R-NCSA-04

(ร่าง) ข้อกำหนดเฉพาะในการรับรองบริการคลาวด์

Particular Certification Requirements : Cloud Service

ประกาศสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
เรื่อง ข้อกำหนดเฉพาะในการรับรองบริการคลาวด์
พ.ศ. ๒๕๖๘

เพื่อให้การดำเนินการรับรองบริการคลาวด์ เป็นไปด้วยความเรียบร้อย มีประสิทธิภาพ สอดคล้องตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๖ ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. ๒๕๖๗ แนวทางการรับรอง และอื่น ๆ ที่เกี่ยวข้องของสำนักงาน

อาศัยอำนาจตามความในข้อ ๑๔ ของประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๖ เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จึงออกประกาศไว้ ดังนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ข้อกำหนดเฉพาะในการรับรองบริการคลาวด์ พ.ศ. ๒๕๖๘”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

ข้อ ๓ ข้อกำหนดเฉพาะในการในการรับรองบริการคลาวด์ ให้เป็นไปตามแนบท้ายประกาศนี้

ข้อ ๔ ให้เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติรักษาการตามประกาศนี้

ในกรณีที่มีปัญหาเกี่ยวกับการปฏิบัติตามประกาศนี้ หรือประกาศนี้มิได้กำหนดเรื่องใดไว้ ให้เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ มีอำนาจตีความและวินิจฉัยชี้ขาด ทั้งนี้ การตีความและคำวินิจฉัยดังกล่าวให้เป็นที่สุด

ประกาศ ณ วันที่ สิงหาคม พ.ศ. ๒๕๖๙

พลอากาศตรี

(อมร ชมเชย)

เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

สำนักงานคณะกรรมการการรักษา
ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

(ร่าง) ข้อกำหนดเฉพาะในการรับรองบริการคลาวด์

Particular Certification Requirements : Cloud Service

ประวัติการปรับปรุงเอกสาร

ครั้งที่	วันที่ประกาศใช้	รายการปรับปรุง
๑	สิงหาคม ๒๕๖๙	จัดทำเอกสารฉบับแรก

ข้อกำหนดเฉพาะในการรับรอง : บริการคลาวด์

Particular Certification Requirements : Cloud Service

๑. วัตถุประสงค์

ข้อกำหนดเฉพาะในการรับรอง: บริการคลาวด์นี้ กำหนดขึ้นโดยมีวัตถุประสงค์ ดังนี้

(๑) เพื่อให้วิธีการ รูปแบบ และข้อกำหนด ที่ใช้เป็นหลักปฏิบัติในการดำเนินงานในการรับรอง: บริการคลาวด์ มีความชัดเจน เป็นที่ยอมรับ และสอดคล้องกับมาตรฐานระดับประเทศ หรือระดับนานาชาติ

(๒) เพื่อใช้เป็นแนวทางในการดำเนินการตรวจประเมิน ผู้ยื่นคำขอหรือผู้ได้รับการรับรอง รวมทั้งใช้ในการประเมิน ทั้งก่อนและหลังได้รับการรับรอง

๒. ขอบเขต

เอกสารนี้เป็นการกำหนดหลักเกณฑ์เฉพาะในการรับรองคุณภาพผลิตภัณฑ์: บริการคลาวด์ โดยครอบคลุมตั้งแต่การชี้บ่งบริการและมาตรฐานที่เกี่ยวข้อง หลักเกณฑ์และข้อกำหนดทั้งหมด ซึ่งรวมถึงการทดสอบ การตรวจประเมิน และการตรวจติดตามผล

๓. เอกสารอ้างอิง(๑)

๓.๑ มอก. 17065 การตรวจสอบและรับรอง – ข้อกำหนดสำหรับหน่วยรับรองผลิตภัณฑ์กระบวนการและการบริการ

๓.๒ มอก. 17020 ข้อกำหนดทั่วไปสำหรับหน่วยตรวจ

๓.๓ มอก. 17025 ข้อกำหนดทั่วไปว่าด้วยความสามารถของห้องปฏิบัติการทดสอบและห้องปฏิบัติการสอบเทียบ

๓.๔ มอก. 17040 การตรวจสอบและรับรอง – ข้อกำหนดทั่วไปว่าด้วยการประเมินเพื่อการยอมรับร่วมของหน่วยตรวจสอบและรับรอง และหน่วยรับรองระบบงาน

๓.๕ ISO/IEC 17065 Conformity assessment – Requirements for bodies certifying products, processes and services

๓.๖ ISO/IEC 17067 Conformity assessment - Fundamentals of product certification and guidelines for product certification schemes

หมายเหตุ : (๑) เอกสารอ้างอิงให้เป็นไปตามข้อกำหนดของมาตรฐานฉบับล่าสุด

๔. นิยาม

๔.๑ สำนักงาน หมายถึง สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

๔.๒ ผู้ยื่นคำขอ หมายถึง ผู้ให้บริการคลาวด์ (Cloud Service Provider: CSP) หรือ ผู้ใช้บริการคลาวด์ (Cloud Service Customer: CSC) ที่ประสงค์จะขอรับการรับรองบริการคลาวด์กับสำนักงาน

๔.๓ บริการคลาวด์ หมายถึง ความสามารถในการประมวลผลคลาวด์ ซึ่งถูกเรียกใช้โดยอินเทอร์เฟซที่กำหนดให้

๔.๔ การประมวลผลคลาวด์ หมายถึง แนวคิดการเข้าถึงเครือข่ายสารสนเทศซึ่งเป็นกลุ่มทรัพยากรทางกายภาพหรือเสมือนที่สามารถแบ่งปัน มีความยืดหยุ่น และขยายขนาดได้ด้วยการจัดการตัวเองและการจัดการตามความต้องการ

๔.๕ ผู้ให้บริการคลาวด์ (Cloud Service Provider: CSP) หมายถึง หน่วยงานของรัฐหรือเอกชนที่ทำให้บริการคลาวด์สามารถใช้ได้กับผู้ใช้บริการคลาวด์ รวมถึงจัดการทรัพยากรเหล่านี้ เพื่อให้มั่นใจว่ามีความพร้อมใช้งาน ความมั่นคงปลอดภัย และความสามารถในการขยายตัวสำหรับผู้ใช้บริการคลาวด์ของตน

๔.๖ ผู้ใช้บริการคลาวด์ (Cloud Service Customer: CSC) หมายถึง หน่วยงานที่มีข้อตกลงทางสัญญาอย่างเป็นทางการในการใช้บริการคลาวด์ที่ให้บริการ โดยผู้ให้บริการคลาวด์

๔.๗ ผู้ได้รับการรับรอง หมายถึง ผู้ยื่นคำขอที่ผ่านการตรวจประเมินและได้รับการรับรองจากสำนักงาน

๔.๘ การรับรองคุณภาพผลิตภัณฑ์ หมายถึง กระบวนการที่สำนักงาน ให้การยอมรับอย่างเป็นทางการแก่ผู้ได้รับการรับรอง ว่ามีขีดความสามารถในการให้บริการ และควบคุมคุณภาพให้เป็นไปตามมาตรฐานที่สำนักงานกำหนดได้อย่างต่อเนื่อง และสามารถรักษาคุณภาพบริการที่ได้รับการรับรองได้ตลอดระยะเวลาที่ได้รับการรับรอง

