บ. ข้อมูลข่าวสารฯ **มาตรา 7** หน่วยงานของรัฐต้องส่งข้อมูลข่าวสารของราชการอย่างน้อยดังต่อไปนี้ ต้องลงพิมพ์ในราชกิจจานุเบกษา **มาตรา 9** ภายใต้บังคับมาตรา 14 และมาตรา 15 หน่วยงานของรัฐต้องจัดให้มีข้อมูลข่าวสารของราชการอย่างน้อยดังต่อไปนี้ไว้ให้ประชาชนเข้าตรวจดูได้ ทั้งนี้ ตามหลักเกณฑ์และวิธีการที่คณะกรรมการกำหนด	**ข้อมูลจะถูกจัดเป็นชั้น "Private" หรือไม่** รวมถึงการเปิดเผยโดยไม่ได้รับอนุญาตหรือไม่: ✓ สร้างความทุกข์ใจให้กับบุคคล ✓ ละเมิดการดำเนินการที่เหมาะสมเพื่อรักษาความเชื่อใจของข้อมูลที่ให้โดยบุคคลที่สาม ✓ ละเมิดข้อจำกัดทางกฎหมายในการเปิดเผยข้อมูล ✓ ทำให้เกิดการสูญเสียทางการเงินหรือสูญเสียศักยภาพในการหารายได้ หรือเพื่ออำนวยความสะดวกในการได้รับผลประโยชน์ที่ไม่เหมาะสม ✓ ให้ผลประโยชน์ที่ไม่เป็นธรรมแก่บุคคลหรือองค์กร ✓ สูญเสียความได้เปรียบขององค์กรเชิงพาณิชย์หรือนโยบายในการเจรจากับผู้อื่น	**ข้อมูลจะถูกจัดเป็นชั้น "Confidential" หรือไม่** รวมถึงการเปิดเผยโดยไม่ได้รับอนุญาตหรือไม่: ✓ ส่งผลกระทบต่อความสัมพันธ์กับองค์กร/ประเทศอื่นในทางลบ ✓ ก่อให้เกิดความทุกข์ใจอย่างมากต่อบุคคล ✓ ทำให้เกิดการสูญเสียทางการเงินหรือการสูญเสียศักยภาพในการหารายได้หรือเพื่ออำนวยความสะดวกในการได้รับผลประโยชน์หรือความได้เปรียบที่ไม่เหมาะสมสำหรับบุคคลหรือองค์กรหรือประเทศต่างๆ ✓ ฝ่าฝืนการดำเนินการที่เหมาะสมเพื่อรักษาความมั่นใจของข้อมูลที่ให้โดยบุคคลที่สาม ✓ ขัดขวางการพัฒนาที่มีประสิทธิภาพหรือการดำเนินงานตามนโยบายขององค์กร ✓ ฝ่าฝืนข้อจำกัดทางกฎหมายในการเปิดเผยข้อมูล ✓ สูญเสียความได้เปรียบขององค์กรเชิงพาณิชย์หรือนโยบายในการเจรจากับผู้อื่น ✓ บ่อนทำลายการจัดการที่เหมาะสมและการดำเนินงานขององค์กร	**ข้อมูลจะถูกจัดเป็นชั้น "Secret" หรือไม่** รวมถึงการเปิดเผยโดยไม่ได้รับอนุญาตหรือไม่: ✓ สร้างความเสียหายอย่างมีนัยสำคัญต่อความสัมพันธ์กับองค์กรอื่นๆ (เช่น ก่อให้เกิดการประท้วงอย่างเป็นทางการหรือการลงโทษอื่นๆ) ✓ สร้างความเสียหายต่อประสิทธิภาพการดำเนินงานหรือความปลอดภัยขององค์กร/ประเทศ ✓ ภารกิจงานสำคัญที่กระทบต่อด้านการเงินขององค์กร หรือผลประโยชน์ทางเศรษฐกิจและการค้าของประเทศ ✓ บ่อนทำลายศักยภาพทางการเงินส่วนใหญ่ขององค์กร/ประเทศ ✓ ขัดขวางการพัฒนาหรือการดำเนินงานของนโยบายองค์กร/ประเทศอย่างจริงจัง ✓ ปิดตัวลงหรือขัดขวางการดำเนินงาน/โครงการที่สำคัญขององค์กร/ประเทศ	**ข้อมูลจะถูกจัดเป็นชั้น "Top Secret"** ตาม พ.ร.บ. ข้อมูลข่าวสารฯ รวมถึงการเปิดเผยโดยไม่ได้รับอนุญาตหรือไม่: มาตรา 14 ข้อมูลข่าวสารของราชการที่อาจก่อให้ เกิดความเสียหายต่อสถาบันพระมหากษัตริย์จะเปิดเผยมิได้ มาตรา 15 ข้อมูลข่าวสารของราชการ... หน่วยงานของรัฐหรือเจ้าหน้าที่ของรัฐอาจมีคำสั่งมิให้เปิดเผยก็ได้ โดยคำนึงถึงการปฏิบัติหน้าที่ตามกฎหมาย ประโยชน์สาธารณะ และประโยชน์ของเอกชนที่เกี่ยวข้องประกอบกัน ✓ ก่อให้เกิดความเสียหายต่อความมั่นคงของประเทศ ความสัมพันธ์ระหว่างประเทศ และความมั่นคงในทางเศรษฐกิจหรือการคลังของประเทศ ✓ ทำให้การบังคับใช้กฎหมายเสื่อมประสิทธิภาพ หรือไม่อาจสำเร็จตามวัตถุประสงค์ได้ ไม่ว่าจะเกี่ยวกับการฟ้องคดี การป้องกัน การปราบปราม การทดสอบ การตรวจสอบ หรือการรู้แหล่งที่มาของข้อมูลข่าวสารหรือไม่ก็ตาม ✓ ความเห็นหรือคำแนะนำภายในหน่วยงานของรัฐในการดำเนินการเรื่องหนึ่งเรื่องใด แต่ทั้งนี้ไม่รวมถึงรายงานทางวิชาการ รายงาน ข้อเท็จจริง หรือข้อมูลข่าวสารที่

Open	Private *(กระทบระดับบุคคล/องค์กร)*	Confidential / sensitive *(กระทบระดับบุคคล/องค์กร)*	Secret / Medium Sensitive *(กระทบระดับองค์กร/ประเทศ)*	Top secret / Highly Sensitive *(กระทบระดับองค์กร/ประเทศ)*
				นำมาใช้ในการทำความเห็นหรือคำแนะนำภายในดังกล่าว ✓ การเปิดเผยจะก่อให้เกิดอันตรายต่อชีวิตหรือความปลอดภัยของบุคคลหนึ่งบุคคลใด ✓ ข้อมูลข่าวสารของราชการที่มีกฎหมายคุ้มครองมิให้เปิดเผย หรือข้อมูลข่าวสารที่มีผู้ให้มาโดยไม่ประสงค์ให้ทางราชการนำไปเปิดเผยต่อผู้อื่น

หมายเหตุ * เกณฑ์การพิจารณาแบ่งระดับชั้นข้อมูล ได้พิจารณาจากผลกระทบ (Impact) ทั้งด้านการเงินและสินทรัพย์ (Financial & Assets) ด้านภาพลักษณ์/ชื่อเสียง (Reputation) ด้านผู้ใช้บริการหรือประชาชน (Operations) ด้านการดำเนินการตามกฎหมาย (Legal and Regulation) โดยไม่มีการจำกัดเงื่อนไขเกณฑ์การพิจารณาการจัดระดับชั้นข้อมูล

การจัดระดับชั้นข้อมูลจะส่งผลให้ข้อมูลได้รับการดูแล โดยหน่วยงานสามารถกำหนดเงื่อนไขการเข้าถึงข้อมูลได้ดังตัวอย่างต่อไปนี้

Open	Private *(กระทบระดับบุคคล/องค์กร)*	Confidential / sensitive *(กระทบระดับบุคคล/องค์กร)*	Secret / Medium Sensitive *(กระทบระดับองค์กร/ประเทศ)*	Top secret / Highly Sensitive *(กระทบระดับองค์กร/ประเทศ)*
การเข้าถึง (Access Control)				
ไม่มีการจำกัดการเข้าถึงข้อมูล/เปิดเผยสู่สาธารณะ	**เจ้าหน้าที่ส่วนใหญ่ขององค์กร**มีแนวโน้มที่จะจัดการกับข้อมูล “Private" ในระหว่างการทำงาน/เปิดเผยเมื่อได้รับอนุญาต	มักจะได้รับการจัดการโดย**ผู้บริหารระดับกลางขึ้นไป** โดยที่เจ้าหน้าที่บางคนที่มีระดับต่ำกว่าจะได้รับการเข้าถึงเฉพาะในบางสถานการณ์เท่านั้น/เปิดเผยเมื่อได้รับอนุญาต	จะต้องได้รับการควบคุมอย่างเข้มงวดโดย**ผู้บริหารระดับสูง** และในหลายกรณีจะมีการแจกจ่ายสำเนาเอกสาร ตามระเบียบขั้นตอนเฉพาะขององค์กรและ/หรือประเทศ/เปิดเผยเมื่อได้รับอนุญาต	คำสั่งมิให้เปิดเผยข้อมูลข่าวสารของราชการจะกำหนดเงื่อนไขก็ได้ แต่**ต้องระบุว่าที่เปิดเผยไม่ได้/ปกปิดเพราะเป็นข้อมูลข่าวสารประเภทใดและเพราะเหตุใด** และให้ถือว่าการมีคำสั่งเปิดเผยข้อมูลข่าวสารของราชการ**เป็นดุลพินิจของเจ้าหน้าที่ของรัฐตามลำดับสายการบังคับบัญชา** แต่อาจอุทธรณ์ต่อคณะกรรมการวินิจฉัยการเปิดเผยข้อมูลข่าวสารได้

3.2.2. เกณฑ์การประเมินความเสี่ยงและผลกระทบของการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต (Data Risk Assessment)

1) ข้อควรคำนึงถึง

(1) วัตถุประสงค์ด้านความปลอดภัย (CIA) เทียบกับโอกาสที่จะเกิดผลกระทบ (Impact) ตามมาตรฐาน NIST 800-60 Volume 1. and 2. Guide for Mapping Types of Information and Information Systems to Security Categories ซึ่งสอดคล้องกับแนวการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ตามมาตรา 54 แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

(2) องค์ประกอบการกำหนดระดับชั้นข้อมูล ตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 ข้อ 19 การกำหนดให้ข้อมูลข่าวสารอยู่ในระดับชั้นข้อมูลใด ให้พิจารณาถึงองค์ประกอบอย่างน้อยดังต่อไปนี้ ความสำคัญของเนื้อหา แหล่งที่มาของข้อมูลข่าวสาร วิธีการนำไปใช้ประโยชน์ จำนวนบุคคลที่ควรรับทราบ ผลกระทบหากมีการเปิดเผย และ หน่วยงานของรัฐที่รับผิดชอบในฐานะเจ้าของเรื่องหรือผู้อนุมัติ

(3) ผลประโยชน์แห่งชาติ ตามนโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ

- การมีเอกราช อธิปไตย และบูรณภาพแห่งเขตอำนาจรัฐ
- การดำรงอยู่อย่างมั่นคงยั่งยืนของสถาบันหลักของชาติ
- การดำรงอยู่อย่างมั่นคงของชาติและประชาชนจากภัยคุกคามทุกรูปแบบ
- การอยู่ร่วมกันในชาติอย่างสันติสุข เป็นปึกแผ่น มั่นคงทางสังคม ท่ามกลางพหุสังคมและการมีเกียรติ และศักดิ์ศรีของความเป็นมนุษย์
- ความเจริญเติบโตของชาติ ความเป็นธรรม และความอยู่ดีของประชาชน
- ความยั่งยืนของฐานทรัพยากรธรรมชาติ สิ่งแวดล้อม ความมั่นคงทางพลังงาน อาหาร
- ความสามารถในการรักษาผลประโยชน์ของชาติภายใต้การเปลี่ยนแปลงของสภาวะแวดล้อม ระหว่างประเทศ
- การอยู่ร่วมกันอย่างสันติ มีเกียรติและศักดิ์ศรีในประชาคมอาเซียนและประชาคมโลก

2) ระดับผลกระทบตามวัตถุประสงค์ด้านความปลอดภัยของข้อมูล (CIA)

วัตถุประสงค์ด้านความปลอดภัย (Security Objective)	ผลกระทบ (Impact)* และ ผลประโยชน์แห่งชาติ (National Interests)		
	น้อย (Low)	ปานกลาง (Moderate)	สูง (High)
ด้านความลับ (Confidentiality) การรักษาข้อจำกัดในการได้รับอนุญาตให้เข้าถึงได้และเปิดเผยเฉพาะผู้มีสิทธิ์ รวมทั้งวิธีการคุ้มครองความเป็นส่วนตัว (privacy) และกรรมสิทธิ์ (proprietary) ของข้อมูลข่าวสาร	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบน้อย/อย่างจำกัด (limited) และเกิดผลประโยชน์แห่งชาติสำคัญน้อย (Less Important or Secondary National Interests)	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบอย่างร้ายแรง (serious) และเกิดผลประโยชน์แห่งชาติที่สำคัญ (Important National Interests)	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบอย่างร้ายแรงมาก (severe or catastrophic) และเกิดผลประโยชน์แห่งชาติสำคัญยิ่ง (Extremely Important National Interests)

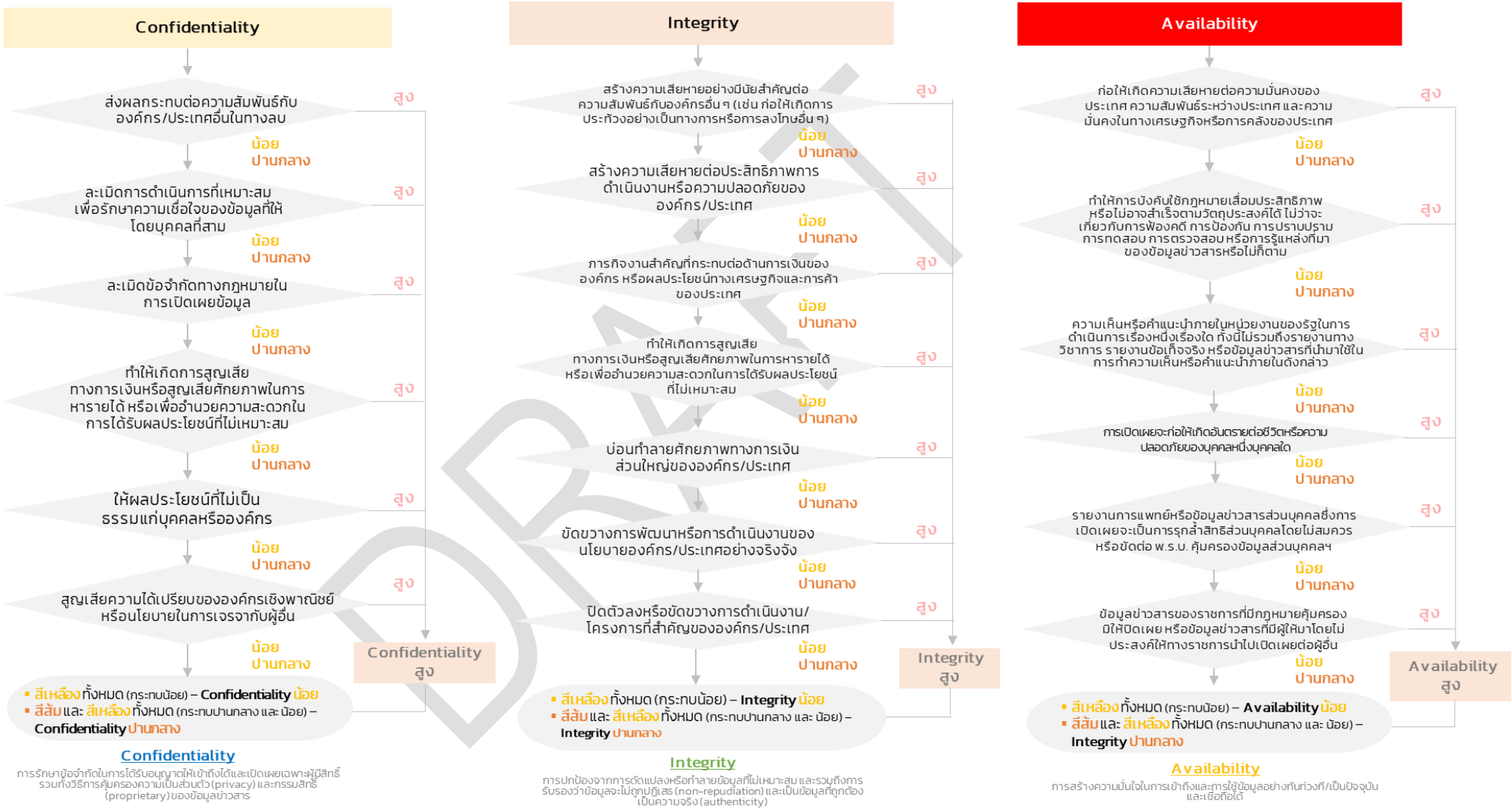
วัตถุประสงค์ด้านความปลอดภัย (Security Objective)	ผลกระทบ (Impact)* และ ผลประโยชน์แห่งชาติ (National Interests)		
	น้อย (Low)	ปานกลาง (Moderate)	สูง (High)
ด้านความถูกต้อง ครบถ้วนสมบูรณ์ ความคงสภาพ (Integrity) การปกป้องจากการดัดแปลงหรือทำลายข้อมูลที่ไม่เหมาะสม และรวมถึงการรับรองว่าข้อมูลจะไม่ถูกปฏิเสธ (non-repudiation) และเป็นข้อมูลที่ถูกต้องเป็นความจริง (authenticity)	การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบน้อย/อย่างจำกัด (limited) และเกิดผลประโยชน์แห่งชาติสำคัญน้อย (Less Important or Secondary National Interests)	การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบอย่างร้ายแรง (serious) และเกิดผลประโยชน์แห่งชาติที่สำคัญ (Important National Interests)	การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบอย่างร้ายแรงมาก (severe or catastrophic) และเกิดผลประโยชน์แห่งชาติสำคัญยิ่ง (Extremely Important National Interests)
ด้านความพร้อมใช้งาน (Availability) การสร้างความมั่นใจในการเข้าถึงและการใช้ข้อมูลอย่างทันท่วงที/เป็นปัจจุบันและเชื่อถือได้	การหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลข่าวสารหรือระบบสารสนเทศอาจส่งผลกระทบน้อย/อย่างจำกัด (limited) และเกิดผลประโยชน์แห่งชาติสำคัญน้อย (Less Important or Secondary National Interests)	การหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลข่าวสารหรือระบบสารสนเทศอาจส่งผลกระทบอย่างร้ายแรง (serious) และเกิดผลประโยชน์แห่งชาติที่สำคัญ (Important National Interests)	การหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลข่าวสารหรือระบบสารสนเทศอาจส่งผลกระทบอย่างร้ายแรงมาก (severe or catastrophic) และเกิดผลประโยชน์แห่งชาติสำคัญยิ่ง (Extremely Important National Interests)

