สพร./PRD
กุมภาพันธ์ 2568

มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัลอยู่ระหว่างการจัดทำ
ห้ามใช้หรือยึดร่างนี้เป็นมาตรฐาน

มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัลฉบับสมบูรณ์จะมีประกาศโดย
สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

ร่าง

มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
DGA Community Standard

ว่าด้วยแนวทางการจำแนกประเภทข้อมูลสำหรับใช้บริการคลาวด์ตามนโยบายการใช้คลาวด์เป็นหลัก
CLOUD DATA CLASSIFICATION GUIDELINE

สำหรับเวียนขอข้อคิดเห็นจากหน่วยงานต่างๆ ที่เกี่ยวข้อง

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

มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

DGA Community Standard

มสพร. X-256X

DGA X-256X

ว่าด้วยแนวทางการจำแนกประเภทข้อมูลสำหรับการใช้คลาวด์ตามนโยบายการใช้คลาวด์เป็นหลัก

CLOUD DATA CLASSIFICATION GUIDELINE

เวอร์ชัน 1.0

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
สำนักนายกรัฐมนตรี

มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

ว่าด้วยแนวทางการจำแนกประเภทข้อมูล สำหรับใช้บริการคลาวด์ตามนโยบาย การใช้คลาวด์เป็นหลัก

มสพร. X-256X

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
เลขที่ 999 ชั้น 4 สถาบันเพื่อการยุติธรรมแห่งประเทศไทย ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210
หมายเลขโทรศัพท์: 0 2612 6000 โทรสาร: 0 2612 6011 0 2612 6012

ประกาศโดย
สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
สำนักนายกรัฐมนตรี
วันที่

คณะกรรมการจัดทำร่างมาตรฐาน ข้อกำหนด และหลักเกณฑ์ ภายใต้พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562

ที่ปรึกษา

นางไอรดา เหลืองวิไล	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

ประธานกรรมการ

ผู้ช่วยศาสตราจารย์ณัฐวุฒิ หนูไพโรจน์	จุฬาลงกรณ์มหาวิทยาลัย

รองประธานกรรมการ

นายอาศิส อัญญะโพธิ์	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

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	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

คณะทำงานเทคนิคด้านมาตรฐานการบริหารจัดการข้อมูลภาครัฐ

ที่ปรึกษา

นางไอรดา เหลืองวิไล	รองผู้อำนวยการ รักษาการแทนผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ผู้ช่วยศาสตราจารย์ณัฐวุฒิ หนูไพโรจน์	จุฬาลงกรณ์มหาวิทยาลัย
นายอาศิส อัญญะโพธิ์	ผู้ช่วยผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
นางสาวฐิติรัตน์ ทิพย์สัมฤทธิ์กุล	มหาวิทยาลัยธรรมศาสตร์

ประธานคณะทำงาน

รองศาสตราจารย์ธีรณี อจลากุล	ผู้อำนวยการสถาบันข้อมูลขนาดใหญ่ (องค์การมหาชน)

รองประธานกรรมการ

ผู้ช่วยศาสตราจารย์โษฆศ์รัตต ธรรมบุษดี	มหาวิทยาลัยมหิดล

คณะทำงาน

นายมารุต บูรณรัช	ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
นางสาวปริสุทธิ์ จิตต์ภักดี	สถาบันข้อมูลขนาดใหญ่ (องค์การมหาชน)
นางสาวธัญลักษณ์ กริตาคม	สำนักข่าวกรองแห่งชาติ
นายอภิสิทธิ์ สุขสาคร	สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์
นางสาวปศิญา เชื้อดี	สำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ
นายนิเวช มิ่งโอฬาร	สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
นางสาวดารารัตน์ โฆษิตพิพัฒน์	สำนักงานคณะกรรมการพัฒนาระบบราชการ
นางกาญจนา ภู่มาลี	สำนักงานสถิติแห่งชาติ
นางสาวณัฐชยา ภาสสัทธา	สำนักงานสภาความมั่นคงแห่งชาติ
นายวันประชา เชาวลิตวงศ์	ธนาคารแห่งประเทศไทย
นางสาวอัญญดา เพ็ญพร	สำนักงานเศรษฐกิจการเกษตร
นายทรงกรด เกษกาญจนานุช	สำนักงานหลักประกันสุขภาพแห่งชาติ
นายกฤษดา มาลีวงศ์	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
นายศะรัณย์ ใจน้อม	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

คณะทำงานและเลขานุการ

นางสาวอุรัชฎา เกตุพรหม	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

วิเคราะห์และจัดทำมาตรฐานรัฐบาลดิจิทัล

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

แนวทางการจำแนกประเภทข้อมูลสำหรับใช้บริการคลาวด์ตามนโยบายการใช้คลาวด์เป็นหลัก เวอร์ชัน 1.0 จัดทำขึ้น เพื่อเป็นแนวทางให้กับภาครัฐพิจารณาจำแนกประเภทข้อมูล เพื่อนำข้อมูลจัดเก็บในระบบคลาวด์ภาครัฐที่มีความเหมาะสมกับประเภทข้อมูลเป็นลำดับแรก โดยแนวทางฉบับนี้ได้จัดทำตามแนวมาตรฐานและแนวปฏิบัติที่ดีของ

1. ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ เวอร์ชัน 1.0
2. มรด. 6 : 2566 มาตรฐานรัฐบาลดิจิทัลว่าด้วยกรอบธรรมาภิบาลข้อมูลภาครัฐ ฉบับปรับปรุง: แนวปฏิบัติ
3. ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์
4. ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567
5. ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม

และได้มีการจัดงานประชาพิจารณ์เพื่อเปิดรับฟังความคิดเห็นเป็นการทั่วไป และนำข้อมูล ข้อสังเกต ข้อคิดเห็นจากผู้ทรงคุณวุฒิและจากหน่วยงานที่เกี่ยวข้อง เพื่อให้ข้อเสนอแนะเกี่ยวกับมาตรฐานฉบับนี้มีความสมบูรณ์ครบถ้วน และสามารถนำไปปรับใช้ในทางปฏิบัติได้อย่างมีประสิทธิภาพ

แนวทางการจำแนกประเภทข้อมูลสำหรับใช้บริการคลาวด์ตามนโยบายการใช้คลาวด์เป็นหลัก เวอร์ชัน 1.0 ฉบับนี้จัดทำโดยฝ่ายมาตรฐานดิจิทัลภาครัฐ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) สำนักนายกรัฐมนตรี

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
เลขที่ 999 ชั้น 4 สถาบันเพื่อการยุติธรรมแห่งประเทศไทย
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210
หมายเลขโทรศัพท์: (+66) 0 2612 6000 โทรสาร: (+66) 0 2612 6011
E-mail: sd-g1_division@dga.or.th
Website: www.dga.or.th

คำนำ

แนวทางการขับเคลื่อนตามนโยบายการใช้คลาวด์เป็นหลัก (Cloud First Policy) ตามมติคณะรัฐมนตรีที่ได้แถลงนโยบาย “Go Cloud First” เมื่อวันที่ 11 กันยายน พ.ศ. 2566 ได้มีการแต่งตั้งคณะอนุกรรมการด้านบริหารจัดการความต้องการใช้บริการคลาวด์ (Demand) การใช้บริการคลาวด์ (Supply) และมาตรฐานสำหรับการบริหารจัดการบริการคลาวด์ภาครัฐ (Government Cloud Management) และแต่งตั้งคณะอนุกรรมการด้านกฎหมายการจัดซื้อจัดจ้างบริการคลาวด์ภาครัฐ จากการประชุมและการดำเนินงานที่ผ่านมาได้มีการสรุปประเด็นที่เกี่ยวข้องออกมาเป็นข้อเสนอกรอบแนวทางในการบริหารจัดการคลาวด์ภาครัฐ เพื่อให้แนวทางการขับเคลื่อนตามนโยบายการใช้คลาวด์เป็นหลักนั้นจึงได้มีแผนงานสำหรับการจัดทำแนวปฏิบัติที่เกี่ยวข้อง จำนวน 3 แนวปฏิบัติ คือ แนวปฏิบัติด้านความต้องการการใช้คลาวด์ แนวทางการจำแนกประเภทข้อมูลสำหรับใช้บริการคลาวด์ และแนวทางการขึ้นทะเบียนผู้ให้บริการคลาวด์ (Cloud Service Provider) และเนื่องจากเป้าหมายของการพัฒนาประเทศตามยุทธศาสตร์ชาติ 20 ปี (พ.ศ. 2561–2580) ให้ความสำคัญกับการใช้เทคโนโลยีระบบคลาวด์มาเป็นเครื่องมือสำคัญในการตอบสนองต่อความต้องการ เพื่อให้กระบวนการทำงานและการให้บริการประชาชนยกระดับเป็นรัฐบาลดิจิทัลได้อย่างรวดเร็ว ประกอบกับพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 กำหนดให้หน่วยงานของรัฐจัดให้มีการบริหารงานภาครัฐและการจัดทำบริการสาธารณะเป็นไปด้วยความสะดวก รวดเร็ว มีประสิทธิภาพ และตอบสนองต่อการให้บริการและการอำนวยความสะดวกแก่ประชาชน โดยหน่วยงานของรัฐต้องจัดให้มีการบริหารงานและการจัดทำบริการสาธารณะในรูปแบบและช่องทางดิจิทัล ซึ่งมีการบริหารจัดการและการบูรณาการข้อมูลภาครัฐและการทำงานให้มีความสอดคล้องกันและเชื่อมโยงเข้าด้วยกันอย่างมั่นคง ปลอดภัย และมีธรรมาภิบาล จึงจำเป็นต้องมีกรอบแนวทางการบริหารจัดการระบบคลาวด์ภาครัฐ สนับสนุนให้หน่วยงานของรัฐสามารถพิจารณาการใช้คลาวด์เป็นหลัก เพื่อมุ่งสู่การเป็นรัฐบาลดิจิทัลต่อไป

มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ว่าด้วยทางการจำแนกประเภทข้อมูลสำหรับใช้บริการคลาวด์ตามนโยบายการใช้คลาวด์เป็นหลัก จัดทำขึ้นเพื่อให้หน่วยงานภาครัฐนำไปใช้เป็นเกณฑ์พิจารณาแนวทางการจำแนกประเภทข้อมูลสำหรับใช้บริการคลาวด์ตามนโยบายการใช้คลาวด์เป็นหลัก โดยประยุกต์แนวทางการพิจารณาจากแบบประเมินการจัดระดับชั้นข้อมูลภาครัฐ ซึ่งเป็นการประเมินความเสี่ยงจากผลกระทบของการเปิดเผยข้อมูลภาพรวมของบริการโดยไม่ได้รับอนุญาตระบุหมวดหมู่และระดับชั้นข้อมูล เพื่อสนับสนุนการนำข้อมูลเพื่อจัดเก็บในคลาวด์ภาครัฐที่มีความเหมาะสมกับประเภทข้อมูลต่อไป

สารบัญ

สารบัญภาพ

สารบัญตาราง

มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ว่าด้วยทางการจำแนกประเภทข้อมูล
สำหรับใช้บริการคลาวด์ตามนโยบายการใช้คลาวด์เป็นหลัก

1. บทนำ

1.1 ความเป็นมา

การประชุมคณะรัฐมนตรี (ครม.) เมื่อวันที่ 11 กันยายน 2566 คณะรัฐมนตรีได้แถลงนโยบาย **"Go Cloud First"** ต่อรัฐสภา โดยเมื่อวันที่ 28 พฤศจิกายน 2566 คณะรัฐมนตรีมีมติให้ให้กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เร่งขับเคลื่อนนโยบาย "Go Cloud First" ซึ่งมีแนวทางการดำเนินการที่สำคัญ 4 องค์ประกอบ ได้แก่

1. การบริหารจัดการความต้องการใช้คลาวด์ (Demand)
2. การบริหารจัดการให้มีบริการคลาวด์อย่างเพียงพอ (Supply)
3. กรอบกลไกการบริหารจัดการการใช้งานคลาวด์ของหน่วยงานภาครัฐ (กรอบกลไก Government Cloud Management)
4. การปรับปรุงระบบนิเวศการใช้บริการคลาวด์ เพื่อเชื่อมโยงฝั่งผู้ใช้บริการ (Demand) และผู้ให้บริการ (Supply)

เมื่อในวันที่ 25 มิถุนายน 2567 คณะรัฐมนตรี มีมติเห็นชอบแต่งตั้งคณะกรรมการเฉพาะด้านการขับเคลื่อนตามนโยบาย Cloud First Policy และให้คณะกรรมการพัฒนารัฐบาลดิจิทัล เป็นผู้ดำเนินการกำหนดรายละเอียดที่เกี่ยวข้องกับนโยบายการใช้คลาวด์ การดำเนินการของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ภายใต้คณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ พิจารณาเห็นชอบแนวทางทางการขับเคลื่อนตามนโยบายการใช้คลาวด์เป็นหลัก (Cloud First Policy) เมื่อวันที่ 22 ธันวาคม 2566 และในคราวการประชุม ครั้งที่ 2/2567 วันที่ 14 มิถุนายน 2567 มีมติ พิจารณาการดำเนินการตามมติคณะรัฐมนตรีเกี่ยวกับการจัดซื้อจัดจ้างหรือเช่าใช้บริการระบบคลาวด์ ให้นำข้อกำหนดมาตรฐานและเงื่อนไขสำหรับผู้ให้บริการระบบคลาวด์ไปดำเนินการ และพิจารณาเห็นชอบการแต่งตั้งคณะกรรมการเฉพาะด้านการขับเคลื่อนตามนโยบายการใช้คลาวด์เป็นหลัก

คณะกรรมการเฉพาะด้านการขับเคลื่อนตามนโยบายการใช้คลาวด์เป็นหลัก ได้กำหนดกรอบแนวทางในการบริหารจัดการคลาวด์ภาครัฐ ตามนโยบายการใช้คลาวด์เป็นหลักจำนวน 8 ข้อ และมีการแต่งตั้งคณะอนุกรรมการ 2 คณะ ประกอบด้วย

1. คณะอนุกรรมการด้านกฎหมายการจัดซื้อจัดจ้างบริการคลาวด์ภาครัฐ
2. คณะอนุกรรมการด้านบริหาร จัดการความต้องการใช้บริการคลาวด์ (Demand) การให้บริการคลาวด์ (Supply) และมาตรฐานการบริหารจัดการการบริการคลาวด์ภาครัฐ (Government Cloud Management)

ทั้งนี้กำหนดให้มี สพร. เป็นอนุกรรมการและเลขาธิการร่วม และในการประชุมเมื่อวันที่ 13 พฤศจิกายน 2567 จากกรอบแนวทางการบริหารจัดการคลาวด์ภาครัฐ 8 ข้อ มีประเด็นเกี่ยวข้องกับคณะกรรมการพัฒนารัฐบาลดิจิทัล มาตรา 4(2) ในด้านการพัฒนามาตรฐาน หลักเกณฑ์และวิธีการเกี่ยวกับระบบดิจิทัล และพัฒนาโครงสร้างพื้นฐานด้านดิจิทัลที่จำเป็น ให้เป็นไปตามมาตรฐานสากล เพื่อสร้างและพัฒนากระบวนการทำงานของหน่วยงานรัฐให้มีความสอดคล้องและมีการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างกัน รวมทั้งมีความมั่นคงปลอดภัยและน่าเชื่อถือ โดยมีการบูรณาการและสามารถทำงานร่วมกัน

อย่างเป็นเอกภาพเกิดการพัฒนาการบริการภาครัฐที่มีประสิทธิภาพและนำไปสู่การบริหารราชการและการบริการประชาชน แบบบูรณาการ รวมทั้งให้ประชาชนเข้าถึงได้โดยสะดวก และมีมติให้เสนอคณะกรรมการพัฒนารัฐบาลดิจิทัลต่อไป

คณะกรรมการพัฒนารัฐบาลดิจิทัล ได้มอบหมายให้ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) จัดทำแนวทางการจำแนกประเภทข้อมูลสำหรับใช้บริการคลาวด์ เพื่อเป็นข้อเสนอแนะให้กับหน่วยงานภาครัฐในการนำไปเป็นแนวทางการพิจารณาข้อมูลเพื่อนำไปจัดเก็บในระบบคลาวด์ ที่มีความเหมาะสมกับการให้บริการของหน่วยงาน ตามประเภทข้อมูล โดยจัดระดับชั้นข้อมูลในภาพรวมของการให้บริการ (Service) เปรียบเทียบผลกระทบและความเสี่ยงที่อาจเกิดกับข้อมูล นำไปสู่การพิจารณาประเภทของคลาวด์ที่เหมาะสมกับบริการของหน่วยงาน เพื่อให้ข้อมูลมีความมั่นคงปลอดภัยและยังเป็นการพัฒนาขีดสามารถในให้บริการแก่ประชาชนเพื่อให้เกิดการเป็นรัฐบาลดิจิทัลอย่างแท้จริง

1.2 วัตถุประสงค์

การจัดทำแนวทางการจำแนกประเภทข้อมูลสำหรับใช้บริการคลาวด์ตามนโยบายการใช้คลาวด์เป็นหลัก เพื่อเป็นข้อเสนอแนะและกรอบแนวทางให้หน่วยงานสามารถนำไปปฏิบัติใช้ให้สอดคล้องและเหมาะสมกับบริการของหน่วยงาน ตามนโยบายการใช้คลาวด์เป็นหลัก

1) เพื่อให้หน่วยงานภาครัฐ สามารถให้บริการ และทำงานร่วมกันละแบ่งปันข้อมูลระหว่างหน่วยงานภาครัฐได้อย่างมีประสิทธิภาพมากยิ่งขึ้นด้วยการเข้าถึงข้อมูลจากทุกที่และทุกเวลา

2) เพื่อเพิ่มประสิทธิภาพการรักษาความปลอดภัยและคุ้มครองข้อมูล ลดความเสี่ยงจากการถูกละเมิดหรือการเปิดเผยที่ไม่ได้รับอนุญาต รวมถึงการสูญหายของข้อมูล โดยหน่วยงานภาครัฐสามารถเลือกผู้ให้บริการคลาวด์ให้สอดคล้องกับความต้องการได้อย่างเหมาะสม

1.3 ขอบข่าย

แนวทางการจำแนกประเภทข้อมูลสำหรับใช้บริการคลาวด์ ฉบับนี้จัดทำขึ้น**เพื่อให้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO) /เจ้าของระบบงาน (System Owner) หน่วยงานนำไปใช้เป็นเกณฑ์พิจารณาแนวทางการจำแนกประเภทข้อมูลสำหรับใช้บริการคลาวด์ตามนโยบายการใช้คลาวด์เป็นหลัก** โดยประยุกต์แนวทางการพิจารณาจากแบบประเมินการระดับชั้นข้อมูลภาครัฐ ซึ่งเป็นการประเมินความเสี่ยงจากผลกระทบของการเปิดเผยข้อมูลภาพรวมของบริการโดยไม่ได้รับอนุญาตระบุหมวดหมู่และระดับชั้นข้อมูล โดยแนวทางฉบับนี้ได้จัดทำตามแนวมาตรฐานและแนวปฏิบัติที่ดีของ

1) มรด. 6 : 2566 มาตรฐานรัฐบาลดิจิทัลว่าด้วยกรอบธรรมาภิบาลข้อมูลภาครัฐ ฉบับปรับปรุง: แนวปฏิบัติ (สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน), 2566)

2) ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ (สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ, 2566)

3) ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 (สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ, 2567)

4) ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม (สำนักข่าวกรองแห่งชาติ, 2544)

5) มาตรฐาน NIST 800-60 Volume 1. and 2. : Guide for Mapping Types of Information and Information Systems to Security Categories (National Institute of Standards and Technology, 2024)

6) มาตรฐาน FIPS PUB 199 : Standards for Security Categorization of Federal Information and Information Systems (Federal Information Processing Standard Publication, 2004)

ในกรณีของข้อมูลข่าวสารลับที่สุดให้เป็นดุลพินิจของหน่วยงานตามกฎหมายเฉพาะที่เกี่ยวข้อง เช่น พระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. 2540 ระเบียบสำนักนายกรัฐมนตรีว่าด้วยงานสารบรรณ (ฉบับที่ 4) พ.ศ. 2564 และระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. 2552 (สำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ, 2540), (สำนักนายกรัฐมนตรี, 2564), (สำนักนายกรัฐมนตรี, 2552)

1.4 บทนิยาม

ข้อมูลอ่อนไหว (Sensitive Data) หมายความว่า ข้อมูลที่ต้องได้รับการป้องกันจากการเข้าถึงโดยไม่ได้รับอนุญาต เพื่อคุ้มครองความเป็นส่วนตัว (privacy) หรือความปลอดภัย (security) ของบุคคลหรือองค์กร ซึ่งหากข้อมูลอ่อนไหวมีการเปิดเผยโดยไม่ได้รับอนุญาต จะมีแนวโน้มที่จะนำไปสู่ผลที่ไม่พึงประสงค์สำหรับบุคคล หน่วยงาน องค์กร หรือ ประเทศ

การจำแนกประเภทข้อมูลสำหรับใช้บริการคลาวด์ (Cloud Data Classification) หมายความว่า การจำแนกชั้นของข้อมูลในบริบทของการใช้คลาวด์ เพื่อจัดเก็บและรักษาความปลอดภัยข้อมูลตามประเภทข้อมูล แบ่งได้เป็น ข้อมูลที่สามารถเปิดเผยได้ ข้อมูลที่ต้องได้รับความคุ้มครอง และข้อมูลที่ต้องได้รับความคุ้มครองสูงสุด ซึ่งจะช่วยกำหนดการควบคุมความปลอดภัยพื้นฐานที่เหมาะสม

ข้อมูลที่สามารถเปิดเผยได้ (Official Data) หมายความว่า ข้อมูลที่สร้าง ประมวลผล ส่ง หรือรับของหน่วยงานภาครัฐและหน่วยงานที่เกี่ยวข้อง ซึ่งอาจก่อให้เกิดความเสียหายได้ไม่เกินความเสียหายในระดับต่ำ หากมีการละเมิดความปลอดภัยจะมีการใช้มาตรฐานการควบคุมที่สามารถ**คุ้มครองข้อมูล**ให้มีความปลอดภัยจากการโจมตีในรูปแบบต่าง ๆ ซึ่งอาจเพิ่มการรับรองมาตรการควบคุมได้

