International Institute for
Trade and Development

มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
ระบบคลาวด์

ของสถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน)

ปี 2568

งานสารสนเทศ

สำนักยุทธศาสตร์และสารสนเทศ

มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์

ของสถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน)

ปี ๒๕๖๘

งานสารสนเทศ

สำนักยุทธศาสตร์และสารสนเทศ

สารบัญ

มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ของ สคพ.

๑. บทนำ (Introduction)

๑.๑ เหตุผลความจำเป็น

จากการประชุมคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ ครั้งที่ ๑/๒๕๖๖ เมื่อวันที่ ๒๒ ธันวาคม ๒๕๖๖ ณ ตึกบัญชาการ ๑ ทำเนียบรัฐบาล และผ่านสื่ออิเล็กทรอนิกส์ ที่ประชุมฯ ได้ให้ความเห็นชอบแนวทางการขับเคลื่อนตามนโยบายการใช้คลาวด์เป็นหลัก (Cloud First Policy) ทั้งในส่วนของข้อกำหนดหน่วยงานรัฐ ผู้รับบริการ แนวทางการปฏิบัติ 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 ขณะที่อันดับ ๒ เป็นหน่วยงานรัฐอื่น ๆ ที่โดนโจมตีไป ๑๔๕ ครั้ง และอันดับ ๓ ได้แก่ ผู้ประกอบการพาณิชย์ที่เป็นบริษัทเอกชนสัญชาติไทย โดนโจมตีสูงสุดจำนวน ๑๔๘ ครั้ง ทั้งนี้ รูปแบบภัยคุกคามทางไซเบอร์ที่พบบ่อยที่สุดในปี พ.ศ. ๒๕๖๖ อันดับ ๑ ได้แก่ เว็บพนันออนไลน์ จำนวน ๕๑๕ ครั้ง อันดับ ๒ ได้แก่ เว็บไซต์ที่ถูกแฮ็กจำนวน ๓๓๖ ครั้ง และอันดับ ๓ ได้แก่เว็บไซต์ปลอม จำนวน ๓๐๑ ครั้ง ทำให้เห็นแนวโน้มของภัยคุกคามทางไซเบอร์ที่มีต่อข้อมูลและระบบสารสนเทศของหน่วยงานต่าง ๆ เพิ่มสูงขึ้นอย่างต่อเนื่อง โดยเฉพาะภัยคุกคามทางไซเบอร์ที่มีต่อหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

จากสถานการณ์ดังกล่าวข้างต้น ทำให้การที่จะส่งเสริมให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมถึงหน่วยงานเอกชน หันมาใช้งานระบบคลาวด์มากขึ้น แม้ว่าจะเกิดผลดีในแง่ของการพัฒนาเศรษฐกิจและสังคมของประเทศไทย และการเพิ่มความสามารถในการเข้าถึงทักษะด้านดิจิทัล แต่ก็มีความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่มีต่อหน่วยงานดังกล่าวเพิ่มสูงขึ้นด้วย จึงเป็นเหตุผลสำคัญที่สถาบันจะต้องจัดทำมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ฉบับนี้

๑.๒ วัตถุประสงค์

เพื่อลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่มีต่อการใช้บริการคลาวด์สาธารณะให้กับสถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน)

๑.๓ ฐานอำนาจ

- มาตรา ๙ (๔) แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ มีหน้าที่และอำนาจกำหนดมาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ สร้างมาตรฐานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ และกำหนดมาตรฐานขั้นต่ำที่เกี่ยวข้องกับคอมพิวเตอร์ ระบบคอมพิวเตอร์ โปรแกรมคอมพิวเตอร์ รวมถึงส่งเสริมการรับรองมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์

ให้กับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานเอกชน

- ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. ๒๕๖๗ ข้อ ๔ กำหนดให้หน่วยงานที่ใช้บริการคลาวด์สาธารณะดำเนินการตามมาตรฐานนี้ โดยคำนึงถึงผลกระทบของข้อมูลหรือระบบสารสนเทศ และดำเนินการไม่น้อยกว่าท้ายประกาศนี้

๑.๔ หลักการสำคัญที่เกี่ยวข้อง

- ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๖

- ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๖

- ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔

๑.๕ ความเสี่ยงจากการใช้บริการคลาวด์

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

๑.๖ โครงสร้างของมาตรฐาน

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

๑.๖.๑ การกำกับดูแลด้านความมั่นคงปลอดภัยระบบคลาวด์ (Cloud Security Governance)

๑) นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Policies)

๒) โครงสร้างองค์กรด้านความมั่นคงปลอดภัยสารสนเทศ (Organization of Information Security)

๓) การปฏิบัติตามกฎ ระเบียบ ข้อบังคับ (Compliance)

๑.๖.๒ การปฏิบัติการและการรักษาความมั่นคงปลอดภัยโครงสร้างพื้นฐานระบบคลาวด์ (Cloud Infrastructure Security and Operation)

๑) การบริหารทรัพยากรมนุษย์ (Human Resource Security)

๒) การจัดการทรัพย์สิน (Asset Management)

๓) การควบคุมการเข้าถึง (Access Control)

๔) การเข้ารหัส (Cryptography)

๕) การรักษาความปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environment Security)

๖) การรักษาความปลอดภัยปฏิบัติการ (Operations Security)

๗) การรักษาความปลอดภัยเครือข่าย (Communication Security)

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

๙) การจัดการผู้ให้บริการภายนอก (Supplier Relationships)

๑๐) การจัดการเหตุภัยคุกคามทางสารสนเทศ (Information Security Incident Management)

๑.๗ กรอบแนวคิด

เนื่องจากความเสี่ยงจากการใช้บริการคลาวด์มาจาก ๒ ส่วนคือ ความเสี่ยงอันเกิดจากผู้ใช้บริการคลาวด์ (สถาบัน) และความเสี่ยงอันเกิดจากผู้ให้บริการคลาวด์ ดังนั้น มาตรฐานฉบับนี้จึงอาศัยหลักการเรื่องความร่วมรับผิดชอบ (Share Responsibilities) ให้กับทั้งผู้ใช้บริการคลาวด์ (CSC) และผู้ให้บริการคลาวด์ (CSP) ซึ่งจะทำให้สามารถลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่มีต่อระบบคลาวด์ได้อย่างครอบคลุมและมีประสิทธิภาพ

