



**DGA**  
DIGITAL GOVERNMENT  
DEVELOPMENT AGENCY

STANDARDS

**ขอเชิญเข้าร่วมงานรับฟังความคิดเห็นต่อ  
(ร่าง) มาตรฐานรัฐบาลดิจิทัล (มรด.)  
เพื่อเป็นกรอบแนวทางการบริหารจัดการคลาวด์ภาครัฐ**

**ร่วมประชุมการรับฟังความคิดเห็น  
19 ธ.ค. 68 | 13.30 - 15.30 น.  
ผ่านทาง  Microsoft Teams**

**พร้อมเสวนาเรื่อง  
มาตรฐานรัฐบาลดิจิทัล (มรด.)  
เพื่อเป็นกรอบแนวทางการบริหารจัดการคลาวด์ภาครัฐ**

**โดยเปิดรับฟังความคิดเห็นวันที่ 12-27 ธ.ค. 2568**



**QR Code**

สำหรับดาวน์โหลดเอกสาร ร่างมาตรฐานฯ  
แบบแสดงความคิดเห็น แบบฟอร์มลงทะเบียน  
Link งานประชุม และเอกสารอื่นที่เกี่ยวข้อง

# กำหนดการทำงานประชาพิจารณ์

(ร่าง) มาตรฐานรัฐบาลดิจิทัล (มรด.) เพื่อเป็นกรอบแนวทางการบริหารจัดการคลาวด์ภาครัฐ  
ในวันศุกร์ที่ 19 ธันวาคม 2568 เวลา 13.30 – 15.30 น.  
ผ่านระบบการประชุมสื่ออิเล็กทรอนิกส์ Microsoft Teams

## ลงทะเบียน

### ประธานกล่าวเปิดงานและปาฐกถาพิเศษ

เสวนาเรื่อง “มาตรฐานรัฐบาลดิจิทัล (มรด.)  
เพื่อเป็นกรอบแนวทางการบริหารจัดการคลาวด์ภาครัฐ”

### การนำเสนอร่างมาตรฐานรัฐบาลดิจิทัล (มรด.) 2 ฉบับ ได้แก่

- แนวทางการใช้คลาวด์
- แนวทางการกำหนดมาตรฐานผู้ให้บริการคลาวด์

### รับฟังข้อเสนอแนะและตอบคำถาม

13.00 – 13.30 น.

13.30 – 13.45 น.

13.45 – 14.30 น.

14.30 – 15.00 น.

15.00 – 15.30 น.



**QR Code ข้อมูล  
งานประชาพิจารณ์**



# ปาฐกถาพิเศษงานประชาพิจารณ์

(ร่าง) มาตรฐานรัฐบาลดิจิทัล (มรต.)

เพื่อเป็นกรอบแนวทางการบริหารจัดการคลาวด์ภาครัฐ

## นโยบายการใช้คลาวด์

เป็นแนวทางสำคัญในการขับเคลื่อนภาครัฐให้บรรลุเป้าหมายของการพัฒนาประเทศตามยุทธศาสตร์ชาติ (ปี 2561–2580) ซึ่งให้ความสำคัญกับการใช้เทคโนโลยีคลาวด์มาเป็นเครื่องมือสำคัญในการตอบสนองต่อความต้องการ **เพื่อให้กระบวนการทำงานและการให้บริการประชาชนมีประสิทธิภาพ ลดต้นทุน และเสริมความมั่นคงปลอดภัยของระบบสารสนเทศภาครัฐ**

ทั้งนี้ เพื่อให้หน่วยงานของรัฐสามารถดำเนินการอย่างสอดคล้อง จึง **จำเป็นต้องมีกรอบการบริหารจัดการระบบคลาวด์ภาครัฐ** รวมทั้งรายละเอียดการปฏิบัติ และการสนับสนุนในส่วนที่เกี่ยวข้อง

”

**ดร.อาคิส อัญญาโพธิ์**

รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล



# การดำเนินงานที่ผ่านมา

## มติการประชุมคณะกรรมการพัฒนารัฐบาลดิจิทัลที่เกี่ยวข้อง

### การประชุมครั้งที่ 2/2567 วันที่ 15 พ.ย. 2567

- เห็นชอบการบริหารจัดการคลาวด์ภาครัฐตามนโยบาย Go Cloud First ที่คณะกรรมการเฉพาะด้านคลาวด์ของกระทรวง DE เสนอ (สพร. มีการจัดทำร่างมาตรฐานที่เกี่ยวข้อง และนำไปรับฟังความคิดเห็น #1 ระหว่างวันที่ 3 ก.พ. – 3 มี.ค. 2568)

### การประชุมครั้งที่ 3/2567 วันที่ 1 ธ.ค. 2567

- มอบหมาย สพร. ให้เป็นผู้ดำเนินการขึ้นทะเบียนผู้ให้บริการคลาวด์
- มอบหมาย สพร. เป็นผู้บริหารจัดการบริการคลาวด์ภาครัฐ (Government Cloud Management)

### การประชุมครั้งที่ 1/2568 วันที่ 21 ก.ค. 2568

- เห็นชอบปรับเปลี่ยนแนวทางการใช้คลาวด์ โดยให้ใช้ Sovereign Cloud สำหรับข้อมูลระดับลับมากและลับที่สุด และกำหนดให้การจัดหาบริการคลาวด์ภาครัฐสำหรับข้อมูลระดับอื่นเป็นแบบรวมศูนย์โดยให้ กระทรวง DE ดำเนินการ (สพร. ปรับปรุงร่างมาตรฐานที่เกี่ยวข้อง และนำไปรับฟังความคิดเห็น #2 ระหว่างวันที่ 29 ก.ค. – 12 ส.ค. 2568)

### การประชุมครั้งที่ 2/2568 วันที่ 3 ก.ย. 2568

- เห็นชอบร่างมาตรฐานผู้ให้บริการคลาวด์และนำไปรับฟังความคิดเห็นจากผู้มีส่วนได้ส่วนเสีย (สพร. จัดรับฟังความคิดเห็นจากผู้ให้บริการคลาวด์ วันที่ 3 ก.ย. 2568)

# การบูรณาการโครงสร้างพื้นฐานทางดิจิทัล (National Cloud)

## การประชุมคณะกรรมการพัฒนารัฐบาลดิจิทัล ครั้งที่ 3/2568 วันที่ 28 พ.ย. 2568

National Cloud คือ การบูรณาการระบบนิเวศคลาวด์ของประเทศไทยที่รวม คลาวด์กลางภาครัฐ (GDCC) และคลาวด์ของหน่วยงานรัฐเข้าไว้ด้วยกัน ภายใต้มาตรฐานที่คณะกรรมการพัฒนารัฐบาลดิจิทัลกำหนด มีการใช้กลไกการจัดหาบริการแบบรวมศูนย์ (Centralized Procurement) เพื่อรวมความต้องการใช้งาน (Demand Aggregation) ลดความซ้ำซ้อนของงบประมาณ และเพิ่มอำนาจต่อรองภาครัฐ และเชื่อมโยงระบบทั้งหมดเข้าสู่ Cloud Management Platform (CMP) ของกระทรวงดิจิทัลฯ เพื่อการบริหารจัดการที่เป็นเอกภาพ

ทั้งนี้ การดำเนินงานจะยึดหลัก อธิปไตยทางข้อมูล (Data Sovereignty) อย่างเคร่งครัด โดยกำหนดให้การจัดหาและจัดเก็บข้อมูลต้องสอดคล้องกับ ระดับชั้นข้อมูล (Security Classification) เพื่อให้มั่นใจว่าข้อมูลความมั่นคงของชาติอยู่ภายใต้อำนาจอธิปไตยของกฎหมายไทย

**ประโยชน์สำหรับประชาชน**

ได้รับ Digital Service ที่ดี มีความเสถียร มีความมั่นคงปลอดภัยสูง รองรับผู้ใช้งานได้จำนวนมาก

**ประโยชน์สำหรับภาครัฐ**

ลดการลงทุนซ้ำซ้อน ลดภาระในการบำรุงรักษาระบบ ยกกระดับการบริหารงานและการให้บริการภาครัฐให้มีประสิทธิภาพ ยกกระดับสู่ "National Data Infrastructure"

# แนวทางการบูรณาการโครงสร้างพื้นฐานทางดิจิทัล (National Cloud)

## Classification and Deployment

- หน่วยงานต้องจำแนกประเภทข้อมูลตามระดับความเสี่ยงเพื่อเลือกใช้ระบบที่เหมาะสม
  - **ภารกิจบริการประชาชน: ให้ใช้ Public Cloud** จากบัญชี Shortlist ของ DGA
  - ข้อมูลลับที่สุด: ให้พิจารณาใช้ Sovereign Cloud ตามที่กระทรวง DE กำหนด
- ในระยะแรกให้มีการ **ยกเว้น ระบบด้านความมั่นคง (ตามนโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ) และบริการ Critical Information Infrastructure (CII) ออกจากเกณฑ์ปกติก่อน** โดยจะกำหนดมาตรการเฉพาะเพิ่มเติมสำหรับระบบ/บริการกลุ่มนี้ในภายหลัง)

## Data Sovereignty

- **ข้อมูลภาครัฐต้องจัดเก็บ (Data Location) อยู่ในราชอาณาจักรไทยเป็นหลัก** เพื่อป้องกันความเสี่ยงทางกฎหมายข้ามพรมแดนและรักษาอธิปไตยของข้อมูล
- ในกรณีที่มีความจำเป็นต้องใช้บริการคลาวด์ที่จัดเก็บข้อมูลนอกราชอาณาจักร อาทิ กรณีไม่มีบริการเทียบเคียงภายในประเทศ หรือเพื่อวัตถุประสงค์ในการสำรองข้อมูล (Disaster Recovery) ให้อยู่ในดุลยพินิจของหัวหน้าส่วนราชการ โดยต้องกำกับดูแลให้สิทธิความเป็นเจ้าของ อำนาจการควบคุม และการบริหารจัดการข้อมูล ยังคงอยู่ภายใต้บังคับของกฎหมายไทยอย่างเคร่งครัด

## Management and Procurement

- การจัดหาบริการคลาวด์ให้ใช้รูปแบบ การจัดหาแบบรวมศูนย์ โดยให้ดำเนินการผ่าน **คลาวด์กลางภาครัฐ (GDCC) เป็นลำดับแรก (First Priority)\*** เพื่อรวมปริมาณความต้องการ (Demand Aggregation) และเพิ่มอำนาจต่อรองสูงสุด
- **ใช้ระบบ Cloud Management Platform ของกระทรวง DE** เป็นศูนย์กลางในการบริหารจัดการทรัพยากร และติดตามการใช้บริการคลาวด์ (Monitoring) ของหน่วยงานรัฐทั้งระบบ

\* **ที่มา:** การประชุมเตรียมการของผู้แทนหน่วยงานที่จะมาเป็นคณะทำงานพิจารณาคลังกรองโครงการฯ (คณะที่ 2)

## Standard and Compliance

- **สพร. (DGA) จัดทำมาตรฐาน**แนวทางการใช้และการให้บริการคลาวด์ (Cloud Standards)
- **สพร. จัดทำบัญชีรายชื่อผู้ให้บริการที่ผ่านการรับรอง (Shortlist)** ซึ่งครอบคลุมทั้งผู้ให้บริการในประเทศและต่างประเทศ ที่ได้มาตรฐาน เพื่อให้หน่วยงานรัฐเลือกใช้ได้อย่างมั่นใจและรวดเร็ว

# ร่างประกาศและมาตรฐานที่อยู่ระหว่างการพิจารณา ของคณะกรรมการพัฒนารัฐบาลดิจิทัล

**ร่าง ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง กรอบแนวทางการบริหารจัดการคลาวด์ภาครัฐตามนโยบาย National Cloud**  
กำหนดแนวทางหลักเพื่อให้เทคโนโลยีคลาวด์เป็นโครงสร้างพื้นฐานด้านดิจิทัลที่สำคัญของหน่วยงานรัฐ ยกกระตือการบริการงานและการให้บริการภาครัฐให้มีประสิทธิภาพ รำรงไว้ซึ่งอธิปไตยข้อมูล (Data Sovereignty)

## มาตรฐานที่เกี่ยวข้องกับนโยบายการใช้คลาวด์เป็นหลัก

**ร่าง ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง มาตรฐานการบริหารจัดการคลาวด์ภาครัฐ**  
กำหนดมาตรฐานเกี่ยวกับการบริหารจัดการคลาวด์สำหรับผู้ให้บริการคลาวด์ภาครัฐ และสำหรับหน่วยงานรัฐที่เป็นผู้ใช้บริการคลาวด์ โดยมาตรฐานต่าง ๆ นี้จะสอดคล้องกับประกาศกรอบแนวทางการบริหารจัดการคลาวด์ภาครัฐ