ข้อมูลที่ต้องได้รับความคุ้มครอง (Protected Data) หมายความว่า ข้อมูลที่มีความอ่อนไหวสูงที่จำเป็นต้องมีมาตรการควบคุมที่เข้มงวด และมีการกำหนดการใช้เครือข่ายที่ปลอดภัยบนโครงสร้างพื้นฐานทางกายภาพที่มีความปลอดภัย และมีการปฏิบัติอย่างเหมาะสม ซึ่งเหมาะสำหรับการ**คุ้มครองข้อมูล**จากผู้ก่อภัยคุกคามซึ่งอาจส่งผลต่อชีวิต (บุคคลหรือกลุ่มบุคคล) หรือสร้างความเสียหายอย่างร้ายแรงต่อความมั่นคงของชาติ และ/หรือความสัมพันธ์ระหว่างประเทศ ความมั่นคง/เสถียรภาพทางการเงิน หรือขัดขวางความสามารถในการสืบสวนคดีอาชญากรรมที่ร้ายแรง หรือองค์กร

ข้อมูลที่ต้องได้รับความคุ้มครองสูงสุด (Highly Protected Data) หมายความว่า ข้อมูลที่มีความอ่อนไหวเป็นพิเศษ ซึ่งส่งผลต่อความมั่นคงของชาติหรือพันธมิตร และต้องการมาตรการควบคุมความปลอดภัยที่สูงมาก เพื่อป้องกันการละเมิดข้อมูลจากภัยคุกคามทั้งหมด โดยการใช้เครือข่ายบนโครงสร้างพื้นฐานทางกายภาพที่มีความปลอดภัยสูง และ**มีการคุ้มครองข้อมูล**และควบคุมความปลอดภัยอย่างเข้มงวด

ทั้งนี้ ข้อมูลข่าวสารลับที่สุดต้องปฏิบัติตามระเบียบความลับทางราชการ และ ระเบียบสารบรรณอิเล็กทรอนิกส์ โดยให้หัวหน้าหน่วยงานรัฐ ใช้ดุลพินิจในการนำข้อมูลเข้าคลาวด์โดยไม่ขัดกับกฎหมายที่เกี่ยวข้อง เช่น การสร้างผ่านคลาวด์ แต่ไม่รวมถึงขั้นตอนการเผยแพร่ (การนำส่ง)

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO) หมายความว่า ผู้มีตำแหน่งที่มีอำนาจหน้าที่ดูแลรับผิดชอบด้านเทคโนโลยีสารสนเทศในหน่วยงาน ซึ่งหมายรวมถึงการดูแลเกี่ยวกับมาตรฐาน กฎเกณฑ์ โครงสร้าง งบประมาณ กระบวนการให้ความรู้แก่บุคลากรของหน่วยงานสารสนเทศ

เจ้าของระบบงาน (System Owner) หมายความว่า ผู้ที่มีหน้าที่รับผิดชอบในการใช้งาน ดูแลและบำรุงรักษา หรือปรับปรุงระบบงานที่ใช้ในหน่วยงาน

1.5 กฎหมายและแนวทางที่เกี่ยวข้อง

1) พระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. 2540

2) ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม

3) พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 มาตรา 7 และมาตรา 8 ธรรมาภิบาลข้อมูลภาครัฐ

4) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล, 2562)

5) นโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ (พ.ศ. 2566-2570) (สำนักงานสภาความมั่นคงแห่งชาติ, 2566)

6) ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัลเรื่อง ธรรมาภิบาลข้อมูลภาครัฐ ข้อ 4 ธรรมาภิบาลข้อมูลภาครัฐในระดับหน่วยงาน (5) การจำแนกหมวดหมู่ของข้อมูล เพื่อกำหนดนโยบายข้อมูลหรือกฎเกณฑ์เกี่ยวกับผู้มีสิทธิเข้าถึงและใช้ประโยชน์จากข้อมูลต่าง ๆ ภายในหน่วยงาน สำหรับให้ผู้ซึ่งมีหน้าที่เกี่ยวข้องปฏิบัติตามนโยบายหรือกฎเกณฑ์ได้อย่างถูกต้อง และสอดคล้องตามกฎหมายที่เกี่ยวข้อง อันจะนำไปสู่การบริหารจัดการข้อมูลภาครัฐอย่างเป็นระบบ

7) ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566

8) ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567

2. แนวคิดการใช้บริการคลาวด์ตามนโยบายการใช้คลาวด์เป็นหลัก

การใช้คลาวด์ในภาครัฐของประเทศไทย เกี่ยวข้องกับความพยายามในการยกระดับประสิทธิภาพและความโปร่งใสในการให้บริการสาธารณะเป็นไปตามเป้าหมายของการพัฒนาประเทศตามยุทธศาสตร์ชาติ (ปี 2561-2580) รวมถึงยังเป็นการลดต้นทุนด้านเทคโนโลยีสารสนเทศในระยะยาว โดยหลายปีที่ผ่านมารัฐบาลไทยได้ส่งเสริมการใช้งานคลาวด์ผ่านนโยบายและแผนการพัฒนาดิจิทัลแห่งชาติ เช่น Thailand Digital Government Development Plan (ปี 2563-2565) และนโยบายไทยแลนด์ 4.0 ที่เน้นการใช้เทคโนโลยีเพื่อขับเคลื่อนการพัฒนาประเทศ ตามมติคณะรัฐมนตรี 7 พฤษภาคม 2562 ที่ให้กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม จัดให้มีโครงการคลาวด์กลางภาครัฐ (Government Data Center and Cloud Service : GDCC) แต่ยังไม่เพียงพอต่อความต้องการของทุกหน่วยงานได้ นโยบาย "Cloud First Policy" ของภาครัฐไทยจึงเกิดขึ้นเพื่อผลักดันการเปลี่ยนผ่านสู่รัฐบาลดิจิทัล โดยมุ่งเน้นการใช้ระบบคลาวด์สำหรับโครงสร้างพื้นฐาน

ด้านไอทีของหน่วยงานภาครัฐอย่างเต็มรูปแบบ แม้จะมีความท้าทาย เป้าหมายหลักคือเพิ่มประสิทธิภาพ ลดต้นทุน และสร้างมาตรฐานการให้บริการสาธารณะที่ตอบสนองความต้องการในยุคดิจิทัลอย่างแท้จริง

ระบบคลาวด์ (Cloud Computing) เป็นการให้บริการสำหรับประมวลผลข้อมูลผ่านอินเทอร์เน็ต โดยผู้ใช้บริการสามารถเข้าถึงทรัพยากรด้านเทคโนโลยีสารสนเทศ เช่น ฐานข้อมูล พื้นที่จัดเก็บข้อมูล เครือข่าย ซอฟต์แวร์ เซิร์ฟเวอร์ และเครื่องมือวิเคราะห์ โดยไม่ต้องลงทุนสร้างโครงสร้างพื้นฐานรวมไปถึงการดูแลบำรุงรักษาด้วยตนเอง โดยหน่วยงานภาครัฐยังคงสามารถให้บริการ และจัดการข้อมูลได้อย่างมีประสิทธิภาพ ปัจจุบันทั้งในภาครัฐ และภาคเอกชน ต่างมีการใช้ระบบคลาวด์เพื่อช่วยสนับสนุนการดำเนินธุรกิจหรือบริการของหน่วยงานอย่างแพร่หลาย เช่น การพัฒนาแอปพลิเคชันเพื่อจัดเก็บข้อมูลต่างๆ อาทิ ด้านการแพทย์และสาธารณสุข มีระบบจัดเก็บข้อมูลผู้ป่วยบนคลาวด์ ด้านการศึกษามีระบบการเรียนออนไลน์ (E-Learning) ผ่านแพลตฟอร์มต่างๆ Google Classroom, Microsoft Teams, และ Zoom โดยใช้ระบบคลาวด์ในการจัดเก็บข้อมูลการสอน เอกสาร และวิดีโอเพื่อการเรียนรู้และเข้าถึงข้อมูลแบบเรียลไทม์ เป็นต้น จะเห็นได้ว่าระบบคลาวด์มีประโยชน์ต่อการพัฒนาธุรกิจและบริการด้านดิจิทัล เพื่อมุ่งสู่การเป็นรัฐบาลดิจิทัลต่อไป

2.1 แนวทางการจัดระดับชั้นข้อมูลและการจำแนกประเภทข้อมูลสำหรับใช้บริการคลาวด์

การจัดระดับชั้นข้อมูลและการจำแนกประเภทข้อมูลเป็นหนึ่งในข้อเสนอแนะจากกรอบแนวทางการบริหารจัดการคลาวด์ภาครัฐ โดยแบ่งเป็น 2 ส่วนได้แก่ 1) การจัดระดับชั้นข้อมูลตามกรอบธรรมาภิบาลข้อมูลภาครัฐ เพื่อกำหนดแนวทางการบริหารจัดการข้อมูลภายในหน่วยงาน โดยพิจารณาเป็นชุดข้อมูล และ 2) การจำแนกประเภทข้อมูลบนคลาวด์ เพื่อพิจารณาประเภทข้อมูลสำหรับการเลือกใช้บริการคลาวด์ได้อย่างเหมาะสมและเกิดประโยชน์สูงสุด โดยพิจารณาเป็นรายบริการ (Service) ซึ่งในรายบริการอาจประกอบด้วยหลายชุดข้อมูล

ทั้งนี้ การจัดระดับชั้นข้อมูลและการจำแนกประเภทข้อมูลจะเป็นเครื่องมือที่ช่วยกลั่นกรองระดับชั้นข้อมูลเบื้องต้น เพื่อนำไปสู่การพิจารณาการจำแนกประเภทข้อมูลสำหรับใช้บริการคลาวด์ โดยคำนึงถึงผลกระทบภาพรวมที่อาจมีโอกาสเกิดขึ้น ลดความเสี่ยงต่อการให้บริการของหน่วยงานภาครัฐ ดังนั้นการจำแนกประเภทข้อมูลในระบบคลาวด์ที่ถูกต้อง จะส่งผลให้หน่วยงานภาครัฐสามารถเลือกใช้บริการคลาวด์ได้อย่างเหมาะสมและเกิดประโยชน์สูงสุดจากการใช้คลาวด์เป็นหลัก ซึ่งหน่วยงานจะได้ประโยชน์จากการใช้บริการคลาวด์สรุปได้ดังนี้

1) ด้านค่าใช้จ่าย ช่วยลดค่าใช้จ่ายของหน่วยงาน โดยลดการลงทุนในซอฟต์แวร์และฮาร์ดแวร์ที่มีราคาแพง ทำให้ลดค่าใช้จ่ายในระบบเทคโนโลยีสารสนเทศ เพราะทุกอย่างถูกให้บริการผ่านอินเทอร์เน็ต มีรูปแบบการชำระค่าใช้บริการแบบจ่ายตามปริมาณการใช้งานจริง (Pay-as-you-go หรือ Pay-per-use) หน่วยงานสามารถจ่ายตามการใช้งานจริงได้พร้อมทั้งลดต้นทุนทางธุรกรรม (Transaction Cost) เพื่อแลกเปลี่ยน เข้าถึง รักษา และประมวลผลข้อมูลรวมทั้งมีความยืดหยุ่นในการปรับเปลี่ยนทรัพยากรตามช่วงเวลา

2) ด้านความยืดหยุ่นและการเปลี่ยนแปลง ด้วยการเพิ่มหรือลดทรัพยากรได้สะดวก สามารถปรับขนาดของทรัพยากรคอมพิวเตอร์ตามความต้องการของหน่วยงานได้โดยง่าย เพื่อตอบสนองต่อการเพิ่มหรือลดปริมาณการใช้งาน การพัฒนา และการปรับปรุงอย่างต่อเนื่อง มีความยืดหยุ่นในการปรับแต่งซอฟต์แวร์และการเพิ่มเติมทรัพยากร (Upgrade) เพื่อให้มีประสิทธิภาพที่สูงขึ้น และสามารถรักษาเสถียรภาพของบริการ

3) ด้านการความเข้าถึงและการใช้ประโยชน์จากข้อมูล สามารถเข้าดึงข้อมูลไปใช้ประโยชน์ต่อได้ง่ายขึ้นจากระบบคลาวด์ได้ทุกที่ทุกเวลาที่มีการเชื่อมต่ออินเทอร์เน็ต และผู้ใช้งานสามารถเข้าถึงทรัพยากรพร้อมกันเพื่อการทำงานร่วมกันได้อย่างเป็นปัจจุบันตามเวลาจริง (Real-time Collaboration) และช่วยให้สามารถสร้างระบบนิเวศข้อมูล และส่งเสริมการใช้ข้อมูลให้เกิดประโยชน์สูงสุด ทั้งจากภาครัฐ เอกชน และประชาชน รวมไปถึงการแบ่งปันข้อมูล (Data Sharing) การใช้งานระบบคลาวด์เป็นหลัก เป็นปัจจัยผลักดันให้มีการจัดเก็บข้อมูลในรูปแบบคอมพิวเตอร์อ่านได้ (Machine-readable) และสามารถเชื่อมโยงข้อมูลจากหลายฐานข้อมูลเข้าไว้ด้วยกัน ทำให้เกิดการแลกเปลี่ยนข้อมูลสองทิศทาง ที่ทำให้การเกิดการแลกเปลี่ยนข้อมูลได้ง่ายขึ้น ลดอุปสรรคในการเข้าถึงข้อมูลระหว่างหน่วยงาน และข้อมูลมีการอัปเดตแบบเรียลไทม์ (Realtime) ซึ่งจะเพิ่มความสามารถในการแข่งขัน และส่งเสริมการวางแผนโยบายภาครัฐ

4) ด้านความปลอดภัยของข้อมูล โดยผู้ใช้งานสามารถใช้ระบบการสำรองข้อมูลที่เชื่อถือได้ ทำให้ข้อมูลมูลปลอดภัยจากความเสี่ยงต่างๆ รวมถึงมีบริการตรวจสอบและรักษาความปลอดภัย ซึ่งผู้ใช้งานได้รับการแบ่งเบาภาระด้านการออกแบบและจัดทำระบบที่ปลอดภัยได้ส่วนหนึ่ง

5) ด้านการส่งเสริมนวัตกรรม ในการพัฒนาแอปพลิเคชันในรูปแบบการบริการซอฟต์แวร์ (SaaS) ช่วยส่งเสริมนวัตกรรมและการพัฒนาโซลูชันใหม่ ๆ ที่ให้บริการผ่านอินเทอร์เน็ต ประกอบกับการให้บริการ API (Application Programming Interface) ทำให้นักพัฒนาสามารถสร้างและปรับแต่งแอปพลิเคชันเพื่อใช้งานกับระบบคลาวด์ได้ อีกทั้งมีบริการที่อัปเดตอยู่เสมอ โดยผู้ให้บริการคลาวด์รับผิดชอบอัปเดตซอฟต์แวร์ให้เสมอ ทำให้สามารถนำเสนอความสามารถและฟีเจอร์ใหม่ๆ เพื่อตอบสนองต่อความต้องการของผู้ใช้งาน

ที่มา : (บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน), 2021) (Microsoft, ม.ป.ป.) (Amazon, n.d.)

2.2 ความสำคัญของระบบคลาวด์ต่อหน่วยงานภาครัฐ

การขับเคลื่อนตามนโยบายการใช้คลาวด์เป็นหลัก “Cloud First Policy”เพื่อมุ่งไปสู่การเป็นรัฐบาลดิจิทัลอย่างมีประสิทธิผลนั้น นอกจากเป็นการเปลี่ยนรูปแบบการใช้จ่ายงบประมาณ จากแบบลงทุน เป็นค่าใช้จ่ายในการดำเนินงาน เพื่อให้ครอบคลุมเฉพาะบริการที่ใช้งานแล้วนั้น ยังส่งผลในอีกหลากหลายมิติด้วยกัน การให้บริการที่มีความยืดหยุ่นมากขึ้นในการทดลองใช้บริการใหม่หรือทำการเปลี่ยนแปลงด้วยต้นทุนลดลง มีความปลอดภัยมากขึ้นเนื่องจากผู้ให้บริการจะปรับปรุงเทคโนโลยีและความปลอดภัยเป็นประจำ เพิ่มศักยภาพลดระยะเวลาในการประมวลผลข้อมูลขนาดใหญ่ และลดต้นทุนโดยรวมด้วยการใช้รูปแบบการกำหนดราคาที่ปรับขนาดได้ตามความเหมาะสมของบริบทบริการ

เป้าหมายการใช้บริการคลาวด์ของหน่วยงานภาครัฐนั้น ตั้งอยู่บนพื้นฐานของการพัฒนาความสามารถ ของหน่วยงานรัฐในการให้บริการสาธารณะต่อภาคประชาชนที่มีประสิทธิภาพมากขึ้น โดยมีค่าใช้จ่ายที่ลดลง และลดการลงทุนและใช้งานซ้ำซ้อนของระบบสารสนเทศ อีกทั้งส่งเสริมความร่วมมือระหว่างหน่วยงานในการใช้ และแลกเปลี่ยนข้อมูลอย่างมีประสิทธิภาพและปลอดภัย

กรณีศึกษานโยบายระบบคลาวด์ภาครัฐ จากต่างประเทศ

1. สหราชอาณาจักร (United Kingdom)

นโยบาย “Cloud-First Policy” เป็นแนวทางที่กำหนดให้ภาครัฐใช้ Public Cloud เป็นตัวเลือกแรก แต่หน่วยงานสามารถเลือกใช้ตัวเลือกอื่นได้โดยต้องแสดงให้เห็นได้ว่ามีความคุ้มค่ากว่า โดยเริ่มประกาศใช้นโยบายตั้งแต่ปี พ.ศ. 2556 ซึ่งมีเป้าหมายเพื่อส่งเสริมการใช้งานคลาวด์ในภาครัฐ ให้มีประสิทธิภาพ ลดต้นทุน และส่งเสริมนวัตกรรม สหราชอาณาจักรได้มีการจำแนกประเภทข้อมูล (Data Classification) เป็น 3 ระดับ ได้แก่ Official, Secret และ Top Secret เพื่อให้ตัดสินใจเลือกประเภทของการใช้บริการคลาวด์ได้ง่าย จากกรณีศึกษา 3-Tiers Model ของสหราชอาณาจักรข้างต้น พบว่ากว่า 90% ของข้อมูลภาครัฐ เช่น ทะเบียน

ราษฎร์ และข้อมูลอื่น ๆ ซึ่งเป็นข้อมูลส่วนบุคคลของประชาชน จะถูกจัดอยู่ใน Public Cloud ได้ทั้งหมด ซึ่งไม่จำเป็นต้องอยู่ภายในประเทศเท่านั้น ยังสามารถอยู่ที่ไหนก็ได้ โดยที่ผู้ให้บริการคลาวด์ (Cloud Service Provider) นั้น ๆ จะต้องได้รับการรับรองมาตรฐาน และปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล (GDPR) มีเพียงข้อมูลระดับสูงเท่านั้น ที่สามารถจัดเก็บอยู่ในศูนย์ข้อมูล (Data Center) ภาครัฐได้ โดยการจำแนกประเภทข้อมูลถูกออกแบบมาเพื่อให้ข้อมูลของรัฐบาลถูกจัดการตามความอ่อนไหวและความปลอดภัยที่เหมาะสม โดยยกระดับความปลอดภัยตามความเสี่ยงและผลกระทบจากการรั่วไหล พร้อมสนับสนุนด้วยมาตรฐานและเทคโนโลยีที่ทันสมัย เช่น แนวทางของ National Cyber Security Centre (NCSC) เพื่อปกป้องข้อมูลในทุกระดับ

ตารางที่ 1: หลักการสำคัญของนโยบายของสหราชอาณาจักร

 **หลักการสำคัญของนโยบาย**	
1. การให้ความสำคัญกับโซลูชันคลาวด์	หน่วยงานรัฐต้องพิจารณาใช้ระบบคลาวด์ 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 2: การจำแนกประเภทข้อมูลและตัวอย่างการใช้งานของสหราชอาณาจักร

ประเภทข้อมูล	ลักษณะ	ตัวอย่างการใช้งานในภาครัฐ	มาตรการรักษาความปลอดภัย	การใช้ประเภทคลาวด์
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	ใช้ Public Cloud เช่น AWS, Azure ที่ผ่านการรับรอง

ประเภทข้อมูล	ลักษณะ	ตัวอย่างการใช้งานในภาครัฐ	มาตรการรักษาความปลอดภัย	การใช้ประเภทคลาวด์
Secret	- เป็นข้อมูลที่หากรั่วไหลอาจก่อให้เกิดความเสียหายร้ายแรงต่อความมั่นคงหรือความปลอดภัยของประเทศ - ใช้ในหน่วยงานหรือองค์กรที่เกี่ยวข้องกับความมั่นคง หรือการบริหารงานเชิงยุทธศาสตร์	- ข้อมูลด้านการป้องกันประเทศ เช่น แผนการเคลื่อนกำลังทหาร - แผนการจัดการภัยพิบัติ หรือข้อมูลบัญชีบุคคลสำคัญ	- ใช้ระบบคลาวด์แบบ Private Cloud หรือ Hybrid Cloud - มีการตรวจสอบสิทธิ์หลายชั้น (Multi-Factor Authentication) - เซิร์ฟเวอร์และข้อมูลอยู่ภายใต้การควบคุมทางกายภาพที่เข้มงวด เช่น ศูนย์ข้อมูลที่มีระบบป้องกันการบุกรุก	ใช้ Private Cloud ภายในประเทศ
Top Secret	- เป็นข้อมูลที่อ่อนไหวที่สุด หากรั่วไหลจะส่งผลเสียหายอย่างร้ายแรงและกว้างขวางต่อประเทศ เช่น ความมั่นคงของชาติหรือชีวิตของประชาชน - ต้องการมาตรการป้องกันที่เข้มงวดที่สุด	- รายละเอียดการดำเนินการด้านความมั่นคง เช่น แผนปฏิบัติการต่อต้านการก่อการร้าย - การสื่อสารระหว่างนายกรัฐมนตรีกับหน่วยข่าวกรอง - ข้อมูลเชิงยุทธศาสตร์ของประเทศหรือข้อมูลที่ส่งผลต่อพันธมิตรระดับนานาชาติ - ข้อมูลของบุคลากรในหน่วยข่าวกรอง	- ใช้ระบบที่มีการแยกเครือข่าย (Air-Gapped Networks) เพื่อป้องกันการเชื่อมต่อกับอินเทอร์เน็ต - ศูนย์ข้อมูลที่มีการป้องกันพิเศษ เช่น ระบบล็อคชีวภาพ (Biometric Lock) - การควบคุมการเข้าถึงที่เข้มงวดที่สุดและการตรวจสอบอย่างต่อเนื่อง	ใช้เครือข่ายแยกเฉพาะ เช่น Secure Isolated Networks

ที่มา : (GOV.UK, n.d.)

