(ร่าง)

ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล
เรื่อง หลักเกณฑ์ วิธีการ และเงื่อนไขการตรวจประเมินและรับรองผู้ให้บริการคลาวด์
พ.ศ. ....

โดยที่เป็นการสมควรกำหนดให้มีหลักเกณฑ์ วิธีการ และเงื่อนไขการตรวจประเมินและรับรองความสอดคล้องการบริหารจัดการคลาวด์ของผู้ให้บริการคลาวด์ตามมาตรฐานที่คณะกรรมการพัฒนารัฐบาลดิจิทัลกำหนด

อาศัยอำนาจตามความในมาตรา ๔ (๒) มาตรา ๗ (๓) และ (๙) แห่งพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ ประกอบกับข้อ ๖ ของประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง กรอบแนวทางการบริหารจัดการคลาวด์ภาครัฐตามนโยบายการใช้คลาวด์เป็นหลัก พ.ศ. .... และมติที่ประชุมคณะกรรมการพัฒนารัฐบาลดิจิทัล ในคราวการประชุมครั้งที่ .../๒๕๖๘ เมื่อวันที่ ... เดือน ..... พ.ศ. ๒๕๖๘ คณะกรรมการพัฒนารัฐบาลดิจิทัลจึงมีมติให้ออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่องหลักเกณฑ์ วิธีการ และเงื่อนไขการตรวจประเมินและรับรองผู้ให้บริการคลาวด์ พ.ศ. ....”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ให้หลักเกณฑ์ วิธีการ และเงื่อนไขการตรวจประเมินและรับรองผู้ให้บริการคลาวด์ เป็นไปตามรายละเอียดแนบท้ายประกาศนี้

ประกาศ ณ วันที่ ๒๕๖๘

(XXXXXXXXXXXXXXX)
รองนายกรัฐมนตรี
ประธานกรรมการพัฒนารัฐบาลดิจิทัล

แนบท้ายประกาศ

หลักเกณฑ์ วิธีการ และ เงื่อนไขการตรวจประเมินและรับรองผู้ให้บริการคลาวด์

สารบัญ

คำนำ

ในยุคดิจิทัลที่เทคโนโลยีคลาวด์มีบทบาทสำคัญต่อการบริหารจัดการข้อมูลและการให้บริการภาครัฐ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.) ได้รับมอบหมายให้กำหนดหลักเกณฑ์การขึ้นทะเบียนผู้ให้บริการคลาวด์ ตามแนวทางของนโยบายการใช้คลาวด์เป็นหลัก (Cloud First Policy) ซึ่งเป็นนโยบายที่รัฐบาลไทยให้ความสำคัญ เพื่อส่งเสริมให้หน่วยงานภาครัฐใช้บริการคลาวด์เป็นหลักในการดำเนินงาน เพิ่มประสิทธิภาพ ลดต้นทุน และเสริมสร้างความมั่นคงปลอดภัยของข้อมูล

โดยอาศัยอำนาจตามพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ สพร. ได้จัดทำหลักเกณฑ์และแนวทางการตรวจประเมินและรับรองคุณสมบัติผู้ให้บริการคลาวด์ เพื่อให้มั่นใจว่าผู้ให้บริการคลาวด์สามารถรองรับการดำเนินงานของหน่วยงานภาครัฐได้อย่างมีประสิทธิภาพ ปลอดภัย และเป็นไปตามมาตรฐานที่กำหนด

๑.ขอบข่าย

เอกสารนี้กำหนดหลักเกณฑ์ วิธีการ และเงื่อนไขการตรวจประเมินและรับรองคุณสมบัติผู้ให้บริการคลาวด์ ในการดำเนินการตรวจประเมิน ความสอดคล้องของกระบวนการหรือระบบให้บริการตามมาตรฐานที่ สพร. กำหนด ซึ่งจะครอบคลุม รายละเอียดการตรวจประเมิน การรายงานผลการตรวจ และการตรวจประเมินเพื่อต่ออายุ

๒.บทนิยาม

ความหมายของคำที่ใช้ในมาตรฐานนี้ มีดังต่อไปนี้

สำนักงาน หมายความว่า สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

ผู้ยื่นคำขอ (Applicant) หมายความว่า บุคคลธรรมดาหรือนิติบุคคลที่ประสงค์ขอให้มีการตรวจประเมินเพื่อรับรองเป็นผู้ให้บริการ

ผู้รับการตรวจประเมิน (Auditee) หมายความว่า ผู้ยื่นคำขอผู้ให้บริการที่เข้ารับการตรวจประเมิน

ผู้ได้รับการพิจารณารับรอง หมายความว่า ผู้ยื่นคำขอที่ผ่านการตรวจประเมิน และได้รับการพิจารณารับรองจากสำนักงาน

ผู้ตรวจประเมิน (Auditor) หมายความว่า เจ้าหน้าที่ของสำนักงานที่มีคุณสมบัติเป็นผู้เชี่ยวชาญหรือมีประสบการณ์ที่เกี่ยวข้องกับการตรวจประเมินความสอดคล้องของกระบวนการหรือระบบให้บริการตามมาตรฐานที่ดำเนินการตรวจประเมินอย่างเป็นระบบ เป็นอิสระ เพื่อให้ได้มาซึ่งหลักฐานการตรวจประเมิน และผลการตรวจประเมินอย่างเป็นรูปธรรม สำหรับการตัดสินระดับการบรรลุผลตามความสอดคล้องของเกณฑ์การตรวจประเมิน

ผู้เชี่ยวชาญด้านเทคนิค (Technical Expert) หมายความว่า บุคคลผู้ให้ความรู้หรือ ความเชี่ยวชาญเฉพาะด้านแก่คณะผู้ตรวจประเมิน แต่ไม่ได้ปฏิบัติหน้าที่ในฐานะผู้ตรวจประเมิน

คณะผู้ตรวจประเมิน หมายความว่า ผู้ตรวจประเมินซึ่งประกอบด้วยหัวหน้าผู้ตรวจประเมิน และผู้ตรวจประเมินที่เป็นสมาชิกในคณะนั้น ๆ ซึ่งได้รับมอบหมายให้รับผิดชอบตรวจประเมินกระบวนการหรือระบบให้บริการตามมาตรฐานที่สำนักงานกำหนด นอกจากนี้ อาจมีผู้เชี่ยวชาญด้านเทคนิคร่วมสนับสนุนการตรวจประเมินด้วยก็ได้ หรือจะมอบหมายหัวหน้าผู้ตรวจประเมินคนใดคนหนึ่งให้รับผิดชอบตรวจประเมิน กระบวนการหรือระบบให้บริการตามมาตรฐานที่สำนักงานกำหนดก็ได้

คณะกรรมการพิจารณา หมายความว่า คณะบุคคลที่สำนักงานแต่งตั้งขึ้น เพื่อทำหน้าที่พิจารณาผลการตรวจประเมินคุณสมบัติของผู้ให้บริการคลาวด์ เพื่อประกาศรายชื่อผู้ผ่านการตรวจประเมินและรับรองความสอดคล้องในการบริหารจัดการคลาวด์ตามมาตรฐานและหลักเกณฑ์ที่กำหนด

