งานประชาพิจารณ์

(ร่าง) มรด. X : 256X ว่าด้วย หลักเกณฑ์การจัดระดับชั้นข้อมูลภาครัฐ

วันที่ 26 กุมภาพันธ์ 2569 เวลา 13.30 – 15.30 น.

โดย ทีมพัฒนามาตรฐาน 2.1
ฝ่ายมาตรฐานดิจิทัลภาครัฐ
สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

DGA
DIGITAL GOVERNMENT DEVELOPMENT AGENCY

DGA
DIGITAL GOVERNMENT DEVELOPMENT AGENCY

ขอเชิญร่วมแสดงความคิดเห็นต่อ

(ร่าง) มาตรฐานรัฐบาลดิจิทัล ว่าด้วยหลักเกณฑ์การจัดระดับชั้นข้อมูลภาครัฐ เวอร์ชัน 1.0

สามารถแสดงความคิดเห็นได้ตั้งแต่วันที่

2 ก.พ. – 3 มี.ค. 69

ผ่านระบบกลางทางกฎหมาย

LAW ระบบกลางทางกฎหมาย

และสามารถร่วมงานรับฟังความคิดเห็นต่อ (ร่าง) มาตรฐานดังกล่าว ภายใต้ชื่องาน

"สร้างรากฐานความมั่นคงข้อมูลภาครัฐ ด้วยการจัดระดับชั้นข้อมูล"

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

สแกน QR CODE
เพื่อรับเอกสารประกอบการแสดงความคิดเห็น

วิทยากรช่วงเสวนา

ผู้ช่วยศาสตราจารย์ ดร.ณัฐวุฒิ หนูไพโรจน์
ประธานกรรมการจัดทำร่างมาตรฐานฯ (SC)

ศาสตราจารย์ ดร.ธีรณี อจลากุล
ผู้อำนวยการสถาบันข้อมูลขนาดใหญ่ (องค์การมหาชน) และ ประธานคณะทำงานเทคนิคฯ (TC2)

พลอากาศตรี จเด็ด คูหะก้องกิจ
ผู้ช่วยเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ดร.อาศิส อัญญะโพธิ์
รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

ดร.อุรัชฎา เกตุพรหม
ผู้อำนวยการฝ่ายมาตรฐานดิจิทัลภาครัฐ สพร.
(ผู้ดำเนินรายการ)

ช่วงเสวนา

- **ประเด็นคำถามที่ 1**

การจัดระดับชั้นข้อมูลของภาครัฐ ควรพัฒนาไปในทิศทางอย่างไร

ช่วงเสวนา

- ประเด็นคำถามที่ 2

อะไรคือความท้าทายหลัก ในการนำการจัดระดับชั้นข้อมูล จากกรอบกฎหมายและนโยบาย ไปสู่ การปฏิบัติจริง ในองค์กรภาครัฐ

ทำไมถึงต้องมีการจัดระดับชั้นข้อมูล?

ผู้ช่วยศาสตราจารย์ ดร.ณัฐวุฒิ หนูไพโรจน์
ประธานกรรมการจัดทำร่างมาตรฐานฯ (SC)

- เพื่อลดความกังวลในการแบ่งปันข้อมูล (เปิด = เสี่ยง, ปิด = ปลอดภัย, ไม่มี KPI ในการเปิด แต่มีบทลงโทษถ้าข้อมูลรั่ว
- เรากำลังเข้าสู่ยุคของ AI Government เพื่อความรวดเร็ว และความโปร่งใส แต่คุณภาพ AI ขึ้นกับคุณภาพของข้อมูล และความสามารถในการเข้าถึงข้อมูล
- การเปิดเผยข้อมูลที่เหมาะสม และถูกต้อง จะช่วยสร้างความสามารถในการแข่งขันทั้งในภาครัฐและภาคเอกชน

การจัดระดับชั้นข้อมูลของภาครัฐ ควรพัฒนาไปในทิศทางอย่างไร ?