2. สหรัฐอเมริกา (United States)

กลยุทธ์การประมวลผลแบบคลาวด์ของรัฐบาลกลางสหรัฐฯ (Federal Cloud Computing Strategy) หรือที่รู้จักกันในชื่อ Cloud Smart ถูกจัดทำโดย Chief Information Officers Council (CIO Council) เป็นนโยบายที่ต่อยอดจากนโยบาย "Cloud First" ซึ่งเริ่มต้น ในปี พ.ศ. 2544 วัตถุประสงค์สำคัญ เพื่อชี้แจงหน่วยงานภาครัฐให้เข้าใจถึงประโยชน์การใช้ระบบคลาวด์ จัดเตรียมกรอบการตัดสินใจและกรณีตัวอย่างเพื่อสนับสนุนหน่วยงานภาครัฐในการย้ายข้อมูลสารสนเทศไปสู่ระบบคลาวด์ เน้นแหล่งทรัพยากรการใช้งานระบบคลาวด์ และการกำหนดบทบาทและความรับผิดชอบในการนำมาระบบคลาวด์มาใช้งานของรัฐบาลกลางสหรัฐอเมริกา โดย Cloud Smart เน้นการทำแนวทางเพื่อไปใช้ในภารกิจภาครัฐ 3 เรื่อง ได้แก่ ความปลอดภัย (Cyber Security) การจัดซื้อ (Procurement) เช่น มีอำนาจการจัดหาให้ถูกลง (Bulk PurchasingPower), วิธีป้องกันการผู้ขาดผู้ให้บริการ (Avoid Vendor Lock-in) และ Workflow การทำงานของการสร้างบริการดิจิทัล นอกจากนี้ สถาบันมาตรฐานและเทคโลยีแห่งชาติของรัฐบาลสหรัฐอเมริกาได้แบ่งรูปแบบการใช้งาน

คลาวด์คอมพิวติ้งมี 4 รูปแบบ ได้แก่ คลาวด์ส่วนตัว (private cloud) คลาวด์ชุมชน (community cloud) และคลาวด์สาธารณะ (public cloud) และคลาวด์ผสม (hybrid cloud)

ตารางที่ 3: หลักการสำคัญของ Cloud Smart ของสหรัฐอเมริกา

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

ที่มา : (Cloud.cio.gov, n.d.)

ตารางที่ 4: การจำแนกประเภทข้อมูลและตัวอย่างการใช้งานของสหรัฐอเมริกา

ประเภทข้อมูล	ลักษณะ	ตัวอย่างการใช้งานในภาครัฐ	มาตรการรักษาความปลอดภัย	การใช้ประเภทคลาวด์
Low-Impact	ข้อมูลสาธารณะที่ไม่มีความอ่อนไหว หากเกิดการละเมิดจะมีผลกระทบต่ำต่อองค์กรหรือบุคคล	- เว็บไซต์ NASA สำหรับเผยแพร่ภาพจากกล้องโทรทรรศน์ Hubble เช่น ภาพจักรวาล (Hubble Space Telescope) - ข้อมูลจากกระทรวงการศึกษาเกี่ยวกับโครงการทุนการศึกษา	- ใช้ HTTPS เพื่อป้องกันการดักจับข้อมูล - ระบบรหัสผ่านสำหรับการแก้ไขเนื้อหา	Public Cloud (เช่น AWS, GCP)
Moderate-Impact	ข้อมูลที่เกี่ยวข้องกับความเป็นส่วนตัวหรือมีความอ่อนไหวปานกลาง หากละเมิดอาจกระทบต่อหน่วยงานและประชาชน	- ระบบ Medicaid US Department of Health and Human Services (HHS) สำหรับการจัดการข้อมูลผู้ป่วย - ระบบสนับสนุนข้อมูลผู้สมัคร Social Security	- เข้ารหัสข้อมูล (Encryption) ทั้งในขณะส่งและจัดเก็บ - ใช้ระบบ Audit Trail - ใช้ Identity and Access Management (IAM) เพื่อควบคุมสิทธิ์การเข้าถึง	Hybrid/Community Cloud
High-Impact	ข้อมูลลับที่เกี่ยวข้องกับความมั่นคงของชาติหรือผลกระทบต่อเศรษฐกิจอย่างร้ายแรง หากเกิดการละเมิด ซึ่งต้องการมาตรการความปลอดภัย	- การจัดการข้อมูลข่าวกรองระดับสูงของ CIA - ระบบสนับสนุนการปฏิบัติการของกระทรวงกลาโหมสหรัฐฯ	- ใช้ Virtual Private Network (VPN) - Multi-Factor Authentication (MFA) - การตรวจสอบช่องโหว่	Private Cloud หรือ On-Premise

ประเภทข้อมูล	ลักษณะ	ตัวอย่างการใช้งานในภาครัฐ	มาตรการรักษาความปลอดภัย	การใช้ประเภทคลาวด์
	และการควบคุมการเข้าถึงอย่างเข้มงวด		(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 (Australian)

นโยบาย Cloud First ของรัฐบาลออสเตรเลียมีจุดมุ่งหมายในการเพิ่มประสิทธิภาพพัฒนาการให้บริการและลดต้นทุนด้านเทคโนโลยีสารสนเทศและการสื่อสารภาครัฐ โดยการส่งเสริมให้หน่วยงานรัฐบาลใช้บริการคลาวด์สาธารณะ โดยคำนึงถึงความปลอดภัยและความคุ้มค่าในการลงทุน เน้นการปรับปรุงการให้บริการของรัฐบาลและลดการใช้ทรัพยากรที่ซ้ำซ้อน โดยทำการประเมินการให้บริการ คลาวด์ส่วนตัว คลาวด์ชุมชน คลาวด์สาธารณะ หรือคลาวด์ผสม นอนจากนี้รัฐบาลออสเตรเลียได้ประกาศนโยบายคลาวด์เพื่อสนับสนุนให้กิจการทั้งหน่วยงานภาครัฐและองค์กรภาคเอกชนใช้ระบบคลาวด์เพิ่มมากขึ้น ภายใต้กรอบนโยบายการรักษาความปลอดภัยของรัฐบาลออสเตรเลียมีการแบ่งระดับของข้อมูลที่จัดประเภทความปลอดภัย (Security Classified Information) มี 4 ระดับ เพื่อประเมินความอ่อนไหวและความเสี่ยงที่อาจเกิดขึ้นจากการละเมิดข้อมูลหรือการจัดการที่ไม่เหมาะสม โดยแต่ละระดับสะท้อนถึงความเสียหายที่อาจเกิดขึ้นต่อผลประโยชน์ของชาติ หน่วยงานหรือบุคคล อันได้แก่ UnClassified ,Protect, Secret, และ Top Secret โดย ข้อกำหนดหลักที่หน่วยงานต้องดำเนินการดังนี้

1) ระบุข้อมูลที่ถือครอง (Identify information holdings):ทำการระบุข้อมูลทั้งหมดที่หน่วยงานถือครอง เพื่อให้เข้าใจถึงลักษณะและขอบเขตของข้อมูลที่ต้องการการปกป้อง

2) ประเมินการจัดประเภทความปลอดภัยของข้อมูล (Assess the security classification of information holdings):ทำการประเมินเพื่อกำหนดระดับความปลอดภัยที่เหมาะสมกับข้อมูล โดยพิจารณาความสำคัญ มูลค่า และความอ่อนไหวของข้อมูลนั้น

3) ดำเนินมาตรการควบคุมการปฏิบัติงาน (Implement operational controls): นำมาตรการควบคุมที่เหมาะสมมาใช้ในการจัดการข้อมูล โดยพิจารณาความสำคัญ มูลค่า และความอ่อนไหวของข้อมูล เพื่อให้การปกป้องข้อมูลสอดคล้องกับความเสี่ยงที่อาจเกิดขึ้น

ตารางที่ 5: หลักการและแนวคิดหลักของนโยบายของออสเตรเลีย

	**หลักการและแนวคิดหลักของนโยบาย**
1. Cloud First Policy	รัฐบาลออสเตรเลียกำหนดให้หน่วยงานภาครัฐต้องพิจารณาการใช้บริการคลาวด์เป็นลำดับแรกหากบริการนั้นเหมาะสมและสามารถคุ้มครองข้อมูลได้อย่างมีประสิทธิภาพ โดยมีเงื่อนไขว่าบริการคลาวด์จะต้องมีการรักษาความปลอดภัยที่เพียงพอและสามารถให้มูลค่าทางการเงินที่ดี
2. การยกระดับการใช้บริการคลาวด์	รัฐบาลมีนโยบายในการใช้บริการคลาวด์เพื่อให้หน่วยงานต่างๆ สามารถลดค่าใช้จ่ายและใช้ทรัพยากรอย่างมีประสิทธิภาพ ใน

	หลักการและแนวคิดหลักของนโยบาย
	ขณะเดียวกันก็ต้องมั่นใจว่ามีมาตรการรักษาความปลอดภัยที่เพียงพอในการจัดการข้อมูลที่สำคัญ
3. ความปลอดภัยและการปฏิบัติตามกฎหมาย	มีการกำหนดมาตรการรักษาความปลอดภัยสำหรับข้อมูลรัฐบาล โดยการใช้ผู้ให้บริการคลาวด์ที่ได้รับการรับรองมาตรฐานและปฏิบัติตามกฎหมาย เช่น Australian Government Information Security Manual (ISM) ซึ่งเป็นมาตรฐานการรักษาความปลอดภัยที่สำคัญ

ตารางที่ 6: การจำแนกประเภทข้อมูลและตัวอย่างการใช้งานของออสเตรเลีย

ประเภทข้อมูล	ลักษณะ	ตัวอย่างการใช้งานในภาครัฐ	มาตรการรักษาความปลอดภัย	การใช้ประเภทคลาวด์
Unclassified (Unofficial , Official)	ข้อมูลทั่วไปที่ไม่ต้องการการจัดประเภทความปลอดภัย แต่ยังคงต้องการการจัดการรอบคอบ	- อีเมลภายใน - แนวทางการดำเนินงานทั่วไป	- ควบคุมการเข้าถึงข้อมูลที่มีการแชร์ทั่วไป - จัดการเอกสารด้วยรหัสผ่านขั้นพื้นฐาน	- Public Cloud - Private Cloud - Hybird Cloud
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)**

ในช่วงปลายปี 2561 รัฐบาลสิงค์โปร์ได้ประกาศแผน 5 ปีในการย้ายระบบเทคโนโลยีสารสนเทศ (IT) ส่วนใหญ่จากโครงสร้างพื้นฐานภายในองค์กรไปยังคลาวด์เชิงพาณิชย์เพื่อเร่งความเร็วในการให้บริการและปรับปรุงคุณภาพบริการสำหรับประชาชนและธุรกิจ GovTech เปิดตัวแพลตฟอร์มที่ช่วยให้หน่วยงานภาครัฐสามารถนำคลาวด์มาใช้ได้อย่างรวดเร็วและไม่ยุ่งยาก คือ Government Commercial Cloud (GCC) ของสิงคโปร์ ใช้ระบบการจำแนกข้อมูลแบบชั้น (Tiered Data Classification) เพื่อกำหนดมาตรการควบคุมตาม

ความสำคัญและความอ่อนไหวของข้อมูลในแต่ละระดับ ซึ่งเป็นส่วนสำคัญของกลยุทธ์การใช้คลาวด์ที่รัฐบาลสิงคโปร์นำมาใช้ โดยมุ่งเน้นให้หน่วยงานภาครัฐสามารถใช้บริการคลาวด์จากผู้ให้บริการเชิงพาณิชย์ได้อย่างปลอดภัย ลดต้นทุนและเพิ่มความคล่องตัวในการให้บริการด้านดิจิทัล ปัจจุบันมีระบบภาครัฐมากกว่า 70% อยู่ใน GCC ทั้งนี้มาตรการควบคุมถูกปรับให้สอดคล้องกับระดับความสำคัญและผลกระทบของข้อมูลตามนโยบายความปลอดภัยไซเบอร์ของรัฐบาลสิงคโปร์ และการเลือกใช้คลาวด์สำหรับข้อมูลต่างระดับ ใน GCC Singapore จะขึ้นอยู่กับความสำคัญ ความอ่อนไหว และผลกระทบของข้อมูลในกรณีที่เกิดการรั่วไหล ตัวอย่างบริการภาครัฐที่สำคัญใน GCC ได้แก่ MyCareersFuture, GoBusiness และ WOGAA [12] ที่มา: (Government Technology Agency (GovTech))

ตารางที่ 7: 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 เพื่อเสริมสร้างบริการดิจิทัลที่มีประสิทธิภาพโดยไม่ต้องพัฒนาจากพื้นฐาน
4. ความคล่องตัวและประสิทธิภาพด้านต้นทุน	แพลตฟอร์ม GCC สนับสนุนการปรับปรุงกระบวนการดิจิทัลของรัฐบาลให้มีความคล่องตัวและลดต้นทุนผ่านการใช้เทคโนโลยีคลาวด์

ที่มา : (Government Technology Agency (GovTech)) (Singapore Government Developer Portal, n.d.)

ตารางที่ 8: การจำแนกประเภทข้อมูลและตัวอย่างการใช้งานของสิงคโปร์

ประเภทข้อมูล	ลักษณะ	ตัวอย่างการใช้งานในภาครัฐ	มาตรการรักษาความปลอดภัย	การใช้ประเภทคลาวด์
Public Data	ข้อมูลที่สามารถเผยแพร่สู่สาธารณะโดยไม่มีความกังวลเกี่ยวกับความลับ	- เว็บไซต์บริการประชาชน - รายงานผลการดำเนินงานของหน่วยงาน	- ตรวจสอบความสมบูรณ์ของเว็บไซต์ ใช้ HTTPS ในการเชื่อมต่อ - ใช้ระบบตรวจสอบป้องกันการดัดแปลงข้อมูล - ระบบการเข้าถึงแบบปลอดภัย - การตรวจสอบข้อมูลก่อนเผยแพร่	Public Data
Restricted Data	ข้อมูลที่อาจก่อให้เกิดความเสียหายเล็กน้อยหากเปิดเผยโดยไม่ได้รับอนุญาต	- บันทึกการประชุมของหน่วยงาน - ข้อมูลการปฏิบัติงาน	- การควบคุมสิทธิ์การเข้าถึง (Role-Based Access) - การเข้ารหัสข้อมูล (AES-	Private Cloud หรือ Hybrid Cloud

ประเภทข้อมูล	ลักษณะ	ตัวอย่างการใช้งานในภาครัฐ	มาตรการรักษาความปลอดภัย	การใช้ประเภทคลาวด์
		ภายใน เช่น แผนงานโครงการภาครัฐ	256) - การเข้ารหัสข้อมูลในระหว่างการส่งและจัดเก็บ - ใช้ Role-Based Access Control (RBAC) - การตรวจสอบการเข้าถึงระบบเป็นประจำ	
Confidential Data	ข้อมูลที่ต้องการความปลอดภัยสูง เพื่อป้องกันความเสี่ยงที่สำคัญ	- ข้อมูลส่วนบุคคล (PII) การจัดเก็บข้อมูลส่วนบุคคลของประชาชน เช่น หมายเลขบัตรประชาชน หรือข้อมูลทางการแพทย์ - ข้อมูลเกี่ยวกับสัญญาการจัดซื้อจัดจ้างของภาครัฐ และเอกสารทางการเงิน	การเข้ารหัสขั้นสูง (Advanced Encryption) - ยืนยันตัวตนแบบหลายปัจจัย (MFA) - ข้อมูลเข้ารหัสทั้งขณะส่งและขณะเก็บ - การเก็บบันทึกและตรวจสอบการเข้าถึง	Private Cloud หรือ Highly Secure Hybrid Cloud
Secret/National Security Data	ข้อมูลที่หากเปิดเผยจะส่งผลกระทบต่อความมั่นคงแห่งชาติหรือสวัสดิภาพของประชาชน	- ข้อมูลด้านความมั่นคง เช่น การเฝ้าระวังภัยไซเบอร์หรือข้อมูลข่าวกรองทางการทหาร - แผนปฏิบัติการทางการทหาร เช่น การออกแบบระบบป้องกันประเทศ	- การแยกข้อมูลออกจากระบบเชิงพาณิชย์ (Data Isolation) - โครงสร้างพื้นฐานที่ปลอดภัยสูง ใช้ระบบเฝ้าระวังภัยคุกคามแบบเรียลไทม์ - ระบบการควบคุมทางกายภาพ เช่น ใช้การสแกนไบโอเมตริกซ์ (ลายนิ้วมือ/ใบหน้า) เพื่อเข้าถึงเซิร์ฟเวอร์	Government Cloud หรือ On-Premises Infrastructure

จากกรณีศึกษานโยบายระบบคลาวด์ภาครัฐของต่างประเทศ พบว่าแนวทางทุกประเทศมีการจำแนกประเภทข้อมูลสำหรับใช้บริการคลาวด์ออกเป็น 3 กลุ่มใหญ่ๆ ได้แก่ ข้อมูลที่เปิดเผยได้ ข้อมูลที่ต้องได้รับการคุ้มครอง และ ข้อมูลลับที่สุด โดยข้อมูลทุกประเภทสามารถนำขึ้นระบบคลาวด์ได้ โดยต้องมีมาตรการควบคุมความปลอดภัย ส่วนใหญ่พบว่าในกรณีข้อมูลที่ต้องได้รับการคุ้มครอง หรือข้อมูลที่เกี่ยวข้องกับความเป็นส่วนตัว หรือมีความอ่อนไหวปานกลาง หากละเมิดอาจกระทบต่อหน่วยงานและประชาชน หรือข้อมูลในระดับชั้นลับจะเลือกใช้คลาวด์สาธารณะ และคลาวด์ผสมโดยมีมาตรการรักษาความปลอดภัยของแต่ละประเทศโดยเฉพาะ เช่น การกำหนดและควบคุมสิทธิ์การเข้าถึง การเข้ารหัสข้อมูล เป็นต้น การเลือกใช้คลาวด์ส่วนตัว โดยแต่ละประเทศเลือกใช้กับข้อมูลในระดับชั้นลับขึ้นไป เช่นในประเทศอังกฤษ ข้อมูลที่อยู่ในระดับชั้นลับจะมีการใช้คลาวด์ส่วนตัว และข้อมูลในระดับชั้นลับที่สุด มีการใช้เครือข่ายแยกเฉพาะ เช่น Secure Isolated Networks

ซึ่งเป็นมาตรการด้านความปลอดภัยที่เข้มงวดเพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต มีการควบคุมการเข้าถึงที่เข้มงวดที่สุดและมีการตรวจสอบอย่างต่อเนื่อง ในขณะที่ประเทศออสเตรเลียมีการใช้เครือข่ายแยกเฉพาะ ในระดับชั้นข้อมูลลับกับบริการที่อาจส่งผลต่อความสัมพันธ์ระหว่างประเทศ สำหรับประเทศสิงคโปร์มีการใช้ Government Cloud หรือ On-Premises Infrastructure สำหรับกลุ่มข้อมูลลับที่สุด

ดังนั้นการเตรียมความพร้อมและแนวทางการบริหารจัดการข้อมูลในการใช้งานระบบประมวลผลแบบคลาวด์ เป็นเรื่องสำคัญที่องค์กรต้องพิจารณาในการเคลื่อนย้ายข้อมูลขององค์กรเข้าสู่ระบบการประมวลผลแบบคลาวด์ เพื่อให้เกิดประสิทธิภาพและประสิทธิผลต่อองค์กรมากที่สุด ภายใต้ความมั่นคงปลอดภัยและเป็นส่วนตัวของข้อมูลด้วยการจัดระดับชั้นข้อมูลซึ่งเป็น 1 ใน ขั้นตอนที่มีความสำคัญของการเตรียมองค์กรเข้าสู่การประมวลผลข้อมูลแบบคลาวด์ ซึ่งเป็นไปตามการจัดทำธรรมาภิบาลข้อมูลภาครัฐ ดังแสดงดังภาพ

ภาพที่ 1: ขั้นตอนในการเตรียมองค์กรเข้าสู่การประมวลผลข้อมูลแบบคลาวด์ (Prinya.org, 2022)

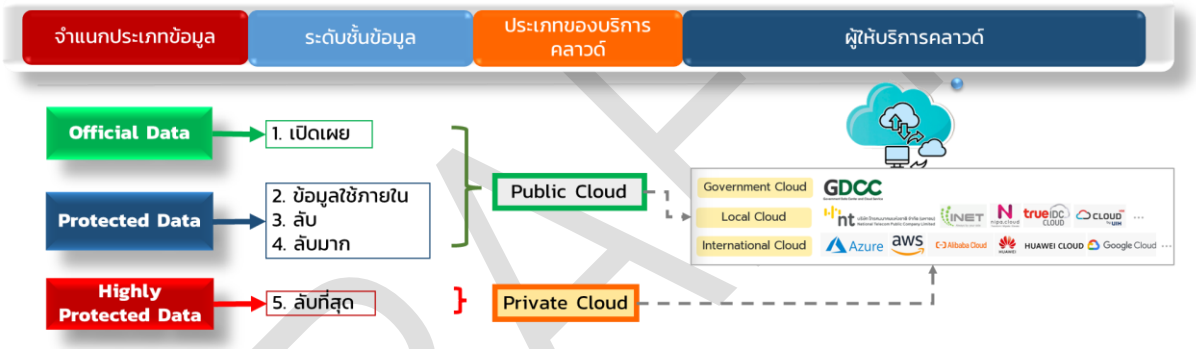
สำหรับ **ประเทศไทย** มีหลักการและแนวคิดที่ช่วยให้หน่วยงานภาครัฐสามารถพิจารณาการจัดหมวดหมู่ข้อมูลให้เป็นไปตามกรอบธรรมาภิบาลข้อมูลภาครัฐ (DGF) ได้แก่ ข้อมูลสาธารณะ ข้อมูลใช้ภายใน ข้อมูลส่วนบุคคล ข้อมูลความลับทางราชการ และข้อมูลความมั่นคง โดยพิจารณาการจัดระดับชั้นข้อมูลภาครัฐที่มีความอ่อนไหวให้สอดคล้องตามแนวมาตรฐานสากลและเป็นไปตามข้อกฎหมายที่เกี่ยวข้อง โดยการจัดระดับชั้นข้อมูลเพื่อบริหารจัดการข้อมูลภายในหน่วยงานแบ่งออกเป็น 5 ระดับ ได้แก่ ชั้นเปิดเผย (Open) สู่สาธารณะ เปิดเผยเมื่อได้รับอนุญาต ได้แก่ ชั้นเผยแพร่ภายในองค์กร (Private) ชั้นลับ (Confidential) และ ชั้นลับมาก (Secret) และเปิดเผยไม่ได้/ปกปิด ได้แก่ ชั้นลับที่สุด (Top Secret) (สำนักงานพัฒนารัฐบาลดิทัล (องค์การมหาชน), 2565) ทั้งนี้สอดคล้องตามกฎหมายและมาตรฐานที่เกี่ยวข้อง ดังแสดงตามภาพที่ 2