### 1. Cloud Usage

- แนวปฏิบัติให้หน่วยงานภาครัฐสามารถวางแผนบริหารจัดการ และย้ายโอนระบบงาน (Migration) ขึ้นสู่ระบบคลาวด์ได้อย่างมีประสิทธิภาพ เป็นระบบ และมีความมั่นคงปลอดภัย ภายใต้การปฏิบัติตามกฎหมายและระเบียบที่เกี่ยวข้องอย่างเคร่งครัด
- มีการจัดทำ (ร่าง) มาตรฐานไว้แล้ว

### 2. Cloud Providers

- มาตรฐานที่ผู้ให้บริการคลาวด์ต้องปฏิบัติตาม เพื่อสร้างความมั่นใจให้แก่หน่วยงานรัฐ ในด้านความมั่นคงปลอดภัยและคุณภาพของบริการคลาวด์ที่นำมาใช้งาน
- มีการจัดทำ (ร่าง) มาตรฐานไว้แล้ว

**ร่าง ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง หลักเกณฑ์ วิธีการ และเงื่อนไขการตรวจประเมินและรับรองผู้ให้บริการคลาวด์**  
กำหนดหลักเกณฑ์ วิธีการ และเงื่อนไขในการตรวจประเมินและรับรองความสอดคล้องของการบริหารจัดการคลาวด์ของผู้ให้บริการคลาวด์ตามมาตรฐานที่คณะกรรมการฯ กำหนด โดยการรับรองนี้ เป็นไปตาม พ.ร.บ. การบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 และประกาศกรอบแนวทางการบริหารจัดการคลาวด์ภาครัฐ

ผ่านการประชาพิจารณ์แล้วในวันที่ 29 ก.ค. - 12 ส.ค. 2568 และผ่าน Focus group ร่วมกับผู้ให้บริการคลาวด์ เมื่อวันที่ 3 ก.ย. 2568 แต่ต้องได้รับการปรับปรุงให้สอดคล้องกับแนวนโยบายปัจจุบัน

# แนวทางการจำแนกประเภทข้อมูลเพื่อใช้บริการคลาวด์

ระดับชั้นข้อมูล	จำแนกประเภทข้อมูล	คำอธิบาย	ประเภทบริการคลาวด์ที่แนะนำ	ข้อกำหนดด้านถิ่นที่อยู่ของข้อมูล
1 เปิดเผย (Public)	Official Data	ข้อมูลข่าวสารที่รัฐเปิดเผยให้ประชาชนโดยทั่วไปผ่านเว็บไซต์ Social media	Public Cloud	<b>ควรอยู่ในประเทศไทย</b> (ให้หัวหน้าส่วนราชการพิจารณาความจำเป็นและความเหมาะสม)
2 เผยแพร่ภายในองค์กร (Internal)		ข้อมูลที่หน่วยงานใช้ในการปฏิบัติงานภายใน เช่น หนังสือสารบรรณ การประชุมออนไลน์ เอกสารจัดซื้อจัดจ้าง เป็นต้น		
3 ลับ (Confidential)	Protected Data	ข้อมูลที่หากเปิดเผยอาจเกิดความเสียหายต่อรัฐ เช่น ข้อมูลการเสียหาย ข้อมูลบัญชีธนาคาร ข้อมูลประวัติการรักษาพยาบาล	<b>Public Cloud</b> (with enhanced security e.g. VPC)	
4 ลับมาก (Secret)		ข้อมูลที่หากเปิดเผยอาจเกิดความเสียหายร้ายแรงต่อรัฐ เช่น ข้อมูลประวัติการรักษาพยาบาลของประชาชนจำนวนมาก ข้อมูลเกี่ยวกับการบังคับใช้กฎหมาย แผนการป้องกันประเทศ ข้อมูลเกี่ยวกับความสัมพันธ์ระหว่างประเทศ		
5 ลับที่สุด (Top Secret)	Highly Protected Data	ข้อมูลที่หากเปิดเผยอาจเกิดความเสียหายร้ายแรงที่สุดต่อรัฐ เช่น แผนปฏิบัติการทางทหาร ข้อมูลเกี่ยวกับความมั่นคงของสถาบันพระมหากษัตริย์	<b>Sovereign Cloud</b> (กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม กำหนดผู้ให้บริการ)  <b>หรือ Hybrid Cloud</b> (เฉพาะบริการด้านความมั่นคงที่กำหนด)	

## หมายเหตุ

- ข้อมูลที่ควรอยู่ในประเทศไทย หมายถึง ข้อมูลที่จัดเก็บอยู่ในสถานะพัก (Data-at-Rest) โดยไม่รวมถึงข้อมูลที่อยู่ระหว่างการรับส่ง (Data-in-Transit) หรือการประมวลผล (Data Processing)
- หากมีการทบทวนปรับเปลี่ยนระดับชั้นความลับของข้อมูล (Re-classification) หรือการยกเลิกชั้นความลับ (De-classification) ในภายหลัง ให้นำหน่วยงานสามารถปรับเปลี่ยนรูปแบบการใช้บริการคลาวด์ให้สอดคล้องกับสถานะความสำคัญใหม่ของข้อมูลได้
- Sovereign Cloud (คลาวด์อธิปไตย) หมายถึง บริการคลาวด์ที่อยู่ภายใต้การควบคุมโดยภาครัฐและดูแลโดยบุคลากรที่ได้รับอนุญาต และใช้สำหรับให้บริการกับหน่วยงานของรัฐเท่านั้น

# แนวทางการขึ้นทะเบียนผู้ให้บริการคลาวด์

	Cloud Service Provider Tier 1	Cloud Service Provider Tier 2	Cloud Service Provider Tier 3
<b>1. ขอบเขตการให้บริการรับรอง</b>	ผู้ให้บริการคลาวด์หรือผู้แทนที่ประสงค์จะให้บริการภาครัฐ ให้ครอบคลุมทั้งด้านความมั่นคงปลอดภัยและการคุ้มครองข้อมูลส่วนบุคคล การรักษาอธิปไตยทางข้อมูล คุณภาพบริการและธรรมาภิบาล ตลอดจนขีดความสามารถในการเชื่อมโยงระบบ (Interoperability) เข้ากับแพลตฟอร์มบริหารจัดการกลางของภาครัฐได้อย่างมีประสิทธิภาพ		
<b>2. อายุการรับรอง</b>	3 ปี / รูปแบบการรับรองตามมาตรฐานสากล		
<b>3. คุณสมบัติของผู้ยื่นคำขอ</b>	<ol style="list-style-type: none"> <li>เป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย และมีทุนจดทะเบียน โดยจะต้องพิจารณามูลค่าของทุนจดทะเบียนที่เรียกชำระมูลค่าหุ้นแล้ว และมูลค่าสุทธิของกิจการ ณ วันที่ตรวจประเมิน</li> <li>กรณีเป็นตัวแทนจะต้องมีหนังสือแต่งตั้งจากผู้ให้บริการคลาวด์ หรือผู้จัดจำหน่ายประเภท <b>Distributor</b> ของผู้ให้บริการคลาวด์ต้นทาง</li> <li>มีบริการและผลิตภัณฑ์ อยู่ในกลุ่มบริการในการเลือกใช้บริการคลาวด์ พร้อมรายละเอียด และราคาต่อหน่วย</li> </ol>	คุณสมบัติของผู้ยื่นคำขอ Tier 1-2 และ เป็นผู้ให้บริการคลาวด์อธิปไตย (Sovereign Cloud) หรือ คลาวด์แบบผสม (Hybrid Cloud) ตามที่กระทรวงดิจิทัลฯ กำหนด	
<b>4. เสถียรภาพทางการเงิน</b>	<ol style="list-style-type: none"> <li>มีเสถียรภาพทางการเงิน ทุนจดทะเบียน และมูลค่าสุทธิของกิจการ ณ วันที่ขอรับการตรวจประเมิน</li> <li>หลังได้รับการตรวจประเมินแล้ว: สำนักงานจะพิจารณาจาก ผลการดำเนินการ และ รายงานสถานะทางการเงิน อย่างต่อเนื่อง หากพบว่ามีความเสี่ยงต่อการให้บริการ ผู้ให้บริการจะต้องจัดทำรายละเอียดเพื่อชี้แจงเพิ่มเติม เช่น แผนการชดเชยหรือเยียวยาผู้ใช้บริการ</li> </ol>		
<b>5. มาตรฐานที่จำเป็นที่ต้องใช้ในการขึ้นทะเบียน</b>	<b>ด้านการรักษาความมั่นคงปลอดภัยในการใช้คลาวด์:</b> CSA STAR, ISO/IEC 27001 <b>ด้านการบริหารจัดการบริการ :</b> ISO/IEC 20000 <b>ด้านการป้องกันข้อมูลส่วนบุคคล :</b> ISO/IEC 27701	<b>ด้านการรักษาความมั่นคงปลอดภัยในการใช้คลาวด์:</b> CSA STAR, ISO/IEC 27001, ISO/IEC 27017 <b>ด้านการบริหารจัดการบริการ :</b> ISO/IEC 20000 <b>ด้านการป้องกันข้อมูลส่วนบุคคล :</b> ISO/IEC 27701, ISO/IEC 27018	มาตรฐานที่จำเป็นต้องใช้ในการขึ้นทะเบียนระดับ Tier 2 และมาตรการรักษาความมั่นคงปลอดภัยเพิ่มเติม เช่น การใช้ isolated network
<b>6. ระดับชั้นข้อมูลที่ให้บริการกับหน่วยงานภาครัฐได้</b>	ข้อมูลที่สามารถเปิดเผยได้ (Official Data)	ข้อมูลที่สามารถเปิดเผยได้ (Official Data) และ ข้อมูลที่ต้องได้รับความคุ้มครอง(Protected Data)	ข้อมูลที่ต้องได้รับความคุ้มครองสูงสุด (Highly Protected Data) เท่านั้น

ทั้งนี้ มติที่ประชุม กกต DG มีมติให้จัดทำรายละเอียดเพิ่มเติม เรื่อง

1. ความชัดเจน เรื่อง เสถียรภาพทางการเงิน ให้เป็นไปตามหนังสือเวียนกรมบัญชีกลาง ที่ กค (ทวจ) 56/ว 48 เรื่องแนวทางการพิจารณางบแสดงฐานะการเงินฯ
2. มาตรฐานที่จำเป็นสำหรับศูนย์ข้อมูล (Data Center) โดยทาง สพร. จะนำไปประชาสัมพันธ์และร่วมหารือกับผู้ให้บริการคลาวด์ (CSP) ต่อไป

# แนวทางการจัดหาบริการคลาวด์ ปี 2570

ที่มา : คณะทำงานพิจารณากลับกรองโครงการ/กิจกรรม และงบประมาณรายจ่ายบูรณาการรัฐบาลดิจิทัลฯ (คณะที่ 2)

1. ใช้รูปแบบการจัดหาแบบรวมศูนย์ (Centralized) ผ่านคลาวด์กลางภาครัฐ (GDCC) เป็นอันดับแรก
2. กรณีมีการใช้คลาวด์ ให้ขอรับจัดสรรงบประมาณภายใต้แผนงานบูรณาการรัฐบาลดิจิทัล หากมีการของบประมาณเพื่อจัดหาคลาวด์นอกแผนงานบูรณาการรัฐบาลดิจิทัล จะไม่รับการพิจารณาจัดสรรงบประมาณให้
3. การขอรับจัดสรรงบประมาณเพื่อจัดหาคลาวด์ ภายใต้แผนงานบูรณาการรัฐบาลดิจิทัล ไม่ว่าจะอยู่ในแนวทางใด (แนวทางที่ 1, 2 หรือ 3) ต้องทำตามแบบฟอร์มคำขอของงบประมาณภายใต้แผนงานบูรณาการรัฐบาลดิจิทัล และตามตารางสรุปรายการ งบประมาณ จำนวน และรูปแบบการใช้คลาวด์
4. หากคลาวด์กลางภาครัฐ (GDCC) ไม่เพียงพอ หรือไม่มีบริการที่หน่วยงานต้องการ รวมทั้งกรณีเป็นการจัดหาคลาวด์แบบต่อเนื่อง จะได้รับการพิจารณาอนุมัติยกเว้นจาก กกก. บูรณาการฯ เพื่อให้หน่วยงานจัดหาเอง
5. หน่วยงานที่จัดหาคลาวด์เอง หรือมีการใช้บริการบนคลาวด์ จะต้องให้ผู้ให้บริการคลาวด์ดำเนินการเชื่อมโยงข้อมูลระบบคลาวด์กับระบบบริหารจัดการคลาวด์กลาง (Cloud Management Platforms) ของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
6. แนวทางนี้ ใช้สำหรับหน่วยงานที่ขอรับจัดสรรงบประมาณแผ่นดินเท่านั้น