๔.๙ การตรวจประเมิน หมายถึง การตรวจประเมินระบบการควบคุมคุณภาพ และการประเมินบริการคลาวด์ของผู้ยื่นคำขอ ด้วยวิธีการและหลักเกณฑ์ที่สำนักงานกำหนด

๔.๑๐ การตรวจติดตามผล หมายถึง การตรวจประเมินระบบการควบคุมคุณภาพและการประเมินบริการคลาวด์ในขอบข่ายที่ได้รับการรับรองของผู้ได้รับการรับรองด้วยวิธีการและหลักเกณฑ์ที่สำนักงานกำหนด

๔.๑๑ มาตรฐานและหลักเกณฑ์อ้างอิง หมายถึง มาตรฐานหรือหลักเกณฑ์อ้างอิงของประเทศ

๔.๑๒ มาตรฐานที่เทียบเท่า หมายถึง มาตรฐานระดับนานาชาติ หรือมาตรฐานระดับชาติของประเทศอื่นที่รับเอามาตรฐาน ระดับนานาชาติมาเป็นต้นแบบในการกำหนด

๕. การชี้บ่งบริการคลาวด์และมาตรฐานที่กำหนด

๕.๑ การชี้บ่งบริการคลาวด์

บริการคลาวด์ที่ประสงค์จะขอรับการรับรองตามข้อกำหนดฉบับนี้ ต้องมีการชี้บ่งอย่างน้อย ดังต่อไปนี้

- ชื่อบริการคลาวด์
- ประเภทบริการคลาวด์ : การให้บริการโครงสร้างพื้นฐานหลัก (Infrastructure as a Service : IaaS),การให้บริการแพลตฟอร์ม (Platform as a Service : PaaS), การให้บริการซอฟต์แวร์ (Software as a Service : SaaS)
- เครื่องหมายการค้าที่จดทะเบียน
- รุ่น (Version)
- ลักษณะการใช้งาน (Function) หรือความสามารถของบริการคลาวด์
- รายการอุปกรณ์ หรือระบบที่จำเป็นต้องใช้ร่วมกับบริการ (ถ้ามี)

๕.๒ มาตรฐานและหลักเกณฑ์อ้างอิงที่กำหนด

สำนักงานจะดำเนินการรับรองบริการคลาวด์แก่ผู้ให้บริการคลาวด์และผู้ใช้บริการคลาวด์ โดยกำหนดเกณฑ์การประเมินตามประเภทข้อมูลหรือระบบสารสนเทศ โดยมีมาตรฐานและหลักเกณฑ์อ้างอิง ดังตารางที่ ๑

ตารางที่ ๑ รายละเอียดมาตรฐาน หลักเกณฑ์และข้อกำหนดที่เกี่ยวข้อง

ประเภทข้อมูลหรือระบบสารสนเทศ(๑)(๒)	ผู้ใช้บริการคลาวด์ (CSC)	ผู้ให้บริการคลาวด์ (CSP)
ผลกระทบระดับต่ำ	มาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์	มาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ และ ISO/IEC 27001 และ CSA STAR Level 1/CCM Lite
ผลกระทบระดับกลาง	มาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์	มาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ และ CSA STAR Level 2/CCM และ ISO/IEC 27701
ผลกระทบระดับสูง	มาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์	มาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ และ ISO/IEC 27017 หรือ CSA STAR Level 2/CCM และ ISO/IEC 27018 และ ISO/IEC 27701

หมายเหตุ (๑) ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๖

(๒) ข้อกำหนดขั้นต่ำและการตรวจรับรองสำหรับผู้ใช้บริการคลาวด์และผู้ให้บริการคลาวด์ ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. ๒๕๖๗

๖. หลักเกณฑ์และข้อกำหนดในการรับรอง

๖.๑ หลักเกณฑ์การตรวจประเมินเพื่อให้การรับรองบริการคลาวด์

การตรวจประเมินเพื่อให้การรับรองบริการคลาวด์จะพิจารณาจากขีดความสามารถของผู้ยื่นคำขอ โดยมีวัตถุประสงค์ เพื่อให้

(๑) การให้บริการคลาวด์ และการใช้บริการคลาวด์ มีความมั่นคงปลอดภัย ลดความเสี่ยงต่อภัยคุกคามทางไซเบอร์ที่มีต่อระบบคลาวด์ได้อย่างคลอบคลุม และมีประสิทธิภาพ เป็นไปตามมาตรฐานที่สำนักงานกำหนด และ

(๒) การควบคุมดูแล รักษาระดับคุณภาพ ให้เป็นไปตามมาตรฐานทั้งหมดอย่างสม่ำเสมอ

๖.๒ การตรวจประเมินเพื่อการรับรอง

๖.๒.๑ การตรวจประเมินเพื่อการรับรอง ประกอบด้วย

(๑) ด้านการกำกับดูแลด้านความมั่นคงปลอดภัยระบบคลาวด์ (Cloud Security Governance)

(๒) ด้านการปฏิบัติและการรักษาความมั่นคงปลอดภัยโครงสร้างพื้นฐานระบบคลาวด์ (Cloud Infrastructure Security and Operation)

สำนักงานจะประเมินเอกสารที่เกี่ยวข้องกับนโยบาย มาตรฐาน การจัดการองค์กร วิธีการ/ขั้นตอนการทำงาน และเอกสารอื่นที่เกี่ยวข้องกับความมั่นคงปลอดภัย ว่ามีความสอดคล้องตามมาตรฐานและหลักเกณฑ์ที่กำหนด

๖.๒.๒ การตรวจประเมินสถานประกอบการ/สถานที่ปฏิบัติการ

สำนักงานจะดำเนินการตรวจประเมินการปฏิบัติงานและการรักษาความมั่นคงปลอดภัยโครงสร้างพื้นฐานระบบคลาวด์ ณ สถานประกอบการ/สถานที่ปฏิบัติงานของผู้ยื่นคำขอ เพื่อทวนสอบความสามารถ

และประสิทธิผลของการปฏิบัติงาน ว่าสอดคล้องตามข้อกำหนดของมาตรฐานและหลักเกณฑ์อ้างอิงที่กำหนดในข้อ ๕.๒ ด้วยวิธีที่ระบุไว้ในข้อที่ ๙.๓ ของหลักเกณฑ์ทั่วไป สำหรับการรับรองผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์ (R-NCSA-01)

ทั้งนี้ ตัวอย่างรายการตรวจประเมินตามมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ เป็นไปตามภาคผนวก ก

๖.๓ การประเมินผลการตรวจสอบ

๖.๓.๑ สำนักงานจะประเมินผลการตรวจสอบ โดยใช้ผลการประเมินในข้อ ๖.๒ เทียบกับเกณฑ์การยอมรับที่เกี่ยวข้องของมาตรฐานที่กำหนดไว้ในข้อ ๕.๒ ทั้งนี้ การประเมินขึ้นอยู่กับประเภทการรับรอง (Certification Scheme) และขอบข่ายที่ยื่นขอรับการรับรองด้วย

๖.๓.๒ สำนักงานยอมรับผลการตรวจสอบ ดังนี้

(๑) ผลการประเมินตนเอง (Self-assessment) ตามรูปแบบที่สำนักงานกำหนด เฉพาะกรณีผู้ใช้บริการคลาวด์ ที่จัดอยู่ในผลกระทบระดับต่ำ

(๒) ผลการตรวจประเมินหรือผลการรับรองจากหน่วยงานควบคุมหรือกำกับดูแล ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดหลักเกณฑ์ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมายการควบคุมและกำกับดูแล

(๓) ผลการตรวจประเมินหรือผลการรับรอง จากหน่วยตรวจสอบรับรองที่สำนักงานขึ้นทะเบียนไว้

๖.๔ ใบรับรอง

สำนักงานจะออกใบรับรองให้แก่ผู้ยื่นคำขอที่ผ่านการตรวจประเมินทุกหัวข้อแล้ว โดยในใบรับรองจะระบุรายละเอียดขอบข่ายของบริการคลาวด์ที่ให้การรับรอง ดังต่อไปนี้

ตารางที่ ๒ รายละเอียดขอบข่ายของผลิตภัณฑ์ที่จะระบุในใบรับรองคุณภาพผลิตภัณฑ์

ชื่อขอบข่าย	รายละเอียดที่จะระบุในใบรับรอง
ผู้ใช้บริการคลาวด์	- ชื่อผู้ใช้บริการคลาวด์ - ขอบเขตการใช้บริการคลาวด์ (Scope) - ประเภทข้อมูลหรือระบบสารสนเทศ
ผู้ให้บริการคลาวด์	- ชื่อผู้ให้บริการคลาวด์ - ชื่อบริการ - ขอบเขตการให้บริการคลาวด์ (Scope) - ประเภทข้อมูลหรือระบบสารสนเทศ

๖.๕ การแสดงเครื่องหมายรับรอง

รูปแบบและวิธีการแสดงเครื่องหมายรับรองคุณภาพผลิตภัณฑ์ให้เป็นไปตามที่กำหนดไว้ในหลักเกณฑ์และเงื่อนไขการใช้เครื่องหมายรับรอง

๗. การดำเนินการหลังได้รับการรับรอง

๗.๑ การตรวจติดตามผล

เพื่อให้บริการคลาวด์ที่ได้รับการรับรองของผู้ได้รับการรับรองเป็นไปตามข้อกำหนดเฉพาะในการรับรองฉบับนี้โดยสม่ำเสมอ จะมีการตรวจติดตามผลผู้ได้รับการรับรอง แบบหนึ่งแบบใด หรือหลายแบบรวมกัน ดังนี้

(๑) การตรวจประเมินระบบการควบคุมคุณภาพ /ระบบบริหารจัดการ ณ สถานประกอบการ

(๒) การประเมินกระบวนการในการให้บริการ

โดยมีรายละเอียดในข้อกำหนดทั่วไปในการรับรองคุณภาพผลิตภัณฑ์

๗.๒ เงื่อนไขที่ผู้ได้รับการรับรองต้องปฏิบัติ

ผู้ได้รับการรับรองต้องปฏิบัติตาม ข้อกำหนดทั่วไปในการรับรอง สำหรับการรับรองผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์ และหลักเกณฑ์และเงื่อนไขการใช้เครื่องหมายรับรอง รวมทั้งต้องปฏิบัติตามเงื่อนไข ดังต่อไปนี้

(๑) ผู้ได้รับการรับรองต้องจัดให้มีระบบตรวจสอบและควบคุมคุณภาพของบริการภายใต้ขอบข่ายที่ได้รับการรับรอง ให้เป็นไปตามข้อกำหนดเฉพาะในการรับรองฉบับนี้ตลอดเวลา รวมถึงต้องจัดเก็บข้อร้องเรียนและข้อบกพร่องที่เกี่ยวข้องกับคุณภาพบริการที่ได้รับการรับรองไว้ในแบบที่เหมาะสม

(๒) ผู้ได้รับการรับรอง (เฉพาะผู้ให้บริการคลาวด์) ต้องแจ้งปริมาณการให้บริการภายใต้ขอบข่ายที่ได้รับการรับรอง และจำนวนผลิตภัณฑ์ที่แสดงเครื่องหมายรับรอง ต่อสำนักงานภายในสัปดาห์ที่ ๒ ของทุก ๓ เดือน นับจากเดือนที่ได้รับการรับรอง พร้อมชำระค่าแสดงเครื่องหมายรับรองคุณภาพผลิตภัณฑ์ตามอัตราที่กำหนดไว้

หากผู้ได้รับการรับรองไม่ปฏิบัติตามเงื่อนไขที่สำนักงานกำหนด อาจถูกพักใช้ เพิกถอน หรือยกเลิกการรับรอง และดำเนินการอื่น ๆ ตามเงื่อนไขที่ประกาศแจ้งไว้แล้ว

ภาคผนวก ก

ตัวอย่างรายการตรวจประเมิน /มาตรการที่ใช้ในการควบคุมคุณภาพสำหรับบริการคลาวด์

ตารางที่ ก.๑ รายการตรวจประเมินผู้ใช้บริการ ตามมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์

ข้อ	รายการตรวจประเมิน	ข้อกำหนดอ้างอิง	ผู้ใช้บริการ (CSC)			สิ่งที่ตรวจพบ	ผล		
			ต่ำ	กลาง	สูง		C	N	NA
ส่วนที่ ๑ การกำกับดูแลด้านความมั่นคงปลอดภัยระบบคลาวด์									
๑	มีนโยบายด้านความมั่นคงปลอดภัยสารสนเทศสำหรับการประมวลผลคลาวด์ ที่ต้องสอดคล้องกับระดับความเสี่ยงด้านความมั่นคงปลอดภัย	๕.๑.๑ (ก)	✓	✓	✓				
๒	การกำหนดนโนบายต้องคำนึงถึงสิ่งที่กำหนดอย่างครบถ้วน	๕.๑.๑ (ข)	✓	✓	✓				
๓	นโนบายคุ้มครองข้อมูลส่วนบุคคลต้องระบุข้อความเกี่ยวกับข้อตกลงสัญญาระหว่างผู้ประมวลผลข้อมูลส่วนบุคคลบนคลาวด์และผู้ให้บริการคลาวด์	๕.๑.๑ (ค)	✓	✓	✓				
๔	ข้อตกลงสัญญาต้องกำหนดความรับผิดชอบระหว่างผู้ประมวลผลข้อมูลส่วนบุคคล ผู้รับจ้างช่วง และผู้ให้บริการคลาวด์	๕.๑.๑ (ง)	✓	✓	✓				
๕	มีโครงสร้างองค์กรด้านความมั่นคงสารสนเทศ	๕.๑.๒	✓	✓	✓				
๖	มีข้อตกลงกับผู้ให้บริการคลาวด์เกี่ยวกับการแบ่งหน้าที่และความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ	๕.๑.๒.๑ (ก)	✓	✓	✓				
๗	ต้องระบุและจัดการความสัมพันธ์กับส่วนงานสนับสนุนลูกค้าและฟังก์ชันการดูแลของผู้ให้บริการคลาวด์	๕.๑.๒.๑ (ข)	✓	✓	✓				
๘	ต้องระบุหน่วยงานที่ต้องดำเนินงานร่วมกับผู้ให้บริการ	๕.๑.๒.๒	✓	✓	✓				
๙	การปฏิบัติตามกฎ ระเบียบ ข้อบังคับ	๕.๑.๓		✓	✓				
๑๐	ผู้ใช้บริการคลาวด์ต้องพิจารณากฎหมายและข้อบังคับที่ครอบคลุมผู้ให้บริการคลาวด์ตามขอบเขตอำนาจศาล	๕.๑.๓.๑ (ก)		✓	✓				
๑๑	ต้องขอหลักฐานที่แสดงว่าผู้ให้บริการคลาวด์ปฏิบัติตามกฎระเบียบ และมาตรฐานที่เกี่ยวข้อง	๕.๑.๓.๑ (ข)		✓	✓				
๑๒	ต้องมีขั้นตอนในการให้สิทธิการใช้งานซอฟต์แวร์ที่อาจมีผลกระทบต่อสิทธิในทรัพย์สินทางปัญญา	๕.๑.๓.๒		✓	✓				
๑๓	ต้องขอข้อมูลจากผู้ให้บริการคลาวด์เกี่ยวกับการปกป้องบันทึกข้อมูลที่รวบรวมและจัดเก็บโดยผู้ให้บริการคลาวด์	๕.๑.๓.๓		✓	✓				
๑๔	ต้องตรวจสอบให้มั่นใจว่าชุดของมาตรการควบคุมการเข้ารหัสข้อมูลสอดคล้องกับข้อตกลง กฎหมาย และระเบียบข้องบังคับที่เกี่ยวข้อง	๕.๑.๓.๔		✓	✓				
๑๕	ต้องขอหลักฐานที่เป็นเอกสารว่ามีการนำมาตรการควบคุมและแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศสำหรับบริการคลาวด์ไปปฏิบัติ	๕.๑.๓.๕		✓	✓				