สถาบันในฐานะหน่วยงานของรัฐ ซึ่งตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัย ไซเบอร์ พ.ศ. ๒๕๖๒ มีการใช้งานระบบสารสนเทศและข้อมูลสารสนเทศซึ่งมีระดับผลกระทบ (Criticality) และระดับอ่อนไหว (Sensitivity) ที่แตกต่างกัน ประกอบกับประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๖ กำหนดให้หน่วยงานมีการประเมินและจัดระดับผลกระทบที่อาจเกิดขึ้นตามวัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ (Security Objective) ดังนั้น มาตรฐานฉบับนี้ สถาบันจึงกำหนดให้มีข้อกำหนดขั้นต่ำด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Baseline) เพื่อให้สถาบันสามารถปฏิบัติได้อย่างมีประสิทธิภาพ โดยมีค่าใช้จ่ายที่เหมาะสมกับประโยชน์ที่จะได้รับ

นอกจากนี้ ผู้ให้บริการคลาวด์ (Cloud Service Provider : CSP) ที่จะให้บริการกับสถาบัน มีหน้าที่ต้องดำเนินการให้เป็นไปตามที่สถาบันร้องขอด้วย

๑.๘ กระบวนการตรวจรับรองมาตรฐาน

มาตรฐานฉบับนี้กำหนดแนวทางการตรวจรับรองมาตรฐานสำหรับผู้ใช้บริการคลาวด์ (สถาบัน) และผู้ให้บริการคลาวด์ที่จะขอรับรองดังนี้

๑.๘.๑ ประเภทของการตรวจรับรอง

- การประเมินตนเอง (Self-assessment) เป็นการประเมินหน่วยงานของตนตามรูปแบบที่สถาบันกำหนด พร้อมแนบหลักฐานและขออนุมัติไปยังผู้อำนวยการสถาบัน โดยเก็บรักษาไว้ที่สถาบัน

- การตรวจรับรองโดยหน่วยงานควบคุมหรือกำกับดูแล (Attestation) เป็นการตรวจให้การรับรองโดยหน่วยงานควบคุมหรือกำกับดูแลตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมายการควบคุมและกำกับดูแล

- การตรวจรับรองโดยหน่วยงานให้บริการตรวจรับรอง (Certify Body) เป็นการตรวจให้การรับรองโดยหน่วยงานให้บริการตรวจรับรองในระดับขั้นก้าวหน้า หรือสูงกว่า ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๖ ทั้งนี้ ในช่วงแรกของการดำเนินการที่ สกมช. ยังมิได้ให้การรับรองหน่วยงานให้บริการตรวจรับรอง อาจดำเนินการโดยหน่วยงานให้บริการตรวจรับรองตามมาตรฐานสากลที่ สกมช. ประกาศกำหนด ก็ได้

๑.๘.๒ ความถี่ในการตรวจรับรอง

<u>กรณีของผู้ใช้บริการคลาวด์ (สถาบัน)</u>

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

- ผลกระทบระดับกลาง : ได้รับการรับรองโดยหน่วยงานควบคุมหรือกำกับดูแล (Attestation) หรือ ได้รับการรับรองโดยหน่วยงานให้บริการตรวจรับรอง (Certify Body) ตามวงรอบ ๓ ปี ประกอบด้วยการตรวจรับรองในปีที่ ๑ และการสำรวจในปีที่ ๒ และ ๓

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

<u>กรณีของผู้ให้บริการคลาวด์</u>

- ผลกระทบระดับต่ำ : ได้รับการรับรองโดยหน่วยงานให้บริการตรวจรับรอง (Certify Body) ตามวงรอบ ๓ ปี ประกอบด้วยการตรวจรับรองในปีที่ ๑ และการสำรวจในปีที่ ๒ และ ๓ และได้รับการรับรองตามมาตรฐาน ISO/IEC ๒๗๐๐๑ Certification และ CSA STAR Level ๑/CCM Lite เป็นอย่างน้อย

- ผลกระทบระดับกลาง : ได้รับการรับรองโดยหน่วยงานให้บริการตรวจรับรอง (Certify Body) ตามวงรอบ ๓ ปี ประกอบด้วยการตรวจรับรองในปีที่ ๑ และการสำรวจในปีที่ ๒ และ ๓ และได้รับการรับรองตามมาตรฐาน CSA STAR Level ๒/CCM และ ISO/IEC ๒๗๗๐๑ Certification เป็นอย่างน้อย

- ผลกระทบระดับสูง : ได้รับการรับรองโดยหน่วยงานให้บริการตรวจรับรอง (Certify Body) ตามวงรอบ ๓ ปี ประกอบด้วยการตรวจรับรองในปีที่ ๑ และการสำรวจในปีที่ ๒ และ ๓ และได้รับการรับรองตามมาตรฐาน ISO/IEC ๒๗๐๑๗ Certification และ CSA STAR Level ๒/CCM และ ISO/IEC ๒๗๐๑๘ Certification และ ISO/IEC ๒๗๗๐๑ Certification เป็นอย่างน้อย

๑.๘.๓ ในกรณีที่ผู้ให้บริการคลาวด์ ได้รับการรับรองโดยหน่วยงานให้บริการตรวจรับรอง (Certify Body) แล้ว ก็ไม่จำเป็นต้องดำเนินการประเมินตนเอง (Self-assessment)

๑.๘.๔ ในกรณีที่ผู้ให้บริการคลาวด์ ได้รับการรับรอง CSA STAR Level ๒/CCM แล้ว ก็ไม่จำเป็นต้องดำเนินการตรวจรับรองตามมาตรฐาน CSA STAR Level ๑/CCM Lite

๒. ขอบเขต (Scope)

๒.๑ มาตรฐานฉบับนี้ใช้สำหรับสถาบัน รวมถึงผู้ให้บริการคลาวด์ให้แก่สถาบันด้วย

๒.๒ มาตรฐานฉบับนี้กำหนดมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์สำหรับสถาบัน รวมถึงผู้ให้บริการคลาวด์สาธารณะ (Public Cloud Service Provider) โดยใช้ฐานสัญญาระหว่างสถาบัน กับผู้ให้บริการคลาวด์

๓. การอ้างอิงที่เกี่ยวข้อง (Normative Reference)

๓.๑ ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๖

๓.๒ ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๖

๓.๓ ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานขั้นต่ำของข้อมูล หรือระบบสารสนเทศ พ.ศ. ๒๕๖๖

