มาตรฐานรัฐบาลดิจิทัล

Digital Government Standard

มรด. X-1 : 256X

DGS X -1 : 256X

DRAFT

ว่าด้วยแนวทางการจำแนกประเภทข้อมูลสำหรับการใช้คลาวด์ตามนโยบายการใช้คลาวด์เป็นหลัก

CLOUD DATA CLASSIFICATION GUIDELINE

เวอร์ชัน 1.0

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

สำนักนายกรัฐมนตรี

เอกสารฉบับนี้ถือเป็นทรัพย์สินของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ห้ามมิให้ทำการคัดลอก ทำซ้ำ เผยแพร่ ส่วนหนึ่งส่วนใดในเอกสารฉบับนี้ ในรูปแบบใด ๆ แก่บุคคลภายนอก โดยไม่ได้รับอนุญาต การฝ่าฝืนถือเป็นความผิดตามระเบียบของสำนักงานฯ

มาตรฐานรัฐบาลดิจิทัล

ว่าด้วยแนวทางการจำแนกประเภทข้อมูลสำหรับการใช้คลาวด์ตามนโยบายการใช้คลาวด์เป็นหลัก

DRAFT

มรด. X-1 : 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

คณะกรรมการพัฒนารัฐบาลดิจิทัล

วันที่ กรุณาเลือกวันที่ประกาศ

ประกาศในราชกิจจานุเบกษา ฉบับ.....(ชื่อฉบับ).....

เล่ม xxx ตอน...(พิเศษ)... xxx x วันที่ xx xxxxxx พ.ศ. xxx

เอกสารฉบับนี้ถือเป็นทรัพย์สินของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ห้ามมิให้ทำการคัดลอก ทำซ้ำ เผยแพร่ ส่วนหนึ่งส่วนใดในเอกสารฉบับนี้ ในรูปแบบใด ๆ แก่บุคคลภายนอก โดยไม่ได้รับอนุญาต การฝ่าฝืนถือเป็นความผิดตามระเบียบของสำนักงานฯ

คณะกรรมการพัฒนารัฐบาลดิจิทัล

ประธานกรรมการ

นายกรัฐมนตรี ประธานกรรมการ

มอบหมายและมอบอำนาจให้รองนายกรัฐมนตรี (นายประเสริฐ จันทรรวงทอง)

กรรมการ

รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

ปลัดสำนักนายกรัฐมนตรี

ปลัดกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม

ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

ผู้อำนวยการสำนักงบประมาณ

เลขาธิการคณะกรรมการข้าราชการพลเรือน

เลขาธิการคณะกรรมการพัฒนาระบบราชการ

เลขาธิการสภาพัฒนาการเศรษฐกิจและสังคมแห่งชาติ

กรรมการผู้ทรงคุณวุฒิในคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคม

กรรมการผู้ทรงคุณวุฒิในคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

กรรมการผู้ทรงคุณวุฒิในคณะกรรมการข้อมูลข่าวสารของราชการ

กรรมการผู้ทรงคุณวุฒิในคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

กรรมการผู้ทรงคุณวุฒิในคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์

กรรมการและเลขานุการ

ผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

ผู้ช่วยเลขานุการ

เจ้าหน้าที่สำนักงานพัฒนารัฐบาลดิจิทัล

DRAFT

คณะกรรมการจัดทำร่างมาตรฐาน ข้อกำหนด และหลักเกณฑ์
ภายใต้พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562

ที่ปรึกษา

นางไอรดา เหลืองวิไล	รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล รักษาการแทนผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

ประธานกรรมการ

ผู้ช่วยศาสตราจารย์ณัฐวุฒิ หนูไพโรจน์	จุฬาลงกรณ์มหาวิทยาลัย

รองประธานกรรมการ

นายอาศิส อัญญะโพธิ์	รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

กรรมการ

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

กรรมการและเลขานุการ

นางสาวอุรัชฎา เกตุพรหม	ผู้อำนวยการฝ่ายมาตรฐานดิจิทัลภาครัฐ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

DRAFT

คณะทำงานเทคนิคด้านมาตรฐานการบริหารจัดการข้อมูลภาครัฐ

ที่ปรึกษา

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

ประธานคณะทำงาน

รองศาสตราจารย์ธีรณี อจลากุล	ผู้อำนวยการสถาบันข้อมูลขนาดใหญ่ (องค์การมหาชน)

รองประธานกรรมการ

ผู้ช่วยศาสตราจารย์โษฆศ์รัตต ธรรมบุษดี	มหาวิทยาลัยมหิดล

คณะทำงาน

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

คณะทำงานและเลขานุการ

นางสาวอุรัชฎา เกตุพรหม	ผู้อำนวยการฝ่ายมาตรฐานดิจิทัลภาครัฐ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

ผู้ช่วยเลขานุการ

นางสาวสุภัทรา เรืองวานิช	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

DRAFT

วิเคราะห์และจัดทำมาตรฐานรัฐบาลดิจิทัล

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

DRAFT

แนวทางการจำแนกประเภทข้อมูลสำหรับการใช้คลาวด์ตามนโยบายการใช้คลาวด์เป็นหลัก เวอร์ชัน 1.0 จัดทำขึ้น เพื่อเป็นแนวทางให้กับภาครัฐพิจารณาจำแนกประเภทข้อมูล เพื่อนำข้อมูลจัดเก็บในระบบคลาวด์ภาครัฐที่มีความเหมาะสมกับประเภทข้อมูลเป็นลำดับแรก โดยแนวทางฉบับนี้ได้จัดทำตามแนวมาตรฐานและแนวปฏิบัติที่ดีของ

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

และได้มีการจัดงานประชาพิจารณ์เพื่อเปิดรับฟังความคิดเห็นเป็นการทั่วไป และนำข้อมูล ข้อสังเกต ข้อคิดเห็นจากผู้ทรงคุณวุฒิและจากหน่วยงานที่เกี่ยวข้อง เพื่อให้ข้อเสนอแนะเกี่ยวกับมาตรฐานฉบับนี้มีความสมบูรณ์ครบถ้วน และสามารถนำไปปรับใช้ในทางปฏิบัติได้อย่างมีประสิทธิภาพ

แนวทางการจำแนกประเภทข้อมูลสำหรับการใช้คลาวด์ตามนโยบายการใช้คลาวด์เป็นหลัก 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-g2_division@dga.or.th
Website: www.dga.or.th

DRAFT

คำนำ

จากนโยบาย "Go Cloud First" ที่คณะรัฐมนตรีได้แถลงเมื่อวันที่ 11 กันยายน พ.ศ. 2566 รัฐบาลได้ขับเคลื่อนการใช้เทคโนโลยีคลาวด์เป็นหลัก โดยมีการแต่งตั้งคณะอนุกรรมการด้านบริหารจัดการความต้องการใช้คลาวด์ (Demand) การใช้บริการคลาวด์ (Supply) และมาตรฐานสำหรับการบริหารจัดการบริการคลาวด์ภาครัฐ (Government Cloud Management) และแต่งตั้งคณะอนุกรรมการด้านกฎหมายการจัดซื้อจัดจ้างบริการคลาวด์ภาครัฐ ผลจากการดำเนินงานและข้อสรุปที่ผ่านมา ได้นำไปสู่การจัดทำข้อเสนอกรอบแนวทางการบริหารจัดการคลาวด์ภาครัฐ และวางแผนจัดทำแนวปฏิบัติที่เกี่ยวข้อง 3 ด้าน ได้แก่ แนวปฏิบัติด้านความต้องการการใช้คลาวด์, แนวทางการจำแนกประเภทข้อมูลสำหรับการใช้คลาวด์ และแนวทางการขึ้นทะเบียนผู้ให้บริการคลาวด์ (Cloud Service Provider) ซึ่งได้รับความเห็นชอบจากคณะกรรมการพัฒนารัฐบาลดิจิทัลแล้ว

การขับเคลื่อนนี้สอดคล้องกับ ยุทธศาสตร์ชาติ 20 ปี ที่ให้ความสำคัญกับการใช้เทคโนโลยีคลาวด์เป็นเครื่องมือสำคัญในการยกระดับกระบวนการทำงานและการให้บริการประชาชนสู่รัฐบาลดิจิทัลอย่างรวดเร็ว นอกจากนี้ พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 ยังกำหนดให้หน่วยงานของรัฐต้องจัดบริการภาครัฐในรูปแบบดิจิทัลที่สะดวก รวดเร็ว มีประสิทธิภาพ บูรณาการข้อมูลอย่างมั่นคงปลอดภัย และมีธรรมาภิบาล ซึ่งล้วนเป็นปัจจัยที่ทำให้กรอบแนวทางการบริหารจัดการระบบคลาวด์ภาครัฐ มีความจำเป็นอย่างยิ่ง เพื่อสนับสนุนให้หน่วยงานภาครัฐสามารถพิจารณาและใช้คลาวด์เป็นหลักในการก้าวสู่การเป็นรัฐบาลดิจิทัลอย่างสมบูรณ์

มาตรฐานรัฐบาลดิจิทัลว่าด้วยแนวทางการจำแนกประเภทข้อมูลสำหรับการใช้คลาวด์ตามนโยบายการใช้คลาวด์เป็นหลัก จัดทำขึ้นเพื่อให้หน่วยงานภาครัฐนำไปใช้เป็นเกณฑ์พิจารณาแนวทางการจำแนกประเภทข้อมูลสำหรับการใช้คลาวด์ตามนโยบายการใช้คลาวด์เป็นหลัก โดยประยุกต์แนวทางการพิจารณาจากแบบประเมินการจัดระดับชั้นข้อมูลภาครัฐ ซึ่งเป็นการประเมินความเสี่ยงจากผลกระทบของการเปิดเผยข้อมูลภาพรวมของบริการโดยไม่ได้รับอนุญาต โดยยังคงธำรงไว้ซึ่งความเป็นเจ้าของอธิปไตยข้อมูล (Data Sovereignty) ของประเทศอย่างเคร่งครัด และในขณะเดียวกันก็ เปิดกว้างสำหรับโอกาสในการพัฒนา ร่วมกับทุกภาคส่วน เพื่อสนับสนุนการนำข้อมูลจัดเก็บในคลาวด์ภาครัฐที่มีความเหมาะสมกับประเภทข้อมูลต่อไป

DRAFT

สารบัญ

1. บทนำ 1

1.1 ความเป็นมา 1

1.2 วัตถุประสงค์ 3

1.3 ขอบข่าย 3

1.4 บทนิยาม 4

1.5 กฎหมายและแนวทางที่เกี่ยวข้อง 5

2. แนวคิดการใช้คลาวด์ตามนโยบายการใช้คลาวด์เป็นหลัก 6

2.1 ความสำคัญของระบบคลาวด์ต่อหน่วยงานภาครัฐในต่างประเทศ 8

2.2 ความสำคัญของอธิปไตยข้อมูล (Data Sovereignty) และการจัดเก็บข้อมูลในประเทศ (Data Localization) 17

3. แนวทางการจำแนกประเภทข้อมูลสำหรับการใช้คลาวด์ในประเทศไทย 21

3.1 แนวทางการจำแนกประเภทข้อมูลกับการใช้คลาวด์ 24

3.1.1. ข้อมูลที่ต้องได้รับความคุ้มครองสูงสุด (Highly Protected Data) 26

3.1.2. ข้อมูลที่ต้องได้รับความคุ้มครอง (Protected Data) 26

3.1.3. ข้อมูลที่สามารถเปิดเผยได้ (Official Data) 27

3.2 ตัวอย่างการประเมินจำแนกประเภทข้อมูลสำหรับการใช้คลาวด์ 31

4. ภาคผนวก 39

4.1 รายชื่อหน่วยงานตามนโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ 39

5. บรรณานุกรม 41

DRAFT

สารบัญภาพ

ภาพที่ 1: การจำแนกประเภทข้อมูล.....1
ภาพที่ 2: ขั้นตอนในการเตรียมองค์กรเข้าสู่การประมวลผลข้อมูลแบบคลาวด์ (Prinya.org, 2022).....16
ภาพที่ 3: รูปแบบการพิจารณาถิ่นที่อยู่ข้อมูล 17
ภาพที่ 4: กรอบแนวทางการจำแนกประเภทข้อมูลสำหรับการใช้คลาวด์ 21
ภาพที่ 6: แผนผังการตัดสินใจสำหรับการจำแนกประเภทข้อมูลสำหรับการใช้คลาวด์.....25
ภาพที่ 7: สรุปแนวทางการจำแนกประเภทข้อมูลสำหรับการใช้คลาวด์.....30
ภาพที่ 8: ผลกระทบตาม CIA ตามประกาศ กมช. เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566.....32
ภาพที่ 9: วิธีการประเมินความเสี่ยง.....38
ภาพที่ 10: การติดป้ายหรือแท็กกำกับระดับชั้นข้อมูลตามความอ่อนไหว.....38

DRAFT

สารบัญตาราง

ตารางที่ 1: หลักการสำคัญของนโยบายของสหราชอาณาจักร 9
ตารางที่ 2: การจำแนกประเภทข้อมูลและตัวอย่างการใช้งานของสหราชอาณาจักร 9
ตารางที่ 3: หลักการสำคัญของ Cloud Smart ของสหรัฐอเมริกา 11
ตารางที่ 4: การจำแนกประเภทข้อมูลและตัวอย่างการใช้งานของสหรัฐอเมริกา 11
ตารางที่ 5: หลักการและแนวคิดหลักของนโยบายของออสเตรเลีย 13
ตารางที่ 6: การจำแนกประเภทข้อมูลและตัวอย่างการใช้งานของออสเตรเลีย 13
ตารางที่ 7: หลักการสำคัญของแพลตฟอร์ม GCC 14
ตารางที่ 8: การจำแนกประเภทข้อมูลและตัวอย่างการใช้งานของสิงคโปร์ 15
ตารางที่ 9: ตารางเปรียบเทียบรูปแบบของถิ่นที่อยู่ข้อมูล 18
ตารางที่ 10: การจำแนกประเภทข้อมูลของประเทศไทย 22
ตารางที่ 11: ลักษณะผลกระทบระดับต่ำ 33
ตารางที่ 12: ลักษณะผลกระทบระดับกลาง 33
ตารางที่ 13: ลักษณะผลกระทบระดับสูง 33

DRAFT

มาตรฐานรัฐบาลดิจิทัลว่าด้วยแนวทางการจำแนกประเภทข้อมูล สำหรับการใช้คลาวด์ตามนโยบายการใช้คลาวด์เป็นหลัก

1. บทนำ

มาตรฐานรัฐบาลดิจิทัลว่าด้วยแนวทางการจำแนกประเภทข้อมูลสำหรับการใช้คลาวด์ตามนโยบายการใช้คลาวด์เป็นหลักฉบับนี้ มีวัตถุประสงค์ในการทำข้อมูลสารสนเทศให้มีความพร้อม เพื่อใช้บริการคลาวด์ **โดยไม่ได้เน้นการนำข้อมูลทั้งหมดขึ้นคลาวด์ แต่ต้องการให้มีการพิจารณาใช้คลาวด์ที่เหมาะสมกับระดับชั้นข้อมูล** ซึ่งดำเนินการโดยฝ่ายเทคโนโลยีสารสนเทศของหน่วยงาน โดยพิจารณาข้อมูลที่มีการใช้งานจากเจ้าของข้อมูล เช่น ฝ่ายบุคคล ฝ่ายแผนและยุทธศาสตร์ ซึ่งได้จัดระดับชั้นข้อมูล แบ่งได้ 5 ระดับชั้น ได้แก่ ระดับเปิดเผย ระดับเผยแพร่ภายในองค์กร ระดับลับ ระดับลับมาก ระดับลับที่สุด ตาม มสพร. 8-2565 มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล ว่าด้วยหลักเกณฑ์การจัดระดับชั้นและการแบ่งปันข้อมูลภาครัฐ และฉบับปรับปรุง มาจัดเตรียมข้อมูลสารสนเทศตามกลุ่มประเภทข้อมูล แบ่งออกเป็น 3 ประเภท ได้แก่

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

ระดับชั้นข้อมูล	ประเภทข้อมูล	รายละเอียด
เปิดเผย	Official	ข้อ 3.1.3
เผยแพร่ภายในองค์กร		
ลับ	Protected	ข้อ 3.1.2
ลับมาก	Highly Protected	ข้อ 3.1.1
ลับที่สุด		

