

งานประชาพิจารณ์

(ร่าง) มรต. X : 256X ว่าด้วย หลักเกณฑ์การจัดระดับชั้น ข้อมูลภาครัฐ

วันที่ 26 กุมภาพันธ์ 2569 เวลา 13.30 – 15.30 น.

โดย ทีมพัฒนามาตรฐาน 2.1
ฝ่ายมาตรฐานดิจิทัลภาครัฐ

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)



เวลา	กิจกรรม
13.00 – 13.30 น.	ลงทะเบียนเข้าร่วมงาน
13.30 – 13.45 น.	พิธีเปิดงาน <i>โดยรองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล รักษาการแทน ผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล</i>
13.45 – 14.45 น.	เสวนาในหัวข้อ สร้างรากฐานความมั่นคงข้อมูลภาครัฐด้วย “การจัดระดับชั้นข้อมูล” <i>โดยผู้ทรงคุณวุฒิ</i>
14.45 – 15.15 น.	นำเสนอ (ร่าง) มรต. X : 256X มาตรฐานรัฐบาลดิจิทัลว่า ด้วย หลักเกณฑ์การจัดระดับชั้นข้อมูลภาครัฐ เวอร์ชัน 1.0 <i>โดยผู้เชี่ยวชาญ ฝ่ายมาตรฐานดิจิทัลภาครัฐ</i>
15.15 – 15.30 น.	ถาม - ตอบ



<https://dg.th/zhtkp95nem>

• **โดย**
ดร.อาศิษ อัษฎะโพธิ์
 รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล



DGA
 ขอเชิญร่วมแสดงความคิดเห็นต่อ
(ร่าง) มาตรฐานรัฐบาลดิจิทัล
 ว่าด้วยหลักเกณฑ์การจัดระดับชั้น
 ข้อมูลภาครัฐ เวอร์ชัน 1.0

สามารถแสดงความคิดเห็นได้ตั้งแต่วันที่
2 ก.พ. – 3 มี.ค. 69
 ผ่านระบบกลางทางกฎหมาย
LAW

และสามารถร่วมงานรับฟังความคิดเห็นต่อ (ร่าง) มาตรฐานดังกล่าว ภายใต้อีชื่องาน
“สร้างรากฐานความมั่นคงข้อมูลภาครัฐ
ด้วยการจัดระดับชั้นข้อมูล”
 ในรูปแบบออนไลน์ ผ่าน **MS Teams** วันที่ 26 ก.พ. 2569 เวลา 13.30 - 15.30 น.

สแกน QR CODE
 เพื่อรับเอกสารประกอบการ
 แสดงความคิดเห็น

เชิญร่วมแสดงความคิดเห็นต่อ (ร่าง) มาตรฐานดังกล่าว ภายใต้อีชื่องาน
“สร้างรากฐานความมั่นคงข้อมูลภาครัฐ
ด้วยการจัดระดับชั้นข้อมูล”
 ในรูปแบบออนไลน์ ผ่าน **MS Teams** วันที่ 26 ก.พ. 2569 เวลา 13.30 - 15.30 น.

สแกน QR CODE
 เพื่อรับเอกสารประกอบการ
 แสดงความคิดเห็น

(ร่าง) มรต. X : 256X ว่าด้วย หลักเกณฑ์การจัดระดับชั้นข้อมูลภาครัฐ

เพื่อ เป็นหลักเกณฑ์ประกอบการใช้ดุลพินิจของ
ผู้มีอำนาจในการตัดสินใจกำหนดระดับชั้นข้อมูล
สามารถกำหนดการเข้าถึงและใช้งานข้อมูลและ
กำกับดูแลข้อมูลที่มีความอ่อนไหวหรือข้อมูลที่มีชั้น
ความลับอย่างเหมาะสม





ขอเชิญร่วมแสดงความคิดเห็นต่อ (ร่าง) มาตรฐานรัฐบาลดิจิทัล ว่าด้วยหลักเกณฑ์การจัดระดับชั้น ข้อมูลภาครัฐ เวอร์ชัน 1.0

สามารถแสดงความคิดเห็นได้ตั้งแต่วันที่

2 ก.พ. – 3 มี.ค. 69

ผ่านระบบกลางทางกฎหมาย



และสามารถร่วมงานรับฟังความคิดเห็นต่อ (ร่าง) มาตรฐานดังกล่าว ภายใต้ชื่องาน

**“สร้างรากฐานความมั่นคงข้อมูลภาครัฐ
ด้วยการจัดระดับชั้นข้อมูล”**

ในรูปแบบออนไลน์ ผ่าน  MS Teams วันที่ 26 ก.พ. 2569 เวลา 13.30 - 15.30 น.