Data Class. Level / Data Category	เปิดเผย (Open)	เผยแพร่ภายในองค์กร (Private)	ลับ (Confidential / sensitive)	ลับมาก (Secret / Medium Sensitive)	ลับที่สุด (Top secret / Highly Sensitive)
ข้อมูลสาธารณะ	▪ พ.ร.บ. ข้อมูลข่าวสารของทางราชการ 2540 (มาตรา 7 และมาตรา 9) ▪ มาตรฐานและหลักเกณฑ์การเปิดเผยข้อมูลภาครัฐ				
ข้อมูลใช้ภายใน		ISO 27001: 2013			
ข้อมูลส่วนบุคคล			พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล 2562 (มาตรา 24 – มาตรา 27)		
ข้อมูลข่าวสารลับ			พ.ร.บ. ข้อมูลข่าวสารของทางราชการ 2540 (มาตรา 9 และมาตรา 15 ที่เปิดเผยได้) ระเบียบว่าด้วยการรักษาความลับของทางราชการ 2544		▪ พ.ร.บ. ข้อมูลข่าวสารของทางราชการ 2540 (มาตรา 14 – มาตรา 15 อาจมีคำสั่งมิให้เปิดเผย)
ข้อมูลความมั่นคง			นโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ (พ.ศ. 2562-2565)		

ภาพที่ 2: การจัดหมวดหมู่และระดับชั้นข้อมูลภาครัฐ

สามารถศึกษาเพิ่มเติมได้ที่ มสพร. 8-2565 ว่าด้วยหลักเกณฑ์การจัดระดับชั้นและการแบ่งปันข้อมูลภาครัฐ

สอดคล้องตามนโยบาย “Go Cloud First” มุ่งเน้นให้หน่วยงานภาครัฐมีการใช้ระบบคลาวด์เป็นหลัก เพื่อส่งเสริมและพัฒนาให้หน่วยงานภาครัฐเป็นรัฐบาลดิจิทัล จึงจำเป็นต้องมีการจัดระดับชั้นข้อมูลในภาพรวมของการให้บริการ (Service) เพื่อเปรียบเทียบผลกระทบและความเสี่ยงที่อาจเกิดกับข้อมูล นำไปสู่การพิจารณาประเภทของคลาวด์ และถิ่นที่อยู่ของข้อมูลตามลักษณะข้อมูลที่จำเป็นต้องอยู่ในประเทศไทย หรือแนะนำให้ควรอยู่ในประเทศไทยให้เหมาะสมกับหน่วยงานภาครัฐ เพื่อเป็นกรอบแนวทางในการจำแนกประเภทข้อมูลสำหรับใช้บริการคลาวด์ โดยให้หน่วยงานภาครัฐพิจารณาการนำข้อมูลจัดเก็บในระบบคลาวด์เป็นลำดับแรก แล้วจึงพิจารณาประเภทของคลาวด์ที่เหมาะสมเป็นลำดับถัดไป ซึ่งข้อสรุปจากการประชุมคณะอนุกรรมการด้านบริหาร จัดการความต้องการใช้บริการคลาวด์ การให้บริการคลาวด์ และมาตรฐานการบริหารจัดการการบริการคลาวด์ภาครัฐ ได้กำหนดกรอบการจำแนกประเภทข้อมูลสำหรับใช้บริการคลาวด์ออกเป็น 3 ประเภท ซึ่งสอดคล้องกับระดับชั้นข้อมูล แบ่งได้ดังนี้



ภาพที่ 3: กรอบแนวทางการจำแนกประเภทข้อมูลสำหรับใช้บริการคลาวด์

1) Official Data เป็นข้อมูลในระดับชั้น เปิดเผย โดยประเภทของคลาวด์ที่แนะนำคือ Public Cloud

2) Protected Data เป็นข้อมูลในระดับชั้น เผยแพร่ภายในองค์กร ลับ ลับมาก โดยประเภทของคลาวด์ที่แนะนำคือ Public Cloud

3) Highly Protected Data เป็นข้อมูลในระดับชั้น ลับที่สุด โดยประเภทของคลาวด์ที่แนะนำคือ Private Cloud

ทั้งนี้ เพื่อให้การดำเนินการตามกรอบเป็นไปตามขั้นตอนหน่วยงานภาครัฐจึงต้องดำเนินการประเมินความเสี่ยงเพื่อพิจารณาเลือกใช้บริการคลาวด์ที่เหมาะสมกับหน่วยงาน โดยสามารถศึกษาเพิ่มเติมได้ที่ บทที่ 3 แนวทางการจำแนกประเภทข้อมูลสำหรับใช้บริการคลาวด์

3. แนวทางการจำแนกประเภทข้อมูลสำหรับใช้บริการคลาวด์

3.1 หลักเกณฑ์การจำแนกประเภทข้อมูล

การจำแนกประเภทข้อมูลสำหรับใช้บริการคลาวด์ ในหน่วยงานภาครัฐถือเป็นส่วนสำคัญในการรักษาความปลอดภัยและความเป็นส่วนตัวของข้อมูล รวมถึงเพื่อเลือกใช้บริการคลาวด์ที่เหมาะสม โดยหน่วยงานสามารถพิจารณาหลักการสำคัญในการกำหนดรายละเอียดการจำแนกประเภทข้อมูลสำหรับใช้บริการคลาวด์ ให้สอดคล้องตามแนวมาตรฐานสากลและเป็นไปตามข้อกฎหมายที่เกี่ยวข้อง เช่น ประกาศ

คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ และ ISO 27001 (Risk management) โดยระดับชั้นความลับแบ่งออกเป็น

1) ชั้นเปิดเผย (Open) สู่สาธารณะ

2) เปิดเผยเมื่อได้รับอนุญาต ได้แก่ ชั้นเผยแพร่ภายในองค์กร (Private) ชั้นลับ (Confidential) และ ชั้นลับมาก (Secret)

3) และเปิดเผยไม่ได้/ปกปิด ได้แก่ ชั้นลับที่สุด (Top Secret) โดยหลักการพิจารณาข้อมูลหรือระบบสารสนเทศ (บริการ) ในระดับลับที่สุดของหน่วยงานเป็นข้อมูลหรือระบบสารสนเทศ(บริการ) ที่เกี่ยวข้องในการดำเนินการป้องกัน แจ้งเตือน แก้ไข หรือระงับยับยั้งภัยคุกคามเพื่อธำรงไว้ซึ่งความมั่นคงแห่งชาติ ตามนโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ (พ.ศ. 2566 – 2570) 17 ด้าน ประกอบด้วย 1. หมวดประเด็นความมั่นคง 2. หมวดประเด็นศักยภาพความมั่นคง[1] อ้างอิง : **(หมายเหตุ : นโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ อาจมีการปรับปรุงหรือทบทวนตามรอบ) ซึ่งรวมถึงเป็นข้อมูลดิบ (Raw Data) หรือระบบสารสนเทศ(บริการ) ผลกระทบระดับสูง**

หลักเกณฑ์การจำแนกประเภทข้อมูลสำหรับใช้บริการคลาวด์ ประกอบด้วย 2 ส่วนได้แก่ การใช้เครื่องมือประเมินระดับชั้นข้อมูลและการพิจารณาถิ่นที่อยู่ข้อมูล รายละเอียดมีดังนี้

3.1.1. การประยุกต์การจำแนกประเภทข้อมูลจากเครื่องมือ มสพร. 8-2565

การจำแนกประเภทข้อมูลสำหรับใช้บริการคลาวด์เป็นแนวทางให้หน่วยงานพิจารณาประเภทข้อมูลเพื่อจัดเก็บบนคลาวด์ ซึ่งเป็นการประเมินความเสี่ยงข้อมูลเป็นภาพรวมของการให้บริการ (Service) โดยเทียบผลกระทบจากการเปิดเผยข้อมูลโดยไม่ได้อนุญาตกับโอกาสที่จะเกิดขึ้น ซึ่งสามารถประยุกต์การประเมินจากเครื่องมือแบบประเมินระดับชั้นข้อมูลภาครัฐจากเครื่องมือ มสพร. 8-2565 (Data Classification) เพื่อพิจารณาความเสี่ยงบริการของหน่วยงานภาครัฐในการใช้บริการคลาวด์ โดยขั้นตอนดังนี้

1) ประเมินข้อมูลในบริการ โดยพิจารณาจากระดับผลกระทบตามวัตถุประสงค์ด้านความปลอดภัยของข้อมูล (Security Objective) โดยนำผลประโยชน์แห่งชาติ จากการเปิดเผยข้อมูลโดยไม่ได้อนุญาตมาประกอบการพิจารณา ซึ่งหลักการวัตถุประสงค์ด้านความปลอดภัย 3 ด้าน ดังนี้

(ข้อเสนอแนะ : ผู้ประเมิน ควรเป็น ฝ่ายเทคโนโลยีสารสนเทศ)

- ด้านความลับ (Confidentiality) : การรักษาข้อจำกัดในการได้รับอนุญาตให้เข้าถึงได้และเปิดเผยเฉพาะผู้มีสิทธิ์ รวมทั้งวิธีการคุ้มครองความเป็นส่วนตัว (Privacy) และกรรมสิทธิ์ของข้อมูล
- ด้านความถูกต้อง ครบถ้วนสมบูรณ์ ความคงสภาพ (Integrity) : การปกป้องจากการดัดแปลงหรือทำลายข้อมูลที่ไม่เหมาะสม และรับรองว่าเป็นข้อมูลที่ถูกต้อง
- ด้านความพร้อมใช้งาน (Availability) : สร้างความมั่นใจในการเข้าถึงและการใช้ข้อมูลอย่างทันท่วงที/เป็นปัจจุบันและเชื่อถือได้

ทั้งนี้ การพิจารณาตามหลักการ CIA ตาม มสพร. 8-2565 (Data Classification) ที่กล่าวมาข้างต้น มี**ความสอดคล้องกับการประเมินในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยทางไซเบอร์ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566** ซึ่งการประเมินและจัดระดับผลกระทบที่อาจเกิดขึ้นแบ่งเป็น 3 ระดับ ได้แก่ ระดับต่ำ ระดับกลาง และ ระดับสูง ซึ่งเป็นการพิจารณาผลกระทบที่อาจเกิดต่อข้อมูลหรือระบบสารสนเทศในด้านความมั่นคงปลอดภัยไซเบอร์ ตามการประเมินและจัดระดับผลกระทบต่อการดำเนินงานของหน่วยงาน จะช่วยให้

[1] นโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ (พ.ศ. 2566 – 2570) สภาความมั่นคงแห่งชาติ

หน่วยงานสามารถออกแบบระบบความปลอดภัยให้เหมาะสมกับความสำคัญของข้อมูลหรือระบบสารสนเทศ เพื่อให้สามารถลดความเสี่ยงและตอบสนองต่อเหตุการณ์ไซเบอร์ได้อย่างมีประสิทธิภาพดังนี้

ภาพที่ 4: ผลกระทบตาม CIA ตามประกาศ กมช. เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566

ภายหลังจากหน่วยงานได้กำหนดคุณลักษณะความมั่นคงปลอดภัยทางไซเบอร์ และ ได้ระดับผลกระทบที่อาจเกิดขึ้นแก่ข้อมูลหรือระบบสารสนเทศแล้ว ควรมีกำหนดมาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำ สำหรับข้อมูลของระบบสารสนเทศในแต่ละระดับตามที่ประกาศฯ กำหนดไว้ ดังนี้

ลักษณะของผลกระทบ ในแต่ละระดับ อธิบายได้พอสังเขปดังนี้

ผลกระทบระดับต่ำ

ลักษณะผลกระทบ : ความเสียหายที่เกิดขึ้นมีผลกระทบจำกัดในวงแคบ เช่น ส่งผลต่อการทำงานบางส่วนของหน่วยงานในลักษณะที่ไม่สำคัญ ไม่มีผลกระทบต่อชื่อเสียงหลัก หรือการให้บริการที่สำคัญ

ตารางที่ 9: ลักษณะผลกระทบระดับต่ำ

ระดับผลกระทบ	ตัวอย่างข้อมูล/ระบบ	มาตรการป้องกัน
ระดับต่ำ (Low Impact)	เว็บไซต์เผยแพร่ข่าวหรือข้อมูลที่ไม่ได้อ่อนไหว เช่น ระบบประกาศทั่วไปของหน่วยงาน	- ควบคุมสิทธิ์การเข้าถึง (Access Control)
	ระบบจัดการทรัพยากรเบื้องต้น เช่น ระบบจองห้องประชุม	- สำรองข้อมูลอย่างสม่ำเสมอ

ผลกระทบระดับกลาง

ลักษณะผลกระทบ : ความเสียหายที่มีผลต่อการดำเนินงานหรือชื่อเสียงองค์กรในระยะสั้น อาจส่งผลต่อความเชื่อมั่นของประชาชนหรือการบริการ

ตารางที่ 10: ลักษณะผลกระทบระดับกลาง

ระดับผลกระทบ	ตัวอย่างข้อมูล/ระบบ	มาตรการป้องกัน
ระดับปานกลาง (Moderate Impact)	ระบบการจัดเก็บข้อมูลลูกค้า/ผู้รับบริการ/หน่วยงานรับทุน เช่น ฐานข้อมูลประวัติการใช้บริการ	- การเข้ารหัสข้อมูลสำคัญ (Data Encryption)
	ระบบจัดการเอกสารภายในองค์กร	- ตรวจสอบสิทธิ์ด้วย Multi-Factor Authentication (MFA)

ผลกระทบระดับสูง

ลักษณะผลกระทบ : ความเสียหายร้ายแรง กระทบต่อความมั่นคงของชาติ ความปลอดภัยประชาชน หรือเศรษฐกิจระดับชาติ

ตารางที่ 11: ลักษณะผลกระทบระดับสูง

ระดับผลกระทบ	ตัวอย่างข้อมูล/ระบบ	มาตรการป้องกัน
ระดับสูง (High Impact)	ระบบที่เกี่ยวกับความมั่นคงของประเทศ เช่น ระบบฐานข้อมูลผู้ต้องสงสัยในด้านความมั่นคงของรัฐ	- การตรวจสอบภัยคุกคามแบบเรียลไทม์
	ระบบโครงสร้างพื้นฐานสำคัญ เช่น ระบบพลังงาน(จ่ายไฟฟ้า) หรือ หรือระบบเครือข่ายด้านการเงินของประเทศ	- การแบ่งส่วนเครือข่าย (Network Segmentation)

ในกรณีผลการพิจารณาตามหลักการ CIA ที่กล่าวมาข้างต้น หากได้ผลกระประเมินอยู่ที่ระดับสูง จะต้องปฏิบัติตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 ได้กำหนดว่า กรณีที่ข้อมูลที่มีความเสี่ยงระดับสูง หากใช้บริการคลาวด์ต้องใช้ศูนย์ข้อมูลหลักในประเทศไทย

ทั้งนี้ การวางมาตรการควบคุมความปลอดภัยในแต่ละระดับจะต้องพิจารณาตามกรอบมาตรฐาน เช่น ISO 27001 สำหรับการจัดการความมั่นคงปลอดภัยของข้อมูล NIST Cybersecurity Framework สำหรับการตรวจสอบและป้องกันภัยทางไซเบอร์ เป็นต้น

อย่างไรก็ดี หน่วยงานควรทบทวนการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศทุก 3 ปีเป็นอย่างน้อย หรือ ทบทวนเมื่อข้อมูล ระบบสารสนเทศ หรือหน้าที่ของหน่วยงานมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ และ ทำการบันทึกผลการพิจารณาทบทวนพร้อมเหตุผล[2]

1) **ประเมินหาระดับความเสี่ยง**ของข้อมูลในบริการตามเกณฑ์การประเมินความเสี่ยงและผลกระทบจากการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต โดยประเมินหาค่าระดับความรุนแรงของผลกระทบ (Impact) ในแต่ละด้าน ได้แก่

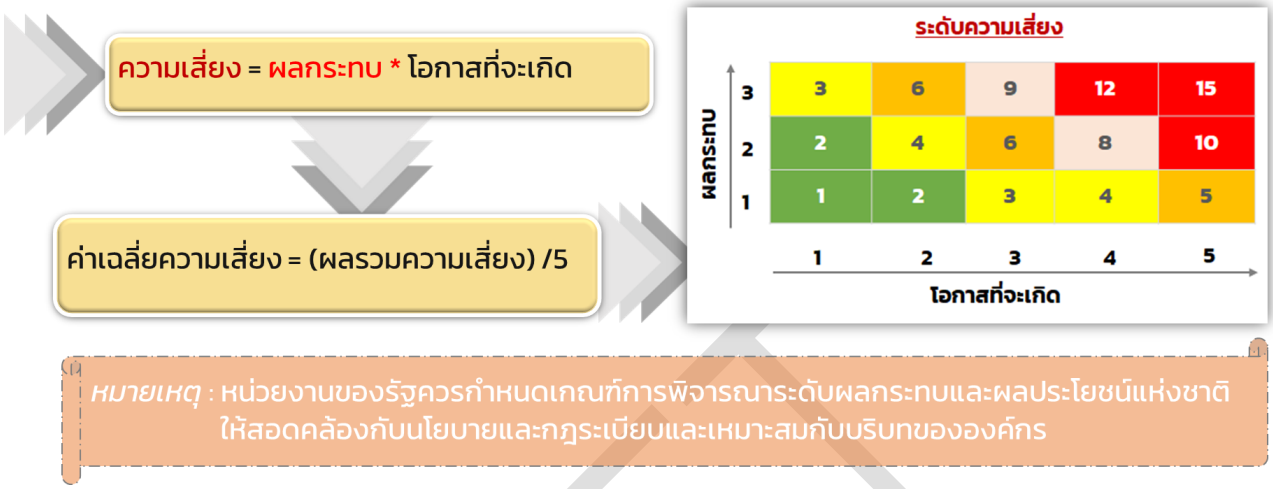
- ด้านภาพลักษณ์/ชื่อเสียง (Reputation)
- ผู้ใช้บริการและการดำเนินงานตามภารกิจ (Users & Operations)
- การเงินและสินทรัพย์ (Financial & Assets)
- ความสอดคล้องกับกฎระเบียบ ข้อบังคับ (Legal & Regulation)
- ผลประโยชน์แห่งชาติ (National Interests) ทั้งนี้ ให้หน่วยงานนำค่าเฉลี่ยที่ได้จากการประเมินใน ข้อที่1 (ค่าเฉลี่ย CIA) มาใส่เพื่อทำการประเมิน

และ**ประเมินหาค่าเฉลี่ยระดับผลกระทบโดยรวม** ซึ่งเกณฑ์การพิจารณาระดับผลกระทบและผลประโยชน์แห่งชาติ ตามมาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ว่าด้วยหลักเกณฑ์การจัดระดับชั้น และการแบ่งปันข้อมูลภาครัฐ (มสพร. 8:2565) ซึ่งสอดคล้องกับข้อ 6 ใน*ประกาศ*คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์

[2] ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยทางไซเบอร์ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566

จากนั้น **ประเมินโอกาสที่จะเกิด** ของความเสี่ยงจากการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต หรือการรั่วไหลของข้อมูลที่มีระดับชั้นความลับ ที่จะเกิดขึ้น โดยการพิจารณาจากสถิติการเกิดเหตุการณ์ในอดีต ปัจจุบัน หรือการคาดการณ์ล่วงหน้าของโอกาสที่จะเกิดในอนาคตต่อชุดข้อมูลนั้น ๆ

(ข้อเสนอแนะ: ผู้ประเมิน ควรเป็น เจ้าของข้อมูลร่วมกับฝ่ายเทคโนโลยีสารสนเทศ)



ภาพที่ 5: วิธีการประเมินความเสี่ยง

3.ติดป้ายหรือแท็กกำกับระดับชั้นข้อมูลตามความอ่อนไหว ความเสี่ยงและผลกระทบจากการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

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

ค่าระดับความเสี่ยงสูง ระดับ 10 ขึ้นไป จัดอยู่ในระดับความเสี่ยงสูงมาก และ สอดคล้องตามนโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ (พ.ศ. 2566 – 2570) ซึ่งข้อมูลจะอยู่ในระดับลับที่สุด หน่วยงานต้องมีการจัดทำเอกสารประกอบการเสนอโครงการและงบประมาณด้านระบบคลาวด์ฯ เพื่อใช้คลาวด์ประเภท Private Cloud

ภาพที่ 6: การติดป้ายหรือแท็กกำกับระดับชั้นข้อมูลตามความอ่อนไหว

3.1.2. การพิจารณาถิ่นที่อยู่ข้อมูล

เพื่อให้หน่วยงานสามารถพิจารณาการเลือกมาประเภทคลาวด์ได้อย่างเหมาะสมแล้ว นอกจากการประเมินความอ่อนไหวของข้อมูลตามหัวข้อ 3.1.1 และต้องพิจารณาถึงการกำหนดถิ่นที่อยู่ข้อมูลด้วย เพื่อให้หน่วยงานสามารถพิจารณาได้ว่าควรมีการกำหนดถิ่นที่อยู่ข้อมูลอย่างไร โดยมี 3 รูปแบบดังนี้

การจัดเก็บและประมวลผลข้อมูลในประเทศ (Data Localization) คือการจัดเก็บข้อมูลที่ต้องจัดเก็บและประมวลผลภายในประเทศที่ข้อมูลมีการจัดเก็บหรือประมวลผลเท่านั้น ซึ่งจะไม่สามารถโอนย้ายไปนอกประเทศได้

อธิปไตยของข้อมูล (Data Sovereignty) คือการจัดเก็บข้อมูลที่สามารถจัดเก็บข้อมูลที่ไหนก็ได้ โดยสิทธิในการครอบครองและการควบคุมข้อมูลต้องดำเนินการตามกฎหมายของประเทศที่จัดเก็บและประมวลผลข้อมูล

การกำหนดพื้นที่ในการส่งข้อมูล (Data Residency) คือ การกำหนดสถานที่ในการส่งข้อมูล เพื่อให้สอดคล้องกับข้อกำหนดทางกฎหมายหรือระเบียบข้อบังคับ

