

ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล

เรื่อง กรอบแนวทางการบริหารจัดการคลาวด์ภาครัฐ

โดยที่เทคโนโลยีคลาวด์เป็นโครงสร้างพื้นฐานด้านดิจิทัลสำคัญที่หน่วยงานของรัฐนำมาใช้ในการพัฒนาและบริหารจัดการระบบงานและการให้บริการสาธารณะในรูปแบบดิจิทัล ซึ่งจะช่วยให้การดำเนินงานรวมทั้งการจัดการข้อมูลมีความยืดหยุ่น ปลอดภัย และสามารถเชื่อมโยงข้อมูลระหว่างหน่วยงานได้อย่างมีประสิทธิภาพ และเพื่อให้การนำเทคโนโลยีคลาวด์มาใช้ในภาครัฐเป็นไปอย่างมีประสิทธิภาพและเต็มศักยภาพ ซึ่งจะช่วยยกระดับการบริหารงานและการให้บริการสาธารณะในรูปแบบดิจิทัลให้สามารถตอบสนองความต้องการของประชาชนได้อย่างทั่วถึง และช่วยขับเคลื่อนการเติบโตของเศรษฐกิจดิจิทัลควบคู่กับการธำรงไว้ซึ่งความเป็นเจ้าของอธิปไตยข้อมูลของประเทศอย่างเคร่งครัด

อาศัยอำนาจตามความในมาตรา ๔ (๒) มาตรา ๗ (๓) และ (๔) แห่งพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ ประกอบกับมติคณะกรรมการพัฒนารัฐบาลดิจิทัล ครั้งที่ .../๒๕๖๔ เมื่อวันที่ ... เดือน พ.ศ. ๒๕๖๔ คณะกรรมการพัฒนารัฐบาลดิจิทัลจึงออกประกาศดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง กรอบแนวทางการบริหารจัดการคลาวด์ภาครัฐ”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันที่ ๑ ตุลาคม ๒๕๖๔ เป็นต้นไป เว้นแต่หมวด ๒ ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ในประกาศนี้

“หน่วยงานของรัฐ” หมายความว่า ราชการส่วนกลาง ราชการส่วนภูมิภาค ราชการส่วนท้องถิ่น รัฐวิสาหกิจ องค์การมหาชน สถาบันอุดมศึกษาของรัฐ หน่วยธุรการของศาล องค์การอัยการ องค์การอิสระตามรัฐธรรมนูญ หน่วยงานสังกัดรัฐสภาหรือในกำกับของรัฐสภา และหน่วยงานอิสระของรัฐ

“คณะกรรมการ” หมายความว่า คณะกรรมการพัฒนารัฐบาลดิจิทัล

“สำนักงาน” หมายความว่า สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

“การประมวลผลแบบคลาวด์ (Cloud Computing) หรือคลาวด์ (Cloud)” หมายความว่า รูปแบบการประมวลผลที่สามารถเข้าถึงทรัพยากรที่ใช้ร่วมกันได้อย่างยืดหยุ่น โดยมีการจัดเตรียมทรัพยากร (Self-service Provisioning) และการบริหารจัดการด้วยตนเองตามความต้องการ (On-demand)

“คลาวด์สาธารณะ (Public Cloud)” หมายความว่า บริการคลาวด์ที่เปิดให้บริการแก่ผู้ให้บริการทั่วไปโดยทรัพยากรทั้งหมดอยู่ภายใต้การควบคุมของผู้ให้บริการคลาวด์

“คลาวด์ส่วนตัว (Private Cloud)” หมายความว่า บริการคลาวด์ที่ใช้งานโดยผู้ให้บริการเพียงรายเดียวโดยทรัพยากรทั้งหมดอยู่ภายใต้การควบคุมของผู้ให้บริการรายนั้น

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

“คลาวด์อธิปไตย (Sovereign Cloud)” หมายความว่า บริการคลาวด์ ภายใต้การควบคุมโดยภาครัฐและดูแลโดยบุคลากรที่ได้รับอนุญาต และใช้สำหรับให้บริการกับหน่วยงานของรัฐเท่านั้น