ภาพที่ 1: การจำแนกประเภทข้อมูล

ในกรณีที่เจ้าของข้อมูลร่วมกับฝ่ายเทคโนโลยีสารสนเทศมีการประเมินจัดระดับชั้นข้อมูล โดยมีความเข้าใจตรงกันตามวัตถุประสงค์ของบริการที่สอดคล้องกับพันธกิจของหน่วยงานแล้ว สามารถนำผลการประเมินระดับชั้นข้อมูลเทียบเคียงกับประเภทข้อมูลสำหรับการใช้คลาวด์ได้ โดยศึกษารายละเอียดได้ที่ข้อ 3.1 แนวทางการจำแนกประเภทข้อมูลกับการใช้คลาวด์

1.1 ความเป็นมา

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

1. การบริหารจัดการความต้องการใช้คลาวด์ (Demand)
2. การบริหารจัดการให้มีบริการคลาวด์อย่างเพียงพอ (Supply)
3. กรอบกลไกการบริหารจัดการการใช้งานคลาวด์ของหน่วยงานภาครัฐ (กรอบกลไก Government Cloud Management)

4. การปรับปรุงระบบนิเวศการใช้คลาวด์ เพื่อเชื่อมโยงฝั่งผู้ใช้บริการ (Demand) และผู้ให้บริการ (Supply)

เมื่อวันที่ 25 มิถุนายน 2567 คณะรัฐมนตรี มีมติเห็นชอบแต่งตั้งคณะกรรมการเฉพาะด้านการขับเคลื่อนตามนโยบายการใช้คลาวด์เป็นหลักและให้คณะกรรมการพัฒนารัฐบาลดิจิทัล เป็นผู้ดำเนินการกำหนดรายละเอียดที่เกี่ยวข้องกับนโยบายการใช้คลาวด์ การดำเนินการของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ภายใต้คณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ พิจารณาเห็นชอบแนวทางการขับเคลื่อนตามนโยบายการใช้คลาวด์เป็นหลัก (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 จัดการความต้องการใช้คลาวด์ (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 เพื่อสร้างและพัฒนากระบวนการทำงานของหน่วยงานของรัฐให้มีความสอดคล้องและมีการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างกัน รวมทั้งมีความมั่นคงปลอดภัยและน่าเชื่อถือ โดยมีการบูรณาการและสามารถทำงานร่วมกันอย่างเป็นเอกภาพเกิดการพัฒนาการบริการภาครัฐที่มีประสิทธิภาพและนำไปสู่การบริหารราชการและการบริการประชาชน แบบบูรณาการ รวมทั้งให้ประชาชนเข้าถึงได้โดยสะดวก และมีมติให้เสนอคณะกรรมการพัฒนารัฐบาลดิจิทัลต่อไป

คณะกรรมการพัฒนารัฐบาลดิจิทัล ได้มอบหมายให้ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) จัดทำแนวทางการจำแนกประเภทข้อมูลสำหรับการใช้คลาวด์ เพื่อเป็นข้อเสนอแนะให้กับหน่วยงานภาครัฐในการนำไปเป็นแนวทางการพิจารณาข้อมูลเพื่อนำไปจัดเก็บในระบบคลาวด์ที่มีความเหมาะสมกับการให้บริการของหน่วยงาน โดยจัดกลุ่มประเภทข้อมูลสารสนเทศในภาพรวมของการให้บริการ (Service) เปรียบเทียบผลกระทบและความเสี่ยงที่อาจเกิดกับข้อมูล นำไปสู่การพิจารณาประเภทของคลาวด์ที่เหมาะสมกับบริการของ

DRAFT

หน่วยงาน เพื่อให้ข้อมูลมีความมั่นคงปลอดภัยและยังเป็นการพัฒนาขีดความสามารถในการให้บริการแก่ประชาชนเพื่อให้เกิดการเป็นรัฐบาลดิจิทัลอย่างแท้จริง

1.2 วัตถุประสงค์

เอกสารฉบับนี้จัดทำขึ้นเพื่อเป็น แนวทางการจำแนกประเภทข้อมูลสำหรับการใช้คลาวด์ตามนโยบายการใช้คลาวด์เป็นหลัก (Cloud First Policy) โดยมีวัตถุประสงค์หลักดังนี้

1) เพื่อให้หน่วยงานภาครัฐ สามารถให้บริการ ทำงานร่วมกัน และแบ่งปันข้อมูลระหว่างหน่วยงานภาครัฐได้อย่างมีประสิทธิภาพมากยิ่งขึ้นด้วยการเข้าถึงข้อมูลจากทุกที่และทุกเวลา
2) เพื่อเพิ่มประสิทธิภาพการรักษาความปลอดภัยและคุ้มครองข้อมูล ลดความเสี่ยงจากการถูกละเมิดหรือการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต รวมถึงการสูญหายของข้อมูล โดยเสนอแนะแนวทางให้หน่วยงานภาครัฐสามารถเลือกผู้ให้บริการคลาวด์ที่เหมาะสมสอดคล้องกับระดับความสำคัญ และความอ่อนไหวของข้อมูล

ทั้งนี้ วัตถุประสงค์ของการจำแนกประเภทข้อมูลสำหรับการใช้คลาวด์ ไม่ได้มุ่งเน้นให้หน่วยงานนำข้อมูลทั้งหมดขึ้นสู่ระบบคลาวด์ หากแต่ต้องการให้หน่วยงานเลือกใช้บริการคลาวด์ที่เหมาะสมและสอดคล้องกับระดับชั้นของข้อมูลแต่ละประเภท เพื่อให้เกิดประโยชน์สูงสุดทั้งด้านประสิทธิภาพและความมั่นคงปลอดภัย

1.3 ขอบข่าย

แนวทางการจำแนกประเภทข้อมูลสำหรับการใช้คลาวด์ ฉบับนี้จัดทำขึ้น**เพื่อให้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO) /เจ้าของระบบงาน (System Owner) หน่วยงานนำไปใช้เป็นเกณฑ์พิจารณาแนวทางการจำแนกประเภทข้อมูลสำหรับการใช้คลาวด์ตามนโยบายการใช้คลาวด์เป็นหลัก** ประยุกต์แนวทางการพิจารณาจากแบบประเมินระดับชั้นข้อมูลภาครัฐ ซึ่งเป็นการประเมินความเสี่ยงของข้อมูล ที่เกิดจากผลกระทบของการเปิดเผยข้อมูลของบริการโดยไม่ได้รับอนุญาต โดยแนวทางฉบับนี้ได้จัดทำตามแนวมาตรฐานและแนวปฏิบัติที่ดีของ

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

2) ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2566 (สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ, 2567)

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

4) ประกาศสำนักคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง แนวทางการใช้บริการคลาวด์สาธารณะที่มีศูนย์ข้อมูลหลักในประเทศ ไทย พ.ศ. 2567 (สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ, 2567)

DRAFT

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

6) 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)

7) 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) และร่างระเบียบว่าด้วยการรักษาความลับของทางราชการ (ฉบับที่ ..) พ.ศ. .... ร่างคู่มือแนวทางการปฏิบัติข้อมูลข่าวสารลับอิเล็กทรอนิกส์ ซึ่งอยู่ระหว่างการประกาศ

1.4 บทนิยาม

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

ข้อมูลที่สามารถเปิดเผยได้ (Official Data) หมายความว่า ข้อมูลที่สร้าง ประมวลผล ส่ง หรือรับของหน่วยงานภาครัฐและหน่วยงานที่เกี่ยวข้อง ซึ่งอาจก่อให้เกิดความเสียหายได้ไม่เกิน**ความเสียหายในระดับต่ำ** หากมีการละเมิดความปลอดภัยจะมีการใช้มาตรฐานการควบคุมที่สามารถคุ้มครองข้อมูลให้มีความปลอดภัยจากการโจมตีในรูปแบบต่างๆ ซึ่งอาจเพิ่มการรับรองมาตรการควบคุม

ข้อมูลที่ต้องได้รับความคุ้มครอง (Protected Data) หมายความว่า ข้อมูลที่มีความอ่อนไหวสูงที่จำเป็นต้องมีมาตรการควบคุมที่เข้มงวด และมีการกำหนดการใช้เครือข่ายที่ปลอดภัยบนโครงสร้างพื้นฐานทางกายภาพที่มีความปลอดภัย และมีการปฏิบัติอย่างเหมาะสม ซึ่งอาจส่งผลต่อชีวิต (บุคคลหรือกลุ่มบุคคล) หรือสร้าง**ความเสียหายต่อรัฐ**ซึ่งส่งผลต่อความมั่นคงของชาติ และ/หรือความสัมพันธ์ระหว่างประเทศ ความมั่นคง/เสถียรภาพทางการเงิน หรือขัดขวางความสามารถในการสืบสวนคดีอาชญากรรมที่ร้ายแรง หรือองค์กร

ข้อมูลที่ต้องได้รับความคุ้มครองสูงสุด (Highly Protected Data) หมายความว่า ข้อมูลที่มีความอ่อนไหวเป็นพิเศษ หากเปิดเผย**อาจเกิดความเสียหายอย่างร้ายแรงและร้ายแรงที่สุดต่อรัฐ**ซึ่งส่งผลความมั่นคงของชาติหรือพันธมิตร และต้องการมาตรการควบคุมความปลอดภัยที่สูงมาก เพื่อป้องกันการละเมิดข้อมูลจากภัยคุกคามทั้งหมด โดยการใช้เครือข่ายบนโครงสร้างพื้นฐานทางกายภาพที่มีความปลอดภัยสูง และมีการควบคุมความปลอดภัยอย่างเข้มงวด **ทั้งนี้ ข้อมูลข่าวสารลับที่สุดต้องปฏิบัติตามระเบียบความลับ**

ทางราชการ และ ระเบียบสารบรรณอิเล็กทรอนิกส์ โดยให้หัวหน้าหน่วยงานของรัฐใช้ดุลพินิจในการนำข้อมูลเข้าคลาวด์โดยไม่ขัดกับกฎหมายที่เกี่ยวข้อง เช่น การสร้างข้อมูลผ่านคลาวด์ แต่ไม่รวมถึงขั้นตอนการเผยแพร่หรือการนำส่ง

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

คลาวด์สาธารณะ (Public Cloud) หมายความว่า บริการคลาวด์ที่เปิดให้บริการแก่ผู้ใช้บริการทั่วไป โดยทรัพยากรทั้งหมดอยู่ภายใต้การควบคุมของผู้ให้บริการคลาวด์

คลาวด์อธิปไตย (Sovereign Cloud) หมายความว่า บริการคลาวด์ที่ฮาร์ดแวร์และข้อมูลทั้งหมดตั้งอยู่ในราชอาณาจักรไทย และเป็นบริการคลาวด์ที่ให้บริการโดยหน่วยงานของรัฐ หรือองค์กรที่รัฐบาลเป็นเจ้าของทั้งหมดหรือส่วนใหญ่ หรือมีอำนาจควบคุม รวมถึงต้องเป็นบริการคลาวด์ที่ให้หน่วยงานของรัฐใช้งานเท่านั้น

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) ระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. 2552 และที่แก้ไขเพิ่มเติม

4) พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562

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

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

7) ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ พ.ศ. 2563 และ ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง มาตรฐานรัฐบาลดิจิทัลว่าด้วยว่าด้วยกรอบธรรมาภิบาลข้อมูลภาครัฐ ฉบับปรับปรุง: แนวปฏิบัติ พ.ศ. 2566

DRAFT

8) ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566

9) ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567

ทั้งนี้ หากมีกฎหมายอื่นๆ ที่เกี่ยวข้อง สามารถใช้ประกอบการพิจารณาได้

2. แนวคิดการใช้คลาวด์ตามนโยบายการใช้คลาวด์เป็นหลัก

การนำเทคโนโลยีคลาวด์มาใช้ในภาครัฐของประเทศไทยเป็นส่วนสำคัญในการยกระดับประสิทธิภาพและความโปร่งใสของการให้บริการสาธารณะ ซึ่งสอดคล้องกับเป้าหมายของ ยุทธศาสตร์ชาติ (พ.ศ. 2561-2580) และยังช่วยลดต้นทุนด้านเทคโนโลยีสารสนเทศในระยะยาวอีกด้วย ตลอดหลายปีที่ผ่านมา รัฐบาลไทยได้ส่งเสริมการใช้งานคลาวด์อย่างต่อเนื่องผ่านนโยบายและแผนการพัฒนาดิจิทัลแห่งชาติ อาทิ แผนพัฒนารัฐบาลดิจิทัลของประเทศไทย (พ.ศ. 2563-2565) และนโยบายไทยแลนด์ 4.0 ที่มุ่งเน้นการใช้เทคโนโลยีเป็นกลไกขับเคลื่อนประเทศ

แม้จะมีการจัดตั้ง โครงการคลาวด์กลางภาครัฐ (Government Data Center and Cloud Service: GDCC) ตามมติคณะรัฐมนตรีเมื่อวันที่ 7 พฤษภาคม พ.ศ. 2562 แต่ยังคงไม่เพียงพอต่อความต้องการของทุกหน่วยงาน ด้วยเหตุนี้ นโยบาย "Cloud First Policy" ของภาครัฐไทยจึงเกิดขึ้นเพื่อผลักดันการเปลี่ยนผ่านสู่การเป็นรัฐบาลดิจิทัลอย่างเต็มรูปแบบ โดยมุ่งเน้นให้หน่วยงานภาครัฐพิจารณาใช้บริการคลาวด์สาธารณะเป็นทางเลือกแรกสำหรับโครงสร้างพื้นฐานด้านไอที แม้จะมีความท้าทาย แต่เป้าหมายหลักคือการเพิ่มประสิทธิภาพ ลดต้นทุน และสร้างมาตรฐานการให้บริการสาธารณะที่ตอบสนองความต้องการในยุคดิจิทัลได้อย่างแท้จริง

การประมวลผลแบบคลาวด์ (Cloud Computing) คือ การให้บริการประมวลผลข้อมูลผ่านเครือข่ายต่างๆ ทำให้ผู้ใช้บริการสามารถเข้าถึงทรัพยากรด้านเทคโนโลยีสารสนเทศ เช่น ฐานข้อมูล พื้นที่จัดเก็บข้อมูล เครือข่าย ซอฟต์แวร์ เซิร์ฟเวอร์ และเครื่องมือวิเคราะห์ โดยไม่จำเป็นต้องลงทุนสร้างโครงสร้างพื้นฐาน หรือรับภาระการดูแลบำรุงรักษาด้วยตนเอง ซึ่งช่วยให้หน่วยงานภาครัฐยังคงสามารถให้บริการและจัดการข้อมูลได้อย่างมีประสิทธิภาพ ปัจจุบันทั้งภาครัฐและภาคเอกชนต่างนำระบบคลาวด์มาใช้เพื่อสนับสนุนการดำเนินธุรกิจและบริการอย่างแพร่หลาย ตัวอย่างเช่น ในด้านการแพทย์และสาธารณสุข มีการจัดเก็บข้อมูลผู้ป่วยบนคลาวด์ หรือด้านการศึกษาก็มีการเรียนออนไลน์ (E-Learning) ผ่านแพลตฟอร์มต่าง ๆ เช่น Google Classroom, Microsoft Teams, และ Zoom โดยใช้ระบบคลาวด์ในการจัดเก็บข้อมูลการสอน เอกสาร และวิดีโอ เพื่อให้สามารถเข้าถึงข้อมูลแบบเรียลไทม์ได้ การนำระบบคลาวด์มาใช้จึงมีประโยชน์อย่างยิ่งต่อการพัฒนาธุรกิจและบริการด้านดิจิทัล เพื่อก้าวไปสู่การเป็นรัฐบาลดิจิทัลอย่างยั่งยืน

DRAFT

การขับเคลื่อนตามนโยบายการใช้คลาวด์เป็นหลัก (Cloud First Policy) จะนำมาซึ่งประโยชน์หลากหลายมิติสำหรับหน่วยงานภาครัฐ ดังนี้:

1. ด้านค่าใช้จ่าย

การใช้คลาวด์ช่วยลดค่าใช้จ่ายด้านเทคโนโลยีสารสนเทศ ของหน่วยงานได้อย่างมีนัยสำคัญ โดยลดภาระการลงทุนเริ่มต้นในซอฟต์แวร์และฮาร์ดแวร์ที่มีราคาสูง เนื่องจากบริการทั้งหมดสามารถเข้าถึงได้ผ่านเครือข่ายต่างๆ นอกจากนี้ยังมีรูปแบบการชำระค่าบริการแบบจ่ายตามปริมาณการใช้งานจริง (Pay-as-you-go หรือ Pay-per-use) ซึ่งช่วยให้หน่วยงานสามารถควบคุมค่าใช้จ่ายได้อย่างมีประสิทธิภาพ และลดต้นทุนทางธุรกรรม (Transaction Cost) ที่เกี่ยวข้องกับการแลกเปลี่ยน เข้าถึง รักษา และประมวลผลข้อมูล อีกทั้งยังมีความยืดหยุ่นในการปรับเปลี่ยนทรัพยากรตามความต้องการในแต่ละช่วงเวลา