๓.๔ ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔

๔. การประเมินระดับผลกระทบของข้อมูลหรือระบบสารสนเทศ

ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. ๒๕๖๗ ข้อ ๔ กำหนดให้หน่วยงานที่ใช้บริการคลาวด์สาธารณะดำเนินการตามมาตรฐานฉบับนี้ โดยคำนึงถึงระดับผลกระทบของข้อมูลหรือระบบสารสนเทศ ตามที่กำหนดไว้ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๖ และดำเนินการไม่น้อยกว่าข้อกำหนดขั้นต่ำ

และตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๖ ข้อ ๔ กำหนดให้หน่วยงานกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ โดยพิจารณาวัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ (Security Objectives) ในเรื่อง

๑) การรักษาความลับ (Confidentiality) หมายถึง การรักษาหรือสงวนไว้ ซึ่งการจำกัดการเข้าถึงหรือการเปิดเผยข้อมูลให้แก่บุคคล หน่วยงานอื่น หรือชุดคำสั่งที่ไม่ได้รับอนุญาต

๒) การรักษาความถูกต้องครบถ้วน (Integrity) หมายถึง การรักษาหรือสงวนไว้ ซึ่งความถูกต้องและความครบถ้วนของข้อมูล

๓) การรักษาสภาพพร้อมใช้งาน (Availability) หมายถึง การดำเนินการ เพื่อให้บุคคล สถาบัน หรือชุดคำสั่งที่ได้รับอนุญาตสามารถเข้าถึงและใช้งานข้อมูลหรือระบบสารสนเทศได้ตามต้องการและได้อย่างมีประสิทธิภาพ

ข้อ ๕ การพิจารณาวัตถุประสงค์ตามข้อ ๔ วรรคหนึ่ง (๑) (๒) และ (๓) ให้ประเมินและจัดระดับผลกระทบที่อาจเกิดขึ้นเป็นสามระดับ ได้แก่ ระดับต่ำ ระดับกลาง และระดับสูง

ข้อ ๖ การจัดระดับผลกระทบที่อาจเกิดขึ้นในแต่ละระดับตามข้อ ๕ ให้พิจารณาการประเมินผลกระทบในแต่ละด้าน

๔.๑ เกณฑ์การประเมินระดับผลกระทบที่อาจเกิดขึ้นตามวัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ (Security Objectives)

สถาบันได้กำหนดเกณฑ์การประเมินระดับผลกระทบที่อาจเกิดขึ้นในแต่ละระดับ โดยพิจารณาจากวัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ (Security Objectives) ในแต่ละเรื่องตามประกาศ กมช. เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๖ ซึ่งสามารถสรุปได้ดังนี้

ตารางที่ ๑ ระดับผลกระทบที่อาจเกิดขึ้นในแต่ละระดับตามวัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ (Security Objectives)[๑]

วัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ (Security Objectives)	**ผลกระทบ (Impact)* และ ผลประโยชน์แห่งชาติ(National Interests)**		
	ระดับต่ำ	**ระดับกลาง**	**ระดับสูง**
ด้านความลับ (Confidentiality) การรักษาข้อจำกัดในการได้รับอนุญาตให้เข้าถึงได้และเปิดเผยเฉพาะผู้มีสิทธิ์ รวมทั้งวิธีการคุ้มครองความเป็นส่วนตัว (Privacy) และกรรมสิทธิ์ (Proprietary) ของข้อมูลข่าวสาร	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบน้อย/อย่างจำกัด (Limited) และเกิดผลประโยชน์แห่งชาติสำคัญน้อย (Less Important or Secondary National Interests)	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบอย่างร้ายแรง (Serious) และเกิดผลประโยชน์แห่งชาติที่สำคัญ (Important National Interests)	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบอย่างร้ายแรงมาก (Severe or Catastrophic) และเกิดผลประโยชน์แห่งชาติสำคัญยิ่ง (Extremely Important National Interests)
ด้านความถูกต้องครบถ้วน (Integrity) การปกป้องจากการดัดแปลงหรือทำลายข้อมูลที่ไม่เหมาะสม และรวมถึงการรับรองว่าข้อมูลจะไม่ถูกปฏิเสธ (Non-Repudiation) และเป็นข้อมูลที่ถูกต้องเป็นความจริง (Authenticity)	การแก้ไขหรือทำลายข้อมูลโดย ไม่ได้รับอนุญาตอาจส่งผล กระทบน้อย/อย่างจำกัด (Limited) และเกิดผลประโยชน์แห่งชาติสำคัญน้อย (Less Important or Secondary National Interests)	การแก้ไขหรือทำลายข้อมูลโดย ไม่ได้รับอนุญาตอาจส่งผลกระทบอย่างร้ายแรง (Serious) และเกิดผลประโยชน์แห่งชาติที่สำคัญ (Important National Interests)	การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบอย่างร้ายแรงมาก (Severe or Catastrophic) และเกิดผลประโยชน์แห่งชาติสำคัญยิ่ง (Extremely Important National Interests)
ด้านความพร้อมใช้งาน (Availability) การสร้างความมั่นใจในการเข้าถึง และการใช้ข้อมูลอย่างทันท่วงที/เป็นปัจจุบันและเชื่อถือได้	การหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลข่าวสารหรือระบบสารสนเทศอาจส่งผลกระทบน้อย/อย่างจำกัด (Limited) และเกิดผลประโยชน์ แห่งชาติสำคัญน้อย (Less Important or Secondary National Interests)	การหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลข่าวสารหรือระบบสารสนเทศอาจส่งผลกระทบอย่างร้ายแรง (Serious) และเกิดผลประโยชน์แห่งชาติที่สำคัญ (Important National Interests)	การหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลข่าวสารหรือระบบสารสนเทศอาจส่งผลกระทบอย่างร้ายแรงมาก (Severe or Catastrophic) และเกิดผลประโยชน์แห่งชาติ สำคัญยิ่ง (Extremely Important National Interests)

[1] อ้างอิงตามประกาศสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ที่ ม ๑/๒๕๖๕ เรื่อง มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ว่าด้วยหลักเกณฑ์การจัดระดับชั้นและแบ่งปันข้อมูลภาครัฐ

๔.๒ สรุปผลการประเมินระดับผลกระทบที่อาจเกิดขึ้นตามวัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ (Security Objectives) และการรับรองมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์

๔.๒.๑ ผลการประเมินระดับผลกระทบที่อาจเกิดขึ้นของสถาบันตามวัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ (Security Objectives)

๑) ด้านการรักษาความลับ (Confidentiality)

