



ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์
พ.ศ. ๒๕๖๗

โดยที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติมีหน้าที่และอำนาจสร้างมาตรฐานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ และกำหนดมาตรฐานขั้นต่ำที่เกี่ยวข้องกับคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือโปรแกรมคอมพิวเตอร์ จึงสมควรมีมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ เพื่อให้การดำเนินงานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นไปอย่างมีประสิทธิภาพ

อาศัยอำนาจตามความในมาตรา ๙ (๔) แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ประกอบกับมติที่ประชุมคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ในคราวการประชุมครั้งที่ ๒/๒๕๖๗ เมื่อวันที่ ๓๑ กรกฎาคม ๒๕๖๗ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติจึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. ๒๕๖๗”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับเมื่อพ้นกำหนดหนึ่งปีนับแต่วันประกาศในราชกิจจานุเบกษา เป็นต้นไป

ข้อ ๓ ในประกาศนี้

“หน่วยงาน” หมายความว่า หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

“การประมวลผลคลาวด์” (Cloud Computing) หมายความว่า แนวคิดการเข้าถึงเครือข่ายสารสนเทศซึ่งเป็นกลุ่มทรัพยากรทางกายภาพหรือเสมือนที่สามารถแบ่งปัน (Shareable) มีความยืดหยุ่น (Elastic) และขยายขนาดได้ (Scalable) ด้วยการจัดหาตัวเอง (Self-service Provisioning) และการจัดการตามความต้องการ (Administration On-demand)

“บริการคลาวด์” (Cloud Service) หมายความว่า ความสามารถ (Capability) ในการประมวลผลคลาวด์ ซึ่งถูกเรียกใช้โดยอินเทอร์เน็ตที่กำหนดให้

“ประเภทบริการคลาวด์” (Cloud Service Category) หมายความว่า กลุ่มของบริการคลาวด์ที่มีคุณสมบัติร่วมกันบางอย่าง โดยมีรูปแบบ ดังนี้

(๑) การให้บริการโครงสร้างพื้นฐานหลัก (Infrastructure as a Service: IaaS) ประกอบด้วยระบบประมวลผลข้อมูล ระบบการจัดเก็บข้อมูล ระบบเครือข่าย และทรัพยากรพื้นฐานอื่น ๆ ที่เกี่ยวข้องกับระบบประมวลผล ผู้ใช้บริการสามารถใช้งานซอฟต์แวร์บนโครงสร้างพื้นฐานและทรัพยากรที่ผู้ให้บริการจัดหาให้ได้อย่างมีประสิทธิภาพ โดยไม่ต้องบริหารจัดการโครงสร้างพื้นฐานที่จำเป็นด้วยตนเอง หรือ

(๒) การให้บริการแพลตฟอร์ม (Platform as a Service: PaaS) ประกอบด้วย ระบบโปรแกรมงานคอมพิวเตอร์ ระบบฐานข้อมูล และระบบจัดการหรืองานบริการจากคอมพิวเตอร์ ผู้ใช้บริการสามารถพัฒนาติดตั้ง และปรับแต่งซอฟต์แวร์ได้ โดยไม่ต้องบริหารจัดการในส่วนที่เกี่ยวข้องกับโครงสร้างพื้นฐาน เครือข่าย ระบบปฏิบัติการ และระบบจัดการฐานข้อมูล หรือ

(๓) การให้บริการซอฟต์แวร์ (Software as a Service: SaaS) ผู้ให้บริการจัดเตรียมซอฟต์แวร์สำเร็จรูปแล้ว โดยผู้ให้บริการสามารถกำหนดค่าความต้องการ พารามิเตอร์ ปริมาณหน่วยประมวลผลข้อมูล หน่วยเก็บข้อมูล และบริหารจัดการเพื่อให้ได้บริการตามวัตถุประสงค์ หรือ

(๔) การให้บริการใดที่เป็นารรวมกันของสองบริการขึ้นไป จาก ข้อ (๑) ถึง (๓) หรือ

(๕) การให้บริการอื่นที่สำนักงานประกาศกำหนด

“คลาวด์สาธารณะ” (Public Cloud) หมายความว่า รูปแบบการใช้คลาวด์ที่บริการคลาวด์สามารถใช้ได้กับผู้ให้บริการคลาวด์ใด ๆ และทรัพยากรถูกควบคุมโดยผู้ให้บริการคลาวด์

“ผู้ให้บริการคลาวด์” (Cloud Service Customer : CSC) หมายความว่า หน่วยงานที่มีข้อตกลงทางสัญญาอย่างเป็นทางการในการใช้บริการคลาวด์ที่ให้บริการโดยผู้ให้บริการคลาวด์

“ผู้ให้บริการคลาวด์” (Cloud Service Provider : CSP) หมายความว่า หน่วยงานของรัฐหรือเอกชนที่ทำให้บริการคลาวด์สามารถใช้ได้กับผู้ให้บริการคลาวด์ รวมถึงจัดการทรัพยากรเหล่านี้เพื่อให้มั่นใจว่ามีความพร้อมใช้งานความมั่นคงปลอดภัย และความสามารถในการขยายตัวสำหรับผู้ให้บริการคลาวด์ของตน

“ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลส่วนบุคคลตามที่ กำหนดไว้ในมาตรา ๖ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

“สำนักงาน” หมายความว่า สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ข้อ ๔ ให้หน่วยงานที่ใช้บริการคลาวด์สาธารณะดำเนินการตามมาตรฐานฉบับนี้ โดยคำนึงถึงระดับผลกระทบของข้อมูลหรือระบบสารสนเทศ ตามที่กำหนดไว้ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๖ และดำเนินการไม่น้อยกว่าข้อกำหนดขั้นต่ำท้ายประกาศนี้

ข้อ ๕ การดำเนินการตามข้อ ๔ กรณีเป็นข้อมูลส่วนบุคคล ให้จัดระดับผลกระทบด้านการรักษาความลับระดับกลางเป็นอย่างน้อย ตามที่กำหนดไว้ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๖ และดำเนินการไม่น้อยกว่าข้อกำหนดขั้นต่ำท้ายประกาศนี้

ข้อ ๖ ให้หน่วยงานจัดส่งผลสรุปรายงานการดำเนินการต่อสำนักงานภายในสามสิบวันนับแต่วันที่ดำเนินการแล้วเสร็จ

ข้อ ๗ ให้เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ รักษาการตามประกาศนี้ และให้มีอำนาจออกประกาศ คำสั่ง หลักเกณฑ์และวิธีการเพื่อปฏิบัติตามประกาศนี้

ในกรณีที่มีปัญหาเกี่ยวกับการปฏิบัติตามประกาศนี้ หรือประกาศนี้ไม่ได้กำหนดเรื่องใดไว้ให้ประธานกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเป็นผู้มีอำนาจตีความและวินิจฉัยชี้ขาด ทั้งนี้ การตีความและคำวินิจฉัยของประธานกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติให้เป็นที่สิ้นสุด

ประกาศ ณ วันที่ กันยายน พ.ศ. ๒๕๖๗

(นายภูมิธรรม เวชยชัย)

รองนายกรัฐมนตรี ปฏิบัติหน้าที่

ประธานกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

แนบท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. ๒๕๖๗

๑. บทนำ

๑.๑ เหตุผลความจำเป็น

จากการประชุมคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ ครั้งที่ ๑/๒๕๖๖ เมื่อวันที่ ๒๒ ธันวาคม ๒๕๖๖ ณ ตึกบัญชาการ ๑ ทำเนียบรัฐบาล และผ่านสื่ออิเล็กทรอนิกส์ ที่ประชุมฯ ได้ให้ความเห็นชอบแนวทางการขับเคลื่อนตามนโยบายการใช้คลาวด์เป็นหลัก (Cloud First Policy) ทั้งในส่วนของการกำหนดหน่วยงานรัฐ ผู้รับบริการ แนวทางปฏิบัติ ข้อมูล มาตรฐาน ประเภทของบริการคลาวด์ ผู้ให้บริการคลาวด์ และการบริหารจัดการบริการ ซึ่งได้กำหนดแนวทางการดำเนินงานด้านบริการคลาวด์ (Cloud Service) ในระยะ ๕ ปี โดยเห็นชอบให้จัดตั้งคณะกรรมการเฉพาะด้านการขับเคลื่อนตามนโยบายการใช้คลาวด์เป็นหลัก (Cloud First Policy) เพื่อกำกับ ติดตาม และให้ข้อเสนอแนะในการขับเคลื่อนการดำเนินงาน

นอกจากนี้ จากการที่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ได้เปิดเผยสถิติภัยคุกคามทางไซเบอร์ ประจำปี พ.ศ. ๒๕๖๖ พบว่าหน่วยงานที่ถูกโจมตีมากที่สุด ได้แก่ หน่วยงานด้านการศึกษา จำนวน ๖๓๒ ครั้ง ขณะที่อันดับที่ ๒ เป็นหน่วยงานรัฐอื่น ๆ ที่โดนโจมตีไปจำนวน ๑๔๕ ครั้ง และอันดับที่ ๓ ได้แก่ ผู้ประกอบการพาณิชย์ที่เป็นบริษัทเอกชนสัญชาติไทย โดนโจมตีสูงสุดจำนวน ๑๔๘ ครั้ง ทั้งนี้ รูปแบบภัยคุกคามทางไซเบอร์ที่พบได้บ่อยที่สุดในปี พ.ศ. ๒๕๖๖ อันดับ ๑ ได้แก่ เว็บบันไดออนไลน์จำนวน ๕๑๕ ครั้ง อันดับ ๒ ได้แก่ เว็บไซต์ที่ถูกแฮ็กจำนวน ๓๓๖ ครั้ง และอันดับ ๓ ได้แก่ เว็บไซต์ปลอม จำนวน ๓๐๑ ครั้ง ทำให้เห็นแนวโน้มของภัยคุกคามทางไซเบอร์ที่มีต่อข้อมูลและระบบสารสนเทศของหน่วยงานต่าง ๆ เพิ่มสูงขึ้นอย่างต่อเนื่อง โดยเฉพาะภัยคุกคามทางไซเบอร์ที่มีต่อหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