สแกน QR CODE
เพื่อรับเอกสารประกอบการ
การแสดงความคิดเห็น



แนะนำร่างมาตรฐาน



โดย **คุณสุภัทรา เรืองวานิช**

ผู้เชี่ยวชาญ ฝ่ายมาตรฐานดิจิทัลภาครัฐ

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

**(ร่าง) มรด. X : 256X
ว่าด้วยหลักเกณฑ์การจัด
ระดับชั้นข้อมูลภาครัฐ**



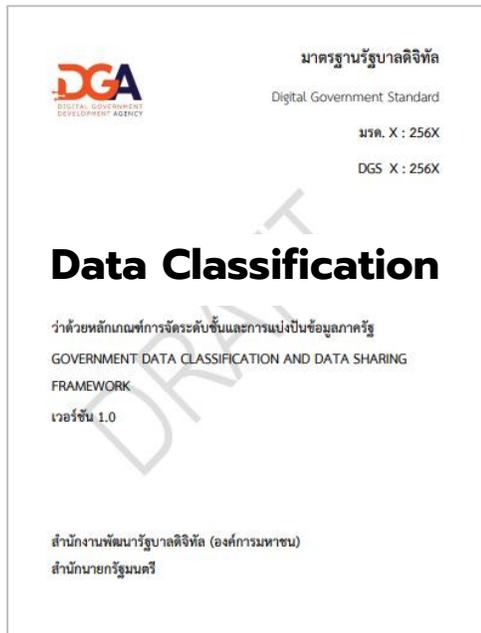
<https://dg.th/zhtkp95nem>

แนวทางการยกระดับ คงหลักการเดิมไว้ และปรับปรุงเพิ่มเติม

- เพิ่มอ้างอิงกฎหมายใหม่และหลักการสากล (NIST: SP 800-60)
- ปรับหลักการการจדרะดับชั้นเพื่อรองรับการแบ่งปันข้อมูลในอนาคต
- เพิ่มตัวอย่างข้อมูลในตาราง (Data Handling) ตามประกาศที่เกี่ยวข้อง
- ปรับแบบประเมินให้ใช้งานได้ง่ายขึ้น
- ปรับลดเนื้อหาบางส่วนเพื่อไม่ให้เกิดความซ้ำซ้อนโดยเพิ่มอ้างอิงไปยังมาตรฐานที่เกี่ยวข้อง
- เสนอปรับชื่อเล่มมาตรฐาน หลักเกณฑ์การจדרะดับชั้นข้อมูลภาครัฐ

โครงสร้าง มรด. ว่าด้วยหลักเกณฑ์การจדרะดับชั้นข้อมูล ภาครัฐ

1. บทนำ	1.1 ความเป็นมา	
	1.2 วัตถุประสงค์	
	1.3 ขอบข่าย	
	1.4 บทนิยาม	
	1.5 กฎหมายและแนวทางที่เกี่ยวข้อง	
2. กรอบแนวคิด	2.1 กรอบหลักการจדרะดับชั้นข้อมูล	2.1.1 หลักการจדרะดับชั้นข้อมูล 2.1.2 การตัดสินใจจדרะดับชั้นข้อมูลที่ต้องถูกต้อง
	2.2 วิธีการจדרะดับชั้นข้อมูล	
3. หลักเกณฑ์การจדרะดับชั้นข้อมูล	3.1 เป้าประสงค์	
	3.2 หลักเกณฑ์การจדרะดับชั้นข้อมูลภาครัฐ	3.2.1 เกณฑ์การแบ่งระดับชั้นข้อมูลภาครัฐ 3.2.2 เกณฑ์การประเมินความเสี่ยงและผลกระทบของการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต 3.2.3 ข้อเสนอแนะการจัดการข้อมูลภาครัฐที่มีการจדרะดับชั้นข้อมูล
	3.3 หลักเกณฑ์การจדרะดับชั้นข้อมูลภาครัฐ	
4. การบูรณาการจדרะดับชั้นข้อมูลกับการใช้คลาวด์	4.1 ความสำคัญของระบบคลาวด์ต่อหน่วยงานภาครัฐในต่างประเทศ	
	4.2 แนวทางการจำแนกประเภทข้อมูลกับการใช้คลาวด์	4.2.1 ข้อมูลที่ต้องได้รับความคุ้มครองสูงสุด 4.2.2 ข้อมูลที่ต้องได้รับความคุ้มครอง 4.2.3 ข้อมูลที่สามารถเปิดเผยได้
	4.3 แนวทางการจדרะดับชั้นข้อมูลกับการใช้คลาวด์	
5. เครื่องมือเพื่อนำไปสู่การปฏิบัติ	5.1 เครื่องมือและตัวอย่างการประเมิน	
	5.2 ข้อเสนอแนะสู่การปฏิบัติ	
6. ภาคผนวก	รายชื่อหมวดประเด็นความมั่นคงตามนโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ	



1. บทนำ

1. บทนำ

- 1.1 ความเป็นมา
- 1.2 วัตถุประสงค์
- 1.3 ขอบข่าย
- 1.4 บทนิยาม
- 1.5 กฎหมายและแนวทางที่เกี่ยวข้อง

วัตถุประสงค์

เพื่อเป็นเครื่องมือประกอบการใช้ดุลพินิจของผู้มีอำนาจในการตัดสินใจกำหนดระดับชั้นข้อมูล สามารถกำหนดการเข้าถึงและใช้งานข้อมูลและกำกับดูแลข้อมูลที่มีความอ่อนไหวหรือข้อมูลที่มีชั้นความลับอย่างเหมาะสม เพื่อรักษาความเป็นส่วนตัวและความปลอดภัยของข้อมูล

ขอบข่าย

1) มาตรฐาน NIST : SP 800-60 / 2) มาตรฐาน FIPS PUB 199 / 3) มาตรฐาน ISO/IEC 27001: 2022

บทนิยาม

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

กฎหมายและแนวทางที่เกี่ยวข้อง

- พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540
- ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม
- ระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. 2552 และที่แก้ไขเพิ่มเติม
- พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 มาตรา 7 และมาตรา 8 ธรรมนูญข้อมูลภาครัฐ
- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
- นโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ (พ.ศ. 2566-2570)
- ประกาศคณะกรรมการพัฒนานาธิรัฐบาลดิจิทัลเรื่อง ธรรมนูญข้อมูลภาครัฐ