หมายเหตุ * ผลกระทบ (Impact) แบ่งออกเป็น ด้านการเงินและสินทรัพย์ (Financial & Assets) ด้านภาพลักษณ์/ชื่อเสียง (Reputation) ด้านผู้ใช้บริการหรือประชาชน (Operations) ด้านการดำเนินการตามกฎหมาย (Legal and Regulation) ด้านความมั่นคงของรัฐ (ผลรวมเฉลี่ย CIA) (National Interests)

ในการประเมินผลกระทบโดยรวมในแต่ละระดับชั้นข้อมูลให้พิจารณาตามเกณฑ์การแบ่งระดับชั้นข้อมูล (Classification Criteria) ของข้อมูลตามวัตถุประสงค์ด้านความปลอดภัยของข้อมูล (CIA) [4] ซึ่งสามารถทำได้เป็นแผนผังการตัดสินใจจัดระดับชั้นข้อมูลเทียบกับผลกระทบจากการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต ดังตัวอย่างในภาพที่ 8 [12]

[4] ความมั่นคงปลอดภัยของสารสนเทศมีองค์ประกอบด้วยกัน 3 ประการ ได้แก่ ด้านความลับ (Confidentiality) ด้านความถูกต้อง ครบถ้วนสมบูรณ์ ความคงสภาพ (Integrity) ด้านความพร้อมใช้งาน (Availability)

ตัวอย่าง: แผนผังการตัดสินใจจัดระดับชั้นความลับของข้อมูลเทียบกับผลกระทบหากมีการเปิดเผยข้อมูล



ภาพที่ 8 แผนผังการตัดสินใจจัดระดับชั้นข้อมูลเทียบกับผลกระทบจากการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

1 **3) เกณฑ์พิจารณาระดับผลประโยชน์แห่งชาติ (National Interest)**

ผลประโยชน์แห่งชาติที่สำคัญยิ่งยวด (Vital National Interests)	ผลประโยชน์แห่งชาติสำคัญยิ่ง (Extremely Important National Interests)	ผลประโยชน์แห่งชาติที่สำคัญ (Important National Interests)	ผลประโยชน์แห่งชาติสำคัญน้อย (Less Important or Secondary National Interests)
คำอธิบาย (Description)			
เป็นเงื่อนไขที่จำเป็นอย่างยิ่งยวดต่อการปกป้องรักษาและการเพิ่มพูนความอยู่รอดปลอดภัยและการอยู่ดีกินดีภายใน ประเทศที่มีเสรีภาพและปลอดภัย ผลประโยชน์แห่งชาติของประเทศไทยที่มีความสำคัญยิ่งยวดที่นำเสนอในด้านทรัพยากร ที่ใช้ในการป้องกัน ผลประโยชน์แห่งชาติที่สำคัญยิ่งยวดนั้น จะต้องเพิ่มพูนและป้องกันโดยการสนับสนุนให้ประเทศไทยมีความเป็นผู้นำเพิ่มขึ้นในระดับภูมิภาค การเป็นผู้นำทางด้านการทหารในภูมิภาค ในด้านอำนาจกำลังรบที่เหนือกว่าขีดความสามารถทางด้านการข่าวกรองที่เพียงพอ รวมถึงการสร้างชื่อเสียงและเกียรติภูมิของประเทศไทยในสังคมโลก นอกจากนั้นยังต้องมีการสร้างความเข้มแข็งในองค์การระหว่างประเทศที่ประเทศไทยเข้าไปมีส่วนร่วมด้วย โดยเฉพาะอย่างยิ่งความร่วมมือกับประเทศพันธมิตรที่เป็นมหาอำนาจที่มีพลังอำนาจในระดับโลกทั้งหลาย	สภาพเงื่อนไขซึ่งถ้าประนีประนอมแล้วอาจทำให้เกิดความเสียหายอย่างร้ายแรงแต่ไม่ทำให้ตกอยู่ในอันตรายอย่างร้ายแรงต่อรัฐบาลไทยในการที่จะปกป้องและส่งเสริมความเป็นกินอยู่ที่ดีในการเป็นประเทศที่มีความเสรีภาพและมีความปลอดภัย	สภาพที่ว่าถ้าประนีประนอมแล้วจะเกิดผลทางลบอย่างมากตามมาในภายหลังต่อความสามารถ ของรัฐบาลไทยในการที่จะปกป้องและเสริมสร้างความเป็นอยู่ที่ดีของคนไทยในฐานะที่เป็นประเทศอิสระและมีความปลอดภัย	เป็นสภาพเงื่อนไขที่ต้องการเพียงแต่ว่ามีผลกระทบโดยตรงเพียงเล็กน้อยต่อความสามารถของรัฐบาลไทยในอันที่จะปกป้องและเพิ่มพูนความเป็นอยู่ที่ดีของคนไทยในประเทศที่มีเสรีภาพและมีความปลอดภัย ผลประโยชน์แห่งชาติสำคัญน้อยหรือสำคัญระดับรองของประเทศไทยที่นำเสนอ ซึ่งทรัพยากรที่มีอยู่ ผลประโยชน์แห่งชาติที่สำคัญจะเป็นไปเพื่อที่จะดำรงความแข็งแกร่งของประเทศไทยและประเทศที่เป็นพันธมิตรต่างๆ ในภูมิภาค รวมถึงกลไกด้านความร่วมมือต่างๆ ด้วย
เกณฑ์การพิจารณาระดับผลประโยชน์แห่งชาติ			
- ป้องกันป้องปราม และลดภัยคุกคามของอาวุธนิวเคลียร์ ชีวะและเคมีหรืออาวุธอื่น ๆ ต่อประเทศไทยหรือต่อกองกำลังทหารใด ๆ ของประเทศไทย ทั้งที่ตั้งอยู่ในประเทศ และนอกประเทศ - การทำให้เชื่อมั่นถึงความอยู่รอดของพันธมิตรตามสนธิสัญญาต่าง ๆ หรือตามข้อตกลงต่าง ๆ ในระดับนานาชาติที่ประเทศไทยได้กระทำไว้อันเป็นการรักษาไว้ซึ่งประโยชน์ของไทย	- ป้องกันกีดขวาง และลดภัยคุกคามในอันที่จะใช้อาวุธนิวเคลียร์ ชีวะและเคมี ในทุกๆ พื้นที่ของประเทศ - ป้องกันพื้นที่ของประเทศจากการถูกโจมตีจากอาวุธทำลายล้างสูง - ส่งเสริมการยอมรับการบังคับใช้กฎหมายของนานาชาติรวมทั้งกลไกที่ใช้ในการแก้ไขความขัดแย้งอย่างสันติร่วมกับนานาชาติ	- การขัดขวางต่อการละเมิดสิทธิมนุษยชนที่ร้ายแรงและที่มีจำนวนมากของประเทศเพื่อนบ้าน อันอาจจะ กระทบต่อความสงบเรียบร้อยของประเทศไทย - ส่งเสริมพหุนิยม เสรีภาพ และประชาธิปไตยในประเทศที่มีความสำคัญทางยุทธศาสตร์ต่อประเทศไทยให้มากที่สุด	- การทำให้เกิดความสมดุลด้านการค้าในลักษณะทวิภาคี - ขยายขอบเขตของการปกครองในระบอบประชาธิปไตยไปทุกแห่งหนเท่าที่เป็นประโยชน์ต่อประเทศชาติ - สนับสนุนความเป็นเอกภาพแห่งดินแดน - ขยายการส่งออกของสินค้าเฉพาะบางประเภท

ผลประโยชน์แห่งชาติที่สำคัญยิ่งยวด (Vital National Interests)	ผลประโยชน์แห่งชาติสำคัญยิ่ง (Extremely Important National Interests)	ผลประโยชน์แห่งชาติที่สำคัญ (Important National Interests)	ผลประโยชน์แห่งชาติสำคัญน้อย (Less Important or Secondary National Interests)
- ทำให้มั่นใจในความอยู่รอดและเสถียรภาพของระบบต่างๆ ทั้งในประเทศและอยู่นอกประเทศ (เช่น ระบบการค้า ระบบตลาดเงิน ระบบการขนส่งพลังงาน หรือระบบการรักษาสิ่งแวดล้อมของประเทศ เป็นต้น) - การสถาปนาความสัมพันธ์อย่างเป็นผลและเข้ากันได้กับผลประโยชน์ของประเทศไทยกับประเทศซึ่งอาจจะเป็นคู่แข่งทางยุทธศาสตร์ใด ๆ - การสถาปนาความสัมพันธ์อย่างเป็นผลและเข้ากันได้กับผลประโยชน์ของประเทศไทยกับประเทศซึ่งอาจจะเป็นคู่แข่งทางยุทธศาสตร์ใด ๆ	- ป้องกันการเกิดขึ้นของระบบการครอบงำที่จะเกิดขึ้นในประเทศ - การส่งเสริมประชาธิปไตย ความมั่งคั่งและความมีเสถียรภาพของประเทศ - ป้องกันจัดการ ความขัดแย้งที่เกิดขึ้นในภูมิภาคอันจะกระทบต่อความสงบเรียบร้อยของประเทศ - การดำรงรักษาความเป็นผู้นำ ทางด้านเกี่ยวกับการทหาร เทคโนโลยี โดยเฉพาะอย่างยิ่งระบบงานด้านการข่าวกรอง ข่าวกรองยุทธศาสตร์ - ป้องกันการอพยพของผู้อพยพเข้ามายังชายแดนของประเทศที่มีขนาดใหญ่ที่ไม่สามารถควบคุมได้ - การปราบปรามการก่อการร้าย (โดยเฉพาะการก่อการร้ายที่ได้รับการสนับสนุนจากรัฐใดๆ) อาชญากรรมข้ามชาติ และการค้ายาเสพติดข้ามชาติ - ป้องกันการฆ่าล้างเผ่าพันธุ์	เท่าที่จะกระทำได้ โดยปราศจากการทำให้เกิดการเสียเสถียรภาพ - ป้องกันหรือลดความรุนแรงของความขัดแย้งในประเทศที่มีความสำคัญทางยุทธศาสตร์ต่อประเทศไทย - ปกป้องชีวิตและความเป็นอยู่ของคนสัญชาติไทย ผู้ซึ่งเป็นเป้าหมายของการถูกลักพาตัวของขบวนการก่อการร้าย - ป้องกันทรัพย์สินของชาติซึ่งอยู่ในต่างแดน - ร่วมกับนานาชาติในการส่งเสริมนโยบายด้านสิ่งแวดล้อมในระยะยาว	

ที่มา ผลงานวิจัย “ตัวแบบในการกำหนดยุทธศาสตร์และยุทธศาสตร์ชาติในศตวรรษที่ 21” โดย พันเอก โสภณ ศิริงาม หลักสูตร วปอ. รุ่นที่ 59 ผู้อำนวยการกองยุทธศาสตร์ และความมั่นคงวิทยาลัยป้องกันราชอาณาจักร สถาบันวิชาการป้องกันประเทศ [13]

4) เกณฑ์การประเมินความเสี่ยงและผลกระทบของการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

การวิเคราะห์ความเสี่ยงเป็นข้อมูลในการตัดสินใจเพื่อจัดการกับความเสี่ยง โดยพิจารณาเงื่อนไขในการกำหนดเกณฑ์การประเมินความเสี่ยงใน 2 มิติ คือ โอกาสที่จะเกิด (Likelihood) และผลกระทบ (Impact) เพื่อกำหนดระดับความเสี่ยง (Level of Risk) การวิเคราะห์ความเสี่ยงสามารถเป็นได้ทั้งการวิเคราะห์เชิงคุณภาพ (Qualitative) กึ่งปริมาณ (Semi-Quantitative) เชิงปริมาณ (Quantitative) หรือผสมผสานกันไป กระบวนการประเมินความเสี่ยงของหน่วยงานจะทำการวิเคราะห์โอกาสที่จะเกิดเหตุการณ์ความเสี่ยงและผลกระทบอันเนื่องมาจากความเสี่ยง ซึ่งในที่นี้

ผลกระทบ (Impact) หมายถึง ความเสียหายที่จะเกิดขึ้นหากความเสี่ยงนั้นเกิดขึ้น เป็นการพิจารณาระดับความรุนแรงและมูลค่าความเสียหายจากความเสี่ยงที่คาดว่าจะได้รับ โดยมีระดับคะแนนและตัวอย่างเกณฑ์การพิจารณาระดับผลกระทบและผลประโยชน์แห่งชาติ ดังนี้

ระดับคะแนน	ความหมาย
3	ความรุนแรงของผลกระทบระดับสูง
2	ความรุนแรงของผลกระทบระดับปานกลาง
1	ความรุนแรงของผลกระทบระดับน้อย

ตัวอย่างเกณฑ์การพิจารณาระดับผลกระทบ

เกณฑ์	ค่าคะแนนระดับความรุนแรงของระดับผลกระทบ*		
	1 = น้อย	**2 = ปานกลาง**	**3 = สูง**
***ด้านการเงินและสินทรัพย์ (Financial & Assets)**	*มูลค่าความเสียหายในระดับต่ำ*	*มูลค่าความเสียหายในระดับปานกลาง*	*มูลค่าความเสียหายในระดับสูง*
ด้านภาพลักษณ์/ชื่อเสียง (Reputation)	*น้อย/อย่างจำกัด*	*อย่างร้ายแรง*	*อย่างร้ายแรงมาก*
ด้านผู้ใช้บริการหรือประชาชน (Operations)	*รายบริการ/การดำเนินงานขององค์กร*	*ราย กลุ่มบริการ/การดำเนินของกระทรวง/ระหว่าง องค์กร/จังหวัด*	*ข้ามกลุ่มบริการ/ภูมิภาคการดำเนินงานตามแผนบูรณาการ/กลุ่มจังหวัด*
ด้านการดำเนินการตามกฎหมาย (Legal and Regulation)	*ละเว้นการปฏิบัติตามระเบียบข้อบังคับขององค์กรซึ่งเกิดผลกระทบน้อย*	*ละเว้นการปฏิบัติตามระเบียบข้อบังคับและกฎกระทรวงซึ่งเกิดผลกระทบที่มีนัยสำคัญและไม่เป็นไปตามเป้าของ ก.พ.ร.*	*ละเว้นการปฏิบัติตามกฎหมาย มติ ครม. หรือระเบียบข้อบังคับซึ่งเกิดผลกระทบที่มีนัยสำคัญและไม่เป็นไปตามเป้าของแผนบูรณาการ/กลุ่มจังหวัด*
ด้านความมั่นคงของรัฐ (ผลรวมเฉลี่ย CIA) **(National Interests)**	*ผลประโยชน์แห่งชาติสำคัญน้อย*	*ผลประโยชน์แห่งชาติที่สำคัญ*	***ผลประโยชน์แห่งชาติที่สำคัญยิ่ง*

หมายเหตุ หน่วยงานของรัฐสามารถกำหนดเกณฑ์การพิจารณาระดับผลกระทบและผลประโยชน์แห่งชาติให้สอดคล้องกับนโยบายและกฎระเบียบที่เกี่ยวข้อง และเหมาะสมกับบริบทขององค์กร

***** ด้านการเงินและสินทรัพย์ พิจารณาความเสียหายจากการนำไปใช้งาน เช่น๕* การให้บริการแล้วข้อมูลรั่วออกไปหรือข้อมูลถูกโจรกรรม แล้วอาจเกิดความเสียหายที่ทำให้หน่วยงานต้องจ่ายค่าปรับ

- ตัวอย่างการพิจารณาค่าปรับ : ประเทศไทย แหล่งที่มา PDPA Thailand คลิกที่นี่ (PDPA Thailand, 2025) โทษปรับทางปกครองสูงสุดไม่เกิน 5 ล้านบาท และมีโทษทางอาญาที่ไม่สามารถยอมความได้

- ตัวอย่างการพิจารณาค่าปรับ : ต่างประเทศ แหล่งที่มา GDPR คลิกที่นี่ (GDPR, 2018) โทษปรับสูงสุด สำหรับความผิดร้ายแรง (Serious Infringements) เช่น การละเมิดหลักการพื้นฐาน การละเมิดสิทธิเจ้าของข้อมูล ค่าปรับ สูงสุด 20 ล้านยูโร หรือ 4% ของรายได้ทั่วโลกต่อปี

** ตัวอย่างเกณฑ์การพิจารณาระดับผลกระทบที่สอดคล้องกับมาตรา 14 และ 15 พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540