ตารางที่ ก.๑ รายการตรวจประเมินผู้ใช้บริการ ตามมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ (ต่อ)

ข้อ	รายการตรวจประเมิน	ข้อกำหนดอ้างอิง	ผู้ใช้บริการ (CSC)			สิ่งที่ตรวจพบ	ผล		
			ต่ำ	กลาง	สูง		C	N	NA
ส่วนที่ ๒ การปฏิบัติและการรักษาความมั่นคงปลอดภัยโครงสร้างพื้นฐานระบบคลาวด์									
๑๖	การบริหารทรัพยากรมนุษย์	๕.๒.๑	✓	✓	✓				
๑๗	ต้องสร้างความตระหนักรู้ การอบรมให้แก่บุคลากรที่เกี่ยวข้อง	๕.๒.๑.๑ (ก)	✓	✓	✓				
๑๘	ต้องสร้างความตระหนักรู้ แก่ผู้บริหาร ผู้จัดการ รวมถึงหน่วยงานธุรกิจ	๕.๒.๑.๑ (ข)	✓	✓	✓				
๑๙	การจัดการทรัพย์สิน	๕.๒.๒	✓	✓	✓				
๒๐	ต้องมีการจัดทำทะเบียนทรัพย์สิน โดยต้องคำนึงถึงข้อมูลและทรัพย์สิน ซึ่งจัดเก็บในสภาพแวดล้อมการประมวลผลบนคลาวด์ บันทึกทะเบียนทรัพย์สินต้องระบุสถานที่จัดเก็บทรัพย์สิน	๕.๒.๒.๑	✓	✓	✓				
๒๑	ต้องชี้บ่งข้อมูลและทรัพย์สินขององค์กรที่ใช้งานหรือเก็บรักษาไว้บนคลาวด์	๕.๒.๒.๒	✓	✓	✓				
๒๒	การควบคุมการเข้าถึง	๕.๒.๓	✓	✓	✓				
๒๓	มีนโบายการควบคุมการเข้าถึงที่ระบุถึงข้อกำหนดสำหรับผู้ใช้งานในการเข้าถึงบริการคลาวด์	๕.๒.๓.๑	✓	✓	✓				
๒๔	มีขั้นตอนการลงทะเบียนและยกเลิกการลงทะเบียนสำหรับผู้ใช้ ที่ครอบคลุมสถานการณ์ที่การควบคุมการเข้าถึงของผู้ใช้ถูกคุกคาม	๕.๒.๓.๒	✓	✓	✓				
๒๕	การจัดสรรการเข้าถึงของผู้ใช้	๕.๒.๓.๓							
๒๖	ต้องใช้เทคนิคการยืนยันตัวตนที่เพียงพอสำหรับการตรวจสอบสิทธิของผู้ดูแลระบบของผู้ใช้บริการคลาวด์	๕.๒.๓.๔	✓	✓	✓				
๒๗	ต้องตรวจสอบว่ากระบวนการจัดการของผู้ให้บริการคลาวด์สำหรับการจัดสรรข้อมูลการตรวจสอบความลับเป็นไปตามข้อกำหนดของผู้ใช้บริการคลาวด์	๕.๒.๓.๕	✓	✓	✓				
๒๘	ต้องตรวจสอบให้แน่ใจว่าสามารถจำกัดการเข้าถึงข้อมูลในระบบคลาวด์ได้ตามนโยบายที่กำหนด	๕.๒.๓.๖	✓	✓	✓				
๒๙	หากอนุญาตให้ใช้โปรแกรมอรรถประโยชน์ได้ ต้องระบุโปรแกรมฯที่จะใช้ในสภาพแวดล้อมการประมวลผลบนคลาวด์และตรวจสอบให้มั่นใจว่า ไม่รบกวนการควบคุมของบริการคลาวด์	๕.๒.๓.๗	✓	✓	✓				
๓๐	ต้องกำหนดให้ผู้ใช้ที่อยู่ภายใต้การควบคุมของผู้ใช้บริการตลาวด์ปฏิบัติตามขั้นตอนการเข้าสู่ระบบอย่างปลอดภัย	๕.๒.๓.๘	✓	✓	✓				
๓๑	การเข้ารหัส	๕.๒.๔	✓	✓	✓				

ตารางที่ ก.๑ รายการตรวจประเมินผู้ใช้บริการ ตามมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ (ต่อ)