# การประชุมครั้งที่ 3/2568 วันที่ 28 พ.ย. 2568

## หลักการการบูรณาการโครงสร้างพื้นฐานทางดิจิทัล (National Cloud)

### ประเด็นเสนอที่ประชุมคณะกรรมการพัฒนารัฐบาลดิจิทัลพิจารณา

1. เพื่อพิจารณาเห็นชอบ แนวทางการบูรณาการโครงสร้างพื้นฐานทางดิจิทัล (National Cloud)
2. เพื่อพิจารณาเห็นชอบ แนวทางการจำแนกประเภทข้อมูลบนคลาวด์ แนวทางการขึ้นทะเบียนผู้ให้บริการคลาวด์ ที่เสนอ และมอบหมาย สพร. ให้ปรับปรุง ร่างมาตรฐานต่าง ๆ ที่เกี่ยวข้อง พร้อมนำไปรับฟังความคิดเห็นและเสนอคณะกรรมการฯ เห็นชอบก่อนประกาศบังคับใช้
3. เพื่อพิจารณามอบหมาย กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เป็นผู้บริหารจัดการบริการคลาวด์ภาครัฐ (Government Cloud Management) เพื่อให้สอดคล้องกับนโยบายการจัดการจัดหาแบบรวมศูนย์
4. เพื่อพิจารณาเห็นชอบ แนวทางการจัดหาบริการคลาวด์ ปี 2570

## คณะกรรมการ/คณะอนุกรรมการ/ข้อกฎหมายที่เกี่ยวข้อง

- คณะกรรมการจัดทำร่างมาตรฐาน ข้อกำหนดและหลักเกณฑ์ ภายใต้พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 (SC)
- คณะอนุกรรมการสถาปัตยกรรมและมาตรฐานการพัฒนารัฐบาลดิจิทัล (DGS)
- คณะกรรมการพัฒนารัฐบาลดิจิทัล (DG)

# มติที่ประชุมคณะกรรมการพัฒนารัฐบาลดิจิทัล

เนื่องจากการประชุมคณะกรรมการพัฒนารัฐบาลดิจิทัล ครั้งที่ 3/2568 เมื่อวันศุกร์ที่ 28 พฤศจิกายน 2568 คณะกรรมการพัฒนารัฐบาลดิจิทัลมีมติเรื่องแนวทางการบูรณาการโครงสร้างพื้นฐานทางดิจิทัล (National Cloud) ของไทย ดังนี้

## มติที่ประชุมคณะกรรมการพัฒนารัฐบาลดิจิทัล

(เรื่องเพื่อพิจารณา ระเบียบวาระที่ 3.1 แนวทางการบูรณาการโครงสร้างพื้นฐานทางดิจิทัล (National Cloud) ของไทย

1. เห็นชอบ แนวทางการบูรณาการโครงสร้างพื้นฐานทางดิจิทัล (National Cloud)
2. เห็นชอบ แนวทางการจำแนกประเภทข้อมูลบนคลาวด์ แนวทางการขึ้นทะเบียนผู้ให้บริการคลาวด์ ที่เสนอ และมอบหมาย สพร. ให้ปรับปรุง ร่างมาตรฐานต่าง ๆ ที่เกี่ยวข้อง พร้อมนำไปรับฟังความคิดเห็นและเสนอคณะกรรมการฯ เห็นชอบก่อนประกาศบังคับใช้
3. มอบหมาย กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เป็นผู้บริหารจัดการบริการคลาวด์ภาครัฐ (Government Cloud Management) เพื่อให้สอดคล้องกับนโยบายการจัดการจัดหาแบบรวมศูนย์
4. เห็นชอบ แนวทางการจัดหาบริการคลาวด์ ปี 2570

ดังนั้น สพร. จึงมีความจำเป็นต้องปรับปรุง ร่างมาตรฐานคลาวด์ และร่างประกาศที่เกี่ยวข้อง ให้มีความสอดคล้องกับมติที่ประชุมคณะกรรมการฯ



# “ มาตรฐานรัฐบาลดิจิทัล (มรด.) เพื่อเป็นกรอบแนวทางการบริหารจัดการคลาวด์ภาครัฐ ”



**ผู้ช่วยศาสตราจารย์  
ดร.ณัฐวุฒิ หนูไพโรจน์**

อาจารย์ประจำภาควิชาวิศวกรรมคอมพิวเตอร์  
คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย  
และดำรงตำแหน่ง ประธานคณะกรรมการจัดทำร่างมาตรฐาน  
ข้อกำหนด และหลักเกณฑ์ ภายใต้พระราชบัญญัติ  
การบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562



**รองศาสตราจารย์  
ดร.เกริก ภิรมย์โสกา**

อาจารย์ประจำภาควิชาวิศวกรรมคอมพิวเตอร์  
คณะวิศวกรรมศาสตร์  
จุฬาลงกรณ์มหาวิทยาลัย  
และดำรงตำแหน่ง ประธานคณะทำงานเทคนิค  
ด้านมาตรฐานกระบวนการ  
และการดำเนินงานทางดิจิทัล



**ผู้ช่วยศาสตราจารย์  
ดร.มารอง พงศ์สิทธิ์**

รองอธิการบดีฝ่ายการเงิน ทรัพย์สินและสารสนเทศ  
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี  
และดำรงตำแหน่ง  
ประธานคณะทำงานเทคนิคด้านมาตรฐานการเชื่อมโยง  
และแลกเปลี่ยนข้อมูลภาครัฐ



**ดร.อุริชฎา เกตุพรหม**

ผู้อำนวยการฝ่ายมาตรฐานดิจิทัลภาครัฐ  
สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

## ข้อคำถามการเสวนา

Q:

ในฐานะที่ท่านเป็นประธานคณะกรรมการจัดทำร่างมาตรฐาน ข้อกำหนด และหลักเกณฑ์ ภายใต้พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 หรือ SC **จากประสบการณ์ที่ใช้งานคลาวด์ ท่านมีความคิดเห็นอย่างไรเกี่ยวกับ ความจำเป็น และประโยชน์ของ มาตรฐานรัฐบาลดิจิทัล เพื่อกำหนดกรอบแนวทางการบริหารจัดการคลาวด์ภาครัฐ**

**ผู้ช่วยศาสตราจารย์ ดร.ณัฐวุฒิ หนูไพโรจน์**

- อาจารย์ประจำภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
- ประธานคณะกรรมการจัดทำร่างมาตรฐาน ข้อกำหนด และหลักเกณฑ์ ภายใต้พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562

## ข้อคำถามการเสวนา

Q:

ในฐานะที่ท่านเป็นประธานคณะทำงานเทคนิคด้านมาตรฐานกระบวนการและการดำเนินงานทางดิจิทัล หรือ TC1 อยากให้ท่านช่วย**แบ่งปันประสบการณ์ การประยุกต์ใช้คลาวด์ของทางมหาวิทยาลัย** หรือให้**ข้อคิดเห็นอันเป็นประโยชน์**

### รองศาสตราจารย์ ดร.เกริก ภิรมย์โสภา

- อาจารย์ประจำภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
- ประธานคณะทำงานเทคนิคด้านมาตรฐานกระบวนการ และการดำเนินงานทางดิจิทัล (TC1)



## ข้อคำถามการเสวนา

**Q:**

ในฐานะที่ท่านเป็นประธานคณะกรรมการทำงานเทคนิคด้านมาตรฐานการเชื่อมโยงแลกเปลี่ยนข้อมูลภาครัฐ หรือ TC3 อยากให้ท่าน

- **ช่วยให้มุมมองหรือแนวทางการเลือกผู้ให้บริการคลาวด์ เพื่อให้สามารถตอบสนองความต้องการของหน่วยงานรัฐได้อย่างเหมาะสม**
- **แบ่งปันประสบการณ์ การประยุกต์ใช้คลาวด์ของทางมหาวิทยาลัย หรือให้ข้อคิดเห็นอันเป็นประโยชน์**

### ผู้ช่วยศาสตราจารย์ ดร.มารอง พดุงสิทธิ์

- รองอธิการบดีฝ่ายการเงิน ทรัพย์สินและสารสนเทศ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี
- ประธานคณะกรรมการทำงานเทคนิคด้านมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ (TC3)

# ถาม & ตอบ ช่วงการเสวนา



**QR Code**  
ข้อมูลงานประชาพิจารณ์

# การนำเสนอร่างมาตรฐาน รัฐบาลดิจิทัล (มรต.)





# (ร่าง) มาตรฐานรัฐบาลดิจิทัล (มรต.) แนวทางการใช้คลาวด์ เวอร์ชัน 1.0

# (ร่าง) มาตรฐานรัฐบาลดิจิทัล (มรด.) ว่าด้วยแนวทางการใช้คลาวด์ เวอร์ชัน 1.0



## มาตรฐานรัฐบาลดิจิทัล

Digital Government Standard

มรด. 9-X : 256X

DGS 9-X : 256X

## ว่าด้วยแนวทางการใช้คลาวด์

Cloud Usage Standard

เวอร์ชัน 1.0

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

สำนักนายกรัฐมนตรี

เอกสารนี้เป็นทรัพย์สินของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ห้ามให้ทำการคัดลอก ทำซ้ำ แพร่ หรือหนึ่งส่วนใด  
ในเอกสารฉบับนี้ ในรูปแบบใด ๆ แก่บุคคลภายนอก โดยไม่ได้รับอนุญาต การฝ่าฝืนถือเป็นความผิดตามระเบียบของสำนักงานฯ

## สารบัญ

1. บทนำ .....	1
2. แนวทางการเลือกใช้บริการคลาวด์ของหน่วยงานภาครัฐ .....	5
3. แนวทางการประเมินราคา วางแผนงบประมาณ และบริหารการใช้บริการ .....	16
บรรณานุกรม .....	26

# (ร่าง) มาตรฐานรัฐบาลดิจิทัล (มรด.) ว่าด้วยแนวทางการใช้คลาวด์ เวอร์ชัน 1.0

## หลักการและความจำเป็น

เพื่อรองรับการเปลี่ยนผ่านสู่รัฐบาลดิจิทัล หน่วยงานของรัฐจึงนำเทคโนโลยีคลาวด์มาใช้เพื่อเพิ่มประสิทธิภาพและลดภาระด้านโครงสร้างพื้นฐาน อย่างไรก็ตาม ความแตกต่างของบริบทแต่ละหน่วยงานทำให้การเลือกใช้คลาวด์ต้องคำนึงถึงการบูรณาการ ความมั่นคงปลอดภัย และความคุ้มค่าโดยรวม เพื่อให้การบริหารจัดการทรัพยากรเกิดประสิทธิผลในระยะยาว

## วัตถุประสงค์

มาตรฐานว่าด้วยแนวทางการใช้คลาวด์ฉบับนี้จัดทำขึ้น เพื่อเป็นกรอบให้หน่วยงานของรัฐนำเทคโนโลยีคลาวด์ไปใช้ได้อย่างเหมาะสม สอดคล้องกับบริบทของบริการ สนับสนุนการเปลี่ยนผ่านสู่รัฐบาลดิจิทัล เพิ่มประสิทธิภาพและความมั่นคงปลอดภัยในการให้บริการประชาชน พร้อมทั้งส่งเสริมความคุ้มค่าในการใช้งบประมาณและการใช้ทรัพยากรร่วมกันอย่างมีประสิทธิภาพ

# (ร่าง) มาตรฐานรัฐบาลดิจิทัล (มรด.) ว่าด้วยแนวทางการใช้คลาวด์ เวอร์ชัน 1.0

## บทนิยาม

**“การประมวลผลแบบคลาวด์ (Cloud Computing)”** หมายความว่า รูปแบบการเข้าถึงทรัพยากร ทางกายภาพหรือเสมือน ผ่านเครือข่ายสารสนเทศ ซึ่งสามารถแบ่งปันให้ใช้งานร่วมกันได้ (Shareable) อย่างยืดหยุ่น (Elastic) และปรับขยายได้ (Scalable) โดยรองรับการจัดสรรและบริหารจัดการทรัพยากรด้วยตนเอง (Self-service Provisioning ) ตามความต้องการ (On-demand)