2. กรอบแนวคิด

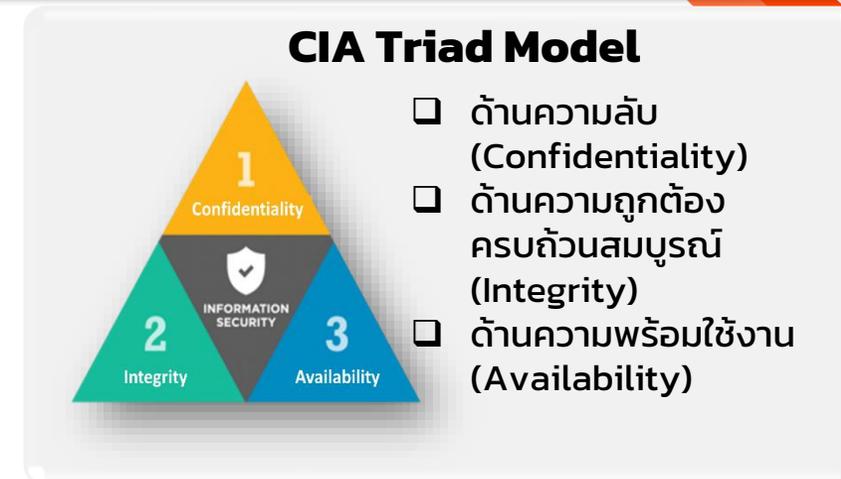
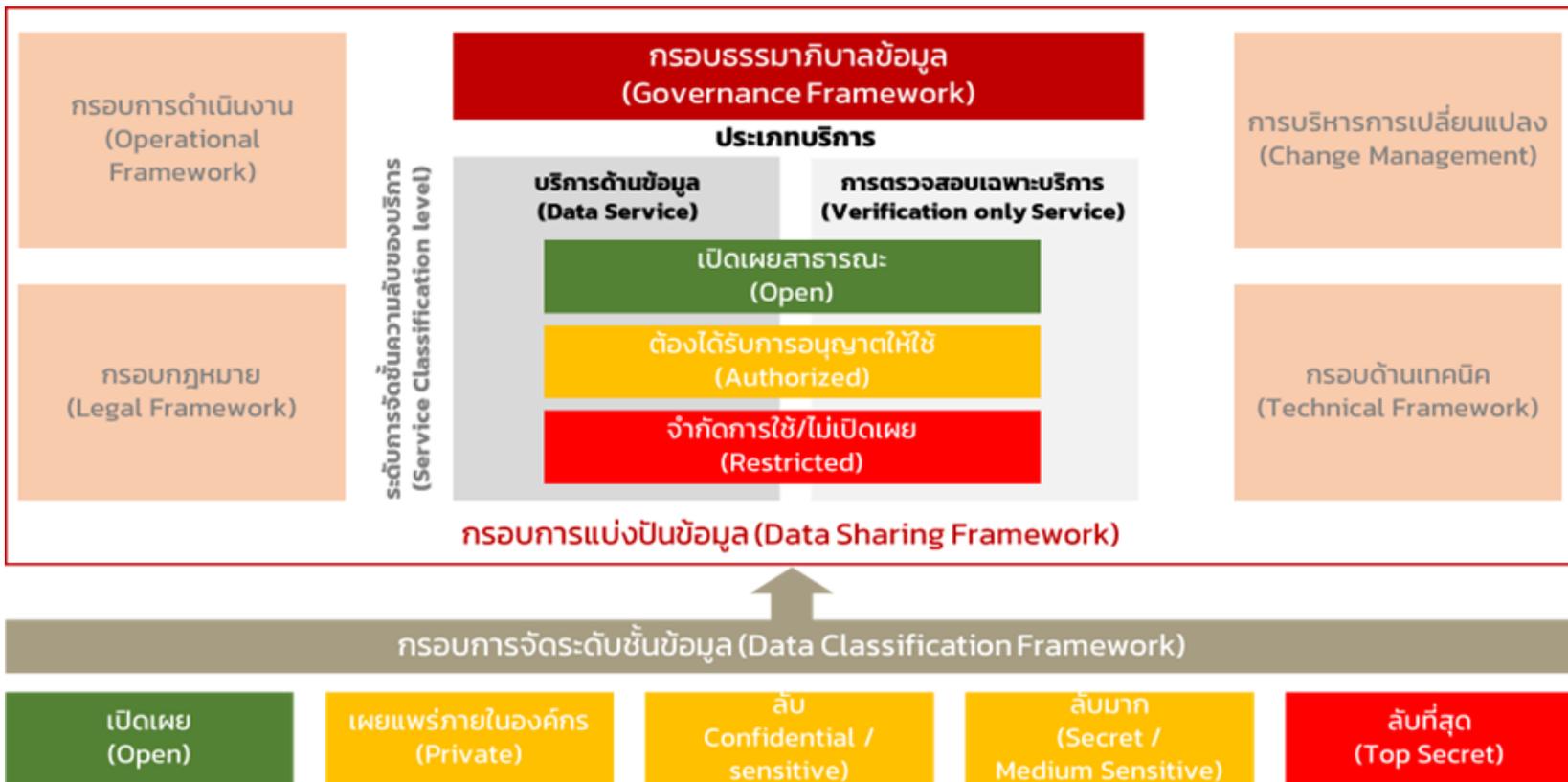
2. กรอบแนวคิด

2.1 กรอบหลักการจัดระดับชั้นข้อมูล

2.1.1 หลักการจัดระดับชั้นข้อมูล

2.1.2 การตัดสินใจจัดระดับชั้นข้อมูลที่ถูกต้อง

2.2 วิธีการจัดระดับชั้นข้อมูล



เกณฑ์การประเมิน ผลกระทบ 5 ด้าน

สอดคล้องตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566

- ด้านการเงินและสินทรัพย์
- ด้านภาพลักษณ์/ชื่อเสียง
- ด้านผู้ใช้บริการหรือประชาชน
- ด้านการดำเนินการตามกฎหมาย
- ด้านความมั่นคงของรัฐ (รวมเฉลี่ยCIA)