ภาพที่ 7: รูปแบบการพิจารณาถิ่นที่อยู่ข้อมูล

ในแต่ละรูปแบบมีความแตกต่างกันดังนี้

ตารางที่ 12: ตารางเปรียบเทียบรูปแบบของถิ่นที่อยู่ข้อมูล

หัวข้อ	ข้อดี	ข้อเสีย
การจัดเก็บและประมวลผลข้อมูลในประเทศ (Data Localization)	- เพิ่มความมั่นคงทางข้อมูล โดยให้ความสำคัญกับสถานที่เก็บข้อมูลทางกายภาพ - รองรับการบังคับใช้กฎหมายภายในประเทศ - กระตุ้นเศรษฐกิจภายใน เช่น การพัฒนาโครงสร้างพื้นฐานดิจิทัล	- เพิ่มต้นทุนการจัดเก็บและการดำเนินการ จำกัดการค้าและนวัตกรรม เนื่องจากการปิดกั้นการแลกเปลี่ยนข้อมูลระหว่างประเทศ
อธิปไตยของข้อมูล (Data Sovereignty)	- ช่วยให้ปฏิบัติตามกฎระเบียบในแต่ละพื้นที่ได้ง่ายขึ้น - ให้ความสำคัญกับการควบคุมและกฎหมายที่ใช้กับข้อมูล - ยืดหยุ่นในการจัดการข้อมูลตามความต้องการของธุรกิจหรือผู้ใช้งานในพื้นที่	- ซับซ้อนในการบริหารจัดการข้อมูลในหลายพื้นที่ - การปรับปรุงกฎหมายอาจส่งผลต่อการจัดเก็บข้อมูล
การกำหนดพื้นที่ในการส่งข้อมูล (Data Residency)	- ควบคุมข้อมูลได้ดีขึ้นภายใต้กฎหมายในท้องถิ่น - เสริมความมั่นคงของประเทศและอธิปไตยทางดิจิทัล - ให้ความสำคัญกับสถานที่เก็บข้อมูลทางกายภาพ	- อาจจำกัดการใช้บริการคลาวด์ข้ามประเทศ - ซับซ้อนในการทำธุรกิจระหว่างประเทศ โดยเฉพาะองค์กรที่ทำงานข้ามพรมแดน

สรุปการพิจารณาเลือกใช้ถิ่นที่อยู่ข้อมูล

จากการพิจารณาข้อดีและข้อเสียดังตารางด้านบนจะเห็นได้ว่า รูปแบบการกำหนดถิ่นที่อยู่ข้อมูลที่มีลักษณะยืดหยุ่นต่อการดำเนินงานและสามารถบังคับการดำเนินการให้สอดคล้องตามกฎหมายได้ คือ อธิปไตยของข้อมูล (Data Sovereignty) เพราะไม่มีการกำหนดพื้นที่จัดเก็บข้อมูลและกฎหมายภายในประเทศก็ยังสามารถบังคับใช้ได้

ปัจจุบันแม้ว่า ประเทศไทย**มีการกำหนดเรื่อง การจัดเก็บและประมวลผลข้อมูลในประเทศ (Data Localization) ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567** ซึ่งเป็นมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของระบบคลาวด์ ซึ่งมีวัตถุประสงค์เพื่อลดความเสี่ยงของการใช้บริการคลาวด์สาธารณะในหน่วยงานรัฐ โดยได้มีการกำหนดข้อกำหนดขั้นต่ำสำหรับประเภทของข้อมมูลหรือระบบสารสนเทศ[3] **โดยผลกระทบระดับสูงจะต้องต้องใช้ศูนย์ข้อมูลหลักในประเทศไทย (Data Localization)**

ในส่วนของการกำหนดเรื่องถิ่นที่อยู่ข้อมูลของประเทศไทย ควรให้ความสำคัญกับอธิปไตยของข้อมูล (Data Sovereignty) ในการใช้คลาวด์ อย่างไรก็ดี หน่วยงานควรมีการพิจารณากฎหมายที่เกี่ยวข้องเพิ่มเติม เพื่อให้มีจำแนกประเภทข้อมูลสำหรับใช้บริการคลาวด์อย่างมีประสิทธิภาพ โดยพิจารณาการโอนข้อมูลส่วนบุคคลข้ามพรมแดน ดังนี้

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

มาตรา 28 ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศหรือประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลต้องมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ ทั้งนี้ ต้องเป็นไปตามหลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลตามที่คณะกรรมการประกาศ

ทั้งนี้ ให้หน่วยงานพิจารณากฎหมายที่เกี่ยวข้องเพิ่มเติมในการพิจารณาถิ่นที่อยู่ข้อมูลได้ โดยไม่ว่าข้อมูลจะถูกเก็บที่ไหนให้หน่วยงานของรัฐมีอำนาจในการควบคุมและบริหารจัดการข้อมูลนั้นให้สอดคล้องกับกฎหมายหรือข้อบังคับที่เกี่ยวข้องได้ (Data Sovereignty) โดยที่หน่วยงานต้องสามารถเข้าถึงและกำหนดสิทธิการเข้าถึงข้อมูล รวมถึงแนวทางการบริหารจัดการข้อมูลบนคลาวด์ได้

[3] ประเภทของข้อมูลหรือระบบสารสนเทศที่ผ่านการประเมินตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยทางไซเบอร์ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566 ที่กล่าวมาใน หัวข้อ 3.1.1

3.2 แนวทางการจำแนกประเภทข้อมูลกับการใช้บริการคลาวด์

การจำแนกประเภทข้อมูลเพื่อเลือกใช้บริการคลาวด์ มีแนวทางตามหัวข้อ 3.1 หลักเกณฑ์การจำแนกประเภทข้อมูล ซึ่งเป็นการจำแนกประเภทข้อมูลในบริการว่ามีระดับความเสี่ยงเป็นอย่างไร เพื่อพิจารณาการใช้บริการคลาวด์ที่เหมาะสม ประกอบด้วย 2 ส่วนดังนี้

1. เป็นข้อมูลที่อยู่ในระดับชั้นลับที่สุดหรือไม่

☐ เป็นข้อมูลที่ห้ามเผยแพร่นอกองค์กร หรือไม่

☐ ในกรณีที่เป็นข้อมูลที่ห้ามเปิดเผยตาม พรบ. ตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 หรือไม่ โดยเป็นข้อมูลตามมาตรา 14 หรือมาตรา 15 ตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 หรือไม่

☐ หากเป็นข้อมูลตามมาตรา 14 ตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ให้ **จัดว่าเป็นข้อมูลข่าวสารลับที่สุด** ตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 ซึ่งเป็นหนึ่งหมวดหมู่ในระดับชั้นข้อมูลลับที่สุด จะต้องมีการบริหารจัดการตามตามระเบียบว่าด้วยการรักษาความลับฯ และเป็นดุลพินิจของหัวหน้าหน่วยงานในการดำเนินการต่างๆ

☐ หากเป็นข้อมูลตามมาตรา 15 ตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ให้ **พิจารณาว่าเป็นข้อมูลที่ได้มีการกำหนดให้เป็นข้อมูลข่าสารจัดว่าเป็นข้อมูลข่าวสารลับในระดับลับที่สุด ตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 และสอดคล้องกับนโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ (พ.ศ. 2566 – 2570)** หรือไม่ หากเข้าเงื่อนไขตามเกณฑ์นี้ ให้ถือว่า **เป็นข้อมูลข่าวสารลับที่สุด ซึ่งเป็นหนึ่งหมวดหมู่ในระดับชั้นข้อมูลลับที่สุด** และจะต้องมีการบริหารจัดการตามตามที่คณะกรรมการข้อมูลข่าวสารของราชการและคณะอนุกรรมการพัฒนาการปฏิบัติกำหนด และดุลพินิจของหัวหน้าหน่วยงานในการดำเนินการต่างๆ

หลักการพิจารณาข้อมูลข่าวสารลับที่สุด

พรบ. ข้อมูลข่าวสารของราชการ พ.ศ. 2540	ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544	นโยบายและแผนความมั่นคงแห่งชาติ พ.ศ. 2566 – 2570
เป็นข้อมูลที่สอดคล้องตาม ม. 14 , 15 หรือไม่ ? **มาตรา 14** ข้อมูลข่าวสารของราชการที่เปิดเผยไม่ได้ ข้อมูลข่าวสารของราชการที่อาจ**ก่อให้เกิดความเสียหายต่อสถาบันพระมหากษัตริย์**จะเปิดเผยมิได้ **มาตรา 15** (1) การเปิดเผยจะก่อให้เกิดความเสียหาย**ต่อความมั่นคงของประเทศ ความสัมพันธ์ระหว่างประเทศ หรือความมั่นคงในทางเศรษฐกิจหรือการคลัง**ของประเทศ (2) การเปิดเผยจะทำให้**การบังคับใช้กฎหมายเสื่อมประสิทธิภาพ...**ไม่ว่าจะเกี่ยวกับการฟ้องคดีการป้องกัน การปราบปราม การทดสอบการตรวจสอบ... (3) **ความเห็นหรือคำแนะนำภายในหน่วยงาน**ของรัฐ.. แต่ไม่รวมถึงรายงานทางวิชาการ รายงานข้อเท็จจริง... (4) การเปิดเผยจะก่อให้เกิด**อันตรายต่อชีวิต**หรือความปลอดภัยของบุคคลหนึ่งบุคคลใด (5) **รายงานการแพทย์หรือข้อมูลข่าวสารส่วนบุคคล...** (6) ข้อมูลข่าวสารของราชการที่**มีกฎหมายคุ้มครองมิให้เปิดเผย**... (7) **กรณีอื่น...**	**เป็นข้อมูลที่สอดคล้องตามระเบียบว่าด้วยการรักรักษาความลับ หรือไม่?** **ข้อ 13** ชั้นความลับของข้อมูลข่าวสารลับ แบ่งออกเป็น 3 ชั้น คือ (1) ลับที่สุด (TOP SECRET) (2) ลับมาก (SECRET) (3) ลับ (CONFIDENTIAL) **ข้อ 13** **ลับที่สุด** หมายความถึง ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรงที่สุด **ข้อ 14** **ลับมาก** หมายความถึง ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรง **ข้อ 15** **ลับ** หมายความถึง ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐ	**เป็นข้อมูลตามประเด็นความมั่นคงหรือไม่ ?** 1. การเสริมสร้างความมั่นคงของสถาบันหลักของชาติ 2. การปกป้องอธิปไตยและผลประโยชน์ของชาติ และการพัฒนาศักยภาพการป้องกันประเทศ 3. การรักษาความมั่นคงและผลประโยชน์ของชาติพื้นที่ชายแดน 4. การรักษาความมั่นคงและผลประโยชน์ของชาติทางทะเล 5. การป้องกันและแก้ไขปัญหาจังหวัดชายแดนภาคใต้ 6. การบริหารจัดการผู้หลบหนีเข้าเมืองและ ผู้โยกย้ายถิ่นฐานแบบไม่ปกติ และผู้โยกย้ายถิ่นฐานแบบไม่ปกติ 7. การป้องกันและแก้ไขปัญหาการค้ามนุษย์ 8. การป้องกัน ปราบปราม และแก้ไขปัญหายาเสพติด 9. การป้องกันและบรรเทาสาธารณภัย 10. การป้องกันและแก้ไขปัญหาความมั่นคงทางไซเบอร์ 11. การป้องกันและแก้ไขปัญหาการก่อการร้าย 12. การสร้างดุลยภาพระหว่างประเทศ 13. การบริหารจัดการภาวะฉุกเฉินด้านสาธารณสุข และโรคติดต่ออุบัติใหม่ 14. การพัฒนาศักยภาพการเตรียมพร้อมแห่งชาติ และการบริหารจัดการวิกฤตการณ์ระดับชาติ 15. การพัฒนาระบบข่าวกรองแห่งชาติ 16. การบูรณาการข้อมูลด้านความมั่นคง 17. การเสริมสร้างความมั่นคงเชิงพื้นที

ภาพที่ 8: หลักการพิจารณาข้อมูลข่าวสารลับที่สุด

☐ หากไม่เข้าเงื่อนไขตามมาตรา 14 และมาตรา 15 ตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ต้องมีการใช้เครื่องมือตาม มสพร. 8 ในการจัดระดับชั้นข้อมูล ซึ่งหากได้ผลการประเมินที่ 10 คะแนนขึ้นไป และ สอดคล้องตามนโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ (พ.ศ. 2566 – 2570) ก็ให้ถือว่า ข้อมูลในบริการนั้นเป็น**ข้อมูลระดับชั้นลับที่สุด รายละเอียดดูเพิ่มเติมได้ในหัวข้อ 3.2.1**

สำหรับข้อมูลระดับชั้นลับที่สุด หากจะนำขึ้นคลาวด์จะถือว่าเป็นข้อมูลข้อมูลที่ต้องได้รับความคุ้มครองสูงสุดซึ่งต้องจัดเก็บใน Private Cloud พร้อมมาตรการป้องกันเข้มงวดตามความดุลพินิจของหัวหน้าหน่วยงานของรัฐ และจัดเก็บในประเทศไทยเท่านั้น **รายละเอียดดูเพิ่มเติมได้ในหัวข้อ 3.2.1**

2. หากไม่ได้เป็นข้อมูลที่อยู่ในระดับชั้นลับที่สุด ให้นำเครื่องมือจากข้อ 3.1 มาพิจารณาประกอบกันดังนี้

☐ หากได้ผลการประเมินอยู่ที่ 10 – 15 คะแนน แต่ไม่สอดคล้องตามนโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ (พ.ศ. 2566 – 2570) กำหนด ให้ถือว่าเป็นข้อมูลในบริการในระดับ**ชั้นลับมาก** ซึ่งเป็นประเภทข้อมูลในที่ต้องได้รับการคุ้มครอง สามารถเลือกใช้ Public Cloud ได้ โดยหน่วยงานต้องมีมาตรการควบคุมความปลอดภัยทางไซเบอร์ เพื่อการบริหารจัดการที่เหมาะสม **รายละเอียดดูเพิ่มเติมได้ในหัวข้อ 3.2.2**

☐ หากได้ผลการประเมินอยู่ระหว่าง 3-9 คะแนนขึ้นไป ข้อมูลในบริการนั้นเป็นข้อมูลประเภทข้อมูลที่ต้องได้รับความคุ้มครอง (Protected) ซึ่งจะประกอบด้วย ข้อมูลระดับ ชั้นเผยแพร่ภายในองค์กร ชั้นลับ และชั้นลับมาก ซึ่งเป็นประเภทข้อมูลในที่ต้องได้รับการคุ้มครอง สามารถเลือกใช้ Public Cloud ได้ โดยหน่วยงานต้องมีมาตรการควบคุมความปลอดภัยทางไซเบอร์ เพื่อการบริหารจัดการที่เหมาะสม **รายละเอียดดูเพิ่มเติมได้ในหัวข้อ 3.2.2**

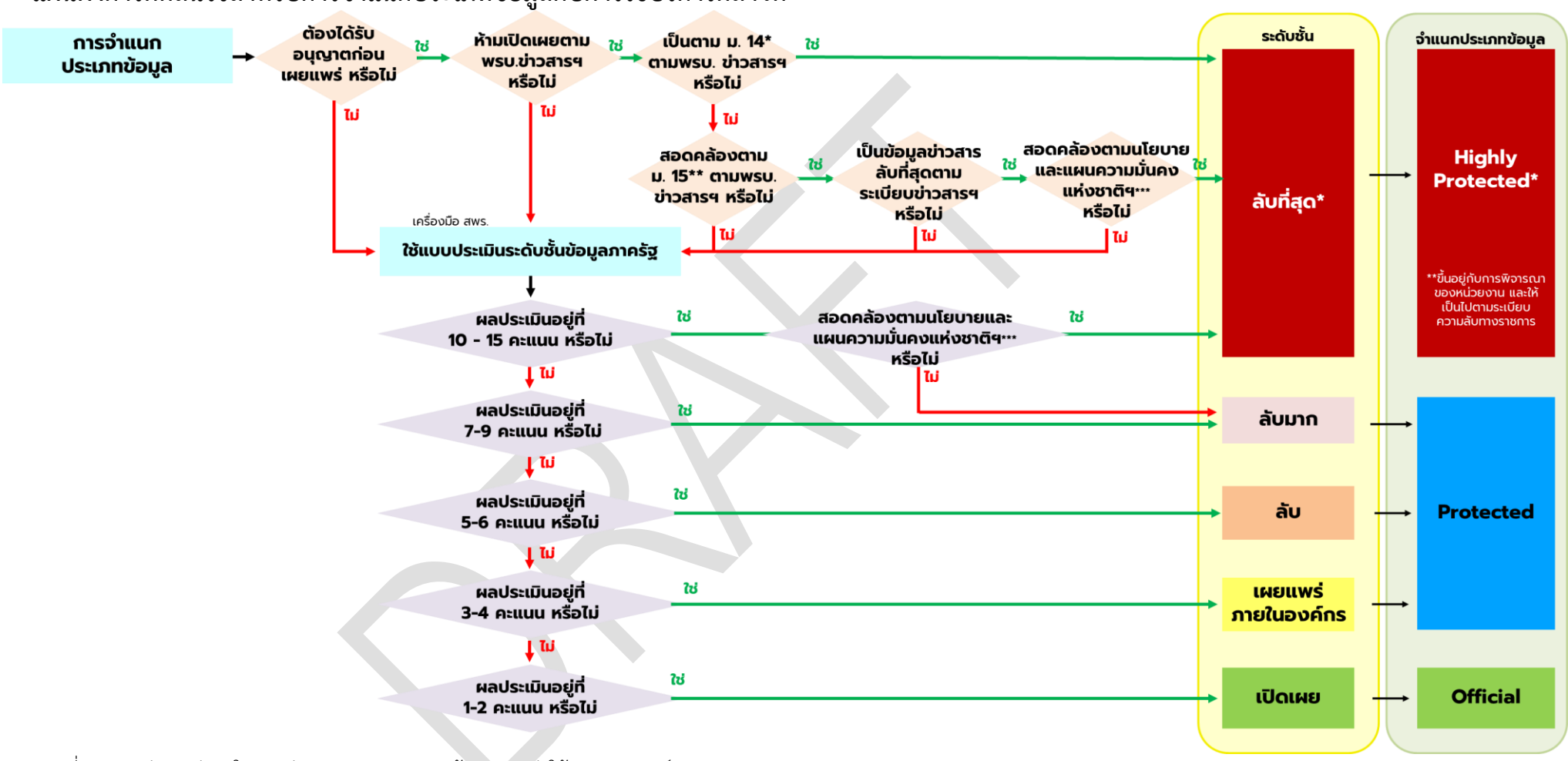
☐ หากได้ผลการประเมินอยู่ระหว่าง 1-2 คะแนนขึ้นไป ข้อมูลในบริการนั้นเป็นข้อมูลประเภทข้อมูลที่สามารถเปิดเผยได้ จะประกอบด้วย ข้อมูลระดับชั้นเปิดเผย เป็นข้อมูลที่มีความเสี่ยงต่ำ **สามารถเลือกใช้ Public Cloud ได้ โดยหน่วยงานต้องมีมาตรการควบคุมความปลอดภัยทางไซเบอร์ เพื่อการบริหารจัดการที่เหมาะสม รายละเอียดดูเพิ่มเติมได้ในหัวข้อ 3.2.**3

ตารางที่ 13: หัวข้อการจำแนกประเภทข้อมูล

ค่าระดับความเสี่ยง	ระดับชั้นข้อมูล	ประเภทข้อมูล	รายละเอียด
10 - 15	ลับที่สุด	Highly Protected	ข้อ 3.2.1
7-9	ลับมาก	Protected	ข้อ 3.2.2
5-6	ลับ		
3-4	เผยแพร่ภายในองค์กร		
1-2	เปิดเผย	Official	ข้อ 3.2.3

การจำแนกประเภทข้อมูลสามารถใช้แผนผังการตัดสินใจสำหรับการจำแนกประเภทข้อมูลกับการใช้บริการคลาวด์ได้ดังนี้

27 แผนผังการตัดสินใจสำหรับการจำแนกประเภทข้อมูลกับการใช้บริการคลาวด์



28

29 ภาพที่ 9: แผนผังการตัดสินใจสำหรับการจำแนกประเภทข้อมูลสำหรับใช้บริการคลาวด์

3.2.1. ข้อมูลที่ต้องได้รับความคุ้มครองสูงสุด (Highly Protected Data)

ข้อมูลที่ต้องได้รับความคุ้มครองสูงสุด คือ ประเภทข้อมูลในบริการที่มีความเสี่ยงสูง ซึ่งส่งผลต่อความมั่นคงของชาติ และต้องการการรับรองมาตรการควบคุมความปลอดภัยที่สูงมาก ประกอบด้วย ข้อมูลที่มีความอ่อนไหวเป็นพิเศษ ซึ่งส่งผลต่อความมั่นคงของชาติหรือพันธมิตร และต้องการมาตรการควบคุมความปลอดภัยที่สูงมาก เพื่อป้องกันการละเมิดข้อมูลจากภัยคุกคามทั้งหมด โดยการใช้เครือข่ายบนโครงสร้างพื้นฐานทางกายภาพที่มีความปลอดภัยสูง และมีการคุ้มครองข้อมูลและควบคุมความปลอดภัยอย่างเข้มงวด

ทั้งนี้ เจ้าของระบบ/CIO จะต้องเป็นผู้ประเมินระดับชั้นเพื่อพิจารณาประเภทข้อมูล โดยประยุกต์จากเครื่องมือในหัวข้อ 3.1 ซึ่งต้องมีระดับความเสี่ยงที่ **10 – 15 คะแนน** และเป็น**นโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ (พ.ศ. 2566 – 2570)** และควรสอดคล้องกับเกณฑ์ระดับความรุนแรงของระดับผลกระทบและผลประโยชน์แห่งชาติ สรุปได้ดังนี้

ตารางที่ 14: เกณฑ์การพิจารณาผลกระทบสำหรับข้อมูลที่ต้องได้รับความคุ้มครองสูงสุด[4]