คณะกรรมการ หมายความว่า คณะกรรมการพัฒนารัฐบาลดิจิทัล ซึ่งมีหน้าที่รับทราบผลการดำเนินงานด้านการตรวจประเมินและรับรองความสอดคล้องในการบริหารจัดการคลาวด์ของผู้ให้บริการ อย่างน้อยปีละหนึ่งครั้ง หรือในช่วงเวลาที่คณะกรรมการเห็นสมควร

การตรวจประเมินคุณสมบัติผู้ให้บริการคลาวด์ หมายความว่า การตรวจประเมินตามรูปแบบตามมาตรฐานที่สำนักงานกำหนด อาทิ การตรวจประเมินความสอดคล้องของกระบวนการหรือระบบ ซึ่งครอบคลุมการตรวจประเมินเมื่อยื่นขอคำขอตรวจประเมินครั้งแรก หรือขอรับการตรวจประเมินใหม่กรณีไม่ได้ขอต่ออายุหรือไม่สามารถต่ออายุได้ภายในเวลาที่กำหนด โดยมีวัตถุประสงค์เพื่อประเมินความสอดคล้องตามเกณฑ์การตรวจประเมิน

การตรวจประเมินเพื่อต่ออายุ (Re-assessment Audit) หมายความว่า การตรวจประเมินเพื่อต่ออายุสถานะการรับรอง โดยมีวัตถุประสงค์เพื่อการทบทวนความมั่นคงปลอดภัยของกระบวนการหรือระบบของผู้ได้รับการรับรองอีกครั้งว่าผู้ได้รับการรับรองมีการนำเกณฑ์การตรวจประเมินไปปฏิบัติ และยังมีประสิทธิผลอยู่ ซึ่งการตรวจประเมินเพื่อต่ออายุดังกล่าวจะดำเนินการก่อนสถานะการรับรองสิ้นอายุ

ความไม่สอดคล้อง (Nonconformity) หมายความว่า ความล้มเหลวที่ไม่บรรลุตามเกณฑ์การตรวจประเมินผู้ให้บริการ

เกณฑ์การตรวจประเมิน (Audit Criteria) หมายความว่า มาตรฐาน กฎหมาย ประกาศ หรือชุดของนโยบาย ขั้นตอนการดำเนินการ หรือข้อกำหนดที่ใช้อ้างอิง หลักเกณฑ์ วิธีการ และเงื่อนไข และระเบียบอื่น ๆ เพื่อนำไปเปรียบเทียบกับหลักฐานการตรวจประเมินเพื่อพิจารณาคุณสมบัติผู้ให้บริการคลาวด์

หลักฐานการตรวจประเมิน (Audit Evidence) หมายความว่า บันทึกข้อมูล ข้อเท็จจริงหรือข้อมูลอื่นที่เกี่ยวข้องกับเกณฑ์การตรวจประเมินและสามารถทวนสอบได้

สิ่งที่พบจากการตรวจประเมิน (Audit Findings) หมายความว่า ผลจากการประเมินหลักฐาน การตรวจประเมินที่เก็บรวบรวมได้ แล้วนำมาเปรียบเทียบกับเกณฑ์การตรวจประเมิน เพื่อประเมินบ่งชี้ถึงระดับความสอดคล้อง หรือความไม่สอดคล้อง

แบบการเปิดเผยข้อมูลของผู้ให้บริการคลาวด์ หมายความว่า แบบคำขอรับการตรวจประเมินคุณสมบัติผู้ให้บริการคลาวด์กับสำนักงาน

ผู้ตรวจสอบอิสระ หมายความว่า ผู้ตรวจสอบภายนอกที่ได้รับประกาศนียบัตรตามที่สำนักงานกำหนด

ผู้ตรวจสอบภายในองค์กร หมายความว่า ผู้ตรวจสอบงานด้านเทคโนโลยีสารสนเทศของบริษัท ที่เป็นอิสระจากหน่วยงานที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศที่ได้รับประกาศนียบัตรตามที่สำนักงานกำหนด

๓. หลักเกณฑ์ วิธีการ และเงื่อนไข

๓.๑ การตรวจประเมินคุณสมบัติผู้ให้บริการคลาวด์

๓.๑.๑ ทั่วไป

(๑) การตรวจประเมินจะดำเนินการสำหรับผู้ยื่นคำขอ ตามที่กำหนดไว้ในประกาศสำนักงานเรื่อง หลักเกณฑ์ วิธีการ และเงื่อนไขการประเมิน ทั้งนี้ สำนักงานจัดเก็บค่าบริการในการยื่นคำขอรับการตรวจประเมินและรับรองความสอดคล้องเป็นไปตามระเบียบการดำเนินการที่เกี่ยวข้อง ที่สำนักงานกำหนด เพื่อเป็นค่าใช้จ่ายในการดำเนินการตรวจประเมินและบริหารจัดการระบบที่เกี่ยวข้อง

(๒) หน่วยงานที่รับผิดชอบจะดำเนินการตรวจสอบความครบถ้วนของเอกสาร รวมถึงพิจารณาคุณสมบัติของผู้ยื่นคำขอภายในระยะเวลาไม่เกิน ๓๐ วันทำการ นับแต่วันที่ได้รับเอกสารประกอบการพิจารณาครบถ้วน ทั้งนี้ ระยะเวลาในการตรวจสอบอาจเปลี่ยนแปลงได้ตามความเหมาะสม ขึ้นอยู่กับปริมาณคำขอและความซับซ้อนของแต่ละกรณี

(๓) ผู้รับการตรวจประเมินต้องยินยอมให้ผู้แทนจากสำนักงาน หรือบุคคลอื่นใดที่สำนักงานแจ้งรายชื่อเข้าร่วมสังเกตการณ์การตรวจประเมินของคณะผู้ตรวจประเมินของสำนักงาน ภายใต้ขอบข่ายที่ขอรับรองได้ตลอดระยะเวลาการตรวจประเมินเมื่อสำนักงานร้องขอ

(๔) ผู้รับการตรวจประเมินต้องให้ความร่วมมือแก่สำนักงานในการตรวจประเมินทุกครั้ง รวมทั้งต้องจัดเตรียมเอกสารและบันทึกที่เกี่ยวข้องกับการดำเนินงานเพื่อการตรวจสอบ และให้การอำนวยความสะดวกในการเข้าถึงอุปกรณ์และสถานที่ พื้นที่ บุคลากร และผู้รับจ้างของผู้รับการตรวจประเมิน ตลอดจนการสืบสวนข้อร้องเรียน

๓.๑.๒ การกำหนดคณะผู้ตรวจประเมิน

(๑) คณะผู้ตรวจประเมินที่ดำเนินการตรวจประเมินในแต่ละครั้งอย่างเป็นทางการต้องประกอบด้วย หัวหน้าผู้ตรวจประเมิน และผู้ตรวจประเมิน ตามที่ได้รับมอบหมายจากสำนักงาน ทั้งนี้ คณะผู้ตรวจประเมินให้มีจำนวนตามความเหมาะสม และอาจมีผู้เชี่ยวชาญด้านเทคนิคร่วมในคณะผู้ตรวจประเมินด้วยก็ได้ ซึ่งต้องกำหนดอำนาจหน้าที่ให้ชัดเจน และแจ้งให้ผู้ยื่นคำขอทราบ