ตารางที่ 1: ตารางตัวอย่างเกณฑ์การพิจารณาผลกระทบจากการประยุกต์ใช้แบบประเมิน

ด้าน	ตัวอย่างเกณฑ์การพิจารณาผลกระทบ		
	1 = ต่ำ	2 = ปานกลาง	3 = สูง
การเงินและสินทรัพย์	**มูลค่าความเสียหายในระดับต่ำ** โดย ✓ มีมูลค่าความเสียหายหลักแสนบาท ✓ ข้อมูลผิดพลาดเล็กน้อย ไม่กระทบการตัดสินใจหลัก กรณีตัวอย่าง การพิมพ์นามสกุลผิดในระบบสารบรรณเบิกจ่ายล่าช้าภายในกรม	**มูลค่าความเสียหายในระดับปานกลาง** โดย ✓ มีมูลค่าความเสียหายหลักล้านบาท ✓ ข้อมูลผิดพลาดทำให้การให้บริการหยุดชะงักหรือข้อมูลรั่วไหลจนต้องเยียวยาเจ้าของข้อมูล ✓ ต้องชดเชยค่าปรับและค่าสินไหมทดแทน กรณีตัวอย่าง ระบบสวัสดิการโอนเงินผิดบัญชีจำนวนต้องมีการทวงคืน ข้อมูลถูกโจรกรรมแล้วนำไปทำ Spam Call จนเกิดการร้องเรียน	**มูลค่าความเสียหายในระดับสูง** โดย ✓ มีมูลค่าความเสียหายหลักสิบล้านบาทขึ้นไป ✓ ข้อมูลสำคัญสูญหาย/ถูกเข้าหัส หรือ ข้อมูลรั่วไหลสู่สาธารณะจนเกิดการฟ้องร้อง ต้องชดเชยความเสียหายวงกว้าง ✓ ความเสียหายต่อระบบการเงินการคลังของรัฐ และค่ากู้คืนระบบ กรณีตัวอย่าง ข้อมูลสุขภาพรั่วไหลและถูกนำไปบังคับข่มขู่ (Blackmail) หรือฐานข้อมูลจัดซื้อจัดจ้างถูกแก้ไขตัวเลข ทำให้รัฐอนุมัติงบเกินจริงไปมหาศาล
ภาพลักษณ์/ชื่อเสียง	**น้อย/อย่างจำกัด** โดย ✓ ส่งผลกระทบเฉพาะภาพลักษณ์หน่วยงาน ใช่หรือไม่ ✓ ส่งผลต่อการรับรู้บทบาทหน้าที่ของหน่วยงาน ใช่หรือไม่ ✓ ส่งผลต่อภาพลักษณ์ของระบบการให้บริการ ใช่หรือไม่	**อย่างร้ายแรง** โดย ✓ ส่งผลต่อภาพลักษณ์ของระบบการให้บริการ ใช่หรือไม่ ✓ ส่งผลความเชื่อมั่นของผู้ใช้บริการ ใช่หรือไม่ ✓ สามารถฟ้องร้องทางคดีแพ่ง ใช่หรือไม่	**อย่างร้ายแรงมาก** โดย ✓ ส่งผลกระทบต่อภาพลักษณ์ชื่อเสียงของรัฐในระดับประเทศ ใช่หรือไม่ ✓ สามารถฟ้องร้องทางคดีแพ่ง และคดีอาญา ใช่หรือไม่
ผู้ใช้บริการหรือประชาชน	**รายบริการ/การดำเนินงานขององค์กร** โดย ✓ ส่งผลกระทบต่อการทำงานภายในหน่วยงาน ใช่หรือไม่ ✓ ส่งผลกระทบต่อประสิทธิภาพการทำงานของผู้ปฏิบัติงานของหน่วยงานลดลง ใช่หรือไม่ ✓ ส่งผลการใช้งานของจำนวนผู้ใช้งานในวงแคบ ใช่หรือไม่	**รายDomain/การดำเนินของกระทรวง/ระหว่างองค์กร/จังหวัด** โดย ✓ ส่งผลให้เกิดอุปสรรคต่อการทำงานหน่วยงาน และคู่สัญญา ✓ ส่งผลต่อประสิทธิภาพการให้บริการของระบบ ✓ บางบริการมีความไม่สะดวก /ล่าช้า แต่ไม่สูญเสียข้อมูลใช่หรือไม่ ✓ ส่งผลกระทบต่อผู้ใช้บริการบางส่วน ใช่หรือไม่	**การดำเนินงานตามแผนบูรณาการ/กลุ่มจังหวัด** โดย ✓ ส่งผลกระทบต่อ 2 หน่วยงานขึ้นไป ใช่หรือไม่ ✓ ส่งผลต่อผู้มาใช้บริการทุกคน และกระทบวงกว้างในระดับประเทศ ใช่หรือไม่ ✓ ระบบล่ม/ใช้งานไม่ได้ เกิดความเสียหายต่อผู้ใช้บริการ ใช่หรือไม่ ✓ ข้อมูลในระบบสูญหาย ใช่หรือไม่
การดำเนินงานตามกฎหมาย	**ละเว้นการปฏิบัติตามระเบียบข้อบังคับขององค์กร ซึ่งเกิดผลกระทบน้อย** โดย ✓ ไม่ปฏิบัติตามกฎระเบียบระดับองค์กร ใช่หรือไม่ ✓ ส่งผลให้หน่วยงานได้รับบทลงโทษของหน่วยงาน ใช่หรือไม่ ✓ ส่งผลให้หน่วยงานได้รับบทลงโทษตามกฎหมายปกครอง ใช่หรือไม่	**ละเว้นการปฏิบัติตามระเบียบข้อบังคับและกฎกระทรวง ซึ่งเกิดผลกระทบที่มีนัยสำคัญ และไม่เป็นไปตามเป้าของ ก.พ.ร.** โดย ✓ ไม่ปฏิบัติตามกฎระเบียบระดับกระทรวง เช่น กฎกระทรวง ใช่หรือไม่ ✓ ส่งผลให้หน่วยงานได้รับบทลงโทษตามกฎหมายปกครองและกฎหมายแพ่ง ใช่หรือไม่	**ละเว้นการปฏิบัติตามกฎหมายมติ ครม.หรือระเบียบข้อบังคับซึ่งเกิดผลกระทบที่มีนัยสำคัญ และไม่เป็นไปตามเป้าของแผนบูรณาการ/กลุ่มจังหวัด** โดย ✓ ไม่ปฏิบัติตามกฎหมาย/มติ ครม. รัฐบาล อย่างชัดเจน และไม่เป็นไปตามเป้าหมายของแผนบูรณาการ ใช่หรือไม่ ✓ ส่งผลให้ได้รับบทลงโทษกฎหมายปกครอง กฎหมายแพ่ง และกฎหมายอาญา ใช่หรือไม่
ความมั่นคงของรัฐ	**ผลประโยชน์แห่งชาติสำคัญน้อย** โดย ✓ มีผลกระทบตามหลักการ CIA ในระดับต่ำ ใช่หรือไม่ ✓ การเปิดเผยข้อมูลจะส่งผลให้เกิดอันตรายต่อทรัพย์สิน/ชีวิต/ความปลอดภัยของบุคคลใดบุคคลหนึ่ง ใช่หรือไม่	**ผลประโยชน์แห่งชาติที่สำคัญ** โดย ✓ มีผลกระทบตามหลักการ CIA ในระดับปานกลาง ใช่หรือไม่ ✓ การเปิดเผยข้อมูลจะส่งผลให้เกิดอันตรายต่อทรัพย์สิน/ชีวิต/ความปลอดภัยของประชาชนบางส่วน ใช่หรือไม่ ✓ สร้างความเสียหายต่อความสัมพันธ์ระหว่างหน่วยงานอื่นๆ ใช่หรือไม่	**ผลประโยชน์แห่งชาติที่สำคัญยิ่ง** โดย ✓ มีผลกระทบตามหลักการ CIA ในระดับสูง ใช่หรือไม่ ✓ ส่งผลให้เกิดอันตรายต่อทรัพย์สิน/ชีวิต/ความปลอดภัยของประชาชนส่วนใหญ่ ใช่หรือไม่ ✓ เกิดความเสียหายต่อความมั่นคงของประเทศ หรือความสัมพันธ์ระหว่างประเทศ หรือความมั่นคงทางเศรษฐกิจของประเทศใช่หรือไม่

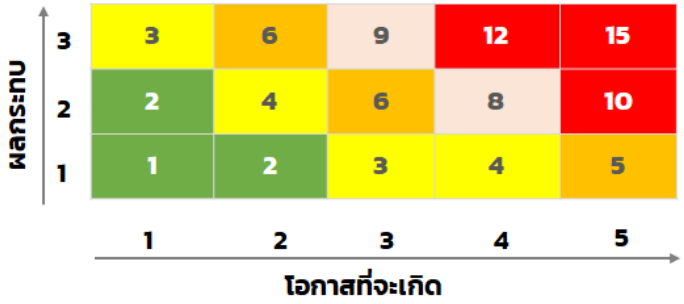
หมายเหตุ หน่วยงานสามารถกำหนดเกณฑ์การพิจารณาระดับผลกระทบให้สอดคล้องกับนโยบายและกฎระเบียบที่เกี่ยวข้อง และเหมาะสมกับบริบทขององค์กร

โอกาสที่จะเกิด (Likelihood) หมายถึง การประเมินโอกาสของความเสี่ยงจากการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตหรือการรั่วไหลของข้อมูลที่มีระดับชั้นความลับที่จะเกิดขึ้น โดยการพิจารณาจากสถิติการเกิดเหตุการณ์ในอดีต ปัจจุบัน หรือการคาดการณ์ล่วงหน้าของโอกาสที่จะเกิดในอนาคต ทั้งนี้ ให้ผู้ดูแลข้อมูลและเจ้าของข้อมูลร่วมกันประเมินโอกาสที่จะเกิดขึ้นตามบริบทของแต่ละหน่วยงาน โดยมีระดับคะแนนดังนี้

ระดับคะแนน	ความหมาย	ตัวอย่างโอกาสที่จะเกิด
5	มีโอกาสเกิดขึ้นสูงมาก/เป็นประจำ	• มีความแน่นอนที่จะเกิดเหตุการณ์นี้ขึ้น • โอกาสเกิดเป็นประจำ หรืออย่างน้อยเดือนละ 1 ครั้ง
4	มีโอกาสเกิดขึ้นสูง/บ่อยครั้ง	• มีข้อบ่งชี้หรือหลักฐานที่คาดว่าจะเกิดเหตุการณ์นี้ขึ้น ในระยะอันใกล้ • โอกาสเกิดค่อนข้างบ่อย หรือปีละ 6-10 ครั้ง

ระดับคะแนน	ความหมาย	ตัวอย่างโอกาสที่จะเกิด
3	มีโอกาสเกิดขึ้นบ้าง/บางครั้ง	• มีข้อบ่งชี้หรือหลักฐานที่แสดงถึงความเป็นไปได้ที่จะเกิดเหตุการณ์นี้ขึ้น • โอกาสเกิดปานกลาง หรือปีละ 3-5 ครั้ง
2	มีโอกาสเกิดขึ้นน้อยครั้ง	• ไม่มีข้อบ่งชี้หรือหลักฐาน แต่มีความเป็นไปได้ยากที่จะเกิดเหตุการณ์นี้ขึ้น • โอกาสเกิดน้อย หรืออย่างมาก ไม่เกินปีละ 2 ครั้ง
1	มีโอกาสเกิดขึ้นยาก	• เป็นไปไม่ได้ที่จะเกิดเหตุการณ์นี้ขึ้น • แทบจะไม่เกิด หรืออย่างมาก ปีละ 1 ครั้ง

ระดับความเสี่ยง (Risk Level) กำหนดค่าเท่ากับผลคูณของระดับโอกาสที่ความเสี่ยงอาจเกิดขึ้น (Likelihood) และระดับความรุนแรงของผลกระทบ (Impact) อันเนื่องมาจากความเสี่ยง ซึ่งระดับความเสี่ยงแบ่งตามความสำคัญและการจัดการความเสี่ยงได้ดังนี้



ค่าระดับความเสี่ยง	ระดับความเสี่ยง	ความหมาย
1 - 2	ต่ำมาก	*ระดับความเสี่ยงที่องค์กรสามารถยอมรับได้ โดยไม่ต้องมีมาตรการควบคุมก็ได้*
3 - 4	ต่ำ	*ระดับความเสี่ยงที่องค์กรสามารถยอมรับได้ โดยมีมาตรการควบคุมอยู่แล้วหรือไม่ก็ได้ แต่อาจต้องมีการติดตามเป็นระยะๆ*
5 - 6	ปานกลาง	*ระดับความเสี่ยงที่องค์กรสามารถยอมรับได้โดยต้องมีมาตรการควบคุมหรือมีแผนการลดความเสี่ยง เพื่อลดความเสี่ยงให้ไปอยู่ในระดับต่ำและป้องกันไม่ให้ความเสี่ยงเพิ่มขึ้น*
7 - 9	สูง	*ระดับความเสี่ยงที่องค์กรไม่สามารถยอมรับได้ และต้องจัดการลดความเสี่ยงให้ไปอยู่ในระดับต่ำลงโดยเร็ว โดยต้องจัดให้มีแผนการลดความเสี่ยงและป้องกันไม่ให้ความเสี่ยงกลับเพิ่มสูงขึ้นด้วย*
10 - 15	สูงมาก	*ระดับความเสี่ยงที่องค์กรไม่สามารถยอมรับได้ และต้องจัดการลดความเสี่ยงให้ไปอยู่ในระดับต่ำลงในทันที หรืออาจมีการถ่ายโอนความเสี่ยง โดยต้องจัดให้มีแผนการลดความเสี่ยงและป้องกันไม่ให้ความเสี่ยงกลับเพิ่มสูงขึ้นด้วย*

สำหรับการประยุกต์ใช้หลักเกณฑ์การจัดระดับชั้นข้อมูลภาครัฐ **สามารถศึกษาตัวอย่างและใช้เครื่องมือการพิจารณาหมวดหมู่และจัดระดับชั้นข้อมูล** [โดยคลิกที่นี่]() ซึ่งหน่วยงานสามารถปรับให้สอดคล้องกับบริบทของหน่วยงานได้

3.2.3. ข้อเสนอแนะการจัดการข้อมูลภาครัฐ (Data Handling) ที่มีการจัดระดับชั้นข้อมูล

ข้อมูลทั้งหมดไม่ได้ถูกสร้างขึ้นอย่างเท่าเทียมกันนับตั้งแต่เวลาที่ข้อมูลถูกสร้างขึ้นจนกระทั่งถูกทำลาย การจัดระดับชั้นข้อมูลสามารถช่วยให้องค์กรมั่นใจได้ว่า ข้อมูลจะได้รับการป้องกัน จัดเก็บ และบริหารจัดการอย่างมีประสิทธิภาพ การจัดระดับชั้นข้อมูลเป็นหัวใจสำคัญของกลยุทธ์การปกป้องคุ้มครองข้อมูลขององค์กรซึ่งช่วยลดความเสี่ยงต่อข้อมูลที่มีความอ่อนไหว สนับสนุนการตัดสินใจและเพิ่มประสิทธิภาพของการป้องกันข้อมูลสูญหาย การเข้ารหัส และการควบคุมความปลอดภัยอื่นๆ ด้วยการกำหนดรูปแบบการจัดระดับชั้นข้อมูลที่ชัดเจนตรงไปตรงมา การประเมินและกำหนดตำแหน่ง/แหล่งที่มาของข้อมูลอย่างครอบคลุมและประยุกต์ใช้โซลูชันที่เหมาะสม องค์กรสามารถมั่นใจได้ว่าข้อมูลที่มีความอ่อนไหวจะได้รับการจัดการ (Handling) อย่างเหมาะสมและลดภัยคุกคามต่อการดำเนินงานขององค์กร

ทั้งนี้ หน่วยงานของรัฐสามารถกำหนดรูปแบบการจัดการข้อมูล (Data Handling) ในแต่ละระดับชั้นข้อมูลได้ตามความเหมาะสมและสอดคล้องกับนโยบายการบริหารจัดการข้อมูลและจัดระดับชั้นข้อมูลของหน่วยงาน

ข้อเสนอแนะการจัดการข้อมูลภาครัฐ (Data Handling) ที่มีการจัดระดับชั้น มีดังนี้

ระดับชั้นข้อมูล / การบริหารจัดการ	เปิดเผย (Open)	เผยแพร่ภายในองค์กร (Private)[5]	ลับ (Confidential / Sensitive)	ลับมาก (Secret / Medium sensitive)	ลับที่สุด (Top secret / Highly sensitive)
ตัวอย่างชุดข้อมูล	- กฎ มติ ครม. ข้อบังคับ - รายงานผลการศึกษาทางวิชาการ - ข้อมูลเปิดภาครัฐ - ข้อมูลรายชื่อผู้บริหารของหน่วยงาน - ประกาศ/ข้อบังคับหน่วยงาน	- ข้อมูลระเบียน - ข้อมูลพนักงาน - เอกสารประกอบการปฏิบัติงาน - วิธีปฏิบัติภายในหน่วยงาน - ปฏิทินกิจกรรมภายในองค์กร - ข้อมูลติดต่อผู้บริหารและพนักงานของหน่วยงาน	- ข้อมูลการฟ้องคดี - ความเห็นภายในหน่วยงานที่ยังไม่ได้ข้อยุติ - เอกสารประกอบการประชุมคณะรัฐมนตรีที่ยังไม่ผ่านการประชุมหรือยังไม่มีมติ - ข้อมูลเงินเดือนผู้บริหารและพนักงานของหน่วยงาน	- รายงานการแพทย์ - ข้อมูลความสัมพันธ์ระหว่างประเทศ - นโยบายสำคัญที่ใช้ปฏิบัติต่อรัฐต่างประเทศ - ข้อมูลด้านสุขภาพของผู้บริหารของหน่วยงาน	- ข่าวสารที่อาจก่อความเสียหายต่อสถาบันพระมหากษัตริย์ - ข้อมูลที่กระทบต่อความมั่นคงทางทหาร เช่น คลังอาวุธ - ชุดข้อมูลตามนโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ (พ.ศ. 2566 – 2570)