การประเมินความเสี่ยงของข้อมูล Risk Based Approach จาก ผลกระทบ และ โอกาสที่จะเกิด

3. หลักเกณฑ์การจัดระดับชั้นข้อมูล

3. หลักเกณฑ์การจัดระดับชั้นข้อมูล

3.1 เป้าประสงค์

3.2 หลักเกณฑ์การจัดระดับชั้นข้อมูลภาครัฐ

3.2.1 เกณฑ์การแบ่งระดับชั้นข้อมูลภาครัฐ

3.2.2 เกณฑ์การประเมินความเสี่ยงและผลกระทบของการเปิดเผยข้อมูล โดยไม่ได้รับอนุญาต

3.2.3 ข้อเสนอแนะการจัดการข้อมูลภาครัฐ ที่มีการจัดระดับชั้นข้อมูล

หมวดหมู่ข้อมูล	ระดับชั้นข้อมูล	เปิดเผย (Open)	เผยแพร่ภายในองค์กร (Private)	ลับ (Confidential)	ลับมาก (Secret)	ลับที่สุด (Top Secret)
ข้อมูลสาธารณะ		พ.ร.บ ข้อมูลข่าวสารของทางราชการ พ.ศ. 2540 (มาตรา 7 และมาตรา 9 มรด. 8 : 2567 ว่าด้วยแนวทางการเปิดเผยข้อมูลเปิดภาครัฐ)				
ข้อมูลใช้ภายใน			<ul style="list-style-type: none"> มาตรฐาน ISO/IEC 27001: 2022 			
ข้อมูลส่วนบุคคล			<ul style="list-style-type: none"> พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (มาตรา 24- 27) 	<ul style="list-style-type: none"> พ.ร.บ ข้อมูลข่าวสารของทางราชการ พ.ศ. 2540 (มาตรา 9 และมาตรา 15 ที่เปิดเผยได้) 		
ข้อมูลความลับทางราชการ		สามารถทบทวนหมวดหมู่และระดับชั้นข้อมูลได้ตามระยะเวลาและเทคโนโลยีที่เปลี่ยนแปลง		<ul style="list-style-type: none"> ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.2544 และที่แก้ไขเพิ่มเติม 		<ul style="list-style-type: none"> พ.ร.บ ข้อมูลข่าวสารของทางราชการ มาตรา 15
ข้อมูลความมั่นคง						<ul style="list-style-type: none"> พ.ร.บ ข้อมูลข่าวสารของทางราชการ มาตรา 14 นโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ

ชั้นลับที่สุด (Top Secret) เปิดเผยไม่ได้ เป็นข้อมูลที่จัดระดับ Top Secret หรือ Highly Sensitive จำกัดการใช้/ไม่เปิดเผยสำหรับข้อมูลที่จะก่อให้เกิดความสูญเสีย/ผลกระทบร้ายแรงที่สุด อาจทำให้เสียชื่อเสียงและการสูญเสียทางการเงิน/ทรัพย์สิน ต่อความมั่นคงและผลประโยชน์แห่งรัฐอย่างร้ายแรง หรือที่สำคัญยิ่งยวด (Vital) หากสูญหายหรือเปิดเผยอย่างไม่ถูกต้องเหมาะสม ซึ่งในกรณีข้อมูลข่าวสารลับที่สุดให้เป็นไปตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยงานสารบรรณ (ฉบับที่ 4) พ.ศ. 2564 ซึ่งกำหนดว่า "ข้อ 29 การติดต่อราชการให้ดำเนินการด้วยระบบสารบรรณอิเล็กทรอนิกส์เป็นหลัก เว้นแต่กรณีที่เป็นข้อมูลข่าวสารลับชั้นลับที่สุด" และให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 เช่น ข้อมูลกำลังรบ ข้อมูลด้านการข่าวกรอง ยุทธศาสตร์ ข้อมูลความมั่นคงเชิงนโยบาย

ทั้งนี้ นิยามการกำหนดข้อมูลข่าวสารลับให้อ้างอิงตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม

4. การบูรณาการจัดระดับชั้นข้อมูลกับการใช้คลาวด์

4. การบูรณาการจัดระดับชั้นข้อมูลกับการใช้คลาวด์

4.1 ความสำคัญของระบบคลาวด์ต่อหน่วยงานภาครัฐในต่างประเทศ

4.2 แนวทางการจำแนกประเภทข้อมูลกับการใช้คลาวด์

4.2.1 ข้อมูลที่ต้องได้รับความคุ้มครองสูงสุด

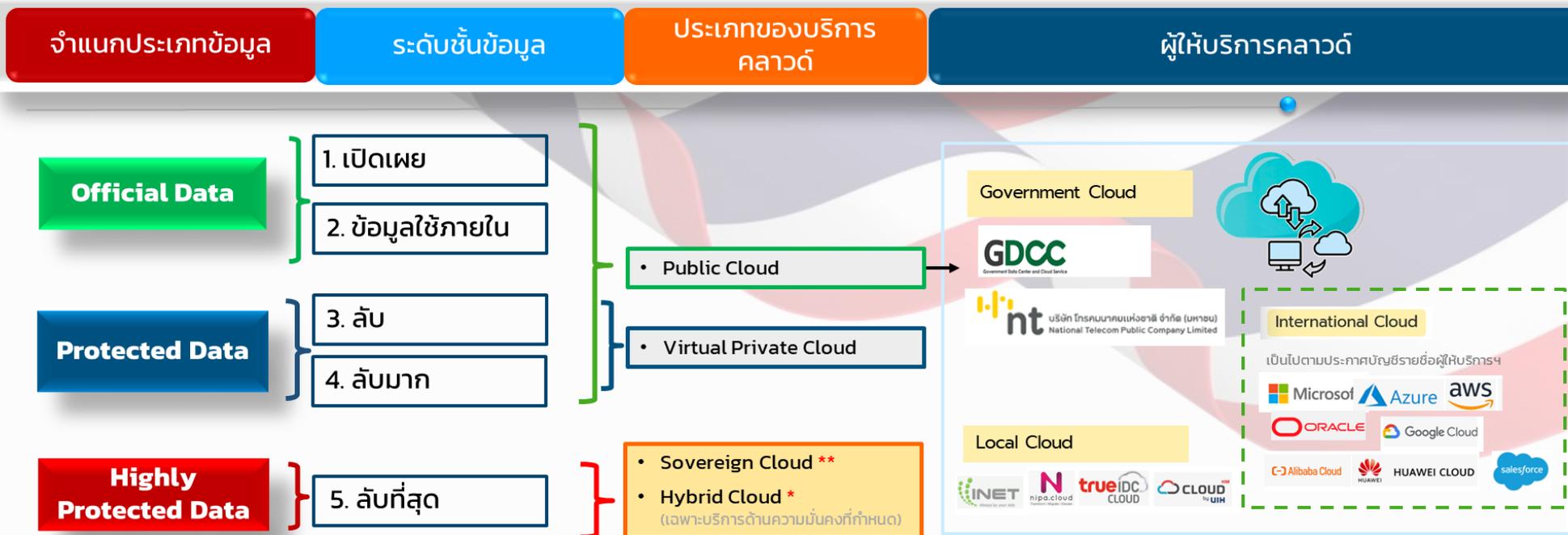
4.2.2 ข้อมูลที่ต้องได้รับความคุ้มครอง

4.2.3 ข้อมูลที่สามารถเปิดเผยได้

กรณีศึกษา ต่างประเทศ



กรอบแนวทางการจำแนกประเภทข้อมูลสำหรับการใช้คลาวด์



*ซึ่งมีการแยกข้อมูลที่ต้องได้รับความคุ้มครองสูงสุดไว้บนคลาวด์ส่วนตัว (Private Cloud)
**ผู้ให้บริการ Sovereign Cloud ให้เป็นไปตามที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมกำหนด

รายละเอียดเพิ่มเติมได้ที่ มาตรฐานฯ ว่าด้วยแนวทางการกำหนดมาตรฐานผู้ให้บริการคลาวด์ตามนโยบายการใช้คลาวด์เป็นหลัก

***อยู่ระหว่างการเสนอต่อคณะกรรมการพัฒนารัฐบาลดิจิทัล**

5. เครื่องมือเพื่อนำไปสู่การปฏิบัติ



<https://dg.th/9z07efg6li>

5. เครื่องมือเพื่อนำไปสู่การปฏิบัติ

5.1 เครื่องมือและตัวอย่างการประเมิน

5.2 ข้อเสนอแนะสู่การปฏิบัติ

การประเมินระดับชั้นข้อมูล

1 การพิจารณาหมวดหมู่

วัตถุประสงค์

- เพื่อหาหมวดหมู่ข้อมูลตาม DGF
- อ้างอิงกฎหมาย ตาม ม.14
- พรบ.ข้อมูลข่าวสาร ม.15(1) + ข้อมูลที่อยู่ในแผนความมั่นคงฯ

ผลการประเมิน

- หมวดหมู่ข้อมูลที่ไม่ต้องประเมินเพราะสามารถรู้ระดับชั้นข้อมูลได้

➤ ข้อมูลสาธารณะ เปิดเผย

➤ ข้อมูลความมั่นคง ลับที่สุด

• หมวดหมู่ข้อมูลที่ต้องประเมินต่อ

- ข้อมูลใช้ภายใน
- ข้อมูลส่วนบุคคล
- ข้อมูลข่าวสารลับ

2 การประเมิน CIA

วัตถุประสงค์

- ประเมิน CIA
- อ้างอิงกฎหมาย ตาม แผนความมั่นคงฯ
- อ้างอิงประกาศ กมช.

ผลการประเมิน

- ข้อมูลที่อยู่ในแผนความมั่นคงฯ + คะแนนรวมเฉลี่ย 3 = ข้อมูลมั่นคง
- หมวดหมู่ข้อมูลที่ไม่ต้องประเมินเพราะสามารถรู้ระดับชั้นข้อมูลได้

➤ ข้อมูลความมั่นคง ลับที่สุด

• หมวดหมู่ข้อมูลที่ต้องประเมินต่อ

- ข้อมูลใช้ภายใน
- ข้อมูลส่วนบุคคล
- ข้อมูลความลับทางราชการ

3 การประเมินความเสี่ยง

วัตถุประสงค์

- พิจารณาระดับชั้นข้อมูลของหมวดหมู่ที่ยังไม่ชัดเจน
- ความเสี่ยง=ผลกระทบ 5 ด้าน * โอกาสที่จะเกิดขึ้น

ผลการประเมิน

- ผลการประเมิน CIA จะมาอยู่ในผลกระทบด้านผลประโยชน์แห่งชาติ
- ถ้าความเสี่ยงสูง + เป็นข้อมูลตามแผนความมั่นคง = ลับที่สุด

	เปิดเผย	เผยแพร่ภายในองค์กร	ลับ	ลับมาก	ลับที่สุด
ข้อมูลสาธารณะ	/				
ข้อมูลใช้ภายใน	/	/	/	/	/
ข้อมูลส่วนบุคคล	/	/	/	/	/
ข้อมูลความลับทางราชการ			/	/	/
ข้อมูลความมั่นคง					/

5. เครื่องมือเพื่อนำไปสู่การปฏิบัติ



Template (Word)