จากสถานการณ์ดังกล่าวข้างต้น ทำให้การที่จะส่งเสริมให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมถึงหน่วยงานเอกชน หันมาใช้ระบบคลาวด์มากขึ้น แม้ว่าจะเกิดผลดีในแง่ของการพัฒนาเศรษฐกิจและสังคมของประเทศไทย และการเพิ่มความสามารถในการเข้าถึงทักษะด้านดิจิทัล แต่ก็มีความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่มีต่อหน่วยงานดังกล่าวเพิ่มสูงขึ้นด้วย จึงเป็นเหตุผลสำคัญที่สำนักงานจะต้องจัดทำมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ฉบับนี้

๑.๒ วัตถุประสงค์

เพื่อลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่มีต่อการให้บริการคลาวด์สาธารณะให้กับหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๑.๓ ขั้วอำนาจ

มาตรา ๙ (๔) แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ มีหน้าที่และอำนาจกำหนดมาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ สร้างมาตรฐานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ และกำหนดมาตรฐานขั้นต่ำที่เกี่ยวข้องกับคอมพิวเตอร์ ระบบคอมพิวเตอร์ โปรแกรมคอมพิวเตอร์ รวมถึงส่งเสริมการรับรองมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานเอกชน

๑.๔ หลักการสำคัญที่เกี่ยวข้อง

- ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๖
- ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๖
- ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลผลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔

๑.๕ ความเสี่ยงจากการใช้บริการคลาวด์

มาตรฐานฉบับนี้ กำหนดความเสี่ยงจากการใช้บริการระบบคลาวด์เป็น ๒ ประเภท ได้แก่ ความเสี่ยงจากผู้ใช้บริการคลาวด์ (Cloud Service Customer : CSC) และความเสี่ยงจากผู้ให้บริการคลาวด์ (Cloud Service Provider : CSP)

๑.๖ โครงสร้างของมาตรฐาน

มาตรฐานฉบับนี้ แบ่งข้อกำหนด (Requirements) ออกได้เป็น ๒ ส่วน (Areas) ดังนี้

๑. การกำกับดูแลด้านความมั่นคงปลอดภัยระบบคลาวด์ (Cloud Security Governance)

- ๑.๑ นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Policies)
- ๑.๒ โครงสร้างองค์กรด้านความมั่นคงปลอดภัยสารสนเทศ (Organization of Information Security)
- ๑.๓ การปฏิบัติตามกฎ ระเบียบ ข้อบังคับ (Compliance)

๒. การปฏิบัติการและการรักษาความมั่นคงปลอดภัยโครงสร้างพื้นฐานระบบคลาวด์ (Cloud Infrastructure Security and Operation)

- ๒.๑ การบริหารทรัพยากรมนุษย์ (Human Resource Security)
- ๒.๒ การจัดการทรัพย์สิน (Asset Management)
- ๒.๓ การควบคุมการเข้าถึง (Access Control)
- ๒.๔ การเข้ารหัส (Cryptography)
- ๒.๕ การรักษาความปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environment Security)
- ๒.๖ การรักษาความมั่นคงปลอดภัยการปฏิบัติการ (Operations Security)
- ๒.๗ การรักษาความมั่นคงปลอดภัยเครือข่าย (Communication Security)
- ๒.๘ การจัดหา การพัฒนา และการบำรุงรักษา (System Acquisition, Development, and Maintenance)
- ๒.๙ การจัดการผู้ให้บริการภายนอก (Supplier Relationships)
- ๒.๑๐ การจัดการเหตุการณ์คุกคามทางสารสนเทศ (Information Security Incident Management)

๑.๗ กรอบแนวคิด

เนื่องจากความเสี่ยงจากการใช้บริการคลาวด์มาจาก ๒ ส่วน คือ ความเสี่ยงอันเกิดจากผู้ให้บริการคลาวด์และความเสี่ยงอันเกิดจากผู้ให้บริการคลาวด์ ดังนั้น มาตรฐานฉบับนี้จึงอาศัยหลักการเรื่องความร่วมรับผิดชอบ (Share Responsibilities) ให้กับทั้งผู้ใช้บริการคลาวด์ (CSC) และผู้ให้บริการคลาวด์ (CSP) ซึ่งจะทำให้สามารถลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่มีต่อระบบคลาวด์ได้อย่างครอบคลุมและมีประสิทธิภาพ

นอกจากนี้ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มีการใช้งานระบบสารสนเทศและข้อมูลสารสนเทศซึ่งมีระดับผลกระทบ (Criticality) และระดับความอ่อนไหว (Sensitivity) ที่แตกต่างกัน ประกอบกับประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๖ กำหนดให้หน่วยงานดังกล่าวมีการประเมินและจัดระดับผลกระทบที่อาจเกิดขึ้นตามวัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ (Security Objectives) ดังนั้น มาตรฐานฉบับนี้จึงกำหนดให้มีข้อกำหนดขั้นต่ำด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Baseline) เป็น ๓ ระดับ คือ ระดับต่ำ ระดับกลาง และระดับสูง เพื่อให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ สามารถปฏิบัติตามมาตรฐานฉบับนี้ได้อย่างมีประสิทธิภาพ โดยมีค่าใช้จ่ายที่เหมาะสมกับประโยชน์ที่จะได้รับ

นอกจากนี้ ผู้ให้บริการคลาวด์ (Cloud Service Provider : CSP) ที่จะให้บริการกับหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ มีหน้าที่ต้องดำเนินการให้เป็นไปตามที่หน่วยงานดังกล่าวร้องขอด้วย

๑.๘ กระบวนการตรวจรับรองมาตรฐาน

มาตรฐานฉบับนี้ กำหนดแนวทางการตรวจรับรองมาตรฐานสำหรับผู้ให้บริการคลาวด์ และผู้ให้บริการคลาวด์ ที่จะขอรับการรับรอง ดังนี้

๑.๘.๑ ประเภทของการตรวจรับรอง

- การประเมินตนเอง (Self-assessment) เป็นการประเมินหน่วยงานของตนเองตามรูปแบบที่สำนักงานกำหนด พร้อมแนบหลักฐานและขออนุมัติไปยังผู้บริหารสูงสุดของหน่วยงาน โดยเก็บรักษาไว้ที่หน่วยงานและส่งให้สำนักงานด้วย

- การตรวจรับรองโดยหน่วยงานควบคุมหรือกำกับดูแล (Attestation) เป็นการตรวจให้การรับรองโดยหน่วยงานควบคุมหรือกำกับดูแลตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมายการควบคุมและกำกับดูแล

- การตรวจรับรองโดยหน่วยงานให้บริการตรวจรับรอง (Certify Body) เป็นการตรวจให้การรับรองโดยหน่วยงานให้บริการตรวจรับรองในระดับขั้นก้าวหน้า หรือสูงกว่า ตามประกาศคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๖ ทั้งนี้ ในช่วงแรกของการดำเนินการที่สำนักงานยังมีได้ให้การรับรองหน่วยงานให้บริการตรวจรับรอง อาจดำเนินการโดยหน่วยงานให้บริการตรวจรับรองตามมาตรฐานสากลที่สำนักงานประกาศกำหนด ก็ได้

๑.๘.๒ ความถี่ในการตรวจรับรอง

- กรณีของผู้ให้บริการคลาวด์

- ผลกระทบระดับต่ำ : ให้ดำเนินการประเมินตนเอง (Self-assessment) รวมทั้งมีการทบทวนอย่างน้อยปีละ ๑ ครั้ง

- ผลกระทบระดับกลาง : ได้รับการรับรองโดยหน่วยงานควบคุมหรือกำกับดูแล (Attestation) หรือ ได้รับการรับรองโดยหน่วยงานให้บริการตรวจรับรอง (Certify Body) ตามวงรอบ ๓ ปี ประกอบด้วย การตรวจรับรองในปีที่ ๑ และการตรวจสำรวจในปีที่ ๒ และ ๓

- ผลกระทบระดับสูง : ได้รับการรับรองโดยหน่วยงานให้บริการตรวจรับรอง (Certify Body) ตามวงรอบ ๓ ปี ประกอบด้วยการตรวจรับรองในปีที่ ๑ และการตรวจสอบซ้ำในปีที่ ๒ และ ๓

- กรณีของผู้ให้บริการคลาวด์

- ผลกระทบระดับต่ำ : ได้รับการรับรองโดยหน่วยงานให้บริการตรวจรับรอง (Certify Body) ตามวงรอบ ๓ ปี ประกอบด้วยการตรวจรับรองในปีที่ ๑ และการตรวจสอบซ้ำในปีที่ ๒ และ ๓ และได้รับการรับรองตามมาตรฐาน ISO/IEC 27001 Certification และ CSA STAR Level 1/CCM Lite เป็นอย่างน้อย

- ผลกระทบระดับกลาง : ได้รับการรับรองโดยหน่วยงานให้บริการตรวจรับรอง (Certify Body) ตามวงรอบ ๓ ปี ประกอบด้วยการตรวจรับรองในปีที่ ๑ และการตรวจสอบซ้ำในปีที่ ๒ และ ๓ และได้รับการรับรองตามมาตรฐาน CSA STAR Level 2/CCM และ ISO/IEC 27701 Certification เป็นอย่างน้อย

- ผลกระทบระดับสูง : ได้รับการรับรองโดยหน่วยงานให้บริการตรวจรับรอง (Certify Body) ตามวงรอบ ๓ ปี ประกอบด้วยการตรวจรับรองในปีที่ ๑ และการตรวจสอบซ้ำในปีที่ 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

๑.๘.๓ ในกรณีที่ผู้ให้บริการคลาวด์ ได้รับการรับรองโดยหน่วยงานให้บริการตรวจรับรอง (Certify Body) แล้วก็ไม่จำเป็นต้องดำเนินการประเมินตนเอง (Self-assessment)

๑.๘.๔ ในกรณีที่ผู้ให้บริการคลาวด์ ได้รับการรับรองตามมาตรฐาน CSA STAR Level 2/CCM แล้วก็ไม่จำเป็นต้องดำเนินการตรวจรับรองตามมาตรฐาน CSA STAR Level 1/CCM Lite

๒. ขอบเขต (Scope)

- มาตรฐานฉบับนี้ ใช้บังคับกับหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ รวมถึงผู้ให้บริการคลาวด์กับหน่วยงานดังกล่าวข้างต้นด้วย