[5] ในกรณีของการจัดเก็บข้อมูลส่วนบุคคลควรจัดเก็บตามหลักการประมวลผลข้อมูลส่วนบุคคลอย่างน้อยที่สุด (Data Minimization) คือ การประมวลผลข้อมูลจะต้องดำเนินการกับข้อมูลเท่าที่เพียงพอ เกี่ยวข้องและจำเป็นกับวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล

ระดับชั้นข้อมูล / การบริหารจัดการ	เปิดเผย (Open)	เผยแพร่ภายในองค์กร (Private)[5]	ลับ (Confidential / Sensitive)	ลับมาก (Secret / Medium sensitive)	ลับที่สุด (Top secret / Highly sensitive)
การควบคุมการเข้าถึง (Access Control)	- ไม่มีการจำกัดการเข้าถึงข้อมูล/เปิดเผยสู่สาธารณะ	- จำกัดการเข้าถึงข้อมูลเฉพาะบุคคลภายในหน่วยงาน	- จำกัดการเข้าถึงเฉพาะบุคคลที่จำเป็นต้องรู้หรือมีสิทธิ์รู้โดยและลงนามข้อตกลงไม่เปิดเผยข้อมูล (non-disclosure agreements) - สามารถตรวจสอบคำขอการเข้าถึงข้อมูล การทบทวน การอนุมัติ และกระบวนการยกเลิกได้	- จำกัดการเข้าถึงเฉพาะบุคคลที่จำเป็นต้องรู้หรือมีสิทธิ์รู้โดยและลงนามข้อตกลงไม่เปิดเผยข้อมูล (non-disclosure agreements) - ต้องได้รับการอนุญาตจากเจ้าของข้อมูล - สามารถตรวจสอบคำขอการเข้าถึงข้อมูล การทบทวน การอนุมัติ และกระบวนการยกเลิกได้	- ไม่เปิดเผย/ปกปิด
การเข้ารหัส (Encryption)	- ไม่มีการเข้ารหัส	- ไม่มีการเข้ารหัสการสร้างการจัดเก็บ การประมวลผล และการส่งข้อมูล - มีการเข้ารหัสสำหรับบุคคลที่สาม	- การเข้ารหัสระหว่างการสร้างการจัดเก็บ การประมวลผล และการส่งข้อมูล - มีการเข้ารหัสสำหรับบุคคลที่สาม	- มีการเข้ารหัสที่ซับซ้อนระหว่างการสร้าง การจัดเก็บ การประมวลผล และการส่งข้อมูล - มีการเข้ารหัสที่ซับซ้อนสำหรับบุคคลที่สาม	- ไม่เปิดเผย/ปกปิด
การจัดเก็บ (Storage)	- ไม่มีข้อจำกัดการจัดเก็บข้อมูล	- การจัดเก็บข้อมูลเป็นไปตามนโยบายองค์กรหรือดุลยพินิจของผู้จัดการหรือผู้คุ้มครองข้อมูล	- ห้ามจัดเก็บข้อมูลที่ลับในเครื่องและอุปกรณ์คอมพิวเตอร์โดยไม่ได้รับอนุญาต	- ห้ามจัดเก็บข้อมูลที่ลับมากในเครื่องและอุปกรณ์คอมพิวเตอร์โดยไม่ได้รับอนุญาต เว้นแต่จะได้รับอนุมัติจากเจ้าหน้าที่รักษาความปลอดภัยข้อมูล และต้องมีการเข้ารหัส - จัดเก็บที่ปลอดภัยเมื่อไม่ใช้งาน	- ไม่เปิดเผย/ปกปิด

1

4. การบูรณาการจัดระดับชั้นข้อมูลกับการใช้คลาวด์

ยุทธศาสตร์ชาติ 20 ปี (ปี พ.ศ. 2561-2580) ให้ความสำคัญกับการใช้เทคโนโลยีเพื่อพัฒนาการให้บริการภาครัฐ ให้สามารถดำเนินงานได้เทียบเท่ามาตรฐานสากล หน่วยงานรัฐจึงจำเป็นต้องพัฒนาเพื่อเพิ่มขีดความสามารถในการให้บริการตามภารกิจของหน่วยงาน โดยการพิจารณาสรรหาเทคโนโลยีใหม่ๆ เข้ามาช่วยส่งเสริมกระบวนการทำงานให้มีประสิทธิภาพและประสิทธิผลมากยิ่งขึ้น โดยเทคโนโลยีคลาวด์ ถือเป็นโครงสร้างพื้นฐานทางดิจิทัลที่มีความสำคัญอย่างยิ่งต่อการขับเคลื่อนการทำงานของภาครัฐ ทั้งในด้านการเพิ่มประสิทธิภาพการปฏิบัติภารกิจและการยกระดับการให้บริการประชาชนให้มีความสะดวก รวดเร็ว และทันสมัย

ตามประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง กรอบแนวทางการบริหารจัดการระบบคลาวด์ภาครัฐ ซึ่งเป็นกรอบแนวทางการบริหารจัดการระบบคลาวด์ภาครัฐ ตลอดจนเพื่อเพิ่มอำนาจในการต่อรองของภาครัฐสำหรับการใช้บริการคลาวด์ เพื่อสนับสนุนให้ภาครัฐสามารถพิจารณาระบบคลาวด์เป็นหลัก มุ่งสู่การเป็นรัฐบาลดิจิทัล โดยการผลักดันนโยบายการใช้คลาวด์ ตามกรอบแนวทางการบริหารจัดการคลาวด์ภาครัฐ ในเรื่องการใช้บริการของคลาวด์สาธารณะนั้น เพื่อให้หน่วยงานรัฐมีการใช้คลาวด์สาธารณะเป็นหลัก ก่อนการเลือกใช้คลาวด์ในประเภทอื่นๆ ซึ่งคลาวด์สาธารณะมีฟังก์ชันการทำงานและมีบริการจากผู้ให้บริการที่หลากหลาย ดังนั้นเพื่อให้เกิดประโยชน์สูงสุดหน่วยงานรัฐจึงควรเลือกใช้บริการคลาวด์ที่มีความเหมาะสมกับการให้บริการของหน่วยงาน ทั้งนี้สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) จัดทำข้อเสนอแนะแนวทางการดำเนินงานที่สำคัญภายใต้กรอบแนวทางการบริหารจัดการคลาวด์ภาครัฐ เพื่อเป็นข้อเสนอแนะและกรณีศึกษาให้หน่วยงานภาครัฐสามารถนำไปปรับใช้กับหน่วยงานเพื่อรองรับนโยบายการใช้คลาวด์ โดยสามารถศึกษารายละเอียดเพิ่มเติมได้ที่ https://standard.dga.or.th/category/standard/

4.1 ความสำคัญของระบบคลาวด์ต่อหน่วยงานภาครัฐในต่างประเทศ

การนำเทคโนโลยีคลาวด์มาใช้งานเพื่อเพิ่มประสิทธิภาพการทำงานและอำนวยความสะดวกในการให้บริการแก่ประชาชน สู่การเป็นรัฐบาลดิจิทัลนั้น ไม่ได้เป็นเพียงการเปลี่ยนรูปแบบการใช้จ่ายงบประมาณจากการลงทุนเป็นการดำเนินงานที่ครอบคลุมเฉพาะบริการที่ใช้งานจริงเท่านั้น แต่ยังส่งผลดีในหลากหลายมิติ ได้แก่:

1. ความยืดหยุ่นและการทดลองนวัตกรรม: การใช้คลาวด์ช่วยให้หน่วยงานภาครัฐมีความยืดหยุ่นสูงขึ้นในการทดลองใช้บริการใหม่ ๆ หรือทำการเปลี่ยนแปลงระบบด้วยต้นทุนที่ลดลง
2. ความปลอดภัยที่เพิ่มขึ้น: ผู้ให้บริการคลาวด์มักมีการปรับปรุงเทคโนโลยีและระบบรักษาความปลอดภัยอย่างสม่ำเสมอ ซึ่งช่วยเพิ่มระดับความปลอดภัยของข้อมูลภาครัฐ
3. ศักยภาพในการประมวลผลข้อมูล: คลาวด์ช่วยเพิ่มศักยภาพและลดระยะเวลาในการประมวลผลข้อมูลขนาดใหญ่ได้อย่างมีนัยสำคัญ
4. การลดต้นทุนโดยรวม: ด้วยรูปแบบการกำหนดราคาที่ปรับขนาดได้ตามความเหมาะสมของบริบทบริการ ทำให้สามารถลดต้นทุนโดยรวมได้อย่างมีประสิทธิภาพ

เป้าหมายหลักของการนำบริการคลาวด์มาใช้ในหน่วยงานภาครัฐตั้งอยู่บนพื้นฐานของการพัฒนาขีดความสามารถในการให้บริการสาธารณะแก่ภาคประชาชนให้มีประสิทธิภาพมากยิ่งขึ้น ด้วยค่าใช้จ่ายที่ลดลง นอกจากนี้ยังช่วยลดการลงทุนและการใช้งานระบบสารสนเทศที่ซ้ำซ้อน รวมถึงส่งเสริมความร่วมมือระหว่างหน่วยงานในการใช้และแลกเปลี่ยนข้อมูลอย่างมีประสิทธิภาพและปลอดภัย

ปัจจุบันรัฐบาลในหลายประเทศชั้นนำทั่วโลก เช่น สหราชอาณาจักร สหรัฐอเมริกา ออสเตรเลีย และสิงคโปร์ ต่างดำเนินนโยบายที่คล้ายคลึงกัน นั่นคือ นโยบาย Government Cloud First Policy ซึ่งสะท้อนให้เห็นถึงความสำคัญของการนำข้อมูลภาครัฐเข้าสู่ระบบการประมวลผลแบบคลาวด์ โดยทุกประเทศได้มีการจัดจำแนกประเภทข้อมูลเพื่อใช้บริการคลาวด์ตามบริบทเฉพาะของแต่ละประเทศ ซึ่งมีกรณีศึกษาที่น่าสนใจดังนี้:

กรณีศึกษานโยบายระบบคลาวด์ภาครัฐจากต่างประเทศ

1. สหราชอาณาจักร (United Kingdom)

สหราชอาณาจักรใช้ “Cloud-First Policy” ตั้งแต่ปี 2556 กำหนดให้หน่วยงานรัฐพิจารณาใช้ Public Cloud เป็นตัวเลือกแรก หากไม่ใช้ต้องมีเหตุผลด้านความคุ้มค่าที่ดีกว่า นโยบายนี้มุ่งลดต้นทุน เพิ่มประสิทธิภาพ และส่งเสริมนวัตกรรม โดยข้อมูลภาครัฐถูกจำแนกเป็น 3 ระดับ ได้แก่ Official, Secret และ Top Secret

จากโมเดล 3 ระดับของสหราชอาณาจักร พบว่าข้อมูลภาครัฐกว่า 90% เช่น ข้อมูลประชาชน สามารถจัดเก็บบน Public Cloud ได้ทั่วโลกภายใต้มาตรฐานความปลอดภัยสากลและการปฏิบัติตาม GDPR ข้อมูลที่ต้องเก็บในศูนย์ข้อมูลภาครัฐมีเพียงข้อมูลระดับ Top Secret เท่านั้น ระบบจำแนกข้อมูลนี้ช่วยให้การจัดการความปลอดภัยเป็นไปตามระดับความอ่อนไหวและความเสี่ยง โดยได้รับการสนับสนุนจากมาตรฐานและแนวทางของ National Cyber Security Centre (NCSC) เพื่อคุ้มครองข้อมูลภาครัฐทุกระดับ

ตารางที่ 2: หลักการสำคัญของนโยบายของสหราชอาณาจักร

หลักการสำคัญของนโยบาย	
1. การให้ความสำคัญกับโซลูชันคลาวด์	หน่วยงานของรัฐต้องพิจารณาใช้ระบบคลาวด์ เช่น Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), และ Infrastructure-as-a-Service (IaaS) เป็นตัวเลือกแรก
	โซลูชันที่เลือกต้องเป็นไปตามมาตรฐานด้านความปลอดภัยและการปกป้องข้อมูลที่กำหนดโดย National Cyber Security Centre (NCSC)
2. ความยืดหยุ่นและการปรับตัว	ระบบคลาวด์ช่วยให้ปรับเปลี่ยนทรัพยากรได้ตามความต้องการของงาน เพิ่มความคุ้มค่าด้านต้นทุนและลดการลงทุนในโครงสร้างพื้นฐานที่ไม่จำเป็น
3. ส่งเสริมนวัตกรรม	การใช้งานมาตรฐานแบบเปิด (Open Standards) และแพลตฟอร์มที่แชร์ร่วมกันช่วยลดการทำงานซ้ำซ้อนระหว่างหน่วยงานและส่งเสริมนวัตกรรม
4. อิสระจากผู้ให้บริการ (Vendor Independence)	นโยบายนี้ช่วยลดความเสี่ยงจากการพึ่งพาผู้ให้บริการเพียงรายเดียว และส่งเสริมการแข่งขันในตลาดเทคโนโลยี

ตารางที่ 3: การจำแนกประเภทข้อมูลและตัวอย่างการใช้งานของสหราชอาณาจักร

ประเภทข้อมูล	ลักษณะ	ตัวอย่างการใช้งานในภาครัฐ	มาตรการรักษาความปลอดภัย
Official	- เป็นข้อมูลที่ไม่อ่อนไหวหรือมีผลกระทบต่ำหากเกิดการรั่วไหล - ข้อมูลนี้มักใช้ในงานประจำวันของภาครัฐ เช่น การให้บริการประชาชนหรือข้อมูลเว็บไซต์ - ต้องการการป้องกันขั้นพื้นฐาน เช่น การเข้ารหัสข้อมูล (Encryption) และการควบคุมการเข้าถึง (Access Control)	- ข้อมูลในเว็บไซต์รัฐบาล เช่น GOV.UK - ตารางเวลารถไฟสาธารณะหรือประกาศจากหน่วยงาน	- การเข้าถึงข้อมูลผ่านเครือข่ายที่มีความปลอดภัย เช่น Virtual Private Network (VPN) - ระบบคลาวด์แบบ Public Cloud ที่ผ่านมาตรฐานการรักษาความปลอดภัย เช่น ISO 27001
Secret	- เป็นข้อมูลที่หากรั่วไหลอาจก่อให้เกิดความเสียหายร้ายแรงต่อความมั่นคงหรือความปลอดภัยของประเทศ - ใช้ในหน่วยงานหรือองค์กรที่เกี่ยวข้องกับความมั่นคง หรือการบริหารงานเชิงยุทธศาสตร์	- ข้อมูลด้านการป้องกันประเทศ เช่น แผนการเคลื่อนกำลังทหาร - แผนการจัดการภัยพิบัติ หรือข้อมูลบัญชีบุคคลสำคัญ	- ใช้ระบบคลาวด์แบบ Private Cloud หรือ Hybrid Cloud - มีการตรวจสอบสิทธิ์หลายชั้น (Multi-Factor Authentication) - เซิร์ฟเวอร์และข้อมูลอยู่ภายใต้การควบคุมทางกายภาพที่เข้มงวด เช่น ศูนย์ข้อมูลที่มีระบบป้องกันการบุกรุก
Top Secret	- เป็นข้อมูลที่อ่อนไหวที่สุด หากรั่วไหลจะส่งผลเสียหายอย่างร้ายแรงและกว้างขวางต่อประเทศ เช่น ความมั่นคงของชาติหรือชีวิตของประชาชน - ต้องการมาตรการป้องกันที่เข้มงวดที่สุด	- รายละเอียดการดำเนินการด้านความมั่นคง เช่น แผนปฏิบัติการต่อต้านการก่อการร้าย - การสื่อสารระหว่างนายกรัฐมนตรีกับหน่วยข่าวกรอง - ข้อมูลเชิงยุทธศาสตร์ของประเทศหรือข้อมูลที่ส่งผลต่อพันธมิตรระดับนานาชาติ - ข้อมูลของบุคลากรในหน่วยข่าวกรอง	- ใช้ระบบที่มีการแยกเครือข่าย (Air-Gapped Networks) เพื่อป้องกันการเชื่อมต่อกับอินเทอร์เน็ต - ศูนย์ข้อมูลที่มีการป้องกันพิเศษ เช่น ระบบล็อคชีวภาพ (Biometric Lock) - การควบคุมการเข้าถึงที่เข้มงวดที่สุดและการตรวจสอบอย่างต่อเนื่อง

ที่มา : (GOV.UK, n.d.)