ข้อ	รายการตรวจประเมิน	ข้อกำหนดอ้างอิง	ผู้ใช้บริการ (CSC)			สิ่งที่ตรวจพบ	ผล		
			ต่ำ	กลาง	สูง		C	N	NA
๓๒	ต้องใช้มาตรการควบคุมการเข้ารหัสสำหรับการใช้บริการคลาวด์ที่แข็งแรงเพียงพอ และสอดคล้องตามความเสี่ยง	๕.๒.๔.๑ (ก)	✓	✓	✓				
๓๓	เมื่อผู้ให้บริการคลาวด์เสนอการเข้ารหัสใดๆ ผู้ให้บริการคลาวด์ต้องตรวจสอบข้อมูลเพื่อยืนยันความสามารถในการเข้ารหัส	๕.๒.๔.๑ (ข)	✓	✓	✓				
๓๔	ต้องระบุกุญแจสำหรับการเข้ารหัสในแต่ละบริการคลาวด์ และดำเนินการตามขั้นตอนการจัดการกุญแจ	๕.๒.๔.๒ (ก)	✓	✓	✓				
๓๕	ในกรณีที่คลาวด์มีฟังก์ชันการจัดการกุญแจ ต้องขอข้อมูลเกี่ยวกับขั้นตอนการจัดการกุญแจตามที่กำหนด	๕.๒.๔.๒ (ข)							
๓๖	ต้องไม่อนุญาตให้ผู้ให้บริการคลาวด์ จัดเก็บการจัดการกุญแจสำหรับการเข้ารหัส เมื่อผู้ใช้บริการคลาวด์ ใช้กุญแจเข้ารหัสของตนเอง	๕.๒.๔.๒ (ค)	✓	✓	✓				
๓๗	การรักษาความปลอดภัยทางกายภาพและสภาพแวดล้อม	๕.๒.๕			✓				
๓๘	ต้องใช้ศูนย์ข้อมูลหลักในประเทศไทย	๕.๒.๕.๑			✓				
๓๙	ต้องร้องขอการยืนยันว่าผู้ให้บริการคลาวด์มีนโยบายและขั้นตอนการในการกำจัดหรือนำทรัพยากรกลับมาใช้ใหม่อย่างปลอดภัย	๕.๒.๕.๒			✓				
๔๐	การรักษาความมั่นคงปลอดภัยการปฏิบัติการ	๕.๒.๖			✓				
๔๑	กระบวนการจัดการการเปลี่ยนแปลงของผู้ใช้บริการคลาวด์ ต้องคำนึงถึงผลกระทบของการเปลี่ยนแปลงที่เกิดจากผู้ให้บริการคลาวด์	๕.๒.๖.๑							
๔๒	ต้องตรวจสอบให้แน่ใจว่าขีดความสามารถของทรัพยากรที่ตกลงกันไว้ ตรงตามข้อกำหนดของผู้ใช้บริการคลาวด์	๕.๒.๖.๒ (ก)			✓				
๔๓	ต้องตรวจสอบการใช้บริการคลาวด์และคาดการณ์ความต้องการด้านขีดความสามารถของทรัพยากร	๕.๒.๖.๒ (ข)			✓				
๔๔	ในกรณีที่ผู้ให้บริการคลาวด์มีความสามารถในการสำรองข้อมูล ซึ่งเป็นส่วนหนึ่งของบริการคลาวด์ ผู้ใช้บริการคลาวด์จ้องขอข้อมูลจำเพาะของความสามารถในการสำรองข้อมูล และต้องตรวจสอบว่าการสำรองข้อมูลเป็นไปตามข้อกำหนด	๕.๒.๖.๓ (ก)			✓				
๔๕	ต้องรับผิดชอบการสำรองข้อมูล เมื่อผู้ให้บริการไม่ได้ให้บริการ	๕.๒.๖.๓ (ข)			✓				
๔๖	ต้องจัดทำข้อกำหนดสำหรับการบันทึกเหตุการณ์และตรวจสอบว่าบริการคลาวด์ตรงตามข้อกำหนด	๕.๒.๖.๔			✓				

ตารางที่ ก.๑ รายการตรวจประเมินผู้ใช้บริการ ตามมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ (ต่อ)

ข้อ	รายการตรวจประเมิน	ข้อกำหนดอ้างอิง	ผู้ใช้บริการ (CSC)			สิ่งที่ตรวจพบ	ผล		
			ต่ำ	กลาง	สูง		C	N	NA
๔๗	บันทึกเหตุการณ์ อาจมีข้อมูลส่วนบุคคลอยู่ด้วย ต้องมีมาตรการเพื่อให้มั่นใจว่าบันทึกนั้นถูกนำไปใช้ตามวัตถุประสงค์ที่ตั้งไว้เท่านั้น	๕.๒.๖.๕ (ก)			✓				
๔๘	ต้องมีขั้นตอนการดำเนินการ เพื่อให้มั่นใจว่าข้อมูลที่บันทึกไว้ในบันทึกเหตุการณ์จะถูกลบภายในระยะเวลาที่กำหนด และเอกสารระบุไว้	๕.๒.๖.๕ (ข)			✓				
๔๙	หากมีการให้สิทธิพิเศษแก่ผู้ใช้บริการคลาวด์ ต้องมีการบันทึกเหตุการณ์และประสิทธิภาพของการดำเนินการ ผู้ใช้บริการคลาวด์ต้องพิจารณาว่าความสามารถในการบันทึกเหตุการณ์ที่ผู้ให้บริการจัดหาให้เหมาะสมหรือไม่ หรือผู้ใช้บริการต้องบันทึกเหตุการณ์เพิ่มเติมหรือไม่	๕.๒.๖.๖			✓				
๕๐	ต้องขอข้อมูลเกี่ยวกับการซิงโครไนซ์นาฬิกาที่ใช้ในระบบของผู้ให้บริการคลาวด์	๕.๒.๖.๗			✓				
๕๑	ต้องขอข้อมูลจากผู้ให้บริการคลาวด์ เกี่ยวกับการจัดการช่องโหว่ทางเทคนิคที่อาจส่งผลกระทบต่อบริการคลาวด์ ต้องระบุช่องโหว่ทางเทคนิคที่ผู้ใช้บริการคลาวด์ จะเป็นผู้รับผิดชอบในการจัดการและกำหนดกระบวนการในการจัดการให้ชัดเจน	๕.๒.๖.๘			✓				
๕๒	ในกรณีที่ไม่สามารถหลีกเลี่ยงการใช้ข้อมูลส่วนบุคคลสำหรับวัตถุประสงค์ในการทดสอบได้ ต้องมีการประเมินความเสี่ยง มาตรการด้านเทคนิคและการจัดการองค์กรต้องถูกนำมาใช้เพื่อลดความเสี่ยง	๕.๒.๖.๙			✓				
๕๓	การรักษาความมั่นคงปลอดภัยเครือข่าย	๕.๒.๗		✓	✓				
๕๔	เมื่อมีการใช้สื่อทางกายภาพสำหรับการถ่ายโอนข้อมูล ต้องมีระบบที่จะบันทึกสื่อทางการกายภาพที่เข้ามาและออกไป	๕.๒.๗.๑ (ก)		✓	✓				
๕๕	ต้องขอให้ผู้ให้บริการคลาวด์ใช้มาตรการเพิ่มเติมเพื่อให้มั่นใจว่าข้อมูลสามารถเข้าถึงได้เฉพาะจุดปลายทางเท่านั้น	๕.๒.๗.๑ (ข)			✓				
๕๖	ต้องจัดทำข้อกำหนดสำหรับการแยกเครือข่ายเพื่อให้เกิดการแยกผู้เช่าในสภาพแวดล้อมที่เป็นการใช้บริการคลาวด์ร่วมกัน และตรวจสอบว่าผู้ให้บริการคลาวด์มีคุณสมบัติตรงตามข้อกำหนด	๕.๒.๗.๒							
๕๗	การจัดหา การพัฒนา และการบำรุงรักษา	๕.๒.๘	✓	✓	✓				
๕๘	ต้องกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศสำหรับการใช้บริการคลาวด์	๕.๒.๘.๑ (ก)	✓	✓	✓				

ตารางที่ ก.๑ รายการตรวจประเมินผู้ใช้บริการ ตามมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ (ต่อ)