2. ด้านความยืดหยุ่นและการเปลี่ยนแปลง

ระบบคลาวด์มีความยืดหยุ่นสูงในการปรับเปลี่ยนทรัพยากรคอมพิวเตอร์ตามความต้องการของหน่วยงานได้อย่างง่ายดาย ไม่ว่าจะเป็นการเพิ่มหรือลดปริมาณการใช้งาน การพัฒนา และการปรับปรุงระบบอย่างต่อเนื่อง หน่วยงานสามารถปรับแต่งซอฟต์แวร์และเพิ่มเติมทรัพยากร (Upgrade) เพื่อให้มีประสิทธิภาพที่สูงขึ้น พร้อมทั้งสามารถรักษาเสถียรภาพของบริการได้อย่างต่อเนื่อง

3. ด้านการเข้าถึงและการใช้ประโยชน์จากข้อมูล

ระบบคลาวด์ช่วยให้หน่วยงานสามารถ เข้าถึงและดึงข้อมูลไปใช้ประโยชน์ได้อย่างง่ายดาย จากระบบคลาวด์ได้ทุกที่ทุกเวลาที่มีการเชื่อมต่อผ่านเครือข่ายต่างๆ ผู้ใช้งานสามารถเข้าถึงทรัพยากรพร้อมกันเพื่อการ ทำงานร่วมกันแบบเรียลไทม์ (Real-time Collaboration) ซึ่งส่งเสริมการสร้างระบบนิเวศข้อมูลและการใช้ข้อมูลให้เกิดประโยชน์สูงสุด ทั้งจากภาครัฐ ภาคเอกชน และประชาชน การนำระบบคลาวด์เป็นหลักยังเป็นปัจจัยสำคัญที่ผลักดันให้มีการจัดเก็บข้อมูลในรูปแบบที่คอมพิวเตอร์อ่านได้ (Machine-readable) และสามารถเชื่อมโยงข้อมูลจากหลายฐานข้อมูลเข้าไว้ด้วยกัน ก่อให้เกิดการแลกเปลี่ยนข้อมูลแบบสองทิศทาง ลดอุปสรรคในการเข้าถึงข้อมูลระหว่างหน่วยงาน และข้อมูลมีการอัปเดตแบบเรียลไทม์ ซึ่งจะช่วยเพิ่มขีดความสามารถในการแข่งขัน และสนับสนุนการวางแผนนโยบายภาครัฐ

4. ด้านความปลอดภัยของข้อมูลและนวัตกรรม

ผู้ใช้งานสามารถใช้ระบบการสำรองข้อมูลที่เชื่อถือได้ ทำให้ข้อมูลปลอดภัยจากความเสี่ยงต่างๆ รวมถึงได้รับประโยชน์จากบริการตรวจสอบและรักษาความปลอดภัยจากผู้ให้บริการคลาวด์ ซึ่งช่วยแบ่งเบาภาระด้านการออกแบบและจัดทำระบบที่ปลอดภัยได้ส่วนหนึ่ง นอกจากนี้ คลาวด์ยังส่งเสริมนวัตกรรมในการพัฒนาแอปพลิเคชันในรูปแบบการบริการซอฟต์แวร์ (SaaS) และการนำเสนอ API (Application Programming Interface) ทำให้นักพัฒนาสามารถสร้างและปรับแต่งแอปพลิเคชันเพื่อใช้งานกับระบบคลาวด์ได้อย่างรวดเร็ว ผู้ให้บริการคลาวด์ยังรับผิดชอบในการอัปเดตซอฟต์แวร์อย่างสม่ำเสมอ ทำให้หน่วยงานสามารถเข้าถึงความสามารถและฟีเจอร์ใหม่ๆ ที่ตอบสนองต่อความต้องการของผู้ใช้งานได้อย่างต่อเนื่อง

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

DRAFT

2.1 ความสำคัญของระบบคลาวด์ต่อหน่วยงานภาครัฐในต่างประเทศ

การขับเคลื่อน นโยบายการใช้คลาวด์เป็นหลัก (Cloud First Policy) สู่การเป็นรัฐบาลดิจิทัลที่มีประสิทธิผลนั้น ไม่ได้เป็นเพียงการเปลี่ยนรูปแบบการใช้จ่ายงบประมาณจากการลงทุนเป็นการดำเนินงานที่ครอบคลุมเฉพาะบริการที่ใช้งานจริงเท่านั้น แต่ยังส่งผลดีในหลากหลายมิติ ได้แก่:

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

เป้าหมายหลักของการนำบริการคลาวด์มาใช้ในหน่วยงานภาครัฐตั้งอยู่บนพื้นฐานของการพัฒนาขีดความสามารถในการให้บริการสาธารณะแก่ภาคประชาชนให้มีประสิทธิภาพมากยิ่งขึ้น ด้วยค่าใช้จ่ายที่ลดลง นอกจากนี้ยังช่วยลดการลงทุนและการใช้งานระบบสารสนเทศที่ซ้ำซ้อน รวมถึงส่งเสริมความร่วมมือระหว่างหน่วยงานในการใช้และแลกเปลี่ยนข้อมูลอย่างมีประสิทธิภาพและปลอดภัย

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

กรณีศึกษานโยบายระบบคลาวด์ภาครัฐจากต่างประเทศ

1. สหราชอาณาจักร (United Kingdom)

สหราชอาณาจักรได้ประกาศใช้นโยบาย "Cloud-First Policy" มาตั้งแต่ปี พ.ศ. 2556 โดยกำหนดให้หน่วยงานภาครัฐพิจารณาใช้ Public Cloud เป็นตัวเลือกแรกในการจัดหาระบบและบริการด้านไอที อย่างไรก็ตาม หน่วยงานยังคงสามารถเลือกใช้ทางเลือกอื่นได้ หากสามารถแสดงให้เห็นถึงความคุ้มค่าที่เหนือกว่าได้

นโยบายนี้มีเป้าหมายหลักเพื่อส่งเสริมการใช้งานคลาวด์ในภาครัฐให้มีประสิทธิภาพสูงสุด ลดต้นทุน และส่งเสริมนวัตกรรม เพื่อให้การตัดสินใจเลือกใช้บริการคลาวด์เป็นไปอย่างเหมาะสม สหราชอาณาจักรได้มีการจำแนกประเภทข้อมูล (Data Classification) ออกเป็น 3 ระดับ ได้แก่ Official, Secret และ Top Secret

จากการศึกษา 3-Tiers Model ของสหราชอาณาจักร พบว่า กว่า 90% ของข้อมูลภาครัฐ เช่น ข้อมูลทะเบียนราษฎร์และข้อมูลส่วนบุคคลอื่น ๆ ของประชาชน สามารถจัดเก็บใน Public Cloud ได้ทั้งหมด โดยไม่จำเป็นต้องจำกัดการจัดเก็บเฉพาะในประเทศเท่านั้น แต่สามารถจัดเก็บได้ทุกที่ทั่วโลก โดยมีเงื่อนไขสำคัญว่าผู้ให้บริการคลาวด์ (Cloud Service Provider) ต้องได้รับการรับรองมาตรฐานสากลและปฏิบัติตาม

DRAFT

กฎหมายคุ้มครองข้อมูลส่วนบุคคล (GDPR) อย่างเคร่งครัด มีเพียงข้อมูลระดับสูง (Top Secret) เท่านั้นที่อนุญาตให้จัดเก็บในศูนย์ข้อมูล (Data Center) ภาครัฐได้

ระบบการจำแนกประเภทข้อมูลนี้ถูกออกแบบมาเพื่อให้ข้อมูลของรัฐบาลได้รับการบริหารจัดการตามระดับความอ่อนไหวและความปลอดภัยที่เหมาะสม โดยยกระดับมาตรการความปลอดภัยตามความเสี่ยงและผลกระทบที่อาจเกิดขึ้นจากการรั่วไหลของข้อมูล นอกจากนี้ ยังได้รับการสนับสนุนด้วยมาตรฐานและเทคโนโลยีที่ทันสมัย เช่น แนวทางของ National Cyber Security Centre (NCSC) ซึ่งเป็นหน่วยงานหลักในการปกป้องข้อมูลภาครัฐในทุกระดับชั้น

ตารางที่ 1: หลักการสำคัญของนโยบายของสหราชอาณาจักร

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

ตารางที่ 2: การจำแนกประเภทข้อมูลและตัวอย่างการใช้งานของสหราชอาณาจักร

ประเภทข้อมูล	ลักษณะ	ตัวอย่างการใช้งานในภาครัฐ	มาตรการรักษาความปลอดภัย
Official	- เป็นข้อมูลที่ไม่อ่อนไหวหรือมีผลกระทบต่ำหากเกิดการรั่วไหล - ข้อมูลนี้มักใช้ในงานประจำวันของภาครัฐ เช่น การให้บริการประชาชนหรือข้อมูลเว็บไซต์ - ต้องการการป้องกันขั้นพื้นฐาน เช่น การเข้ารหัสข้อมูล (Encryption) และการควบคุมการเข้าถึง (Access Control)	- ข้อมูลในเว็บไซต์รัฐบาล เช่น GOV.UK - ตารางเวลารถไฟสาธารณะหรือประกาศจากหน่วยงาน	- การเข้าถึงข้อมูลผ่านเครือข่ายที่มีความปลอดภัย เช่น Virtual Private Network (VPN) - ระบบคลาวด์แบบ Public Cloud ที่ผ่านมาตรฐานการรักษาความปลอดภัย เช่น ISO 27001

DRAFT

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

ที่มา : (GOV.UK, n.d.)

2. สหรัฐอเมริกา (United States)

กลยุทธ์การประมวลผลแบบคลาวด์ของรัฐบาลกลางสหรัฐอเมริกา หรือที่รู้จักกันในชื่อ "Cloud Smart" ซึ่งจัดทำโดย Chief Information Officers Council (CIO Council) เป็นนโยบายที่พัฒนาต่อยอดมาจากนโยบาย "Cloud First" ที่ริเริ่มขึ้นในปี พ.ศ. 2544

วัตถุประสงค์หลักของนโยบาย Cloud Smart คือการชี้แจงและให้ความเข้าใจแก่หน่วยงานภาครัฐถึงประโยชน์ของการใช้ระบบคลาวด์ รวมถึงการจัดเตรียมกรอบการตัดสินใจและกรณีศึกษาที่เป็นรูปธรรม เพื่อสนับสนุนให้หน่วยงานภาครัฐสามารถย้ายข้อมูลสารสนเทศและระบบงานไปสู่ระบบคลาวด์ได้อย่างมีประสิทธิภาพ นอกจากนี้ยังเน้นการระบุแหล่งทรัพยากรสำหรับการใช้งานระบบคลาวด์ และการกำหนดบทบาทความรับผิดชอบในการนำระบบคลาวด์มาใช้งานของรัฐบาลกลางสหรัฐอเมริกาอย่างชัดเจน

Cloud Smart มุ่งเน้นการจัดทำแนวทางเพื่อสนับสนุนภารกิจภาครัฐใน 3 ด้านสำคัญ ได้แก่:

1. ความปลอดภัยทางไซเบอร์ (Cyber Security): การเสริมสร้างความมั่นคงปลอดภัยของข้อมูลและระบบบนคลาวด์

DRAFT

2. การจัดซื้อจัดจ้าง (Procurement): การปรับปรุงกระบวนการจัดซื้อจัดจ้างบริการคลาวด์ เช่น การใช้ประโยชน์จากอำนาจการจัดหาแบบรวมศูนย์ (Bulk Purchasing Power) เพื่อให้ได้ราคาที่เหมาะสม และการกำหนดมาตรการป้องกันการผูกขาดผู้ให้บริการ (Avoid Vendor Lock-in)
3. ขั้นตอนการทำงาน (Workflow) ในการสร้างบริการดิจิทัล: การปรับปรุงกระบวนการและเครื่องมือเพื่อสนับสนุนการพัฒนาและส่งมอบบริการดิจิทัล

นอกจากนี้ สถาบันมาตรฐานและเทคโนโลยีแห่งชาติของรัฐบาลสหรัฐอเมริกา (National Institute of Standards and Technology - NIST) ได้แบ่งรูปแบบการประมวลผลแบบคลาวด์ออกเป็น 4 รูปแบบหลัก ได้แก่ คลาวด์ส่วนตัว (Private Cloud), คลาวด์แบบกลุ่ม (Community Cloud), คลาวด์สาธารณะ (Public Cloud) และคลาวด์ผสม (Hybrid Cloud) เพื่อเป็นแนวทางในการเลือกใช้บริการคลาวด์ให้เหมาะสมกับความต้องการและบริบทของแต่ละหน่วยงาน

ตารางที่ 3: หลักการสำคัญของ Cloud Smart ของสหรัฐอเมริกา

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

ที่มา : (Cloud.cio.gov, n.d.)

ตารางที่ 4: การจำแนกประเภทข้อมูลและตัวอย่างการใช้งานของสหรัฐอเมริกา

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

DRAFT

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

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

3. ออสเตรเลีย (Australia)

รัฐบาลออสเตรเลียได้ริเริ่ม นโยบาย Cloud First Policy โดยมีวัตถุประสงค์หลักเพื่อ เพิ่มประสิทธิภาพพัฒนาการให้บริการ และลดต้นทุนด้านเทคโนโลยีสารสนเทศและการสื่อสารของภาครัฐ นโยบายนี้ส่งเสริมให้หน่วยงานภาครัฐเลือกใช้บริการคลาวด์สาธารณะเป็นทางเลือกแรก โดยคำนึงถึงความมั่นคงปลอดภัยและความคุ้มค่าในการลงทุนเป็นสำคัญ การดำเนินการดังกล่าวมีเป้าหมายเพื่อปรับปรุงการให้บริการของรัฐบาลและลดการใช้ทรัพยากรที่ซ้ำซ้อน โดยมีการพิจารณาประเมินทางเลือกระหว่างคลาวด์ส่วนตัว (Private Cloud), คลาวด์แบบกลุ่ม (Community Cloud), คลาวด์สาธารณะ (Public Cloud) หรือคลาวด์ผสม (Hybrid Cloud) ให้เหมาะสมกับบริบทของแต่ละบริการ นอกจากนี้ รัฐบาลออสเตรเลียยังได้ประกาศนโยบายคลาวด์เพื่อสนับสนุนให้ทั้งหน่วยงานภาครัฐและองค์กรภาคเอกชนหันมาใช้ระบบคลาวด์เพิ่มมากขึ้น

ภายใต้กรอบนโยบายการรักษาความปลอดภัยของรัฐบาลออสเตรเลีย (Australian Government Security Classification Policy) มีการแบ่งระดับชั้นของข้อมูลตามประเภทความปลอดภัย (Security Classified Information) ออกเป็น 4 ระดับ เพื่อประเมินความอ่อนไหวและความเสี่ยงที่อาจเกิดขึ้นจากการละเมิดข้อมูลหรือการจัดการที่ไม่เหมาะสม โดยแต่ละระดับสะท้อนถึงระดับความเสียหายที่อาจเกิดขึ้นต่อผลประโยชน์ของชาติ หน่วยงาน หรือบุคคล หากข้อมูลถูกเปิดเผยโดยไม่ได้รับอนุญาต ได้แก่ Unclassified, Protected, Secret, และ Top Secret

ทั้งนี้ ข้อกำหนดหลักที่หน่วยงานภาครัฐของออสเตรเลียต้องดำเนินการภายใต้นโยบายนี้ มีดังนี้:

1. ระบุข้อมูลที่ถือครอง (Identify information holdings) คือทำการระบุข้อมูลทั้งหมดที่หน่วยงานถือครอง เพื่อให้เข้าใจถึงลักษณะและขอบเขตของข้อมูลที่ต้องการการปกป้อง
2. ประเมินการจัดประเภทความปลอดภัยของข้อมูล (Assess the security classification of information holdings) โดยทำการประเมินเพื่อกำหนดระดับความปลอดภัยที่เหมาะสมกับข้อมูล โดยพิจารณาความสำคัญของมูลค่า และความอ่อนไหวของข้อมูลนั้น