**“บริการคลาวด์ (Cloud Service)”** หมายความว่า การนำเสนอความสามารถของการประมวลผลแบบคลาวด์รูปแบบใดแบบหนึ่งหรือมากกว่านั้นให้กับผู้ใช้บริการ โดยสามารถเรียกใช้งานผ่านอินเทอร์เน็ตที่กำหนดไว้

**“คลาวด์สาธารณะ (Public Cloud)”** หมายความว่า บริการคลาวด์ที่เปิดให้บริการกับผู้ใช้บริการทั่วไป โดยทรัพยากรทั้งหมดอยู่ภายใต้การควบคุมของผู้ให้บริการคลาวด์

**“คลาวด์ส่วนตัว (Private Cloud)”** หมายความว่า บริการคลาวด์ที่ใช้งานโดยผู้ใช้บริการเพียงรายเดียว โดยทรัพยากรทั้งหมดอยู่ภายใต้การควบคุมของผู้ใช้บริการรายนั้น

**“คลาวด์แบบกลุ่ม (Community Cloud)”** หมายความว่า บริการคลาวด์ที่ใช้เฉพาะกลุ่มผู้ใช้บริการที่มีความต้องการใช้งาน และมีความเกี่ยวข้องกัน ซึ่งทรัพยากรถูกควบคุมโดยสมาชิกในกลุ่ม

# (ร่าง) มาตรฐานรัฐบาลดิจิทัล (มรด.) ว่าด้วยแนวทางการใช้คลาวด์ เวอร์ชัน 1.0

## บทนิยาม (ต่อ)

“**คลาวด์แบบผสม (Hybrid Cloud)**” หมายความว่า การใช้คลาวด์ที่รวมการใช้งานคลาวด์ส่วนตัว (Private Cloud) และคลาวด์สาธารณะ (Public Cloud) เข้าด้วยกัน

“**คลาวด์อธิปไตย (Sovereign Cloud)**” หมายความว่า บริการคลาวด์ ภายใต้การควบคุมโดยภาครัฐและดูแลโดยบุคลากรที่ได้รับอนุญาต และใช้สำหรับให้บริการกับหน่วยงานของรัฐเท่านั้น

“**คลาวด์ส่วนตัวเสมือน (Virtual Private Cloud - VPC)**” หมายความว่า บริการคลาวด์สาธารณะ (Public Cloud) ที่มีการเพิ่มมาตรการคุ้มครองข้อมูลมากกว่าการใช้งานคลาวด์สาธารณะทั่วไป โดยมีการแยกการบริหารจัดการทรัพยากรและการใช้งานเฉพาะผู้ใช้บริการแต่ละราย (Isolation)

“**การให้บริการโครงสร้างพื้นฐาน (Infrastructure as a Service: IaaS)**” หมายความว่า หมวดหมู่ของบริการคลาวด์ที่ผู้ใช้บริการสามารถกำหนดการใช้งานหน่วยประมวลผล พื้นที่จัดเก็บข้อมูล และเครือข่ายได้เองตามความต้องการ

“**การให้บริการแพลตฟอร์ม (Platform as a Service: PaaS)**” หมายความว่า หมวดหมู่ของบริการคลาวด์ที่ผู้ใช้บริการสามารถติดตั้ง บริหารจัดการ หรือเรียกใช้แอปพลิเคชันที่ผู้ใช้บริการกำหนดเองด้วยคำสั่ง ภาษา หรือสภาพแวดล้อมที่ผู้ใช้บริการรองรับ

# (ร่าง) มาตรฐานรัฐบาลดิจิทัล (มรด.) ว่าด้วยแนวทางการใช้คลาวด์ เวอร์ชัน 1.0

## บทนิยาม (ต่อ)

**“การให้บริการซอฟต์แวร์ (Software as a Service: SaaS)”** หมายความว่า หมวดหมู่ของบริการคลาวด์ที่ผู้ใช้บริการสามารถใช้งานแอปพลิเคชันที่ผู้ให้บริการจัดเตรียมไว้ได้

**“ข้อมูลที่สามารถเปิดเผยได้ (Official Data)”** หมายความว่า ข้อมูลที่สร้าง ประมวลผล ส่ง หรือรับของหน่วยงานภาครัฐ และหน่วยงานที่เกี่ยวข้อง ซึ่งอาจก่อให้เกิดความเสียหายได้ไม่เกินความเสียหายในระดับต่ำ หากมีการละเมิดความปลอดภัยจะมีการใช้มาตรฐานการควบคุมที่สามารถคุ้มครองข้อมูลให้มีความปลอดภัยจากการโจมตีในรูปแบบต่างๆ ซึ่งอาจเพิ่มการรับรองมาตรการควบคุม

**“ข้อมูลที่ต้องได้รับความคุ้มครอง (Protected Data)”** หมายความว่า ข้อมูลที่มีความอ่อนไหวสูงหากเปิดเผยอาจก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐ หรือเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรง ซึ่งส่งผลกระทบต่อความมั่นคงของชาติ และ/หรือความสัมพันธ์ระหว่างประเทศ ความมั่นคง/เสถียรภาพทางการเงิน หรือขัดขวางความสามารถในการสืบสวนคดีอาชญากรรมที่ร้ายแรง หรือองค์กร ที่จำเป็นต้องมีมาตรการควบคุมที่เข้มงวด และมีการกำหนดการใช้เครือข่ายที่ปลอดภัยบนโครงสร้างพื้นฐานทางกายภาพที่มีความปลอดภัย และมีการปฏิบัติอย่างเหมาะสม ซึ่งรวมถึงการใช้สถาปัตยกรรมแบบ Zero - Trust การเข้ารหัส และการปฏิบัติตามมาตรฐานความปลอดภัยทั้งในระดับชาติและระดับสากลอย่างเคร่งครัด

# (ร่าง) มาตรฐานรัฐบาลดิจิทัล (มรด.) ว่าด้วยแนวทางการใช้คลาวด์ เวอร์ชัน 1.0

## บทนิยาม (ต่อ)

**“ข้อมูลที่ต้องได้รับความคุ้มครองสูงสุด (Highly Protected Data)”** หมายความว่า ข้อมูลที่มีความอ่อนไหวเป็นพิเศษ หากเปิดเผยอาจเกิดความเสียหายอย่างร้ายแรงที่สุดต่อรัฐ ซึ่งส่งผลความมั่นคงของชาติหรือพันธมิตร และต้องการมาตรการควบคุมความปลอดภัยที่สูงมาก เพื่อป้องกันการละเมิดข้อมูลจากภัยคุกคามทั้งหมด โดยการใช้เครือข่ายบนโครงสร้างพื้นฐานทางกายภาพที่มีความปลอดภัยสูง และมีการควบคุมความปลอดภัยอย่างเข้มงวด ซึ่งรวมถึงการใช้สถาปัตยกรรมแบบ Zero-Trust การเข้ารหัส และการปฏิบัติตามมาตรฐานความปลอดภัยทั้งในระดับชาติและระดับสากลอย่างเคร่งครัด

# (ร่าง) มาตรฐานรัฐบาลดิจิทัล (มรด.) ว่าด้วยแนวทางการใช้คลาวด์ เวอร์ชัน 1.0

## แนวทางการเลือกประเภทคลาวด์ (Cloud Deployment Models)

ตารางที่ 2 แนวทางการจำแนกประเภทข้อมูลเพื่อใช้บริการคลาวด์

ประเภทข้อมูล	คำอธิบาย	ประเภทบริการคลาวด์ที่แนะนำ
Official Data	ข้อมูลที่สร้าง ประมวลผล ส่ง หรือรับของหน่วยงานภาครัฐและหน่วยงานที่เกี่ยวข้อง ซึ่งอาจก่อให้เกิดความเสียหายได้ไม่เกินความเสียหายในระดับต่ำ หากมีการละเมิดความปลอดภัยจะมีการใช้มาตรฐานการควบคุมที่สามารถคุ้มครองข้อมูลให้มีความปลอดภัยจากการโจมตีในรูปแบบต่างๆ ซึ่งอาจเพิ่มการรับรองมาตรฐานการควบคุม	Public Cloud

ประเภทข้อมูล	คำอธิบาย	ประเภทบริการคลาวด์ที่แนะนำ
Protected Data	ข้อมูลที่มีความอ่อนไหวสูงหากเปิดเผยอาจก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐ หรือเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรง ซึ่งส่งผลกระทบต่อความมั่นคงของชาติ และ/หรือความสัมพันธ์ระหว่างประเทศ ความมั่นคง/เสถียรภาพทางการเงิน หรือขีดความสามารถในการสืบสวนคดีอาชญากรรมที่ร้ายแรง หรือองค์กร ที่จำเป็นต้องมีมาตรการควบคุมที่เข้มงวด และมีการกำหนดการใช้เครือข่ายที่ปลอดภัยบนโครงสร้างพื้นฐานทางกายภาพที่มีความปลอดภัย และมีการปฏิบัติอย่างเหมาะสม ซึ่งรวมถึงการใช้สถาปัตยกรรมแบบ ZERO - TRUST การเข้ารหัส และการปฏิบัติตามมาตรฐานความปลอดภัยทั้งในระดับชาติและระดับสากลอย่างเคร่งครัด	Public Cloud ที่มีมาตรการด้านความปลอดภัยสูง เช่น คลาวด์ส่วนตัวเสมือน (Virtual Private Cloud หรือ VPC)
Highly Protected Data	ข้อมูลที่มีความอ่อนไหวเป็นพิเศษ หากเปิดเผยอาจเกิดความเสียหายอย่างร้ายแรงที่สุดต่อรัฐ ซึ่งส่งผลกระทบต่อความมั่นคงของชาติหรือพันธมิตร และต้องการมาตรการควบคุมความปลอดภัยที่สูงมาก เพื่อป้องกันการละเมิดข้อมูลจากภัยคุกคามทั้งหมด โดยการใช้เครือข่ายบนโครงสร้างพื้นฐานทางกายภาพที่มีความปลอดภัยสูง และมีการควบคุมความปลอดภัยอย่างเข้มงวด ซึ่งรวมถึงการใช้สถาปัตยกรรมแบบ ZERO-TRUST การเข้ารหัส และการปฏิบัติตามมาตรฐานความปลอดภัย ทั้ง ในระดับชาติและระดับสากลอย่างเคร่งครัด	Sovereign Cloud (กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม กำหนดผู้ให้บริการ) หรือ Hybrid Cloud (เฉพาะบริการด้านความมั่นคงที่กำหนด)

### หมายเหตุ

1. ข้อมูลที่ควรอยู่ในประเทศไทย หมายถึง ข้อมูลที่จัดเก็บอยู่ในสถานะพัก (Data-at-Rest) โดยไม่รวมถึงข้อมูลที่อยู่/ระหว่างการรับส่ง (Data-in-Transit) หรือการประมวล (Data Processing)
2. หากมีการทบทวนปรับเปลี่ยนระดับชั้นความลับของข้อมูล (Re-classification) หรือการยกเลิกชั้นความลับ (De-classification) ในภายหลัง ให้หน่วยงานสามารถปรับเปลี่ยนรูปแบบการใช้บริการคลาวด์ให้สอดคล้องกับสถานะความสำคัญใหม่ของข้อมูลได้
3. Sovereign Cloud (คลาวด์อธิปไตย) หมายถึง บริการคลาวด์ภายใต้การควบคุมโดยภาครัฐและดูแลโดยบุคลากรที่ได้รับอนุญาต และใช้สำหรับให้บริการกับหน่วยงานของรัฐเท่านั้น

# (ร่าง) มาตรฐานรัฐบาลดิจิทัล (มรด.) ว่าด้วยแนวทางการใช้คลาวด์ เวอร์ชัน 1.0

## บริการคลาวด์ (CLOUD SERVICE)

บริการคลาวด์ของผู้ให้บริการมีด้วยกัน 3 รูปแบบหลัก ซึ่งมีลักษณะการใช้งานต่างกัน โดยแสดงตัวอย่างแนวทางการใช้งาน