ด้าน	เกณฑ์การพิจารณาผลกระทบ		
	1 = ต่ำ	2 = ปานกลาง	3 = สูง
ชื่อเสียง	**น้อย/อย่างจำกัด** โดย ✓ ส่งผลกระทบเฉพาะภาพลักษณ์หน่วยงาน ใช่หรือไม่ ✓ ส่งผลกระทบต่อการรับรู้บทบาทหน้าที่ของหน่วยงาน ใช่หรือไม่ ✓ ส่งผลกระทบต่อภาพลักษณ์ของระบบการให้บริการ ใช่หรือไม่	**อย่างร้ายแรง** โดย ✓ ส่งผลกระทบต่อภาพลักษณ์ของระบบการให้บริการ ใช่หรือไม่ ✓ ส่งผลความเชื่อมั่นของผู้ใช้บริการ ใช่หรือไม่ ✓ สามารถฟ้องร้องทางคดีแพ่ง ใช่หรือไม่	**อย่างร้ายแรงมาก** โดย ✓ ส่งผลกระทบต่อภาพลักษณ์ชื่อเสียงของรัฐในระดับประเทศ ใช่หรือไม่ ✓ สามารถฟ้องร้องทางคดีแพ่ง ใช่หรือไม่ ✓ สามารถฟ้องร้องทางคดีอาญา ใช่หรือไม่
ผู้ใช้และการดำเนินงาน	**รายบริการ/การดำเนินงานขององค์กร** โดย ✓ ส่งผลกระทบต่อการทำงานภายในหน่วยงาน ใช่หรือไม่ ✓ ส่งผลกระทบต่อประสิทธิภาพการทำงานของผู้ปฏิบัติงานของหน่วยงานลดลง ใช่หรือไม่ ✓ ส่งผลการใช้งานของจำนวนผู้ใช้งานในวงแคบ ใช่หรือไม่	**ราย Domain/การดำเนินของกระทรวง/ระหว่างองค์กร/จังหวัด** โดย ✓ ส่งผลให้เกิดอุปสรรคต่อการทำงานภายในหน่วยงาน และหน่วยงานคู่สัญญา ✓ ส่งผลต่อประสิทธิภาพการให้บริการของระบบ ✓ บางบริการมีความไม่สะดวก หรือล่าช้า เสียเวลา แต่ยังไม่สูญเสียข้อมูล ใช่หรือไม่ ✓ ส่งผลกระทบต่อผู้ใช้บริการบางส่วน ใช่หรือไม่	**Cross Domains, Sectors, Region/การดำเนินงานตามแผนบูรณาการ/กลุ่มจังหวัด** โดย ✓ ส่งผลกระทบต่อการทำงานภายในหน่วยงานเครือข่ายมากกว่า 2 หน่วยงาน ใช่หรือไม่ ✓ ส่งผลกระทบต่อผู้มาใช้บริการทุกคน และกระทบวงกว้างในระดับประเทศ ใช่หรือไม่ ✓ ระบบล่มหรือใช้งานไม่ได้ ทำให้เกิดความเสียหายของผู้ใช้บริการ ใช่หรือไม่ ✓ ข้อมูลในระบบสูญหาย ใช่หรือไม่
การเงินและสินทรัพย์	**มูลค่าไม่เกิน 5 ล้าน/ Small project** โดย ✓ มูลค่าความเสียหายของการให้บริการหรือโครงการ เช่น ค่าดำเนินการ เช่น ค่าปรับ ค่าเยียวยา ค่าเสียหาย โดยมีมูลค่าไม่เกิน 5 ล้าน ใช่หรือไม่	**ตั้งแต่ 5 ล้าน แต่ไม่ถึง 100 ล้าน/ Medium project** โดย ✓ มูลค่าความเสียหายของการให้บริการหรือโครงการ เช่น ค่าดำเนินการ เช่น ค่าปรับ ค่าเยียวยา ค่าเสียหาย โดยมีมูลค่า	**ตั้งแต่ 100 ล้านบาท ขึ้นไป /Large Project** โดย ✓ มูลค่าความเสียหายของการให้บริการหรือโครงการ เช่น ค่าดำเนินการ เช่น

[4] สามารถกำหนดเกณฑ์การพิจารณาระดับผลกระทบให้สอดคล้องกับนโยบายและกฎระเบียบที่เกี่ยวข้อง และเหมาะสมกับบริบทขององค์กร เช่น การให้หัวหน้าหน่วยงานหน่วยงานเป็นผู้พิจารณา

ด้าน	เกณฑ์การพิจารณาผลกระทบ		
	1 = ต่ำ	2 = ปานกลาง	3 = สูง
	ทั้งนี้ การพิจารณาเป็นตัวเงินและความสูญเสียหายของ Asset อาจเป็นเรื่องบทลงโทษทางกฎหมาย มูลค่าความเสียหาย ค่าดำเนินการต่างๆ	ตั้งแต่ 5 ล้าน แต่ไม่ถึง 100 ล้านบาท ใช่หรือไม่ ทั้งนี้ การพิจารณาเป็นตัวเงินและความสูญเสียหายของ Asset อาจเป็นเรื่องบทลงโทษทางกฎหมาย มูลค่าความเสียหาย ค่าดำเนินการต่างๆ	ค่าปรับ ค่าเยียวยา ค่าเสียหาย โดยมีมูลค่า ตั้งแต่ 100 ล้าน ใช่หรือไม่ ทั้งนี้ การพิจารณาเป็นตัวเงินและความสูญเสียหายของ Asset อาจเป็นเรื่องบทลงโทษทางกฎหมาย มูลค่าความเสียหาย ค่าดำเนินการต่างๆ
กฎหมายและระเบียบข้อบังคับ	**ละเว้นการปฏิบัติตามระเบียบข้อบังคับขององค์กร ซึ่งเกิดผลกระทบน้อย** โดย ✓ ไม่ปฏิบัติตามกฎระเบียบระดับองค์กร ใช่หรือไม่ ✓ ส่งผลให้หน่วยงานได้รับบทลงโทษของหน่วยงาน ใช่หรือไม่	**ละเว้นการปฏิบัติตามระเบียบข้อบังคับและกฎกระทรวง ซึ่งเกิดผลกระทบที่มีนัยสำคัญและไม่เป็นไปตามเป้าของ ก.พ.ร.** โดย ✓ ไม่ปฏิบัติตามกฎระเบียบระดับกระทรวง เช่น กฎกระทรวง ใช่หรือไม่ ✓ ส่งผลให้หน่วยงานได้รับบทลงโทษทางอาญาและทางแพ่ง หรือ โทษทางปกครอง ใช่หรือไม่	**ละเว้นการปฏิบัติตามกฎหมาย มติ ครม. หรือระเบียบข้อบังคับ ซึ่งเกิดผลกระทบที่มีนัยสำคัญ และไม่เป็นไปตามเป้าของแผนบูรณาการ/กลุ่มจังหวัด** โดย ✓ ไม่ปฏิบัติตามกฎหมายอย่างชัดเจน หรือไม่ปฏิบัติตามมติ ครม. รัฐบาล และไม่เป็นไปตามเป้าหมายของแผนบูรณาการ ใช่หรือไม่ ✓ ไม่ปฏิบัติตามกฎหมายส่งผลให้หน่วยงานได้รับบทลงโทษทางอาญาและทางแพ่ง หรือ โทษทางปกครอง ใช่หรือไม่
ผลประโยชน์แห่งชาติ	**ผลประโยชน์แห่งชาติสำคัญน้อย** โดย ✓ มีผลกระทบจากการเปิดเผยข้อมูลโดยไม่ได้อนุญาต ตามหลักการ CIA ในระดับต่ำ ใช่หรือไม่ ✓ การเปิดเผยข้อมูลจะส่งผลให้เกิดอันตรายต่อทรัพย์สิน/ชีวิต/ความปลอดภัยของบุคคลใดบุคคลหนึ่ง ใช่หรือไม่	**ผลประโยชน์แห่งชาติที่สำคัญ** โดย ✓ มีผลกระทบจากการเปิดเผยข้อมูลโดยไม่ได้อนุญาต ตามหลักการ CIA ในระดับปานกลาง ใช่หรือไม่ ✓ การเปิดเผยข้อมูลจะส่งผลให้เกิดอันตรายต่อทรัพย์สิน/ชีวิต/ความปลอดภัยของประชาชนบางส่วน ใช่หรือไม่ ✓ สร้างความเสียหายต่อความสัมพันธ์ระหว่างหน่วยงานอื่นๆ ใช่หรือไม่	**ผลประโยชน์แห่งชาติที่สำคัญยิ่ง** โดย ✓ มีผลกระทบจากการเปิดเผยข้อมูลโดยไม่ได้อนุญาต ตามหลักการ CIA ในระดับสูง ใช่หรือไม่ ✓ การเปิดเผยข้อมูลจะส่งผลให้เกิดอันตรายต่อทรัพย์สิน/ชีวิต/ความปลอดภัยของประชาชนส่วนใหญ่ ใช่หรือไม่ ✓ เกิดความเสียหายต่อความมั่นคงของประเทศ หรือความสัมพันธ์ระหว่างประเทศ หรือความมั่นคงทางเศษฐกิจของประเทศใช่หรือไม่

ทั้งนี้ ในกรณีของการนำเข้าข้อมูลข่าวสารลับที่สุดเข้าสู่ระบบอิเล็กทรอนิกส์ให้เป็นดุลพินิจของหัวหน้าหน่วยงาน

หากเข้าเกณฑ์ทุกข้อด้านบนจะเห็นได้ว่า ข้อมูลที่ต้องได้รับความคุ้มครองสูงสุด (Highly Protection Data) ข้อมูลในบริการมีความเสี่ยงระดับสูง ซึ่งหมายถึง เป็นระดับความเสี่ยงที่องค์กรไม่สามารถยอมรับได้ และต้องจัดการลดความเสี่ยงให้ไปอยู่ในระดับต่ำลงในทันที หรืออาจมีการถ่ายโอนความเสี่ยง โดยต้องจัดให้มีแผนการลดความเสี่ยงและป้องกันไม่ให้ความเสี่ยงกลับเพิ่มสูงขึ้นด้วย

สำหรับข้อมูลที่ต้องได้รับความคุ้มครองสูงสุด และมีความเสี่ยงระดับสูง**ที่สอดคล้องตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ว่า จะต้องมีมาตรการควบคุมความปลอดภัยทางไซเบอร์ตามที่กำหนดไว้ในข้อ**

4 ตามประกาศคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566 ด้วย

นอกจากนี้ ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 ได้กำหนดว่า กรณีที่ข้อมูลที่มีความเสี่ยงระดับสูง หากใช้บริการคลาวด์ต้องใช้ศูนย์ข้อมูลหลักในประเทศไทย ประกอบกับมติที่ประชุมการประชุมคณะกรรมการเฉพาะด้านการขับเคลื่อนตามนโยบายการใช้คลาวด์เป็นหลัก (Cloud First Policy) ครั้งที่ 3/2567 กำหนดไว้ ข้อมูลที่มีระดับชั้นลับที่สุดต้องจัดเก็บในประเทศไทย

จึงสรุปได้ว่า ข้อมูลที่ต้องได้รับความคุ้มครองสูงสุด (Highly Protected Data) ต้องจัดเก็บในประเทศไทยเท่านั้น เนื่องจากเป็นข้อมูลที่ไม่สามารถเปิดเผยได้และต้องได้มีการควบคุมความปลอดภัยที่เข้มงวด หน่วยงานจึงควรมีการกำหนดพื้นที่ในการจัดเก็บข้อมูลที่ชัดเจน จึง**ควรเลือกใช้ Private Cloud** โดยหน่วยงานต้องมีการบริหารจัดการข้อมูลที่เหมาะสม ซึ่งเป็นการทำงานร่วมกันระหว่าง ผู้ปฏิบัติงานด้านสารสนเทศ ฝ่าย IT หรือ เจ้าของระบบงาน กับผู้ปฏิบัติงานด้านข้อมูลขององค์กร ได้แก่ เจ้าของข้อมูล ซึ่งควรมีการบริหารจัดการข้อมูลที่เหมาะสม ดังตัวอย่างต่อไปนี้

ตารางที่ 15: ข้อเสนอแนะเบื้องต้นต่อการบริหารจัดการข้อมูลที่ต้องได้รับความคุ้มครองสูงสุด

ข้อเสนอแนะเบื้องต้นต่อการบริหารจัดการข้อมูลที่ต้องได้รับความคุ้มครองสูงสุด[5]	
ประเภทคลาวด์	• Private Cloud
ข้อเสนอแนะต่อการบริหารจัดการตามกรอบธรรมาภิบาลข้อมูล	• กำหนดบทบาทผู้ที่เกี่ยวข้องกับกรอบธรรมาภิบาลข้อมูลภาครัฐ • จัดทำนโยบายและแนวปฏิบัติการบริหารจัดการข้อมูลเป็นลายลักษณ์อักษรเพื่อสนับสนุนการการดำเนินงาน เช่น ➢ เจ้าของระบบ/CIO เป็นผู้กำหนดสิทธิเจ้าของข้อมูลในการเข้าถึงข้อมูลได้เท่าที่จำเป็น (need to know basis) และมีต้องมีการลงนามข้อตกลงไม่เปิดเผยข้อมูล (non-disclosure agreements) ➢ กำหนดบทบาทและแนวปฏิบัติของของเจ้าของข้อมูลและผู้ที่เกี่ยวข้องตลอดวงจรชีวิตข้อมูล • จัดทำนโยบาย มาตรการ วิธีการ และแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลที่สอดคล้องกับกฎหมาย ระเบียบ และแนวปฏิบัติของหน่วยงาน • จัดทำนโยบาย มาตรการ วิธีการ และแนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ เพื่อป้องกันการละเมิด การเข้าถึง การสูญหาย การทำลาย หรือการเปลี่ยนแปลงข้อมูล เช่น ➢ เจ้าของระบบ/CIO มีอำนาจในการพัฒนามาตรการควบคุมความปลอดภัยที่สูงกว่าระดับพื้นฐานความลับสูงสุดเพื่อจัดการความเสี่ยงเฉพาะ ➢ ควรมีมาตรการรักษาความมั่นคงปลอดภัยข้อมูลที่เหมาะสม เช่น การควบคุมการเข้าถึงฐานข้อมูล การเข้ารหัสข้อมูล การใช้เทคโนโลยี

[5] https://www.gov.uk/government/publications/government-security-classifications/guidance-13-working-at-top-secret-html#application-of-the-top-secret-baseline-behaviours

ข้อเสนอแนะเบื้องต้นต่อการบริหารจัดการข้อมูลที่ต้องได้รับความคุ้มครองสูงสุด[5]	
	กุญแจคู่ ตามที่ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติกำหนด ➢ มีการควบคุมเข้าถึงหรืออ่านข้อมูลที่ต้องได้รับการคุ้มครองสูงสุด เช่น มีการเข้ารหัสที่ซับซ้อนระหว่างการสร้าง การจัดเก็บ ➢ ห้ามส่งข้อมูลนอกระบบเครือข่าย Secure Isolated Network ➢ กำหนดล็อกอุปกรณ์ทุกครั้งเมื่อออกจากพื้นที่ทำงานทุกครั้ง
ข้อเสนอแนะต่อถิ่นที่อยู่ข้อมูล	• การใช้ศูนย์ข้อมูลหลักในประเทศไทยเท่านั้น • การกำหนดให้เจ้าของระบบ/CIO สามารถเข้าถึงและมีสิทธิในการบริหารจัดการข้อมูลบนคลาวด์ได้

ข้อเสนอแนะนี้เป็นเพียงข้อเสนอแนะเบื้องต้นในการจำแนกประเภทข้อมูลสำหรับใช้บริการคลาวด์และแนวทางการบริหารจัดการข้อมูลเพื่อใช้บริการคลาวด์เท่านั้น อย่างไรก็ดี ท่านควรศึกษา มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ว่าด้วยแนวทางการใช้คลาวด์ตามนโยบายการใช้คลาวด์เป็นหลัก เพิ่มเติม เพื่อประกอบการพิจารณา การเลือกประเภทของคลาวด์ และบริการคลาวด์ที่สอดคล้องกับนโยบายการใช้คลาวด์เป็นหลัก

3.2.2. ข้อมูลที่ต้องได้รับความคุ้มครอง (Protected Data)

ข้อมูลที่ต้องได้รับความคุ้มครอง คือ ประเภทข้อมูลในบริการที่มีความเสี่ยงปานกลาง ประกอบด้วย ข้อมูลที่มีความอ่อนไหวสูงที่จำเป็นต้องมีมาตรการควบคุมที่เข้มงวด และมีการกำหนดการใช้เครือข่ายที่ปลอดภัยบนโครงสร้างพื้นฐานทางกายภาพที่มีความปลอดภัย และมีการปฏิบัติอย่างเหมาะสม ซึ่งเหมาะสำหรับการคุ้มครองข้อมูลจากผู้ก่อภัยคุกคามซึ่งอาจส่งผลต่อชีวิต (บุคคลหรือกลุ่มบุคคล) หรือสร้างความเสียหายอย่างร้ายแรงต่อความมั่นคงของชาติ และ/หรือความสัมพันธ์ระหว่างประเทศ ความมั่นคง/เสถียรภาพทางการเงิน หรือขัดขวางความสามารถในการสืบสวนคดีอาชญากรรมที่ร้ายแรง หรือองค์กร ซึ่งข้อมูลประเภทนี้ได้แก่ ข้อมูลระดับ ชั้นเผยแพร่ภายในองค์กร ชั้นลับ และชั้นลับมาก โดยบริการที่มีข้อมูลประเภทนี้ ได้แก่ การบริการข้อมูลสำหรับการดำเนินการภายใน บริการ ERP ระบบเงินเดือน เป็นต้น

ทั้งนี้ เจ้าของระบบ/CIO จะต้องเป็นผู้ประเมินโดยประยุกต์จากเครื่องมือในหัวข้อ 3.1 สรุปได้ดังนี้

ตารางที่ 16: เกณฑ์การพิจารณาผลกระทบสำหรับข้อมูลที่ต้องได้รับความคุ้มครอง[6]

ด้าน	เกณฑ์การพิจารณาผลกระทบ		
	1 = ต่ำ	2 = ปานกลาง	3 = สูง
ชื่อเสียง	**น้อย/อย่างจำกัด** โดย ✓ ส่งผลกระทบเฉพาะภาพลักษณ์หน่วยงาน ใช่หรือไม่ ✓ ส่งผลกระทบต่อการรับรู้บทบาทหน้าที่ของหน่วยงาน ใช่หรือไม่	**อย่างร้ายแรง** โดย ✓ ส่งผลกระทบต่อภาพลักษณ์ของระบบการให้บริการ ใช่หรือไม่	**อย่างร้ายแรงมาก** โดย ✓ ส่งผลกระทบต่อภาพลักษณ์ชื่อเสียงของรัฐในระดับประเทศ ใช่หรือไม่ ✓ สามารถฟ้องร้องทางคดีแพ่ง ใช่หรือไม่ ✓ สามารถฟ้องร้องทางคดีอาญา ใช่หรือไม่

[6] สามารถกำหนดเกณฑ์การพิจารณาระดับผลกระทบให้สอดคล้องกับนโยบายและกฎระเบียบที่เกี่ยวข้อง และเหมาะสมกับบริบทขององค์กร

ด้าน	เกณฑ์การพิจารณาผลกระทบ		
	1 = ต่ำ	2 = ปานกลาง	3 = สูง
	✓ ส่งผลกระทบต่อภาพลักษณ์ของระบบการให้บริการ ใช่หรือไม่	✓ ส่งผลความเชื่อมั่นของผู้ใช้บริการ ใช่หรือไม่ ✓ สามารถฟ้องร้องทางคดีแพ่ง ใช่หรือไม่	
ผู้ใช้และการดำเนินงาน	**รายบริการ/การดำเนินงานขององค์กร** โดย ✓ ส่งผลกระทบต่อการทำงานภายในหน่วยงาน ใช่หรือไม่ ✓ ส่งผลกระทบต่อประสิทธิภาพการทำงานของผู้ปฏิบัติงานของหน่วยงานลดลง ใช่หรือไม่ ✓ ส่งผลการใช้งานของจำนวนผู้ใช้งานในวงแคบ ใช่หรือไม่	**ราย Domain/การดำเนินของกระทรวง/ระหว่าง องค์กร/จังหวัด** โดย ✓ ส่งผลให้เกิดอุปสรรคต่อการทำงานภายในหน่วยงาน และหน่วยงานคู่สัญญา ✓ ส่งผลต่อประสิทธิภาพการให้บริการของระบบ ✓ บางบริการมีความไม่สะดวก หรือล่าช้าเสียเวลา แต่ยังไม่สูญเสียข้อมูล ใช่หรือไม่ ✓ ส่งผลกระทบต่อผู้ใช้บริการบางส่วน ใช่หรือไม่	**Cross Domains, Sectors, Region/การดำเนินงานตามแผนบูรณาการ/กลุ่มจังหวัด** โดย ✓ ส่งผลกระทบต่อการทำงานภายในหน่วยงานเครือข่ายมากกว่า 2 หน่วยงาน ใช่หรือไม่ ✓ ส่งผลกระทบต่อผู้มาใช้บริการทุกคนและกระทบวงกว้างในระดับประเทศ ใช่หรือไม่ ✓ ระบบล่มหรือใช้งานไม่ได้ ทำให้เกิดความเสียหายของผู้ใช้บริการ ใช่หรือไม่ ✓ ข้อมูลในระบบสูญหายและไม่สามารถกู้คืนมา ใช่หรือไม่
การเงินและสินทรัพย์	**มูลค่าไม่เกิน 5 ล้าน/ Small project** โดย ✓ มูลค่าความเสียหายของการให้บริการหรือโครงการ เช่น ค่าดำเนินการ เช่น ค่าปรับ ค่าเยียวยา ค่าเสียหาย โดยมีมูลค่าไม่เกิน 5 ล้าน ใช่หรือไม่ ทั้งนี้ การพิจารณาเป็นตัวเงินและความสูญเสียหายของ Asset อาจเป็นเรื่องบทลงโทษทางกฎหมาย มูลค่าความเสียหาย ค่าดำเนินการต่างๆ	**ตั้งแต่ 5 ล้าน แต่ไม่ถึง 100 ล้าน/ Medium project** โดย ✓ มูลค่าความเสียหายของการให้บริการหรือโครงการ เช่น ค่าดำเนินการ เช่น ค่าปรับ ค่าเยียวยา ค่าเสียหาย โดยมีมูลค่า ตั้งแต่ 5 ล้าน แต่ไม่ถึง 50 ล้านบาท ใช่หรือไม่ ทั้งนี้ การพิจารณาเป็นตัวเงินและความสูญเสียหายของ Asset อาจเป็นเรื่องบทลงโทษทางกฎหมาย มูลค่าความเสียหาย ค่าดำเนินการต่างๆ	**ตั้งแต่ 100 ล้านบาท ขึ้นไป / Large Project** โดย ✓ มูลค่าความเสียหายของการให้บริการหรือโครงการ เช่น ค่าดำเนินการ เช่น ค่าปรับ ค่าเยียวยา ค่าเสียหาย โดยมีมูลค่าตั้งแต่ 100 ล้านบาท ใช่หรือไม่ ทั้งนี้ การพิจารณาเป็นตัวเงินและความสูญเสียหายของ Asset อาจเป็นเรื่องบทลงโทษทางกฎหมาย มูลค่าความเสียหาย ค่าดำเนินการต่างๆ
กฎหมายและระเบียบข้อบังคับ	**ละเว้นการปฏิบัติตามระเบียบข้อบังคับขององค์กร ซึ่งเกิดผลกระทบน้อย** โดย ✓ ไม่ปฏิบัติตามกฎระเบียบระดับองค์กร ใช่หรือไม่ ✓ ส่งผลให้หน่วยงานได้รับบทลงโทษของหน่วยงาน ใช่หรือไม่	**ละเว้นการปฏิบัติตามระเบียบข้อบังคับและกฎกระทรวง ซึ่งเกิดผลกระทบที่มีนัยสำคัญ และไม่เป็นไปตามเป้าของ ก.พ.ร.** โดย ✓ ไม่ปฏิบัติตามกฎระเบียบระดับกระทรวง เช่น กฎกระทรวง ใช่หรือไม่ ✓ ส่งผลให้หน่วยงานได้รับบทลงโทษทางอาญาและทางแพ่ง หรือ โทษทางปกครอง ใช่หรือไม่	**ละเว้นการปฏิบัติตามกฎหมาย มติ ครม. หรือระเบียบข้อบังคับ ซึ่งเกิดผลกระทบที่มีนัยสำคัญและไม่เป็นไปตามเป้าของแผนบูรณาการ/กลุ่มจังหวัด** โดย ✓ ไม่ปฏิบัติตามกฎหมายอย่างชัดเจน หรือไม่ปฏิบัติตามมติ ครม. รัฐบาล และไม่เป็นไปตามเป้าหมายของแผนบูรณาการ ใช่หรือไม่ ✓ ไม่ปฏิบัติตามกฎหมายส่งผลให้หน่วยงานได้รับบทลงโทษทางอาญาและทางแพ่ง หรือ โทษทางปกครอง ใช่หรือไม่
ระเบียบในผลประโยชน์แห่งชาติ	**ผลประโยชน์แห่งชาติสำคัญน้อย** โดย ✓ มีผลกระทบจากการเปิดเผยข้อมูลโดยไม่ได้อนุญาต ตามหลักการ CIA ในระดับต่ำ ใช่หรือไม่ ✓ การเปิดเผยข้อมูลจะส่งผลให้เกิดอันตรายต่อทรัพย์สิน/ชีวิต/ความปลอดภัยของบุคคลใดบุคคลหนึ่ง ใช่หรือไม่	**ผลประโยชน์แห่งชาติที่สำคัญ** โดย ✓ มีผลกระทบจากการเปิดเผยข้อมูลโดยไม่ได้อนุญาต ตามหลักการ CIA ในระดับปานกลาง ใช่หรือไม่ ✓ การเปิดเผยข้อมูลจะส่งผลให้เกิดอันตรายต่อทรัพย์สิน/ชีวิต/ความปลอดภัยของประชาชนบางส่วน ใช่หรือไม่	**ผลประโยชน์แห่งชาติที่สำคัญยิ่ง** โดย ✓ มีผลกระทบจากการเปิดเผยข้อมูลโดยไม่ได้อนุญาต ตามหลักการ CIA ในระดับสูง ใช่หรือไม่ ✓ การเปิดเผยข้อมูลจะส่งผลให้เกิดอันตรายต่อทรัพย์สิน/ชีวิต/ความปลอดภัยของประชาชนส่วนใหญ่ ใช่หรือไม่