ผู้ช่วยศาสตราจารย์
ดร.ณัฐวุฒิ หนูไพโรจน์
ประธานกรรมการจัดทำร่าง
มาตรฐานฯ (SC)

- การจัดระดับชั้นข้อมูลเป็นเพียงขั้นแรกเท่านั้น
- สิ่งที่ควรจะไปต่อคือการจัดระดับชั้นข้อมูลตามการใช้งาน เพื่อให้เกิดการใช้ประโยชน์ หน่วยงานที่เข้าถึงได้ อย่างถูกต้อง มีกฎระเบียบรองรับ
  - –การใช้งานข้อมูลภายในหน่วยงาน
  - –การใช้งานข้อมูลข้ามหน่วยงาน
  - –การใช้งานข้อมูลรัฐโดยประชาชน/ภาคเอกชน
- การพัฒนาไปสู่ Government Data Sharing Framework (National-Level Trust Framework)

อะไรคือความท้าทายหลักในการจัดระดับชั้นข้อมูลจากกรอบกฎหมายและนโยบาย ไปสู่การปฏิบัติจริง ในองค์กรภาครัฐ?

ผู้ช่วยศาสตราจารย์
ดร.ณัฐวุฒิ หนูไพโรจน์
ประธานกรรมการจัดทำร่าง
มาตรฐานฯ (SC)

- การเปลี่ยนแปลงที่รวดเร็วของเทคโนโลยีกับการออกกฎหมายให้สอดคล้องกัน
- ขาดเจ้าของข้อมูลและโครงสร้างกำกับ
- ค่านิยมในอดีต: "Data Sharing = Risk”, “Secret Data = Power”
- ไม่มีแรงจูงใจเชิงนโยบายที่ชัดเจน

แนวทางการจำแนกประเภทข้อมูลเพื่อใช้บริการคลาวด์ (*อยู่ระหว่างการเสนอต่อคณะกรรมการ DG)

หน่วยงานควรมีการกำหนดระดับชั้นข้อมูลที่สอดคล้องกับกฎหมาย เพื่อพิจารณาเลือกใช้คลาวด์ที่เหมาะสม

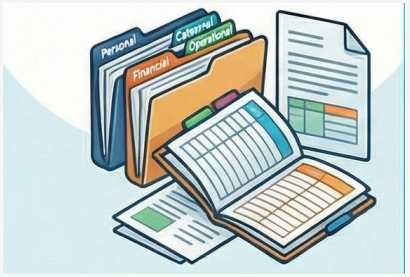
	ระดับชั้นข้อมูล	จำแนกประเภทข้อมูล	คำอธิบาย	ประเภทบริการคลาวด์ที่แนะนำ	ข้อกำหนดด้านถิ่นที่อยู่ข้อมูล
1	เปิดเผย (Public)	Official Data	ข้อมูลข่าวสารที่รัฐเปิดเผยให้ประชาชนโดยทั่วไป ผ่านเว็บไซต์ social media	Public Cloud	ควรอยู่ในประเทศไทย (ให้หัวหน้าส่วนราชการพิจารณาความจำเป็นและความเหมาะสม)
2	เผยแพร่ภายในองค์กร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

หมายเหตุ

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

การกำหนดคุณลักษณะข้อมูลหรือระบบสารสนเทศ

ประกาศ กมช. เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566



STEP 1
ระบุประเภทข้อมูล/ระบบ

ประเภทข้อมูล/ระบบสารสนเทศที่ถูกใช้ เช่น

- ❑ ภารกิจในการบริการประชาชน
- ❑ การบริหารทรัพยากร
- ❑ งานสนับสนุน

STEP 2
กำหนดระดับผลกระทบเบื้องต้น

จัดระดับผลกระทบตาม **CIA** เป็น 3 ระดับ *(ต่ำ, กลาง, สูง)* พิจารณาแต่ละด้าน ดังนี้