การรักษาความลับ หมายถึง การทำให้แน่ใจว่าข้อมูลที่ละเอียดอ่อน ข้อมูลส่วนบุคคล หรือข้อมูลที่เป็นกรรมสิทธิ์ของสถาบันจะไม่ถูกเปิดเผยต่อบุคคลภายในและภายนอกที่ไม่ได้รับอนุญาต ซึ่งระดับผลกระทบของการละเมิดการรักษาความลับขึ้นอยู่กับความสำคัญของข้อมูลที่ถูกเปิดเผยและสถานการณ์ของการละเมิด ทั้งนี้ เมื่อพิจารณาข้อมูลหรือระบบสารสนเทศของสถาบัน พบว่า ข้อมูลที่สถาบันจัดเก็บไม่มีลักษณะเป็นความลับหรือข้อมูลที่มีความอ่อนไหวสูง ไม่ใช่ข้อมูลลับของทางราชการหรือเป็นภัยต่อความมั่นคงของรัฐ ดังนี้ผลกระทบที่อาจเกิดขึ้นจึงอยู่ใน “ระดับต่ำ”

๒) การรักษาความถูกต้องครบถ้วน (Integrity)

การรักษาความถูกต้องครบถ้วน (Integrity) หมายถึง การรับประกันว่าข้อมูลและระบบมีความถูกต้อง สมบูรณ์ เชื่อถือได้ และได้รับการปกป้องจากการแก้ไขเปลี่ยนแปลงหรือการทำลายโดยไม่ได้รับอนุญาต ทั้งนี้ เมื่อพิจารณาข้อมูลหรือระบบสารสนเทศของสถาบัน พบว่า ข้อมูลที่สถาบันจัดเก็บส่วนใหญ่เกี่ยวข้องกับภารกิจด้านการฝึกอบรม ประชุม และสัมมนา ซึ่งไม่ส่งผลกระทบต่อการดำเนินงานหรือการตัดสินใจ ดังนี้ผลกระทบที่อาจเกิดขึ้นจึงอยู่ใน “ระดับต่ำ”

๓) การรักษาสภาพพร้อมใช้งาน (Availability)

การรักษาสภาพพร้อมใช้งาน (Availability) หมายถึง การที่ผู้มีสิทธิ์ไม่สามารถเข้าถึงข้อมูลหรือระบบได้ตามต้องการ ซึ่งอาจนำไปสู่ผลกระทบที่สำคัญหลายประการ ทั้งนี้ เมื่อพิจารณาข้อมูลหรือระบบสารสนเทศของสถาบัน พบว่า ข้อมูลที่สถาบันมิใช่ข้อมูลที่มีความสำคัญสูงหรือเป็นข้อมูลที่หากสูญหายจะส่งให้ผลการดำเนินงานหยุดชะงัก ดังนี้ผลกระทบที่อาจเกิดขึ้นจึงอยู่ใน “ระดับต่ำ”

๔.๒.๒ ผลการประเมินระดับการตรวจรับรองมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์

การตรวจรับรองมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับระบบคลาวด์เป็นกระบวนการตรวจสอบและรับรองว่าระบบคลาวด์มีมาตรการความปลอดภัยที่เพียงพอและเป็นไปตามมาตรฐานที่กำหนด เพื่อป้องกันข้อมูลสำคัญจากการถูกโจมตี การรั่วไหล หรือการเข้าถึงโดยไม่ได้รับอนุญาต ซึ่งจากผลการประเมินระดับผลกระทบที่อาจเกิดขึ้นของสถาบันตามวัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ (Security Objectives) พบว่า ระดับผลกระทบอยู่ในระดับต่ำ ดังนั้น เพื่อให้สอดคล้องกับแนวทางการตรวจรับรองมาตรฐานฯ สถาบันจึงควรมีการประเมินตนเอง (Self-Assessment) ตามรูปแบบที่สถาบันกำหนด พร้อมแนบหลักฐาน และขออนุมัติไปยังผู้อำนวยการ โดยเก็บรักษาไว้ที่สถาบัน

ตารางที่ ๒ สรุประดับผลกระทบที่อาจเกิดขึ้นและวิธีการตรวจรับรองมาตรฐาน

ระดับผลกระทบที่อาจเกิดขึ้น	การตรวจรับรอง
ผลกระทบระดับต่ำ	ประเมินตนเอง (Self-Assessment) และมีการทบทวนอย่างน้อยปีละ ๑ ครั้ง

๕. มาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์

๕.๑ การกำกับดูแลด้านความมั่นคงปลอดภัยระบบคลาวด์ (Cloud Security Governance)

๕.๑.๑ นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Policies)

ข้อกำหนดของสถาบัน

๑) สถาบันต้องกำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศสำหรับการประมวลผลบนคลาวด์ให้เป็นนโยบายเฉพาะหัวข้อของสถาบัน นโยบายความมั่นคงปลอดภัยสารสนเทศสำหรับการประมวลผลบนคลาวด์ของสถาบัน ต้องสอดคล้องกับระดับความเสี่ยงที่ยอมรับได้ด้านความมั่นคงปลอดภัยสารสนเทศที่มีต่อข้อมูลและทรัพย์สินอื่น ๆ ของสถาบัน

๒) เมื่อกำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศ สำหรับการประมวลผลบนคลาวด์ สถาบันต้องคำนึงถึงสิ่งต่อไปนี้

- ข้อมูลที่จัดเก็บในสภาพแวดล้อมที่ประมวลผลบนคลาวด์อาจอยู่ภายใต้การเข้าถึงการจัดการโดยผู้ให้บริการคลาวด์
- ทรัพย์สินของสถาบันอาจจะได้รับการดูแลรักษาในสภาพแวดล้อมการประมวลผลบนคลาวด์ เช่น โปรแกรมแอปพลิเคชั่น
- กระบวนการต่าง ๆ สามารถทำงานบนบริการคลาวด์เสมือนจริงที่มีผู้ใช้หลายราย
- สถาบันที่เป็นผู้ใช้บริการคลาวด์และบริบทที่ใช้บริการคลาวด์
- ผู้ดูแลระบบบริการคลาวด์ของสถาบันที่ได้รับสิทธิพิเศษในการเข้าถึง
- ตำแหน่งทางภูมิศาสตร์ขององค์กรของผู้ให้บริการคลาวด์ และประเทศที่ผู้ให้บริการคลาวด์สามารถจัดเก็บข้อมูลของสถาบันได้ (แม้จะเป็นการชั่วคราว)

๓) นโยบายคุ้มครองส่วนบุคคลของสถาบันต้องระบุข้อความเกี่ยวกับข้อตกลงทางสัญญาระหว่างผู้ประมวลผลข้อมูลส่วนบุคคลบนคลาวด์และสถาบัน