2. สหรัฐอเมริกา (United States)

กลยุทธ์คลาวด์ของรัฐบาลกลางสหรัฐอเมริกา ภายใต้ชื่อ “Cloud Smart” ซึ่งพัฒนาโดย CIO Council เป็นการต่อยอดจากนโยบาย “Cloud First” มีจุดมุ่งหมายเพื่อให้หน่วยงานรัฐเข้าใจประโยชน์ของคลาวด์ พร้อมกรอบการตัดสินใจและตัวอย่างเชิงปฏิบัติ เพื่อสนับสนุนการย้ายข้อมูลและระบบขึ้นคลาวด์อย่างมีประสิทธิภาพ รวมถึงกำหนดทรัพยากรและบทบาทความรับผิดชอบที่เกี่ยวข้องอย่างชัดเจน

Cloud Smart มุ่งสนับสนุนภารกิจภาครัฐใน 3 ด้านหลัก ได้แก่ ความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) การจัดซื้อจัดจ้าง (Procurement) บริการคลาวด์อย่างคุ้มค่าและหลีกเลี่ยงการผูกขาดผู้ให้บริการ และการปรับปรุงขั้นตอนการทำงาน (Workflow) เพื่อสร้างบริการดิจิทัล นอกจากนี้ NIST ยังจำแนกรูปแบบคลาวด์ออกเป็น 4 ประเภท ได้แก่ Private, Community, Public และ Hybrid เพื่อใช้เป็นแนวทางให้หน่วยงานเลือกใช้ตามความเหมาะสม

ตารางที่ 4: หลักการสำคัญของ Cloud Smart ของสหรัฐอเมริกา

หลักการสำคัญของ Cloud Smart	
1. ความปลอดภัย (Security)	ให้ความสำคัญกับการใช้เทคโนโลยีคลาวด์ที่มีมาตรการความปลอดภัยที่แข็งแกร่ง เช่น การปฏิบัติตามมาตรฐาน FedRAMP ซึ่งเป็นกรอบการประเมินความปลอดภัยสำหรับผู้ให้บริการคลาวด์
2. การจัดซื้อ (Procurement)	กระตุ้นให้หน่วยงานของรัฐบาลเลือกใช้บริการคลาวด์ที่สอดคล้องกับเป้าหมายการดำเนินงาน พร้อมเพิ่มประสิทธิภาพต้นทุนและการทำงาน
3. การพัฒนาทักษะบุคลากร (Workforce Readiness)	ส่งเสริมให้พนักงานในหน่วยงานของรัฐบาลได้รับการฝึกอบรมและพัฒนาทักษะเพื่อจัดการและใช้ประโยชน์จากเทคโนโลยีคลาวด์ได้อย่างมีประสิทธิภาพ

ที่มา : (Cloud.cio.gov, n.d.)

ตารางที่ 5: การจำแนกประเภทข้อมูลและตัวอย่างการใช้งานของสหรัฐอเมริกา

ประเภทข้อมูล	ลักษณะ	ตัวอย่างการใช้งานในภาครัฐ	มาตรการรักษาความปลอดภัย
Low-Impact	ข้อมูลสาธารณะที่ไม่มีความอ่อนไหว หากเกิดการละเมิดจะมีผลกระทบต่ำต่อองค์กรหรือบุคคล	- เว็บไซต์ NASA สำหรับเผยแพร่ภาพจากกล้องโทรทรรศน์ Hubble เช่น ภาพจักรวาล (Hubble Space Telescope) - ข้อมูลจากกระทรวงการศึกษาเกี่ยวกับโครงการทุนการศึกษา	- ใช้ HTTPS เพื่อป้องกันการดักจับข้อมูล - ระบบรหัสผ่านสำหรับการแก้ไขเนื้อหา
Moderate-Impact	ข้อมูลที่เกี่ยวข้องกับความเป็นส่วนตัวหรือมีความอ่อนไหวปานกลาง หากละเมิดอาจกระทบต่อหน่วยงานและประชาชน	- ระบบ Medicaid US Department of Health and Human Services (HHS) สำหรับการจัดการข้อมูลผู้ป่วย	- เข้ารหัสข้อมูล (Encryption) ทั้งในขณะส่งและจัดเก็บ - ใช้ระบบ Audit Trail - ใช้ Identity and Access

ประเภทข้อมูล	ลักษณะ	ตัวอย่างการใช้งานในภาครัฐ	มาตรการรักษาความปลอดภัย
		- ระบบสนับสนุนข้อมูลผู้สมัคร Social Security	Management (IAM) เพื่อควบคุมสิทธิ์การเข้าถึง
High-Impact	ข้อมูลลับที่เกี่ยวข้องกับความมั่นคงของชาติหรือผลกระทบต่อเศรษฐกิจอย่างร้ายแรง หากเกิดการละเมิด ซึ่งต้องการมาตรการความปลอดภัยและการควบคุมการเข้าถึงอย่างเข้มงวด	- การจัดการข้อมูลข่าวกรองระดับสูงของ CIA - ระบบสนับสนุนการปฏิบัติการของกระทรวงกลาโหมสหรัฐฯ	- ใช้ Virtual Private Network (VPN) - Multi-Factor Authentication (MFA) - การตรวจสอบช่องโหว่ (Penetration Testing) - จัดเก็บในศูนย์ข้อมูลที่ได้มาตรฐาน ISO 27001

ที่มา : (Cloud.cio.gov, n.d.) (Digital.gov, n.d.) (Oversight.house.gov, n.d.) (Amazon, n.d.)

3. ออสเตรเลีย (Australia)

รัฐบาลออสเตรเลียกำหนดนโยบาย Cloud First เพื่อเพิ่มประสิทธิภาพ ลดต้นทุน และยกระดับบริการภาครัฐ โดยสนับสนุนให้หน่วยงานเลือกใช้ Public Cloud เป็นทางเลือกแรก ภายใต้เงื่อนไขด้านความปลอดภัยและความคุ้มค่า พร้อมพิจารณาทางเลือกอื่น เช่น Private, Community หรือ Hybrid Cloud ตามความเหมาะสม นโยบายนี้ยังส่งเสริมให้ทั้งภาครัฐและเอกชนใช้คลาวด์มากขึ้น

ในด้านความปลอดภัย ออสเตรเลียใช้ระบบจำแนกข้อมูล 4 ระดับ ได้แก่ Unclassified, Protected, Secret และ Top Secret เพื่อประเมินความอ่อนไหวและระดับความเสี่ยงของข้อมูล ข้อกำหนดสำคัญสำหรับหน่วยงานรัฐ ได้แก่ การระบุข้อมูลที่ถือครอง ประเมินระดับความปลอดภัยของข้อมูล และนำมาตรการควบคุมที่เหมาะสมมาปฏิบัติให้สอดคล้องกับความเสี่ยง

ตารางที่ 6: หลักการและแนวคิดหลักของนโยบายของออสเตรเลีย

	หลักการและแนวคิดหลักของนโยบาย
1. Cloud First Policy	รัฐบาลออสเตรเลียกำหนดให้หน่วยงานภาครัฐต้องพิจารณาการใช้คลาวด์เป็นลำดับแรกหากบริการนั้นเหมาะสมและสามารถคุ้มครองข้อมูลได้อย่างมีประสิทธิภาพ โดยมีเงื่อนไขว่าบริการคลาวด์จะต้องมีการรักษาความปลอดภัยที่เพียงพอและสามารถให้มูลค่าทางการเงินที่ดี
2. การยกระดับการใช้คลาวด์	รัฐบาลมีนโยบายในการใช้คลาวด์เพื่อให้หน่วยงานต่างๆ สามารถลดค่าใช้จ่ายและใช้ทรัพยากรอย่างมีประสิทธิภาพ ในขณะเดียวกันก็ต้องมั่นใจว่ามีมาตรการรักษาความปลอดภัยที่เพียงพอในการจัดการข้อมูลที่สำคัญ
3. ความปลอดภัยและการปฏิบัติตามกฎหมาย	มีการกำหนดมาตรการรักษาความปลอดภัยสำหรับข้อมูลรัฐบาล โดยการใช้ผู้ให้บริการคลาวด์ที่ได้รับการรับรองมาตรฐานและปฏิบัติตามกฎหมาย เช่น Australian Government Information Security Manual (ISM) ซึ่งเป็นมาตรฐานการรักษาความปลอดภัยที่สำคัญ

ตารางที่ 7: การจำแนกประเภทข้อมูลและตัวอย่างการใช้งานของออสเตรเลีย

ประเภทข้อมูล	ลักษณะ	ตัวอย่างการใช้งานในภาครัฐ	มาตรการรักษาความปลอดภัย
Unclassified (Unofficial , Official)	ข้อมูลทั่วไปที่ไม่ต้องการจัดประเภทความปลอดภัย แต่ยังคงต้องการการจัดการอย่างรอบคอบ	- อีเมลภายใน - แนวทางการดำเนินงานทั่วไป	- ควบคุมการเข้าถึงข้อมูลที่มีการแชร์ทั่วไป - จัดการเอกสารด้วยรหัสผ่านขั้นพื้นฐาน
Protected	ข้อมูลที่ต้องการการป้องกันเพื่อหลีกเลี่ยงความเสียหายสำคัญ	- ข้อมูลส่วนบุคคล เช่น บันทึกทางการแพทย์ - ข้อมูลทางการเงินที่จำกัดการเข้าถึง	- การเข้าถึงด้วยรหัสผ่านที่เข้ารหัส - จัดเก็บในระบบที่ได้รับการรับรอง - ตรวจสอบการเข้าถึงข้อมูลอย่างสม่ำเสมอ
Secret	ข้อมูลที่การละเมิดอาจก่อให้เกิดความเสียหายร้ายแรงต่อผลประโยชน์ของชาติ	- รายงานข่าวกรองเกี่ยวกับความมั่นคง - แผนการปฏิบัติการทางการทหาร	**- ใช้เครือข่ายแยกเฉพาะ (isolated networks)** - การเข้ารหัสข้อมูลด้วยมาตรฐานระดับสูง
Top Secret	ข้อมูลที่อ่อนไหวสูงสุดและต้องการการปกป้องอย่างเข้มงวดที่สุด	- กลยุทธ์ต่อต้านข่าวกรอง - ข้อมูลการพัฒนาเทคโนโลยีด้านการป้องกันประเทศขั้นสูง	- จัดเก็บในพื้นที่ที่มีระบบรักษาความปลอดภัยทางกายภาพสูงสุด - การตรวจสอบประวัติผู้เข้าถึง (Background check)

ที่มา : (Intelligence.gov.au, 2024) , (Protectivesecurity.gov.au, 2024)

4. **สิงคโปร์ (Singapore)**

ปลายปี 2561 สิงคโปร์ประกาศแผน 5 ปีในการย้ายระบบ IT ภาครัฐจากโครงสร้างพื้นฐานภายในไปสู่บริการคลาวด์เชิงพาณิชย์ เพื่อเร่งความเร็วและยกระดับคุณภาพบริการต่อประชาชน โดย GovTech ได้พัฒนาแพลตฟอร์ม Government Commercial Cloud (GCC) เพื่อช่วยให้หน่วยงานรัฐใช้งานคลาวด์ได้อย่างมีประสิทธิภาพ พร้อมนำระบบจำแนกข้อมูลแบบระดับชั้นมาใช้เพื่อกำหนดมาตรการป้องกันตามความอ่อนไหวของข้อมูล

นโยบายนี้ช่วยลดต้นทุน เพิ่มความคล่องตัว และทำให้หน่วยงานรัฐสามารถใช้บริการคลาวด์เชิงพาณิชย์ได้อย่างปลอดภัย ปัจจุบันกว่า 70% ของระบบภาครัฐย้ายเข้าสู่ GCC แล้ว โดยมาตรการความปลอดภัยจะถูกกำหนดตามความสำคัญของข้อมูลตามนโยบายความปลอดภัยไซเบอร์ของประเทศ บริการสำคัญที่อยู่บน GCC เช่น MyCareersFuture, GoBusiness และ WOGAA สะท้อนถึงความสำเร็จของสิงคโปร์ในการขับเคลื่อนนโยบาย Cloud First

1 **ตารางที่ 8: หลักการสำคัญของแพลตฟอร์ม GCC**

หลักการสำคัญของแพลตฟอร์ม GCC	
1. นโยบาย Cloud-First	การนำระบบคลาวด์มาใช้งานจะเป็นลำดับแรกในการปรับปรุงระบบของรัฐบาล หากเป็นไปได้ ให้ใช้บริการคลาวด์จากผู้ให้บริการเชิงพาณิชย์ เช่น AWS, Microsoft Azure, และ Google Cloud แต่ยังคงมีมาตรการรักษาความปลอดภัยที่เข้มงวดเพื่อปกป้องข้อมูลของรัฐบาล
2. ความปลอดภัยและการปฏิบัติตามมาตรฐาน	แพลตฟอร์ม GCC ทำให้มั่นใจว่าระบบที่ถูกนำไปใช้งานจะต้องมีการปฏิบัติตามข้อกำหนดด้านความปลอดภัย รวมถึงการจัดการข้อมูลที่ระดับ Confidential (ข้อมูลที่สามารถใช้งานในคลาวด์ได้)
3. การบูรณาการกับระบบคลาวด์เชิงพาณิชย์	แพลตฟอร์มนี้ช่วยให้หน่วยงานภาครัฐสามารถเข้าถึงระบบที่มีอยู่แล้วจากคลาวด์เชิงพาณิชย์ เพื่อเสริมสร้างบริการดิจิทัลที่มีประสิทธิภาพ โดยไม่ต้องพัฒนาจากพื้นฐาน
4. ความคล่องตัวและประสิทธิภาพด้านต้นทุน	แพลตฟอร์ม GCC สนับสนุนการปรับปรุงกระบวนการดิจิทัลของรัฐบาลให้มีความคล่องตัวและลดต้นทุนผ่านการใช้เทคโนโลยีคลาวด์

2 **ตารางที่ 9: การจำแนกประเภทข้อมูลและตัวอย่างการใช้งานของสิงคโปร์**

ประเภทข้อมูล	ลักษณะ	ตัวอย่างการใช้งานในภาครัฐ	มาตรการรักษาความปลอดภัย
Public Data	ข้อมูลที่สามารถเผยแพร่สู่สาธารณะโดยไม่มีความกังวลเกี่ยวกับความลับ	- เว็บไซต์บริการประชาชน - รายงานผลการดำเนินงานของหน่วยงาน	- ตรวจสอบความสมบูรณ์ของเว็บไซต์ ใช้ HTTPS ในการเชื่อมต่อ - ใช้ระบบตรวจสอบป้องกันการดัดแปลงข้อมูล - ระบบการเข้าถึงแบบปลอดภัย - การตรวจสอบข้อมูลก่อนเผยแพร่
Restricted Data	ข้อมูลที่อาจก่อให้เกิดความเสียหายเล็กน้อยหากเปิดเผยโดยไม่ได้รับอนุญาต	- บันทึกการประชุมของหน่วยงาน - ข้อมูลการปฏิบัติงานภายใน เช่น แผนงานโครงการภาครัฐ	- การควบคุมสิทธิ์การเข้าถึง (Role-Based Access) - การเข้ารหัสข้อมูล (AES-256) - การเข้ารหัสข้อมูลในระหว่างการส่งและจัดเก็บ - ใช้ Role-Based Access Control (RBAC) - การตรวจสอบการเข้าถึงระบบเป็นประจำ
Confidential Data	ข้อมูลที่ต้องการความปลอดภัยสูง เพื่อป้องกันความเสี่ยงที่สำคัญ	- ข้อมูลส่วนบุคคล (PII) การจัดเก็บข้อมูลส่วนบุคคลของประชาชน เช่น หมายเลขบัตรประชาชน หรือข้อมูลทางการแพทย์	การเข้ารหัสขั้นสูง (Advanced Encryption) - ยืนยันตัวตนแบบหลายปัจจัย (MFA) - ข้อมูลเข้ารหัสทั้งขณะส่งและขณะเก็บ

ประเภทข้อมูล	ลักษณะ	ตัวอย่างการใช้งานในภาครัฐ	มาตรการรักษาความปลอดภัย
		- ข้อมูลเกี่ยวกับสัญญาการจัดซื้อจัดจ้างภาครัฐ และเอกสารทางการเงิน	- การเก็บบันทึกและตรวจสอบการเข้าถึง
Secret/National Security Data	ข้อมูลที่หากเปิดเผยจะส่งผลกระทบต่อความมั่นคงแห่งชาติหรือสวัสดิภาพของประชาชน	- ข้อมูลด้านความมั่นคง เช่น การเฝ้าระวังภัยไซเบอร์หรือข้อมูลข่าวกรองทางการทหาร - แผนปฏิบัติการทางการทหาร เช่น การออกแบบระบบป้องกันประเทศ	**- การแยกข้อมูลออกจากระบบเชิงพาณิชย์ (Data Isolation)** - โครงสร้างพื้นฐานที่ปลอดภัยสูง ใช้ระบบเฝ้าระวังภัยคุกคามแบบเรียลไทม์ - ระบบการควบคุมทางกายภาพ เช่น ใช้การสแกนไบโอเมตริกซ์ (ลายนิ้วมือ/ใบหน้า) เพื่อเข้าถึงเซิร์ฟเวอร์

จากกรณีศึกษานโยบายระบบคลาวด์ภาครัฐของนานาประเทศ พบว่าทุกประเทศมีแนวทางร่วมกันในการจำแนกประเภทข้อมูลสำหรับการใช้คลาวด์ออกเป็น 3 กลุ่มหลัก ได้แก่ ข้อมูลที่เปิดเผยได้ (Public/Open Data), ข้อมูลที่ต้องได้รับการคุ้มครอง (Protected Data), และ ข้อมูลลับที่สุด (Top Secret Data) โดยข้อมูลทุกประเภทสามารถนำขึ้นระบบคลาวด์ได้ หากมีการกำหนดมาตรการควบคุมความปลอดภัยที่เหมาะสม

โดยทั่วไปแล้ว สำหรับข้อมูลที่ต้องได้รับการคุ้มครอง หรือข้อมูลที่มีความอ่อนไหวปานกลาง เช่น ข้อมูลส่วนบุคคลที่หากถูกละเมิดอาจส่งผลกระทบต่อหน่วยงานและประชาชน หรือข้อมูลในระดับชั้นลับ มักจะเลือกใช้ คลาวด์สาธารณะ (Public Cloud) และ คลาวด์แบบผสม (Hybrid Cloud) ควบคู่ไปกับการใช้มาตรการรักษาความปลอดภัยเฉพาะของแต่ละประเทศ เช่น การควบคุมสิทธิ์การเข้าถึงและการเข้ารหัสข้อมูลอย่างเข้มงวด