ข้อ	รายการตรวจประเมิน	ข้อกำหนดอ้างอิง	ผู้ใช้บริการ (CSC)			สิ่งที่ตรวจพบ	ผล		
			ต่ำ	กลาง	สูง		C	N	NA
๕๙	ต้องขอข้อมูลเกี่ยวกับความสามารถในการรักษาความมั่นคงปลอดภัยสารสนเทศจากผู้ให้บริการคลาวด์	๕.๒.๘.๑ (ข)	✓	✓	✓				
๖๐	ต้องขอข้อมูลจากผู้ให้บริการคลาวด์ เกี่ยวกับการใช้ขั้นตอนและวิธีปฏิบัติในการพัฒนาที่ปลอดภัยของผู้ให้บริการคลาวด์	๕.๒.๘.๒	✓	✓	✓				
๖๑	การจัดการผู้ให้บริการภายนอก	๕.๒.๙	✓	✓	✓				
๖๒	ต้องระบุว่าผู้ให้บริการคลาวด์เป็นผู้ให้บริการภายนอกประเภทหนึ่ง ในนโยบายความมั่นคงปลอดภัยสารสนเทศ	๕.๒.๙.๑	✓	✓	✓				
๖๓	ต้องยืนยันบทบาทและความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับบริการคลาวด์ในกระบวนการที่กำหนด	๕.๒.๙.๒	✓	✓	✓				
๖๔	ห่วงโซ่อุปทานของเทคโนโลยีสารสนเทศและการสื่อสาร	๕.๒.๙.๓							
๖๕	การจัดการเหตุภัยคุกคามทางสารสนเทศ	๕.๒.๑๐		✓	✓				
๖๖	ต้องตรวจสอบการจัดสรรความรับผิดชอบในการจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อให้มั่นใจว่าเป็นไปตามข้อกำหนดของผู้ใช้บริการคลาวด์	๕.๒.๑๐.๑ (ก)		✓	✓				
๖๗	เหตุภัยคุกคามทางสารสนเทศต้องนำไปสู่การทบทวนโดยใช้ผู้บริการคลาวด์ หรือทบทวนร่วมกันระหว่างผู้ให้บริการคลาวด์และผู้ใช้บริการคลาวด์ เพื่อพิจารณาว่ามีการละเมิดข้อมูลส่วนบุคคลหรือไม่	๕.๒.๑๐.๑ (ข)		✓	✓				
๖๘	ต้องขอข้อมูลจากผู้ให้บริการเกี่ยวกับการรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ	๕.๒.๑๐.๒		✓	✓				

ตารางที่ ก.๒ รายการตรวจประเมินผู้ให้บริการ ตามมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์

ข้อ	รายการตรวจประเมิน	ข้อกำหนดอ้างอิง	ผู้ให้บริการ (CSP)			สิ่งที่ตรวจพบ	ผล		
			ต่ำ	กลาง	สูง		C	N	NA
ส่วนที่ ๑ การกำกับดูแลด้านความมั่นคงปลอดภัยระบบคลาวด์									
๑	มีนโยบายด้านความมั่นคงปลอดภัยสารสนเทศเพื่อจัดการกับการจัดหาและใช้บริการคลาวด์	๕.๑.๑	✓	✓	✓				
๒	มีโครงสร้างองค์กรด้านความมั่นคงสารสนเทศ	๕.๑.๒	✓	✓	✓				
๓	ต้องตกลงและบันทึกการแบ่งบทบาทหน้าที่และความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศที่เหมาะสมกับผู้ใช้บริการ ผู้ให้บริการคลาวด์และผู้ให้บริการภายนอก	๕.๑.๒.๑ (ก)	✓	✓	✓				
๔	ต้องแต่งตั้งผู้ประสานงานด้านการคุ้มครองข้อมูลส่วนบุคคล เพื่อประสานงานกับผู้ใช้บริการคลาวด์	๕.๑.๒.๑ (ข)	✓	✓	✓				
๕	ควรแจ้งให้ผู้ใช้บริการทราบถึงที่ตั้งทางภูมิศาสตร์ขององค์กรที่เป็นเจ้าของผู้ให้บริการคลาวด์ และประเทศผู้ให้บริการคลาวด์สามารถจัดเก็บข้อมูลผู้ใช้บริการคลาวด์ได้	๕.๑.๒.๒	✓	✓	✓				
๖	การปฏิบัติตามกฎ ระเบียบ ข้อบังคับ	๕.๑.๓		✓	✓				
๗	ต้องแจ้งให้ผู้ใช้บริการคลาวด์ทราบถึงเขตอำนาจศาลทางกฎหมายที่ควบคุมบริการคลาวด์	๕.๑.๓.๑ (ก)		✓	✓				
๘	ต้องระบุข้อกำหนดทางกฎหมายที่เกี่ยวข้องของตนเองและต้องให้ข้อมูลนี้แก่ผู้ใช้บริการคลาวด์เมื่อได้รับการร้องขอ	๕.๑.๓.๑ (ข)		✓	✓				
๙	ต้องแสดงหลักฐานให้ผู้ใช้บริการคลาวด์ทราบถึงการปฏิบัติตามกฎหมายที่บังคับใช้ในปัจจุบันและข้อกำหนดตามสัญญา	๕.๑.๓.๑ (ค)		✓	✓				
๑๐	ต้องกำหนดกระบวนการในการตอบสนองต่อการร้องเรียนเรื่องสิทธิในทรัพย์สินทางปัญญา	๕.๑.๓.๒		✓	✓				
๑๑	ต้องให้ข้อมูลแก่ผู้ใช้บริการคลาวด์เกี่ยวกับการปกป้องบันทึกข้อมูลที่รวบรวมและจัดเก็บโดยผู้ให้บริการคลาวด์	๕.๑.๓.๓		✓	✓				
๑๒	ต้องให้คำอธิบายกับผู้ใช้บริการคลาวด์ เกี่ยวกับมาตรการควบคุมการเข้ารหัสข้อมูลที่ดำเนินการโดยผู้ให้บริการคลาวด์	๕.๑.๓.๔		✓	✓				
๑๓	ต้องให้หลักฐานที่เป็นเอกสารแก่ผู้ใช้บริการคลาวด์เพื่อยืนยันข้อเรียกร้องของผู้ให้บริการคลาวด์ ในการนำมาตรการควบคุมความมั่นคงปลอดภัยสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคล	๕.๑.๓.๕ (ก)		✓	✓				
๑๔	ต้องแสดงหลักฐานที่เป็นอิสระว่ามีการนำไปปฏิบัติและดำเนินการด้านความมั่นคงปลอดภัยสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคล	๕.๑.๓.๕ (ข)		✓	✓				

ตารางที่ ก.๒ รายการตรวจประเมินผู้ให้บริการ ตามมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ (ต่อ)