๔) ข้อตกลงทางสัญญาต้องกำหนดความรับผิดชอบระหว่างผู้ประมวลผลขอมูลส่วนบุคคลบนคลาวด์ ผู้รับจ้างช่วง (Sub-contractors) และสถาบันอย่างชัดเจน โดยพิจารณาจากประเภทของบริการคลาวด์ (เช่น บริการประเภท IaaS, PaaS หรือ SaaS) ตัวอย่างเช่น การกำหนดความรับผิดชอบในการควบคุมระดับแอปพลิเคชันอาจแตกต่างกัน ขึ้นอยู่กับว่าผู้ประมวลผลข้อมูลส่วนบุคคลบนคลาวด์นั้นให้บริการ SaaS หรือ PaaS หรือ IaaS

ข้อกำหนดของผู้ให้บริการคลาวด์

ผู้ให้บริการคลาวด์ต้องเพิ่มนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศเพื่อจัดการกับการจัดหาและใช้บริการคลาวด์ โดยคำนึงถึงสิ่งต่อไปนี้

- ข้อกำหนดขั้นต่ำด้านความมั่นคงปลอดภัยสารสนเทศที่ใช้กับการออกแบบและการใช้งานบริการคลาวด์
- ความเสี่ยงจากบุคคลภายในที่ได้รับอนุญาต
- การเช่าหลายรายและการแยก ผู้ใช้บริการคลาวด์ (รวมถึงการจำลองเสมือน)
- การเข้าถึงทรัพย์สินของผู้ใช้บริการคลาวด์
- ขั้นตอนการควบคุมการเข้าถึง เช่น การยืนยันตัวตนที่เข้มงวดสำหรับการเข้าถึงบริการคลาวด์ของผู้ดูและระบบ
- การสื่อสารกับผู้ใช้บริการคลาวด์ระหว่างการจัดการการเปลี่ยนแปลง
- ความปลอดภัยของการจำลองเสมือน

- การเข้าถึงและปกป้องข้อมูลของผู้ใช้บริการคลาวด์
- การสื่อสารกรณีเกิดเหตุละเมิดและแนวทางการแบ่งปันข้อมูลเพื่อช่วยสืบสวนและนิติเวช

๕.๑.๒ โครงสร้างองค์กรด้านความมั่นคงปลอดภัยสารสนเทศ (Organization of Information Security)

๕.๑.๒.๑ บทบาทและความรับผิดชอบด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security Roles and responsibilities)

ข้อกำหนดของสถาบัน

๑) สถาบันต้องมีการตกลงกับผู้ให้บริการคลาวด์เกี่ยวกับการแบ่งบทบาทหน้าที่ และความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศอย่างเหมาะสม และยืนยันว่า สถาบันซึ่งเป็นผู้ใช้บริการคลาวด์ สามารถทำหน้าที่และความรับผิดชอบที่จัดสรรได้ ต้องระบุบทบาทและความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศของทั้งสองฝ่ายไว้ในข้อตกลง

๒) สถาบันต้องระบุและจัดการความสัมพันธ์กับส่วนงานที่เกี่ยวกับการสนับสนุนลูกค้าและฟังก์ชั่นการดูแลของผู้ให้บริการคลาวด์

ข้อกำหนดของผู้ให้บริการคลาวด์

๑) ผู้ให้บริการคลาวด์ต้องตกลงและบันทึกการแบ่งบทบาทหน้าที่และความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศอย่างเหมาะสมระหว่างสถาบัน กับผู้ให้บริการคลาวด์ และผู้ให้บริการภายนอก

๒) ผู้ให้บริการคลาวด์ต้องแต่งตั้งผู้ประสานงานด้านการคุ้มครองข้อมูลส่วนบุคคลเพื่อประสานงานกับสถาบัน

๕.๑.๒.๒ การติดต่อกับเจ้าหน้าที่ (Contact with Authorities)

ข้อกำหนดของสถาบัน

สถาบันต้องระบุหน่วยงานที่เกี่ยวข้องกับการดำเนินการร่วมกันระหว่างสถาบันและผู้ให้บริการคลาวด์

ข้อกำหนดของผู้ให้บริการคลาวด์

ผู้ให้บริการคลาวด์ควรแจ้งให้ผู้ใช้บริการคลาวด์ทราบถึงที่ตั้งทางภูมิศาสตร์ขององค์กรที่เป็นเจ้าของผู้ให้บริการคลาวด์ และประเทศที่ผู้ให้บริการคลาวด์สามารถจัดเก็บข้อมูลผู้ให้บริการคลาวด์ได้

๕.๒ การปฏิบัติการและการรักษาความมั่นคงปลอดภัยโครงสร้างพื้นฐานระบบคลาวด์ (Cloud Infrastructure Security and Operation)

๕.๒.๑ การบริหารทรัพยากรมนุษย์ (Human resource Security)

๕.๒.๑.๑ การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศ การศึกษาและการฝึกอบรม (Information Security Aware, Education and Training)

ข้อกำหนดของสถาบัน

๑) สถาบันต้องเพิ่มรายการต่อไปนี้ในโปรแกรมสร้างความตระหนักรู้ การศึกษาและการฝึกอบรมสำหรับผู้จัดการธุรกิจบริการคลาวด์ ผู้ดูแลระบบบริการคลาวด์ ผู้ประกอบการบริการคลาวด์และผู้ใช้บริการคลาวด์ รวมถึงพนักงานและผู้รับจ้างที่เกี่ยวข้อง

- มาตรฐานและขั้นตอนการใช้บริการคลาวด์
- ความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับบริการคลาวด์และวิธีการจัดการความเสี่ยงเหล่านั้น
- ความเสี่ยงด้านสภาพแวดล้อมของระบบและเครือข่ายจากการใช้บริการคลาวด์
- การคุ้มครองข้อมูลส่วนบุคคล
- ขอพิจารณาทางกฎหมายและข้อบังคับที่เกี่ยวข้อง

๒) ต้องจัดให้มีโปรแกรมการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศ การศึกษา และการฝึกอบรมเกี่ยวกับบริการคลาวด์แก่ผู้บริหารและเจ้าหน้าที่