- มาตรฐานฉบับนี้ กำหนดมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์สำหรับผู้ให้บริการคลาวด์ รวมถึงผู้ให้บริการคลาวด์สาธารณะ (Public Cloud Service Provider) เฉพาะที่ต้องให้บริการกับผู้ให้บริการคลาวด์ที่เป็นหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ เท่านั้น โดยใช้ฐานสัญญาระหว่างผู้ให้บริการคลาวด์ ดังกล่าวข้างต้น กับผู้ให้บริการคลาวด์

- ผู้ที่เกี่ยวข้องกับมาตรฐานฉบับนี้ ประกอบด้วย หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ รวมถึงผู้ให้บริการคลาวด์สาธารณะ ผู้ตรวจสอบภายในด้านความมั่นคงปลอดภัยไซเบอร์ และหน่วยงานให้บริการตรวจรับรอง (Certify Body)

๓. การอ้างอิงที่เกี่ยวข้อง (Normative Reference)

- ISO/IEC 27017:2015 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services

- ISO/IEC 27018:2019 Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

- ISO/IEC 22123-1:2023 Information technology — Cloud computing Part 1: Vocabulary

- ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๖
- ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๖
- ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔

๔. ข้อกำหนดขั้นต่ำและการตรวจรับรองสำหรับผู้ให้บริการคลาวด์และผู้ให้บริการคลาวด์

ตารางข้อกำหนดขั้นต่ำและการตรวจรับรองสำหรับผู้ให้บริการคลาวด์และผู้ให้บริการคลาวด์

ประเภทของข้อมูลหรือระบบสารสนเทศ ^๑	ข้อกำหนดขั้นต่ำ	การตรวจรับรองสำหรับผู้ให้บริการคลาวด์	การตรวจรับรองสำหรับผู้ให้บริการคลาวด์
ผลกระทบระดับต่ำ	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 โดยเก็บรักษาไว้ที่หน่วยงาน และส่งให้สำนักงานด้วย	ได้รับการรับรองโดยหน่วยงานให้บริการตรวจรับรอง (Certify Body) ตามวงรอบ ๓ ปี ประกอบด้วย การตรวจรับรองในปีที่ ๑ และการตรวจสำรวจในปีที่ ๒ และ ๓ และได้รับการรับรองตามมาตรฐาน ISO/IEC 27001 Certification และ CSA STAR Level 1/CCM Lite เป็นอย่างน้อย
ผลกระทบระดับกลาง	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 ประกอบด้วย การตรวจรับรองในปีที่ ๑ และการตรวจสำรวจในปีที่ ๒ และ ๓	ได้รับการรับรองโดยหน่วยงานให้บริการตรวจรับรอง (Certify Body) ตามวงรอบ ๓ ปี ประกอบด้วย การตรวจรับรองในปีที่ ๑ และการตรวจสำรวจในปีที่ ๒ และ ๓ และได้รับการรับรองตามมาตรฐาน CSA STAR Level 2/CCM และ ISO/IEC 27701 Certification เป็นอย่างน้อย
ผลกระทบระดับสูง	ข้อกำหนดส่วนที่ ๑ - ทุกข้อ ข้อกำหนดส่วนที่ ๒ - ทุกข้อ	ได้รับการรับรองโดยหน่วยงานให้บริการตรวจรับรอง (Certify Body) ตามวงรอบ ๓ ปี ประกอบด้วย การตรวจรับรองในปีที่ ๑ และการตรวจสำรวจในปีที่ ๒ และ ๓	ได้รับการรับรองโดยหน่วยงานให้บริการตรวจรับรอง (Certify Body) ตามวงรอบ ๓ ปี ประกอบด้วย การตรวจรับรองในปีที่ ๑ และการตรวจสำรวจในปีที่ ๒ และ ๓ และได้รับการรับรองตามมาตรฐาน ISO/IEC 27017 Certification

^๑ ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์

ประเภทของข้อมูลหรือระบบสารสนเทศ ^๑	ข้อกำหนดขั้นต่ำ	การตรวจรับรองสำหรับผู้ให้บริการคลาวด์	การตรวจรับรองสำหรับผู้ให้บริการคลาวด์
			หรือ CSA STAR Level 2/CCM และ ISO/IEC 27018 Certification และ ISO/IEC 27701 Certification เป็นอย่างน้อย

๕. มาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์

๕.๑ การกำกับดูแลด้านความมั่นคงปลอดภัยระบบคลาวด์ (Cloud Security Governance)

๕.๑.๑ นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Policies)

ผู้ให้บริการคลาวด์	ผู้ให้บริการคลาวด์
<p>ก) ผู้ให้บริการคลาวด์ต้องกำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศสำหรับการประมวลผลบนคลาวด์ให้เป็นนโยบายเฉพาะหัวข้อของผู้ให้บริการคลาวด์ นโยบายความมั่นคงปลอดภัยสารสนเทศสำหรับการประมวลผลบนคลาวด์ของผู้ให้บริการคลาวด์ ต้องสอดคล้องกับระดับความเสี่ยงที่ยอมรับได้ด้านความมั่นคงปลอดภัยสารสนเทศ ที่มีต่อข้อมูลและทรัพย์สินอื่น ๆ ขององค์กร</p> <p>ข) เมื่อกำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศ สำหรับการประมวลผลบนคลาวด์ ผู้ให้บริการคลาวด์ ต้องคำนึงถึงสิ่งต่อไปนี้</p> <ul style="list-style-type: none"> - ข้อมูลที่จัดเก็บในสภาพแวดล้อมการประมวลผลบนคลาวด์อาจอยู่ภายใต้การเข้าถึงและการจัดการโดย ผู้ให้บริการคลาวด์ - ทรัพย์สินขององค์กรอาจจะได้รับการดูแลรักษาในสภาพแวดล้อมการประมวลผลบนคลาวด์ เช่น โปรแกรมแอปพลิเคชัน - กระบวนการต่าง ๆ สามารถทำงานบนบริการคลาวด์เสมือนจริงที่มีผู้ใช้หลายราย - ผู้ให้บริการคลาวด์และบริษัทที่ใช้บริการคลาวด์ - ผู้ดูแลระบบบริการคลาวด์ของผู้ให้บริการคลาวด์ที่ได้รับสิทธิพิเศษในการเข้าถึง - ตำแหน่งทางภูมิศาสตร์ขององค์กรของผู้ให้บริการคลาวด์ และประเทศที่ผู้ให้บริการคลาวด์สามารถจัดเก็บข้อมูลผู้ให้บริการคลาวด์ ได้ (แม้จะเป็นการชั่วคราว) <p>ค) นโยบายคุ้มครองข้อมูลส่วนบุคคลของผู้ให้บริการคลาวด์ต้องระบุข้อความเกี่ยวกับข้อตกลงทางสัญญา</p>	<p>ก) ผู้ให้บริการคลาวด์ต้องเพิ่มนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศเพื่อจัดการกับการจัดหาและใช้บริการคลาวด์ โดยคำนึงถึงสิ่งต่อไปนี้</p> <ul style="list-style-type: none"> - ข้อกำหนดขั้นต่ำด้านความมั่นคงปลอดภัยสารสนเทศที่ใช้กับการออกแบบและการใช้งานบริการคลาวด์ - ความเสี่ยงจากบุคคลภายในที่ได้รับอนุญาต - การเข้าถึงหลายรายและการแยก ผู้ให้บริการคลาวด์ (รวมถึงการจำลองเสมือน) - การเข้าถึงทรัพย์สินของผู้ให้บริการคลาวด์ โดยเจ้าหน้าที่ของผู้ให้บริการคลาวด์ - ขั้นตอนการควบคุมการเข้าถึง เช่น การยืนยันตัวตน ที่เข้มงวดสำหรับการเข้าถึงบริการคลาวด์ของผู้ดูแลระบบ - การสื่อสารกับผู้ให้บริการคลาวด์ระหว่างการจัดการการเปลี่ยนแปลง - ความปลอดภัยของการจำลองเสมือน - การเข้าถึงและปกป้องข้อมูลของผู้ให้บริการคลาวด์ - การจัดการวงจรชีวิตของบัญชีผู้ให้บริการคลาวด์ - การสื่อสารกรณีเกิดเหตุละเมิดและแนวทางการแบ่งปันข้อมูลเพื่อช่วยในการสืบสวนและนิติเวช

ผู้ให้บริการคลาวด์	ผู้ให้บริการคลาวด์
<p>ระหว่างผู้ประมวลผลข้อมูลส่วนบุคคลบนคลาวด์และผู้ให้บริการคลาวด์</p> <p>ง) ข้อตกลงทางสัญญาต้องกำหนดความรับผิดชอบระหว่างผู้ประมวลผลข้อมูลส่วนบุคคลบนคลาวด์ ผู้รับจ้างช่วง (Sub-contractors) และผู้ให้บริการคลาวด์อย่างชัดเจน โดยพิจารณาจากประเภทของบริการคลาวด์ (เช่น บริการประเภท IaaS, PaaS หรือ SaaS) ตัวอย่างเช่น การกำหนดความรับผิดชอบในการควบคุมระดับแอปพลิเคชันอาจแตกต่างกันขึ้นอยู่กับว่าผู้ประมวลผลข้อมูลส่วนบุคคลบนคลาวด์นั้นให้บริการ SaaS หรือ PaaS หรือ IaaS</p>	

๕.๑.๒ โครงสร้างองค์กรด้านความมั่นคงปลอดภัยสารสนเทศ (Organization of Information Security)

๕.๑.๒.๑ บทบาทและความรับผิดชอบด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ

(Information Security Roles and Responsibilities)