“ข้อมูลที่สามารถเปิดเผยได้ (Official Data)” หมายความว่า ข้อมูลที่สร้าง ประมวลผล ส่งหรือรับของหน่วยงานภาครัฐและหน่วยงานที่เกี่ยวข้อง ซึ่งอาจก่อให้เกิดความเสียหายได้ไม่เกินความเสียหายในระดับต่ำ หากมีการละเมิดความปลอดภัยจะมีการใช้มาตรฐานการควบคุมที่สามารถคุ้มครองข้อมูลให้มีความปลอดภัยจากการโจมตีในรูปแบบต่าง ๆ ซึ่งอาจเพิ่มการรับรองมาตรการควบคุม

“ข้อมูลที่ต้องได้รับความคุ้มครอง (Protected Data)” หมายความว่า ข้อมูลที่มีความอ่อนไหวสูง หากเปิดเผยอาจก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐหรือเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรง ซึ่งส่งผลกระทบต่อความมั่นคงของชาติ และ/หรือความสัมพันธ์ระหว่างประเทศ ความมั่นคง/เสถียรภาพทางการเงิน หรือขัดขวางความสามารถในการสืบสวนคดีอาชญากรรมที่ร้ายแรง หรือองค์กรที่จำเป็นต้องมีมาตรการควบคุมที่เข้มงวด และมีการกำหนดการใช้เครือข่ายที่ปลอดภัยบนโครงสร้างพื้นฐานทางกายภาพที่มีความปลอดภัย และมีการปฏิบัติอย่างเหมาะสม ซึ่งรวมถึงการใช้สถาปัตยกรรมแบบ Zero - Trust การเข้ารหัส และการปฏิบัติตามมาตรฐานความปลอดภัยทั้งในระดับชาติและระดับสากลอย่างเคร่งครัด

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

“แพลตฟอร์มบริหารจัดการคลาวด์” หมายความว่า แพลตฟอร์มกลางสำหรับการบริหารจัดการทรัพยากรคลาวด์ภาครัฐเพื่อกำกับดูแลและติดตามตรวจสอบการใช้ทรัพยากรคลาวด์ของหน่วยงานของรัฐ

“ผู้ให้บริการ” หมายความว่า ผู้ให้บริการคลาวด์หรือตัวแทนของผู้ให้บริการคลาวด์

ข้อ ๔ ให้ประธานกรรมการพัฒนารัฐบาลดิจิทัลรักษาการตามประกาศนี้ และให้มีอำนาจตีความและวินิจฉัยปัญหาอันเกิดจากการปฏิบัติตามประกาศนี้

ในการตีความและการวินิจฉัยปัญหา ประธานกรรมการพัฒนารัฐบาลดิจิทัลอาจตั้งคณะทำงานเพื่อร่วมพิจารณาและดำเนินการให้เป็นไปตามประกาศนี้

หมวด ๑

การบริหารจัดการคลาวด์ภาครัฐ

ข้อ ๕ หน่วยงานของรัฐที่ต้องมีการใช้คลาวด์ ให้ดำเนินการดังต่อไปนี้

(๑) ให้หน่วยงานของรัฐต้องมีการจัดระดับชั้นข้อมูล และจำแนกประเภทข้อมูลตามระดับความเสี่ยง ดังนี้

๑.๑ ให้มีการจัดระดับชั้นข้อมูล โดยแบ่งเป็น ๕ ระดับ ดังนี้

- (ก) ข้อมูลเปิดเผย (Public)
- (ข) ข้อมูลเผยแพร่ภายในองค์กร (Internal)
- (ค) ข้อมูลลับ (Confidential)
- (ง) ข้อมูลลับมาก (Secret)
- (จ) ข้อมูลลับที่สุด (Top Secret)

๑.๒ ให้จำแนกประเภทข้อมูลในแต่ละระดับชั้นข้อมูล ดังนี้

- (ก) ข้อมูลเปิดเผย และข้อมูลเผยแพร่ภายในองค์กร ให้จัดอยู่ในประเภทข้อมูลที่สามารถเปิดเผยได้
- (ข) ข้อมูลลับ และข้อมูลลับมาก ให้จัดอยู่ในประเภทข้อมูลที่ต้องได้รับความคุ้มครอง
- (ค) ข้อมูลลับที่สุด ให้จัดอยู่ในประเภทข้อมูลที่ต้องได้รับความคุ้มครองสูงสุด

โดยรายละเอียดในการจัดระดับชั้นข้อมูลและการจำแนกประเภทข้อมูลให้เป็นไปตามมาตรฐานและหลักเกณฑ์ที่คณะกรรมการประกาศกำหนด"