ข้อกำหนดของผู้ให้บริการคลาวด์

ผู้ให้บริการคลาวด์ต้องสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศและด้านการคุ้มครองข้อมูลส่วนบุคคล การศึกษา และการฝึกอบรมแก่พนักงาน รวมทั้งให้ผู้รับจ้างดำเนินการเช่นเดียวกันเกี่ยวกับการจัดการข้อมูลของสถาบัน และข้อมูลที่ได้จากบริการคลาวด์อย่างเหมาะสม โดยข้อมูลนี้อาจมีข้อมูลที่เป็นความลับต่อผู้ใช้บริการคลาวด์หรืออยู่ภายใต้ข้อจำกัดเฉพาะ รวมถึงข้อจำกัดด้านกฎระเบียบในการเข้าถึงและใช้งานโดยผู้ให้บริการคลาวด์

๕.๒.๒ การจัดการทรัพย์สิน (Asset Management)

๕.๒.๒.๑ ทะเบียนทรัพย์สิน (Inventory of Asset)

ข้อกำหนดของสถาบัน

ทะเบียนทรัพย์สินของสถาบันต้องคำนึงถึงข้อมูลและทรัพย์สินที่เกี่ยวข้อง ซึ่งจัดเก็บในสภาพแวดล้อมการประมวลผลบนคลาวด์ ทั้งนี้ บันทึกทะเบียนทรัพย์สินต้องระบุสถานที่จัดเก็บทรัพย์สิน เช่น ชื่อของผู้ให้บริการคลาวด์

ข้อกำหนดของผู้ให้บริการคลาวด์

ทะเบียนทรัพย์สินของผู้ให้บริการคลาวด์ต้องระบุอย่างชัดเจนในเรื่อง

- ข้อมูลของผู้ใช้บริการคลาวด์
- ข้อมูลที่เกิดจากการใช้บริการคลาวด์

๕.๒.๒.๒ การบ่งชี้ข้อมูล (Labelling of Information)

ข้อกำหนดของสถาบัน

สถาบันต้องบ่งชี้ข้อมูลและทรัพย์สินของสถาบันที่ใช้งานหรือเก็บรักษาไว้บนระบบคลาวด์ตามขั้นตอนปฏิบัติสำหรับการบ่งชี้ข้อมูลของสถาบัน

ข้อกำหนดของผู้ให้บริการคลาวด์

ผู้ให้บริการคลาวด์ต้องจัดทำเอกสารและเปิดเผยฟังก์ชั่นการทำงานของบริการใด ๆ ที่สถาบันสามารถนำไปใช้เพื่อการบ่งชี้ข้อมูลและทรัพย์สินที่เกี่ยวข้องได้

๕.๒.๓ การควบคุมการเข้าถึง (Access Control)

๕.๒.๓.๑ การควบคุมการเข้าถึงเครือข่ายและบริการเครือข่าย (Access to Networks and Network Services)

ข้อกำหนดของสถาบัน

นโยบายการควบคุมการเข้าถึงของสถาบันสำหรับการใช้บริการเครือข่ายต้องระบุข้อกำหนดสำหรับผู้ใช้งานในการเข้าถึงบริการคลาวด์ตามแต่ละบริบทที่ใช้งาน

๕.๒.๓.๒ การลงทะเบียนและยกเลิกการลงทะเบียนสำหรับผู้ใช้งาน (User Registration and Deregistration)

ข้อกำหนดของสถาบัน

ขั้นตอนการลงทะเบียนและยกเลิกการลงทะเบียนสำหรับผู้ใช้ต้องครอบคลุมถึงสถานการณ์ที่การควบคุมการข้าถึงของผู้ใช้ถูกคุกคาม เช่น การที่รหัสผ่านหรือข้อมูลการลงทะเบียนผู้ใช้อื่น ๆ (ยกตัวอย่างเช่น จากการเปิดเผยโดยไม่ได้ตั้งใจ) ถูกทำให้เสียหายหรือถูกคุกคาม

ข้อกำหนดของผู้ให้บริการคลาวด์

เพื่อจัดการการเข้าถึงบริการคลาวด์โดยเจ้าหน้าที่ของสถาบัน ผู้ให้บริการคลาวด์ต้องจัดเตรียมฟังก์ชั่นการลงทะเบียนและการยกเลิกการลงทะเบียนผู้ใช้งาน รวมถึงข้อกำหนดสำหรับการใช้งานฟังก์ชั่นเหล่านี้แก่สถาบัน

๕.๒.๓.๓ การจัดสรรการเข้าถึงของผู้ใช้ (User Access Provisioning)

ข้อกำหนดของผู้ให้บริการคลาวด์

ผู้ให้บริการคลาวด์ต้องจัดเตรียมฟังก์ชั่นสำหรับการจัดการสิทธิการเข้าถึงของสถาบัน รวมถึงข้อกำหนดสำหรับการใช้งานฟังก์ชั่นเหล่านี้

๕.๒.๓.๔ การจัดการสิทธิการเข้าถึงที่ได้รับสิทธิพิเศษ (Management of Privileged Access Rights)

ข้อกำหนดของสถาบัน

สถาบันต้องใช้เทคนิคการยืนยันตัวตนที่เพียงพอ (เช่น การยืนยันตัวตนแบบหลายปัจจัย) สำหรับการตรวจสอบสิทธิของผู้ดูแลระบบบริการคลาวด์ของสถาบัน ให้มีความสามารถในการจัดการบริการคลาวด์ที่สอดคล้องตามความเสี่ยงที่ระบุไว้

ข้อกำหนดของผู้ให้บริการคลาวด์

ผู้ให้บริการคลาวด์ต้องมีเทคนิคการยืนยันตัวตนที่เพียงพอ (เช่น การยืนยันตัวตนแบบหลายปัจจัย) สำหรับการตรวจสอบสิทธิของผู้ดูแลระบบบริการคลาวด์ของสถาบัน ให้มีความสามารถในการบริหารจัดการระบบคลาวด์ที่สอดคล้องตามความเสี่ยงที่ระบุไว้

๕.๒.๓.๕ การจัดการข้อมูลการพิสูจน์ตัวตนที่เป็นความลับของผู้ใช้ (Management of Secret Authentication Information of User)

ข้อกำหนดของสถาบัน

สถาบันต้องตรวจสอบว่ากระบวนการจัดการของผู้ให้บริการคลาวด์สำหรับการจัดสรรข้อมูลการตรวจสอบความลับ (Secret Authentication Information) เช่น รหัสผ่าน เป็นไปตามข้อกำหนดของสถาบัน