- ❑ ความเสียหาย**ทางการเงิน หรือทรัพย์สิน** หรือต่อชื่อเสียงของหน่วยงาน
- ❑ ผลกระทบต่อจำนวนผู้ใช้บริการ บุคลากร หรือประชาชนที่**อาจได้รับอันตรายถึงชีวิต** ร่างกาย อนามัย ทรัพย์สิน หรือความเสียหายอื่นใด
- ❑ ผลกระทบต่อ**ความสามารถในการดำเนินการตามหน้าที่**ของหน่วยงาน
- ❑ ผลกระทบต่อ**ความมั่นคงของรัฐ และความสงบเรียบร้อย**ภายในประเทศ

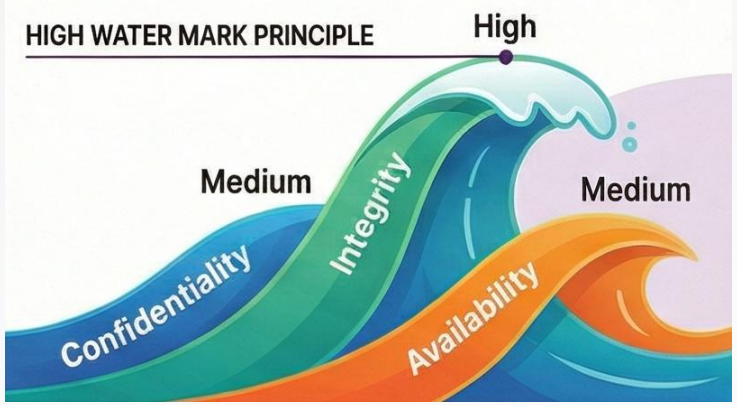
- ➢ กรณีเป็นหน่วยงาน CII ให้หน่วยงาน REG กำหนดแนวทางประเมินผลกระทบให้หน่วยงาน CII
- ➢ กรณีที่สถานการณ์ด้านความมั่นคงปลอดภัยไซเบอร์เปลี่ยนแปลงไป REG อาจกำหนดผลกระทบเพิ่มเติม หรือยกเว้น หรือยกเลิกผลกระทบข้อใดข้อหนึ่ง หรือหลายข้อก็ได้

STEP 3
ทบทวน และสรุประดับผลกระทบรายข้อมูล/ระบบ

สรุประดับผลกระทบรายข้อมูล/ระบบ

STEP 4
กำหนดระดับผลกระทบที่สูงที่สุด

ใช้ระดับ**ผลกระทบสูงที่สุด**จากข้อมูลทุกประเภทในระบบนั้น มาเป็นตัวกำหนดระดับผลกระทบรวม



FINAL IMPACT LEVEL : HIGH

The Security Characteristic Formula:

{(Confidentiality, **HIGH**), (Integrity, **MEDIUM**), (Availability, **MEDIUM**)}

"ผลลัพธ์" เพื่อการเลือกมาตรการควบคุม

ระดับผลกระทบที่สรุปได้จะใช้เป็นเกณฑ์ในการเลือกมาตรการควบคุม (Security Controls) ตาม "มาตรฐานขั้นต่ำ"

การดำเนินการตาม "มาตรฐานขั้นต่ำ"