(๒) ให้หน่วยงานของรัฐพิจารณาเลือกใช้คลาวด์ตามประเภทและรูปแบบที่เหมาะสมกับระบบงานตามภารกิจของหน่วยงานของรัฐ และต้องสอดคล้องกับประเภทข้อมูล ดังนี้

๒.๑ ใช้คลาวด์สาธารณะ สำหรับประเภทข้อมูลที่สามารถเปิดเผยได้

๒.๒ ใช้คลาวด์สาธารณะที่มีการเพิ่มมาตรการคุ้มครองข้อมูลมากกว่าการใช้งานคลาวด์สาธารณะทั่วไปตามข้อ ๒.๑ สำหรับประเภทข้อมูลที่ต้องได้รับความคุ้มครอง

๒.๓ ใช้คลาวด์อธิปไตย สำหรับประเภทข้อมูลที่ต้องได้รับความคุ้มครองสูงสุด เว้นแต่เป็นข้อมูลที่อยู่ในระบบงานที่เกี่ยวกับความมั่นคงของประเทศ ตามนโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ หรือระบบงานที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure (CII)) ซึ่งคณะกรรมการพัฒนารัฐบาลดิจิทัลจะกำหนดหลักเกณฑ์การใช้คลาวด์สำหรับข้อมูลนี้เป็นการเฉพาะ

ทั้งนี้ รายละเอียดแนวทางการใช้คลาวด์ของหน่วยงานรัฐให้เป็นไปตามมาตรฐานและหลักเกณฑ์ที่คณะกรรมการประกาศกำหนด โดยหน่วยงานของรัฐต้องเลือกใช้บริการคลาวด์จากผู้ให้บริการที่ได้รับการประกาศรายชื่อเป็นผู้ผ่านการตรวจประเมินและรับรองความสอดคล้องการบริหารจัดการคลาวด์แล้วเท่านั้น เว้นแต่กรณีผู้ให้บริการคลาวด์อธิปไตยให้เป็นไปตามที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมกำหนด

(๓) กรณีที่หน่วยงานของรัฐมีการทบทวนและปรับปรุงระดับชั้นข้อมูล (Re-classification) หรือ ยกเลิกระดับชั้นข้อมูล (De-classification) ในภายหลัง ให้หน่วยงานของรัฐดำเนินการทบทวนและปรับเปลี่ยน รูปแบบการใช้บริการคลาวด์ให้สอดคล้องกับระดับชั้นข้อมูลและประเภทของข้อมูลที่ได้มีการปรับปรุงหรือ ยกเลิกดังกล่าว

(๔) ให้หน่วยงานของรัฐพิจารณาเลือกใช้คลาวด์จากผู้ให้บริการคลาวด์ที่มีศูนย์ข้อมูลและมีการ จัดเก็บข้อมูลอยู่ในราชอาณาจักรไทยเป็นหลัก เว้นแต่มีเหตุจำเป็นต้องใช้คลาวด์ที่จัดเก็บข้อมูลนอก ราชอาณาจักร ทั้งนี้ ให้เป็นดุลยพินิจของหัวหน้าหน่วยงานของรัฐ โดยในกรณีที่ต้องใช้คลาวด์ที่จัดเก็บข้อมูล นอกราชอาณาจักร ต้องมีการกำกับดูแลให้สิทธิความเป็นเจ้าของ และอำนาจการควบคุม และการบริหาร จัดการข้อมูล ยังคงอยู่ภายใต้บังคับของกฎหมายไทยอย่างเคร่งครัด

(๕) กรณีหน่วยงานของรัฐไม่สามารถใช้คลาวด์ตามที่ประกาศนี้กำหนด สามารถยื่นขออนุมัติพร้อม หลักฐานและเหตุผลความจำเป็นต่อคณะกรรมการหรือคณะอนุกรรมการที่ได้รับมอบหมาย เพื่อยกเว้น การปฏิบัติตามประกาศนี้ เป็นรายกรณีได้

ข้อ ๖ ให้หน่วยงานของรัฐพิจารณาใช้คลาวด์ โดย

(๑) กรณีหน่วยงานของรัฐมีระบบงานที่มีการใช้ระบบเทคโนโลยีสารสนเทศ ให้จัดลำดับความสำคัญ และความเหมาะสมของระบบงาน เพื่อดำเนินการโอนย้ายระบบงานนั้นไปใช้คลาวด์

(๒) กรณีหน่วยงานของรัฐต้องการจัดหาหรือปรับปรุงระบบงานโดยมีการใช้ระบบเทคโนโลยี สารสนเทศ ให้หน่วยงานของรัฐดำเนินการดังนี้