ชุดข้อมูลคณะกรรมการ/คณะทำงาน					
ชุดข้อมูลคณะกรรมการ/คณะทำงาน เพื่อใช้ในการติดตามประเมินผลเกี่ยวกับการจัดประชุม การเบิกค่าตอบแทน เป็นต้น					
ประเภทข้อมูล					
ชุดข้อมูล คณะกรรมการ/ คณะทำงาน	ชุดข้อมูลติดต่อคณะกรรมการ/คณะทำงานของฝ่ายมาตรฐานรัฐบาลดิจิทัล ประกอบด้วย ประกอบด้วยข้อมูลส่วนบุคคลของคณะกรรมการ/คณะทำงานของฝ่ายมาตรฐานรัฐบาลดิจิทัล เช่น ชื่อ-นามสกุล ข้อมูลติดต่อ				
วัตถุประสงค์ด้าน ความปลอดภัย (CIA)	ผลกระทบด้านความลับ (Confidentiality)	ผลกระทบด้านความ ถูกต้อง ครบถ้วนสมบูรณ์ ความคงสภาพ (Integrity)	ผลกระทบด้านความพร้อม ใช้งานข้อมูล (Availability)		
	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตอย่างสงคราะห์ที่น้อย/อย่างจำกัด (limited) และเกิดผลประโยชน์แห่งชาติสำคัญน้อย (Less Important or Secondary National Interests)	การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาตอย่างสงคราะห์ที่น้อย/อย่างจำกัด (limited) และเกิดผลประโยชน์แห่งชาติสำคัญน้อย (Less Important or Secondary National Interests)	การหยุดชะงักของงานเข้าถึงหรือการใช้ข้อมูลข่าวสารหรือระบบสารสนเทศทางสงคราะห์ที่น้อย/อย่างจำกัด (limited) และเกิดผลประโยชน์แห่งชาติสำคัญน้อย (Less Important or Secondary National Interests)		
ระดับผลกระทบ	ต่ำ (1 คะแนน)	ต่ำ (1 คะแนน)	ต่ำ (1 คะแนน)		
ค่าเฉลี่ย CIA	ต่ำ (1 คะแนน)				
ผลกระทบ/ ผลประโยชน์	ภาพลักษณ์/ ชื่อเสียง	ผู้ใช้และการ ดำเนินงาน	การเงินและ สินทรัพย์	กฎหมายและ ระเบียบข้อบังคับ	ผลประโยชน์ แห่งชาติ
โอกาสที่จะเกิดขึ้น (Likelihood)	น้อย (2 คะแนน)	น้อย (2 คะแนน)	น้อย (2 คะแนน)	น้อย (2 คะแนน)	น้อยมาก (1 คะแนน)
ประเมินภาวะระดับความ รุนแรงของผลกระทบ (Impact)	ต่ำ (1 คะแนน)	ต่ำ (1 คะแนน)	ปานกลาง (2 คะแนน)	ปานกลาง (2 คะแนน)	ต่ำ (1 คะแนน)
ความเสี่ยง (Likelihood x Impact)	2 คะแนน	2 คะแนน	4 คะแนน	4 คะแนน	1 คะแนน
ระดับความเสี่ยง โดยรวม	ต่ำ 3 คะแนน (ระดับความเสี่ยง 3.4 คะแนน)				
ระดับชั้นความลับ	เผยแพร่ภายในองค์กร (Private)				

- ✓ รูปแบบกระดาษ
- ✓ การคำนวณต้องใช้การกรอกข้อมูล
- ✓ ต้องคำนวณผลด้วยตนเอง

Template (Excel)

1 ส่วนที่ 1: การพิจารณาหมวดหมู่ข้อมูล		2 ส่วนที่ 2: การประเมินวัตถุประสงค์ด้านความปลอดภัย (CIA)	
ข้อมูลเป็นข้อมูลลับที่สุดหรือไม่	จงเลือกคำตอบ	โมเดลที่ต้องประเมินในส่วนที่ 3 ค่าคะแนนในส่วนนี้จะถูกนำไปคำนวณเป็นค่าผลประโยชน์แห่งชาติ (ผลรวมเฉลี่ยCIA)	
จงกว่าจะเห็นคำว่า "จบคำถามในส่วนที่ 1"		วัตถุประสงค์ด้านความปลอดภัย	จงเลือกระดับผลกระทบ โดยคลิกที่เซลล์ด้านล่าง
1) เป็นข้อมูลเกี่ยวกับพระมหากษัตริย์ ตาม มาตรา.14* ตาม พรบ.ข่าวสารฯหรือไม่ ?	ไม่	1) ด้านความลับ (Confidentiality)	กลาง (ผลกระทบจากการเปิดเผยข้อมูลมาก/วงกว้าง)
2) เป็นข้อมูลตาม พรบ.ข้อมูลข่าวสารฯ มาตรา 15 (1) ความมั่นคงของรัฐหรือไม่ ?	ไม่	2) ด้านความถูกต้อง สมบูรณ์ (Integrity)	กลาง (แก้ไขได้ ต้องใช้ระยะเวลา/กู้คืนได้)
3) ห้ามเปิดเผยตามมาตรา 15 ตาม พรบ.ข่าวสารฯ และมีกำหนดขึ้นความลับหรือไม่?	ไม่	3) ด้านความพร้อมใช้งาน (Availability)	กลาง (กระทบต่อการดำเนินงานหลัก แต่แก้ไขได้)
4) เป็นข้อมูลส่วนบุคคลหรือไม่ ?	ไม่	ผลรวมเฉลี่ย	กลาง (กระทบ CIA ระดับกลาง)
5) ห้ามเปิดเผยตามมาตรา 15 ตาม พรบ.ข่าวสารฯ หรือไม่ ?	ไม่		
6) ต้องได้รับอนุญาตก่อนเผยแพร่ หรือไม่	ใช่		
จบคำถามในส่วนที่ 1			

3 ส่วนที่ 3: การประเมินความเสี่ยงและผลกระทบของการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต		
การประเมินความเสี่ยง	จงเลือกระดับผลกระทบ โดยคลิกที่เซลล์ด้านล่าง	จงเลือกโอกาสที่จะเกิดขึ้น โดยคลิกที่เซลล์ด้านล่าง
ยกเว้นด้าน "ด้านความมั่นคงของรัฐ" ซึ่งเป็นค่าคะแนนจากส่วนที่ 2		
ด้านการเงินและสินทรัพย์	มูลค่าความเสียหายในระดับต่ำ	น้อยครั้ง (ปีละไม่เกิน 2 ครั้ง)
ด้านภาพลักษณ์/ชื่อเสียง	ต่ำ (ระดับองค์กร)	บางครั้ง (ไตรมาสละ 1 ครั้ง)
ด้านผู้ใช้บริการหรือประชาชน	ต่ำ (ระดับองค์กร)	น้อยครั้ง (ปีละไม่เกิน 2 ครั้ง)
ด้านการดำเนินงานตามกฎหมาย	ต่ำ (ได้รับบทลงโทษตามกฎหมายปกครอง)	น้อยมาก (แทบจะไม่เกิด หรือปีละ 1 ครั้ง)
ด้านความมั่นคงของรัฐ (ผลรวมเฉลี่ยCIA)	กลาง (กระทบ CIA ระดับกลาง)	น้อยครั้ง (ปีละไม่เกิน 2 ครั้ง)
ผลรวมความเสี่ยงเฉลี่ย	ต่ำมาก	

แนวทางการปรับปรุง

- ✓ อยู่ในรูปแบบที่ใช้งานง่าย
- ✓ แสดงตัวเลือก Drop-down
- ✓ ตัวเลือก Drop-down สามารถปรับเปลี่ยนได้ ตามบริบทหน่วยงาน
- ✓ แสดงผลสรุปการประเมินอัตโนมัติ