- **การให้บริการโครงสร้างพื้นฐาน (Infrastructure as a Service: IaaS)**
  - ✓ กรณีต้องการสร้างและควบคุมโครงสร้างพื้นฐาน เช่น เครื่องแม่ข่ายเสมือน (VM) หรือระบบเครือข่ายเสมือน
- **การให้บริการแพลตฟอร์ม (Platform as a Service: PaaS)**
  - ✓ กรณีต้องการพัฒนาและปรับใช้แอปพลิเคชันเฉพาะ เช่น ระบบบริหารจัดการฐานข้อมูล
- **การให้บริการซอฟต์แวร์ (Software as a Service: SaaS)**
  - ✓ กรณีต้องการใช้งานแอปพลิเคชันสำเร็จรูป เช่น อีเมล การจัดการเอกสาร หรือระบบ CRM

# (ร่าง) มาตรฐานรัฐบาลดิจิทัล (มรด.) ว่าด้วยแนวทางการใช้คลาวด์ เวอร์ชัน 1.0

## แนวทางการย้ายระบบขึ้นคลาวด์ (Migration)

เมื่อหน่วยงานต้องการย้าย ระบบหรือบริการ ซึ่งเดิมจัดทำและใช้งานในรูปแบบ เครื่องแม่ข่ายแบบกายภาพ หรือรูปแบบอื่น ๆ ที่มีการติดตั้งภายในองค์กร (On-Premise) ไปสู่ระบบคลาวด์ สามารถดำเนินการได้ตามแนวทาง ดังนี้

1. การประเมินความพร้อม (Assessment) ก่อนการย้ายข้อมูลและระบบไปยังระบบคลาวด์

2. การเลือกรูปแบบการย้าย (Cloud Migration Models)

3. การย้ายข้อมูลและการทดสอบ (Migration and Testing) การย้ายข้อมูลไปยัง Public Cloud ควรทำทีละขั้นตอนและมีการทดสอบระบบหลังจากการย้าย

4. การบริหารจัดการหลังการย้าย (Post-migration Management) หลังจากการย้ายเสร็จสิ้น ควรมีการบริหารจัดการและการตรวจสอบอย่างต่อเนื่อง

# (ร่าง) มาตรฐานรัฐบาลดิจิทัล (มรด.) ว่าด้วยแนวทางการใช้คลาวด์ เวอร์ชัน 1.0

## แนวทางการออกจากระบบคลาวด์ (CLOUD EXIT)

การวางแผนล่วงหน้าเพื่อให้การเปลี่ยนผ่านจากระบบคลาวด์ของผู้ให้บริการรายเดิมเป็นไปอย่างราบรื่น โดยมีเป้าหมายเพื่อป้องกันการเกิด "Vendor Lock-In" หรือการพึ่งพาผู้ให้บริการรายเดียวมากเกินไป ซึ่งอาจส่งผลกระทบต่อความต่อเนื่องของบริการหรือความปลอดภัยของข้อมูลเมื่อมีการเปลี่ยนแปลงระบบ ประกอบด้วยหลักการสำคัญเบื้องต้น ดังนี้

### วางแผนตั้งแต่เริ่มต้น

กำหนด สัญญา เงื่อนไขต่าง ๆ ค่าใช้จ่าย ในการเคลื่อนย้ายข้อมูล (Data portability)

ป้องกันการพึ่งพาผู้ให้บริการรายเดียว ใช้เทคโนโลยีและมาตรฐานที่เป็นอิสระ

กำหนดข้อมูลและบริการที่ต้องจัดการในกระบวนการออกจากระบบ ระบุข้อมูลและบริการที่ต้องถ่ายโอนหรือกู้คืน ประเมินผลกระทบของการเปลี่ยนแปลง

ความปลอดภัยและการปฏิบัติตามข้อกำหนด ดำเนินการให้มั่นใจว่า ข้อมูลถูกลบอย่างปลอดภัยจากระบบเดิม ปฏิบัติตามกฎหมายและข้อกำหนดด้านการคุ้มครองข้อมูล

# (ร่าง) มาตรฐานรัฐบาลดิจิทัล (มรด.) ว่าด้วยแนวทางการใช้คลาวด์ เวอร์ชัน 1.0

## แนวทางการประเมินราคาและวางแผนงบประมาณ

### แนวทางการประเมินราคาและวางแผนงบประมาณ

สามารถสรุปแนวทางการประเมินราคาและวางแผนงบประมาณ สำหรับการจัดซื้อจัดจ้างระบบคลาวด์ภาครัฐ ดังนี้

1. รูปแบบการคิดค่าบริการ  
จากการใช้บริการคลาวด์

2. การวิเคราะห์ความ  
ต้องการทรัพยากร

3. การวิเคราะห์ต้นทุน  
ทางตรงและทางอ้อม

4. การใช้เครื่องมือประเมินค่าบริการ (Pricing  
Calculator) ที่มีมาตรฐานการจัดทำเพดาน  
งบประมาณ (Not-To-Exceed Ceiling)

# (ร่าง) มาตรฐานรัฐบาลดิจิทัล (มรด.) ว่าด้วยแนวทางการใช้คลาวด์ เวอร์ชัน 1.0

## แนวทางในด้านความปลอดภัย และด้านอื่นที่เกี่ยวข้อง

### แนวทางในด้านความปลอดภัย

หน่วยงานสามารถดำเนินการโดยอ้างอิงตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 ซึ่งสรุปโดยสังเขปเนื้อหาแบ่งออกเป็น แนวทางด้านความปลอดภัยผู้ให้บริการคลาวด์ (Cloud Service Provider) และผู้ใช้บริการคลาวด์ (Cloud Service Consumer) มีความแตกต่างและเชื่อมโยงกันในด้านความรับผิดชอบ และมีจุดมุ่งหมายเพื่อปกป้องข้อมูล ระบบและโครงสร้างพื้นฐานของคลาวด์อย่างครบวงจรโดยแบ่งเป็น

- 1) การกำกับดูแลความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์
- 2) การปฏิบัติการและการรักษาความมั่นคงปลอดภัยโครงสร้างพื้นฐานระบบคลาวด์

# (ร่าง) มาตรฐานรัฐบาลดิจิทัล (มรด.) ว่าด้วยแนวทางการใช้คลาวด์ เวอร์ชัน 1.0

## แนวทางในด้านความปลอดภัย และด้านอื่นที่เกี่ยวข้อง (ต่อ)

### แนวทางการจัดการระบบสำรองข้อมูลและกู้คืนข้อมูลบนคลาวด์

แนวทางการจัดการระบบสำรองข้อมูลและกู้คืนข้อมูลบนคลาวด์ จะเน้นการดำเนินการด้านการสำรองข้อมูล (Backup) และ การกู้คืนข้อมูล (Restore) ตามแนวทางดังนี้



# (ร่าง) มาตรฐานรัฐบาลดิจิทัล (มรด.) ว่าด้วยแนวทางการใช้คลาวด์ เวอร์ชัน 1.0

หัวข้อ	เดิม	ปรับปรุง
ชื่อมาตรฐาน	มาตรฐานรัฐบาลดิจิทัล ว่าด้วยแนวทางการใช้คลาวด์ ตามนโยบายการใช้คลาวด์เป็นหลัก เวอร์ชัน 1.0	มาตรฐานรัฐบาลดิจิทัล ว่าด้วยแนวทางการใช้คลาวด์ เวอร์ชัน 1.0
คำนำ	การอ้างอิงนโยบาย แนวทางการขับเคลื่อนตามนโยบายการใช้คลาวด์เป็นหลัก (Cloud First Policy) ตามที่คณะรัฐมนตรีได้แถลงนโยบาย "Go Cloud First" และกล่าวถึงชุดมาตรฐานคลาวด์ เนื้อหาที่จะมีในเล่มนี้	อ้างอิงคณะกรรมการพัฒนารัฐบาลดิจิทัล ที่มีมติมอบหมายให้สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) จัดทำมาตรฐาน เพื่อให้หน่วยงานภาครัฐสามารถนำไปปฏิบัติได้อย่างเป็นรูปธรรม เพื่อให้บริการประชาชน โดยกล่าวถึงชุดมาตรฐานด้านคลาวด์ และเนื้อหาที่จะมีในเล่มนี้
1.3 ขอบข่าย	ประเภทของคลาวด์  คลาวด์สาธารณะ (Public Cloud) คลาวด์ส่วนตัว (Private Cloud) คลาวด์แบบกลุ่ม (Community Cloud) คลาวด์แบบผสม (Hybrid Cloud)	เพิ่มประเภทของคลาวด์  คลาวด์อธิปไตย (Sovereign Cloud) คลาวด์ส่วนตัวเสมือน (Virtual Private Cloud)

# (ร่าง) มาตรฐานรัฐบาลดิจิทัล (มรด.) ว่าด้วยแนวทางการใช้คลาวด์ เวอร์ชัน 1.0

หัวข้อ	เดิม	ปรับปรุง
1.4 นิยาม	<p><b>คำนิยามด้านคลาวด์</b></p> <p>- การประมวลผลแบบคลาวด์ (Cloud Computing) หรือคลาวด์ (Cloud) หมายความว่า รูปแบบการประมวลผลที่สามารถเข้าถึงทรัพยากรที่ใช้ร่วมกันได้อย่างยืดหยุ่น โดยมีการจัดเตรียมทรัพยากร (Self-service Provisioning) และการบริหารจัดการด้วยตนเองตามความต้องการ (On-demand)</p> <p>- <b>คำนิยามประเภทของคลาวด์ (ISO 22123-1)</b></p> <ul style="list-style-type: none"> <li>• คลาวด์สาธารณะ (Public Cloud)</li> <li>• คลาวด์ส่วนตัว (Private Cloud)</li> <li>• คลาวด์แบบกลุ่ม (Community Cloud)</li> <li>• คลาวด์แบบผสม (Hybrid Cloud)</li> </ul>	<p><b>คำนิยามด้านคลาวด์ - เพิ่มการอธิบายให้ชัดเจน และเพิ่มคำนิยามตามบริบทของไทย</b></p> <p>- การประมวลผลแบบคลาวด์ (Cloud Computing) หรือคลาวด์ (Cloud) หมายความว่า รูปแบบการเข้าถึงทรัพยากรทางกายภาพหรือเสมือนผ่านเครือข่ายสารสนเทศ ซึ่งสามารถแบ่งปันให้ใช้งานร่วมกันได้ (Shareable) อย่างยืดหยุ่น (Elastic) และปรับขยายได้ (Scalable) โดยรองรับการจัดสรรและบริหารจัดการทรัพยากรด้วยตนเอง (Self-service Provisioning) ตามความต้องการ (On-demand)</p> <p>(ISO 22123-1 Cloud Computing - paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand)</p> <p>- <b>เพิ่มคำนิยามประเภทของคลาวด์</b></p> <ul style="list-style-type: none"> <li>• คลาวด์อธิปไตย (Sovereign Cloud) หมายความว่า บริการคลาวด์ ภายใต้การควบคุมโดยภาครัฐและดูแลโดยบุคลากรที่ได้รับอนุญาต และใช้สำหรับให้บริการกับหน่วยงานของรัฐเท่านั้น</li> <li>• คลาวด์ส่วนตัวเสมือน (Virtual Private Cloud - VPC) หมายความว่า บริการคลาวด์สาธารณะ (Public Cloud) ที่มีการเพิ่มมาตรการคุ้มครองข้อมูลมากกว่าการใช้งานคลาวด์สาธารณะทั่วไป โดยมีการแยกการบริหารจัดการทรัพยากรและการใช้งานเฉพาะผู้ใช้บริการแต่ละราย (Isolation)</li> </ul>