ในทางกลับกัน การเลือกใช้ คลาวด์ส่วนตัว (Private Cloud) หรือ Government Cloud มักจำกัดอยู่เฉพาะข้อมูลในระดับชั้นลับขึ้นไป ตัวอย่างเช่น สหราชอาณาจักรกำหนดให้ข้อมูลระดับชั้นลับใช้คลาวด์ส่วนตัว และสำหรับข้อมูลระดับชั้นลับที่สุด จะใช้เครือข่ายแยกเฉพาะ (Secure Isolated Networks) ซึ่งเป็นมาตรการด้านความปลอดภัยที่เข้มงวดที่สุดเพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต มีการควบคุมการเข้าถึงที่เข้มงวดและมีการตรวจสอบอย่างต่อเนื่อง ในทำนองเดียวกัน ออสเตรเลียใช้เครือข่ายแยกเฉพาะสำหรับข้อมูลระดับชั้นลับในบริการที่อาจส่งผลกระทบต่อความสัมพันธ์ระหว่างประเทศ ขณะที่สิงคโปร์ใช้ Government Cloud หรือโครงสร้างพื้นฐานภายในองค์กร (On-Premises Infrastructure) สำหรับกลุ่มข้อมูลลับที่สุด

ดังนั้น การเตรียมความพร้อมและกำหนดแนวทางการบริหารจัดการข้อมูล จึงเป็นสิ่งสำคัญอย่างยิ่งสำหรับองค์กรภาครัฐในการเคลื่อนย้ายข้อมูลเข้าสู่ระบบคลาวด์ เพื่อให้เกิดประสิทธิภาพและประสิทธิผลสูงสุดภายใต้ความมั่นคงปลอดภัยและความเป็นส่วนตัวของข้อมูล การจัดระดับชั้นข้อมูลจึงถือเป็นหนึ่งในขั้นตอน

พื้นฐานที่มีความสำคัญสำหรับการเตรียมความพร้อมขององค์กรเข้าสู่การประมวลผลข้อมูลแบบคลาวด์ ซึ่งสอดคล้องกับหลักการจัดทำธรรมาภิบาลข้อมูลภาครัฐ ดังแสดงตามภาพ

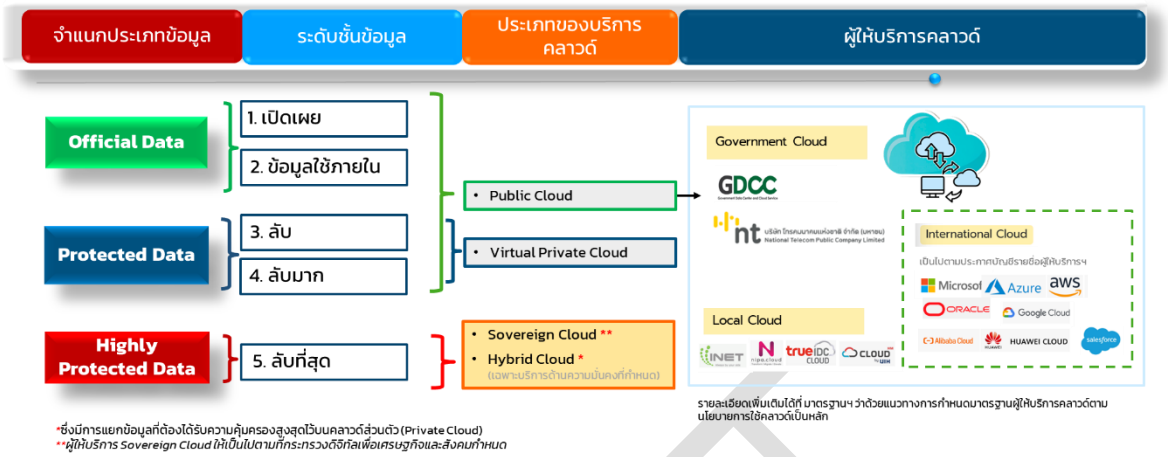
ภาพที่ 8 ขั้นตอนในการเตรียมองค์กรเข้าสู่การประมวลผลข้อมูลแบบคลาวด์

4.2 แนวทางการจำแนกประเภทข้อมูลกับการใช้คลาวด์

ประเทศไทย มีหลักการและแนวคิดที่ช่วยให้หน่วยงานภาครัฐสามารถพิจารณาหมวดหมู่ข้อมูลให้เป็นไปตามกรอบธรรมาภิบาลข้อมูลภาครัฐ (DGF) โดยพิจารณาการจัดระดับชั้นข้อมูลภาครัฐที่มีความอ่อนไหวให้สอดคล้องตามแนวมาตรฐานสากลและเป็นไปตามข้อกฎหมายที่เกี่ยวข้อง โดยการจัดระดับชั้นข้อมูลเพื่อบริหารจัดการข้อมูลภายในหน่วยงานแบ่งออกเป็น 5 ระดับ ได้แก่ 1. ชั้นข้อมูลเปิดเผย (Open) สู่สาธารณะ และ ชั้นข้อมูลที่สามารถเปิดเผยเมื่อได้รับอนุญาต ได้แก่ 2. ชั้นเผยแพร่ภายในองค์กร (Private) 3. ชั้นลับ (Confidential) ชั้นลับมาก (Secret) และ ชั้นข้อมูลที่เปิดเผยไม่ได้/ปกปิด ได้แก่ 5.ชั้นลับที่สุด (Top Secret) (สำนักงานพัฒนารัฐบาลดิทัล (องค์การมหาชน), 2565) โดยเจ้าของข้อมูล (Data Owner) เป็นผู้ประเมินระดับชั้นข้อมูลของหน่วยงาน ส่วนของฝ่ายเทคโนโลยีสารสนเทศ (IT department) ซึ่งมีหน้าที่ดูแลระบบและบริการของหน่วยงานให้สอดคล้องตามนโยบายหน่วยงานเป็นผู้ประเมินเพื่อการจำแนกประเภทข้อมูล ทั้งนี้หน่วยงานสามารถใช้เครื่องมือประเมินที่มี หรือใช้เครื่องมือการพิจารณาหมวดหมู่และระดับชั้นข้อมูล ซึ่งสามารถปรับให้สอดคล้องกับบริบทของหน่วยงานได้

โดยมุ่งเน้นให้หน่วยงานภาครัฐมีการใช้ระบบคลาวด์เป็นหลัก เพื่อส่งเสริมและพัฒนาให้หน่วยงานภาครัฐเป็นรัฐบาลดิจิทัล **จึงจำเป็นต้องมีการจัดระดับชั้นข้อมูลในภาพรวมของการให้บริการ (Service) โดยพิจารณาจากผลกระทบและความเสี่ยงที่อาจเกิดกับข้อมูล โดยแบ่งข้อมูลตามประเภทและมาตรการควบคุมความปลอดภัยที่เหมาะสม เพื่อนำไปสู่การพิจารณาประเภทของคลาวด์ และถิ่นที่อยู่ของข้อมูลตามลักษณะข้อมูล** โดยคำนึงถึงความสอดคล้องกับกฎหมายที่เกี่ยวข้อง เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) ที่กำหนดว่าการประมวลผลข้อมูลส่วนบุคคลนอกประเทศต้องได้รับการอนุญาต และข้อมูลที่เป็นความลับตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ยังเป็นการเพิ่มความมั่นคงและปลอดภัยของข้อมูล โดยมีการควบคุมทางกายภาพ (Physical control) ของศูนย์ข้อมูลได้โดยตรง **โดยเฉพาะข้อมูลบริการที่ประกอบด้วย ข้อมูลในระดับชั้นลับที่สุด และสอดคล้องตามนโยบายและแผนความมั่นคงแห่งชาติฯ หรือเป็นไปตามประกาศ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง หลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐาน**

สำคัญทางสารสนเทศ (CII) และการมอบหมายการควบคุมและกำกับดูแล พ.ศ. 2568 โดยสามารถพิจารณาเลือกใช้คลาวด์ตามประกาศ**กรอบแนวทางการบริหารจัดการคลาวด์ภาครัฐ**



ภาพที่ 9 กรอบแนวทางการจำแนกประเภทข้อมูลสำหรับการใช้คลาวด์

กรอบแนวทางในการจำแนกประเภทข้อมูลสำหรับการใช้คลาวด์ โดยหน่วยงานภาครัฐพิจารณาการนำข้อมูลจัดเก็บในระบบคลาวด์เป็นลำดับแรก แล้วจึงพิจารณาประเภทของคลาวด์ที่เหมาะสมเป็นลำดับถัดไป ซึ่งข้อสรุปจากการประชุมคณะอนุกรรมการด้านบริหาร จัดการความต้องการใช้คลาวด์ การให้บริการคลาวด์ และมาตรฐานการบริหารจัดการคลาวด์ภาครัฐ ได้กำหนดกรอบการจำแนกประเภทข้อมูลสำหรับการใช้คลาวด์ออกเป็น 3 ประเภท ซึ่งสอดคล้องกับระดับชั้นข้อมูล แบ่งได้ดังนี้

จากภาพที่กล่าวมา จะเห็นได้ว่า ประเทศไทยมีการจำแนกประเภทข้อมูลออกเป็น 3 ประเภท ได้แก่ ข้อมูลที่สามารถเปิดเผยได้ (Official Data) ข้อมูลที่ต้องได้รับความคุ้มครอง (Protected Data) ข้อมูลที่ต้องได้รับความคุ้มครองสูงสุด (Highly Protected Data) ซึ่งในแต่ละประเภทต้องมีการกำหนดมาตรการรักษาความปลอดภัยตามลักษณะข้อมูล และสามารถกำกับดูแลข้อมูลภายใต้กฎหมายไทย สรุปได้ดังนี้

ตารางที่ 10: การจำแนกประเภทข้อมูลของประเทศไทย

จำแนกประเภทข้อมูล	ลักษณะ	ตัวอย่างข้อมูล	มาตรการรักษาความปลอดภัย
Official Data	• ข้อมูลข่าวสารที่รัฐเปิดเผยให้ประชาชนโดยทั่วไป • ข้อมูลที่หน่วยงานใช้ในการปฏิบัติงานภายใน	• เว็บไซต์ • Social Media • หนังสือสารบรรณ • เอกสารประกอบการประชุมออนไลน์ • เอกสารจัดซื้อจัดจ้าง	• กำหนดมาตรการควบคุมความปลอดภัย • กำหนดให้มีผู้ที่สามารถเข้าถึงข้อมูลได้เท่าที่จำเป็น (Need to Know Basis)
Protected Data	• ข้อมูลที่หากเปิดเผยอาจเกิดความเสียหายต่อรัฐ • ข้อมูลที่หากเปิดเผยอาจเกิดความเสียหายร้ายแรงต่อรัฐ	• ข้อมูลการเสียภาษี • ข้อมูลบัญชีธนาคาร • ข้อมูลประวัติการรักษาพยาบาล	• กำหนดมาตรการควบคุมความปลอดภัย • กำหนดให้มีผู้ที่สามารถเข้าถึงข้อมูลได้เท่าที่

จำแนกประเภทข้อมูล	ลักษณะ	ตัวอย่างข้อมูล	มาตรการรักษาความปลอดภัย
		• ข้อมูลประวัติการรักษาพยาบาลของประชาชนจำนวนมาก	จำเป็น (Need to Know Basis) • ควบคุมการเข้าถึงฐานข้อมูล • การเข้ารหัสข้อมูล การใช้เทคโนโลยีกุญแจคู่
Highly Protected Data	• ข้อมูลที่หากเปิดเผยอาจเกิดความเสียหายร้ายแรงที่สุดต่อรัฐ เช่น แผนปฏิบัติการทางทหาร	• แผนการป้องกันประเทศ • ข้อมูลเกี่ยวกับความสัมพันธ์ระหว่างประเทศ • ข้อมูลเกี่ยวกับความมั่นคงของสถาบันพระมหากษัตริย์	• มีการควบคุมเข้าถึงหรืออ่านข้อมูลที่ต้องได้รับการคุ้มครองเข้มงวดสูงสุด เช่น มีการเข้ารหัสที่ซับซ้อนระหว่างการสร้าง การจัดเก็บ • ห้ามส่งข้อมูลนอกระบบเครือข่าย Secure Isolated Network

ข้อกำหนดเฉพาะสำหรับข้อมูลระดับ "ลับที่สุด"

คณะกรรมการพัฒนารัฐบาลดิจิทัลยังได้กำหนดข้อบังคับที่เข้มงวดสำหรับหน่วยงานที่จัดทำระบบดิจิทัลซึ่งจำเป็นต้องจัดเก็บข้อมูลระดับ **ลับที่สุด (Top Secret)** ที่มีความสอดคล้องกับนโยบายและแผนความมั่นคงแห่งชาติฯ ดังนี้:

- หากมีความจำเป็นต้องใช้บริการคลาวด์สำหรับกรณีที่เป็นข้อมูลในระดับลับที่สุด และสอดคล้องกับนโยบายและแผนความมั่นคงแห่งชาติฯ โดยสามารถพิจารณาเลือกใช้คลาวด์ตามประกาศกรอบแนวทางการบริหารจัดการคลาวด์ภาครัฐ ตามนโยบายการบูรณการโครงสร้างพื้นฐานทางดิจิทัลคลาวด์แห่งชาติ โดยหน่วยงานรัฐต้องดำเนินการในการควบคุมและคุ้มครองข้อมูลสำคัญของรัฐให้เป็นไปตามกฎหมายที่เกี่ยวข้อง เช่น ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม

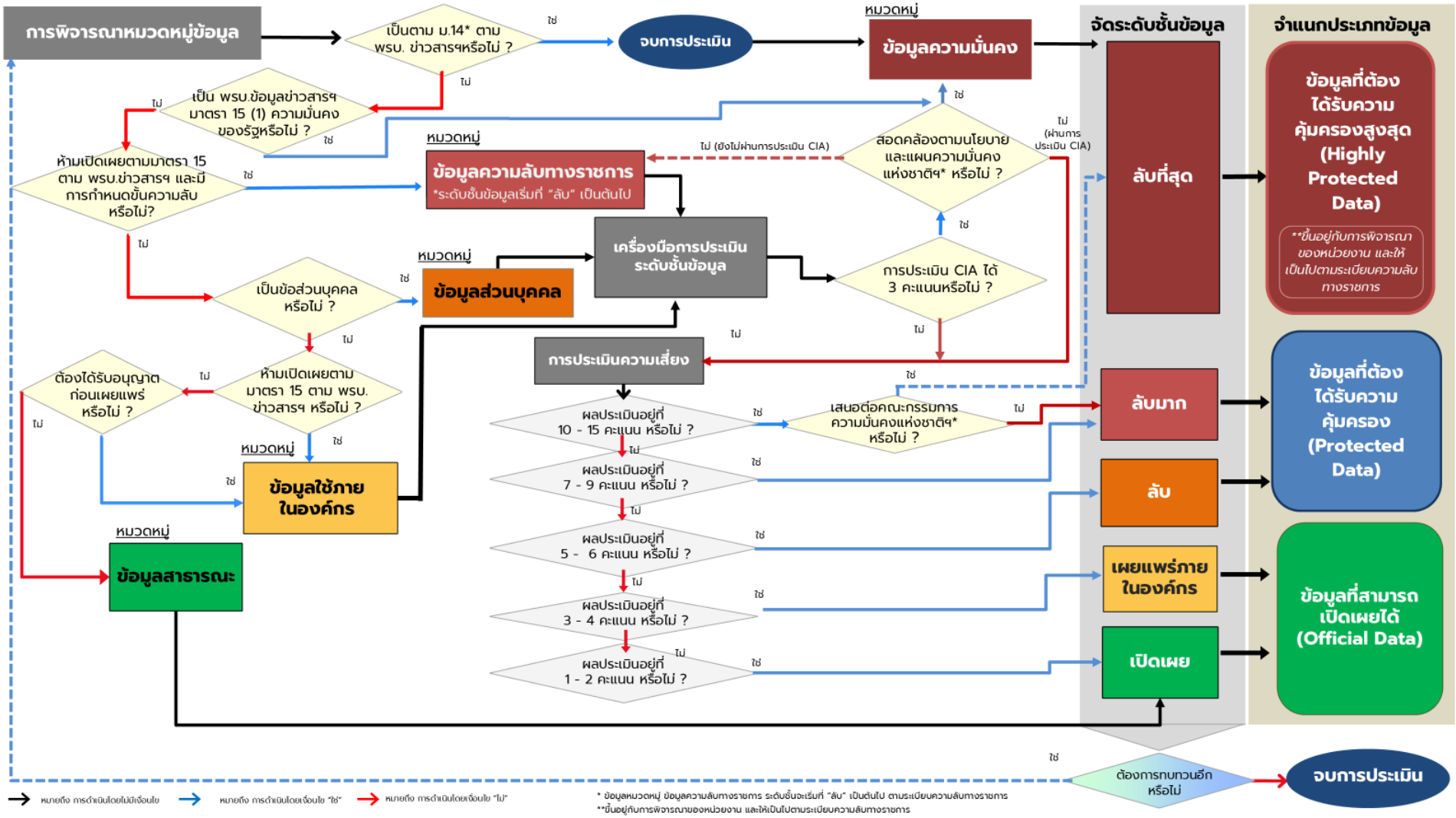
ประเทศไทยได้กำหนดหลักการและแนวคิดเพื่อช่วยให้หน่วยงานภาครัฐสามารถพิจารณาหมวดหมู่ข้อมูลให้เป็นไปตามกรอบธรรมาภิบาลข้อมูลภาครัฐ (DGF) ซึ่งสอดคล้องกับแนวมาตรฐานสากลและข้อกฎหมายที่เกี่ยวข้อง โดยเฉพาะอย่างยิ่งเพื่อสนับสนุนกรอบแนวทางการบริหารจัดการคลาวด์ภาครัฐที่มุ่งเน้นให้หน่วยงานภาครัฐมีการใช้ระบบคลาวด์เป็นหลักในการเป็นรัฐบาลดิจิทัล การจัดระดับชั้นข้อมูลมีความสำคัญอย่างยิ่งในการพิจารณาประเภทของคลาวด์และถิ่นที่อยู่ของข้อมูล เพื่อเพิ่มความมั่นคงปลอดภัยของข้อมูลและปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA)