3. ดำเนินมาตรการควบคุมการปฏิบัติงาน (Implement operational controls) โดยนำมาตรการควบคุมที่เหมาะสมมาใช้ในการจัดการข้อมูล โดยพิจารณาความสำคัญมูลค่า และความอ่อนไหวของข้อมูล เพื่อให้การปกป้องข้อมูลสอดคล้องกับความเสี่ยงที่อาจเกิดขึ้น

ตารางที่ 5: หลักการและแนวคิดหลักของนโยบายของออสเตรเลีย

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

ตารางที่ 6: การจำแนกประเภทข้อมูลและตัวอย่างการใช้งานของออสเตรเลีย

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

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

DRAFT

4. **สิงคโปร์ (Singapore)**

ในช่วงปลายปี พ.ศ. 2561 รัฐบาลสิงคโปร์ได้ประกาศแผนระยะ 5 ปี เพื่อย้ายระบบเทคโนโลยีสารสนเทศ (IT) ส่วนใหญ่จากโครงสร้างพื้นฐานภายในองค์กร (On-premise) ไปยังบริการคลาวด์เชิงพาณิชย์ (Commercial Cloud) โดยมีเป้าหมายหลักในการเร่งความเร็วและปรับปรุงคุณภาพการให้บริการแก่ประชาชนและภาคธุรกิจ

GovTech ซึ่งเป็นหน่วยงานที่รับผิดชอบด้านเทคโนโลยีของรัฐบาลสิงคโปร์ ได้เปิดตัวแพลตฟอร์ม Government Commercial Cloud (GCC) เพื่ออำนวยความสะดวกให้หน่วยงานภาครัฐสามารถนำเทคโนโลยีคลาวด์มาใช้ได้อย่างรวดเร็วและมีประสิทธิภาพ โดย GCC ของสิงคโปร์ได้นำระบบการจำแนกข้อมูลแบบระดับชั้น (Tiered Data Classification) มาใช้ ซึ่งเป็นส่วนสำคัญของกลยุทธ์ Cloud First Policy ของรัฐบาล ระบบนี้ช่วยกำหนดมาตรการควบคุมที่เหมาะสมตามระดับความสำคัญและความอ่อนไหวของข้อมูลในแต่ละระดับ

การดำเนินนโยบายนี้มุ่งเน้นให้หน่วยงานภาครัฐสามารถใช้บริการคลาวด์จากผู้ให้บริการเชิงพาณิชย์ได้อย่างปลอดภัย ลดต้นทุน และเพิ่มความคล่องตัวในการให้บริการด้านดิจิทัล ปัจจุบันระบบภาครัฐของสิงคโปร์มากกว่าร้อยละ 70 ได้ย้ายมาอยู่บนแพลตฟอร์ม GCC แล้ว โดยมาตรการควบคุมความปลอดภัยจะถูกปรับให้สอดคล้องกับระดับความสำคัญและผลกระทบของข้อมูลตามนโยบายความปลอดภัยไซเบอร์ของรัฐบาลสิงคโปร์ และการเลือกใช้คลาวด์สำหรับข้อมูลต่างระดับใน GCC จะขึ้นอยู่กับความสำคัญความอ่อนไหว และผลกระทบที่อาจเกิดขึ้นในกรณีที่ข้อมูลรั่วไหล

ตัวอย่างบริการภาครัฐที่สำคัญซึ่งอยู่บนแพลตฟอร์ม GCC ได้แก่ MyCareersFuture, GoBusiness และ WOGAA ซึ่งสะท้อนให้เห็นถึงความสำเร็จของสิงคโปร์ในการนำนโยบาย Cloud First มาปรับใช้เพื่อยกระดับการบริหารจัดการภาครัฐและการให้บริการประชาชนในยุคดิจิทัล[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 เพื่อเสริมสร้างบริการดิจิทัลที่มีประสิทธิภาพ โดยไม่ต้องพัฒนาจากพื้นฐาน
4. ความคล่องตัวและประสิทธิภาพด้านต้นทุน	แพลตฟอร์ม GCC สนับสนุนการปรับปรุงกระบวนการดิจิทัลของรัฐบาลให้มีความคล่องตัวและลดต้นทุนผ่านการใช้เทคโนโลยีคลาวด์

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

DRAFT

ตารางที่ 8: การจำแนกประเภทข้อมูลและตัวอย่างการใช้งานของสิงคโปร์

ประเภทข้อมูล	ลักษณะ	ตัวอย่างการใช้งานในภาครัฐ	มาตรการรักษาความปลอดภัย
Public Data	ข้อมูลที่สามารถเผยแพร่สู่สาธารณะโดยไม่มีความกังวลเกี่ยวกับความลับ	- เว็บไซต์บริการประชาชน - รายงานผลการดำเนินงานของหน่วยงาน	- ตรวจสอบความสมบูรณ์ของเว็บไซต์ ใช้ HTTPS ในการเชื่อมต่อ - ใช้ระบบตรวจสอบป้องกันการดัดแปลงข้อมูล - ระบบการเข้าถึงแบบปลอดภัย - การตรวจสอบข้อมูลก่อนเผยแพร่
Restricted Data	ข้อมูลที่อาจก่อให้เกิดความเสียหายเล็กน้อยหากเปิดเผยโดยไม่ได้รับอนุญาต	- บันทึกการประชุมของหน่วยงาน - ข้อมูลการปฏิบัติงานภายใน เช่น แผนงานโครงการภาครัฐ	- การควบคุมสิทธิ์การเข้าถึง (Role-Based Access) - การเข้ารหัสข้อมูล (AES-256) - การเข้ารหัสข้อมูลในระหว่างการส่งและจัดเก็บ - ใช้ Role-Based Access Control (RBAC) - การตรวจสอบการเข้าถึงระบบเป็นประจำ
Confidential Data	ข้อมูลที่ต้องการความปลอดภัยสูง เพื่อป้องกันความเสี่ยงที่สำคัญ	- ข้อมูลส่วนบุคคล (PII) การจัดเก็บข้อมูลส่วนบุคคลของประชาชน เช่น หมายเลขบัตรประชาชน หรือข้อมูลทางการแพทย์ - ข้อมูลเกี่ยวกับสัญญาการจัดซื้อจัดจ้างภาครัฐ และเอกสารทางการเงิน	การเข้ารหัสขั้นสูง (Advanced Encryption) - ยืนยันตัวตนแบบหลายปัจจัย (MFA) - ข้อมูลเข้ารหัสทั้งขณะส่งและขณะเก็บ - การเก็บบันทึกและตรวจสอบการเข้าถึง
Secret/National Security Data	ข้อมูลที่หากเปิดเผยจะส่งผลกระทบต่อความมั่นคงแห่งชาติหรือสวัสดิภาพของประชาชน	- ข้อมูลด้านความมั่นคง เช่น การเฝ้าระวังภัยไซเบอร์หรือข้อมูลข่าวกรองทางการทหาร - แผนปฏิบัติการทางการทหาร เช่น การออกแบบระบบป้องกันประเทศ	**- การแยกข้อมูลออกจากระบบเชิงพาณิชย์ (Data Isolation)** - โครงสร้างพื้นฐานที่ปลอดภัยสูง ใช้ระบบเฝ้าระวังภัยคุกคามแบบเรียลไทม์ - ระบบการควบคุมทางกายภาพ เช่น ใช้การสแกนไบโอเมตริกซ์ (ลายนิ้วมือ/ใบหน้า) เพื่อเข้าถึงเซิร์ฟเวอร์

DRAFT

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

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

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

ดังนั้น การเตรียมความพร้อมและกำหนดแนวทางการบริหารจัดการข้อมูล จึงเป็นสิ่งสำคัญอย่างยิ่งสำหรับองค์กรภาครัฐในการเคลื่อนย้ายข้อมูลเข้าสู่ระบบคลาวด์ เพื่อให้เกิดประสิทธิภาพและประสิทธิผลสูงสุดภายใต้ความมั่นคงปลอดภัยและความเป็นส่วนตัวของข้อมูล การจัดระดับชั้นข้อมูลจึงถือเป็นหนึ่งในขั้นตอนพื้นฐานที่มีความสำคัญของการเตรียมองค์กรเข้าสู่การประมวลผลข้อมูลแบบคลาวด์ ซึ่งสอดคล้องกับหลักการจัดทำธรรมาภิบาลข้อมูลภาครัฐ ดังแสดงตามภาพที่ 2

ภาพที่ 2: ขั้นตอนในการเตรียมองค์กรเข้าสู่การประมวลผลข้อมูลแบบคลาวด์ (Prinya.org, 2022)

DRAFT

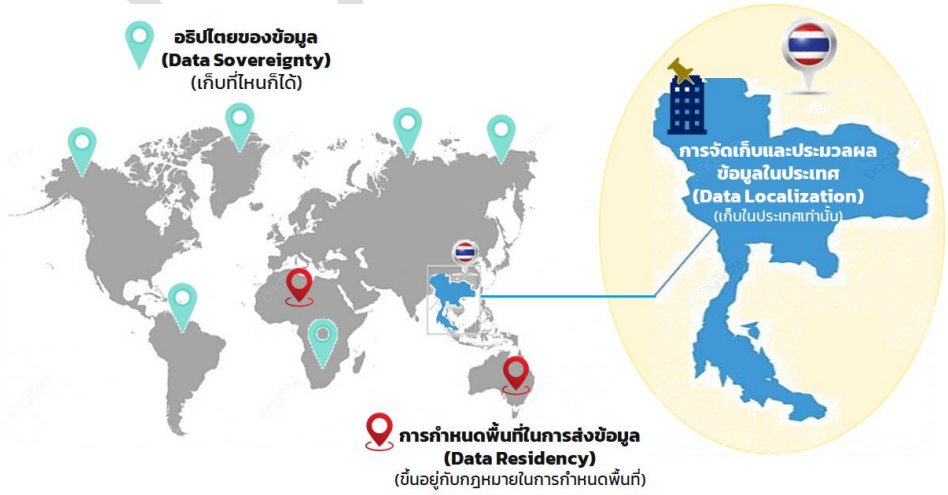
2.2 ความสำคัญของอธิปไตยข้อมูล (Data Sovereignty) และการจัดเก็บข้อมูลในประเทศ (Data Localization)

ในยุคที่รัฐบาลทั่วโลกต่างเร่งขับเคลื่อนการเปลี่ยนผ่านสู่รัฐบาลดิจิทัล (Digital Government) โดยมีนโยบาย Cloud First Policy เป็นหัวใจสำคัญ ประเด็นเรื่อง อธิปไตยข้อมูล (Data Sovereignty) และการจัดเก็บข้อมูลภายในประเทศ (Data Localization) ได้ทวีความสำคัญมากยิ่งขึ้น

อธิปไตยข้อมูล (Data Sovereignty) หมายถึง หลักการที่ข้อมูลดิจิทัลอยู่ภายใต้กฎหมายและอำนาจการกำกับดูแลของประเทศที่ข้อมูลนั้นถูกจัดเก็บหรือประมวลผล ไม่ว่าผู้เป็นเจ้าของข้อมูลหรือผู้ให้บริการคลาวด์จะตั้งอยู่ที่ใดก็ตาม ซึ่งหมายความว่ากฎหมายของประเทศที่ข้อมูลนั้นอยู่มีอำนาจเหนือข้อมูลนั้น และรัฐบาลของประเทศนั้นมีสิทธิ์ในการเข้าถึงหรือควบคุมข้อมูลได้ตามกฎหมาย การรักษาอธิปไตยข้อมูลเป็นสิ่งจำเป็นสำหรับภาครัฐ เพื่อปกป้องข้อมูลสำคัญของชาติ เช่น ข้อมูลด้านความมั่นคง ข้อมูลส่วนบุคคลของประชาชน และข้อมูลเชิงยุทธศาสตร์จากการถูกควบคุมโดยกฎหมายต่างชาติ

การกำหนดถิ่นที่อยู่ของข้อมูล (Data Residency) หมายถึง การกำหนดตำแหน่งทางกายภาพที่ข้อมูลถูกจัดเก็บไว้ในสถานะพัก/จัดเก็บ โดยทั่วไปจะหมายถึงประเทศหรือเขตอำนาจศาลที่ศูนย์ข้อมูล (Data Center) ตั้งอยู่ ถิ่นที่อยู่ของข้อมูลมักถูกกำหนดโดยข้อกำหนดทางกฎหมาย กฎระเบียบ หรือนโยบายภายในองค์กร ซึ่งอาจไม่ได้หมายความว่าข้อมูลนั้นจะอยู่ภายใต้กฎหมายของประเทศนั้นๆ เสมอไป หากไม่มีข้อกำหนดด้าน Data Localization มาเกี่ยวข้อง ถิ่นที่อยู่ของข้อมูลเป็นเพียงการระบุตำแหน่งทางภูมิศาสตร์ของข้อมูล

การจัดเก็บข้อมูลภายในประเทศ (Data Localization) หมายถึง มาตรการทางกฎหมายที่กำหนดให้ข้อมูลบางประเภทหรือข้อมูลทั้งหมดต้องถูกจัดเก็บและประมวลผลภายในขอบเขตทางกายภาพของประเทศนั้นๆ เท่านั้น โดยไม่สามารถถ่ายโอนหรือจัดเก็บนอกประเทศได้เลย นโยบายนี้มักถูกนำมาใช้เพื่อวัตถุประสงค์ด้านความมั่นคงของชาติ การคุ้มครองความเป็นส่วนตัวของข้อมูล หรือการควบคุมการเข้าถึงข้อมูลที่สำคัญอย่างเคร่งครัด สำหรับนโยบาย Cloud First Policy ของภาครัฐ การกำหนดให้มีการจัดเก็บข้อมูลภายในประเทศเป็นการเสริมสร้างอธิปไตยข้อมูลให้แข็งแกร่งยิ่งขึ้น



ภาพที่ 3: รูปแบบการพิจารณาถิ่นที่อยู่ข้อมูล

DRAFT

ตารางที่ 9: ตารางเปรียบเทียบรูปแบบของถิ่นที่อยู่ข้อมูล

หัวข้อ	ข้อดี	ข้อเสีย
อธิปไตยของข้อมูล (Data Sovereignty)	- ช่วยให้ปฏิบัติตามกฎระเบียบในแต่ประเทศได้ง่ายขึ้น - ให้ความสำคัญกับการควบคุมและกฎหมาย - ยืดหยุ่นในการจัดการข้อมูลตามความต้องการของธุรกิจหรือผู้ใช้งานในพื้นที่	- ซับซ้อนในการบริหารจัดการข้อมูลในหลายพื้นที่ - การปรับปรุงกฎหมายอาจส่งผลต่อการจัดเก็บข้อมูล
การกำหนดถิ่นที่อยู่ของข้อมูล (Data Residency)	- ควบคุมข้อมูลได้ดีขึ้นภายใต้กฎหมายในท้องถิ่น - เสริมความมั่นคงของประเทศและอธิปไตยทางดิจิทัล - ให้ความสำคัญกับสถานที่เก็บข้อมูลทางกายภาพ - สามารถติดต่อผู้ให้บริการได้ทันท่วงที เนื่องจากมีที่ตั้งสำนักงานใหญ่/สาขาที่ติดต่อได้ ช่องทางการติดต่อที่ชัดเจน และความสามารถในการตอบสนอง - ส่งเสริมการลงทุนในประเทศ เช่น บริษัทต่างประเทศมีการจดทะเบียนนิติบุคคลภายในประเทศ เพื่อจัดตั้งศูนย์ข้อมูลในประเทศไทย	- อาจจำกัดการใช้คลาวด์ข้ามประเทศ - ความซับซ้อนในการทำธุรกิจระหว่างประเทศ โดยเฉพาะองค์กรที่ทำงานข้ามพรมแดน
การจัดเก็บและประมวลผลข้อมูลในประเทศ (Data Localization)	- เพิ่มความมั่นคงทางข้อมูล โดยให้ความสำคัญกับสถานที่เก็บข้อมูลทางกายภาพ - รองรับการบังคับใช้กฎหมายภายในประเทศ - กระตุ้นเศรษฐกิจภายใน เช่น การพัฒนาโครงสร้างพื้นฐานดิจิทัล	- เพิ่มต้นทุนการจัดเก็บและการดำเนินการ จำกัดการค้าและนวัตกรรม เนื่องจากการปิดกั้นการแลกเปลี่ยนข้อมูลระหว่างประเทศ

ตัวอย่างการบังคับใช้ในกลุ่มประเทศ OECD:

กลุ่มประเทศ OECD มุ่งเน้นการสร้างสมดุลระหว่างการไหลเวียนของข้อมูลข้ามพรมแดนอย่างเสรีกับการปกป้องข้อมูลและความเป็นส่วนตัว โดยมีการออกแนวปฏิบัติและข้อเสนอแนะต่างๆ เช่น **OECD Recommendation on Enhancing Access to and Sharing of Data** ที่ส่งเสริมการแบ่งปันข้อมูลอย่างมีความรับผิดชอบ อย่างไรก็ตาม บางประเทศยังคงมีมาตรการ Data Localization ในบางกรณี:

- **สหภาพยุโรป (EU):** แม้ว่า GDPR จะไม่ได้บังคับ Data Localization โดยตรง แต่ก็มีข้อกำหนดที่เข้มงวดสำหรับการถ่ายโอนข้อมูลส่วนบุคคลไปยังประเทศนอก EU (เช่น ต้องมีกลไกการคุ้มครองข้อมูลที่เทียบเท่า) ซึ่งในทางปฏิบัติอาจนำไปสู่การเลือกจัดเก็บข้อมูลภายใน EU เพื่อลดความซับซ้อนในการปฏิบัติตามกฎระเบียบ นอกจากนี้ สหภาพยุโรปยังได้ประกาศแผนยุทธศาสตร์ด้าน AI และข้อมูลที่เรียกร้องให้มีการจัดเก็บและประมวลผลข้อมูลใน EU มากขึ้นเพื่อเพิ่ม Data Sovereignty
- **เยอรมนี:** รัฐมนตรีเศรษฐกิจของเยอรมนีเคยกล่าวถึงความต้องการโครงสร้างพื้นฐานข้อมูลที่รองรับ Data Sovereignty ของยุโรป

DRAFT

- **สวีเดน:** กฎหมายบัญชีของสวีเดน (Swedish Accounting Act 1999) กำหนดให้ข้อมูลทางบัญชีต้องจัดเก็บและรักษาไว้ภายในประเทศสวีเดนเป็นเวลา 7 ปี
- **เดนมาร์ก:** กฎหมายการทำบัญชีของเดนมาร์ก (Danish Bookkeeping Act) กำหนดให้บริษัทต้องจัดเก็บข้อมูลทางการเงินของพลเมืองเดนมาร์กในเดนมาร์กหรือประเทศนอร์ดิกอื่น ๆ เป็นเวลา 5 ปี

ตัวอย่างการบังคับใช้ในกลุ่มประเทศอาเซียน (ASEAN):

กลุ่มประเทศอาเซียนมีความหลากหลายในแนวทางการบังคับใช้ Data Localization บางประเทศมีการบังคับใช้อย่างเข้มงวด โดยเฉพาะในภาคส่วนที่มีความสำคัญ เช่น การเงิน หรือข้อมูลภาครัฐ เพื่อวัตถุประสงค์ด้านความมั่นคงของชาติและการควบคุม:

- **เวียดนาม:** มีกฎหมายความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Law) ที่เข้มงวด ซึ่งบังคับให้ผู้ให้บริการต่างชาติจัดเก็บข้อมูลผู้ใช้งานในเวียดนามเป็นเวลาอย่างน้อย 24 เดือน และต้องจัดตั้งสำนักงานในประเทศเมื่อได้รับการร้องขอ
- **อินโดนีเซีย:** กำหนดให้ข้อมูลภาครัฐทั้งหมดต้องจัดเก็บภายในประเทศ และยังมีการบังคับใช้ Data Localization ในบางภาคส่วน เช่น ภาคการเงิน ซึ่งส่งผลให้ความต้องการ Data Center ในอินโดนีเซียเพิ่มขึ้นอย่างรวดเร็ว
- **สิงคโปร์:** แม้จะส่งเสริมการใช้ Commercial Cloud แต่ก็มีแพลตฟอร์ม Government Commercial Cloud (GCC) และการจำแนกประเภทข้อมูลอย่างละเอียด โดยสำหรับข้อมูลที่มีความอ่อนไหวสูงสุด (Top Secret) อาจเลือกใช้ Government Cloud หรือโครงสร้างพื้นฐาน On-Premise เพื่อรักษา Data Sovereignty

ข้อพิจารณาด้าน Data Localization, Data Residency และ Data Sovereignty ในบริบทกฎหมายไทย

ปัจจุบัน ประเทศไทยได้มีการกำหนดแนวทางการจัดเก็บและประมวลผลข้อมูลในประเทศ (Data Localization) ตาม**ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567**

ในส่วนของการกำหนดถิ่นที่อยู่ของข้อมูล (Data Residency) ในประเทศไทย ควรให้ความสำคัญกับ**อธิปไตยของข้อมูล (Data Sovereignty)** ในการใช้คลาวด์ ทั้งนี้ หน่วยงานภาครัฐควรพิจารณากฎหมายที่เกี่ยวข้องเพิ่มเติม เพื่อให้สามารถจำแนกประเภทข้อมูลสำหรับการใช้คลาวด์ได้อย่างมีประสิทธิภาพ โดยเฉพาะอย่างยิ่งในประเด็นการโอนข้อมูลส่วนบุคคลข้ามพรมแดน ดังรายละเอียดตาม **พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA)**:

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA)

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้กำหนดหน้าที่และมาตรการเกี่ยวกับการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศไว้ใน **มาตรา 28** ซึ่งระบุว่า ประเทศปลายทางหรือองค์กรระหว่างประเทศที่รับข้อมูลส่วนบุคคลต้องมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ และ **มาตรา 29**

DRAFT

ซึ่งเกี่ยวข้องกับการโอนหรือส่งข้อมูลไปยังต่างประเทศของเครือกิจการหรือเครือธุรกิจเดียวกัน ทั้งนี้ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลได้ออกประกาศเพิ่มเติมเพื่ออธิบายรายละเอียด ดังนี้:

- **ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังต่างประเทศ ตามมาตรา 28 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2566**
- **ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังต่างประเทศ ตามมาตรา 29 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2566**

ประกาศทั้งสองฉบับนี้ ได้กำหนดนิยามของคำว่า “ส่งหรือโอนข้อมูลส่วนบุคคล” ให้มีความชัดเจนยิ่งขึ้น โดย **ไม่รวมถึงการส่งและรับข้อมูลส่วนบุคคลในลักษณะที่เป็นเพียงสื่อกลาง (Intermediary) ในการส่งผ่านข้อมูล (Data Transit) ระหว่างระบบคอมพิวเตอร์หรือระบบเครือข่าย หรือการเก็บพักข้อมูลที่ไม่มีบุคคลภายนอกเข้าถึงข้อมูลส่วนบุคคลได้ นอกจากผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลที่เป็นผู้ส่งข้อมูลนั้น** ตัวอย่างเช่น การส่งข้อมูลผ่านระบบเครือข่ายในต่างประเทศ หรือการส่งข้อมูลผ่านระบบของผู้ให้บริการระบบคลาวด์ (Cloud Computing Service Provider) ที่ไม่มีบุคคลใดนอกจากผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่เป็นผู้ส่งข้อมูล ที่สามารถเข้าถึงข้อมูลส่วนบุคคลได้ เนื่องจากมีมาตรการทางเทคนิคหรือเงื่อนไขทางกฎหมายรองรับ

ดังนั้น หากเป็นการจัดเก็บข้อมูลบนคลาวด์ที่ไม่มีบุคคลภายนอกสามารถเข้าถึงข้อมูลส่วนบุคคลได้นอกจากผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลที่เป็นผู้ส่งข้อมูลแล้ว **แม้ว่าจะเป็นการโอนหรือส่งข้อมูลไปต่างประเทศ ก็ไม่ถือว่าเป็นการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศตามมาตรา 28 และมาตรา 29** ที่กล่าวมาเบื้องต้น ตัวอย่างเช่น หากหน่วยงาน ก. มีการจัดเก็บข้อมูลส่วนบุคคลที่ได้รับความยินยอมจากเจ้าของข้อมูล ซึ่งมีข้อมูลระดับชั้นลับและเป็นข้อมูลประเภทที่ต้องได้รับความคุ้มครอง หน่วยงาน ก. ก็สามารถจัดเก็บข้อมูลบนคลาวด์ได้ทั้งในประเทศไทยและต่างประเทศ โดยไม่ถือว่าเป็นการโอนหรือส่งข้อมูลไปต่างประเทศตามมาตราดังกล่าว แต่ต้องมีมาตรการคุ้มครองข้อมูลที่มีมาตรฐาน เช่น มีการลงนามข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement) เพื่อกำหนดขอบเขตและวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคลอย่างชัดเจน

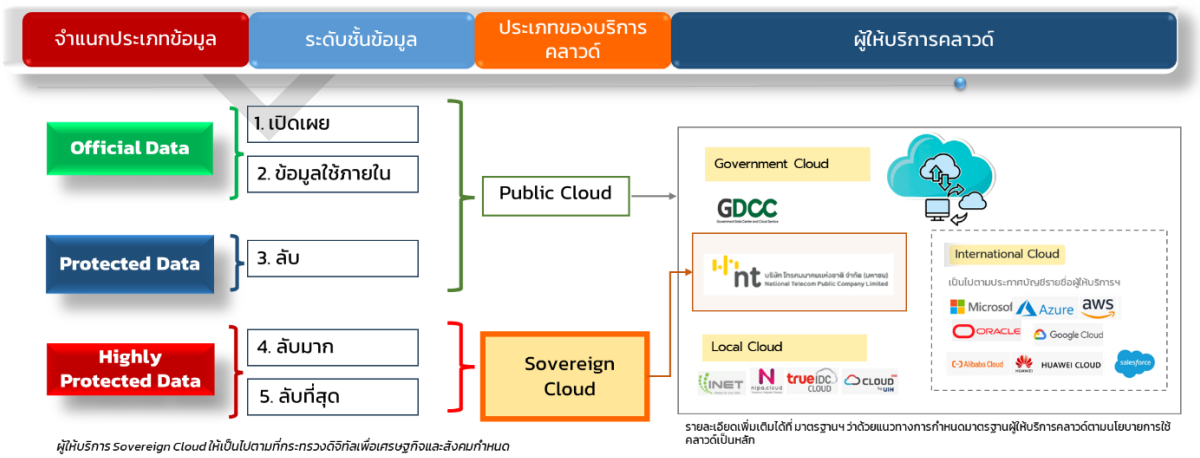
โดยสรุป การนำนโยบาย Cloud First มาใช้ในภาครัฐจำเป็นต้องพิจารณาอย่างถี่ถ้วนถึงประเด็นด้านอธิปไตยข้อมูลและการจัดเก็บข้อมูลภายในประเทศ เพื่อให้มั่นใจว่าการเปลี่ยนผ่านสู่รัฐบาลดิจิทัลเป็นไปอย่างมั่นคงปลอดภัย และเป็นประโยชน์สูงสุดต่อประเทศชาติและประชาชน ควบคู่ไปกับการส่งเสริมการเติบโตของเศรษฐกิจดิจิทัล

DRAFT

3. แนวทางการจำแนกประเภทข้อมูลสำหรับการใช้คลาวด์ในประเทศไทย

สำหรับ **ประเทศไทย** มีหลักการและแนวคิดที่ช่วยให้หน่วยงานภาครัฐสามารถพิจารณาการจัดหมวดหมู่ข้อมูลให้เป็นไปตามกรอบธรรมาภิบาลข้อมูลภาครัฐ (DGF) โดยพิจารณาการจัดระดับชั้นข้อมูลภาครัฐที่มีความอ่อนไหวให้สอดคล้องตามแนวมาตรฐานสากลและเป็นไปตามข้อกฎหมายที่เกี่ยวข้อง โดยการจัดระดับชั้นข้อมูลเพื่อบริหารจัดการข้อมูลภายในหน่วยงานแบ่งออกเป็น 5 ระดับ ได้แก่ ชั้นเปิดเผย (Open) สู่สาธารณะ เปิดเผยเมื่อได้รับอนุญาต ได้แก่ ชั้นเผยแพร่ภายในองค์กร (Private) ชั้นลับ (Confidential) และชั้นลับมาก (Secret) และเปิดเผยไม่ได้/ปกปิด ได้แก่ ชั้นลับที่สุด (Top Secret) (สำนักงานพัฒนารัฐบาลดิทัล (องค์การมหาชน), 2565)

ซึ่งสอดคล้องตามนโยบาย “Cloud First Policy” มุ่งเน้นให้หน่วยงานภาครัฐมีการใช้ระบบคลาวด์เป็นหลัก เพื่อส่งเสริมและพัฒนาให้หน่วยงานภาครัฐเป็นรัฐบาลดิจิทัล จึงจำเป็นต้องมีการจัดระดับชั้นข้อมูลในภาพรวมของการให้บริการ (Service) โดยพิจารณาจากผลกระทบและความเสี่ยงที่อาจเกิดกับข้อมูล **เพื่อนำไปสู่การพิจารณาประเภทของคลาวด์ และถิ่นที่อยู่ของข้อมูลตามลักษณะข้อมูล โดยมุ่งเน้นให้หน่วยงานเลือกศูนย์ข้อมูลในประเทศไทยเป็นลำดับแรก** ซึ่งสอดคล้องกับกฎหมายที่เกี่ยวข้อง เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) ที่กำหนดว่าการประมวลผลข้อมูลส่วนบุคคลนอกประเทศต้องได้รับการอนุญาต และข้อมูลที่เป็นความลับตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ยังเป็นการเพิ่มความมั่นคงและปลอดภัยของข้อมูล โดยมีการควบคุมทางกายภาพ (Physical control) ของศูนย์ข้อมูลได้โดยตรง **โดยเฉพาะข้อมูลบริการที่ประกอบด้วย ข้อมูลในระดับชั้นลับมากและลับที่สุด จำเป็นต้องใช้คลาวด์อธิปไตย (Sovereign Cloud) ซึ่งเป็นบริการคลาวด์ที่ฮาร์ดแวร์และข้อมูลทั้งหมดตั้งอยู่ในราชอาณาจักรไทย และเป็นบริการคลาวด์ที่ให้บริการโดยหน่วยงานของรัฐ หรือองค์กรที่รัฐบาลเป็นเจ้าของทั้งหมดหรือส่วนใหญ่ หรือมีอำนาจควบคุม รวมถึงต้องเป็นบริการคลาวด์ที่ให้หน่วยงานของรัฐใช้งานเท่านั้น เนื่องจากเป็นข้อมูลที่ไม่สามารถเปิดเผยได้เนื่องจากเป็นข้อมูลที่มีผลกระทบสูง และเกี่ยวข้องกับความมั่นคง ดังนั้น การบังคับใช้กฎหมายจึงจำเป็นต้องให้อยู่กับองค์กรที่มีความน่าเชื่อถือ**



ภาพที่ 4: กรอบแนวทางการจำแนกประเภทข้อมูลสำหรับการใช้คลาวด์

DRAFT

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

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

ตารางที่ 10: การจำแนกประเภทข้อมูลของประเทศไทย

จำแนกประเภทข้อมูล	ลักษณะ	ตัวอย่างข้อมูล	มาตรการรักษาความปลอดภัย
Official Data	• ข้อมูลข่าวสารที่รัฐเปิดเผยให้ประชาชนโดยทั่วไป • ข้อมูลที่หน่วยงานใช้ในการปฏิบัติงานภายใน	• เว็บไซต์ • Social Media • หนังสือสารบรรณ • เอกสารประกอบการประชุมออนไลน์ • เอกสารจัดซื้อจัดจ้าง	• กำหนดมาตรการควบคุมความปลอดภัย • กำหนดให้มีผู้ที่สามารถเข้าถึงข้อมูลได้เท่าที่จำเป็น (Need to Know Basis)
Protected Data	• ข้อมูลที่หากเปิดเผยอาจเกิดความเสียหายต่อรัฐ	• ข้อมูลการเสียภาษี • ข้อมูลบัญชีธนาคาร • ข้อมูลประวัติการรักษาพยาบาล	• กำหนดมาตรการควบคุมความปลอดภัย • กำหนดให้มีผู้ที่สามารถเข้าถึงข้อมูลได้เท่าที่จำเป็น (Need to Know Basis) • ควบคุมการเข้าถึงฐานข้อมูล • การเข้ารหัสข้อมูล การใช้เทคโนโลยีกุญแจคู่
Highly Protected Data	• ข้อมูลที่หากเปิดเผยอาจเกิดความเสียหายร้ายแรงต่อรัฐ • ข้อมูลที่หากเปิดเผยอาจเกิดความเสียหายร้ายแรงที่สุดต่อรัฐ เช่น แผนปฏิบัติการทางทหาร	• ข้อมูลประวัติการรักษาพยาบาลของประชาชนจำนวนมาก • แผนการป้องกันประเทศ • ข้อมูลเกี่ยวกับความสัมพันธ์ระหว่างประเทศ	• มีการควบคุมเข้าถึงหรืออ่านข้อมูลที่ต้องได้รับการคุ้มครองเข้มงวดสูงสุด เช่น มีการเข้ารหัสที่ซับซ้อนระหว่างการสร้างการจัดเก็บ