(ก) ออกแบบระบบงานให้มีความสอดคล้องและรองรับกับการใช้คลาวด์ตั้งแต่ต้น (Cloud Native)

(ข) ออกแบบและพัฒนาระบบงานให้รองรับการใช้งานที่สามารถปรับปริมาณการใช้ทรัพยากรได้ ง่ายและสะดวก รวมทั้งรองรับการเชื่อมต่อกับระบบงานอย่างต่อเนื่อง

(ค) ออกแบบระบบงานให้ใช้ระบบและองค์ประกอบมาตรฐานของคลาวด์ โดยให้มีการใช้ ผลิตภัณฑ์หรือบริการตามมาตรฐานของผู้ให้บริการให้มากที่สุด รวมทั้งหลีกเลี่ยงการ ออกแบบและพัฒนาความต้องการแบบเฉพาะเจาะจง เพื่อให้ระบบงานสามารถได้รับการ ปรับปรุงไปตามเทคโนโลยีที่เปลี่ยนแปลงได้ทันที

(ง) การปรับแต่งฟังก์ชันหรือบริการที่แตกต่างไปจากมาตรฐานของระบบการให้บริการคลาวด์ ของผู้ให้บริการควรดำเนินการให้น้อยที่สุด โดยให้ใช้การปรับแต่งฟังก์ชันหรือบริการด้วย วิธีการปรับแต่งการตั้งค่าระบบ และไม่ควรมีการดัดแปลงระบบฟังก์ชันหรือบริการเป็นแบบ เฉพาะเจาะจงที่ไม่เป็นไปตามมาตรฐานของระบบการให้บริการคลาวด์ ทั้งนี้ หากมาตรฐาน ของระบบการให้บริการคลาวด์ไม่สามารถนำมาใช้กับระบบงานได้ ให้หน่วยงานของรัฐ พิจารณาเปลี่ยนแปลงระบบงานด้วยการตั้งค่าระบบแทนการดัดแปลงระบบการให้บริการ คลาวด์ที่มีมาตรฐานอยู่แล้ว

(๓) ระบบงานของหน่วยงานของรัฐต้องมีการติดตั้งมาตรการรักษาความมั่นคงปลอดภัยให้เหมาะสม กับประเภทข้อมูลและกระบวนการทำงาน รวมทั้งมีมาตรการควบคุมดูแลและการตรวจสอบมาตรการรักษา

ความมั่นคงปลอดภัยอย่างสม่ำเสมอ โดยให้มีการทดสอบการโจมตีระบบเป็นระยะเพื่อลดความเสี่ยงต่อระบบงาน

(๔) ให้งานของรัฐบาลมีการติดตามและตรวจสอบการใช้คลาวด์อย่างสม่ำเสมอ โดยอย่างน้อยจะต้องดำเนินการในเรื่องดังต่อไปนี้

(ก) ติดตามและตรวจสอบปริมาณการใช้งานจริง เพื่อให้สามารถประเมินและปรับปริมาณการใช้งานบริการคลาวด์ให้เหมาะสม เพียงพอ และสามารถรองรับการใช้งานระบบงานอย่างต่อเนื่อง

(ข) ติดตาม ตรวจสอบ และตรวจประเมินการปฏิบัติงานของผู้ให้บริการให้เป็นไปตามมาตรฐานและระดับการให้บริการตามที่ตกลง เพื่อให้มีการติดตามปริมาณการใช้คลาวด์และปรับขนาดทรัพยากรคลาวด์ให้มีความเหมาะสม พร้อมกับตรวจสอบความสมบูรณ์ของระบบซึ่งจะต้องมีการรักษาความมั่นคงปลอดภัยอย่างเคร่งครัด

(๕) หน่วยงานของรัฐบาลต้องมีการปฏิบัติตามมาตรฐาน หลักเกณฑ์ วิธีการและเงื่อนไขที่เกี่ยวกับการใช้คลาวด์ตามที่คณะกรรมการหรือคณะอนุกรรมการที่ได้รับมอบหมายประกาศกำหนด