ประกาศ สกมช. เรื่อง มาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566

	ประมวลแนวทางปฏิบัติ	กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์				
		Identify	Protect	Detect	Respond	Recover
"ต่ำ" (Low Impact) ▪ ประมวลฯ 2 ข้อ ▪ กรอบฯ 9 ข้อ	❑ Cybersecurity Risk Assessment ❑ Incident Response Plan	❑ Asset Management ❑ Risk Assessment and Risk Management Strategy	❑ Access Control ❑ System Hardening ❑ Cybersecurity Awareness	❑ Cybersecurity Threat Detection and Monitoring	❑ Cybersecurity Incident Response Plan ❑ Crisis Communication Plan ❑ Cybersecurity Exercise	
"กลาง" (Medium Impact) ▪ ประมวลฯ 3 ข้อ ▪ กรอบฯ 11 ข้อ	❑ **Cybersecurity Audit Plan** ❑ Cybersecurity Risk Assessment ❑ Incident Response Plan	❑ Asset Management ❑ Risk Assessment and Risk Management Strategy	❑ Access Control ❑ System Hardening ❑ **Remote Connection** ❑ **Removable Storage Media** ❑ Cybersecurity Awareness	❑ Cybersecurity Threat Detection and Monitoring	❑ Cybersecurity Incident Response Plan ❑ Crisis Communication Plan ❑ Cybersecurity Exercise	
"สูง" (High Impact) ▪ ประมวลฯ 3 ข้อ ▪ กรอบฯ 15 ข้อ	❑ Cybersecurity Audit Plan ❑ Cybersecurity Risk Assessment ❑ Incident Response Plan	❑ Asset Management ❑ Risk Assessment and Risk Management Strategy ❑ **Vulnerability Assessment and Penetration Testing** ❑ **Third Party Management**	❑ Access Control ❑ System Hardening ❑ Remote Connection ❑ Removable Storage Media ❑ Cybersecurity Awareness ❑ **Information Sharing**	❑ Cybersecurity Threat Detection and Monitoring	❑ Cybersecurity Incident Response Plan ❑ Crisis Communication Plan ❑ Cybersecurity Exercise	❑ **Cybersecurity Resilience and Recovery**

การดำเนินการตาม “ข้อกำหนดขั้นต่ำระบบคลาวด์”

ประกาศ กมช. เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567

Minimum Requirements

High impact

13 controls

Cloud Security Governance = 3
Cloud Infra. Security & Op. = 10

Moderate impact

11 controls

Cloud Security Governance = 3
Cloud Infra. Security & Op. = 8

Low impact

8 controls

Cloud Security Governance = 2
Cloud Infra. Security & Op. = 6

Certification

CSCs	CSPs
- By certify body - This standard	- By certify body - This standard - ISO/IEC 27017 –or– CSA STAR L2/CCM - ISO/IEC 27018 - ISO/IEC 27701
- By regulator –or– certify body - This standard	- By certify body - This standard - CSA STAR L2/CCM - ISO/IEC 27701
- Self-assessment - This standard	- By certify body - This standard - ISO/IEC 27001 - CSA STAR L1/CCM Lite

การดำเนินการตาม “ข้อกำหนดขั้นต่ำระบบคลาวด์”