ข้อ	รายการตรวจประเมิน	ข้อกำหนดอ้างอิง	ผู้ให้บริการ (CSP)			สิ่งที่ตรวจพบ	ผล		
			ต่ำ	กลาง	สูง		C	N	NA
ส่วนที่ ๒ การปฏิบัติและการรักษาความมั่นคงปลอดภัยโครงสร้างพื้นฐานระบบคลาวด์									
๑๕	การบริหารทรัพยากรมนุษย์	๕.๒.๑	✓	✓	✓				
๑๖	ต้องสร้างความตระหนักรู้ ด้านความมั่นคงปลอดภัย สารสนเทศและการคุ้มครองข้อมูลส่วนบุคคล แก่พนักงาน รวมทั้งผู้รับจ้าง	๕.๒.๑.๑	✓	✓	✓				
๑๗	การจัดการทรัพย์สิน	๕.๒.๒	✓	✓	✓				
๑๘	ทะเบียนทรัพย์สินของผู้ให้บริการต้องระบุให้ชัดเจนในเรื่อง - ข้อมูลของผู้ใช้บริการคลาวด์ - ข้อมูลที่เกิดจาการใช้บริการคลาวด์	๕.๒.๒.๑	✓	✓	✓				
๑๙	ต้องจัดทำเอกสารและเปิดเผยฟังก์ชันการทำงานของบริการใด ๆ ที่ผู้ใช้บริการคลาวด์ สามารถนำไปใช้เพื่อการบ่งชี้ข้อมูลและทรัพย์สินที่เกี่ยวข้องได้	๕.๒.๒.๒	✓	✓	✓				
๒๐	การควบคุมการเข้าถึง	๕.๒.๓	✓	✓	✓				
๒๑	การควบคุมการเข้าถึงเครือข่ายและบริการเครือข่าย	๕.๒.๓.๑							
๒๒	ต้องจัดเตรียมฟังก์ชันการลงทะเบียนและการยกเลิกการลงทะเบียนผู้ใช้งาน รวมถึงข้อกำหนดสำหรับการใช้งานฟังก์ชันนี้แก่ ผู้ใช้บริการคลาวด์	๕.๒.๓.๒	✓	✓	✓				
๒๓	ต้องจัดเตรียมฟังก์ชันสำหรับการจัดการสิทธิการเข้าถึงของผู้ใช้บริการคลาวด์รวมถึงข้อกำหนดสำหรับการใช้งานฟังก์ชันเหล่านี้	๕.๒.๓.๓	✓	✓	✓				
๒๔	ต้องมีเทคนิคการยืนยันตัวตนที่เพียงพอ สำหรับการตรวจสอบสิทธิของผู้ดูแลระบบของผู้ใช้บริการคลาวด์	๕.๒.๓.๔	✓	✓	✓				
๒๕	ต้องให้ข้อมูลเกี่ยวกับขั้นตอนการจัดการข้อมูลการตรวจสอบความลับ ของผู้ใช้บริการคลาวด์ รวมถึงขั้นตอนในการจัดสรรข้อมูลสำหรับการตรวจสอบสิทธิผู้ใช้งาน	๕.๒.๓.๕	✓	✓	✓				
๒๖	ต้องให้การควบคุมการเข้าถึงที่อนุญาตให้กับผู้ใช้บริการคลาวด์ เพื่อจำกัดการเข้าถึงบริการต่างๆ บนระบบคลาวด์ และข้อมูลผู้ใช้บริการคลาวด์ที่เก็บไว้ในบริการ	๕.๒.๓.๖	✓	✓	✓				
๒๗	ต้องระบุข้อกำหนดสำหรับโปรแกรมอรรถประโยชน์ต้องตรวจสอบให้มั่นใจว่าการใช้โปรแกรมฯ ที่สามารถข้ามขั้นตอนการทำงานตามปกติหรือการรักษาความปลอดภัยจำกัดเฉพาะบุคลากรที่ได้รับอนุญาตเท่านั้น	๕.๒.๓.๗	✓	✓	✓				
๒๘	ในกรณีที่จำเป็น ต้องมีการตัดให้มีขั้นตอนการเข้าสู่ระบบอย่างปลอดภัยสำหรับบัญชีที่ผู้ใช้บริการคลาวด์ร้องขอ	๕.๒.๓.๘	✓	✓	✓				
๒๙	การเข้ารหัส	๕.๒.๔	✓	✓	✓				

ตารางที่ ก.๒ รายการตรวจประเมินผู้ให้บริการ ตามมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ (ต่อ)

ข้อ	รายการตรวจประเมิน	ข้อกำหนดอ้างอิง	ผู้ให้บริการ (CSP)			สิ่งที่ตรวจพบ	ผล		
			ต่ำ	กลาง	สูง		C	N	NA
๓๐	ต้องให้ข้อมูลเกี่ยวกับการเข้ารหัสเพื่อปกป้องข้อมูลและข้อมูลส่วนบุคคล ที่ผู้ให้บริการคลาวด์ประมวลผล ผู้ให้บริการต้องให้ข้อมูลแก่ผู้ใช้บริการคลาวด์เกี่ยวกับความสามารถที่ผู้ให้บริการมอบให้ ซึ่งสามารถช่วยให้ผู้ใช้บริการคลาวด์ในการใช้การเข้ารหัส	๕.๒.๔.๑	✓	✓	✓				
๓๑	การรักษาความปลอดภัยทางกายภาพและสภาพแวดล้อม	๕.๒.๕			✓				
๓๒	ต้องจัดตั้งศูนย์ข้อมูลหลักในประเทศไทย	๕.๒.๕.๑ (ก)			✓				
๓๓	ต้องจัดตั้งศูนย์ข้อมูลสำรองในประเทศไทย หรือในภูมิภาคเอเชียตะวันออกเฉียงใต้ที่ใกล้กับการใช้งานหลักของผู้ใช้บริการคลาวด์ให้มากที่สุด รวมถึงสิงคโปร์และเขตการปกครองพิเศษฮ่องกง	๕.๒.๕.๑ (ข)			✓				
๓๔	ต้องตรวจสอบให้แน่ใจว่ามีการจัดเตรียมการสำหรับการกำจัดหรือนำทรัพยากรกลับมาใช้อย่างปลอดภัย	๕.๒.๕.๒ (ก)			✓				
๓๕	อุปกรณ์ที่มีสื่อจัดเก็บข้อมูลส่วนบุคคลต้องได้รับการปฏิบัติเสมือนมีข้อมูลส่วนบุคคลจริง	๕.๒.๕.๒ (ข)			✓				
๓๖	การรักษาความมั่นคงปลอดภัยการปฏิบัติการ	๕.๒.๖			✓				
๓๗	ต้องให้ข้อมูลการเปลี่ยนแปลงในบริการคลาวด์ที่อาจส่งผลเสีย ให้ผู้ใช้บริการคลาวด์ ทราบ	๕.๒.๖.๑ (ก)			✓				
๓๘	เมื่อผู้ให้บริการคลาวด์ ให้บริการคลาวด์ที่ขึ้นอยู่กับผู้ใช้บริการรายย่อย ผู้ให้บริการคลาวด์อาจจำเป็นต้องแจ้งการเปลี่ยนแปลงที่เกิดขึ้นให้ผู้ใช้บริการทราบ	๕.๒.๖.๑ (ข)			✓				
๓๙	ต้องตรวจสอบขีดความสามารถของทรัพยากรทั้งหมดเพื่อป้องกันไม่ให้เกิดเหตุการณ์ด้านความมั่งคงปลอดภัย	๕.๒.๖.๒			✓				
๔๐	ต้องให้ข้อมูลจำเพาะของความสามารถในการสำรองข้อมูลแก่ผู้ใช้บริการ	๕.๒.๖.๓ (ก)			✓				
๔๑	ต้องให้บริการการเข้าถึงข้อมูลสำรองที่ปลอดภัยและแยกออกจากกัน หากบริการดังกล่าวมีการนำเสนอให้ผู้ใช้บริการ	๕.๒.๖.๓ (ข)			✓				
๔๒	ต้องให้ผู้ใช้บริการสามารถบันทึกเหตุการณ์ได้	๕.๒.๖.๔ (ก)			✓				
๔๓	ในกรณีที่เป็นไปได้ บันทึกเหตุการณ์ควรบันทึกว่าข้อมูลส่วนบุคคลได้รับการเปลี่ยนแปลงหรือไม่ โดยใคร	๕.๒.๖.๔ (ข)			✓				
๔๔	บันทึกเหตุการณ์ อาจมีข้อมูลส่วนบุคคลอยู่ด้วย ต้องมีมาตรการเพื่อให้มั่นใจว่าบันทึกนั้นถูกนำไปใช้ตามวัตถุประสงค์ที่ตั้งไว้เท่านั้น	๕.๒.๖.๕ (ก)			✓				

ตารางที่ ก.๒ รายการตรวจประเมินผู้ให้บริการ ตามมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ (ต่อ)