# (ร่าง) มาตรฐานรัฐบาลดิจิทัล (มรด.) ว่าด้วยแนวทางการใช้คลาวด์ เวอร์ชัน 1.0

หัวข้อ	เดิม	ปรับปรุง
1.4 นิยาม	<b>คำนิยามประเภทข้อมูล</b> ไม่มีในบทนิยาม	<b>คำนิยามประเภทข้อมูล</b> <ul style="list-style-type: none"><li>- ข้อมูลที่สามารถเปิดเผยได้ (Official Data) หมายความว่า ข้อมูลที่สร้าง ประมวลผล ส่ง หรือรับของหน่วยงานภาครัฐและหน่วยงานที่เกี่ยวข้อง ซึ่งอาจก่อให้เกิดความเสียหายได้ไม่เกินความเสียหายในระดับต่ำ หากมีการละเมิดความปลอดภัยจะมีการใช้มาตรฐานการควบคุมที่สามารถคุ้มครองข้อมูลให้มีความปลอดภัยจากการโจมตีในรูปแบบต่าง ๆ ซึ่งอาจเพิ่มการรับรองมาตรการควบคุม</li><li>- ข้อมูลที่ต้องได้รับความคุ้มครอง (Protected Data) หมายความว่า ข้อมูลที่มีความอ่อนไหวสูงหากเปิดเผยอาจก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐ หรือเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรง ซึ่งส่งผลต่อความมั่นคงของชาติ และ/หรือ ความสัมพันธ์ระหว่างประเทศ ความมั่นคง/เสถียรภาพทางการเงิน หรือขัดขวางความสามารถในการสืบสวนคดีอาชญากรรมที่ร้ายแรง หรือองค์กร ที่จำเป็นต้องมีมาตรการควบคุมที่เข้มงวด และมีการกำหนดการใช้เครือข่ายที่ปลอดภัยบนโครงสร้างพื้นฐานทางกายภาพที่มีความปลอดภัย และมีการปฏิบัติอย่างเหมาะสม ซึ่งรวมถึงการใช้สถาปัตยกรรมแบบ Zero - Trust การเข้ารหัส และการปฏิบัติตามมาตรฐานความปลอดภัยทั้งในระดับชาติและระดับสากลอย่างเคร่งครัด</li><li>- ข้อมูลที่ต้องได้รับความคุ้มครองสูงสุด (Highly Protected Data) หมายความว่า ข้อมูลที่มีความอ่อนไหวเป็นพิเศษ หากเปิดเผยอาจเกิดความเสียหายอย่างร้ายแรงที่สุดต่อรัฐ ซึ่งส่งผลความมั่นคงของชาติหรือพันธมิตร และต้องการมาตรการควบคุมความปลอดภัยที่สูงมาก เพื่อป้องกันการละเมิดข้อมูลจากภัยคุกคามทั้งหมด โดยการใช้เครือข่ายบนโครงสร้างพื้นฐานทางกายภาพที่มีความปลอดภัยสูง และมีการควบคุมความปลอดภัยอย่างเข้มงวด ซึ่งรวมถึงการใช้สถาปัตยกรรมแบบ Zero-Trust การเข้ารหัส และการปฏิบัติตามมาตรฐานความปลอดภัย ทั้งในระดับชาติ และระดับสากลอย่างเคร่งครัด</li></ul>

# (ร่าง) มาตรฐานรัฐบาลดิจิทัล (มรด.) ว่าด้วยแนวทางการใช้คลาวด์ เวอร์ชัน 1.0

หัวข้อ	เดิม	ปรับปรุง
<p>2.2 แนวทางการเลือกใช้คลาวด์</p>	<p><b>แนวทางการเลือกใช้คลาวด์เดิม</b></p> <ul style="list-style-type: none"> <li>- กรณีข้อมูลสาธารณะ (Public) กรณีที่บริการเป็นประเภทข้อมูลที่สามารถเปิดเผยได้ (Official Data) และข้อมูลที่ต้องได้รับความคุ้มครอง (Protected Data) สามารถเลือกใช้คลาวด์สาธารณะ (Public Cloud) คลาวด์แบบผสม (Hybrid Cloud) หรือ คลาวด์ส่วนตัวเสมือน (Virtual Private Cloud)</li> <li>- กรณีที่บริการเป็นประเภทข้อมูลที่ต้องได้รับความคุ้มครองสูงสุด (Highly Protected Data) ให้พิจารณาใช้คลาวด์แบบกลุ่ม (Community Cloud) หรือคลาวด์อธิปไตย (Sovereign Cloud)</li> </ul>	<p><b>แนวทางการเลือกใช้คลาวด์ ที่ปรับปรุงให้สอดคล้องกับประเภทข้อมูล</b></p> <ul style="list-style-type: none"> <li>- กรณีบริการเป็นข้อมูลที่สามารถเปิดเผยได้ (Official Data) ให้เลือกใช้คลาวด์สาธารณะ (Public Cloud) ส่วนบริการที่มี ข้อมูลที่ต้องได้รับความคุ้มครอง (Protected Data) ให้ใช้คลาวด์สาธารณะ (Public Cloud) ที่มีมาตรการด้านความปลอดภัยสูง เช่น คลาวด์ส่วนตัวเสมือน (Virtual Private Cloud) ....</li> <li>- การใช้คลาวด์สาธารณะต้องเลือกใช้ถิ่นที่อยู่ของข้อมูลให้มีความเหมาะสม เป็นไปตามกฎหมาย และข้อบังคับด้านอธิปไตยทางข้อมูล (Data Sovereignty) ของประเทศ</li> <li>- กรณีที่บริการเป็น ประเภทข้อมูลที่ต้องได้รับความคุ้มครองสูงสุด (Highly Protected Data) ให้พิจารณาใช้คลาวด์อธิปไตย (Sovereign Cloud) ซึ่งออกแบบมาเพื่อให้มั่นใจว่า ข้อมูลทั้งหมด (รวมถึง แอปพลิเคชัน และข้อมูลที่อยู่ระหว่างการส่งผ่านเครือข่าย) ถูกจัดเก็บ ประมวลผล และบริหารจัดการ อยู่ภายในประเทศหรือภูมิภาคที่กำหนด และเป็นไปตามกฎหมายและข้อบังคับด้านอธิปไตยทางข้อมูล (Data Sovereignty) ของประเทศอย่างเคร่งครัด และสามารถเลือกใช้คลาวด์แบบผสม (Hybrid Cloud) ซึ่งมีการแยกข้อมูลที่ต้องได้รับความคุ้มครองสูงสุดไว้ในคลาวด์ส่วนตัว (Private Cloud)</li> </ul>

# (ร่าง) มาตรฐานรัฐบาลดิจิทัล (มรด.) ว่าด้วยแนวทางการใช้คลาวด์ เวอร์ชัน 1.0

หัวข้อ	เดิม	ปรับปรุง
3.แนวทางการประเมิน ราคา วางแผน งบประมาณ และบริหาร การใช้บริการ	ไม่มีข้อความเกริ่นนำที่อธิบายหลักการในตอนต้น	เพิ่มข้อความเกริ่นนำที่อธิบายหลักการ  “เพื่อให้การบริหารจัดการงบประมาณภาครัฐเกิดความคุ้มค่าสูงสุดและลดความซ้ำซ้อนในการลงทุนโครงสร้างพื้นฐาน หน่วยงานภาครัฐพึงพิจารณาเลือกใช้บริการคลาวด์จากหน่วยงานกลาง เช่น บริการจากระบบคลาวด์กลางภาครัฐ (GDCC) เป็นลำดับแรก (First Priority) อย่างไรก็ตาม หากหน่วยงานมีเหตุผลความจำเป็นทางด้านเทคนิค หรือภารกิจเฉพาะที่ต้องดำเนินการจัดหาบริการคลาวด์ด้วยตนเอง ให้ดำเนินการพิจารณาเปรียบเทียบความคุ้มค่าและปฏิบัติตามคำแนะนำดังต่อไปนี้ ...”
3.4. แนวทางการขอ งบประมาณโครงการ ด้านระบบคลาวด์	3.4. แนวทางการของงบประมาณโครงการด้านระบบคลาวด์ - อ้างอิง แผนงานบูรณาการรัฐบาลดิจิทัล ประจำปี งบประมาณ พ.ศ. 2569 สำหรับหน่วยงานระดับกรมหรือ เทียบเท่าดิจิทัล - แนวทางที่ 1.3	- ไม่ระบุในมาตรฐาน ให้ระบุในประกาศคณะกรรมการฯ หรือหน่วยงานที่ได้รับมอบหมายหน้าที่บริหารจัดการ ประกาศกำหนด



IaaS



# (ร่าง) มาตรฐานรัฐบาลดิจิทัล (มรด.)

แนวทางการกำหนดมาตรฐานผู้ให้บริการคลาวด์ เวอร์ชัน 1.0

# (ร่าง) มาตรฐานรัฐบาลดิจิทัล (มรด.)

แนวทางการกำหนดมาตรฐานผู้ให้บริการคลาวด์ เวอร์ชัน 1.0



**มาตรฐาน**ฉบับนี้ มุ่งหมายให้

ผู้ให้บริการคลาวด์และผู้ประกอบการที่เกี่ยวข้อง รับผิดชอบต่อหลักเกณฑ์ เจื้อนไข และมาตรฐานต่าง ๆ ที่ต้องปฏิบัติตาม ในการให้บริการคลาวด์แก่หน่วยงานของรัฐ

สร้างความรู้ ความเข้าใจเกี่ยวกับกระบวนการและกลไกในการประกาศรายชื่อผู้ให้บริการคลาวด์ (shortlist) แก่ข้าราชการ บุคลากรภาครัฐ และผู้มีส่วนเกี่ยวข้อง

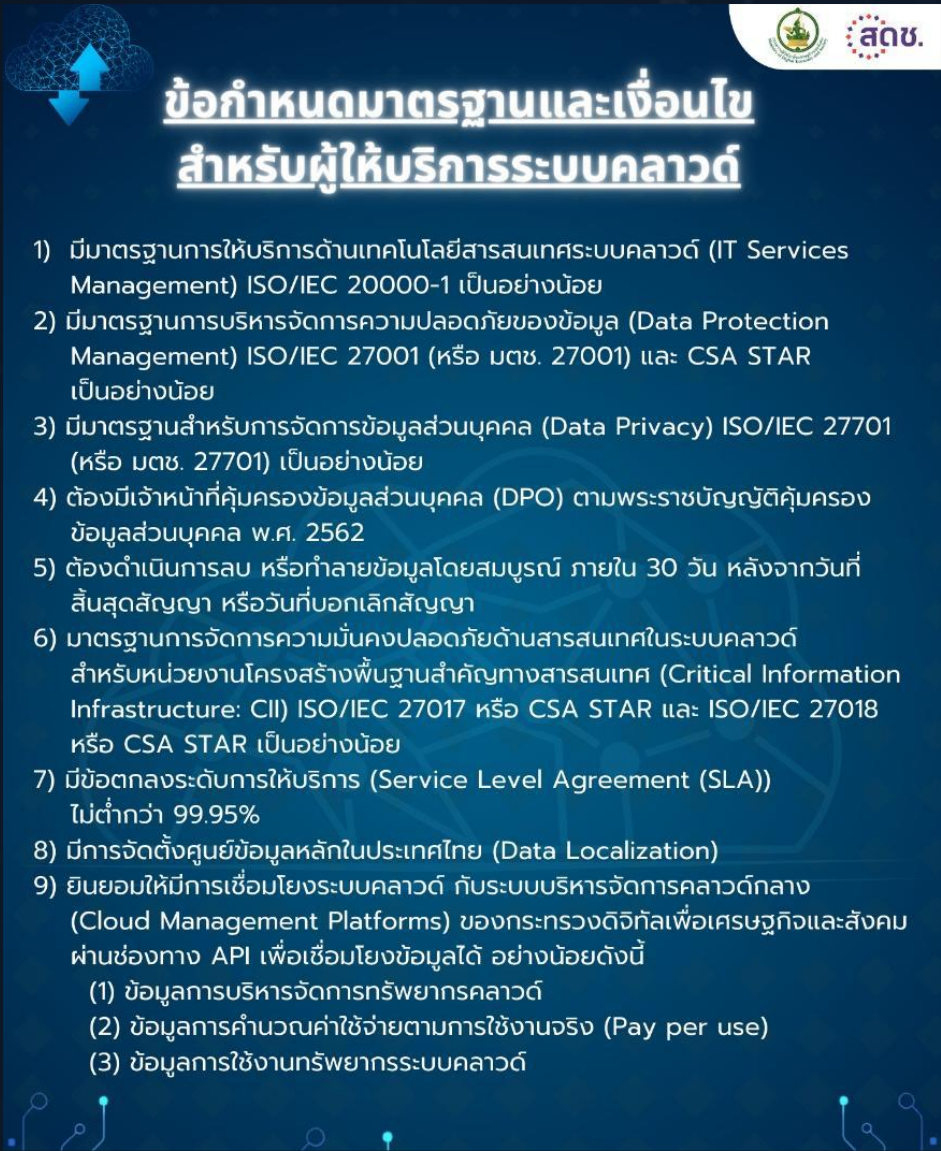
นำเสนอข้อมูลเกี่ยวกับมาตรฐาน หลักเกณฑ์ แนวปฏิบัติ และข้อกำหนด ทั้งของไทยและสากล ในด้านการคัดกรองผู้ให้บริการคลาวด์



1) กระบวนการและกลไก ในการประกาศรายชื่อผู้ให้บริการคลาวด์ (shortlist)