DRAFT

จำแนกประเภทข้อมูล	ลักษณะ	ตัวอย่างข้อมูล	มาตรการรักษาความปลอดภัย
		• ข้อมูลเกี่ยวกับความมั่นคงของสถาบันพระมหากษัตริย์	• ห้ามส่งข้อมูลนอกระบบเครือข่าย Secure Isolated Network

แนวทางการจำแนกประเภทข้อมูลเพื่อใช้บริการคลาวด์ ซึ่งได้รับความเห็นชอบจากคณะกรรมการพัฒนารัฐบาลดิจิทัล ในการประชุมครั้งที่ 1/2568 ได้กำหนด **ข้อกำหนดด้านถิ่นที่อยู่ข้อมูล (Data Residency)** ไว้อย่างชัดเจนดังนี้:

- **หลักการทั่วไป:** ข้อมูลทั้งหมดของหน่วยงานภาครัฐ ไม่ว่าอยู่ในระดับชั้นใด **ควรจัดเก็บอยู่ในประเทศไทย**
- **คำจำกัดความ "ข้อมูลควรอยู่ในประเทศไทย":** ในที่นี้หมายถึง **ข้อมูลที่อยู่ในสถานะพัก/จัดเก็บ (Data at Rest)** ซึ่งไม่รวมถึงข้อมูลที่อยู่ระหว่างการรับส่ง (Data in Transit) หรือข้อมูลที่อยู่ระหว่างการประมวลผล (Data Processing)
- กรณีมีความจำเป็นที่ต้องดำเนินการที่นอกเหนือจากที่แนะนำข้างต้น มี**ข้อยกเว้นสำหรับการจัดเก็บข้อมูลในนอกราชอาณาจักรไทย** หากหน่วยงานภาครัฐมีความจำเป็นต้องใช้บริการคลาวด์ที่จัดเก็บข้อมูลนอกราชอาณาจักรไทย ให้หน่วยงานแจ้ง**สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)** พิจารณาแนวทางและความเหมาะสม เพื่อดำเนินการตามนโยบายการใช้คลาวด์เป็นหลักต่อไป
- โดยปัจจัยที่สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) พิจารณาเพื่อเป็น**แนวทางการใช้บริการคลาวด์ที่เก็บข้อมูลนอกราชอาณาจักรไทย จะเป็นไปตามมาตรฐานฯ ว่าด้วยแนวทางการกำหนดมาตรฐานผู้ให้บริการคลาวด์ ตามนโยบายการใช้คลาวด์เป็นหลัก**

ข้อกำหนดเฉพาะสำหรับข้อมูลระดับ "ลับมาก" และ "ลับที่สุด"

คณะกรรมการพัฒนารัฐบาลดิจิทัลยังได้กำหนดข้อบังคับที่เข้มงวดสำหรับหน่วยงานที่จัดทำระบบดิจิทัลซึ่งจำเป็นต้องจัดเก็บข้อมูลระดับ **ลับมาก (Secret)** และ **ลับที่สุด (Top Secret)** ดังนี้:

- หากมีความจำเป็นต้องใช้บริการคลาวด์สำหรับกรณีที่เป็นข้อมูลในระดับลับมาก (Secret) ขึ้นไป ให้พิจารณาใช้คลาวด์อธิปไตย (Sovereign Cloud) ซึ่งเป็นบริการคลาวด์ที่ฮาร์ดแวร์และข้อมูลทั้งหมดตั้งอยู่ในราชอาณาจักรไทย และเป็นบริการคลาวด์ที่ให้บริการโดยหน่วยงานของรัฐ หรือองค์กรที่รัฐบาลเป็นเจ้าของทั้งหมดหรือส่วนใหญ่ หรือมีอำนาจควบคุม รวมถึงต้องเป็นบริการคลาวด์ที่ให้หน่วยงานของรัฐใช้งานเท่านั้น[1] โดยหน่วยงานรัฐต้องดำเนินการในการควบคุมและคุ้มครองข้อมูลสำคัญของรัฐให้เป็นไปตามกฎหมายที่เกี่ยวข้อง เช่น ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544

[1] ผู้ให้บริการ Sovereign Cloud ให้เป็นไปตามที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมกำหนด

DRAFT

- หากหน่วยงานภาครัฐมีความจำเป็นต้องใช้บริการคลาวด์ที่จัดเก็บข้อมูลนอกราชอาณาจักรไทย ให้หน่วยงาน**แจ้งสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)** เพื่อรวบรวมและนำเสนอต่อ**คณะกรรมการที่เกี่ยวข้องพิจารณา**ให้ความเห็นชอบตามนโยบายการใช้คลาวด์เป็นหลักต่อไป

เพื่อให้การดำเนินงานตามกรอบแนวทางนี้เป็นไปอย่างมีขั้นตอนและมีประสิทธิภาพ หน่วยงานภาครัฐจึงจำเป็นต้อง ดำเนินการประเมินความเสี่ยง เพื่อพิจารณาเลือกใช้บริการคลาวด์ที่เหมาะสมกับบริบทของแต่ละหน่วยงานอย่างรอบคอบ ท่านสามารถศึกษาแนวทางการจำแนกประเภทข้อมูลสำหรับการใช้คลาวด์เพิ่มเติมได้ใน บทที่ 3.1 ของเอกสารฉบับนี้

3.1 แนวทางการจำแนกประเภทข้อมูลกับการใช้คลาวด์

ประเทศไทยได้กำหนดหลักการและแนวคิดเพื่อช่วยให้หน่วยงานภาครัฐสามารถจำแนกหมวดหมู่ข้อมูลให้เป็นไปตามกรอบธรรมาภิบาลข้อมูลภาครัฐ (DGF) ซึ่งสอดคล้องกับแนวมาตรฐานสากลและข้อกฎหมายที่เกี่ยวข้อง โดยเฉพาะอย่างยิ่งเพื่อสนับสนุนนโยบาย “Cloud First Policy” ที่มุ่งเน้นให้หน่วยงานภาครัฐมีการใช้ระบบคลาวด์เป็นหลักในการเป็นรัฐบาลดิจิทัล การจัดระดับชั้นข้อมูลมีความสำคัญอย่างยิ่งในการพิจารณาประเภทของคลาวด์และถิ่นที่อยู่ของข้อมูล เพื่อเพิ่มความมั่นคงปลอดภัยของข้อมูลและปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA)

การจัดระดับชั้นข้อมูลของหน่วยงานภาครัฐแบ่งออกเป็น 5 ระดับ ได้แก่ ชั้นเปิดเผย (Open) ชั้นเผยแพร่ภายในองค์กร (Private) ชั้นลับ (Confidential) ชั้นลับมาก (Secret) และ ชั้นลับที่สุด (Top Secret) โดยข้อมูลที่มีความอ่อนไหวสูง เช่น ข้อมูลในระดับชั้นลับมากและชั้นลับที่สุด จำเป็นต้องใช้คลาวด์อธิปไตย (Sovereign Cloud) ซึ่งเป็นบริการคลาวด์ที่ฮาร์ดแวร์และข้อมูลทั้งหมดตั้งอยู่ในราชอาณาจักรไทย และเป็นบริการคลาวด์ที่ให้บริการโดยหน่วยงานของรัฐ หรือองค์กรที่รัฐบาลเป็นเจ้าของทั้งหมดหรือส่วนใหญ่ หรือมีอำนาจควบคุม รวมถึงต้องเป็นบริการคลาวด์ที่ให้หน่วยงานของรัฐใช้งานเท่านั้น

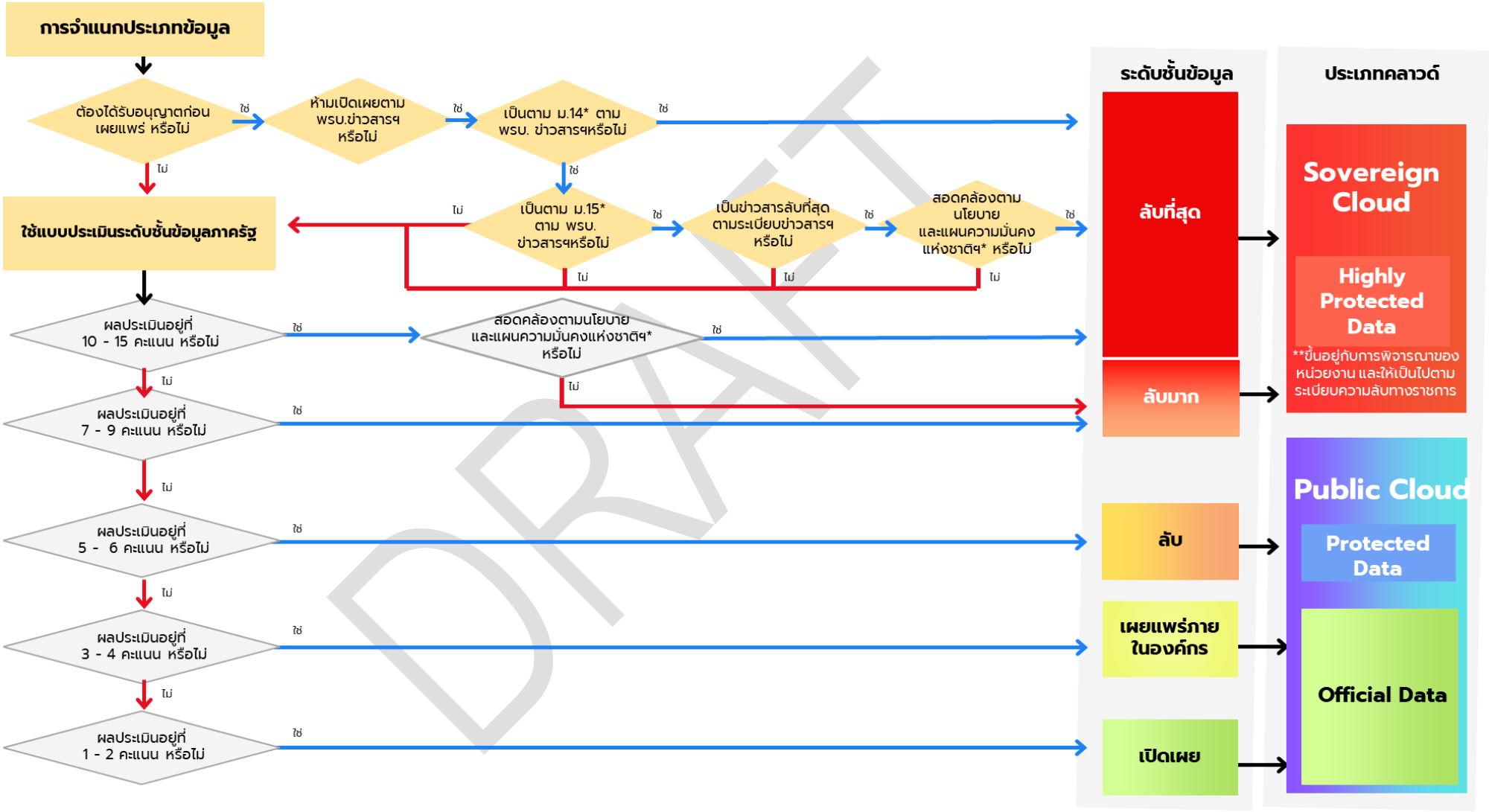
กรอบแนวทางในการจำแนกประเภทข้อมูลสำหรับการใช้คลาวด์ สรุปการจำแนกข้อมูลเป็น 3 ประเภท ซึ่งสอดคล้องกับระดับชั้นข้อมูลข้างต้น โดยพิจารณาจากผลกระทบและความเสี่ยงที่อาจเกิดขึ้นกับข้อมูล

- ข้อมูลที่สามารถเปิดเผยได้ (Official Data)
- ข้อมูลที่ต้องได้รับความคุ้มครอง (Protected Data)
- ข้อมูลที่ต้องได้รับความคุ้มครองสูงสุด (Highly Protected Data)

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

DRAFT

แผนผังการตัดสินใจสำหรับการจำแนกประเภทข้อมูลกับการใช้คลาวด์



ภาพที่ 5: แผนผังการตัดสินใจสำหรับการจำแนกประเภทข้อมูลสำหรับการใช้คลาวด์

DRAFT

3.1.1. ข้อมูลที่ต้องได้รับความคุ้มครองสูงสุด (Highly Protected Data)

<u>คำจำกัดความและลักษณะ:</u>

- เป็นประเภทข้อมูลที่มีความเสี่ยงสูงที่สุด ซึ่งหากเปิดเผยอาจก่อให้เกิดความเสียหายร้ายแรงและร้ายแรงที่สุดต่อความมั่นคงของชาติ[2]
- เทียบเท่ากับข้อมูลระดับ ชั้นลับมาก (Secret) และ ชั้นลับที่สุด (Top Secret)
- ตัวอย่างข้อมูล: แผนปฏิบัติการทางทหาร, แผนการป้องกันประเทศ, ข้อมูลเกี่ยวกับความสัมพันธ์ระหว่างประเทศ, ข้อมูลเกี่ยวกับความมั่นคงของสถาบันพระมหากษัตริย์
- การประเมินความเสี่ยงด้วยเครื่องมือ มสพร. 8-2565 และฉบับปรับปรุง จะได้ผลการประเมินอยู่ระหว่าง 7 – 15 คะแนน

<u>ประเภทคลาวด์และถิ่นที่อยู่ของข้อมูลที่แนะนำ:</u>

- จำเป็นต้องใช้ คลาวด์อธิปไตย (Sovereign Cloud) ซึ่งเป็นบริการคลาวด์ที่ฮาร์ดแวร์และข้อมูลทั้งหมดตั้งอยู่ในราชอาณาจักรไทย และเป็นบริการคลาวด์ที่ให้บริการโดยหน่วยงานของรัฐ หรือองค์กรที่รัฐบาลเป็นเจ้าของทั้งหมดหรือส่วนใหญ่ หรือมีอำนาจควบคุม รวมถึงต้องเป็นบริการคลาวด์ที่ให้หน่วยงานของรัฐใช้งานเท่านั้น[3]
- ข้อมูลที่ต้องได้รับความคุ้มครองสูงสุดต้องใช้ศูนย์ข้อมูลหลักในประเทศไทยเท่านั้น
- การตัดสินใจนำข้อมูลประเภทนี้ขึ้นคลาวด์ให้เป็นดุลพินิจของหัวหน้าหน่วยงาน

<u>มาตรการรักษาความปลอดภัยและข้อเสนอแนะเบื้องต้น:</u>

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

<u>มาตรการรักษาความปลอดภัยและข้อเสนอแนะเบื้องต้นหว่างการสร้างและการจัดเก็บ</u>

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

[2] ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544

[3] มาตรฐานฯ ว่าด้วยแนวทางการใช้คลาวด์ตามนโยบายการใช้คลาวด์เป็นหลัก ในหัวข้อที่ 2.2. แนวทางการเลือกประเภทคลาวด์ (Cloud Deployment Models)

DRAFT

3.1.2. ข้อมูลที่ต้องได้รับความคุ้มครอง (Protected Data)

<u>คำจำกัดความและลักษณะ:</u>

- เป็นประเภทข้อมูลที่มี ความเสี่ยงปานกลาง และต้องการมาตรการควบคุมความปลอดภัยที่สูง
- มักเป็นข้อมูลที่องค์กรไม่ได้เผยแพร่โดยอิสระ โดยทั่วไปเกี่ยวข้องกับข้อมูลที่มีลักษณะเป็นส่วนตัว ไม่ว่าจะเป็นข้อมูลบุคคลหรือองค์กร
- หากเปิดเผยโดยไม่ได้รับอนุญาตอาจก่อให้เกิด ความสูญเสีย/ผลกระทบอย่างร้ายแรงต่อชื่อเสียง การเงิน หรือทรัพย์สิน หรือต่อความมั่นคงและผลประโยชน์แห่งรัฐอย่างร้ายแรงหรือสำคัญ
- ข้อมูลประเภทนี้อยู่ในระดับ ชั้นลับ (Confidential)
- ตัวอย่างข้อมูล: ข้อมูลการเสียภาษี, ข้อมูลบัญชีธนาคาร, ข้อมูลประวัติการรักษาพยาบาล
- บริการที่มีข้อมูลประเภทนี้ ได้แก่ การบริการข้อมูลสำหรับการดำเนินการภายใน, บริการ ERP, ระบบเงินเดือน
- การประเมินความเสี่ยงด้วยเครื่องมือ มสพร. 8-2565 และฉบับปรับปรุง จะได้ผลการประเมินอยู่ระหว่าง 5 – 6 คะแนน