หมวด ๒

มาตรฐานการบริหารจัดการคลาวด์ภาครัฐ

ข้อ ๗ ให้สำนักงานรวบรวมและจัดทำมาตรฐาน รวมทั้งหลักเกณฑ์ วิธีการและเงื่อนไขที่เกี่ยวกับการใช้บริการคลาวด์ และการบริหารจัดการคลาวด์ของผู้ให้บริการ ตลอดจนแนวปฏิบัติและคู่มือในการดำเนินงานเกี่ยวกับการบริหารจัดการคลาวด์ภาครัฐสำหรับหน่วยงานของรัฐบาล เพื่อเสนอคณะกรรมการหรือคณะอนุกรรมการที่ได้รับมอบหมายพิจารณาเห็นชอบและประกาศใช้บังคับต่อไป

ข้อ ๘ เพื่อประโยชน์ในการใช้คลาวด์ของหน่วยงานของรัฐบาล ให้สำนักงานทำหน้าที่ตรวจประเมินและรับรองความสอดคล้องของการบริหารจัดการคลาวด์ของผู้ให้บริการ ตลอดจนรวบรวมและประกาศรายชื่อผู้ให้บริการที่ผ่านการตรวจประเมินและรับรองดังกล่าวให้หน่วยงานของรัฐบาลทราบ

ในการตรวจประเมินและรับรองความสอดคล้องของการบริหารจัดการคลาวด์ตามวรรคหนึ่ง สำนักงานอาจเข้าไปตรวจประเมินมาตรฐานของระบบการให้บริการคลาวด์ของผู้ให้บริการได้ทั้งก่อนประกาศรายชื่อ หรือหลังจากได้รับการประกาศรายชื่อแล้ว

การดำเนินการตามวรรคหนึ่งและวรรคสอง ให้เป็นไปตามหลักเกณฑ์ วิธีการ และเงื่อนไขที่คณะกรรมการหรือคณะอนุกรรมการที่ได้รับมอบหมายกำหนด โดยสำนักงานอาจมีการเรียกเก็บค่าบริการในการดำเนินการได้

ข้อ ๙ ให้สำนักงานรายงานผลการดำเนินงานการตรวจประเมินและรับรองความสอดคล้องของการบริหารจัดการคลาวด์ของผู้ให้บริการให้คณะกรรมการทราบอย่างน้อยปีละหนึ่งครั้งหรือตามที่คณะกรรมการเห็นสมควร

หมวด ๓

การจัดหาบริการคลาวด์

ข้อ ๑๐ ในการจัดหาบริการคลาวด์ภาครัฐ ให้ใช้รูปแบบการจัดหาแบบรวมศูนย์ โดยให้ดำเนินการผ่านระบบบริการคลาวด์กลางภาครัฐ (Government Data Center and Cloud service : GDCC) เป็นลำดับแรก

ข้อ ๑๑ หน่วยงานของรัฐต้องจัดหาบริการคลาวด์จากผู้ให้บริการที่ได้รับการประกาศรายชื่อเป็นผู้ผ่านการตรวจประเมินและรับรองความสอดคล้องการบริหารจัดการคลาวด์ตามข้อ ๘ เว้นแต่กรณีต้องใช้คลาวด์อิมปีไตย ให้จัดหาบริการคลาวด์จากผู้ให้บริการตามที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมกำหนด

ข้อ ๑๒ ให้กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมจัดทำและดำเนินการแพลตฟอร์มบริหารจัดการคลาวด์ เพื่อเป็นแพลตฟอร์มกลางในการกำกับดูแลและติดตามการใช้คลาวด์ของหน่วยงานของรัฐ และให้หน่วยงานของรัฐที่ใช้คลาวด์ต้องมีการเชื่อมโยงและนำส่งข้อมูลการใช้บริการคลาวด์ตามที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมกำหนด

หมวด ๔

บทเฉพาะกาล

ข้อ ๑๓ ในระยะเริ่มแรก ระหว่างที่ยังไม่มีการประกาศบังคับใช้มาตรฐานการจัดระดับชั้นข้อมูลและการจำแนกประเภทข้อมูลสำหรับใช้บริการคลาวด์ ตามข้อ ๕ (๑) ให้หน่วยงานของรัฐใช้แนวทางการจัดระดับชั้นและการแบ่งปันข้อมูลภาครัฐ ตามมาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล ว่าด้วยหลักเกณฑ์การจัดระดับชั้นและการแบ่งปันข้อมูลภาครัฐ (มสพร. ๘-๒๕๖๕) ไปพลางก่อน

ประกาศ ณ วันที่ พ.ศ. ๒๕๖๙

รองนายกรัฐมนตรี

ประธานกรรมการพัฒนารัฐบาลดิจิทัล