ผู้ให้บริการคลาวด์	ผู้ให้บริการคลาวด์
<p>ก) ผู้ให้บริการคลาวด์ต้องมีการตกลงกับผู้ให้บริการคลาวด์เกี่ยวกับการแบ่งบทบาทหน้าที่และความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศอย่างเหมาะสม และยืนยันว่า ผู้ให้บริการคลาวด์ สามารถทำหน้าที่และความรับผิดชอบที่จัดสรรได้ ต้องระบุบทบาทและความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศของทั้งสองฝ่ายไว้ในข้อตกลง</p> <p>ข) ผู้ให้บริการคลาวด์ต้องระบุและจัดการความสัมพันธ์กับส่วนงานที่เกี่ยวข้องกับการสนับสนุนลูกค้าและฟังก์ชันการดูแลของผู้ให้บริการคลาวด์</p>	<p>ก) ผู้ให้บริการคลาวด์ต้องตกลงและบันทึกการแบ่งบทบาทหน้าที่และความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศอย่างเหมาะสมกับ ผู้ให้บริการคลาวด์, ผู้ให้บริการคลาวด์ และผู้ให้บริการภายนอก</p> <p>ข) ผู้ให้บริการคลาวด์ต้องแต่งตั้งผู้ประสานงานด้านการคุ้มครองข้อมูลส่วนบุคคล เพื่อประสานงานกับผู้ให้บริการคลาวด์</p>

๕.๑.๒.๒ การติดต่อกับเจ้าหน้าที่ (Contact with Authorities)

ผู้ให้บริการคลาวด์	ผู้ให้บริการคลาวด์
<p>ก) ผู้ให้บริการคลาวด์ต้องระบุหน่วยงานที่เกี่ยวข้องกับการดำเนินการร่วมกันระหว่างผู้ให้บริการคลาวด์และผู้ให้บริการคลาวด์</p>	<p>ก) ผู้ให้บริการคลาวด์ควรแจ้งให้ผู้ให้บริการคลาวด์ทราบถึงที่ตั้งทางภูมิศาสตร์ขององค์กรที่เป็นเจ้าของผู้ให้บริการคลาวด์ และประเทศที่ผู้ให้บริการคลาวด์สามารถจัดเก็บข้อมูล ผู้ให้บริการคลาวด์ได้</p>

๕.๑.๓ การปฏิบัติตามกฎ ระเบียบ ข้อบังคับ (Compliance)

๕.๑.๓.๑ การระบุกฎหมายที่บังคับใช้และข้อกำหนดตามสัญญา (Identification of Applicable Legislation and Contractual Requirements)

ผู้ให้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ให้บริการคลาวด์ต้องพิจารณาประเด็นที่ว่า กฎหมายและข้อบังคับที่เกี่ยวข้องอาจเป็นกฎหมายของเขตอำนาจศาลที่ควบคุมผู้ให้บริการคลาวด์ นอกเหนือจากกฎหมายที่ควบคุมผู้ให้บริการคลาวด์	ก) ผู้ให้บริการคลาวด์ต้องแจ้งให้ผู้ให้บริการคลาวด์ทราบถึงเขตอำนาจศาลทางกฎหมายที่ควบคุมบริการคลาวด์
ข) ผู้ให้บริการคลาวด์ต้องขอหลักฐานว่าผู้ให้บริการคลาวด์ได้ปฏิบัติตามกฎระเบียบและมาตรฐานที่เกี่ยวข้องกับผู้ให้บริการคลาวด์ โดยหลักฐานดังกล่าวอาจเป็นการรับรองที่จัดทำโดยผู้ตรวจสอบภายนอก	ข) ผู้ให้บริการคลาวด์ต้องระบุข้อกำหนดทางกฎหมายที่เกี่ยวข้องของตนเอง (เช่น เกี่ยวกับการเข้ารหัสเพื่อปกป้องข้อมูลส่วนบุคคล) และต้องให้ข้อมูลนี้แก่ผู้ให้บริการคลาวด์เมื่อได้รับการร้องขอ
	ค) ผู้ให้บริการคลาวด์ต้องแสดงหลักฐานให้ผู้ให้บริการคลาวด์ทราบถึงการปฏิบัติตามกฎหมายที่บังคับใช้ในปัจจุบันและข้อกำหนดตามสัญญา

๕.๑.๓.๒ สิทธิในทรัพย์สินทางปัญญา (Intellectual Property Rights)

ผู้ให้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) การติดตั้งซอฟต์แวร์ที่ได้รับอนุญาตในเชิงพาณิชย์ในบริการคลาวด์อาจทำให้เกิดการละเมิดเงื่อนไขการอนุญาตให้ใช้สิทธิสำหรับซอฟต์แวร์ได้ ผู้ให้บริการคลาวด์ต้องมีขั้นตอนในการระบุข้อกำหนดในการให้สิทธิการใช้งานเฉพาะระบบคลาวด์ก่อนที่จะอนุญาตให้ติดตั้งซอฟต์แวร์ที่ได้รับอนุญาตในบริการคลาวด์ และต้องให้ความสนใจเป็นพิเศษกับกรณีที่บริการคลาวด์มีความยืดหยุ่นและสามารถปรับขนาดได้ และสามารถใช้งานซอฟต์แวร์บนระบบหรือแกนประมวลผลได้มากกว่าที่อนุญาตโดยเงื่อนไขการอนุญาตให้ใช้สิทธิ	ก) ผู้ให้บริการคลาวด์ต้องกำหนดกระบวนการในการตอบสนองต่อการร้องเรียนเรื่องสิทธิในทรัพย์สินทางปัญญา

๕.๑.๓.๓ การปกป้องบันทึกข้อมูล (Protection of Records)

ผู้ให้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ให้บริการคลาวด์ต้องขอข้อมูลจากผู้ให้บริการคลาวด์เกี่ยวกับการปกป้องบันทึกข้อมูลที่รวบรวมและจัดเก็บโดยผู้ให้บริการคลาวด์ที่เกี่ยวข้องกับการใช้บริการคลาวด์ของผู้ให้บริการคลาวด์	ก) ผู้ให้บริการคลาวด์ต้องให้ข้อมูลแก่ผู้ให้บริการคลาวด์เกี่ยวกับการปกป้องบันทึกข้อมูลที่รวบรวมและจัดเก็บโดยผู้ให้บริการคลาวด์ที่เกี่ยวข้องกับการใช้บริการคลาวด์ของผู้ให้บริการคลาวด์

๕.๑.๓.๔ กฎระเบียบที่เกี่ยวกับมาตรการควบคุมการเข้ารหัสข้อมูล (Regulation of Cryptographic Controls)

ผู้ให้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ให้บริการคลาวด์ต้องตรวจสอบให้แน่ใจว่าชุดของมาตรการควบคุมการเข้ารหัสข้อมูลที่ใช้กับการให้บริการคลาวด์สอดคล้องกับข้อตกลง กฎหมาย และระเบียบข้อบังคับที่เกี่ยวข้อง	ก) ผู้ให้บริการคลาวด์ต้องให้คำอธิบายกับ ผู้ให้บริการคลาวด์เกี่ยวกับมาตรการควบคุมการเข้ารหัสข้อมูล ที่ดำเนินการโดยผู้ให้บริการคลาวด์ เพื่อใช้ในการทบทวนการปฏิบัติตามข้อตกลง กฎหมาย และ ข้อบังคับที่เกี่ยวข้อง

๕.๑.๓.๕ การทบทวนด้านการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างเป็นอิสระ (Independent Review of Information Security)

ผู้ให้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ให้บริการคลาวด์ต้องขอหลักฐานที่เป็นเอกสารว่ามีการนำมาตรการควบคุมและแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศสำหรับบริการคลาวด์ไปปฏิบัติ และมีความสอดคล้องกับที่ผู้ให้บริการคลาวด์กล่าวอ้าง ทั้งนี้ หลักฐานดังกล่าวอาจรวมถึงการรับรองมาตรฐานที่เกี่ยวข้องด้วย	ก) ผู้ให้บริการคลาวด์ต้องให้หลักฐานที่เป็นเอกสารแก่ผู้ให้บริการคลาวด์เพื่อยืนยันข้อเรียกร้องของ ผู้ให้บริการคลาวด์ในการนำมาตรการควบคุมความมั่นคงปลอดภัยสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคลไปใช้ ข) ในกรณีที่การตรวจสอบโดยผู้ให้บริการคลาวด์แต่ละรายการไม่สามารถกระทำได้อาจเพิ่มความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศได้ ผู้ให้บริการคลาวด์ต้องแสดงหลักฐานที่เป็นอิสระว่ามีการนำไปปฏิบัติและดำเนินการด้านความมั่นคงปลอดภัยสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคลตามนโยบายและขั้นตอนของผู้ให้บริการคลาวด์ ทั้งนี้ ผู้ให้บริการคลาวด์ต้องแสดงหลักฐานดังกล่าวให้กับผู้ที่คาดว่าจะเป็นผู้ให้บริการคลาวด์ก่อนเข้าทำสัญญา โดยปกติแล้วการตรวจสอบอิสระที่เกี่ยวข้องตามที่ผู้ให้บริการคลาวด์เลือก ควรเป็นวิธีการที่เป็นที่ยอมรับเพื่อตอบสนองความต้องการของ ผู้ใช้ บริการคลาวด์ ในการตรวจสอบการดำเนินงานของ ผู้ให้บริการคลาวด์ หากมีความโปร่งใสเพียงพอ เมื่อการตรวจสอบที่เป็นอิสระไม่สามารถทำได้ ผู้ให้บริการคลาวด์ ต้องทำการประเมินตนเอง และเปิดเผยกระบวนการและผลลัพธ์ต่อผู้ให้บริการคลาวด์

๕.๒ การปฏิบัติการและการรักษาความมั่นคงปลอดภัยโครงสร้างพื้นฐานระบบคลาวด์ (Cloud Infrastructure Security and Operation)

๕.๒.๑ การบริหารทรัพยากรมนุษย์ (Human Resource Security)