<u>ประเภทคลาวด์และถิ่นที่อยู่ของข้อมูลที่แนะนำ:</u>

- สามารถเลือกใช้ Public Cloud ได้
- ควรใช้ศูนย์ข้อมูลในประเทศไทยเป็นลำดับแรก ซึ่งมุ่งเน้นไปที่ ข้อมูลขณะพัก/จัดเก็บ (Data at Rest)

<u>มาตรการรักษาความปลอดภัยและข้อเสนอแนะเบื้องต้น:</u>

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

DRAFT

3.1.3. ข้อมูลที่สามารถเปิดเผยได้ (Official Data)

<u>คำจำกัดความและลักษณะ:</u>

- เป็นประเภทข้อมูลที่มี ความเสี่ยงต่ำ
- เป็นข้อมูลที่สร้าง ประมวลผล ส่ง หรือรับของหน่วยงานภาครัฐและหน่วยงานที่เกี่ยวข้อง
- ข้อมูลประเภทนี้อยู่ในระดับ ชั้นเผยแพร่ภายในองค์กร (Private) และ ชั้นเปิดเผย (Open)
- ตัวอย่างข้อมูล: เว็บไซต์, Social Media, หนังสือสารบรรณ, เอกสารประกอบการประชุมออนไลน์, เอกสารจัดซื้อจัดจ้าง
- บริการที่มีข้อมูลประเภทนี้ ได้แก่ การบริการข้อมูลการดำเนินการของภาครัฐ, การบริการแจ้งข่าวสารต่างๆ
- การประเมินความเสี่ยงด้วยเครื่องมือ มสพร. 8-2565 และฉบับปรับปรุง จะได้ผลการประเมินอยู่ระหว่าง 1 – 4 คะแนน

<u>ประเภทคลาวด์และถิ่นที่อยู่ของข้อมูลที่แนะนำ:</u>

- สามารถเลือกใช้ Public Cloud ได้
- ควรใช้ศูนย์ข้อมูลในประเทศไทยเป็นลำดับแรก ซึ่งมุ่งเน้นไปที่ ข้อมูลขณะพัก/จัดเก็บ (Data at Rest)

<u>มาตรการรักษาความปลอดภัยและข้อเสนอแนะเบื้องต้น:</u>

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

<u>สรุปแนวทางการจำแนกประเภทข้อมูล</u>

การจำแนกประเภทข้อมูลสำหรับการใช้คลาวด์ในราชอาณาจักรไทยมุ่งเน้นที่ข้อมูลขณะพัก/จัดเก็บ (Data at Rest) และกำหนดให้ข้อมูลทุกประเภทควรจัดเก็บอยู่ในประเทศไทยเป็นลำดับแรก และในกรณีมีความจำเป็นต้องใช้คลาวด์ประเภทอื่นนอกเหนือจากที่แนะนำ ให้**แจ้งสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)** เพื่อรวบรวมและนำเสนอต่อ**คณะกรรมการที่เกี่ยวข้อง**พิจารณาให้ความเห็นชอบตามนโยบายการใช้คลาวด์เป็นหลักต่อไป

DRAFT

การจำแนกประเภทข้อมูลสรุปได้ดังนี้

- ข้อมูลที่สามารถเปิดเผยได้ (Official Data) และ ข้อมูลที่ต้องได้รับความคุ้มครอง (Protected Data) ซึ่งมีคะแนนการประเมินความเสี่ยงระหว่าง 1- 6 คะแนน สามารถใช้ Public Cloud ได้
- สำหรับ ข้อมูลที่ต้องได้รับความคุ้มครองสูงสุด (Highly Protected Data) ซึ่งมีคะแนนการประเมินความเสี่ยงที่ 7 คะแนนขึ้นไป เป็นข้อมูลที่มีผลกระทบต่อความมั่นคงของชาติ จำเป็นต้องมีมาตรการควบคุมรักษาความปลอดภัยที่เข้มงวดสูงสุด และต้องใช้คลาวด์อธิปไตย (Sovereign Cloud) ซึ่งเป็นบริการคลาวด์ที่ฮาร์ดแวร์และข้อมูลทั้งหมดตั้งอยู่ในราชอาณาจักรไทย และเป็นบริการคลาวด์ที่ให้บริการโดยหน่วยงานของรัฐ หรือองค์กรที่รัฐบาลเป็นเจ้าของทั้งหมดหรือส่วนใหญ่ หรือมีอำนาจควบคุม รวมถึงต้องเป็นบริการคลาวด์ที่ให้หน่วยงานของรัฐใช้งานเท่านั้น เนื่องจากเป็นข้อมูลที่เกี่ยวข้องกับความมั่นคงของชาติจึงจำเป็นต้องใช้เครือข่ายบนโครงสร้างพื้นฐานทางกายภาพที่มีความปลอดภัยสูงและมีการควบคุมความปลอดภัยอย่างเข้มงวด

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

ทั้งนี้ กระบวนการนี้ยังเกี่ยวข้องกับการทำงานร่วมกันระหว่างเจ้าของระบบงาน ผู้ปฏิบัติงานฝ่ายเทคโนโลยีสารสนเทศ และผู้ปฏิบัติงานด้านข้อมูลขององค์กร เพื่อให้มีการบริหารจัดการข้อมูลที่เหมาะสมตลอดวงจรชีวิตข้อมูล

DRAFT

จำแนกประเภทข้อมูล	ระดับชั้นข้อมูล	คำนิยามการจำแนกประเภทข้อมูล	ประเภทของบริการคลาวด์ที่แนะนำ
Official Data	เปิดเผย (Open)	ข้อมูลที่สร้าง ประมวลผล ส่ง หรือรับของหน่วยงานภาครัฐและหน่วยงานที่เกี่ยวข้อง ซึ่งอาจก่อให้เกิดความเสียหายได้ไม่เกินความเสียหายในระดับต่ำ หากมีการละเมิดความปลอดภัยจะมีการใช้มาตรฐานการควบคุมที่สามารถคุ้มครองข้อมูลให้มีความปลอดภัยจากการโจมตีในรูปแบบต่างๆ ซึ่งอาจเพิ่มการรับรองมาตรการควบคุม	**Public Cloud** ข้อมูลควรอยู่ในประเทศไทย
	เผยแพร่ภายในองค์กร (Private)		
Protected Data	ลับ (Confidential)	ข้อมูลที่มีความอ่อนไหวสูงที่จำเป็นต้องมีมาตรการควบคุมที่เข้มงวด และมีการกำหนดการใช้เครือข่ายที่ปลอดภัยบนโครงสร้างพื้นฐานทางกายภาพที่มีความปลอดภัย และมีการปฏิบัติอย่างเหมาะสม ซึ่งอาจส่งผลต่อชีวิต (บุคคลหรือกลุ่มบุคคล) หรือสร้างความเสียหายต่อรัฐซึ่งส่งผลต่อความมั่นคงของชาติ และ/หรือความสัมพันธ์ระหว่างประเทศ ความมั่นคง/เสถียรภาพทางการเงิน หรือขัดขวางความสามารถในการสืบสวนคดีอาชญากรรมที่ร้ายแรง หรือองค์กร	
Highly Protected Data	ลับมาก (Secret)	ข้อมูลที่มีความอ่อนไหวเป็นพิเศษ หากเปิดเผยอาจเกิดความเสียหายอย่างร้ายแรงและร้ายแรงที่สุดต่อรัฐซึ่งส่งผลความมั่นคงของชาติหรือพันธมิตร และต้องการมาตรการควบคุมความปลอดภัยที่สูงมาก เพื่อป้องกันการละเมิดข้อมูลจากภัยคุกคามทั้งหมด โดยการใช้เครือข่ายบนโครงสร้างพื้นฐานทางกายภาพที่มีความปลอดภัยสูง และมีการควบคุมความปลอดภัยอย่างเข้มงวด ทั้งนี้ ข้อมูลข่าวสารลับที่สุดต้องปฏิบัติตามระเบียบความลับทางราชการ และ ระเบียบสารบรรณอิเล็กทรอนิกส์ โดยให้หัวหน้าหน่วยงานรัฐใช้ดุลพินิจในการนำข้อมูลเข้าคลาวด์โดยไม่ขัดกับกฎหมายที่เกี่ยวข้อง เช่น การสร้างผ่านคลาวด์ แต่ไม่รวมถึงขั้นตอนการเผยแพร่ (การนำส่ง)	**Sovereign Cloud** ข้อมูลต้องอยู่ในประเทศไทย
	ลับที่สุด (Top Secret)		

i. ข้อมูลที่ควรอยู่ในประเทศไทย หมายถึง ข้อมูลที่จัดเก็บอยู่ในสถานะพัก/จัดเก็บ (Data-at-Rest) โดยไม่รวมถึงข้อมูลที่อยู่ระหว่างการรับส่ง (Data-in-Transit) หรือการประมวลผล (Data Processing)
ii. ถิ่นที่อยู่ข้อมูล: หน่วยงานที่จำเป็นต้องใช้บริการคลาวด์จัดเก็บข้อมูลนอกราชอาณาจักรไทยให้แจ้ง สพร. พิจารณาความเหมาะสมต่อไป
iii. ประเภทบริการคลาวด์: กรณีมีความจำเป็นต้องใช้คลาวด์ประเภทอื่นนอกเหนือจากที่แนะนำข้างต้น ให้แจ้งสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) เพื่อรวบรวมและนำเสนอต่อคณะกรรมการที่เกี่ยวข้องพิจารณาให้ความเห็นชอบตามนโยบายการใช้คลาวด์เป็นหลักต่อไป

ภาพที่ 6: สรุปแนวทางการจำแนกประเภทข้อมูลสำหรับการใช้คลาวด์

3.2 ตัวอย่างการประเมินจำแนกประเภทข้อมูลสำหรับการใช้คลาวด์

ตัวอย่างการประเมินบริการทางดิจิทัล (E-Government Service)

ประเภทข้อมูล					
วัตถุประสงค์ด้านความปลอดภัย (CIA)	**ผลกระทบด้านความลับ (Confidentiality)**	**ผลกระทบด้านความถูกต้องครบถ้วนสมบูรณ์ ความคงสภาพ (Integrity)**		**ผลกระทบด้านความพร้อมใช้งานข้อมูล(Availability)**	
	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบน้อย/อย่างจำกัด (limited) และเกิดผลประโยชน์แห่งชาติ**สำคัญน้อย**	การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบน้อย/อย่างจำกัด (limited) และเกิดผลประโยชน์แห่งชาติ**สำคัญ**		การหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลข่าวสารหรือระบบสารสนเทศอาจส่งผลกระทบน้อย/อย่างจำกัด (limited) และเกิดผลประโยชน์แห่งชาติ**สำคัญน้อย**	
ระดับผล CIA	**ปานกลาง** (2 คะแนน)	**ปานกลาง** (2 คะแนน)		**ต่ำ** (1 คะแนน)	
ค่าเฉลี่ย CIA	**ปานกลาง 2** (1.67 ปัดเป็น 2 คะแนน)				
ผลกระทบ/ผลประโยชน์	**ภาพลักษณ์/ชื่อเสียง**	**ผู้ใช้และการดำเนินงาน**	**การเงินและสินทรัพย์**	**กฎหมายและระเบียบ**	**ผลประโยชน์แห่งชาติ / มั่นคงของรัฐ/ความสงบเรียบร้อย** (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 แต่อาจต้องมีการติดตามเป็นระยะๆ
ลับ	5 - 6	ระดับความเสี่ยงที่องค์กรสามารถยอมรับได้โดยต้องมีมาตรการควบคุมหรือมีแผนการลดความเสี่ยง เพื่อลดความเสี่ยงให้ไปอยู่ในระดับต่ำและป้องกันไม่ให้ความเสี่ยงเพิ่มขึ้น
ลับมาก	7 - 9	ระดับความเสี่ยงที่องค์กรไม่สามารถยอมรับได้ และต้องจัดการลดความเสี่ยงให้ไปอยู่ในระดับต่ำลงโดยเร็ว โดยต้องจัดให้มีแผนการลดความเสี่ยงและป้องกันไม่ให้ความเสี่ยงกลับเพิ่มสูงขึ้นด้วย
ลับที่สุด	10 - 15	ระดับความเสี่ยงที่องค์กรไม่สามารถยอมรับได้ และต้องจัดการลดความเสี่ยงให้ไปอยู่ในระดับต่ำลงในทันที หรืออาจมีการถ่ายโอนความเสี่ยง โดยต้องจัดให้มีแผนการลดความเสี่ยงและป้องกันไม่ให้ความเสี่ยงกลับเพิ่มสูงขึ้นด้วย [4]

[4] หน่วยงานสามารถชี้แจงได้ในกรณีที่บริการของหน่วยงานเป็นระดับชั้นลับที่สุดแต่ไม่สอดคล้องกับนโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติฯ

DRAFT

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

ทั้งนี้ หน่วยงานสามารถทำการประเมินจำแนกประเภทข้อมูลสำหรับการใช้คลาวด์ โดยสามารถประยุกต์การจำแนกประเภทข้อมูลจากเครื่องมือตาม มสพร. 8-2565 และฉบับปรับปรุง เพื่อพิจารณาความเสี่ยงบริการของหน่วยงานภาครัฐในการใช้คลาวด์ โดยมีขั้นตอนดังนี้

1) ประเมินข้อมูลในบริการ โดยพิจารณาจากระดับผลกระทบตามวัตถุประสงค์ด้านความปลอดภัยของข้อมูล (Security Objective) โดยนำผลประโยชน์แห่งชาติจากการเปิดเผยข้อมูลโดยไม่ได้อนุญาตมาประกอบการพิจารณา ตามหลักการวัตถุประสงค์ด้านความปลอดภัย 3 ด้าน (CIA) 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 และฉบับปรับปรุง **มีความสอดคล้องกับการประเมินในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยทางไซเบอร์ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566** ซึ่งการประเมินและจัดระดับผลกระทบที่อาจเกิดขึ้นแบ่งเป็น 3 ระดับ ได้แก่ ระดับต่ำ ระดับกลาง และระดับสูง ดังนี้

ภาพที่ 7: ผลกระทบตาม CIA ตามประกาศ กมช. เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566

DRAFT

ภายหลังจากหน่วยงานได้กำหนดคุณลักษณะความมั่นคงปลอดภัยทางไซเบอร์ และได้ระดับผลกระทบที่อาจเกิดขึ้นแก่ข้อมูลหรือระบบสารสนเทศแล้ว ควรมีกำหนดมาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำสำหรับข้อมูลของระบบสารสนเทศในแต่ละระดับตามที่ประกาศฯ กำหนดไว้ ดังนี้

ลักษณะของผลกระทบ ในแต่ละระดับ อธิบายได้พอสังเขปดังนี้

ผลกระทบระดับต่ำ

ลักษณะผลกระทบ : ความเสียหายที่เกิดขึ้นมีผลกระทบจำกัดในวงแคบ เช่น ส่งผลต่อการทำงานบางส่วนของหน่วยงานในลักษณะที่ไม่สำคัญ ไม่มีผลกระทบต่อชื่อเสียงหลัก หรือการให้บริการที่สำคัญ

ตารางที่ 11: ลักษณะผลกระทบระดับต่ำ

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

ผลกระทบระดับกลาง

ลักษณะผลกระทบ : ความเสียหายที่มีผลต่อการดำเนินงานหรือชื่อเสียงองค์กรในระยะสั้น อาจส่งผลต่อความเชื่อมั่นของประชาชนหรือการบริการ

ตารางที่ 12: 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 กระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศ ความปลอดภัยประชาชน หรือเศรษฐกิจระดับชาติ

ตารางที่ 13: ลักษณะผลกระทบระดับสูง

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

DRAFT

ในกรณีผลการพิจารณาตามหลักการ CIA ที่กล่าวมาข้างต้น หากได้ผลการประเมินอยู่ที่ระดับสูง จะต้องปฏิบัติตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 ได้กำหนดว่า กรณีที่ข้อมูลที่มีผลกระทบระดับสูง หากใช้บริการคลาวด์ควรใช้ศูนย์ข้อมูลหลักในประเทศไทย