ด้าน	เกณฑ์การพิจารณาผลกระทบ		
	1 = ต่ำ	2 = ปานกลาง	3 = สูง
		✓ สร้างความเสียหายต่อความสัมพันธ์ระหว่างหน่วยงานอื่นๆ ใช่หรือไม่	✓ เกิดความเสียหายต่อความมั่นคงของประเทศ หรือความสัมพันธ์ระหว่างประเทศ หรือความมั่นคงทางเศษฐกิจของประเทศใช่หรือไม่

หากใช้เกณฑ์ในประการเมินและได้คะแนนต่ำกว่า 10 คะแนนตามหัวข้อใน 3.1.1 จะเห็นได้ว่า ข้อมูลในบริการมีระดับความเสี่ยงที่องค์กรสามารถยอมรับได้ โดยมีมาตรการควบคุมความเสี่ยงและมีการติดตามเป็นระยะๆอย่างต่อเนื่อง อย่างไรก็ดี นอกจากการประเมินความเสี่ยงแล้ว เจ้าของระบบ/CIO ควรมีการพิจารณาประเด็นการกำหนดถิ่นที่อยู่ข้อมูล รายละเอียดดังนี้

ตารางที่ 17: แนวทางการพิจารณาถิ่นที่อยู่ข้อมูล

แนวทางการพิจารณาถิ่นที่อยู่ข้อมูล	
กฎหมายคุ้มครองข้อมูลส่วนบุคคล	ข้อ 1 ข้อมูลในบริการของท่านมีข้อมูลส่วนบุคคลประกอบด้วยหรือไม่ ● ตอบ ใช่ ขอให้ท่านนำข้อกำหนดภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคลเพื่อประกอบการพิจารณา ไปที่ข้อ 2 ● ตอบ ไม่ ขอให้ท่านพิจารณาคำถามในข้อ 3 ต่อไป ข้อ 2 ข้อมูลส่วนบุคคลในบริการนี้เป็นข้อมูลอ่อนไหวตามมาตรา 26 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือไม่ ● ตอบ ใช่ ข้อมูลของท่านควรมีการจัดเก็บในประเทศ อย่างไรก็ดี ขอให้ท่านนำข้อกำหนดภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคลเพื่อประกอบการพิจารณา ไปที่ข้อ 3 ● ตอบ ไม่ ขอให้ท่านพิจารณาคำถามในข้อ 3 ต่อไป
กฎหมายอื่นๆ ที่เกี่ยวข้อง	ข้อ 3 ข้อมูลในบริการมีกฎหมาย/ระเบียนกำหนดให้จัดเก็บเฉพาะในประเทศไทยหรือไม่ ● ตอบ ใช่ ข้อมูลในบริการของท่านสามารถจัดเก็บใน Public Cloud ในประเทศไทยเท่านั้น ● ตอบ ไม่ ข้อมูลในบริการท่านสามารถจัดเก็บใน Public Cloud ที่ต่างประเทศ หรือในประเทศก็ได้

เมื่อพิจารณาได้แล้วว่า เป็นข้อมูลประเภทต้องได้รับการคุ้มครอง สามารถเลือกใช้ **Public Cloud** เพื่อจัดเก็บข้อมูลได้ ซึ่งจะมีถิ่นที่อยู่ในประเทศไทยหรือนอกประเทศไทยก็ได้ แต่ควรมีการบริหารจัดการข้อมูลที่เหมาะสม ซึ่งเป็นการทำงานร่วมกันระหว่าง ผู้ปฏิบัติงานด้านสารสนเทศ ฝ่าย IT หรือ เจ้าของระบบงาน กับผู้ปฏิบัติงานด้านข้อมูลขององค์กร ได้แก่ เจ้าของข้อมูล ดังตัวอย่างต่อไปนี้

ตารางที่ 18: ข้อเสนอแนะเบื้องต้นต่อการบริหารจัดการข้อมูลต้องได้รับการคุ้มครอง

ข้อเสนอแนะเบื้องต้นต่อการบริหารจัดการข้อมูลต้องได้รับการคุ้มครอง	
ประเภทคลาวด์	• Public Cloud

ข้อเสนอแนะเบื้องต้นต่อการบริหารจัดการข้อมูลต้องได้รับการคุ้มครอง	
ข้อเสนอแนะต่อการบริหารจัดการตามกรอบธรรมาภิบาลข้อมูล	• กำหนดบทบาทผู้ที่เกี่ยวข้องกับกรอบธรรมาภิบาลข้อมูลภาครัฐ • จัดทำนโยบายและแนวปฏิบัติการบริหารจัดการข้อมูลเป็นลายลักษณ์อักษร เพื่อสนับสนุนการการดำเนินงาน เช่น ➢ เจ้าของระบบ/CIO เป็นผู้กำหนดสิทธิเจ้าของข้อมูลในการเข้าถึงข้อมูลได้เท่าที่จำเป็น (need to know basis) ➢ กำหนดบทบาทและแนวปฏิบัติของของเจ้าของข้อมูลและผู้ที่เกี่ยวข้องตลอดวงจรชีวิตข้อมูล • จัดทำนโยบาย มาตรการ วิธีการ และแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลที่สอดคล้องกับกฎหมาย ระเบียบ และแนวปฏิบัติของหน่วยงาน ➢ เงื่อนไขในการแบ่งปันข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 • จัดทำนโยบาย มาตรการ วิธีการ และแนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ เพื่อป้องกันการละเมิด การเข้าถึง การสูญหาย การทำลาย หรือการเปลี่ยนแปลงข้อมูล
ข้อเสนอแนะต่อถิ่นที่อยู่ข้อมูล	• หากไม่มีกฎหมายที่กำหนดเรื่องถิ่นที่อยู่ข้อมูลไว้โดยตรง ให้สามารถจัดเก็บข้อมูลไว้ที่ประเทศไทยหรือนอกประเทศก็ได้ ซึ่งเป็นดุลพินิจของเจ้าของระบบ/CIO โดยอำนาจอธิปไตยของข้อมูล (Data Sovereignty) จะต้องเป็นของหน่วยงานในการเข้าถึงและกำหนดสิทธิการเข้าถึงข้อมูล รวมถึงแนวทางการบริหารจัดการข้อมูล

ข้อเสนอแนะนี้เป็นเพียงข้อเสนอแนะเบื้องต้นในการจำแนกประเภทข้อมูลสำหรับใช้บริการคลาวด์และแนวทางการบริหารจัดการข้อมูลเพื่อใช้บริการคลาวด์เท่านั้น **ท่านควรศึกษา มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ว่าด้วยแนวทางการใช้คลาวด์ตามนโยบายการใช้คลาวด์เป็นหลัก เพิ่มเติมเพื่อประกอบการพิจารณาการเลือกป**ระเภทของคลาวด์ และบริการคลาวด์ ที่สอดคล้องกับนโยบายการใช้คลาวด์เป็นหลัก

3.2.3. ข้อมูลที่สามารถเปิดเผยได้ (Official Data)

ข้อมูลที่สามารถเปิดเผยได้ คือ ประเภทข้อมูลในบริการที่มีความเสี่ยงต่ำ เป็นข้อมูลที่สร้างประมวลผล ส่ง หรือรับของหน่วยงานภาครัฐและหน่วยงานที่เกี่ยวข้อง ซึ่งอาจก่อให้เกิดความเสียหายได้ไม่เกินความเสียหายในระดับต่ำ หากมีการละเมิดความปลอดภัยจะมีการใช้มาตรฐานการควบคุมที่สามารถคุ้มครองข้อมูลให้มีความปลอดภัยจากการโจมตีในรูปแบบต่าง ๆ ซึ่งอาจเพิ่มการรับรองมาตรการควบคุมได้ ประกอบด้วย ข้อมูลข่าวสารของราชการที่หน่วยงานของรัฐต้องเปิดเผยให้ประชาชนได้รับรู้ รับทราบ หรือตรวจสอบได้โดยไม่จำเป็นต้องร้องขอ ตามมาตรา 7 แห่งพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 เช่น กฎ มติคณะรัฐมนตรี ข้อบังคับ รายงานผลการ ศึกษาทางวิชาการ และข้อมูลเปิดภาครัฐ ฯลฯ โดยบริการที่มีข้อมูลประเภทนี้ ได้แก่ การบริการข้อมูลการดำเนินการของภาครัฐ การบริการแจ้งข่าวสารต่างๆ เป็นต้น

ทั้งนี้ เจ้าของระบบ/CIO จะต้องเป็นผู้ประเมินโดยประยุกต์จากเครื่องมือในหัวข้อ 3.1 สรุปได้ดังนี้

1 ตารางที่ 19: เกณฑ์การพิจารณาผลกระทบสำหรับข้อมูลที่สามารถเปิดเผยได้[7]

ด้าน	เกณฑ์การพิจารณาผลกระทบ		
	1 = ต่ำ	2 = ปานกลาง	3 = สูง
ชื่อเสียง	**น้อย/อย่างจำกัด** โดย ✓ ส่งผลกระทบเฉพาะภาพลักษณ์หน่วยงาน ใช่หรือไม่ ✓ ส่งผลกระทบต่อการรับรู้บทบาทหน้าที่ของหน่วยงาน ใช่หรือไม่ ✓ ส่งผลกระทบต่อภาพลักษณ์ของระบบการให้บริการ ใช่หรือไม่	**อย่างร้ายแรง** โดย ✓ ส่งผลกระทบต่อภาพลักษณ์ของระบบการให้บริการ ใช่หรือไม่ ✓ ส่งผลความเชื่อมั่นของผู้ใช้บริการ ใช่หรือไม่ ✓ สามารถฟ้องร้องทางคดีแพ่ง ใช่หรือไม่	**อย่างร้ายแรงมาก** โดย ✓ ส่งผลกระทบต่อภาพลักษณ์ชื่อเสียงของรัฐในระดับประเทศ ใช่หรือไม่ ✓ สามารถฟ้องร้องทางคดีแพ่ง ใช่หรือไม่ ✓ สามารถฟ้องร้องทางคดีอาญา ใช่หรือไม่
ผู้ใช้และการดำเนินงาน	**รายบริการ/การดำเนินงานขององค์กร** โดย ✓ ส่งผลกระทบต่อการทำงานภายในหน่วยงาน ใช่หรือไม่ ✓ ส่งผลกระทบต่อประสิทธิภาพการทำงานของผู้ปฏิบัติงานของหน่วยงานลดลง ใช่หรือไม่ ✓ ส่งผลการใช้งานของจำนวนผู้ใช้งานในวงแคบ ใช่หรือไม่	**ราย Domain/การดำเนินของกระทรวง/ระหว่าง องค์กร/จังหวัด** โดย ✓ ส่งผลให้เกิดอุปสรรคต่อการทำงานภายในหน่วยงาน และหน่วยงานคู่สัญญา ✓ ส่งผลต่อประสิทธิภาพการให้บริการของระบบ เช่น การบริการมีความไม่สะดวกหรือล่าช้า เสียเวลา แต่ยังไม่สูญเสียข้อมูล ใช่หรือไม่ ✓ ส่งผลกระทบต่อผู้ใช้บริการบางส่วน ใช่หรือไม่	**Cross Domains, Sectors, Region/การดำเนินงานตามแผนบูรณาการ/กลุ่มจังหวัด** โดย ✓ ส่งผลกระทบต่อการทำงานภายในหน่วยงานเครือข่ายมากกว่า 2 หน่วยงาน ใช่หรือไม่ ✓ ส่งผลกระทบต่อผู้มาใช้บริการทุกคนและกระทบวงกว้างในระดับประเทศ ใช่หรือไม่ ✓ ระบบล่มหรือใช้งานไม่ได้ ทำให้เกิดความเสียหายของผู้ใช้บริการ ใช่หรือไม่ ✓ ข้อมูลในระบบสูญหายและไม่สามารถกู้คืนมา หรือการกู้คืนมีโอกาสไม่สมบูรณ์ ใช่หรือไม่
การเงินและสินทรัพย์	**มูลค่าไม่เกิน 5 ล้าน/ Small project** โดย ✓ มูลค่าความเสียหายของการให้บริการหรือโครงการ เช่น ค่าดำเนินการ เช่น ค่าปรับ ค่าเยียวยา ค่าเสียหาย โดยมีมูลค่าไม่เกิน 5 ล้าน ใช่หรือไม่ ทั้งนี้ การพิจารณาเป็นตัวเงินและความสูญเสียหายของ Asset อาจเป็นเรื่องบทลงโทษทางกฎหมาย มูลค่าความเสียหาย ค่าดำเนินการต่างๆ	**ตั้งแต่ 5 ล้าน แต่ไม่ถึง 100 ล้านบาท/ Medium project** โดย ✓ มูลค่าความเสียหายของการให้บริการหรือโครงการ เช่น ค่าดำเนินการ เช่น ค่าปรับ ค่าเยียวยา ค่าเสียหาย โดยมีมูลค่า ตั้งแต่ 5 ล้าน แต่ไม่ถึง 100 ล้านบาท ใช่หรือไม่ ทั้งนี้ การพิจารณาเป็นตัวเงินและความสูญเสียหายของ Asset อาจเป็นเรื่องบทลงโทษทางกฎหมาย มูลค่าความเสียหาย ค่าดำเนินการต่างๆ	**ตั้งแต่ 100 ล้านขึ้นไป/ Large Project** โดย ✓ มูลค่าความเสียหายของการให้บริการหรือโครงการ เช่น ค่าดำเนินการ เช่น ค่าปรับ ค่าเยียวยา ค่าเสียหาย โดยมีมูลค่า ตั้งแต่ 100 ล้านบาทขึ้นไป ใช่หรือไม่ ทั้งนี้ การพิจารณาเป็นตัวเงินและความสูญเสียหายของ Asset อาจเป็นเรื่องบทลงโทษทางกฎหมาย มูลค่าความเสียหาย ค่าดำเนินการต่างๆ
กฎหมายและระเบียบข้อบังคับ	**ละเว้นการปฏิบัติตามระเบียบข้อบังคับขององค์กร ซึ่งเกิดผลกระทบน้อย** โดย ✓ ไม่ปฏิบัติตามกฎระเบียบระดับองค์กร ใช่หรือไม่ ✓ ส่งผลให้หน่วยงานได้รับบทลงโทษของหน่วยงาน ใช่หรือไม่	**ละเว้นการปฏิบัติตามระเบียบข้อบังคับและกฎกระทรวง ซึ่งเกิดผลกระทบที่มีนัยสำคัญ และไม่เป็นไปตามเป้าของ ก.พ.ร.** โดย ✓ ไม่ปฏิบัติตามกฎระเบียบระดับกระทรวง เช่น กฎกระทรวง ใช่หรือไม่ ✓ ส่งผลให้หน่วยงานได้รับบทลงโทษทางอาญาและทางแพ่ง หรือ โทษทางปกครอง ใช่หรือไม่	**ละเว้นการปฏิบัติตามกฎหมาย มติ ครม. หรือระเบียบข้อบังคับ ซึ่งเกิดผลกระทบที่มีนัยสำคัญ และไม่เป็นไปตามเป้าของแผนบูรณาการ/กลุ่มจังหวัด** โดย ✓ ไม่ปฏิบัติตามกฎหมายอย่างชัดเจน หรือไม่ปฏิบัติตามมติ ครม. รัฐบาล และไม่เป็นไปตามเป้าหมายของแผนบูรณาการ ใช่หรือไม่ ✓ ไม่ปฏิบัติตามกฎหมายส่งผลให้หน่วยงานได้รับบทลงโทษทางอาญา

[7] สามารถกำหนดเกณฑ์การพิจารณาระดับผลกระทบให้สอดคล้องกับนโยบายและกฎระเบียบที่เกี่ยวข้อง และเหมาะสมกับบริบทขององค์กร

ด้าน	เกณฑ์การพิจารณาผลกระทบ		
	1 = ต่ำ	2 = ปานกลาง	3 = สูง
			และทางแพ่ง หรือ โทษทางปกครอง ใช่หรือไม่
ผลประโยชน์แห่งชาติ	**ผลประโยชน์แห่งชาติสำคัญน้อย** โดย ✓ มีผลกระทบจากการเปิดเผยข้อมูลโดยไม่ได้อนุญาต ตามหลักการ CIA ในระดับต่ำ ใช่หรือไม่ ✓ การเปิดเผยข้อมูลจะส่งผลให้เกิดอันตรายต่อทรัพย์สิน/ชีวิต/ความปลอดภัยของบุคคลใดบุคคลหนึ่ง ใช่หรือไม่	**ผลประโยชน์แห่งชาติที่สำคัญ** โดย ✓ มีผลกระทบจากการเปิดเผยข้อมูลโดยไม่ได้อนุญาต ตามหลักการ CIA ในระดับปานกลาง ใช่หรือไม่ ✓ การเปิดเผยข้อมูลจะส่งผลให้เกิดอันตรายต่อทรัพย์สิน/ชีวิต/ความปลอดภัยของประชาชนบางส่วน ใช่หรือไม่ ✓ สร้างความเสียหายต่อความสัมพันธ์ระหว่างหน่วยงานอื่นๆ ใช่หรือไม่	**ผลประโยชน์แห่งชาติที่สำคัญยิ่ง** โดย ✓ มีผลกระทบจากการเปิดเผยข้อมูลโดยไม่ได้อนุญาต ตามหลักการ CIA ในระดับสูง ใช่หรือไม่ ✓ การเปิดเผยข้อมูลจะส่งผลให้เกิดอันตรายต่อทรัพย์สิน/ชีวิต/ความปลอดภัยของประชาชนส่วนใหญ่ ใช่หรือไม่ ✓ เกิดความเสียหายต่อความมั่นคงของประเทศ หรือความสัมพันธ์ระหว่างประเทศ หรือความมั่นคงทางเศษฐกิจของประเทศใช่หรือไม่

หากใช้เกณฑ์ในประการเมินและได้คะแนนต่ำกว่า 3 คะแนนตามหัวข้อใน 3.1.1 จะเห็นได้ว่า ข้อมูลในบริการมีความเสี่ยงระดับต่ำ ระดับความเสี่ยงที่องค์กรสามารถยอมรับได้อาจต้อง และมีการติดตามเป็นระยะๆ อย่างไรก็ดี นอกจากการประเมินความเสี่ยงแล้ว เจ้าของระบบ/CIO ควรมีการพิจารณาประเด็นที่เกี่ยวข้องเพิ่มเติมได้แก่ ถิ่นที่อยู่ข้อมูล รายละเอียดดังนี้

ตารางที่ 20: แนวทางการพิจารณาถิ่นที่อยู่ข้อมูล

แนวทางการพิจารณาถิ่นที่อยู่ข้อมูล	
กฎหมายคุ้มครองข้อมูลส่วนบุคคล	ข้อ 1 ข้อมูลในบริการของท่านมีข้อมูลส่วนบุคคลประกอบด้วยหรือไม่ ● ตอบ ใช่ ขอให้ท่านนำข้อกำหนดภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคลเพื่อประกอบการพิจารณา ไปที่ข้อ 2 ● ตอบ ไม่ ขอให้ท่านพิจารณาคำถามในข้อ 3 ต่อไป ข้อ 2 ข้อมูลส่วนบุคคลในบริการนี้เป็นข้อมูลอ่อนไหวตามมาตรา 26 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือไม่ ● ตอบ ใช่ ขอให้ท่านพิจารณาการประเมินความเสี่ยงอีกรอบ โดยใช้เกณฑ์ใน Protected ● ตอบ ไม่ ขอให้ท่านพิจารณาคำถามในข้อ 3 ต่อไป
กฎหมายอื่นๆที่เกี่ยวข้อง	ข้อ 3 ข้อมูลในบริการมีกฎหมาย/ระเบียบกำหนดให้จัดเก็บเฉพาะในประเทศไทยหรือไม่ ● ตอบ ใช่ ข้อมูลของท่านสามารถจัดเก็บใน Public Cloud ที่ในประเทศไทยเท่านั้น ● ตอบ ไม่ ข้อมูลของท่านสามารถจัดเก็บใน Public Cloud ที่ต่างประเทศ หรือในประเทศก็ได้