กรอบแนวทางในการจำแนกประเภทข้อมูลสำหรับการใช้คลาวด์ สรุปการจำแนกข้อมูลเป็น 3 ประเภท ซึ่งสอดคล้องกับระดับชั้นข้อมูลข้างต้น โดยพิจารณาจากผลกระทบและความเสี่ยงที่อาจเกิดขึ้นกับข้อมูล

1) **ข้อมูลที่สามารถเปิดเผยได้ (Official Data)**
2) **ข้อมูลที่ต้องได้รับความคุ้มครอง (Protected Data)**
3) **ข้อมูลที่ต้องได้รับความคุ้มครองสูงสุด (Highly Protected Data)**

ในแต่ละประเภทข้อมูลนี้ จะมีการกำหนดมาตรการรักษาความปลอดภัยตามลักษณะข้อมูล และสามารถกำกับดูแลข้อมูลภายใต้กฎหมายไทยได้ การจำแนกประเภทข้อมูลนี้มุ่งเน้นไปที่ข้อมูลขณะพัก/จัดเก็บ (Data at Rest) เป็นหลัก โดยไม่รวมถึงข้อมูลที่อยู่ระหว่างการรับส่ง (Data in Transit) หรือการประมวลผล (Data Processing) โดยสามารถศึกษารายละเอียดเพิ่มเติมได้ตามประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง กรอบแนวทางการบริหารจัดการคลาวด์ภาครัฐ

1 **แผนผังการตัดสินใจสำหรับการจำแนกประเภทข้อมูล**



2

3 ภาพที่ 10 : แผนผังการตัดสินใจสำหรับการจำแนกประเภทข้อมูลสำหรับการใช้คลาวด์

4.2.1. ข้อมูลที่ต้องได้รับความคุ้มครองสูงสุด (Highly Protected Data)

<u>คำจำกัดความและลักษณะ:</u>

- เป็นประเภทข้อมูลที่มีความเสี่ยงสูงที่สุด ซึ่งหากเปิดเผยอาจก่อให้เกิดความเสียหายร้ายแรงที่สุดต่อสถาบันพระมหากษัตริย์ และความมั่นคงของชาติ หรือประโยชน์แห่งรัฐ[6]
- เทียบเท่ากับข้อมูลระดับ ชั้นลับที่สุด (Top Secret) ผลการประเมินอยู่ระหว่าง 10 – 15 คะแนน และสอดคล้องตามนโยบายและแผนความมั่นคงแห่งชาติฯ
- ตัวอย่างข้อมูล: แผนปฏิบัติการทางทหาร, แผนการป้องกันประเทศ, ข้อมูลเกี่ยวกับความสัมพันธ์ระหว่างประเทศ, ข้อมูลเกี่ยวกับความมั่นคงของสถาบันพระมหากษัตริย์

<u>ประเภทคลาวด์และถิ่นที่อยู่ของข้อมูลที่แนะนำ:</u>

- ให้พิจารณาเลือกใช้ประเภทของบริการคลาวด์ตาม (ร่าง) มาตรฐานฯ ว่าด้วยแนวทางการใช้คลาวด์
- การตัดสินใจนำข้อมูลประเภทนี้ขึ้นคลาวด์ให้เป็นดุลพินิจของหัวหน้าหน่วยงาน และให้เป็นไปตามกฎหมายที่เกี่ยวข้อง

<u>มาตรการรักษาความปลอดภัยและข้อเสนอแนะเบื้องต้น:</u>

- ต้องมี**มาตรการควบคุมความปลอดภัยที่เข้มงวดสูงสุด**
- มีการ**ควบคุมการเข้าถึงหรืออ่านข้อมูลอย่างเข้มงวดสูงสุด** เช่น มีการเข้ารหัสที่ซับซ้อน

<u>มาตรการรักษาความปลอดภัยและข้อเสนอแนะเบื้องต้นหว่างการสร้างและการจัดเก็บ</u>

- **ห้ามส่งข้อมูลนอกระบบเครือข่าย Secure Isolated Network**
- เจ้าของระบบ/CIO มีอำนาจในการพัฒนามาตรการควบคุมความปลอดภัยที่เข้มงวดสูงสุด
- ต้องมีมาตรการควบคุมความปลอดภัยทางไซเบอร์ตามที่คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติกำหนด
- กำหนดล็อกอุปกรณ์ทุกครั้งเมื่อออกจากพื้นที่ทำงาน
- ในการบริหารจัดการข้อมูล ควรมีการกำหนดบทบาทผู้ที่เกี่ยวข้อง กำหนดนโยบายและแนวปฏิบัติการบริหารจัดการข้อมูลเป็นลายลักษณ์อักษร รวมถึงการลงนามข้อตกลงไม่เปิดเผยข้อมูล (Non-disclosure agreements) และข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement)

[6] ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544

4.2.2. ข้อมูลที่ต้องได้รับความคุ้มครอง (Protected Data)

<u>คำจำกัดความและลักษณะ:</u>

- เป็นประเภทข้อมูลที่มี ความเสี่ยงปานกลาง และต้องการมาตรการควบคุมความปลอดภัยที่สูง
- มักเป็นข้อมูลที่องค์กรไม่ได้เผยแพร่โดยอิสระ โดยทั่วไปเกี่ยวข้องกับข้อมูลที่มีลักษณะเป็นส่วนตัว ไม่ว่าจะเป็นข้อมูลบุคคลหรือองค์กร
- หากเปิดเผยโดยไม่ได้รับอนุญาตอาจก่อให้เกิด ความสูญเสีย/ผลกระทบอย่างร้ายแรงต่อชื่อเสียง การเงิน หรือทรัพย์สิน หรือต่อความมั่นคงและผลประโยชน์แห่งรัฐอย่างร้ายแรงหรือสำคัญ
- ข้อมูลประเภทนี้อยู่ในระดับ ชั้นลับ (Confidential) และ ชั้นลับมาก (Secret) ผลการประเมินอยู่ระหว่าง 5 – 9 คะแนน หรือ ผลการประเมินอยู่ระหว่าง 10 –15 คะแนน และไม่สอดคล้องตามนโยบายและแผนความมั่นคงแห่งชาติฯ
- ตัวอย่างข้อมูล: ข้อมูลการเสียภาษี, ข้อมูลบัญชีธนาคาร, ข้อมูลประวัติการรักษาพยาบาล
- บริการที่มีข้อมูลประเภทนี้ ได้แก่ การบริการข้อมูลสำหรับการดำเนินการภายใน, บริการ ERP, ระบบเงินเดือน

<u>ประเภทคลาวด์และถิ่นที่อยู่ของข้อมูลที่แนะนำ:</u>

- ให้พิจารณาเลือกใช้ประเภทของบริการคลาวดตาม (ร่าง) มาตรฐานฯ ว่าด้วยแนวทางการใช้คลาวด์

<u>มาตรการรักษาความปลอดภัยและข้อเสนอแนะเบื้องต้น:</u>

- ต้องมีมาตรการควบคุมความปลอดภัยที่เข้มงวด
- กำหนดให้มีผู้ที่สามารถเข้าถึงข้อมูลได้เท่าที่จำเป็น (Need to Know Basis)
- ควบคุมการเข้าถึงฐานข้อมูล, การเข้ารหัสข้อมูล, การใช้เทคโนโลยีกุญแจคู่ (Asymmetric Encryption)
- เจ้าของระบบ/CIO มีอำนาจในการเข้าถึงและบริหารจัดการข้อมูลบนคลาวด์
- ควรจัดทำนโยบาย มาตรการ และแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลที่สอดคล้องกับ PDPA และการรักษาความมั่นคงปลอดภัยทางไซเบอร์เพื่อป้องกันการละเมิดข้อมูล รวมถึงการลงนามข้อตกลงการประมวลผลข้อมูลส่วนบุคคล

4.2.3. ข้อมูลที่สามารถเปิดเผยได้ (Official Data)

<u>คำจำกัดความและลักษณะ:</u>

- เป็นประเภทข้อมูลที่มี ความเสี่ยงต่ำ
- เป็นข้อมูลที่สร้าง ประมวลผล ส่ง หรือรับของหน่วยงานภาครัฐและหน่วยงานที่เกี่ยวข้อง
- ข้อมูลประเภทนี้อยู่ในระดับ ชั้นเผยแพร่ภายในองค์กร (Private) และ ชั้นเปิดเผย (Open) ผลการประเมินอยู่ระหว่าง 1 – 4 คะแนน
- ตัวอย่างข้อมูล: เว็บไซต์, Social Media, หนังสือสารบรรณ, เอกสารประกอบการประชุมออนไลน์, เอกสารจัดซื้อจัดจ้าง
- บริการที่มีข้อมูลประเภทนี้ ได้แก่ การบริการข้อมูลการดำเนินการของภาครัฐ, การบริการแจ้งข่าวสารต่างๆ

<u>ประเภทคลาวด์และถิ่นที่อยู่ของข้อมูลที่แนะนำ:</u>

- ให้พิจารณาเลือกใช้ประเภทของบริการคลาวดตาม (ร่าง) มาตรฐานฯ ว่าด้วยแนวทางการใช้คลาวด์

<u>มาตรการรักษาความปลอดภัยและข้อเสนอแนะเบื้องต้น:</u>

- ควรมี การกำหนดมาตรการควบคุมความปลอดภัย
- กำหนดให้มีผู้ที่สามารถเข้าถึงข้อมูลได้เท่าที่จำเป็น (Need to Know Basis)
- เจ้าของระบบ/CIO สามารถเข้าถึงและมีสิทธิในการบริหารจัดการข้อมูลบนคลาวด์ได้
- มีการกำหนดบทบาทผู้ที่เกี่ยวข้องกับกรอบธรรมาภิบาลข้อมูลภาครัฐ และจัดทำนโยบายและแนวปฏิบัติการบริหารจัดการข้อมูลเป็นลายลักษณ์อักษร
- มีการกำหนดนโยบาย มาตรการ วิธีการ และแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของข้อมูล เพื่อป้องกันการละเมิด การเข้าถึง การสูญหาย การทำลาย หรือการเปลี่ยนแปลงข้อมูล

<u>สรุปแนวทางการจำแนกประเภทข้อมูล</u>

การจำแนกประเภทข้อมูลสรุปได้ดังนี้

- ข้อมูลที่สามารถเปิดเผยได้ (Official Data) และ ข้อมูลที่ต้องได้รับความคุ้มครอง (Protected Data) ซึ่งมีคะแนนการประเมินความเสี่ยงระหว่าง 1 – 9 คะแนน และไม่สอดคล้องตามนโยบายและแผนความมั่นคงแห่งชาติฯ หรือคะแนนการประเมินความเสี่ยงต่ำกว่า 10 คะแนน สามารถใช้ Public Cloud ได้
- สำหรับ ข้อมูลที่ต้องได้รับความคุ้มครองสูงสุด (Highly Protected Data) ซึ่งมีคะแนนการประเมินความเสี่ยงที่ 10 – 15 คะแนน และสอดคล้องตามนโยบายและแผนความมั่นคงแห่งชาติฯ

เป็นข้อมูลที่มีผลกระทบต่อความมั่นคงของชาติจำเป็นต้องมีมาตรการควบคุมรักษาความปลอดภัยที่เข้มงวดสูงสุด ต้องพิจารณาเลือกใช้ประเภทของบริการคลาวด์ตาม (ร่าง) มาตรฐานฯ ว่าด้วยแนวทางการใช้คลาวด์

หน่วยงานภาครัฐจำเป็นต้องดำเนินการประเมินความเสี่ยงอย่างรอบคอบ เพื่อพิจารณาเลือกใช้บริการคลาวด์ที่เหมาะสมกับบริบทของแต่ละหน่วยงาน โดยควรคำนึงถึงระดับความเสี่ยง (Risk), ค่าใช้จ่าย (Cost), ความปลอดภัย (Security), ความสามารถในการปรับขยาย (Scalability), ความยืดหยุ่น (Flexibility), ความง่ายในการเริ่มต้นใช้งาน (Ease of 1st time user) และการควบคุมข้อมูล (Data Control)

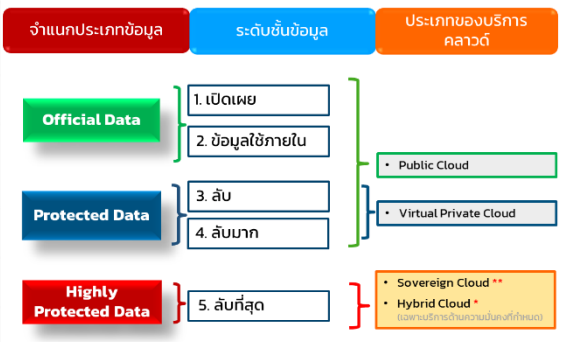
ทั้งนี้ กระบวนการนี้ยังเกี่ยวข้องกับการทำงานร่วมกันระหว่างเจ้าของระบบงาน ผู้ปฏิบัติงานฝ่ายเทคโนโลยีสารสนเทศ และผู้ปฏิบัติงานด้านข้อมูลขององค์กร เพื่อให้มีการบริหารจัดการข้อมูลที่เหมาะสมตลอดวงจรชีวิตข้อมูล

5. เครื่องมือเพื่อนำไปสู่การปฏิบัติ

หน่วยงานสามารถทำการประเมินจำแนกประเภทข้อมูลสำหรับการใช้คลาวด์ โดยสามารถประยุกต์การจำแนกประเภทข้อมูลจาก [เครื่องมือการพิจารณาหมวดหมู่และระดับชั้นข้อมูล โดยคลิกที่นี่](#) เพื่อพิจารณาความเสี่ยงบริการของหน่วยงานภาครัฐในการใช้คลาวด์โดยมีขั้นตอนดังนี้ **(ข้อเสนอแนะ : ผู้ประเมินควรเป็น ฝ่ายเทคโนโลยีสารสนเทศ)**

1. **ประเมินข้อมูลในบริการ** โดยพิจารณาจากระดับผลกระทบตามวัตถุประสงค์ด้านความปลอดภัยของข้อมูล (Security Objective) โดยนำผลประโยชน์แห่งชาติจากการเปิดเผยข้อมูล โดยไม่ได้อนุญาตมาประกอบการพิจารณา
2. **ประเมินหาระดับความเสี่ยง**ของข้อมูลในบริการตามเกณฑ์การประเมินโอกาสที่จะเกิดและผลกระทบจากการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต
3. **ติดป้ายหรือแท็กกำกับระดับชั้นข้อมูล**ตามความอ่อนไหว ความเสี่ยงและผลกระทบจากการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

ระดับชั้นข้อมูล	ระดับความเสี่ยง	ค่าระดับความเสี่ยง
เปิดเผย	น้อยมาก	1 – 2
เผยแพร่ภายในองค์กร	น้อย	3 – 4
ลับ	ปานกลาง	5 – 6
ลับมาก	สูง	7 – 9
ลับที่สุด	สูงมาก	10 – 15



4. **จัดระดับชั้นข้อมูล และ ประเภทข้อมูลบนคลาวด์** เมื่อได้ประเภทข้อมูลบนคลาวด์แล้ว จะได้ เลือกใช้ประเภทของบริการคลาวด์ที่เหมาะสมต่อไป

หมายเหตุ พิจารณารายละเอียดเพิ่มเติมได้ที่เครื่องมือการพิจารณาหมวดหมู่และจัดระดับชั้นข้อมูล

5.1 เครื่องมือและตัวอย่างการประเมิน

ตัวอย่างการประเมินบริการทางดิจิทัล (E-Government Service)

ประเภทข้อมูล					
วัตถุประสงค์ด้านความปลอดภัย (CIA)	**ผลกระทบด้านความลับ (Confidentiality)**		**ผลกระทบด้านความถูกต้องครบถ้วนสมบูรณ์ ความคงสภาพ (Integrity)**		**ผลกระทบด้านความพร้อมใช้งานข้อมูล(Availability)**
	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบน้อย/อย่างจำกัด (limited) และเกิดผลประโยชน์แห่งชาติ**สำคัญน้อย**		การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบน้อย/อย่างจำกัด (limited) และเกิดผลประโยชน์แห่งชาติ**สำคัญ**		การหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลข่าวสารหรือระบบสารสนเทศอาจส่งผลกระทบน้อย/อย่างจำกัด (limited) และเกิดผลประโยชน์แห่งชาติ**สำคัญน้อย**
ระดับผล CIA	**ปานกลาง** (2 คะแนน)		**ปานกลาง** (2 คะแนน)		**ต่ำ** (1 คะแนน)
ค่าเฉลี่ย CIA	**ปานกลาง 2** (1.67 ปัดเป็น 2 คะแนน)				
ผลกระทบ/ผลประโยชน์	**ด้านการเงินและสินทรัพย์**	**ด้านภาพลักษณ์/ชื่อเสียง**	**ด้านผู้ใช้บริการหรือประชาชน**	**ด้านการดำเนินการตามกฎหมาย**	**ด้านความมั่นคงของรัฐ** (ค่าเฉลี่ย CIA)
โอกาสที่จะเกิดขึ้น (Likelihood)	น้อยครั้ง (2 คะแนน)	สูง (4 คะแนน)	บ่อยครั้ง (2 คะแนน)	น้อยมาก (1 คะแนน)	น้อยมาก (2 คะแนน)
ประเมินหาระดับความรุนแรงของผลกระทบ (Impact)	ปานกลาง (2 คะแนน)	ต่ำ (3 คะแนน)	สูง (1 คะแนน)	น้อย (1 คะแนน)	ปานกลาง (2 คะแนน)
ความเสี่ยง (Likelihood x Impact)	4 คะแนน	12 คะแนน	2 คะแนน	1 คะแนน	4 คะแนน
ค่าเฉลี่ยความเสี่ยง	**ปานกลาง 5** (ระดับความเสี่ยง 4.6 คะแนน)				
ระดับชั้น	**ชั้นลับ**				