ทั้งนี้ การวางมาตรการควบคุมความปลอดภัยในแต่ละระดับจะต้องพิจารณาตามกรอบมาตรฐาน เช่น ISO 27001 สำหรับการจัดการความมั่นคงปลอดภัยของข้อมูล NIST Cybersecurity Framework สำหรับการตรวจสอบและป้องกันภัยทางไซเบอร์ เป็นต้น

อย่างไรก็ดี หน่วยงานควรทบทวนการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศทุก 3 ปีเป็นอย่างน้อย หรือ ทบทวนเมื่อข้อมูล ระบบสารสนเทศ หรือหน้าที่ของหน่วยงานมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ และ ทำการบันทึกผลการพิจารณาทบทวนพร้อมเหตุผล[5]

2) ประเมินหาระดับความเสี่ยงของข้อมูลในบริการตามเกณฑ์การประเมินความเสี่ยงและผลกระทบจากการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต โดยประเมินหาค่าระดับความรุนแรงของผลกระทบ (Impact) ในแต่ละด้าน ได้แก่

- ด้านภาพลักษณ์/ชื่อเสียง (Reputation)
- ผู้ใช้บริการและการดำเนินงานตามภารกิจ (Users & Operations)
- การเงินและสินทรัพย์ (Financial & Assets)
- ความสอดคล้องกับกฎระเบียบ ข้อบังคับ (Legal & Regulation)
- ผลประโยชน์แห่งชาติ (National Interests) ซึ่งรวมถึงความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศ ทั้งนี้ ให้หน่วยงานนำค่าเฉลี่ยที่ได้จากการประเมินในข้อที่ 1 (ค่าเฉลี่ย CIA) มาใส่เพื่อทำการประเมิน

DRAFT

[5] ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยทางไซเบอร์ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566

เกณฑ์การพิจารณาผลกระทบ

ด้าน	เกณฑ์การพิจารณาผลกระทบ		
	1 = ต่ำ	2 = ปานกลาง	3 = สูง
ชื่อเสียง	**น้อย/อย่างจำกัด** โดย ✓ ส่งผลกระทบเล็กน้อยเฉพาะภาพลักษณ์หน่วยงาน หรือบุคคลโดยไม่จำเป็นต้องดำเนินการแก้ไข หรือแก้ไขได้ ใช่หรือไม่ ✓ ส่งผลกระทบต่อการรับรู้บทบาทหน้าที่ของหน่วยงาน ใช่หรือไม่ ✓ ส่งผลกระทบต่อภาพลักษณ์ของระบบการให้บริการ ใช่หรือไม่	**อย่างร้ายแรง** โดย ✓ ส่งผลกระทบเล็กน้อยเฉพาะภาพลักษณ์หน่วยงาน ซึ่งต้องมีการรายงานต่อผู้บริหารระดับสูง ใช่หรือไม่ ✓ ส่งผลความเชื่อมั่นของผู้ใช้บริการ ใช่หรือไม่ ✓ สามารถฟ้องร้องทางคดีแพ่ง ใช่หรือไม่	**อย่างร้ายแรงมาก** โดย ✓ ส่งผลกระทบต่อภาพลักษณ์ชื่อเสียงของรัฐในระดับประเทศ ใช่หรือไม่ ✓ ส่งผลให้เกิดการวิพากษ์ วิจารณ์จากสื่อสาธารณะ ทำให้หน่วยงานต้องดำเนินการแถลงข่าว ใช่หรือไม่ ✓ สามารถฟ้องร้องทางคดีแพ่ง และคดีอาญา ใช่หรือไม่
ผู้ใช้และการดำเนินงาน	**รายบริการ/การดำเนินงานขององค์กร** โดย ✓ ส่งผลกระทบต่อการทำงานภายในหน่วยงาน โดยยังสามารถให้บริการได้อย่างต่อเนื่อง ใช่หรือไม่ ✓ ส่งผลกระทบต่อประสิทธิภาพการทำงานของผู้ปฏิบัติงานของหน่วยงานลดลง ใช่หรือไม่ ✓ ส่งผลการใช้งานของจำนวนผู้ใช้งานในวงแคบ ใช่หรือไม่	**ราย Domain/การดำเนินของกระทรวง/ระหว่าง องค์กร/จังหวัด** โดย ✓ ส่งผลให้เกิดอุปสรรคต่อการทำงานภายในหน่วยงาน และหน่วยงานคู่สัญญา ใช่หรือไม่ ✓ ส่งผลต่อประสิทธิภาพการให้บริการของระบบ ใช่หรือไม่ ✓ บางบริการมีความไม่สะดวก หรือล่าช้า เสียเวลา แต่ยังไม่สูญเสียข้อมูล ใช่หรือไม่ ✓ ส่งผลกระทบต่อผู้ใช้บริการบางส่วน โดยหน่วยงานสามารถชี้แจงข้อร้องเรียนได้ตามระยะเวลาที่กำหนดและ	**Cross Domains, Sectors, Region/การดำเนินงานตามแผนบูรณาการ/กลุ่มจังหวัด** โดย ✓ ส่งผลกระทบต่อการทำงานภายในหน่วยงานเครือข่ายมากกว่า 2 หน่วยงาน ใช่หรือไม่ ✓ ส่งผลกระทบต่อผู้มาใช้บริการทุกคน และกระทบวงกว้างในระดับประเทศ ใช่หรือไม่ ✓ ระบบล่มหรือใช้งานไม่ได้ ทำให้เกิดความเสียหายของผู้ใช้บริการ ใช่หรือไม่ ✓ ข้อมูลในระบบสูญหาย ใช่หรือไม่

DRAFT

ด้าน	เกณฑ์การพิจารณาผลกระทบ		
	1 = ต่ำ	2 = ปานกลาง	3 = สูง
		เริ่มส่งผลกระทบต่อความพึงพอใจของผู้รับบริการ ใช่หรือไม่	
การเงินและสินทรัพย์[6]	**มูลค่าไม่เกิน 5 ล้าน/ Small project** โดย ✓ มูลค่าความเสียหายของการให้บริการหรือโครงการ เช่น ค่าดำเนินการ เช่น ค่าปรับ ค่าเยียวยา ค่าเสียหาย โดยมีมูลค่าไม่เกิน 5 ล้าน ใช่หรือไม่	**ตั้งแต่ 5 ล้านแต่ไม่ถึง 100 ล้าน/ Medium project** โดย ✓ มูลค่าความเสียหายของการให้บริการหรือโครงการ เช่น ค่าดำเนินการ เช่น ค่าปรับ ค่าเยียวยา ค่าเสียหาย โดยมีมูลค่า ตั้งแต่ 5 ล้าน แต่ไม่ถึง 100 ล้านบาท ใช่หรือไม่	**ตั้งแต่ 100 ล้านบาท ขึ้นไป/Large project** โดย ✓ มูลค่าความเสียหายของการให้บริการหรือโครงการ เช่น ค่าดำเนินการ เช่น ค่าปรับ ค่าเยียวยา ค่าเสียหาย โดยมีมูลค่า ตั้งแต่ 100 ล้าน ใช่หรือไม่
กฎหมายและระเบียบข้อบังคับ	**ละเว้นการปฏิบัติตามระเบียบข้อบังคับขององค์กร ซึ่งเกิดผลกระทบน้อย** โดย ✓ ไม่ปฏิบัติตามกฎระเบียบระดับองค์กร ใช่หรือไม่ ✓ ส่งผลให้หน่วยงานได้รับบทลงโทษของหน่วยงาน ใช่หรือไม่	**ละเว้นการปฏิบัติตามระเบียบข้อบังคับและกฎกระทรวง ซึ่งเกิดผลกระทบที่มีนัยสำคัญ และไม่เป็นไปตามเป้าของ ก.พ.ร.** โดย ✓ ไม่ปฏิบัติตามกฎระเบียบระดับกระทรวง เช่น กฎกระทรวง ใช่หรือไม่ ✓ ส่งผลให้หน่วยงานอาจได้รับบทลงโทษทางกฎหมายใช่หรือไม่	**ละเว้นการปฏิบัติตามกฎหมาย มติ ครม. หรือระเบียบข้อบังคับ ซึ่งเกิดผลกระทบที่มีนัยสำคัญ และไม่เป็นไปตามเป้าของแผนบูรณาการ/กลุ่มจังหวัด** โดย ✓ ไม่ปฏิบัติตามกฎหมายอย่างชัดเจน หรือไม่ปฏิบัติตามมติ ครม. รัฐบาล และไม่เป็นไปตามเป้าหมายของแผนบูรณการ ใช่หรือไม่ ✓ ไม่ปฏิบัติตามกฎหมายส่งผลให้หน่วยงานได้รับบทลงโทษทางอาญาและทางแพ่ง หรือ โทษทางปกครอง ใช่หรือไม่ ✓ เกิดความเสียหายอย่างร้ายแรงต่อหน่วยงาน หรือต่อบุคคลอื่นจนเป็นเหตุให้ถูกฟ้องร้องดำเนินคดี ใช่หรือไม่

[6] ทั้งนี้ การพิจารณาเป็นตัวเงินและความสูญเสียหายของ Asset อาจเป็นเรื่องบทลงโทษทางกฎหมาย มูลค่าความเสียหาย ค่าดำเนินการต่างๆ

DRAFT

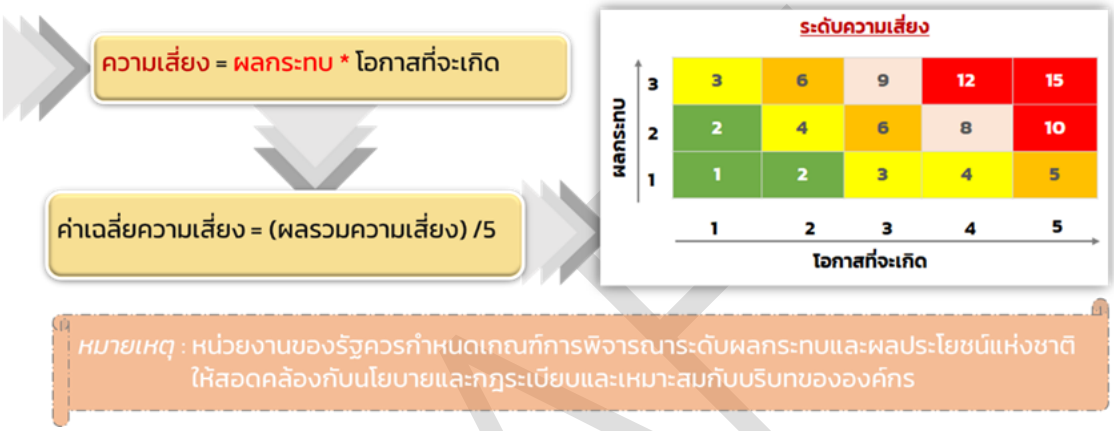
ด้าน	เกณฑ์การพิจารณาผลกระทบ		
	1 = ต่ำ	2 = ปานกลาง	3 = สูง
ผลประโยชน์แห่งชาติ	**ผลประโยชน์แห่งชาติ ที่สำคัญน้อย** โดย ✓ มีผลกระทบจากการเปิดเผยข้อมูลโดยไม่ได้อนุญาตตามหลักการ CIA ในระดับต่ำ ใช่หรือไม่ ✓ การเปิดเผยข้อมูลจะส่งผลให้เกิดอันตรายต่อทรัพย์สิน/ชีวิต/ความปลอดภัยของบุคคลใดบุคคลหนึ่ง ใช่หรือไม่ ✓ ส่งผลกระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศในระดับต่ำ	**ผลประโยชน์แห่งชาติ ที่สำคัญ** โดย ✓ มีผลกระทบจากการเปิดเผยข้อมูลโดยไม่ได้อนุญาต ตามหลักการ CIA ในระดับปานกลาง ใช่หรือไม่ ✓ การเปิดเผยข้อมูลจะส่งผลให้เกิดอันตรายต่อทรัพย์สิน/ชีวิต/ความปลอดภัยของประชาชนบางส่วน ใช่หรือไม่ ✓ สร้างความเสียหายต่อความสัมพันธ์ระหว่างหน่วยงานอื่นๆ ใช่หรือไม่ ✓ ส่งผลกระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศในระดับปานกลาง ใช่หรือไม่	**ผลประโยชน์แห่งชาติ ที่สำคัญยิ่ง** โดย ✓ มีผลกระทบจากการเปิดเผยข้อมูลโดยไม่ได้อนุญาต ตามหลักการ CIA ในระดับสูง ใช่หรือไม่ ✓ การเปิดเผยข้อมูลจะส่งผลให้เกิดอันตรายต่อทรัพย์สิน/ชีวิต/ความปลอดภัยของประชาชนส่วนใหญ่ ใช่หรือไม่ ✓ เกิดความเสียหายต่อความมั่นคงของประเทศ หรือความสัมพันธ์ระหว่างประเทศ หรือความมั่นคงทางเศรษฐกิจของประเทศใช่หรือไม่ ✓ ส่งผลกระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศในระดับสูง

DRAFT

และ**ประเมินหาค่าเฉลี่ยระดับผลกระทบโดยรวม** ซึ่งเกณฑ์การพิจารณาระดับผลกระทบและผลประโยชน์แห่งชาติ ตาม มสพร. 8-2565 และฉบับปรับปรุง ซึ่งสอดคล้องกับข้อ 6 ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566

จากนั้น **ประเมินโอกาสที่จะเกิด** ของความเสี่ยงจากการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต หรือการรั่วไหลของข้อมูลที่จะเกิดขึ้น โดยการพิจารณาจากสถิติการเกิดเหตุการณ์จากในอดีตถึงปัจจุบัน หรือการคาดการณ์ล่วงหน้าของโอกาสที่จะเกิดในอนาคตต่อชุดข้อมูลนั้นๆ

(ข้อเสนอแนะ: ผู้ประเมิน ควรเป็น เจ้าของข้อมูลร่วมกับฝ่ายเทคโนโลยีสารสนเทศ)



ภาพที่ 8: 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

ค่าระดับความเสี่ยง **ระดับ** 7 - 15 จัดอยู่ในระดับความเสี่ยงสูงถึงสูงมาก และ **สอดคล้องตามนโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ (พ.ศ. 2566 – 2570)** หน่วยงานต้องมีการจัดทำเอกสารประกอบการเสนอโครงการและงบประมาณด้านระบบคลาวด์ฯ เพื่อใช้คลาวด์ **ประเภท** Sovereign Cloud

ภาพที่ 9: การติดป้ายหรือแท็กกำกับระดับชั้นข้อมูลตามความอ่อนไหว

ทั้งนี้ หากหน่วยงานของรัฐมีการจัดระดับชั้นข้อมูลและการจำแนกประเภทแล้ว ให้หน่วยงานดำเนินการตาม มรด. 3-2 : 2565 มาตรฐานรัฐบาลดิจิทัลว่าด้วยแนวทางการลงทะเบียนบัญชีข้อมูลภาครัฐ และฉบับปรับปรุง เว้นแต่กรณีชุดข้อมูลที่มีระดับชั้นลับมากและลับที่สุด

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	สำนักงานคณะกรรมการป้องกันและปราบปรามยาเสพติด
9. การป้องกันและบรรเทาสาธารณภัย	● ข้อมูลสาธารณภัยและแผนการบรรเทาทุกข์	กรมป้องกันและบรรเทาสาธารณภัย
10. การป้องกันและแก้ไขปัญหาความมั่นคงทางไซเบอร์	● ข้อมูลการโจมตีทางไซเบอร์และมาตรการในการป้องกัน	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
11. การป้องกันและแก้ไขปัญหาการก่อการร้าย	● ข้อมูลข่าวสารและข่าวกรองด้านการก่อการร้าย	สำนักงานสภาความมั่นคงแห่งชาติ
12. การสร้างดุลยภาพระหว่างประเทศ	● ข้อมูลภัยคุกคามระดับภูมิภาค ● ข้อมูลหมอกควันข้ามแดน	กระทรวงการต่างประเทศ

DRAFT

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

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

DRAFT

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%

DRAFT

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 .

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ. (2567). ประกาศสำนักคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง แนวทางการใช้บริการคลาวด์สาธารณะที่มีศูนย์ข้อมูลหลักในประเทศ ไทย 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.

DRAFT