ข้อกำหนดของผู้ให้บริการคลาวด์

ผู้ให้บริการคลาวด์ต้องให้ข้อมูลเกี่ยวกับขั้นตอนการจัดการข้อมูลการตรวจสอบความลับ (Secret Authentication Information) ของผู้ใช้บริการคลาวด์ รวมถึงขั้นตอนในการจัดสรรข้อมูลดังกล่าวสำหรับการตรวจสอบสิทธิผู้ใช้งาน

๕.๒.๓.๖ การจำกัดการเข้าถึงข้อมูล (Information Access Restriction)

ข้อกำหนดของสถาบัน

สถาบันต้องตรวจสอบให้แน่ใจว่าสามารถจำกัดการเข้าถึงข้อมูลในบริการคลาวด์ได้ตามนโยบายการควบคุมการเข้าถึงและปฏิบัติตามข้อจำกัดดังกล่าว ซึ่งรวมถึงการจำกัดการเข้าถึงบริการต่าง ๆ บนระบบคลาวด์และข้อมูลของสถาบันที่เก็บไว้บนคลาวด์

ข้อกำหนดของผู้ให้บริการคลาวด์

ผู้ให้บริการคลาวด์ต้องให้การควบคุมการเข้าถึงที่อนุญาตให้กับสถาบัน เพื่อจำกัดการเข้าถึงบริการต่าง ๆ บนระบบคลาวด์ และข้อมูลของสถาบันที่เก็บไว้ในบริการ

๕.๒.๓.๗ การใช้โปรแกรมอรรถประโยชน์พิเศษ (Use of Privilege Utility Programs)

ข้อกำหนดของสถาบัน

หากอนุญาตให้ใช้โปรแกรมอรรถประโยชน์ได้ สถาบันต้องระบุโปรแกรมอรรถประโยชน์ที่จะใช้ในสภาพแวดล้อมการประมวลผลบนคลาวด์ และตรวจสอบให้มั่นใจว่าโปรแกรมเหล่านั้นไม่รบกวนการควบคุมของบริการคลาวด์

ข้อกำหนดของผู้ให้บริการคลาวด์

ผู้ให้บริการคลาวด์ต้องระบุข้อกำหนดสำหรับโปรแกรมอรรถประโยชน์ใด ๆ ที่ใช้ในบริการคลาวด์ ผู้ให้บริการคลาวด์ต้องตรวจสอบให้มั่นใจว่าการใช้โปรแกรมอรรถประโยชน์ใด ๆ ที่สามารถข้ามขั้นตอนการทำงานตามปกติ หรือการรักษาความปลอดภัยนั้นจำกัดเฉพาะเจ้าหน้าที่ที่ได้รับอนุญาตเท่านั้น และต้องมีการทบทวนและตรวจสอบการใช้โปรแกรมดังกล่าวอย่างสม่ำเสมอ

๕.๒.๔ การเข้ารหัส (Cryptography)

๕.๒.๔.๑ นโยบายเกี่ยวกับการใช้มาตรการควบคุมการเข้ารหัส (Policy of the Use of Cryptographic Controls)

ข้อกำหนดของสถาบัน

๑) สถาบันต้องใช้มาตรการควบคุมการเข้ารหัสสำหรับการใช้บริการระบบคลาวด์ที่มีความแข็งแรงเพียงพอ และสอดคล้องตามความเสี่ยงที่ได้ระบุไว้ ไม่ว่าสถาบันหรือผู้ให้บริการคลาวด์จะเป็นผู้จัดหามาตรการควบคุมการเข้ารหัสเหล่านั้นก็ตาม

๒) เมื่อผู้ให้บริการคลาวด์นำเสนอการเข้ารหัสใด ๆ สถาบันต้องตรวจสอบข้อมูลที่ผู้ให้บริการคลาวด์จัดหาให้เพื่อยืนยันว่ามีความสามารถในการเข้ารหัสดังนี้หรือไม่

- ปฏิบัติตามข้อกำหนดด้านนโยบายของผู้ใช้บริการคลาวด์
- เข้ากันได้กับการป้องกันการเข้ารหัสลับอื่น ๆ ที่ใช้โดยสถาบัน
- ใช้กับข้อมูลขณะจัดเก็บและระหว่างโอนถ่ายภายในบริการคลาวด์และนอกระบบคลาวด์

ข้อกำหนดของผู้ให้บริการคลาวด์

ผู้ให้บริการคลาวด์ต้องให้ข้อมูลแก่สถาบันเกี่ยวกับการเข้ารหัสเพื่อปกป้องข้อมูลและข้อมูลส่วนบุคคลที่ผู้ให้บริการคลาวด์ประมวลผล นอกจากนี้ ผู้ให้บริการคลาวด์ต้องให้ข้อมูลแก่สถาบันเกี่ยวกับความสามารถใด ๆ ที่ผู้ให้บริการคลาวด์มอบให้ ซึ่งสามารถช่วยให้สถาบันในการใช้การเข้ารหัสดังกล่าว

๕.๒.๔.๒ การจัดการกุญแจ (Key Management)

ข้อกำหนดของสถาบัน

๑) สถาบันต้องระบุกุญแจสำหรับการเข้ารหัสในแต่ละบริการคลาวด์ และดำเนินการตามขั้นตอนสำหรับการจัดการกุญแจ

๒) ในกรณีที่บริการคลาวด์มีฟังก์ชั่นการจัดการกุญแจสำหรับการใช้งานโดยสถาบัน สถาบันต้องขอข้อมูลดังต่อไปนี้เกี่ยวกับขั้นตอนที่ใช้ในการจัดการกุญแจสำหรับการเข้ารหัสที่เกี่ยวข้องกับบริการคลาวด์

- ประเภทกุญแจ
- ข้อกำหนดเฉพาะของระบบการจัดการ รวมถึงขั้นตอนต่าง ๆ ตลอดอายุการใช้งานของกุญแจ เข้ารหัส เช่น การสร้าง การเปลี่ยนแปลง หรือปรับปรุง จัดเก็บ หมดอายุการใช้งาน เรียกคืน เก็บรักษา และทำลาย
- ขั้นตอนการจัดการกุญแจที่แนะนำสำหรับการใช้งานโดยสถาบัน

๓) สถาบันต้องไม่อนุญาตให้ผู้ให้บริการคลาวด์ จัดเก็บและจัดการกุญแจสำหรับการเข้ารหัสเมื่อสถาบัน ใช้กุญแจเข้ารหัสของตนเอง

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

๕.๒.๕.๑ การวิเคราะห์และข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศ (information Security Requirement Analysis and Specification)