๕.๒.๑.๑ การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศ การศึกษา และการฝึกอบรม (Information Security Awareness, Education and Training)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
<p>ก) ผู้ใช้บริการคลาวด์ ต้องเพิ่มรายการต่อไปนี้ ในโปรแกรมสร้างความตระหนักรู้ การศึกษา และการฝึกอบรมสำหรับผู้จัดการธุรกิจบริการคลาวด์ ผู้ดูแลระบบบริการคลาวด์ ผู้ประกอบบริการคลาวด์ และผู้ใช้บริการคลาวด์ รวมถึงพนักงานและผู้รับจ้างที่เกี่ยวข้อง</p> <ul style="list-style-type: none"> - มาตรฐานและขั้นตอนการใช้บริการคลาวด์ - ความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับบริการคลาวด์และวิธีการจัดการความเสี่ยงเหล่านั้น - ความเสี่ยงด้านสภาพแวดล้อมของระบบและเครือข่ายจากการใช้บริการคลาวด์ - การคุ้มครองข้อมูลส่วนบุคคล - ข้อพิจารณาทางกฎหมายและข้อบังคับที่เกี่ยวข้อง <p>ข) ต้องจัดให้มีโปรแกรมการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศ การศึกษา และการฝึกอบรมเกี่ยวกับบริการคลาวด์แก่ผู้บริหารและผู้จัดการที่กำกับดูแล รวมถึงหน่วยงานธุรกิจ (Business Units)</p>	<p>ก) ผู้ให้บริการคลาวด์ ต้องสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศและด้านการคุ้มครองข้อมูลส่วนบุคคล การศึกษา และการฝึกอบรมแก่พนักงาน รวมทั้งให้ผู้รับจ้างดำเนินการเช่นเดียวกันเกี่ยวกับการจัดการข้อมูลของผู้ใช้บริการคลาวด์ และข้อมูลที่ได้จากบริการคลาวด์อย่างเหมาะสม โดยข้อมูลนี้อาจมีข้อมูลที่เป็นความลับต่อผู้ใช้บริการคลาวด์หรืออยู่ภายใต้ข้อจำกัดเฉพาะ รวมถึงข้อจำกัดด้านกฎระเบียบในการเข้าถึงและใช้งานโดย ผู้ให้บริการคลาวด์</p>

๕.๒.๒ การจัดการทรัพย์สิน (Asset Management)

๕.๒.๒.๑ ทะเบียนทรัพย์สิน (Inventory of Assets)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
<p>ก) ทะเบียนทรัพย์สินของผู้ใช้บริการคลาวด์ต้องคำนึงถึงข้อมูลและทรัพย์สินที่เกี่ยวข้องซึ่งจัดเก็บในสภาพแวดล้อมการประมวลผลบนคลาวด์ ทั้งนี้ บันทึกทะเบียนทรัพย์สินต้องระบุสถานที่จัดเก็บทรัพย์สิน เช่น ชื่อของผู้ให้บริการคลาวด์</p>	<p>ก) ทะเบียนทรัพย์สินของผู้ให้บริการคลาวด์ต้องระบุอย่างชัดเจนในเรื่อง</p> <ul style="list-style-type: none"> - ข้อมูลของผู้ใช้บริการคลาวด์ - ข้อมูลที่เกิดจากการใช้บริการคลาวด์

๕.๒.๒.๒ การบ่งชี้ข้อมูล (Labelling of Information)

ผู้ให้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ให้บริการคลาวด์ต้องบ่งชี้ข้อมูลและทรัพย์สินขององค์กรที่ใช้งานหรือเก็บรักษาไว้บนระบบคลาวด์ตามขั้นตอนปฏิบัติสำหรับการบ่งชี้ข้อมูลขององค์กร	ก) ผู้ให้บริการคลาวด์ต้องจัดทำเอกสารและเปิดเผยฟังก์ชันการทำงานของบริการใด ๆ ที่ผู้ให้บริการคลาวด์ สามารถนำไปใช้เพื่อการบ่งชี้ข้อมูลและทรัพย์สินที่เกี่ยวข้องได้

๕.๒.๓ การควบคุมการเข้าถึง (Access Control)

๕.๒.๓.๑ การควบคุมเข้าถึงเครือข่ายและบริการเครือข่าย (Access to Networks and Network Services)

ผู้ให้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) นโยบายการควบคุมการเข้าถึงของผู้ให้บริการคลาวด์สำหรับการใช้บริการเครือข่ายต้องระบุข้อกำหนดสำหรับผู้ใช้งานในการเข้าถึงบริการคลาวด์ตามแต่ละบริการที่ใช้งาน	

๕.๒.๓.๒ การลงทะเบียนและยกเลิกการลงทะเบียนสำหรับผู้ใช้งาน (User Registration and Deregistration)

ผู้ให้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ขั้นตอนการลงทะเบียนและยกเลิกการลงทะเบียนสำหรับผู้ใช้งานต้องครอบคลุมถึงสถานการณ์ที่การควบคุมการเข้าถึงของผู้ใช้ถูกคุกคาม เช่น การที่รหัสผ่านหรือข้อมูลการลงทะเบียนผู้ใช้อื่น ๆ (ยกตัวอย่างเช่นจากการเปิดเผยโดยไม่ได้ตั้งใจ) ถูกทำให้เสียหายหรือถูกคุกคาม	ก) เพื่อจัดการการเข้าถึงบริการคลาวด์โดยผู้ใช้งานของผู้ให้บริการคลาวด์ ผู้ให้บริการคลาวด์ต้องจัดเตรียมฟังก์ชันการลงทะเบียนและการยกเลิกการลงทะเบียนผู้ใช้งาน รวมถึงข้อกำหนดสำหรับการใช้งานฟังก์ชันเหล่านี้แก่ ผู้ให้บริการคลาวด์

๕.๒.๓.๓ การจัดสรรการเข้าถึงของผู้ใช้งาน (User Access Provisioning)

ผู้ให้บริการคลาวด์	ผู้ให้บริการคลาวด์
	ก) ผู้ให้บริการคลาวด์ต้องจัดเตรียมฟังก์ชันสำหรับการจัดการสิทธิการเข้าถึงของผู้ให้บริการคลาวด์ รวมถึงข้อกำหนดสำหรับการใช้งานฟังก์ชันเหล่านี้

๕.๒.๓.๔ การจัดการสิทธิการเข้าถึงที่ได้รับสิทธิพิเศษ (Management of Privileged Access Rights)

ผู้ให้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ให้บริการคลาวด์ต้องใช้เทคนิคการยืนยันตัวตนที่เพียงพอ (เช่น การยืนยันตัวตนแบบหลายปัจจัย) สำหรับการตรวจสอบสิทธิของผู้ดูแลระบบบริการคลาวด์ของผู้ให้บริการคลาวด์ ให้มีความสามารถในการจัดการบริการคลาวด์ที่สอดคล้องตามความเสี่ยงที่ระบุไว้	ก) ผู้ให้บริการคลาวด์ต้องมีเทคนิคการยืนยันตัวตนที่เพียงพอ (เช่น การยืนยันตัวตนแบบหลายปัจจัย) สำหรับการตรวจสอบสิทธิของผู้ดูแลระบบบริการคลาวด์ของผู้ให้บริการคลาวด์ ให้มีความสามารถในการบริหารจัดการระบบคลาวด์ ที่สอดคล้องตามความเสี่ยงที่ระบุไว้

๕.๒.๓.๕ การจัดการข้อมูลการพิสูจน์ตัวตนที่เป็นความลับของผู้ใช้ (Management of Secret Authentication Information of Users)

ผู้ให้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ให้บริการคลาวด์ต้องตรวจสอบว่ากระบวนการจัดการของผู้ให้บริการคลาวด์สำหรับการจัดสรรข้อมูลการตรวจสอบความลับ (Secret Authentication Information) เช่น รหัสผ่าน เป็นไปตามข้อกำหนดของผู้ให้บริการคลาวด์	ก) ผู้ให้บริการคลาวด์ต้องให้ข้อมูลเกี่ยวกับขั้นตอนการจัดการข้อมูลการตรวจสอบความลับ (Secret Authentication Information) ของผู้ให้บริการคลาวด์ รวมถึงขั้นตอนในการจัดสรรข้อมูลดังกล่าว สำหรับการตรวจสอบสิทธิผู้ใช้งาน

๕.๒.๓.๖ การจำกัดการเข้าถึงข้อมูล (Information Access Restriction)

ผู้ให้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ให้บริการคลาวด์ต้องตรวจสอบให้แน่ใจว่าสามารถจำกัดการเข้าถึงข้อมูลในบริการคลาวด์ได้ตามนโยบายการควบคุมการเข้าถึงและปฏิบัติตามข้อกำหนดดังกล่าว ซึ่งรวมถึงการจำกัดการเข้าถึงบริการต่าง ๆ บนระบบคลาวด์ และข้อมูล ผู้ให้บริการคลาวด์ที่เก็บไว้ในบริการ	ก) ผู้ให้บริการคลาวด์ต้องให้การควบคุมการเข้าถึงที่อนุญาตให้กับผู้ให้บริการคลาวด์ เพื่อจำกัดการเข้าถึงบริการต่าง ๆ บนระบบคลาวด์ และข้อมูล ผู้ให้บริการคลาวด์ที่เก็บไว้ในบริการ

๕.๒.๓.๗ การใช้โปรแกรมอรรถประโยชน์พิเศษ (Use of Privilege Utility Programs)

ผู้ให้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) หากอนุญาตให้ใช้โปรแกรมอรรถประโยชน์ได้ ผู้ให้บริการคลาวด์ต้องระบุโปรแกรมอรรถประโยชน์ที่จะใช้ในสภาพแวดล้อมการประมวลผลบนคลาวด์ และตรวจสอบให้แน่ใจว่าโปรแกรมเหล่านั้น ไม่รบกวนการควบคุมของบริการคลาวด์	ก) ผู้ให้บริการคลาวด์ต้องระบุข้อกำหนดสำหรับโปรแกรมอรรถประโยชน์ใด ๆ ที่ใช้ในบริการคลาวด์ ผู้ให้บริการคลาวด์ต้องตรวจสอบให้แน่ใจว่าการใช้โปรแกรมอรรถประโยชน์ใด ๆ ที่สามารถข้ามขั้นตอนการทำงานตามปกติหรือการรักษาความปลอดภัยนั้น จำกัดเฉพาะบุคลากรที่ได้รับอนุญาตเท่านั้น และต้องมีการทบทวนและตรวจสอบการใช้โปรแกรมดังกล่าวอย่างสม่ำเสมอ

๕.๒.๓.๘ ขั้นตอนการเข้าสู่ระบบอย่างปลอดภัย (Secure Log-on Procedures)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ต้องกำหนดให้ผู้ใช้ที่อยู่ภายใต้การควบคุมของผู้ใช้บริการคลาวด์ปฏิบัติตามขั้นตอนการเข้าสู่ระบบอย่างปลอดภัยสำหรับบัญชีใด ๆ	ก) ในกรณีที่จำเป็น ผู้ให้บริการคลาวด์ต้องจัดให้มีขั้นตอนการเข้าสู่ระบบอย่างปลอดภัยสำหรับบัญชีใด ๆ ที่ผู้ใช้บริการคลาวด์ร้องขอสำหรับผู้ใช้ที่อยู่ภายใต้การควบคุมของผู้ใช้บริการคลาวด์