ระดับชั้น	ค่าระดับความเสี่ยง	ความหมาย
เปิดเผย	1 - 2	ต่ำมาก ระดับความเสี่ยงที่องค์กรสามารถยอมรับได้ โดยไม่ต้องมีมาตรการควบคุมก็ได้
เผยแพร่ภายในองค์กร	3 - 4	ระดับความเสี่ยงที่องค์กรสามารถยอมรับได้ โดยมีมาตรการควบคุมอยู่แล้วหรือไม่ก็ได้ แต่อาจต้องมีการติดตามเป็นระยะๆ
ลับ	5 - 6	ระดับความเสี่ยงที่องค์กรสามารถยอมรับได้โดยต้องมีมาตรการควบคุมหรือมีแผนการลดความเสี่ยง เพื่อลดความเสี่ยงให้ไปอยู่ในระดับต่ำและป้องกันไม่ให้ความเสี่ยงเพิ่มขึ้น
ลับมาก	7 - 9	ระดับความเสี่ยงที่องค์กรไม่สามารถยอมรับได้ และต้องจัดการลดความเสี่ยงให้ไปอยู่ในระดับต่ำลงโดยเร็ว โดยต้องจัดให้มีแผนการลดความเสี่ยงและป้องกันไม่ให้ความเสี่ยงกลับเพิ่มสูงขึ้นด้วย
ลับที่สุด	10 - 15	ระดับความเสี่ยงที่องค์กรไม่สามารถยอมรับได้ และต้องจัดการลดความเสี่ยงให้ไปอยู่ในระดับต่ำลงในทันที หรืออาจมีการถ่ายโอนความเสี่ยง โดยต้องจัดให้มีแผนการลดความเสี่ยงและป้องกันไม่ให้ความเสี่ยงกลับเพิ่มสูงขึ้นด้วย [7]

[7] หน่วยงานสามารถชี้แจงได้ในกรณีที่บริการของหน่วยงานเป็นระดับชั้นลับที่สุดแต่ไม่สอดคล้องกับนโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติฯ

สรุป จากการบริการทางดิจิทัล (E-Government Service) มีค่าเฉลี่ยความเสี่ยงอยู่ที่ 5 คะแนน ระดับชั้นข้อมูลเป็นระดับลับ สามารถพิจารณาจำแนกเป็นประเภทข้อมูลเพื่อนำขึ้นคลาวด์ เป็นข้อมูลประเภทต้องได้รับความคุ้มครอง เลือกใช้คลาวด์ประเภท Public Cloud ซึ่งเป็นดุลพินิจของเจ้าของระบบงาน/CIO พิจารณาตามความเหมาะสมของบริการ โดยต้องมีอำนาจในการเข้าถึงข้อมูลและกำหนดสิทธิผู้เข้าถึงข้อมูลบนคลาวด์ได้

5.2 ข้อเสนอแนะสู่การปฏิบัติ

ปัจจุบันมีความจำเป็นในการใช้ข้อมูลภาครัฐอย่างมีประสิทธิภาพเพิ่มมากขึ้นเพื่อปรับปรุงการให้บริการภาครัฐและแก้ปัญหาเชิงนโยบายที่มีความซับซ้อน หลักการพื้นฐานของการจัดระดับชั้นข้อมูลจะช่วยให้ค้นหาแหล่งที่มาของข้อมูลและเรียกดูข้อมูลได้ง่ายขึ้น มีความสะดวกในการเข้าถึง การรักษาการปฏิบัติตามกฎระเบียบ และเพื่อให้เป็นไปตามวัตถุประสงค์ของการดำเนินภารกิจขององค์กรหรือส่วนบุคคลอื่นๆ ดังนั้นหน่วยงานภาครัฐจึงควรให้ความสำคัญมากขึ้น ดังนั้นเพื่อให้เกิดการขับเคลื่อนและเป็นประโยชน์สูงสุดจึงกำหนดข้อเสนอแนะในการปฏิบัติเบื้องต้นเพื่อให้หน่วยงานภาครัฐนำไปใช้เป็นแนวทางดำเนินการ ดังนี้

1) **พิจารณาข้อมูล** : มีการกำหนดข้อมูลสอดคล้องตามนโยบายและยุทธศาสตร์ด้านข้อมูลของหน่วยงาน พิจารณากำหนดหมวดหมู่ข้อมูลตามธรรมาภิบาลข้อมูลภาครัฐ
2) **ประเมินระดับชั้นข้อมูล** : ดำเนินการจัดระดับชั้นข้อมูลตามแบบประเมินที่มีหรือเครื่องมือการพิจารณาหมวดหมู่และระดับชั้นข้อมูล โดยสามารถยึดเกณฑ์การพิจารณาตามแบบประเมินที่กำหนดเป็นหลัก หรือหน่วยงานสามารถกำหนดเกณฑ์การพิจารณาระดับผลกระทบและผลประโยชน์แห่งชาติให้สอดคล้องกับนโยบายและกฎระเบียบที่เกี่ยวข้อง และเหมาะสมกับบริบทขององค์กรได้ ทั้งนี้กรณีข้อมูลสอดคล้องตามนโยบายและแผนความมั่นคงแห่งชาติฯ จะเทียบเท่ากับข้อมูลระดับ ชั้นลับที่สุด (Top Secret) เป็นประเภทข้อมูลที่ต้องได้รับความคุ้มครองสูงสุด (Highly Protected Data)
3) **ปรับใช้งาน** : พิจารณาเลือกใช้ประเภทของบริการคลาวด์อย่างเหมาะสม ตามประกาศกรอบแนวทางการบริหารจัดการคลาวด์ภาครัฐ โดยพิจารณาตามผลการประเมิน
4) **ทบทวนระดับชั้นข้อมูล** : ในกรณีข้อมูลที่มีความเคลื่อนไหวหรือเปลี่ยนแปลงเป็นประจำควรมีการทบทวนอย่างน้อยปีละ 1 ครั้ง หรือในกรณีมีการดำเนินการครบตามกรอบระยะเวลา รวมถึงมีการเปลี่ยนแปลงด้านเทคโนโลยีหรือสภาพแวดล้อมของข้อมูล หน่วยงานควรทบทวนการประเมินข้อมูลใหม่อีกครั้ง ส่วนในกรณีที่ข้อมูลไม่มีการเปลี่ยนแปลงหน่วยงานสามารถพิจารณารอบการทบทวนการจัดระดับชั้นเองได้ ทั้งนี้เพื่อให้ข้อมูลมีความพร้อมในการใช้งาน

6. ภาคผนวก

รายชื่อหน่วยงานตามนโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ (พ.ศ. 2566 – 2570)

หมวดประเด็นความมั่นคง	ตัวอย่างชุดข้อมูล	หน่วยงาน
1. การเสริมสร้างความมั่นคงของสถาบันหลักของชาติ	● ข้อมูลความเกี่ยวกับสถาบันพระมหากษัตริย์	กองอำนวยการรักษาความมั่นคงภายในราชอาณาจักร
2. การปกป้องอธิปไตยและผลประโยชน์ของชาติ และการพัฒนาศักยภาพการป้องกันประเทศ	● ข้อมูลความสามารถเชิงยุทธศาสตร์ของกองทัพ	กระทรวงกลาโหม
3. การรักษาความมั่นคงและผลประโยชน์ของชาติพื้นที่ชายแดน	● ข้อมูลปัญหาความมั่นคงกับประเทศรอบบ้าน	กระทรวงมหาดไทย
4. การรักษาความมั่นคงและผลประโยชน์ของชาติทางทะเล	● ข้อมูลตำแหน่งที่ตั้งสำคัญในภูมิภาคท้องทางบกและทะเล	ศูนย์อำนวยการรักษาผลประโยชน์ของชาติทางทะเล
5. การป้องกันและแก้ไขปัญหาจังหวัดชายแดนภาคใต้	● ข้อมูลที่เกี่ยวข้องกับปัญหาชายแดนภาคใต้	สำนักงานสภาความมั่นคงแห่งชาติ
6. การบริหารจัดการผู้หลบหนีเข้าเมืองและ ผู้โยกย้ายถิ่นฐานแบบไม่ปกติและผู้โยกย้ายถิ่นฐานแบบไม่ปกติ	● ข้อมูลจัดการผู้มีปัญหาสถานะและสิทธิบุคคลของกลุ่มที่มีความเปราะบางต่อความมั่นคงและความสัมพันธ์ระหว่างประเทศ	กองอำนวยการรักษาความมั่นคงภายในราชอาณาจักร
7. การป้องกันและแก้ไขปัญหาการค้ามนุษย์	● ข้อมูลการดำเนินคดีค้ามนุษย์	กระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์
8. การป้องกัน ปราบปราม และแก้ไขปัญหายาเสพติด	● ข้อมูลการลักลอบลำเลียง ปราบปรามผู้ค้ายาเสพติดและเครือข่ายการค้ายาเสพติดในประเทศและอาชญากรรมข้ามชาติ	สำนักงานคณะกรรมการป้องกันและปราบปรามยาเสพติด
9. การป้องกันและบรรเทาสาธารณภัย	● ข้อมูลสาธารณภัยและแผนการบรรเทาทุกข์	กรมป้องกันและบรรเทาสาธารณภัย
10. การป้องกันและแก้ไขปัญหาความมั่นคงทางไซเบอร์	● ข้อมูลการโจมตีทางไซเบอร์และมาตรการในการป้องกัน	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
11. การป้องกันและแก้ไขปัญหาการก่อการร้าย	● ข้อมูลข่าวสารและข่าวกรองด้านการก่อการร้าย	สำนักงานสภาความมั่นคงแห่งชาติ
12. การสร้างดุลยภาพระหว่างประเทศ	● ข้อมูลภัยคุกคามระดับภูมิภาค ● ข้อมูลหมอกควันข้ามแดน	กระทรวงการต่างประเทศ

หมวดประเด็นความมั่นคง	ตัวอย่างชุดข้อมูล	หน่วยงาน
13. การบริหารจัดการภาวะฉุกเฉินด้านสาธารณสุข และโรคติดต่ออุบัติใหม่	● ข้อมูลรายชื่อผู้ป่วยติดต่อโรคอุบัติใหม่ ● ข้อมูลผลวินิจฉัยโรคอุบัติใหม่	กระทรวงสาธารณสุข
14. การพัฒนาศักยภาพการเตรียมพร้อมแห่งชาติ และการบริหารจัดการวิกฤตการณ์ระดับชาติ	● การแจ้งเตือนและการสั่งการระหว่างหน่วยงานและผู้ปฏิบัติภารกิจเมื่อเข้าสู่ภาวะวิกฤติระดับชาติ	สำนักงานสภาความมั่นคงแห่งชาติ
15. การพัฒนาระบบข่าวกรองแห่งชาติ	● ข้อมูลประเมินการตอบสนอง และแจ้งเตือนต่อสถานการณ์ต่อความมั่นคงของชาติ	สำนักข่าวกรองแห่งชาติ
16. การบูรณาการข้อมูลด้านความมั่นคง	● ข้อมูลการป้องกันและแก้ไขภัยคุกคามที่ส่งผลกระทบต่อความมั่นคงแห่งชาติ	กองอำนวยการรักษาความมั่นคงภายในราชอาณาจักร
17. การเสริมสร้างความมั่นคงเชิงพื้นที่	● ข้อมูลความขัดแย้งทางพลังงาน อาหาร และน้ำ	กองอำนวยการรักษาความมั่นคงภายในราชอาณาจักร

หมายเหตุ: ในกรณีที่หน่วยงานของรัฐ มีข้อมูลที่เข้าข่ายข้อมูลความมั่นคง และผลการประเมินความเสี่ยงอยู่ในระดับชั้นข้อมูลลับที่สุด หากเปิดเผยอาจเกิดความเสียหายร้ายแรงที่สุดต่อรัฐ แต่ไม่ได้มีการกำหนดไว้ใน 17 ประเด็นความมั่นคงในตารางข้างต้น สามารถติดต่อ สำนักงานสภาความมั่นคงแห่งชาติ เพื่อขอปรับปรุงให้เป็นปัจจุบันต่อไป

บรรณานุกรม

[1] ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล. (2563) เรื่องธรรมาภิบาลข้อมูลภาครัฐ ประกาศ ณ วันที่ 12 มีนาคม 2563 คัดจากราชกิจจานุเบกษา เล่มที่ 137 ตอนพิเศษ 74 ง วันที่ 31 มีนาคม 2563.

[2] The National Institute of Standards and Technology. (2008) Guide for Mapping Types of Information and Information Systems to Security Categories (NIST 800-60 Volume 1. and 2.)

[3] Federal Information Processing Standards Publication. (2004) Standards for Security Categorization of Federal Information and Information Systems (FIPS PUB 199) (Url: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf)

[4] International Organization for Standardization. (2022) Information technology - Security techniques - Information security management systems – Requirements (ISO/IEC 27001)

[5] Steve Simmonds. (2020, April). The Importance of Implementing Data Classification Frameworks. Retrieved from https://synergygrc.com/the-importance-of-implementing-data-classification-frameworks/

[6] DATA CLASSIFICATION AWS (2022). Retrieved from https://www.oas.org/en/sms/cicte/docs/ENG-Data-Classidication.pdf

[7] ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม ประกาศ ณ วันที่ 30 พฤษภาคม 2561 คัดจากราชกิจจานุเบกษา 135 ตอนพิเศษ 148 ง วันที่ 26 มิถุนายน 2561.

[8] ระเบียบสำนักนายกรัฐมนตรี ว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. 2552 และที่แก้ไขเพิ่มเติม ประกาศ ณ วันที่ 31 ตุลาคม 2560 คัดจากราชกิจจานุเบกษา 134 ตอนพิเศษ 285 ง วันที่ 22 พฤศจิกายน 2560.

[9] Netwrix (2018) Data Classification Policy Example. Retrieved from https://www.netwrix.com/data_classification_policy_template.html

[10] Clark University. (2018) Data Classification Policies. Retrieved from https://www2.clarku.edu/offices/its/policies/pdf/data-classification-policy.pdf

[11] University of New South Wales. (2021) Data Classification Standard. Retrieved from https://www.unsw.edu.au/content/dam/pdfs/governance/policy/2022-01-policies/datastandard.pdf

[12] Harvard. (2017) Information Security Quick Reference Guide. Retrieved from https://security.harvard.edu/files/it-security/files/infosecquickguide20170920.pdf?m=1583529266

[13] Hamilton College. (2016) Procedure: Data Classification Handling Retrieved from https://www.hamilton.edu/documents/HCDataClassificationProcedure_20160808forwebsite.pdf

[14] พันเอก โสภณ ศิริงาม. (2549-2560). ตัวแบบในการกำหนดยุทธศาสตร์และยุทธศาสตร์ชาติ ในศตวรรษที่ 21 Retrieved from http://www.dsdw2016.dsdw.go.th/doc_pr/ndc_2559-2560/PDF/wpa_8293/ALL.pdf

[15] Carnegie Mellon University. (2019) Guidelines for Data Classification. Retrieved from https://www.cmu.edu/iso/governance/guidelines/data-classification.html

[16] Thomas Eck. (2019) 7 Steps to Effective Data Classification. Retrieved from https://edge.siriuscom.com/security/7-steps-to-effective-data-classification

[17] Amazon. (n.d.). ข้อมูลเบื้องต้นเกี่ยวกับ AWS GovCloud (สหรัฐฯ) Region. Retrieved from https://aws.amazon.com/th/govcloud-us/?whats-new-ess.sort-by=item.additionalFields.postDateTime&whats-new-ess.sort-order=desc.

[18] Cloud.cio.gov. (n.d.). Federal Cloud Computing Strategy (Cloud Smart). Retrieved from https://cloud.cio.gov/.

[19] Digital.gov. (n.d.). Cloud and infrastructure. Retrieved from https://digital.gov/topics/cloud-and-infrastructure/.

[20] GDPR. (2018). https://gdpr-info.eu/art-83-gdpr/. Retrieved from https://gdpr-info.eu/art-83-gdpr/.

[21] GOV.UK. (n.d.). Cloud Strategic Roadmap for Defence. Retrieved from https://www.gov.uk/government/publications/cloud-strategic-roadmap-for-defence/cloud-strategic-roadmap-for-defence.

[22] Intelligence.gov.au. (2024). Australian Government Announces Top Secret Cloud. Retrieved from https://www.intelligence.gov.au/news/top-secret-cloud.

[23] Oversight.house.gov. (n.d.). The State of the Cloud. Retrieved from https://oversight.house.gov/hearing/oversight-it-subcommittee-committee-to-examine-cloud-solutions/.

[24] PDPA Thailand. (2025). ปรับจริง 7 ล้าน ไม่ทำตาม PDPA. Retrieved from https://pdpathailand.com/pdpa-news/personal-data-protection-1st-fine-penalty/?srsltid=AfmBOoolqklNKdIpvfnpHPbCzJja2GOmX36ChqOpKE3nMMXQ5mQB0lK9.

[25] Protectivesecurity.gov.au. (2024). New Protective Security Policy Framework. Retrieved from https://www.protectivesecurity.gov.au