(๒) คณะผู้ตรวจประเมินต้องมีคุณสมบัติและไม่มีลักษณะต้องห้าม ดังนี้

(๒.๑) เป็นบุคคลที่มีคุณสมบัติตามที่สำนักงานกำหนด

(๒.๒) มีความรู้เกี่ยวกับเกณฑ์การตรวจประเมิน และเกณฑ์การรับรอง

(๒.๓) มีความรู้ความเข้าใจในวิธีการตรวจประเมิน และในเอกสารการตรวจประเมิน

(๒.๔) มีความรู้ความสามารถทางเทคนิคตามเกณฑ์การตรวจประเมินที่ขอรับการรับรอง

(๒.๕) มีความสามารถในการสื่อความ

(๒.๖) ปราศจากผลประโยชน์ที่อาจทำให้สมาชิกในกลุ่มผู้ตรวจประเมิน ปฏิบัติตนอย่างไม่เป็นกลาง ไม่น่าเชื่อถือ หรืออย่างไม่เสมอภาค รวมทั้ง

(๒.๖.๑) ผู้ตรวจประเมินต้องไม่เคยให้คำปรึกษา หรือเป็นวิทยากรภายใน (In-house Training) หรือทำหน้าที่เป็นที่ปรึกษาให้แก่ผู้ยื่นคำขอภายในระยะเวลา ๒ ปี ที่ผ่านมา ซึ่งอาจมีผลต่อกระบวนการตรวจประเมินและการตัดสินให้การรับรอง

(๒.๖.๑) ผู้ตรวจประเมินต้องไม่เป็นผู้ร่วมลงทุน ผู้ถือหุ้น หรือหุ้นส่วนในหน่วยงานของผู้ยื่นคำขอ

(๒.๖.๓) ผู้ตรวจประเมินต้องเป็นอิสระไม่ถูกกดดันจากผู้ขอรับการตรวจประเมิน และผู้ตรวจประเมินต้องไม่มีแรงกดดันหรือมีอำนาจเหนือผู้ขอรับการตรวจประเมิน เพื่อให้เกิดความโปร่งใส และเป็นกลาง

(๒.๖.๔) ผู้ตรวจประเมินต้องไม่เป็นผู้ที่เข้าข่ายอย่างใดอย่างหนึ่ง ได้แก่ ผู้จัดหา ผู้ออกแบบผลิตภัณฑ์ ผู้ให้บริการ ผู้พัฒนาบริการ ผู้ประกอบการ หรือ ผู้พัฒนากระบวนการหรือระบบ ทั้งในส่วนของตนเองและนายจ้าง ใน ระยะเวลา ๒ ปีที่ผ่านมา

๓.๑.๓ การเตรียมการตรวจประเมิน คณะผู้ตรวจประเมินดำเนินการศึกษาข้อมูลของผู้รับการตรวจประเมิน เพื่อพิจารณาความพร้อม ทางด้านเอกสาร ความรู้ความเข้าใจในข้อกำหนด และการนำไปปฏิบัติ รวมถึงการนำข้อมูลที่ได้รับไปวางแผน กิจกรรม จัดทำแผนการตรวจประเมิน รวมทั้งจัดเตรียมแบบฟอร์มต่างๆ ที่ใช้ในการตรวจประเมิน

๓.๑.๔ ขั้นตอนการตรวจประเมิน การตรวจประเมินเพื่อการรับรองจะตรวจประเมินเอกสาร การปฏิบัติตามกระบวนการหรือระบบ ให้บริการว่ามีความสอดคล้องตามมาตรฐานที่สำนักงานกำหนด โดยรายละเอียดเกี่ยวกับหลักเกณฑ์ วิธีการ และเงื่อนไขในการรับรองคุณสมบัติเบื้องต้นของผู้ให้บริการคลาวด์สำหรับภาครัฐปรากฏอยู่ใน **ภาคผนวก ก** และหลักเกณฑ์การพิจารณาการใช้บริการคลาวด์ที่เก็บข้อมูลนอกราชอาณาจักรปรากฏอยู่ใน **ภาคผนวก ข** ของเอกสารฉบับนี้

ขั้นตอนการตรวจประเมินประกอบด้วยขั้นตอนต่างๆ ดังนี้

(๑) การดำเนินการตรวจประเมิน

- การดำเนินการตรวจประเมิน ประกอบด้วย การตรวจเอกสาร การสัมภาษณ์ และ บันทึกที่เกี่ยวข้อง และการสังเกตการณ์ กิจกรรม และสภาวะของพื้นที่ที่ตรวจ ให้บันทึก สิ่งที่อาจเป็นเหตุนำไปสู่ความไม่เป็นไปตามข้อกำหนด การตรวจประเมินอาจตรวจประเมินรายละเอียดที่ไม่ได้เขียนไว้ในรายการตรวจประเมินก็ได้ ข้อมูลที่ได้จากการสัมภาษณ์จะต้องยืนยันจากแหล่งข้อมูลอิสระอื่น ๆ เช่น การสังเกต เอกสารและการบันทึก เป็นต้น

- ในกรณีที่พบความไม่สอดคล้องสำคัญจำนวนมากที่แสดงให้เห็นว่าผู้รับการตรวจประเมินยังมิได้ดำเนินการตามเกณฑ์ที่ขอรับการรับรองอย่างมีประสิทธิผลเพียงพอ และผู้รับการ

ตรวจประเมินมีความประสงค์ที่จะขอยุติการตรวจประเมิน เพื่อให้มีการตรวจประเมินทั้งกระบวนการหรือระบบใหม่ทั้งหมด

- บันทึกสิ่งที่พบจากการตรวจประเมิน โดยการตรวจประเมินทั้งหมดต้องบันทึกไว้ และหลังจากเสร็จสิ้นการตรวจประเมิน คณะผู้ตรวจประเมินต้องประชุมร่วมกัน เพื่อสรุปผลการตรวจประเมินว่าสิ่งที่ตรวจพบรายการใดถือเป็นความไม่สอดคล้อง จากนั้นสรุปประเด็นความไม่สอดคล้อง (ถ้ามี) โดยต้องมีหลักฐาน สนับสนุนที่เป็นรูปธรรม และให้อ้างถึงข้อกำหนดตามเกณฑ์ที่สำนักงานกำหนดให้ชัดเจน

(๒) การสรุปผลการตรวจประเมิน (Audit Conclusion)

หลังจากการตรวจประเมินแล้วเสร็จ คณะผู้ตรวจประเมินดำเนินการสรุปผลการตรวจประเมิน หากพบว่ามีบางประเด็นที่อาจยังไม่สอดคล้องกับหลักเกณฑ์ที่กำหนดไว้ เพื่อให้การพิจารณาเป็นไปอย่างถูกต้องและเป็นธรรม ทางคณะผู้ตรวจประเมินจะหารือกับผู้รับการตรวจประเมินในประเด็นดังกล่าว เพื่อทำความเข้าใจผลของการตรวจประเมินให้ถูกต้องตรงกันก่อนนำเสนอผลต่อคณะกรรมการพิจารณา

๓.๑.๕ การรายงานผลการตรวจประเมิน (Audit Report)

ภายหลังจากที่คณะผู้ตรวจประเมินได้ดำเนินการตรวจประเมินและสรุปผลการตรวจประเมินแล้วเสร็จ คณะผู้ตรวจประเมินจะจัดทำรายงานสรุปผลการตรวจประเมิน เพื่อเสนอให้คณะกรรมการพิจารณาทบทวนและกลั่นกรองรายงานดังกล่าว รวมถึงพิจารณารายชื่อผู้ให้บริการคลาวด์ที่ผ่านการตรวจประเมินและได้รับการรับรองความสอดคล้องตามมาตรฐานและหลักเกณฑ์ที่กำหนด (Shortlist)