ข้อกำหนดของสถาบัน

๑) สถาบันต้องกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศสำหรับการใช้บริการคลาวด์ จากนั้นประเมินว่าบริการของผู้ให้บริการคลาวด์ สามารถตอบสนองความต้องการเหล่านี้ได้หรือไม่

๒) สำหรับการประเมินนี้ สถาบันต้องขอข้อมูลเกี่ยวกับความสามารถในการรักษาความมั่นคงปลอดภัยสารสนเทศจากผู้ให้บริการคลาวด์

ข้อกำหนดของผู้ให้บริการคลาวด์

ผู้ให้บริการคลาวด์ต้องให้ข้อมูลแก่สถาบันเกี่ยวกับความสามารถในการรักษาความมั่นคงปลอดภัยสารสนเทศที่สถาบันใช้ ข้อมูลนี้ต้องเป็นข้อมูลโดยไม่เปิดเผยข้อมูลที่อาจเป็นประโยชน์ต่อบุคลลที่มีเจตนาร้าย

๕.๒.๕.๒ นโยบายการพัฒนาที่ปลอดภัย (Secure Development Policy)

ข้อกำหนดของสถาบัน

สถาบันต้องขอข้อมูลจากผู้ให้บริการคลาวด์ เกี่ยวกับการใช้ขั้นตอนและวิธีปฏิบัติในการพัฒนาที่ปลอดภัยของผู้ให้บริการ

ข้อกำหนดของผู้ให้บริการคลาวด์

ผู้ให้บริการคลาวด์ต้องให้ข้อมูลเกี่ยวกับการใช้ขั้นตอน และวิธีปฏิบัติในการพัฒนาความปลอดภัยของตนในขอบเขตที่สอดคล้องกับนโยบายในการเปิดเผยข้อมูล

๕.๒.๖ การจัดการผู้ให้บริการภายนอก (Supplier Relationships)

๕.๒.๖.๑ นโยบายความมั่นคงปลอดภัยสารสนเทศสำหรับความสัมพันธ์กับผู้ให้บริการภายนอก (Information Security Policy for Supplier Relationship)

ข้อกำหนดของสถาบัน

สถาบันต้องระบุว่าผู้ให้บริการคลาวด์เป็นผู้ให้บริการภายนอกประเภทหนึ่งในนโยบายความมั่นคงปลอดภัยสารสนเทศสำหรับความสัมพันธ์กับผู้ให้บริการภายนอก ซึ่งจะช่วยลดความเสี่ยงที่เกี่ยวข้องกับการเข้าถึงและจัดการข้อมูลของสถาบัน

๕.๒.๖.๒ การจัดการกับการรักษาความมั่นคงปลอดภัยในข้อตกลงของผู้ให้บริการภายนอก (Addressing Security within Supplier Agreements)

ข้อกำหนดของสถาบัน

สถาบันต้องยืนยันบทบาทและความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับบริการคลาวด์ ดังที่อธิบายไว้ในข้อตกลงการให้บริการ สิ่งเหล่านี้รวมถึงกระบวนการต่อไปนี้

- การป้องกันมัลแวร์
- การสำรองข้อมูล
- มาตรการควบคุมการเข้ารหัส

- การจัดการช่องโหว่
- การจัดการเหตุการณ์
- การตรวจสอบการปฏิบัติตามข้อกำหนดทางเทคนิค
- การทดสอบความปลอดภัย
- การตรวจสอบ
- การรวบรวม การบำรุงรักษา และการปกป้องหลักฐาน รวมถึงบันทึกและเส้นทางการตรวจสอบ
- การปกป้องข้อมูลเมื่อสิ้นสุดข้อตกลงการให้บริการ
- การยืนยันตัวตน และการควบคุมการเข้าถึง
- การยืนยันตัวตน และการควบคุมการเข้าถึง
- การจัดการข้อมูลประจำตัวและการเข้าถึง

<u>ข้อกำหนดของผู้ให้บริการคลาวด์</u>

๑) ผู้ให้บริการคลาวด์ต้องระบุมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องซึ่งผู้ให้บริการคลาวด์จะนำมาใช้เป็นส่วนหนึ่งของข้อตกลงเพื่อให้แน่ใจว่าจะไม่เกิดความเข้าใจผิดระหว่างผู้ให้บริการคลาวด์กับสถาบัน สิ่งเหล่านี้อาจรวมถึงกระบวนการต่อไปนี้

- การป้องกันมัลแวร์
- -การสำรองข้อมูล
- มาตรการควบคุมการเข้ารหัส
- การจัดการช่องโหว่
- การจัดการเหตุการณ์
- การตรวจสอบการปฏิบัติตามข้อกำหนดทางเทคนิค
- การทดสอบความปลอดภัย
- การตรวจสอบ
- การรวบรวม การบำรุงรักษา และการปกป้องหลักฐาน รวมถึงบันทึกและเส้นทางการตรวจสอบ
- การปกป้องข้อมูลเมื่อสิ้นสุดข้อตกลงการให้บริการ
- การยืนยันตัวตน และการควบคุมการเข้าถึง
- การยืนยันตัวตน และการควบคุมการเข้าถึง
- การจัดการข้อมูลประจำตัวและการเข้าถึง

๒) มาตรการรักษาความมั่นคงปลอดภัยสารสนเทศที่ผู้ให้บริการคลาวด์ จะใช้อาจแตกต่างกันออกไปตามประเภทของบริการคลาวด์ที่สถาบันใช้งานอยู่

๕.๒.๖.๓ ห่วงโซ่อุปทานของเทคโนโลยีสารสนเทศและการสื่อสาร (Information and Communication Technology Supply Chain)

<u>ข้อกำหนดของผู้ให้บริการคลาวด์</u>

๑) หากผู้ให้บริการคลาวใช้บริการคลาวด์ของผู้ให้บริการคลาวด์รายย่อย ผู้ให้บริการคลาวด์ต้องตรวจสอบให้แน่ใจว่าระดับความมั่นคงปลอดภัยสารสนเทศของผู้ให้บริการคลาวด์รายย่อยนั้นได้รับการดูแลไม่น้อยกว่าของสถาบัน

๒) เมื่อผู้ให้บริการคลาวด์ให้บริการคลาวด์ตามห่วงโซ่อุปทาน ผู้ให้บริการคลาวด์ต้องกำหนดวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศแก่ผู้ให้บริการคลาวด์ภายนอก และขอให้ผู้ให้บริการภายนอกแต่ละรายดำเนินกิจกรรมการบริหารความเสี่ยงเพื่อให้บรรลุวัตถุประสงค์