ประกาศ กมช. เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567

ประเภทของข้อมูลหรือระบบสารสนเทศ*	ข้อกำหนดขั้นต่ำ	การตรวจรับรองสำหรับผู้ใช้บริการคลาวด์	การตรวจรับรองสำหรับผู้ให้บริการคลาวด์
ผลกระทบระดับต่ำ **ต่ำ**	ข้อกำหนดส่วนที่ ๑ - เฉพาะข้อ ๕.๑.๑, ๕.๑.๒ ข้อกำหนดส่วนที่ ๒ - เฉพาะข้อ ๕.๒.๑, ๕.๒.๒, ๕.๒.๓, ๕.๒.๔, ๕.๒.๘, ๕.๒.๙	ประเมินตนเอง (Self-assessment) พร้อมแนบหลักฐานและขออนุมัติไปยังผู้บริหารสูงสุดของหน่วยงาน โดยเก็บรักษาไว้ที่หน่วยงานและส่งให้สำนักงานด้วย	ได้รับการรับรองโดยหน่วยงานให้บริการตรวจรับรอง (Certify Body) ตามวงรอบ ๓ ปี ประกอบด้วยการตรวจรับรองในปีที่ ๑ และการตรวจสำรวจในปีที่ ๒ และ ๓ และได้รับการรับรองตามมาตรฐาน ISO/IEC 27001 Certification และ CSA STAR Level 1/CCM Lite เป็นอย่างน้อย
ผลกระทบระดับกลาง **กลาง**	ข้อกำหนดส่วนที่ ๑ - ทุกข้อ ข้อกำหนดส่วนที่ ๒ - เฉพาะข้อ ๕.๒.๑, ๕.๒.๒, ๕.๒.๓, ๕.๒.๔, ๕.๒.๗, ๕.๒.๘, ๕.๒.๙, ๕.๒.๑๐	ได้รับการรับรองโดยหน่วยงานควบคุมหรือกำกับดูแล (Attestation) หรือ ได้รับการรับรองโดยหน่วยงานให้บริการตรวจรับรอง (Certify Body) ตามวงรอบ ๓ ปี ประกอบด้วยการตรวจรับรองในปีที่ ๑ และการตรวจสำรวจในปีที่ ๒ และ ๓	ได้รับการรับรองโดยหน่วยงานให้บริการตรวจรับรอง (Certify Body) ตามวงรอบ ๓ ปี ประกอบด้วยการตรวจรับรองในปีที่ ๑ และการตรวจสำรวจในปีที่ ๒ และ ๓ และได้รับการรับรองตามมาตรฐาน CSA STAR Level 2/CCM และ ISO/IEC 27701 Certification เป็นอย่างน้อย

ระดับผลกระทบ	การรักษาความลับ (Confidentiality)	การรักษาความถูกต้องครบถ้วน (Integrity)	สภาพพร้อมใช้งาน (Availability)
ระดับต่ำ	ข้อมูลที่ถูกกำหนดชั้นความลับเป็นชั้นลับ	การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบเพียงเล็กน้อยหรืออย่างจำกัด	กรณีที่ไม่สามารถเข้าถึงและใช้งานได้อาจส่งผลกระทบเพียงเล็กน้อยหรืออย่างจำกัด
ระดับกลาง	ข้อมูลที่ถูกกำหนดชั้นความลับเป็นชั้นลับมาก	การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบอย่างร้ายแรง	กรณีที่ไม่สามารถเข้าถึงและใช้งานได้อาจส่งผลกระทบอย่างร้ายแรง
ระดับสูง	ข้อมูลที่ถูกกำหนดชั้นความลับเป็นชั้นลับที่สุด	การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบอย่างร้ายแรงมาก	กรณีที่ไม่สามารถเข้าถึงและใช้งานได้อาจส่งผลกระทบอย่างร้ายแรงมาก

ผลกระทบระดับสูง **สูง**	ข้อกำหนดส่วนที่ ๑ - ทุกข้อ ข้อกำหนดส่วนที่ ๒ - ทุกข้อ	ได้รับการรับรองโดยหน่วยงานให้บริการตรวจรับรอง (Certify Body) ตามวงรอบ ๓ ปี ประกอบด้วยการตรวจรับรองในปีที่ ๑ และการตรวจสำรวจในปีที่ ๒ และ ๓	ได้รับการรับรองโดยหน่วยงานให้บริการตรวจรับรอง (Certify Body) ตามวงรอบ ๓ ปี ประกอบด้วยการตรวจรับรองในปีที่ ๑ และการตรวจสำรวจในปีที่ ๒ และ ๓ และได้รับการรับรองตามมาตรฐาน ISO/IEC 27017 Certification หรือ CSA STAR Level 2/CCM และ ISO/IEC 27018 Certification และ ISO/IEC 27701 Certification เป็นอย่างน้อย

ตัวอย่างข้อมูลหรือระบบ “ระดับสูง” เช่น เอกสารลับที่สุด, ระบบทะเบียนราษฎร์, ข้อมูลส่วนบุคคลอ่อนไหว (ประวัติการรักษา, ข้อมูลชีวภาพ เป็นต้น)