ทั้งนี้ ผลการตรวจประเมินดังกล่าวต้องเสนอให้คณะกรรมการรับทราบอย่างน้อยปีละหนึ่งครั้ง หรือในช่วงเวลาที่คณะกรรมการเห็นสมควร เพื่อประกอบการกำกับ ติดตาม และส่งเสริมการดำเนินงานด้านการบริหารจัดการคลาวด์ของผู้ให้บริการให้เป็นไปตามแนวทางการพัฒนารัฐบาลดิจิทัล

๓.๒ แจ้งผลการพิจารณา

ภายหลังได้รับความเห็นชอบจากคณะกรรมการพิจารณา สำนักงานจะดำเนินการแจ้งผลการพิจารณา (ผ่าน/ไม่ผ่าน) ให้ผู้รับการตรวจประเมินรับทราบทางไปรษณีย์อิเล็กทรอนิกส์ของสำนักงาน และกรณีผู้รับการตรวจประเมินผ่านการประเมินสำนักงานจะประกาศรายชื่อผู้ให้บริการคลาวด์ที่ผ่านการพิจารณา (Shortlist) บนเว็บไซต์ของสำนักงานภายใน ๑๕ วันทำการนับจากวันที่มีมติอนุมัติ

๓.๓ การตรวจประเมินเพื่อต่ออายุ (Re-assessment Audit)

๓.๓.๑ เมื่อผู้ได้รับการรับรองเป็นผู้ให้บริการตามระยะเวลาที่สำนักงานกำหนด สำนักงานจะตรวจประเมินกระบวนการหรือระบบทั้งหมด เพื่อประกาศคงสถานะการรับรองผู้ให้บริการ โดยผู้ได้รับการรับรองต้อง

ยื่นคำขอต่ออายุสถานะการรับรองก่อนหมดอายุการรับรองไม่น้อยกว่า ๑๘๐ วัน ซึ่งสำนักงานจะตรวจประเมินเพื่อต่ออายุการรับรองให้แล้วเสร็จก่อนวันสิ้นอายุ ทั้งนี้หากผู้ได้รับการรับรองได้ยื่นคำขอต่ออายุแล้ว และอยู่ระหว่างกระบวนการตรวจประเมิน ให้สามารถดำเนินกิจการไปพลางก่อนได้ จนกว่าจะได้รับคำสั่งแจ้งไม่อนุญาตให้ต่ออายุการรับรองจากสำนักงาน โดยขั้นตอนต่าง ๆ จะเป็นไปตามขั้นตอนการตรวจประเมินเพื่อการรับรองรายละเอียดตามที่กำหนดไว้ในข้อ ๓.๑

๓.๓.๒ การกำหนดวันที่มีผลให้การรับรอง สำนักงานจะคงสถานะการรับรองผู้ให้บริการ โดยกำหนดวันที่มีผลให้การรับรองต่อเนื่องจากวันสิ้นอายุการรับรองผู้ให้บริการ เฉพาะกรณีที่ผู้ได้รับการรับรองได้รับการตรวจประเมินเพื่อต่ออายุก่อนสถานะการรับรองสิ้นอายุ รวมถึงผู้ได้รับการรับรองได้จัดการความไม่สอดคล้องตามที่กำหนดไว้

๓.๓.๓ กรณีที่ผู้ได้รับการรับรองไม่ยื่นคำขอต่ออายุสถานะการรับรองก่อนล่วงหน้าตามระยะเวลาที่กำหนดไว้ใน ข้อ ๓.๓.๑ ให้ถือว่าผู้ได้รับการขึ้นทะเบียนไม่ประสงค์จะขอต่ออายุการรับรอง โดยสถานะการรับรองเดิมให้มีผลใช้ได้จนถึงวันสิ้นอายุการรับรอง

๓.๓.๔ หากผู้ได้รับการรับรองได้รับผลกระทบจากสถานการณ์หรือเหตุการณ์ที่ไม่ปกติเป็นเหตุให้สำนักงานไม่สามารถเข้าตรวจประเมินเพื่อต่ออายุได้ให้ผู้ได้การรับรองมีหนังสือแจ้งเหตุผลความจำเป็นในการขอเลื่อนการตรวจประเมินเพื่อต่ออายุต่อสำนักงาน โดยสำนักงานจะพิจารณาเหตุผลความจำเป็น รวมทั้งประเมินความเสี่ยงของการรับรองต่อเนื่อง เพื่อพิจารณาขยายช่วงเวลาของการรับรองไม่เกิน ๑๘๐ วัน นับจากสถานะการรับรองผู้ให้บริการสิ้นอายุ (สถานะการรับรองจะต่อเนื่องจากการรับรองเดิม)

เมื่อครบช่วงเวลาที่สำนักงานได้ขยายให้หากผู้ได้รับการรับรองยังไม่สามารถให้สำนักงานเข้าตรวจประเมินใหม่ตามช่วงเวลาที่กำหนดตามข้างต้นได้ ผู้ได้รับการรับรองจะต้องยื่นคำขอรับการตรวจประเมินเพื่อการรับรองใหม่ โดยขอให้ดำเนินการตามแผนผังแสดงขั้นตอนการตรวจประเมินคุณสมบัติของผู้ให้บริการคลาวด์ปรากฏอยู่ใน **ภาคผนวก ค** ของเอกสารฉบับนี้

๓.๔ เงื่อนไขสำหรับผู้ได้รับการรับรอง

ผู้ได้รับการรับรองต้องปฏิบัติตามเงื่อนไขดังต่อไปนี้

๓.๔.๑ ปฏิบัติตามหลักเกณฑ์ วิธีการ และเงื่อนไขการประเมินและการรับรองตามประกาศนี้ รวมทั้งที่อาจมีการแก้ไขหรือกำหนดเพิ่มเติมในภายหลังตลอดเวลาที่ได้รับการรับรอง

๓.๔.๒ ต้องรักษาไว้ซึ่งการปฏิบัติตามมาตรฐาน และหลักเกณฑ์เงื่อนไข ตลอดระยะเวลา ที่ได้รับการรับรอง

๓.๔.๓ ต้องส่งมอบเอกสารหลักฐานต่าง ๆ ที่เกี่ยวข้องกับการรับรองที่เป็นปัจจุบันให้แก่สำนักงานเมื่อได้รับการร้องขอ

๓.๔.๔ ในกรณีมีเหตุอย่างหนึ่งอย่างใดอันส่งผลให้ผู้ได้รับการรับรองไม่สามารถให้บริการได้หรือไม่อาจให้บริการได้ เช่น การรับรองสิ้นอายุ การถูกพักใช้ การถูกเพิกถอน และการเลิกประกอบกิจการสำนักงาน สามารถกำหนดหลักเกณฑ์ วิธีการ และเงื่อนไขใด ๆ ให้ผู้ได้รับการรับรองปฏิบัติตาม หรือดำเนินการอย่างหนึ่ง อย่างใด เพื่อคุ้มครองประโยชน์ของผู้รับบริการ รวมทั้งการโอนบริการไปยังผู้ได้รับการรับรองรายอื่นเพื่อ ความต่อเนื่องในการใช้งานของผู้รับบริการ โดยผู้ได้รับการรับรองยินยอมที่จะปฏิบัติตามหรือดำเนินการอย่างใด อย่างหนึ่งตามหลักเกณฑ์ วิธีการ และเงื่อนไขดังกล่าวอย่างเคร่งครัด