ข้อ	รายการตรวจประเมิน	ข้อกำหนดอ้างอิง	ผู้ให้บริการ (CSP)			สิ่งที่ตรวจพบ	ผล		
			ต่ำ	กลาง	สูง		C	N	NA
๔๕	ต้องมีขั้นตอนการดำเนินการ เพื่อให้มั่นใจว่าข้อมูลที่บันทึกไว้ในบันทึกเหตุการณ์จะถูกลบภายในระยะเวลาที่กำหนด และเอกสารระบุไว้	๕.๒.๖.๕ (ข)			✓				
๔๖	บันทึกเหตุการณ์ของผู้ดูแลระบบและผู้ปฏิบัติงาน	๕.๒.๖.๖							
๔๗	ต้องให้ข้อมูลเกี่ยวกับนาฬิกาที่ระบบของผู้ให้บริการคลาวด์ใช้ และข้อมูลเกี่ยวกับวิธีการที่ผู้ใช้บริการคลาวด์สามารถซิงโครไนซ์นาฬิกาในบริการคลาวด์	๕.๒.๖.๗			✓				
๔๘	ต้องให้ข้อมูลผู้ใช้บริการคลาวด์ เกี่ยวกับการจัดการช่องโหว่ทางเทคนิคที่อาจส่งผลกระทบต่อบริการคลาวด์ที่ให้บริการ	๕.๒.๖.๘			✓				
๔๙	ในกรณีที่ไม่สามารถหลีกเลี่ยงการใช้ข้อมูลส่วนบุคคลสำหรับวัตถุประสงค์ในการทดสอบได้ ต้องมีการประเมินความเสี่ยง มาตรการด้านเทคนิคและการจัดการองค์กรต้องถูกนำมาใช้เพื่อลดความเสี่ยง	๕.๒.๖.๙			✓				
๕๐	การรักษาความมั่นคงปลอดภัยเครือข่าย	๕.๒.๗		✓	✓				
๕๑	เมื่อมีการใช้สื่อทางกายภาพสำหรับการถ่ายโอนข้อมูล ต้องมีระบบที่จะบันทึกสื่อทางการกายภาพที่เข้ามาและออกไป	๕.๒.๗.๑ (ก)		✓	✓				
๕๒	หากเป็นไปได้ ต้องขอให้ผู้ใช้บริการคลาวด์ใช้มาตรการเพิ่มเติม เพื่อให้มั่นใจว่าข้อมูลสามารถเข้าถึงได้เฉพาะจุดปลายทางเท่านั้น	๕.๒.๗.๑ (ข)		✓	✓				
๕๓	ต้องบังคับใช้การแยกการเข้าถึงเครือข่าย	๕.๒.๗.๒ (ก)		✓	✓				
๕๔	ต้องช่วยผู้ใช้บริการคลาวด์ตรวจสอบการแบ่งแยกที่ดำเนินการโดยผู้ให้บริการคลาวด์	๕.๒.๗.๒ (ข)		✓	✓				
๕๕	การจัดหา การพัฒนา และการบำรุงรักษา	๕.๒.๘	✓	✓	✓				
๕๖	ต้องให้ข้อมูลแก่ผู้ใช้บริการคลาวด์ เกี่ยวกับความสามารถในการรักษาความมั่นคงปลอดภัย สารสนเทศที่ใช้ ข้อมูลต้องเป็นข้อมูลไม่เปิดเผยที่อาจเป็นประโยชน์ต่อผู้ที่มีเจตนาร้าย	๕.๒.๘.๑	✓	✓	✓				
๕๗	ต้องให้ข้อมูลเกี่ยวกับการใช้ขั้นตอนและวิธีปฏิบัติในการพัฒนาที่ปลอดภัย ในขอบเขตที่สอดคล้องกับนโยบายในการเปิดเผยข้อมูล	๕.๒.๘.๒	✓	✓	✓				
๕๘	การจัดการผู้ให้บริการภายนอก	๕.๒.๙	✓	✓	✓				

ตารางที่ ก.๒ รายการตรวจประเมินผู้ให้บริการ ตามมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ (ต่อ)

ข้อ	รายการตรวจประเมิน	ข้อกำหนดอ้างอิง	ผู้ให้บริการ (CSP)			สิ่งที่ตรวจพบ	ผล		
			ต่ำ	กลาง	สูง		C	N	NA
๕๙	โยบายความมั่นคงปลอดภัยสารสนเทศสำหรับความสัมพันธ์กับผู้ให้บริการภายนอก	๕.๒.๙							
๖๐	ต้องระบุมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้อง ซึ่งจะนำมาใช้เป็นส่วนหนึ่งของข้อตกลงเพื่อให้แน่ใจว่าจะไม่เกิดความเข้าใจผิดระหว่างผู้ให้บริการคลาวด์และผู้ใช้บริการคลาวด์	๕.๒.๙.๒ (ก)	✓	✓	✓				
๖๑	มาตรการรักษาความมั่นคงปลอดภัยสารสนเทศที่ผู้ให้บริการคลาวด์จะใช้ อาจแตกต่างกันออกไปตามประเภทของบริการคลาวด์	๕.๒.๙.๒ (ข)	✓	✓	✓				
๖๒	หากมีการใช้บริการคลาวด์ของผู้ให้บริการรายย่อย ผู้ให้บริการคลาวด์ต้องตรวจสอบให้แน่ใจว่าระดับความมั่นคงปลอดภัยสารสนเทศของผู้ให้บริการรายย่อยได้รับการดูแลไม่ต่ำกว่าผู้ใช้บริการคลาวด์	๕.๒.๙.๓ (ก)	✓	✓	✓				
๖๓	เมื่อผู้ให้บริการคลาวด์ ให้บริการตามห่วงโซ่อุปทาน ผู้ให้บริการคลาวด์ต้องกำหนดวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศแก่ผู้ให้บริการภายนอก และขอให้ผู้ให้บริการภายนอกแต่ละรายดำเนินกิจกรรมการบริหารความเสี่ยง	๕.๒.๙.๓ (ข)	✓	✓	✓				
๖๔	การจัดการเหตุภัยคุกคามทางสารสนเทศ	๕.๒.๑๐		✓	✓				
๖๕	ต้องกำหนดขอบเขตความรับผิดชอบและขั้นตอนการจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศระหว่างผู้ใช้บริการคลาวด์ และผู้ให้บริการคลาวด์ โดยเป็นส่วนหนึ่งของข้อกำหนดบริการ	๕.๒.๑๐.๑ (ก)		✓	✓				
๖๖	ต้องจัดเตรียมเอกสารให้ผู้ใช้บริการคลาวด์ ตามที่กำหนด	๕.๒.๑๐.๑ (ข)		✓	✓				
๖๗	เหตุภัยคุกคามทางสารสนเทศต้องนำไปสู่การทบทวนโดยผู้ใช้บริการคลาวด์	๕.๒.๑๐.๑ (ค)		✓	✓				
๖๘	ต้องมีกลไกสำหรับ - ผู้ใช้บริการคลาวด์ รายงานเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศต่อผู้ให้บริการ - ผู้ให้บริการคลาวด์ เพื่อรายงานเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศต่อผู้ใช้บริการคลาวด์ - ผู้ใช้บริการคลาวด์ เพื่อติดตามสถานะของเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศที่รายงาน	๕.๒.๑๐.๒		✓	✓				