๕.๒.๔ การเข้ารหัส (Cryptography)

๕.๒.๔.๑ นโยบายเกี่ยวกับการใช้มาตรการควบคุมการเข้ารหัส (Policy on the Use of Cryptographic Controls)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ต้องใช้มาตรการควบคุมการเข้ารหัสสำหรับการใช้บริการระบบคลาวด์ที่มีความแข็งแกร่งเพียงพอ และสอดคล้องตามความเสี่ยงที่ได้ระบุไว้ ไม่ว่าผู้ใช้บริการคลาวด์หรือผู้ให้บริการคลาวด์จะเป็นผู้จัดทำมาตรการควบคุมการเข้ารหัสเหล่านั้นก็ตาม ข) เมื่อผู้ให้บริการคลาวด์นำเสนอการเข้ารหัสใด ๆ ผู้ใช้บริการคลาวด์ต้องตรวจสอบข้อมูล que ผู้ให้บริการคลาวด์จัดหาให้เพื่อยืนยันว่ามีความสามารถในการเข้ารหัสดังนี้หรือไม่ - ปฏิบัติตามข้อกำหนดด้านนโยบายของ ผู้ใช้บริการคลาวด์ - เข้ากันได้กับการป้องกันการเข้ารหัสลับอื่น ๆ ที่ใช้โดยผู้ใช้บริการคลาวด์ - ใช้กับข้อมูลขณะจัดเก็บและระหว่างโอนถ่ายภายในบริการคลาวด์และนอกระบบคลาวด์	ก) ผู้ให้บริการคลาวด์ต้องให้ข้อมูลแก่ผู้ใช้บริการคลาวด์เกี่ยวกับการเข้ารหัสเพื่อปกป้องข้อมูลและข้อมูลส่วนบุคคล ที่ผู้ให้บริการคลาวด์ประมวลผล นอกจากนี้ ผู้ให้บริการคลาวด์ต้องให้ข้อมูลแก่ผู้ใช้บริการคลาวด์เกี่ยวกับความสามารถใด ๆ ที่ผู้ให้บริการคลาวด์มอบให้ซึ่งสามารถช่วยผู้ใช้บริการคลาวด์ในการใช้การเข้ารหัสดังกล่าว

๕.๒.๔.๒ การจัดการกุญแจ (Key Management)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ต้องระบุกุญแจสำหรับการเข้ารหัสในแต่ละบริการคลาวด์ และดำเนินการตามขั้นตอนสำหรับการจัดการกุญแจ ข) ในกรณีที่บริการคลาวด์มีฟังก์ชันการจัดการกุญแจสำหรับการใช้งานโดยผู้ใช้บริการคลาวด์ ผู้ใช้บริการคลาวด์ต้องขอข้อมูลดังต่อไปนี้เกี่ยวกับขั้นตอนที่ใช้ในการจัดการกุญแจสำหรับการเข้ารหัสที่เกี่ยวข้องกับบริการคลาวด์ - ประเภทของกุญแจ	

ผู้ให้บริการคลาวด์	ผู้ให้บริการคลาวด์
<p>- ข้อกำหนดเฉพาะของระบบการจัดการ รวมถึงขั้นตอนต่าง ๆ ตลอดอายุการใช้งานของกุญแจเข้ารหัส เช่น การสร้าง เปลี่ยนแปลง หรือปรับปรุง จัดเก็บ หมดยุการใช้งาน เรียกคืน เก็บรักษา และทำลาย</p> <p>- ขั้นตอนการจัดการกุญแจที่แนะนำสำหรับการใช้งานโดยผู้ให้บริการคลาวด์</p> <p>ค) ผู้ให้บริการคลาวด์ต้องไม่อนุญาตให้ ผู้ให้บริการคลาวด์ จัดเก็บและจัดการกุญแจสำหรับการเข้ารหัส เมื่อผู้ให้บริการคลาวด์ ใช้กุญแจเข้ารหัสของตนเอง</p>	

๕.๒.๕ การรักษาความปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environment Security)

๕.๒.๕.๑ ตำแหน่งของศูนย์ข้อมูล (Data Center Location)

ผู้ให้บริการคลาวด์	ผู้ให้บริการคลาวด์
<p>ก) ต้องใช้ศูนย์ข้อมูลหลักในประเทศไทย (Data Localization)</p>	<p>ก) ต้องจัดตั้งศูนย์ข้อมูลหลักในประเทศไทย (Data Localization)</p> <p>ข) ต้องจัดตั้งศูนย์ข้อมูลสำรองในประเทศไทย (Data Localization) หรือ อยู่ในภูมิภาคเอเชียตะวันออกเฉียงใต้ที่ใกล้เคียงที่ใกล้เคียงกับการใช้งานหลักของผู้ให้บริการคลาวด์ให้มากที่สุด รวมถึงสิงคโปร์และเขตปกครองพิเศษฮ่องกง</p>

๕.๒.๕.๒ การกำจัดหรือนำอุปกรณ์กลับมาใช้ใหม่อย่างปลอดภัย (Secure Disposal or Reuse of Equipment)

ผู้ให้บริการคลาวด์	ผู้ให้บริการคลาวด์
<p>ก) ผู้ให้บริการคลาวด์ต้องร้องขอการยืนยันว่าผู้ให้บริการคลาวด์มีนโยบายและขั้นตอนในการกำจัดหรือนำทรัพยากรกลับมาใช้ใหม่อย่างปลอดภัย</p>	<p>ก) ผู้ให้บริการคลาวด์ต้องตรวจสอบให้แน่ใจว่ามีการเตรียมการสำหรับการกำจัดหรือนำทรัพยากร (เช่น อุปกรณ์ ที่เก็บข้อมูล ไฟล์ หน่วยความจำ) กลับมาใช้ใหม่อย่างปลอดภัยและทันท่วงที</p> <p>ข) เพื่อวัตถุประสงค์ในการกำจัดหรือนำกลับมาใช้ใหม่อย่างมั่นคงปลอดภัย และไม่สามารถกู้คืนข้อมูลกลับมาได้ อุปกรณ์ที่มีสื่อจัดเก็บข้อมูลที่อาจมีข้อมูลส่วนบุคคลต้องได้รับการปฏิบัติเสมือนว่ามีข้อมูลส่วนบุคคลจริง</p>

๕.๒.๖ การรักษาความมั่นคงปลอดภัยการปฏิบัติการ (Operations Security)

๕.๒.๖.๑ การจัดการการเปลี่ยนแปลง (Change Management)

ผู้ให้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) กระบวนการจัดการการเปลี่ยนแปลงของผู้ให้บริการคลาวด์ ต้องคำนึงถึงผลกระทบของการเปลี่ยนแปลงใด ๆ ที่เกิดขึ้นจากผู้ให้บริการคลาวด์	ก) ผู้ให้บริการคลาวด์ ต้องให้ข้อมูลแก่ ผู้ให้บริการคลาวด์ เกี่ยวกับการเปลี่ยนแปลงในบริการคลาวด์ ที่อาจส่งผลกระทบต่อบริการคลาวด์ ข้อมูลต่อไปนี้ จะช่วยให้ ผู้ให้บริการคลาวด์ ระบุถึงผลกระทบของการเปลี่ยนแปลงที่อาจมีผลต่อความมั่นคงปลอดภัยสารสนเทศ – ประเภทของการเปลี่ยนแปลง – วันที่และเวลาที่วางแผนไว้ของการเปลี่ยนแปลง – คำอธิบายทางเทคนิคเกี่ยวกับการเปลี่ยนแปลงของบริการคลาวด์และระบบที่เกี่ยวข้อง (Underlying Systems) – การแจ้งเตือนการเริ่มต้นและการเปลี่ยนแปลงที่เสร็จสมบูรณ์ ข) เมื่อ ผู้ให้บริการคลาวด์ ให้บริการคลาวด์ที่ขึ้นอยู่กับผู้ให้บริการรายย่อยของ ผู้ให้บริการคลาวด์ ผู้ให้บริการคลาวด์ อาจจำเป็นต้องแจ้งการเปลี่ยนแปลงที่เกิดขึ้นให้ ผู้ให้บริการคลาวด์ ทราบ

๕.๒.๖.๒ การบริหารจัดการความจุ (Capacity Management)

ผู้ให้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ให้บริการคลาวด์ ต้องตรวจสอบให้แน่ใจว่าขีดความสามารถของทรัพยากรที่ตกลงกันไว้ในบริการคลาวด์นั้นตรงตามข้อกำหนดของผู้ให้บริการคลาวด์ ข) ผู้ให้บริการคลาวด์ ต้องตรวจสอบการใช้บริการคลาวด์และคาดการณ์ความต้องการด้านขีดความสามารถของทรัพยากรของบริการคลาวด์ เพื่อให้มั่นใจในประสิทธิภาพของบริการคลาวด์เมื่อเวลาผ่านไป	ก) ผู้ให้บริการคลาวด์ ต้องตรวจสอบขีดความสามารถของทรัพยากรทั้งหมดเพื่อป้องกันไม่ให้เกิดเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่เกิดจากการขาดแคลนทรัพยากร

๕.๒.๖.๓ การสำรองข้อมูล (Information Backup)

ผู้ให้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ในกรณีที่ ผู้ให้บริการคลาวด์ มีความสามารถในการสำรองข้อมูลซึ่งเป็นส่วนหนึ่งของบริการคลาวด์ ผู้ให้บริการคลาวด์ ต้องขอข้อมูลเฉพาะของความสามารถในการสำรองข้อมูลจากผู้ให้บริการคลาวด์ นอกจากนี้ ผู้ให้บริการคลาวด์	ก) ผู้ให้บริการคลาวด์ ต้องให้ข้อมูลเฉพาะของความสามารถในการสำรองข้อมูลแก่ ผู้ให้บริการคลาวด์ ข้อมูลเฉพาะควรมีข้อมูลต่อไปนี้ตามความเหมาะสม – ขอบเขตและกำหนดการของการสำรองข้อมูล