๓.๔.๕ หากมีการเปลี่ยนแปลงแก้ไขใด ๆ ตามขอบข่ายที่ได้รับการรับรองในสาระสำคัญ เช่น การเปลี่ยนแปลงสถานะทางกฎหมายหรือการค้า โครงสร้างการบริหารงานและอำนาจหน้าที่ ระบบสารสนเทศ การเปลี่ยนชื่อที่อยู่ และสถานที่ติดต่อ การย้ายสถานที่ทำการ เป็นต้น ให้ยื่นคำขอ แจ้งการเปลี่ยนแปลงต่อสำนักงานทราบทันทีเพื่อสำนักงานจะได้พิจารณาผลกระทบต่อขอบข่ายที่ได้รับการรับรอง ทั้งนี้ สำนักงานอาจพิจารณาให้มีการดำเนินการตรวจประเมินเพิ่มเติมในกรณีที่มีความจำเป็น

๓.๔.๖ ต้องจัดเก็บบันทึกข้อร้องเรียนที่ได้รับจากบุคคลภายนอก และผลการดำเนินการกับข้อร้องเรียนทั้งหมดที่เกี่ยวข้องกับขอบข่ายที่ได้รับการรับรองไว้ และต้องมอบบันทึกข้อร้องเรียนและผลการดำเนินการ ให้แก่สำนักงานเมื่อได้รับการร้องขอ กรณีที่ข้อร้องเรียนที่ได้รับไม่เป็นลายลักษณ์อักษร ให้ผู้ได้รับการรับรองแจ้งให้ผู้ตรวจประเมินทราบในระหว่างการตรวจประเมินเพื่อต่ออายุ หากผู้ได้รับการรับรองปิดบังข้อมูลเกี่ยวกับข้อร้องเรียน และสำนักงานสืบทราบได้ในภายหลัง สำนักงานจะดำเนินการพักใช้ หรือเพิกถอนการรับรอง เป็นกรณีไป

๓.๕ การเพิกถอนการรับรอง

กรณีที่ผู้ได้รับการรับรองได้กระทำการในกรณีใดกรณีหนึ่ง หรือหลายกรณีดังต่อไปนี้

(๑) ไม่ปฏิบัติตามเงื่อนไขสำหรับผู้ได้รับการรับรอง ตามที่กำหนดในข้อ ๓.๔ และส่งผลกระทบร้ายแรงต่อการรับรอง

(๒) เคยถูกสั่งพักใช้การรับรองจำนวน ๒ ครั้ง ในรอบการรับรอง

(๓) ไม่ดำเนินการแก้ไขปรับปรุงความไม่สอดคล้องหลังถูกพักใช้การรับรอง

(๔) มีข้อร้องเรียนที่พิจารณาแล้วเห็นว่า ทำให้เกิดความเสียหายต่อการรับรอง

(๕) ยกเลิกการประกอบกิจการ และไม่มีการแจ้งสำนักงานเพื่อขอยกเลิกการรับรอง หรือสำนักงานไม่สามารถติดต่อผู้ได้รับการรับรองให้ดำเนินการตามหลักเกณฑ์และเงื่อนไขที่เกี่ยวข้องตามที่สำนักงานกำหนดได้

(๖) กรณีอื่น ๆ ที่สำนักงานพิจารณาเห็นว่าเป็นการกระทำที่ก่อให้เกิดความเสียหายต่อระบบ การรับรอง หรือเป็นการกระทำความผิดที่ก่อให้เกิดความเสียหายอย่างร้ายแรงต่อเศรษฐกิจ หรือต่อประโยชน์สาธารณะ

๓.๖ กรณีอยู่ระหว่างดำเนินการขอใบรับรองมาตรฐานความมั่นคงปลอดภัยสารสนเทศระบบคลาวด์

(๑) ผู้ให้บริการคลาวด์ ตัวแทน และอื่นๆที่อยู่ระหว่างดำเนินการขอใบรับรองมาตรฐานความมั่นคงปลอดภัยสารสนเทศระบบคลาวด์ ให้จัดเตรียมเอกสารประกอบ โดยมีการรับรองจากผู้ตรวจสอบอิสระ หรือผู้ตรวจสอบภายในองค์กร ซึ่งต้องเป็นผู้มีคุณสมบัติเหมาะสมและถือใบประกาศนียบัตรที่เกี่ยวข้อง เช่น Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM), Certified Information Systems Security Professional (CISSP), ISO/IEC 27001 Lead Auditor หรือประกาศนียบัตรอื่นตามที่สำนักงานกำหนด ทั้งนี้ต้องแสดงข้อมูลให้แก่สำนักงานจนเป็นที่พอใจและเป็นที่เชื่อถือได้ว่า ระบบคลาวด์มีความมั่นคงปลอดภัย มีการบริหารจัดการที่เหมาะสม และมีมาตรการในการป้องกันข้อมูลส่วนบุคคลอย่างเพียงพอ

(๒) ผู้ให้บริการคลาวด์ ตัวแทน และอื่นๆ จะต้องดำเนินการตามคู่มือและแบบฟอร์มที่สำนักงานกำหนด ซึ่งเผยแพร่ไว้บนเว็บไซต์ standard.dga.or.th ทั้งนี้ เพื่อให้เป็นไปตามแนวทางที่สำนักงานได้วางไว้

แผนผังขั้นตอนการยื่นเอกสารเพิ่มเติม ในกรณีผู้ให้บริการคลาวด์ ตัวแทนและอื่นๆ อยู่ในระหว่างการขอมาตรฐานด้านความปลอดภัยสารสนเทศระบบคลาวด์ปรากฏอยู่ใน **ภาคผนวก ง** ของเอกสารฉบับนี้

ภาคผนวก

ภาคผนวก ก

หลักเกณฑ์ วิธีการ และเงื่อนไขสำหรับการรับรองการตรวจคุณสมบัติเบื้องต้นผู้ให้บริการคลาวด์สำหรับภาครัฐ ตามนโยบายการใช้คลาวด์เป็นหลัก (Cloud First Policy)