สรุปผลในส่วนที่ 3		
จบการประเมิน		
หมวดหมู่ข้อมูล	ระดับชั้นข้อมูล	การจำแนกประเภทข้อมูล
ข้อมูลใช้ภายในองค์กร	เผยแพร่ภายในองค์กร	Official Data

6. ภาคผนวก

6. ภาคผนวก

รายชื่อหมวดประเด็นความมั่นคงตามนโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ

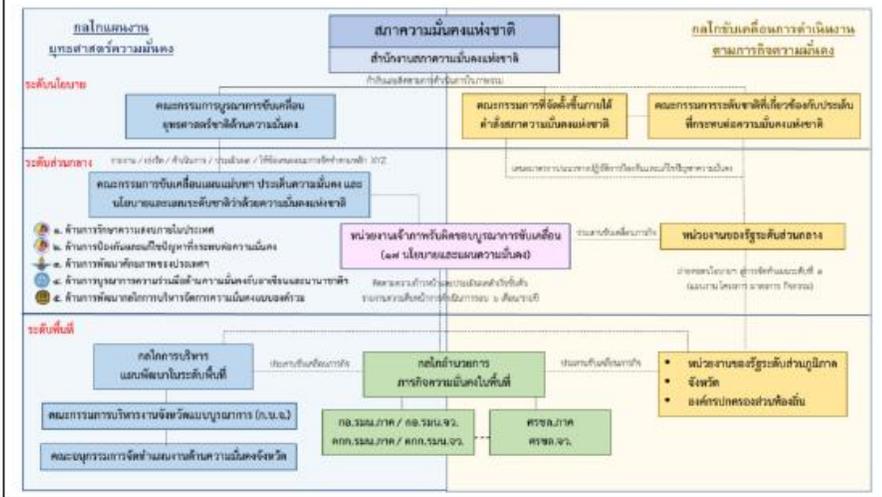
นโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ (พ.ศ. 2566 - 2570)



ส่วนที่ ๔ นโยบายและแผนความมั่นคง	๔๐
• หมวดประเด็นความมั่นคง	
นโยบายและแผนความมั่นคงที่ ๑ การเสริมสร้างความมั่นคงของสถาบันหลักของชาติ	๔๓
นโยบายและแผนความมั่นคงที่ ๒ การปกป้องอธิปไตยและผลประโยชน์ของชาติและการพัฒนาศักยภาพการป้องกันประเทศ	๔๔
นโยบายและแผนความมั่นคงที่ ๓ การรักษาความมั่นคงและผลประโยชน์ของชาติพื้นที่ชายแดน	๔๖
นโยบายและแผนความมั่นคงที่ ๔ การรักษาความมั่นคงและผลประโยชน์ของชาติทางทะเล	๔๙
นโยบายและแผนความมั่นคงที่ ๕ การป้องกันและแก้ไขปัญหาจังหวัดชายแดนภาคใต้	๕๒
นโยบายและแผนความมั่นคงที่ ๖ การบริหารจัดการผู้หลบหนีเข้าเมืองและผู้อพยพย้ายถิ่นฐานแบบไม่ปกติ	๕๕
นโยบายและแผนความมั่นคงที่ ๗ การป้องกันและแก้ไขปัญหาการค้ามนุษย์	๕๘
นโยบายและแผนความมั่นคงที่ ๘ การป้องกันปราบปราม และแก้ไขปัญหาอาชญากรรม	๖๑
นโยบายและแผนความมั่นคงที่ ๙ การป้องกันและบรรเทาสาธารณภัย	๖๔
นโยบายและแผนความมั่นคงที่ ๑๐ การป้องกันและแก้ไขปัญหาความมั่นคงทางไซเบอร์	๖๗
นโยบายและแผนความมั่นคงที่ ๑๑ การป้องกันและแก้ไขปัญหาการก่อการร้าย	๖๙
นโยบายและแผนความมั่นคงที่ ๑๒ การสร้างศุลกาภระหว่างประเทศ	๗๒
นโยบายและแผนความมั่นคงที่ ๑๓ การบริหารจัดการภาวะฉุกเฉินด้านสาธารณสุขและโรคติดต่ออุบัติใหม่	๗๕
• หมวดประเด็นศักยภาพความมั่นคง	
นโยบายและแผนความมั่นคงที่ ๑๔ การพัฒนาศักยภาพการเตรียมพร้อมแห่งชาติและการบริหารจัดการวิกฤตการณ์ระดับชาติ	๗๘
นโยบายและแผนความมั่นคงที่ ๑๕ การพัฒนาระบบข่าวกรองแห่งชาติ	๘๑
นโยบายและแผนความมั่นคงที่ ๑๖ การบูรณาการข้อมูลด้านความมั่นคง	๘๓
นโยบายและแผนความมั่นคงที่ ๑๗ การเสริมสร้างความมั่นคงเชิงพื้นที่	๘๕

๓. กลไกการบริหารจัดการ

กลไกการบริหารจัดการมีความสำคัญในการขับเคลื่อนและติดตามประเมินผลนโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ (พ.ศ. ๒๕๖๖ - ๒๕๗๐) ตามหลักการบริหารงานคุณภาพ (Plan Do Check Act: PDCA) ทั้ง ๔ ขั้นตอน เพื่อให้เกิดกระบวนการทำงาน “ตั้งเป้า ปฏิบัติ ตรวจสอบ ปรับปรุง”



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

17
หมวดประเด็น
ความมั่นคง
12
หน่วยงาน



ขอเชิญร่วมแสดงความคิดเห็นต่อ
(ร่าง) มาตรฐานรัฐบาลดิจิทัล
ว่าด้วยหลักเกณฑ์การจัดระดับชั้น
ข้อมูลภาครัฐ เวอร์ชัน 1.0