ผู้ให้บริการคลาวด์	ผู้ให้บริการคลาวด์
<p>ต้องทำการตรวจสอบเพื่อให้แน่ใจว่าเป็นไปตามข้อกำหนดในการสำรองข้อมูลหรือไม่</p> <p>ข) ผู้ให้บริการคลาวด์ มีหน้าที่รับผิดชอบในการดำเนินการสำรองข้อมูลเมื่อ ผู้ให้บริการคลาวด์ ไม่ได้ให้บริการนี้</p>	<ul style="list-style-type: none"> - วิธีการสำรองข้อมูลและรูปแบบข้อมูล รวมถึงวิธีการเข้ารหัส หากมีความเกี่ยวข้อง - ระยะเวลาเก็บรักษาข้อมูลสำรอง - ขั้นตอนการตรวจสอบความสมบูรณ์ของข้อมูลสำรอง - ขั้นตอนและระยะเวลาที่เกี่ยวข้องกับการกู้คืนข้อมูลจากการสำรองข้อมูล - ขั้นตอนในการทดสอบความสามารถในการสำรองข้อมูล - สถานที่จัดเก็บข้อมูลสำรอง <p>ข) ผู้ให้บริการคลาวด์ ต้องให้บริการการเข้าถึงข้อมูลสำรองที่ปลอดภัยและแยกออกจากกัน หากบริการดังกล่าวมีการนำเสนอให้ ผู้ให้บริการคลาวด์</p>

๕.๒.๖.๔ การบันทึกเหตุการณ์ (Event Logging)

ผู้ให้บริการคลาวด์	ผู้ให้บริการคลาวด์
<p>ก) ผู้ให้บริการคลาวด์ ต้องจัดทำข้อกำหนดสำหรับการบันทึกเหตุการณ์และตรวจสอบว่าบริการคลาวด์ตรงตามข้อกำหนดเหล่านั้นหรือไม่</p>	<p>ก) ผู้ให้บริการคลาวด์ ต้องให้ผู้ให้บริการสามารถบันทึกเหตุการณ์</p> <p>ข) ในกรณีที่เป็นไปได้ บันทึกเหตุการณ์ควรบันทึกว่าข้อมูลส่วนบุคคลได้รับการเปลี่ยนแปลงหรือไม่ (เพิ่ม แก้ไข หรือลบ) จากเหตุการณ์นั้น และโดยใคร (Audit Log) ในกรณีที่มีผู้ให้บริการหลายรายเข้ามาเกี่ยวข้องในการให้บริการจากหลากหลายประเภทบริการของสถาปัตยกรรมอ้างอิงประมวลผลคลาวด์ อาจมีบทบาทที่แตกต่างหรือแบ่งปันกันในการปฏิบัติตามข้อนี้</p>

๕.๒.๖.๕ การปกป้องข้อมูลในบันทึกเหตุการณ์ (Protection of Log information)

ผู้ให้บริการคลาวด์	ผู้ให้บริการคลาวด์
<p>ก) ข้อมูลที่ บันทึกไว้ในบันทึกเหตุการณ์ เพื่อวัตถุประสงค์ต่าง ๆ เช่น การตรวจสอบความปลอดภัยและการวินิจฉัยการทำงาน อาจมีข้อมูลส่วนบุคคลอยู่ด้วย จึงต้องมีมาตรการ เช่น การควบคุมการเข้าถึง เพื่อให้มั่นใจว่าข้อมูลที่บันทึกไว้ในบันทึกเหตุการณ์จะถูกนำไปใช้ตามวัตถุประสงค์ที่ตั้งไว้เท่านั้น</p> <p>ข) ต้องมีขั้นตอนการดำเนินการ ซึ่งดีที่ที่สุดคือเป็นระบบอัตโนมัติ เพื่อให้มั่นใจว่าข้อมูลที่บันทึกไว้ใน</p>	<p>ก) ข้อมูลที่ บันทึกไว้ในบันทึกเหตุการณ์ เพื่อวัตถุประสงค์ต่าง ๆ เช่น การตรวจสอบความปลอดภัยและการวินิจฉัยการทำงาน อาจมีข้อมูลส่วนบุคคลอยู่ด้วย จึงต้องมีมาตรการ เช่น การควบคุมการเข้าถึง เพื่อให้มั่นใจว่าข้อมูลที่บันทึกไว้ในบันทึกเหตุการณ์จะถูกนำไปใช้ตามวัตถุประสงค์ที่ตั้งไว้เท่านั้น</p> <p>ข) ต้องมีขั้นตอนการดำเนินการ ซึ่งดีที่ที่สุดคือเป็นระบบอัตโนมัติ เพื่อให้มั่นใจว่าข้อมูลที่บันทึกไว้ใน</p>

ผู้ให้บริการคลาวด์	ผู้ให้บริการคลาวด์
บันทึกเหตุการณ์จะถูกเก็บไว้ในระยะเวลาที่กำหนด (Log Retention) และเอกสารระบุไว้	บันทึกเหตุการณ์จะถูกเก็บไว้ในระยะเวลาที่กำหนด (Log Retention) และเอกสารระบุไว้

๕.๒.๖.๖ บันทึกเหตุการณ์ของผู้ดูแลระบบและผู้ปฏิบัติงาน (Administrator and Operator Logs)

ผู้ให้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) หากมีการให้สิทธิพิเศษให้แก่ ผู้ให้บริการคลาวด์ การใช้สิทธิพิเศษนั้นต้องมีการบันทึกเหตุการณ์และประสิทธิภาพของการดำเนินการเหล่านั้น ผู้ให้บริการคลาวด์ ต้องพิจารณาว่าความสามารถในการบันทึกเหตุการณ์ที่ ผู้ให้บริการคลาวด์ จัดหาให้ นั้นเหมาะสมหรือไม่ หรือ ผู้ให้บริการคลาวด์ ต้องใช้ความสามารถในการบันทึกเหตุการณ์เพิ่มเติมหรือไม่	

๕.๒.๖.๗ การซิงโครไนซ์นาฬิกา (Clock Synchronization)

ผู้ให้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ให้บริการคลาวด์ต้องขอข้อมูลเกี่ยวกับการซิงโครไนซ์นาฬิกาที่ใช้ในระบบของผู้ให้บริการคลาวด์	ก) ผู้ให้บริการคลาวด์ต้องให้ข้อมูลแก่ผู้ให้บริการคลาวด์เกี่ยวกับนาฬิกาที่ระบบของผู้ให้บริการคลาวด์ใช้ และข้อมูลเกี่ยวกับวิธีที่ผู้ให้บริการคลาวด์สามารถซิงโครไนซ์นาฬิกาภายในกับนาฬิกาในบริการคลาวด์

๕.๒.๖.๘ การจัดการช่องโหว่ทางเทคนิค (Management of Technical Vulnerabilities)

ผู้ให้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ให้บริการคลาวด์ ต้องขอข้อมูลจาก ผู้ให้บริการคลาวด์ เกี่ยวกับการจัดการช่องโหว่ทางเทคนิคที่อาจส่งผลกระทบต่อบริการคลาวด์ ที่ให้บริการ ผู้ให้บริการคลาวด์ ต้องระบุช่องโหว่ทางเทคนิคที่ผู้ให้บริการคลาวด์ จะเป็นผู้รับผิดชอบในการจัดการ และกำหนดกระบวนการในการจัดการให้ชัดเจน	ก) ผู้ให้บริการคลาวด์ ต้องให้ข้อมูล ผู้ให้บริการคลาวด์ เกี่ยวกับการจัดการช่องโหว่ทางเทคนิคที่อาจส่งผลกระทบต่อบริการคลาวด์ที่ให้บริการ

๕.๒.๖.๙ การแยกสภาพแวดล้อมสำหรับการพัฒนา การทดสอบ และการปฏิบัติงาน (Separation of Development, Testing and Operational Environments)

ผู้ให้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ในกรณีที่ไม่สามารถหลีกเลี่ยงการใช้ข้อมูลส่วนบุคคลสำหรับวัตถุประสงค์ในการทดสอบได้ ต้องมีการประเมินความเสี่ยง มาตรการด้านเทคนิคและการจัดการองค์กรต้องถูกนำมาใช้เพื่อลดความเสี่ยงที่ระบุไว้ให้น้อยที่สุด	ก) ในกรณีที่ไม่สามารถหลีกเลี่ยงการใช้ข้อมูลส่วนบุคคลสำหรับวัตถุประสงค์ในการทดสอบได้ ต้องมีการประเมินความเสี่ยง มาตรการด้านเทคนิคและการจัดการองค์กรต้องถูกนำมาใช้เพื่อลดความเสี่ยงที่ระบุไว้ให้น้อยที่สุด

๕.๒.๗ การรักษาความมั่นคงปลอดภัยเครือข่าย (Communication Security)

๕.๒.๗.๑ นโยบายและขั้นตอนปฏิบัติในการถ่ายโอนข้อมูล (Information Transfer Policies and Procedures)

ผู้ให้บริการคลาวด์	ผู้ให้บริการคลาวด์
<p>ก) เมื่อใดก็ตามที่มีการใช้สื่อทางกายภาพสำหรับการถ่ายโอนข้อมูล ต้องมีระบบที่จะบันทึกสื่อทางกายภาพที่เข้ามาและออกไปซึ่งมีข้อมูลส่วนบุคคล รวมถึงประเภทของสื่อทางกายภาพ ผู้ส่ง/ผู้รับที่ได้รับอนุญาต วันที่และเวลา และจำนวนสื่อทางกายภาพ</p> <p>ข) ผู้ให้บริการคลาวด์ต้องขอให้ผู้ให้บริการคลาวด์ใช้มาตรการเพิ่มเติม (เช่น การเข้ารหัส) เพื่อให้มั่นใจว่าข้อมูลสามารถเข้าถึงได้เฉพาะจุดปลายทางเท่านั้น ไม่ใช่ระหว่างทาง</p>	<p>ก) เมื่อใดก็ตามที่มีการใช้สื่อทางกายภาพสำหรับการถ่ายโอนข้อมูล ต้องมีระบบที่จะบันทึกสื่อทางกายภาพที่เข้ามาและออกไปซึ่งมีข้อมูลส่วนบุคคล รวมถึงประเภทของสื่อทางกายภาพ ผู้ส่ง/ผู้รับที่ได้รับอนุญาต วันที่และเวลา และจำนวนสื่อทางกายภาพ</p> <p>ข) หากเป็นไปได้ ต้องขอให้ผู้ให้บริการคลาวด์ใช้มาตรการเพิ่มเติม (เช่น การเข้ารหัส) เพื่อให้มั่นใจว่าข้อมูลสามารถเข้าถึงได้เฉพาะจุดปลายทางเท่านั้น ไม่ใช่ระหว่างทาง</p>