ขอบเขตการรับรอง	คุณสมบัติเบื้องต้นผู้ให้บริการคลาวด์ ตัวแทนและอื่นๆ ตามนโยบายการใช้คลาวด์เป็นหลัก
เกณฑ์การตรวจประเมิน	๑. ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง กรอบแนวทางการบริหารจัดการคลาวด์ภาครัฐตามนโยบายการใช้คลาวด์เป็นหลัก มอบอำนาจให้ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.) เป็นหน่วยงานตรวจประเมินรับรองมาตรฐานคลาวด์ ตามที่คณะกรรมการพัฒนารัฐบาลดิจิทัลกำหนด ๒. ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง หลักเกณฑ์ วิธีการและเงื่อนไขการตรวจประเมินผู้ให้บริการคลาวด์ ตามนโยบายการใช้คลาวด์เป็นหลัก ๓. ประกาศคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่งคงปลอดภัยไซเบอร์ระบบคลาวด์ ๒๕๖๗ ๔. พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ ๕. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ๖. มาตรฐานรัฐบาลดิจิทัลว่าด้วยแนวทางการกำหนดมาตรฐานผู้ให้บริการคลาวด์ตามนโยบายการใช้คลาวด์เป็นหลัก เลขที่ มรด ๙-๓ : ๒๕๖๘
อายุการรับรอง	๓ ปี
รูปแบบการรับรอง	ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง หลักเกณฑ์ วิธีการ และเงื่อนไขการตรวจประเมินและรับรองผู้ให้บริการคลาวด์ พ.ศ. ๒๕๖๘
ภาษาที่ใช้ในการตรวจประเมิน	ใช้ภาษาไทยเป็นหลัก
คุณสมบัติของยื่นคำขอ	๑. เป็นนิติบุคคล ๑.๑ ให้บริการระบบคลาวด์ หรือ ๑.๒ ที่จัดการการใช้งาน การทำงาน และการจัดส่งบริการระบบคลาวด์ รวมถึงเจรจาความสัมพันธ์ระหว่างผู้ให้บริการระบบคลาวด์และผู้ใช้บริการ ๒. ไม่เป็นผู้ถูกเพิกถอนการให้บริการระบบคลาวด์ การจัดการการใช้งาน การทำงาน การจัดส่งบริการระบบคลาวด์ และเจรจาความสัมพันธ์ระหว่าง

	ผู้ให้บริการระบบคลาวด์และผู้ใช้บริการ เว้นแต่ได้พ้นระยะเวลา ๑๘๐ วัน นับแต่วันที่ได้รับแจ้งคำสั่งคำสั่งเพิกถอนการรับรอง
ผลการรับรอง	มีผลใช้ภายในประเทศไทยเท่านั้น
การยื่นคำขอตรวจประเมิน	กรอกรายละเอียดในแบบฟอร์ม **"แบบการเปิดเผยข้อมูลของผู้ให้บริการคลาวด์"** และลงลายมือชื่อ พร้อมเอกสารประกอบ
ช่องทางการแจ้งความประสงค์ขอรับการตรวจประเมิน	https://standard.dga.or.th/
ช่องทางการรับคำขอตรวจประเมิน	อีเมล sd-g4_division@dga.or.th

รายการเอกสารที่จำเป็น ตามภาคผนวก ก

รายการเอกสาร ข้อมูลรายละเอียดทั่วไปผู้ให้บริการคลาวด์ ตัวแทนและอื่นๆ		
๑	หนังสือรับรองการจดทะเบียนนิติบุคคล จากกรมพัฒนาธุรกิจการค้า (DBD) * อายุไม่เกิน ๖ เดือนนับจากวันที่ยื่น	☐
๒	“หนังสือแต่งตั้ง” หรือ “ข้อตกลงตัวแทนจำหน่าย” อย่างเป็นทางการจากผู้ให้บริการคลาวด์ต้นทาง หรือเอกสารอื่นๆ เพื่อยืนยันสถานะความร่วมมือและสิทธิในการขาย บริการ และให้การสนับสนุนลูกค้า (ในกรณีที่ผู้ยื่นคำขอเป็น ตัวแทนหรืออื่นๆ)	☐
รายการเอกสาร แสดงมาตรฐานควบคุมด้านความมั่นคงปลอดภัยสารสนเทศระบบคลาวด์		
สำหรับผู้ให้บริการคลาวด์		
๑	ใบรับรองมาตรฐาน ISO/IEC 20000 (ยังมีผลบังคับใช้ (Valid Date) ณ วันที่ยื่นหลักฐาน)	☐
๒	ใบรับรองมาตรฐาน ISO/IEC 27001 (ยังมีผลบังคับใช้ (Valid Date) ณ วันที่ยื่นหลักฐาน)	☐
๓	ใบรับรองมาตรฐาน CSA STAR (ยังมีผลบังคับใช้ (Valid Date) ณ วันที่ยื่นหลักฐาน)	☐
๔	ใบรับรองมาตรฐาน ISO/IEC 27017 (ยังมีผลบังคับใช้ (Valid Date) ณ วันที่ยื่นหลักฐาน)	☐
๕	ใบรับรองมาตรฐาน ISO/IEC 27701 (ยังมีผลบังคับใช้ (Valid Date) ณ วันที่ยื่นหลักฐาน)	☐
๖	ใบรับรองมาตรฐาน ISO/IEC 27018 (ยังมีผลบังคับใช้ (Valid Date) ณ วันที่ยื่นหลักฐาน)	☐
สำหรับตัวแทนและอื่นๆ		
๑	ใบรับรองมาตรฐาน ISO/IEC 20000 (ยังมีผลบังคับใช้ (Valid Date) ณ วันที่ยื่นหลักฐาน)	☐
๒	เอกสารรับรองมาตรฐานผู้ให้บริการคลาวด์ ที่เป็นตัวแทน	☐
สำหรับพิจารณาลำดับชั้น (Tier) ผู้ให้บริการคลาวด์ ตัวแทนและอื่นๆ		
อ้างอิง ประกาศ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ ๒๕๖๗ (สำหรับผู้ประกอบการคลาวด์ต้องการเป็นระดับชั้น Tier II ขึ้นไป)		
๑	การปฏิบัติตามกฎ ระเบียบ ข้อบังคับ (Compliance)	☐

๒	การรักษาความปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environment Security)	☐
๓	การรักษาความมั่นคงปลอดภัยการปฏิบัติการ (Operations Security)	☐
๔	การรักษาความมั่นคงปลอดภัยเครือข่าย (Communication Security)	☐
๕	การจัดการเหตุภัยคุกคามทางสารสนเทศ (Information Security Incident Management)	☐

ภาคผนวก ข

หลักเกณฑ์การพิจารณาการใช้บริการคลาวด์ที่เก็บข้อมูลนอกราชอาณาจักร

การใช้บริการคลาวด์นอกราชอาณาจักรสำหรับภาครัฐ ทางสำนักงานมีหลักเกณฑ์การพิจารณาผู้ให้บริการ ตัวแทน และอื่นๆ ที่เป็นไปตามมาตรฐานรัฐบาลดิจิทัลว่าด้วยแนวทางการกำหนดมาตรฐานผู้ให้บริการคลาวด์ตามนโยบายการใช้คลาวด์เป็นหลัก เลขที่ มรด ๙-๓ : ๒๕๖๘ ดังต่อไปนี้

๑. ความจำเป็นในการใช้บริการนอกราชอาณาจักร
   - บริการที่ขึ้นทะเบียนต้องตอบสนองความต้องการทางธุรกิจหรือทางเทคนิคที่ไม่สามารถตอบสนองได้ด้วยบริการคลาวด์ที่มีการจัดเก็บข้อมูลในประเทศไทยอย่างชัดเจน

๒. ประสบการณ์และความน่าเชื่อถือ
   - มีประวัติการให้บริการแก่หน่วยงานภาครัฐหรือองค์กรขนาดใหญ่ที่ได้รับการยอมรับในระดับสากลหรือมีชื่อเสียงในอุตสาหกรรม
   - บริการเชิงนวัตกรรม พิจารณาจากศักยภาพของเทคโนโลยีและทีมงาน

๓. ความปลอดภัยและการปกป้องข้อมูล
   - มีมาตรฐานความปลอดภัย การเข้ารหัสข้อมูล การควบคุมการเข้าถึง ระบบสำรองและกู้คืน การตรวจจับและป้องกันภัยคุกคาม และนโยบายความเป็นส่วนตัวที่สอดคล้องกับ PDPA