2) ข้อเสนอแนะกรอบแนวทางการขับเคลื่อน ที่เกี่ยวข้อง

3) ข้อมูลเกี่ยวกับมาตรฐาน หลักเกณฑ์ แนวปฏิบัติ และข้อกำหนด ทั้งของประเทศไทยและมาตรฐานสากล สำหรับการคัดกรองผู้ให้บริการคลาวด์



## ข้อกำหนดมาตรฐานและเงื่อนไขสำหรับผู้ให้บริการระบบคลาวด์

- 1) มีมาตรฐานการให้บริการด้านเทคโนโลยีสารสนเทศระบบคลาวด์ (IT Services Management) ISO/IEC 20000-1 เป็นอย่างน้อย
- 2) มีมาตรฐานการบริหารจัดการความปลอดภัยของข้อมูล (Data Protection Management) ISO/IEC 27001 (หรือ มตช. 27001) และ CSA STAR เป็นอย่างน้อย
- 3) มีมาตรฐานสำหรับการจัดการข้อมูลส่วนบุคคล (Data Privacy) ISO/IEC 27701 (หรือ มตช. 27701) เป็นอย่างน้อย
- 4) ต้องมีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
- 5) ต้องดำเนินการลบ หรือทำลายข้อมูลโดยสมบูรณ์ ภายใน 30 วัน หลังจากวันที่สิ้นสุดสัญญา หรือวันที่บอกเลิกสัญญา
- 6) มาตรฐานการจัดการความมั่นคงปลอดภัยด้านสารสนเทศในระบบคลาวด์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) ISO/IEC 27017 หรือ CSA STAR และ ISO/IEC 27018 หรือ CSA STAR เป็นอย่างน้อย
- 7) มีข้อตกลงระดับการให้บริการ (Service Level Agreement (SLA)) ไม่ต่ำกว่า 99.95%
- 8) มีการจัดตั้งศูนย์ข้อมูลหลักในประเทศไทย (Data Localization)
- 9) ยินยอมให้มีการเชื่อมโยงระบบคลาวด์ กับระบบบริหารจัดการคลาวด์กลาง (Cloud Management Platforms) ของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ผ่านช่องทาง API เพื่อเชื่อมโยงข้อมูลได้ อย่างน้อยดังนี้
  - (1) ข้อมูลการบริหารจัดการทรัพยากรคลาวด์
  - (2) ข้อมูลการคำนวณค่าใช้จ่ายตามการใช้งานจริง (Pay per use)
  - (3) ข้อมูลการใช้งานทรัพยากรระบบคลาวด์

- **มติคณะรัฐมนตรี** เรื่อง “ขอยกเว้นการปฏิบัติตามมติคณะรัฐมนตรีเมื่อวันที่ 26 สิงหาคม 2568 เรื่อง การชะลอการดำเนินการจัดซื้อหรือเช่าใช้บริการระบบคลาวด์ (Cloud)” วันที่ 11 พฤศจิกายน 2568 กำหนดให้ หน่วยงานภาครัฐนำข้อกำหนดมาตรฐานและเงื่อนไขสำหรับผู้ให้บริการระบบคลาวด์ ตามมติคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ ครั้งที่ 2/2567 เมื่อวันที่ 14 มิถุนายน 2567 ไปประกอบการดำเนินการไปพลางก่อน จนกว่าจะมีข้อกำหนดมาตรฐานและเงื่อนไขสำหรับผู้ให้บริการระบบคลาวด์ฉบับใหม่ และต้องเชื่อมโยงระบบคลาวด์กับระบบบริหารจัดการคลาวด์กลาง (Cloud Management Platform) ของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมได้
- **มาตรฐานและเงื่อนไขนี้ ควรได้รับการขยายผล/ปรับปรุง ดังนี้**
  - จัดทำแนวทางเลือกใช้ตามความเสี่ยง (Risk-Based Selection): กำหนดเกณฑ์จำแนกประเภทข้อมูล เพื่อให้หน่วยงานเลือกใช้รูปแบบคลาวด์ ได้เหมาะสมกับระดับชั้นของข้อมูล
  - ทบทวนข้อกำหนดบางประการ เช่น การลบ/ทำลายข้อมูล มาตรฐานของศูนย์ข้อมูล การจัดตั้งศูนย์ข้อมูลหลักในประเทศไทย
  - ยกระดับมาตรฐานแบบแบ่งชั้น (Tiered Security): กำหนดมาตรการทางเทคนิคเพิ่มเติมให้ผู้ให้บริการตามระดับความสำคัญของข้อมูล
  - กำหนดหน้าที่ผู้ใช้บริการ (Shared Responsibility): ระบุข้อปฏิบัติที่ชัดเจนสำหรับหน่วยงานรัฐในการใช้งานอย่างปลอดภัย
  - กลไกคัดกรอง (Trusted Shortlist): จัดตั้งกลไกตรวจสอบประเมิน และประกาศบัญชีรายชื่อผู้ให้บริการที่ผ่านการรับรองในแต่ละระดับชั้น เพื่อลดภาระการตรวจสอบรายโครงการและเอื้อต่อการจัดหาที่รวดเร็ว

# (ร่าง) มาตรฐานรัฐบาลดิจิทัล (มรต.)

## แนวทางการกำหนดมาตรฐานผู้ให้บริการคลาวด์ เวอร์ชัน 1.0



### มาตรฐานรัฐบาลดิจิทัล

Digital Government Standard

มรต. 9-X : 256X

DGS 9-X : 256X

ว่าด้วยแนวทางการกำหนดมาตรฐานผู้ให้บริการคลาวด์  
Cloud Service Provider Standard

เวอร์ชัน 1.0

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)  
สำนักนายกรัฐมนตรี

## 1. บทนำ

1.1 ความเป็นมา

1.2 วัตถุประสงค์

1.3 ขอบข่าย

1.4 บทนิยาม

1.5 กฎหมายและแนวทางที่เกี่ยวข้อง

2. มาตรฐาน กฏระเบียบ และแนวปฏิบัติสากลที่เกี่ยวข้อง  
กับการบริหารจัดการบริการคลาวด์

3. แนวทางการบริหารจัดการบริการคลาวด์ของไทย

4. แนวทางการจัดเตรียมข้อมูลและเอกสารหลักฐาน  
ประกอบสำหรับการขอรับการตรวจประเมินฯ

5. ภาคผนวก

บรรณานุกรม

# (ร่าง) มาตรฐานรัฐบาลดิจิทัล (มรด.)

## แนวทางการกำหนดมาตรฐานผู้ให้บริการคลาวด์ เวอร์ชัน 1.0



### คำนำ



### 1. บทนำ

1.1 ความเป็นมา

1.2 วัตถุประสงค์

1.3 ขอบข่าย

1.4 บทนิยาม

1.5 กฎหมายและแนวทางที่เกี่ยวข้อง



### 2. มาตรฐานกฎระเบียบ และแนวปฏิบัติสากลที่เกี่ยวข้องกับการบริหารจัดการบริการคลาวด์

2.1 มาตรฐาน และกฎระเบียบที่เกี่ยวข้อง

2.2 บทเรียนกรณีศึกษาต่างประเทศ



### ภาคผนวก



### 3. แนวทางการบริหารจัดการบริการคลาวด์ของไทย

3.1 กรอบแนวทางการบริหารจัดการคลาวด์ประเทศไทย (Framework T-Cloud)

3.2 รายชื่อผู้ให้บริการคลาวด์ (Shortlist)

3.3 คุณสมบัติของผู้ให้บริการคลาวด์และการจัดระดับความสามารถในการให้บริการ (Cloud Service Provider Tier)



### 4. แนวทางการจัดเตรียมข้อมูลและเอกสารหลักฐานประกอบสำหรับการขอรับการตรวจประเมินฯ

4.1 กรอบการจัดเตรียมข้อมูลและเอกสารหลักฐาน

4.2 การอ้างอิงมาตรฐานและแนวปฏิบัติสากล

4.3 แบบฟอร์มการเปิดเผยข้อมูลของผู้ให้บริการคลาวด์

4.4 ตัวอย่างแนวทางการตรวจประเมินตนเอง



### บรรณานุกรม

# (ร่าง) มาตรฐานรัฐบาลดิจิทัล (มรด.)

## แนวทางการกำหนดมาตรฐานผู้ให้บริการคลาวด์ เวอร์ชัน 1.0

21 มาตรฐาน และกฎระเบียบที่เกี่ยวข้อง

มาตรฐานที่ผู้ให้บริการคลาวด์ควรได้รับการรับรอง เพื่อใช้ในการคัดกรองผู้ให้บริการคลาวด์ โดยแบ่งออกเป็น **5** ด้านหลัก

ด้านการรักษาความมั่นคงปลอดภัย  
ในการใช้คลาวด์ (Cloud Security)

1



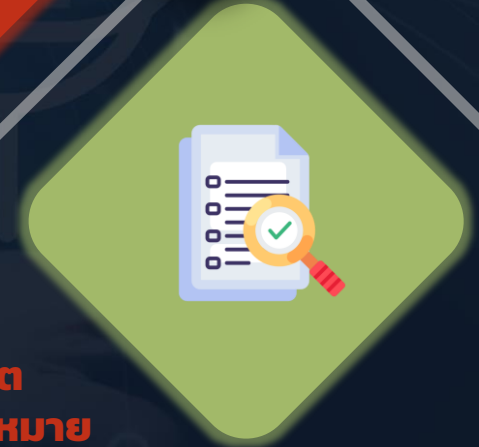
ด้านการป้องกันข้อมูลส่วนบุคคล  
(Data Protection/Privacy)

3



ด้านการป้องกันการทุจริต  
ในการจัดซื้อจัดจ้าง

5



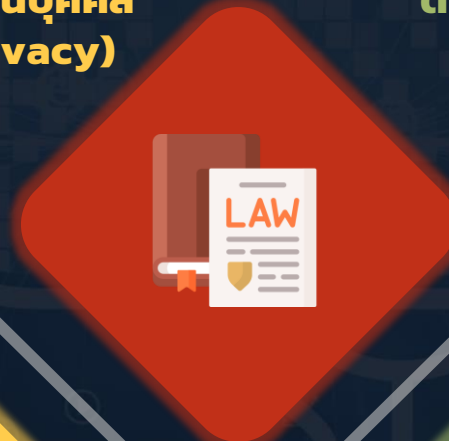
ด้านการบริหารจัดการบริการ  
(Service Management)

2



ด้านการขออนุญาต  
และการปฏิบัติตามกฎหมาย  
(Licensing & Legal Compliance)