๕.๒.๗.๒ การแบ่งแยกในเครือข่าย (Segregation in Networks)

ผู้ให้บริการคลาวด์	ผู้ให้บริการคลาวด์
<p>ก) ผู้ให้บริการคลาวด์ ต้องจัดทำข้อกำหนดสำหรับการแยกเครือข่ายเพื่อให้เกิดการแยกผู้เช่า (Tenant) ในสภาพแวดล้อมที่เป็นการใช้บริการคลาวด์ร่วมกัน และตรวจสอบว่า ผู้ให้บริการคลาวด์ มีคุณสมบัติตรงตามข้อกำหนดเหล่านั้นหรือไม่</p>	<p>ก) ผู้ให้บริการคลาวด์ ต้องบังคับใช้การแยกการเข้าถึงเครือข่ายในกรณีต่อไปนี้</p> <ul style="list-style-type: none"> - การแบ่งแยกระหว่างผู้เช่าในสภาพแวดล้อมที่มีผู้เช่าหลายราย - การแยกระหว่างสภาพแวดล้อมการดูแลระบบภายในของ ผู้ให้บริการคลาวด์ และสภาพแวดล้อมการประมวลผลบนคลาวด์ของผู้ใช้บริการคลาวด์ <p>ข) ผู้ให้บริการคลาวด์ ต้องช่วย ผู้ใช้บริการคลาวด์ ตรวจสอบการแบ่งแยกที่ ดำเนินการโดยผู้ให้บริการคลาวด์</p>

๕.๒.๘ การจัดหา การพัฒนา และการบำรุงรักษา (System Acquisition, Development, and Maintenance)

๕.๒.๘.๑ การวิเคราะห์และข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Requirements Analysis and Specification)

ผู้ให้บริการคลาวด์	ผู้ให้บริการคลาวด์
<p>ก) ผู้ให้บริการคลาวด์ ต้องกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศสำหรับการใช้บริการคลาวด์ จากนั้นประเมินว่าบริการของผู้ให้บริการคลาวด์ สามารถตอบสนองความต้องการเหล่านี้ได้หรือไม่</p>	<p>ก) ผู้ให้บริการคลาวด์ ต้องให้ข้อมูลแก่ ผู้ใช้บริการคลาวด์ เกี่ยวกับความสามารถในการรักษาความมั่นคงปลอดภัยสารสนเทศที่ตนใช้ ข้อมูลนี้ต้องเป็นข้อมูลโดยไม่เปิดเผยข้อมูลที่สามารถเป็นประโยชน์ต่อบุคคลที่มีเจตนาร้าย</p>

ผู้ให้บริการคลาวด์	ผู้ให้บริการคลาวด์
ข) สำหรับการประเมินนี้ ผู้ให้บริการคลาวด์ ต้องขอข้อมูลเกี่ยวกับความสามารถในการรักษาความมั่นคงปลอดภัยสารสนเทศจากผู้ให้บริการคลาวด์	

๕.๒.๘.๒ นโยบายการพัฒนาที่ปลอดภัย (Secure Development Policy)

ผู้ให้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ให้บริการคลาวด์ ต้องขอข้อมูลจากผู้ให้บริการคลาวด์ เกี่ยวกับการใช้ขั้นตอนและวิธีปฏิบัติในการพัฒนาที่ปลอดภัยของผู้ให้บริการคลาวด์	ก) ผู้ให้บริการคลาวด์ ต้องให้ข้อมูลเกี่ยวกับการใช้ขั้นตอนและวิธีปฏิบัติในการพัฒนาความปลอดภัยของตนในขอบเขตที่สอดคล้องกับนโยบายในการเปิดเผยข้อมูล

๕.๒.๙ การจัดการผู้ให้บริการภายนอก (Supplier Relationships)

๕.๒.๙.๑ นโยบายความมั่นคงปลอดภัยสารสนเทศสำหรับความสัมพันธ์กับผู้ให้บริการภายนอก (Information Security Policy for Supplier Relationships)

ผู้ให้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ให้บริการคลาวด์ ต้องระบุว่า ผู้ให้บริการคลาวด์ เป็นผู้ให้บริการภายนอกประเภทหนึ่งในนโยบายความมั่นคงปลอดภัยสารสนเทศสำหรับความสัมพันธ์กับผู้ให้บริการภายนอก ซึ่งจะช่วยลดความเสี่ยงที่เกี่ยวข้องกับการเข้าถึงและจัดการข้อมูล ผู้ให้บริการคลาวด์ ของ ผู้ให้บริการคลาวด์	

๕.๒.๙.๒ การจัดการกับการรักษาความมั่นคงปลอดภัยภายในข้อตกลงของผู้ให้บริการภายนอก (Addressing Security within Supplier Agreements)

ผู้ให้บริการคลาวด์	ผู้ให้บริการคลาวด์
<p>ก) ผู้ให้บริการคลาวด์ ต้องยืนยันบทบาทและความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับบริการคลาวด์ ดังที่อธิบายไว้ในข้อตกลงการให้บริการ สิ่งเหล่านี้อาจรวมถึงกระบวนการต่อไปนี้</p> <ul style="list-style-type: none"> - การป้องกันมัลแวร์ - การสำรองข้อมูล - มาตรการควบคุมการเข้ารหัส - การจัดการช่องโหว่ - การจัดการเหตุการณ์ - การตรวจสอบการปฏิบัติตามข้อกำหนดทางเทคนิค - การทดสอบความปลอดภัย 	<p>ก) ผู้ให้บริการคลาวด์ ต้องระบุมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องซึ่งผู้ให้บริการคลาวด์ จะนำมาใช้เป็นส่วนหนึ่งของข้อตกลงเพื่อให้แน่ใจว่าจะไม่เกิดความเข้าใจผิดระหว่าง ผู้ให้บริการคลาวด์ และ ผู้ให้บริการคลาวด์ สิ่งเหล่านี้อาจรวมถึงกระบวนการต่อไปนี้</p> <ul style="list-style-type: none"> - การป้องกันมัลแวร์ - การสำรองข้อมูล - มาตรการควบคุมการเข้ารหัส - การจัดการช่องโหว่ - การจัดการเหตุการณ์ - การตรวจสอบการปฏิบัติตามข้อกำหนดทางเทคนิค

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
<ul style="list-style-type: none"> - การตรวจสอบ - การรวบรวม การบำรุงรักษา และการปกป้องหลักฐาน รวมถึงบันทึกและเส้นทางการตรวจสอบ - การปกป้องข้อมูลเมื่อสิ้นสุดข้อตกลงการให้บริการ - การยืนยันตัวตน และการควบคุมการเข้าถึง - การจัดการข้อมูลประจำตัวและการเข้าถึง 	<ul style="list-style-type: none"> - การทดสอบความปลอดภัย - การตรวจสอบ - การรวบรวม การบำรุงรักษา และการปกป้องหลักฐาน รวมถึงบันทึกและเส้นทางการตรวจสอบ - การปกป้องข้อมูลเมื่อสิ้นสุดข้อตกลงการให้บริการ - การยืนยันตัวตน และการควบคุมการเข้าถึง - การจัดการข้อมูลประจำตัวและการเข้าถึง <p>ข) มาตรการรักษาความมั่นคงปลอดภัยสารสนเทศที่ผู้ให้บริการคลาวด์ จะใช้อาจแตกต่างกันออกไปตามประเภทของบริการคลาวด์ที่ ผู้ใช้บริการคลาวด์ใช้งานอยู่</p>

๕.๒.๙.๓ ห่วงโซ่อุปทานของเทคโนโลยีสารสนเทศและการสื่อสาร (Information and Communication Technology Supply Chain)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
	<p>ก) หาก ผู้ให้บริการคลาวด์ ใช้บริการคลาวด์ของผู้ให้บริการรายย่อย ผู้ให้บริการคลาวด์ ต้องตรวจสอบให้แน่ใจว่าระดับความมั่นคงปลอดภัยสารสนเทศของผู้ให้บริการรายย่อยนั้นได้รับการดูแลไม่น้อยกว่าผู้ใช้บริการคลาวด์</p> <p>ข) เมื่อผู้ให้บริการคลาวด์ ให้บริการคลาวด์ตามห่วงโซ่อุปทาน ผู้ให้บริการคลาวด์ ต้องกำหนดวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศแก่ผู้ให้บริการภายนอก และขอให้ผู้ให้บริการภายนอกแต่ละรายดำเนินการจัดการบริหารความเสี่ยง เพื่อให้บรรลุวัตถุประสงค์</p>

๕.๒.๑๐ การจัดการเหตุภัยคุกคามทางสารสนเทศ (Information Security Incident Management)

๕.๒.๑๐.๑ ความรับผิดชอบและขั้นตอน (Responsibilities and Procedures)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
<p>ก) ผู้ใช้บริการคลาวด์ ต้องตรวจสอบการจัดสรรความรับผิดชอบสำหรับการจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ และต้องตรวจสอบให้แน่ใจว่าเป็นไปตามข้อกำหนดของผู้ใช้บริการคลาวด์</p> <p>ข) เหตุภัยคุกคามทางสารสนเทศต้องนำไปสู่การทบทวนโดยผู้ให้บริการคลาวด์ หรือทบทวนร่วมกันระหว่างผู้ให้บริการคลาวด์และผู้ใช้บริการคลาวด์</p>	<p>ก) ผู้ให้บริการคลาวด์ ต้องกำหนดขอบเขตความรับผิดชอบและขั้นตอนการจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศระหว่างผู้ให้บริการคลาวด์ และ ผู้ให้บริการคลาวด์ โดยเป็นส่วนหนึ่งของข้อกำหนดบริการ</p> <p>ข) ผู้ให้บริการคลาวด์ ต้องจัดเตรียมเอกสารให้ผู้ให้บริการคลาวด์ ครอบคลุม</p>