๔. อธิปไตยข้อมูลความเป็นส่วนตัว และสิทธิในการควบคุมข้อมูล
   - ตรวจสอบที่ตั้งศูนย์ข้อมูล กฎหมายที่บังคับใช้ มาตรการการโอนย้ายข้อมูลข้ามประเทศ การเป็นเจ้าของข้อมูล สิทธิการเข้าถึงข้อมูล/ลบข้อมูล และการปฏิบัติตาม PDPA

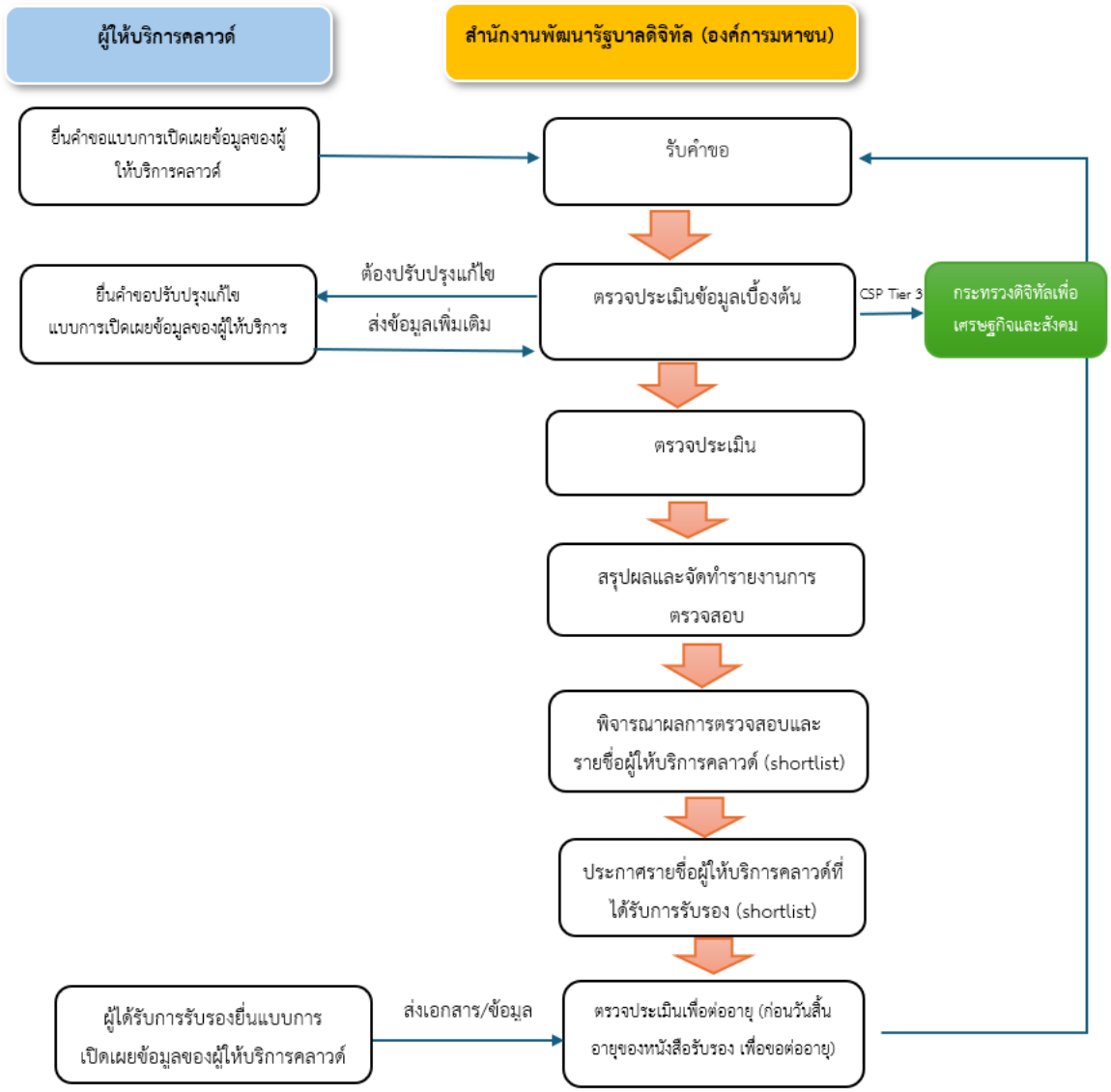
๕. ความสามารถในการขยาย
   - ประเมินความสามารถในการปรับเพิ่ม/ลดทรัพยากรได้อย่างรวดเร็ว เพื่อรองรับการเปลี่ยนแปลงของปริมาณงานในอนาคต

๖. ราคาและแผนการชำระเงิน
   - โครงสร้างราคาที่โปร่งใส รูปแบบการคิดค่าบริการ ความยืดหยุ่นในการปรับเปลี่ยน ส่วนลดสำหรับหน่วยงานภาครัฐ รวมถึงช่องทางการชำระเงินที่สะดวกและปลอดภัย

๗. ที่ตั้งและการติดต่อ
   - ที่ตั้งสำนักงานใหญ่/สาขาที่ติดต่อได้ ช่องทางการติดต่อที่ชัดเจน และความสามารถในการตอบสนองสำหรับข้อมูลสำคัญ ควรพิจารณาผู้ให้บริการที่มีตัวแทนในประเทศ