4



# (ร่าง) มาตรฐานรัฐบาลดิจิทัล (มรด.)



	Cloud Service Provider Tier 1	Cloud Service Provider Tier 2	Cloud Service Provider Tier 3
<b>1. ขอบเขตการให้บริการรับรอง</b>	ผู้ให้บริการคลาวด์หรือผู้แทนที่ประสงค์จะให้บริการภาครัฐ ให้ครอบคลุมทั้งด้าน ความมั่นคงปลอดภัยและการคุ้มครองข้อมูลส่วนบุคคล การรักษา อริปไตยทางข้อมูล คุณภาพบริการและธรรมาภิบาล ตลอดจนขีดความสามารถในการ เชื่อมโยงระบบ (Interoperability) เข้ากับแพลตฟอร์มบริหารจัดการกลางของภาครัฐได้อย่างมีประสิทธิภาพ		
<b>2. อายุการรับรอง</b>	3 ปี / รูปแบบการรับรองตามมาตรฐานสากล		
<b>3. คุณสมบัติของผู้ยื่นคำขอ</b>	<ol style="list-style-type: none"> <li>เป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย และมีทุนจดทะเบียน โดยจะต้องพิจารณามูลค่าของทุนจดทะเบียนที่เรียกชำระมูลค่าหุ้นแล้ว และมูลค่าสุทธิของกิจการ ณ วันที่ตรวจประเมิน</li> <li>กรณีเป็นตัวแทนจะต้องมีหนังสือแต่งตั้งจากผู้ให้บริการคลาวด์ หรือผู้จัดจำหน่ายประเภท Distributor ของผู้ให้บริการคลาวด์ต้นทาง</li> <li>มีบริการและผลิตภัณฑ์ อยู่ในกลุ่มบริการในการเลือกใช้ใช้บริการคลาวด์ พร้อมรายละเอียด และราคาต่อหน่วย</li> </ol>	คุณสมบัติของผู้ยื่นคำขอ Tier 1-2 และ เป็นผู้ให้บริการคลาวด์อริปไตย (Sovereign Cloud) หรือ คลาวด์แบบผสม (Hybrid Cloud) ตามที่กระทรวงดิจิทัลฯ กำหนด	
<b>4. เสถียรภาพทางการเงิน</b>	<ol style="list-style-type: none"> <li>มีเสถียรภาพทางการเงิน ทุนจดทะเบียน และมูลค่าสุทธิของกิจการ ณ วันที่ขอรับการตรวจประเมิน</li> <li>หลังได้รับการตรวจประเมินแล้ว: สำนักงานจะพิจารณาจาก ผลการดำเนินการ และ รายงานสถานะทางการเงิน อย่างต่อเนื่อง หากพบว่ามีความเสี่ยงต่อการให้บริการ ผู้ให้บริการจะต้องจัดทำรายละเอียดเพื่อชี้แจงเพิ่มเติม เช่น แผนการชดเชยหรือเยียวยาผู้ใช้บริการ</li> </ol>		
<b>5. มาตรฐานที่จำเป็นที่ต้องใช้ในการขึ้นทะเบียน</b>	<b>ด้านการรักษาความมั่นคงปลอดภัยในการใช้คลาวด์:</b> CSA STAR, ISO/IEC 27001 <b>ด้านการบริหารจัดการบริการ :</b> ISO/IEC 20000 <b>ด้านการป้องกันข้อมูลส่วนบุคคล :</b> ISO/IEC 27701	<b>ด้านการรักษาความมั่นคงปลอดภัยในการใช้คลาวด์:</b> CSA STAR, ISO/IEC 27001, ISO/IEC 27017 <b>ด้านการบริหารจัดการบริการ :</b> ISO/IEC 20000 <b>ด้านการป้องกันข้อมูลส่วนบุคคล :</b> ISO/IEC 27701, ISO/IEC 27018	มาตรฐานที่จำเป็นต้องใช้ในการขึ้นทะเบียนระดับ Tier 2 และมาตรการรักษาความมั่นคงปลอดภัยเพิ่มเติม เช่น การใช้ isolated network
<b>6. ระดับชั้นข้อมูลที่ให้บริการกับหน่วยงานภาครัฐได้</b>	ข้อมูลที่สามารถเปิดเผยได้ (Official Data)	ข้อมูลที่สามารถเปิดเผยได้ (Official Data) และ ข้อมูลที่ต้องได้รับความคุ้มครอง(Protected Data)	ข้อมูลที่ต้องได้รับความคุ้มครองสูงสุด (Highly Protected Data) เท่านั้น

ทั้งนี้ มติที่ประชุม กกค DG มีมติให้จัดทำรายละเอียดเพิ่มเติม เรื่อง

1. ความชัดเจนเรื่องเสถียรภาพทางการเงิน ให้เป็นไปตามหนังสือเวียนกรมบัญชีกลาง ที่ กก (ทวจ) 56/ว 48 เรื่องแนวทางการพิจารณางบแสดงฐานะการเงินฯ



2. มาตรฐานที่จำเป็นสำหรับศูนย์ข้อมูล (Data Center)

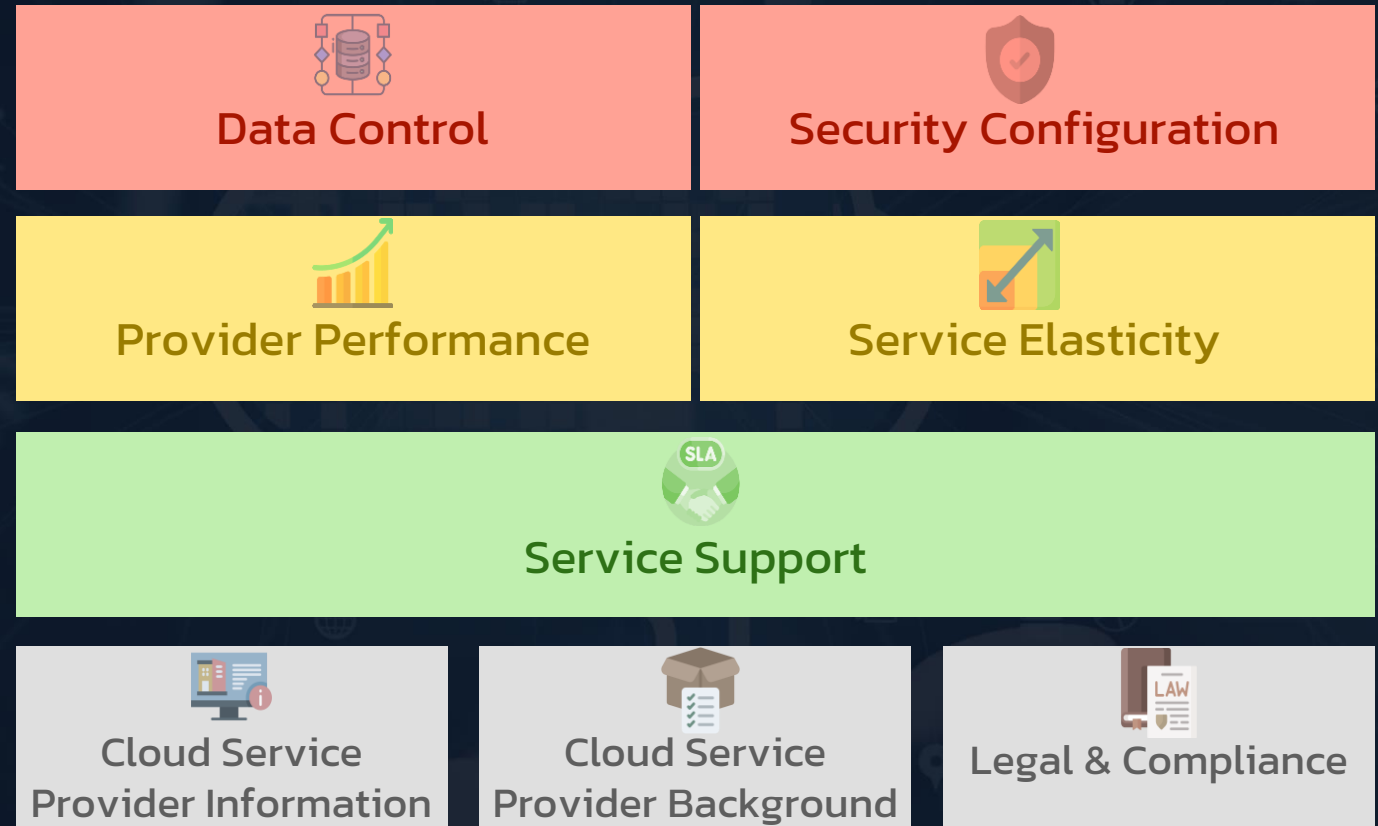
โดยทาง สพร. จะนำไปประชาสัมพันธ์และร่วมหารือกับผู้ให้บริการคลาวด์ (CSP) ต่อไป

# (ร่าง) มาตรฐานรัฐบาลดิจิทัล (มรด.)

## แนวทางการกำหนดมาตรฐานผู้ให้บริการคลาวด์ เวอร์ชัน 1.0

### 4. . แนวทางการจัดเตรียมข้อมูลฯ

หัวข้อ	ประเทศสิงคโปร์ 	ประเทศอังกฤษ 	
1. Cloud Service Provider Information	<ul style="list-style-type: none"> <li>General Information</li> <li>Certification Body Information</li> </ul>	Information	
2. Cloud Service Provider Background	<ul style="list-style-type: none"> <li>Overview</li> <li>Service Model</li> <li>Deployment Model</li> <li>Tier</li> </ul>	What the service is	
3. Legal & Compliance	<ul style="list-style-type: none"> <li>Right to audit</li> <li>Compliance</li> </ul>	Compliance	
4. Data Control	<ul style="list-style-type: none"> <li>Data ownership</li> <li>Data retention</li> </ul>	<ul style="list-style-type: none"> <li>Data Sovereignty</li> <li>Non-disclosure</li> </ul>	Hosting options and locations
5. Provider Performance	<ul style="list-style-type: none"> <li>Availability</li> <li>3<sup>rd</sup> party dependency</li> <li>BCP/DR</li> </ul>	<ul style="list-style-type: none"> <li>Liability</li> <li>Shared responsibility</li> </ul>	The levels of data backup and restore, and disaster recovery you'll provide, such as business continuity and disaster recovery plans
6. Service Support	<ul style="list-style-type: none"> <li>Change management</li> <li>Self service provisioning and management portal</li> <li>Incident and problem management</li> </ul>	<ul style="list-style-type: none"> <li>Billing</li> <li>Data portability</li> <li>Interoperability</li> <li>Access</li> <li>User management</li> <li>Life cycle</li> </ul>	<ul style="list-style-type: none"> <li>Any onboarding and offboarding support you provide</li> <li>Service levels like performance, availability and support hours</li> <li>After sales support</li> <li>Any technical requirements</li> <li>Outage and maintenance management</li> <li>Access to data (upon exit)</li> </ul>
7. Security Configuration	<ul style="list-style-type: none"> <li>Security configuration checks</li> <li>Multi-tenancy</li> <li>Hybrid cloud provisioning</li> </ul>		Security
8. Service Elasticity	<ul style="list-style-type: none"> <li>Capacity elasticity</li> <li>Network resiliency and elasticity</li> <li>Storage redundancy and elasticity</li> </ul>		Service constraints like maintenance windows or the level of customization allowed



# (ร่าง) มาตรฐานรัฐบาลดิจิทัล (มรด.)

## แนวทางการกำหนดมาตรฐานผู้ให้บริการคลาวด์ เวอร์ชัน 1.0



มาตรฐานรัฐบาลดิจิทัล

Digital Government Standard

มรด. 9-X : 256X

DGS 9-X : 256X

ว่าด้วยแนวทางการกำหนดมาตรฐานผู้ให้บริการคลาวด์  
Cloud Service Provider Standard

เวอร์ชัน 1.0

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)  
สำนักนายกรัฐมนตรี

เอกสารนี้เป็นทรัพย์สินของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ห้ามมิให้มีการเผยแพร่ ใช้งาน หรือ ใช้งานซ้ำโดยไม่ได้รับอนุญาต  
โดยคณะกรรมการนโยบายรัฐบาลดิจิทัล กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

หัวข้อ	เดิม	ปรับปรุง
ชื่อมาตรฐาน	มาตรฐานรัฐบาลดิจิทัล ว่าด้วยแนวทางการกำหนดมาตรฐานผู้ให้บริการคลาวด์ ตามนโยบายการใช้คลาวด์เป็นหลัก เวอร์ชัน 1.0	มาตรฐานรัฐบาลดิจิทัล ว่าด้วยแนวทางการกำหนดมาตรฐานผู้ให้บริการคลาวด์ เวอร์ชัน 1.0
ขอบข่าย	ประเภทของคลาวด์ คลาวด์สาธารณะ (Public Cloud) คลาวด์ส่วนตัว (Private Cloud) คลาวด์แบบกลุ่ม (Community Cloud) คลาวด์แบบผสม (Hybrid Cloud)	เพิ่มประเภทของคลาวด์ คลาวด์อธิปไตย (Sovereign Cloud) คลาวด์ส่วนตัวเสมือน (Virtual Private Cloud)  หมายเหตุ คำนิยามและประเภทสอดคล้องกับ แนวทางการใช้คลาวด์ v1.0
ระดับชั้นข้อมูลที่ให้บริการกับหน่วยงานภาครัฐได้ Tier 3	Tier 3 บริการคลาวด์ที่เกี่ยวข้องกับ ข้อมูลทั่วไป และ ข้อมูลลับ ลับมาก และ ลับที่สุดของทางราชการ  โดยเป็นเป็นผู้ให้บริการคลาวด์ <b>Sovereign Cloud</b> ตามที่กระทรวงดิจิทัลฯ กำหนด	Tier 3 บริการคลาวด์ที่เกี่ยวข้องกับ ข้อมูลที่ต้องได้รับความคุ้มครองสูงสุด (Highly Protected Data) เท่านั้น  โดยเป็นผู้ให้บริการคลาวด์อธิปไตย ( <b>Sovereign Cloud</b> ) หรือ <b>คลาวด์แบบผสม (Hybrid Cloud)</b> ตามที่กระทรวงดิจิทัลฯ กำหนด

# หากมีคำถาม หรือข้อเสนอนั้นะเกี่ยวกับมาตรฐานฯ



# THANK YOU

## DGA Contact Center

☎ 02 612 6060

✉ [contact@dga.or.th](mailto:contact@dga.or.th)

[standard.dga.or.th](http://standard.dga.or.th)