เมื่อพิจารณาได้แล้วว่า เป็นข้อมูลในบริการนี้สามารถเปิดเผยได้ และควรเลือกใช้ Public Cloud ซึ่งควรมีการบริหารจัดการข้อมูลที่เหมาะสม เป็นการทำงานร่วมกันระหว่าง ผู้ปฏิบัติงานด้านสารสนเทศ ฝ่าย IT หรือ เจ้าของระบบงาน กับผู้ปฏิบัติงานด้านข้อมูลขององค์กร ได้แก่ เจ้าของข้อมูล หน่วยงานควรมีการบริหารจัดการที่เหมาะสม ดังตัวอย่างต่อไปนี้

ตารางที่ 21: ข้อเสนอแนะเบื้องต้นต่อการบริหารจัดการข้อมูลที่สามารถเปิดเผยได้

ข้อเสนอแนะเบื้องต้นต่อการบริหารจัดการข้อมูลที่สามารถเปิดเผยได้	
ประเภทคลาวด์	• Public Cloud
ข้อเสนอแนะต่อการบริหารจัดการตามกรอบธรรมาภิบาลข้อมูล	• มีการกำหนดบทบาทผู้ที่เกี่ยวข้องกับกรอบธรรมาภิบาลข้อมูลภาครัฐ • มีกำหนดบทบาท หน้าที่ และความรับผิดชอบของเจ้าของข้อมูลเพื่อทำหน้าที่รับผิดชอบดูแลข้อมูลในบริการ และทำหน้าที่ในการบริหารจัดการข้อมูลนั้น ๆ • การควบคุมการเข้าถึงควรเป็นผู้ที่ได้รับการอนุญาตจากเจ้าของระบบ/CIO โดยกำหนดให้มีผู้ที่สามารถเข้าถึงข้อมูลได้เท่าที่จำเป็น (need to know basis) • มีการจัดทำนโยบายและแนวปฏิบัติการบริหารจัดการข้อมูลเป็นลายลักษณ์อักษรเพื่อสนับสนุนการปฏิบัติงานให้สอดคล้องตามนโยบาที่กล่าวมา • มีการกำหนดนโยบาย มาตรการ วิธีการ และแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของข้อมูล เพื่อป้องกันการละเมิด การเข้าถึง การสูญหาย การทำลาย หรือการเปลี่ยนแปลงข้อมูล • กำหนดมาตรการ วิธีการ และแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลที่สอดคล้องกับกฎหมาย ระเบียบ และแนวปฏิบัติของหน่วยงาน
ข้อเสนอแนะต่อถิ่นที่อยู่ข้อมูล	• หากไม่มีกฎหมายที่กำหนดเรื่องถิ่นที่อยู่ข้อมูลไว้โดยตรง ให้สามารถจัดเก็บข้อมูลไว้ที่ประเทศไทยหรือนอกประเทศก็ได้ โดยอำนาจอธิปไตยของข้อมูล (Data Sovereignty) ต้องเป็นของหน่วยงานในการเข้าถึงและกำหนดสิทธิการเข้าถึงข้อมูล รวมถึงแนวทางการบริหารจัดการข้อมูล

ข้อเสนอแนะนี้เป็นเพียงข้อเสนอแนะเบื้องต้นในการจำแนกประเภทข้อมูลสำหรับใช้บริการคลาวด์และแนวทางการบริหารจัดการข้อมูลเพื่อใช้บริการคลาวด์เท่านั้น อย่างไรก็ดี ท่านควรศึกษา มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ว่าด้วยแนวทางการใช้คลาวด์ตามนโยบายการใช้คลาวด์เป็นหลัก เพื่อประกอบการพิจารณา ประเภทของคลาวด์ และบริการคลาวด์ ที่สอดคล้องกับนโยบายการใช้คลาวด์เป็นหลัก

แนวทางการจำแนกประเภทข้อมูล

จากแนวทางการจำแนกประเภทข้อมูลสำหรับใช้บริการคลาวด์สามารถสรุปได้ว่า ประเภทข้อมูลทั้ง 3 ประเภทที่กล่าวมาด้านบน มี 2 ประเภทที่สามารถใช้กับคลาวด์ประเภท Public Cloud ได้ ได้แก่ ข้อมูลที่สามารถเปิดเผยได้และข้อมูลที่ต้องได้รับความคุ้มครอง เนื่องจากมีคะแนนความเสี่ยงที่ต่ำว่า 10 คะแนน ซึ่งเป็นความเสี่ยงที่จำเป็นต้องมีมาตรการควบคุมที่เข้มงวด โดยสามารถมีถิ่นที่อยู่ข้อมูลในประเทศหรือนอกประเทศก็ได้ขึ้นอยู่กับการพิจารณาของเจ้าของระบบ/CIO

ในทางกลับกัน ข้อมูลที่ต้องได้รับความคุ้มครองสูงสุด สามารถได้กับคลาวด์ประเภท Private Cloud ได้อย่างเดียวเท่านั้น เนื่องจากเป็นข้อมูลที่มีความเสี่ยงสูงและมีผลกระทบต่อประเทศ หากเปิดเผยจะก่อให้เกิดความสูญเสีย/ผลกระทบร้ายแรงที่สุด อาจทำให้ชื่อเสียงและการสูญเสียทางการเงิน/ทรัพย์สิน ต่อความมั่นคงและผลประโยชน์แห่งรัฐอย่างร้ายแรงหรือที่สำคัญยิ่งยวด (Vital) ซึ่งจำเป็นต้องมีการใช้เครือข่ายบนโครงสร้างพื้นฐานทางกายภาพที่มีความปลอดภัยสูง และมีการควบคุมความปลอดภัยอย่างเข้มงวด และต้องอยู่ในประเทศไทยเท่านั้น รายละเอียดดังภาพ

Government Cloud of Thailand

ระดับชั้นข้อมูล	ค่าระดับความเสี่ยง	ผลกระทบที่จะเกิดขึ้น	จำแนกประเภทข้อมูล	คำนิยามการจำแนกประเภทข้อมูล	ประเภทของบริการคลาวด์		ถิ่นที่อยู่ของข้อมูล
					Public Cloud	Private Cloud	
เปิดเผย (Open)	1 - 2	ระดับต่ำ (กระทบระดับบุคคล/องค์กร)	**Official Data**	ข้อมูลที่สร้าง ประมวลผล ส่ง หรือรับของหน่วยงานภาครัฐและหน่วยงานที่เกี่ยวข้อง ซึ่งอาจก่อให้เกิดความเสียหายได้ไม่เกินความเสียหายในระดับต่ำ หากมีการละเมิดความปลอดภัยจะมีการใช้มาตรฐานการควบคุมที่สามารถ**คุ้มครองข้อมูล**ให้มีความปลอดภัยจากการโจมตีในรูปแบบต่าง ๆ ซึ่งอาจเพิ่มการรับรองมาตรการควบคุมได้	✓		ไม่มีข้อกำหนด
เผยแพร่ภายในองค์กร (Private)	3 - 4	ระดับปานกลาง (กระทบระดับองค์กร/ประเทศ)	**Protected Data**	ข้อมูลที่มีความอ่อนไหวสูงที่จำเป็นต้องมีมาตรการควบคุมที่เข้มงวด และมีการกำหนดการใช้เครือข่ายที่ปลอดภัยบนโครงสร้างพื้นฐานทางกายภาพที่มีความปลอดภัย และมีการปฏิบัติอย่างเหมาะสม ซึ่งเหมาะสำหรับการ**คุ้มครองข้อมูล**จากผู้ก่อภัยคุกคามซึ่งอาจส่งผลต่อชีวิต (บุคคลหรือกลุ่มบุคคล) หรือสร้างความเสียหายอย่างร้ายแรงต่อความมั่นคงของชาติ และ/หรือความสัมพันธ์ระหว่างประเทศ ความมั่นคง/เสถียรภาพทางการเงิน หรือขัดขวางความสามารถในการสืบสวนคดีอาชญากรรมที่ร้ายแรง หรือองค์กร	✓		ควรอยู่ในประเทศไทย
ลับ (Confidential)	5 - 6						
ลับมาก (Secret)	7 - 9						
ลับที่สุด (Top Secret)	10-15	ระดับสูง (กระทบระดับองค์กร/ประเทศ อย่างร้ายแรง)	**Highly Protected Data**	ข้อมูลที่มีความอ่อนไหวเป็นพิเศษ ซึ่งส่งผลต่อความมั่นคงของชาติ หรือพันธมิตร และต้องการมาตรการควบคุมความปลอดภัยที่สูงมาก เพื่อป้องกันการละเมิดข้อมูลจากภัยคุกคามทั้งหมด โดยการใช้เครือข่ายบนโครงสร้างพื้นฐานทางกายภาพที่มีความปลอดภัยสูง และมีการคุ้มครองข้อมูลและควบคุมความปลอดภัยอย่างเข้มงวด ทั้งนี้ ข้อมูลข่าวสารลับที่สุดต้องปฏิบัติตามระเบียบความลับทางราชการ และ ระเบียบสารบรรณอิเล็กทรอนิกส์ โดยให้หัวหน้าหน่วยงานรัฐ ใช้ดุลพินิจในการนำข้อมูลเข้าคลาวด์โดยไม่ขัดกับกฎหมายที่เกี่ยวข้อง เช่น การสร้างผ่านคลาวด์ แต่ไม่รวมถึงขั้นตอนการเผยแพร่ (การนำส่ง)		✓	ต้องอยู่ในประเทศไทย

ภาพที่ 10: สรุปแนวทางการจำแนกประเภทข้อมูลสำหรับใช้บริการคลาวด์

3.3 ตัวอย่างการประเมินจำแนกประเภทข้อมูลสำหรับใช้บริการคลาวด์

ตัวอย่างการประเมินบริการทางดิจิทัล (E-Government Service)

ประเภทข้อมูล					
วัตถุประสงค์ด้านความปลอดภัย (CIA)	**ผลกระทบด้านความลับ (Confidentiality)**		**ผลกระทบด้านความถูกต้องครบถ้วนสมบูรณ์ ความคงสภาพ (Integrity)**		**ผลกระทบด้านความพร้อมใช้งานข้อมูล(Availability)**
	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบน้อย/อย่างจำกัด (limited) และเกิดผลประโยชน์แห่งชาติสำคัญน้อย (Less Important or Secondary National Interests)		การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบน้อย/อย่างจำกัด (limited) และเกิดผลประโยชน์แห่งชาติสำคัญน้อย (Less Important or Secondary National Interests)		การหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลข่าวสารหรือระบบสารสนเทศอาจส่งผลกระทบน้อย/อย่างจำกัด (limited) และเกิดผลประโยชน์แห่งชาติสำคัญน้อย (Less Important or Secondary National Interests)
ระดับผล CIA	**ปานกลาง** (2 คะแนน)		**ปานกลาง** (2 คะแนน)		**ต่ำ** (1 คะแนน)
ค่าเฉลี่ย CIA	**ปานกลาง 2** (1.67 ปัดเป็น 2 คะแนน)				
ผลกระทบ/ผลประโยชน์	**ภาพลักษณ์/ชื่อเสียง**	**ผู้ใช้และการดำเนินงาน**	**การเงินและสินทรัพย์**	**กฎหมายและระเบียบ**	**ผลประโยชน์แห่งชาติ** (ค่าเฉลี่ย CIA)
โอกาสที่จะเกิดขึ้น (Likelihood)	บ่อยครั้ง (4 คะแนน)	น้อยครั้ง (2 คะแนน)	น้อยครั้ง (2 คะแนน)	น้อยมาก (1 คะแนน)	น้อยมาก (2 คะแนน)
ประเมินหาระดับความรุนแรงของผลกระทบ (Impact)	สูง (3 คะแนน)	ต่ำ (1 คะแนน)	ปานกลาง (2 คะแนน)	น้อย (1 คะแนน)	ปานกลาง (2 คะแนน)
ความเสี่ยง (Likelihood x Impact)	12 คะแนน	2 คะแนน	4 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 แต่อาจต้องมีการติดตามเป็นระยะ ๆ
ลับ	5-6	ระดับความเสี่ยงที่องค์กรสามารถยอมรับได้โดยต้องมีมาตรการควบคุมหรือมีแผนการลดความเสี่ยง เพื่อลดความเสี่ยงให้ไปอยู่ในระดับต่ำและป้องกันไม่ให้ความเสี่ยงเพิ่มขึ้น
ลับมาก	7-9	ระดับความเสี่ยงที่องค์กรไม่สามารถยอมรับได้ และต้องจัดการลดความเสี่ยงให้ไปอยู่ในระดับต่ำลงโดยเร็ว โดยต้องจัดให้มีแผนการลดความเสี่ยงและป้องกันไม่ให้ความเสี่ยงกลับเพิ่มสูงขึ้นด้วย
ลับที่สุด	10 ขึ้นไป	ระดับความเสี่ยงที่องค์กรไม่สามารถยอมรับได้ และต้องจัดการลดความเสี่ยงให้ไปอยู่ในระดับต่ำลงในทันที หรืออาจมีการถ่ายโอนความเสี่ยง โดยต้องจัดให้มีแผนการลดความเสี่ยงและป้องกันไม่ให้ความเสี่ยงกลับเพิ่มสูงขึ้นด้วย [8]

[8] หน่วยงานสามารถชี้แจงได้ในกรณีที่บริการของหน่วยงานเป็นระดับชั้นลับที่สุดแต่ไม่สอดคล้องกับนโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติฯ

สรุป จากการบริการทางดิจิทัล (E-Government Service) มีผลระดับความเสี่ยงอยู่ที่ 5 คะแนน ระดับชั้นข้อมูลเป็นระดับชั้นลับ สามารถพิจารณาจำแนกเป็นประเภทข้อมูลเพื่อนำขึ้นคลาวด์ ข้อมูลที่ต้องได้รับความคุ้มครอง เลือกใช้คลาวด์ประเภท Public Cloud โดยถิ่นที่อยู่ข้อมูลจะอยู่ในประเทศ หรือนอกประเทศก็ได้ เป็นดุลพินิจของเจ้าของระบบงาน/CIO พิจารณาตามความเหมาะสมของการบริการ โดยต้องมีอำนาจในการเข้าถึงข้อมูลและกำหนดสิทธิผู้เข้าถึงข้อมูลบนคลาวด์ได้

4. ภาคผนวก

4.1 รายชื่อหน่วยงานตามนโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ

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	สำนักงานคณะกรรมการองกันและปราบปรามยาเสพติด
9. การป้องกันและบรรเทาสาธารณภัย	● ข้อมูลสาธารณภัยและแผนการบรรเทาทุกข์	กรมป้องกันและบรรเทาสาธารณภัย
10. การป้องกันและแก้ไขปัญหาความมั่นคงทางไซเบอร์	● ข้อมูลการโจมตีทางไซเบอร์และมาตรการในการป้องกัน	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
11. การป้องกันและแก้ไขปัญหาการก่อการร้าย	● ข้อมูลข่าวสารและข่าวกรองด้านการก่อการร้าย	สำนักงานสภาความมั่นคงแห่งชาติ
12. การสร้างดุลยภาพระหว่างประเทศ	● ข้อมูลภัยคุกคามระดับภูมิภาค ● ข้อมูลหมอกควันข้ามแดน	กระทรวงการต่างประเทศ
13. การบริหารจัดการภาวะฉุกเฉินด้านสาธารณสุข และโรคติดต่ออุบัติใหม่	● ข้อมูลรายชื่อผู้ป่วยติดต่อโรคอุบัติใหม่ ● ข้อมูลผลวินิจฉัยโรคอุบัติใหม่	กระทรวงสาธารณสุข

หมวดประเด็นความมั่นคง	ตัวอย่างชุดข้อมูล	หน่วยงาน
14. การพัฒนาศักยภาพการเตรียมพร้อมแห่งชาติ และการบริหารจัดการวิกฤตการณ์ระดับชาติ	● การแจ้งเตือนและการสั่งการระหว่างหน่วยงานและผู้ปฏิบัติภารกิจเมื่อเข้าสู่ภาวะวิกฤติระดับชาติ	สำนักงานสภาความมั่นคงแห่งชาติ
15. การพัฒนาระบบข่าวกรองแห่งชาติ	● ข้อมูลประเมินการตอบสนอง และแจ้งเตือนต่อสถานการณ์ต่อความมั่นคงของชาติ	สำนักข่าวกรองแห่งชาติ
16. การบูรณาการข้อมูลด้านความมั่นคง	● ข้อมูลการป้องกันและแก้ไขภัยคุกคามที่ส่งผลกระทบต่อความมั่นคงแห่งชาติ	กองอำนวยการรักษาความมั่นคงภายในราชอาณาจักร
17. การเสริมสร้างความมั่นคงเชิงพื้นที	● ข้อมูลความขัดแย้งทางพลังงาน อาหาร และน้ำ	กองอำนวยการรักษาความมั่นคงภายในราชอาณาจักร

1

5. บรรณานุกรม

Amazon. (ม.ป.ป.). *ข้อมูลเบื้องต้นเกี่ยวกับ AWS GovCloud (สหรัฐฯ) Region*. เข้าถึงได้จาก https://aws.amazon.com/th/govcloud-us/?whats-new-ess.sort-by=item.additionalFields.postDateTime&whats-new-ess.sort-order=desc.

Amazon. (ม.ป.ป.). *พื้นที่เก็บข้อมูลบนระบบคลาวด์คืออะไร*. เข้าถึงได้จาก https://aws.amazon.com/th/what-is/cloud-storage/.

Cloud.cio.gov. (ม.ป.ป.). *Federal Cloud Computing Strategy (Cloud Smart)*. เข้าถึงได้จาก https://cloud.cio.gov/.

Digital.gov. (ม.ป.ป.). *Cloud and infrastructure*. เข้าถึงได้จาก https://digital.gov/topics/cloud-and-infrastructure/.

Federal Information Processing Standard Publication. (2004). *Standards for Security Categorization of Federal Information and Information Systems.*

GOV.UK. (2023). *Government Cloud First policy*. เข้าถึงได้จาก https://www.gov.uk/guidance/government-cloud-first-policy.

GOV.UK. (ม.ป.ป.). *Cloud Strategic Roadmap for Defence*. เข้าถึงได้จาก https://www.gov.uk/government/publications/cloud-strategic-roadmap-for-defence/cloud-strategic-roadmap-for-defence.

Government Technology Agency (GovTech). (ม.ป.ป.). Government on Commercial Cloud (GCC 2.0). ใน Government on Commercial Cloud (GCC 2.0).

Intelligence.gov.au. (2024). *Australian Government Announces Top Secret Cloud*. เข้าถึงได้จาก https://www.intelligence.gov.au/news/top-secret-cloud.

ISO/IEC 27001:2022. (2022). *Information security, cybersecurity and privacy protection — Information security management systems — Requirements.*

Microsoft. (ม.ป.ป.). *ประโยชน์ของการประมวลผลแบบคลาวด์*. เข้าถึงได้จาก https://www.microsoft.com/th-th/windows-365/cloud-computing-advantages.

National Institute of Standards and Technology. (2024). *NIST SP 800-60 Guide for Mapping Types of Information and Systems to Security Categories.*

Oversight.house.gov. (ม.ป.ป.). *The State of the Cloud*. เข้าถึงได้จาก https://oversight.house.gov/hearing/oversight-it-subcommittee-committee-to-examine-cloud-solutions/.

Prinya.org. (2022). *งานระบบประมวลผลแบบคลาวด์ ภาครัฐ-เอกชน*. เข้าถึงได้จาก https://www.prinya.org/2022/02/26/%E0%B8%87%E0%B8%B2%E0%B8%99%E0%B8%A3%E0%B8%B0%E0%B8%9A%E0%B8%9A%E0%B8%9B%E0%B8%A3%E0%B8%B0%E0%B8%A1%E0%B8%A7%E0%B8%A5%E0%B8%9C%E0%B8%A5%E0%B9%81%E0%B8%9A%E0%B8%9A%E0%B8%84%E0%B8%84%E0%B8%A5%E0%B8%B2/.

Protectivesecurity.gov.au. (2024). *New Protective Security Policy Framework*. เข้าถึงได้จาก https://www.protectivesecurity.gov.au/.

Singapore Government Developer Portal. (ม.ป.ป.). *GCC Key Benefits*. เข้าถึงได้จาก https://www.developer.tech.gov.sg/products/categories/infrastructure-and-hosting/gcc/overview.html.

บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน). (2021). *5 ข้อดี ของบริการ Cloud ที่ช่วยให้ธุรกิจเติบโตอย่างมั่นคง*. เข้าถึงได้จาก https://www.tot.co.th/sme-tips/SME-tips/2021/02/08/.

ปิติยาศักดิ์ ดร.สราวุธ. (2561). *โครงการวิจัย นโยบายคลาวด์และการคุ้มครองข้อมูลส่วนบุคคลในระบบคลาวด์ระหว่างสหภาพยุโรป สหรัฐอเมริกา ออสเตรเลียและอาเซียน: มุมมองของไทย.*

สำนักนายกรัฐมนตรี. (2552). *ระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. 2552.*

สำนักข่าวกรองแห่งชาติ. (2544). *ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544.*

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ. (2566). *ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์.*

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ. (2567). *ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 .*

สำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ. (2540). *พระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. 2540 .*

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล. (2562). *พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562.*

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน). (2566). *มาตรฐานรัฐบาลดิจิทัลว่าด้วยกรอบธรรมาภิบาลข้อมูลภาครัฐ ฉบับปรับปรุง: แนวปฏิบัติ.*

สำนักงานพัฒนารัฐบาลดิทัล (องค์การมหาชน). (2565). *มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล ว่าด้วยหลักเกณฑ์การจัดระดับชั้นและการแบ่งปันข้อมูลภาครัฐ.*

สำนักงานสภาความมั่นคงแห่งชาติ. (2566). *นโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ (พ.ศ. 2566-2570).*

สำนักนายกรัฐมนตรี. (2564). *ระเบียบสำนักนายกรัฐมนตรีว่าด้วยงานสารบรรณ (ฉบับที่ 4) พ.ศ. 2564.*