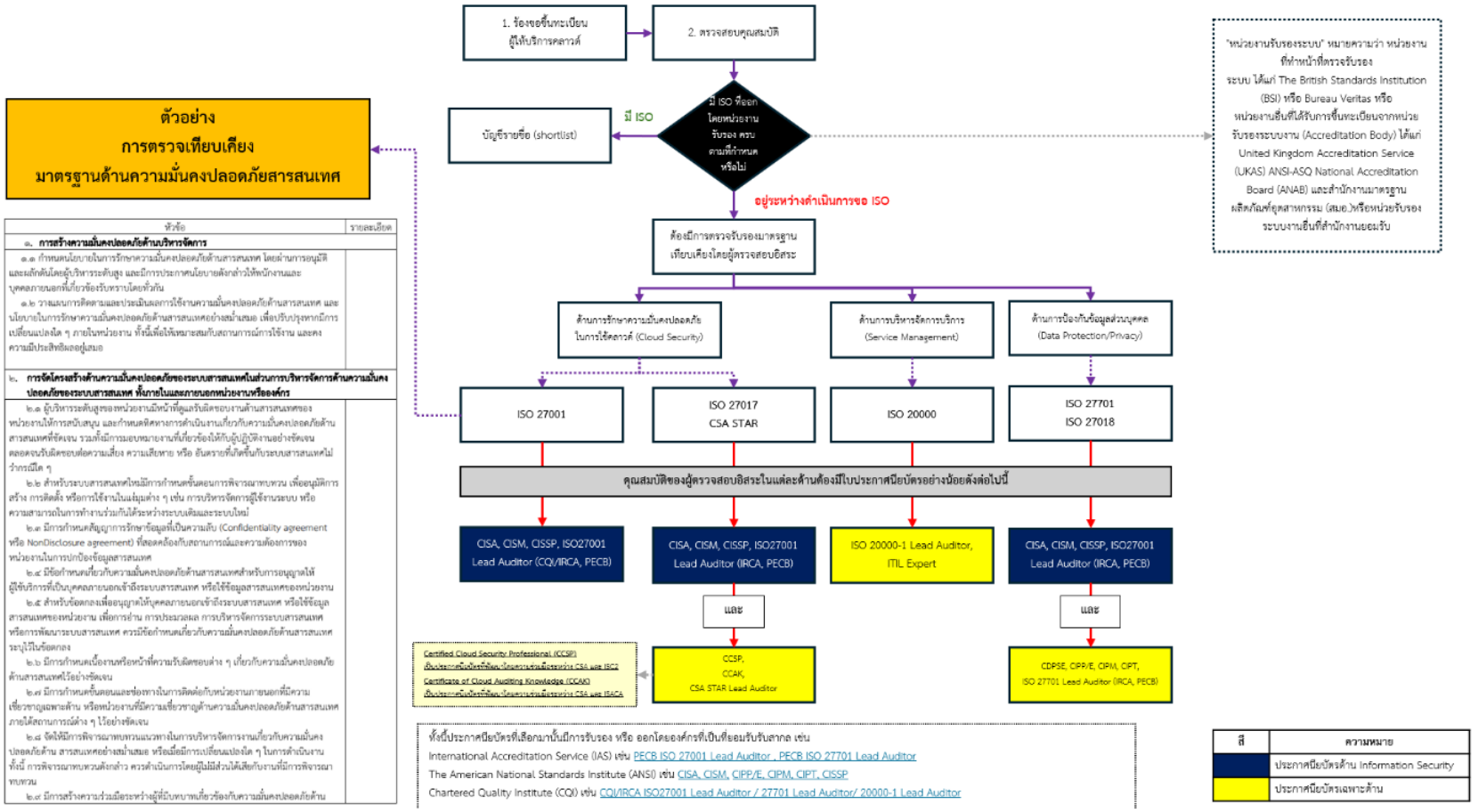
๘. การสนับสนุนและบริการลูกค้า
   - มีช่องทางการบริการลูกค้า ระดับการให้บริการ (SLA) และภาษาในการให้บริการที่ชัดเจน เพื่อให้มั่นใจว่าหน่วยงานได้รับการช่วยเหลือทันท่วงทีเมื่อเกิดปัญหา

ภาคผนวก ค
แผนผังขั้นตอนการตรวจประเมินคุณสมบัติผู้ให้บริการคลาวด์



ภาคผนวก ง

แผนผังขั้นตอนการยื่นเอกสารเพิ่มเติม ในกรณีผู้ให้บริการคลาวด์ ตัวแทนและอื่นๆ อยู่ในระหว่างการขอมาตรฐานด้านความปลอดภัยสารสนเทศระบบคลาวด์



หัวข้อ	รายละเอียด
๑. **การสร้างความมั่นคงปลอดภัยด้านบริหารจัดการ**	
๑.๑ กำหนดนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยผ่านการอนุมัติและผลักดันโดยผู้บริหารระดับสูง และมีการประกาศนโยบายดังกล่าวให้พนักงานและบุคคลภายนอกที่เกี่ยวข้องรับทราบโดยทั่วกัน ๑.๒ วางแผนการติดตามและประเมินผลการใช้งานความมั่นคงปลอดภัยด้านสารสนเทศ และนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างสม่ำเสมอ เพื่อปรับปรุงหากมีการเปลี่ยนแปลงใด ๆ ภายในหน่วยงาน ทั้งนี้เพื่อให้เหมาะสมกับสถานการณ์การใช้งาน และคงความมีประสิทธิผลอยู่เสมอ	
๒. **การจัดโครงสร้างด้านความมั่นคงปลอดภัยของระบบสารสนเทศในส่วนการบริหารจัดการด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ทั้งภายในและภายนอกหน่วยงานหรือองค์กร**	
๒.๑ ผู้บริหารระดับสูงของหน่วยงานมีหน้าที่ดูแลรับผิดชอบงานด้านสารสนเทศของหน่วยงานให้การสนับสนุน และกำหนดทิศทางการดำเนินงานเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศที่ชัดเจน รวมทั้งมีการมอบหมายงานที่เกี่ยวข้องให้กับผู้ปฏิบัติงานอย่างชัดเจน ตลอดจนรับผิดชอบต่อความเสี่ยง ความเสียหาย หรือ อันตรายที่เกิดขึ้นกับระบบสารสนเทศไม่ว่ากรณีใด ๆ ๒.๒ สำหรับระบบสารสนเทศใหม่มีการกำหนดขั้นตอนการพิจารณาทบทวน เพื่ออนุมัติการสร้าง การติดตั้ง หรือการใช้งานในแง่มุมต่าง ๆ เช่น การบริหารจัดการผู้ใช้งานระบบ หรือความสามารถในการทำงานร่วมกันได้ระหว่างระบบเดิมและระบบใหม่ ๒.๓ มีการกำหนดสัญญาการรักษาข้อมูลที่เป็นความลับ (Confidentiality agreement หรือ NonDisclosure agreement) ที่สอดคล้องกับสถานการณ์และความต้องการของหน่วยงานในการปกป้องข้อมูลสารสนเทศ ๒.๔ มีข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศสำหรับการอนุญาตให้ผู้ใช้บริการที่เป็นบุคคลภายนอกเข้าถึงระบบสารสนเทศ หรือใช้ข้อมูลสารสนเทศของหน่วยงาน ๒.๕ สำหรับข้อตกลงเพื่ออนุญาตให้บุคคลภายนอกเข้าถึงระบบสารสนเทศ หรือใช้ข้อมูลสารสนเทศของหน่วยงาน เพื่อการอ่าน การประมวลผล การบริหารจัดการระบบสารสนเทศ หรือการพัฒนาระบบสารสนเทศ ควรมีข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศระบุไว้ในข้อตกลง ๒.๖ มีการกำหนดเนื้องานหรือหน้าที่ความรับผิดชอบต่าง ๆ เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศไว้อย่างชัดเจน ๒.๗ มีการกำหนดขั้นตอนและช่องทางในการติดต่อกับหน่วยงานภายนอกที่มีความเชี่ยวชาญเฉพาะด้าน หรือหน่วยงานที่มีความเชี่ยวชาญด้านความมั่นคงปลอดภัยด้านสารสนเทศภายใต้สถานการณ์ต่าง ๆ ไว้อย่างชัดเจน ๒.๘ จัดให้มีการพิจารณาทบทวนแนวทางในการบริหารจัดการงานเกี่ยวกับความมั่นคงปลอดภัยด้าน สารสนเทศอย่างสม่ำเสมอ หรือเมื่อมีการเปลี่ยนแปลงใด ๆ ในการดำเนินงาน ทั้งนี้ การพิจารณาทบทวนดังกล่าว ควรดำเนินการโดยผู้ไม่มีส่วนได้เสียกับงานที่มีการพิจารณาทบทวน ๒.๙ มีการสร้างความร่วมมือระหว่างผู้ที่มีบทบาทเกี่ยวข้องกับความมั่นคงปลอดภัยด้าน	

เอกสารอ้างอิง

ISO 19011. แนวทางในการตรวจประเมินระบบการจัดการ. องค์การระหว่างประเทศว่าด้วยการมาตรฐาน (ISO).