สามารถแสดงความคิดเห็นได้ตั้งแต่วันที่
2 ก.พ. – 3 มี.ค. 69

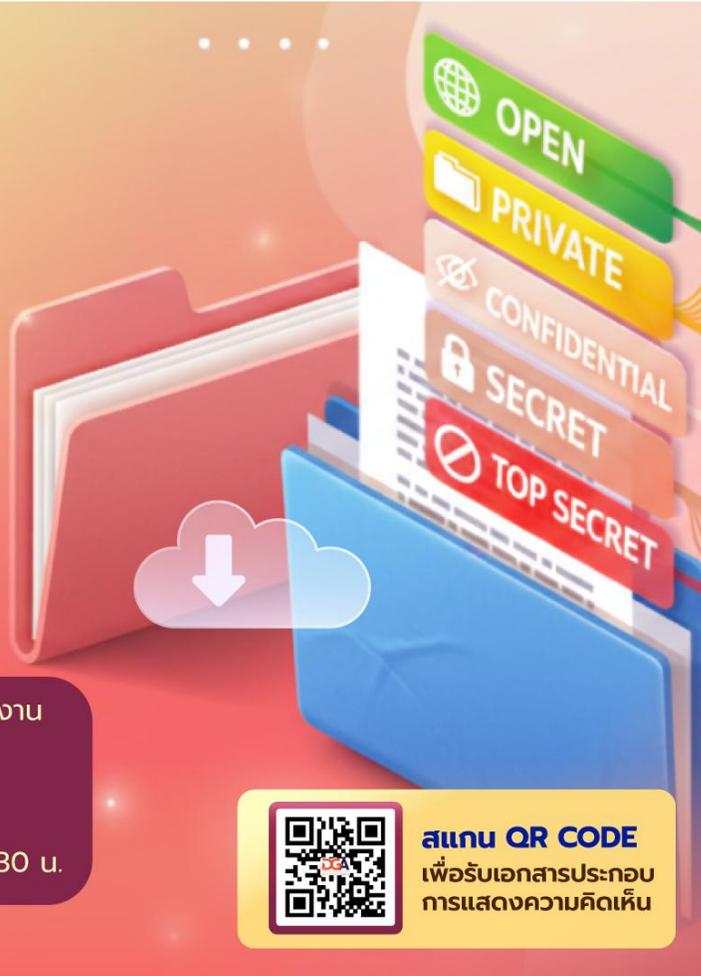
ผ่านระบบกลางทางกฎหมาย



และสามารถร่วมงานรับฟังความคิดเห็นต่อ (ร่าง) มาตรฐานดังกล่าว ภายใต้ชื่องาน

**“สร้างรากฐานความมั่นคงข้อมูลภาครัฐ
ด้วยการจัดระดับชั้นข้อมูล”**

ในรูปแบบออนไลน์ ผ่าน MS Teams วันที่ 26 ก.พ. 2569 เวลา 13.30 - 15.30 น.



สแกน QR CODE
เพื่อรับเอกสารประกอบ
การแสดงความคิดเห็น



แสดงความคิดเห็นผ่าน
ระบบกลางทางกฎหมาย

แนะนำเว็บไซต์
แหล่งข้อมูล เสริมพลัง สร้างความรู้

standard.dga.or.th



DGA Thailand



DGA Thailand



DGA Thailand



contact@dga.or.th

แนวทางการจำแนกประเภทข้อมูลเพื่อใช้บริการคลาวด์ (*อยู่ระหว่างการเสนอต่อคณะกรรมการ DG)

หน่วยงานควรมีการกำหนดระดับชั้นข้อมูลที่สอดคล้องกับกฎหมาย เพื่อพิจารณาเลือกใช้คลาวด์ที่เหมาะสม

ระดับชั้นข้อมูล		จำแนกประเภทข้อมูล	คำอธิบาย	ประเภทบริการคลาวด์ที่แนะนำ	ข้อกำหนดด้านถิ่นที่อยู่ข้อมูล
1	เปิดเผย (Public)	Official Data	ข้อมูลข่าวสารที่รัฐเปิดเผยให้ประชาชนโดยทั่วไป ผ่านเว็บไซต์ social media	Public Cloud	ควรอยู่ในประเทศไทย (ให้หัวหน้าส่วนราชการพิจารณาความจำเป็นและความเหมาะสม)
2	เผยแพร่ภายในองค์กร (Internal)		ข้อมูลที่หน่วยงานใช้ในการปฏิบัติงานภายใน เช่น หนังสือสารบรรณ การประชุมออนไลน์ เอกสารจัดซื้อจัดจ้าง เป็นต้น		
3	ลับ (Confidential)	Protected Data	ข้อมูลที่หากเปิดเผยอาจเกิดความเสียหายต่อรัฐ เช่น ข้อมูลการเสียหาย ข้อมูลบัญชีธนาคาร ข้อมูลประวัติการรักษาพยาบาล	Public Cloud (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	Sovereign Cloud (กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม กำหนดผู้ให้บริการ) หรือ Hybrid Cloud (เฉพาะบริการด้านความมั่นคงที่กำหนด)	

หมายเหตุ

- ข้อมูลที่ควรอยู่ในประเทศไทย หมายถึง ข้อมูลที่จัดเก็บอยู่ในสถานะพัก (Data-at-Rest) โดยไม่รวมถึงข้อมูลที่อยู่ระหว่างการรับส่ง (Data-in-Transit) หรือการประมวลผล (Data Processing)
- Sovereign Cloud (คลาวด์อธิปไตย) หมายถึง บริการคลาวด์ที่อยู่ภายใต้การควบคุมโดยภาครัฐและดูแลโดยบุคลากรที่ได้รับอนุญาต และใช้สำหรับให้บริการกับหน่วยงานของรัฐเท่านั้น
- การจัดระดับชั้นข้อมูลมีความสอดคล้องกับกฎหมาย: พ.ร.บ. ข้อมูลข่าวสารของราชการ พ.ศ. 2540 , พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และ ประกาศ กมช. เรื่อง หลักเกณฑ์ลักษณะหน่วยงานที่มีการทิวหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมายการควบคุมและกำกับดูแล พ.ศ. 2568