ประกาศกรมบังคับคดี

เรื่อง มาตรฐานและแนวปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์

ของกรมบังคับคดี พ.ศ. ๒๕๖๙

ด้วยพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ตามมาตรา ๔๔ กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว และเพื่อให้มาตรฐานความปลอดภัยทางไซเบอร์ของกรมบังคับคดีสอดคล้องกับมาตรฐานสากล อาศัยอำนาจตามความในมาตรา ๔๖ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กรมบังคับคดีจึงออกประกาศมาตรฐานและแนวปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ ของกรมบังคับคดี พ.ศ. ๒๕๖๙ เพื่อให้เจ้าหน้าที่ในสังกัดกรมบังคับคดีถือปฏิบัติ ดังนี้

ข้อ ๑ ปฏิบัติตามมาตรฐานและแนวปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ของกรมบังคับคดี พ.ศ. ๒๕๖๙ ตามบัญชีแนบท้ายประกาศนี้

ข้อ ๒ กรณีที่มีการแก้ไขเพิ่มเติมมาตรฐานและแนวปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์โดยคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์หรือสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติที่แตกต่างไปจากที่กำหนดไว้ในประกาศนี้ให้หน่วยงานในสังกัดกรมบังคับคดีถือปฏิบัติตามที่ได้มีการแก้ไขหรือเพิ่มเติม

ประกาศ ณ วันที่ ๓๑ สิงหาคม พ.ศ. ๒๕๖๙

(นายเสกสรร สุขแสง)
อธิบดีกรมบังคับคดี

อรอุมา ตรวจ/ทาน
วิทวัฒน์ ร่าง/พิมพ์

บัญชีแนบท้ายประกาศกรมบังคับคดี
เรื่อง มาตรฐานและแนวปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์
ของกรมบังคับคดี พ.ศ. ๒๕๖๙

สารบัญ

สารบัญ

บัญชีแนบท้ายประกาศกรมบังคับคดี
เรื่อง มาตรฐานและแนวปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์ของกรมบังคับคดี
พ.ศ. ๒๕๖๙
****

๑. บทนำ

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๔๔ ได้กำหนดให้หน่วยงานของรัฐ จัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว กรมบังคับคดีในฐานะหน่วยงานของรัฐ จึงดำเนินการจัดทำมาตรฐานและแนวปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์ของกรมบังคับคดี โดยกำหนดมาตรการในการประเมินความเสี่ยง การตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์เมื่อมีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบหรือความเสียหายอย่างมีนัยสำคัญ หรืออย่างร้ายแรงต่อระบบสารสนเทศ เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ของกรมบังคับคดีปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ สอดคล้องกับมาตรฐานสากล

๒. วัตถุประสงค์

เพื่อให้การรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกรมบังคับคดีปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ และเป็นไปในทิศทางเดียวกันสอดคล้องกับมาตรฐานสากล

๓. ขอบเขตการใช้

ใช้กับกรมบังคับคดี

๔. คำนิยาม

Recovery Time Objective (RTO)	หมายถึง	ระยะเวลาในการกู้คืนระบบ
Recovery Point Objective (RPO)	หมายถึง	ระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย
Maximum Tolerance Period of Disruption (MTPD)	หมายถึง	ระยะเวลาสูงสุดที่ยอมให้ธุรกิจหยุดชะงักเพื่อรองรับการดำเนินธุรกิจอย่างต่อเนื่องของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและรองรับการเกิดเหตุการณ์ผิดปกติต่าง ๆ ที่อาจส่งผลให้เกิดการหยุดชะงักหรือเกิดความเสียหายต่อระบบ เช่น ภัยคุกคามการทำงานได้ตามปกติให้เร็วที่สุด
Business Continuity Plan	หมายถึง	แผนบริหารความต่อเนื่องทางธุรกิจ

ส่วนที่ ๑
แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์

แนวปฏิบัติ

๑. แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

กรมบังคับคดีมีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยคณะอนุกรรมการด้านความมั่นคงปลอดภัยไซเบอร์ของกระทรวงยุติธรรม รับรอง อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง โดยมีขอบเขตของการตรวจสอบอย่างน้อย ดังนี้

๑) นโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์

๒) แนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๒. การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

กรมบังคับคดีมีการกำหนดนโยบายการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามที่ระบุไว้ในนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งมีการกำหนด เรื่องโครงสร้างองค์กรและบทบาทหน้าที่ของผู้ที่เกี่ยวข้องในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และมีการจัดทำระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยจัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง ประกอบด้วยรายละเอียดอย่างน้อย ดังนี้

๒.๑ การประเมินความเสี่ยง (Risk Assessment)

๑) การระบุความเสี่ยง (Risk Identification)

ระบุถึงความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ซึ่งรวมถึงความเสี่ยงจากภัยคุกคามทางไซเบอร์ และช่องโหว่ต่าง ๆ โดยความเสี่ยงดังกล่าวอาจมีสาเหตุมาจากกระบวนการปฏิบัติงาน ระบบงาน บุคลากร หรือปัจจัยภายนอก

๒) การวิเคราะห์ความเสี่ยง (Risk Analysis)

เข้าใจและวิเคราะห์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อหาแนวทางในการจัดการความเสี่ยงที่เหมาะสม

๓) การประเมินค่าความเสี่ยง (Risk Evaluation)

ประเมินถึงโอกาสที่ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์จะเกิดขึ้นและผลกระทบต่อการปฏิบัติงานและการดำเนินธุรกิจรวมถึงกำหนดระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ (Risk Appetite)

๒.๒ การจัดการความเสี่ยง (Risk Treatment)

มีแนวทางจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อให้ความเสี่ยงที่เหลืออยู่ (Residual Risk) อยู่ในระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้

๒.๓ ติดตามและทบทวนความเสี่ยง (Risk Monitoring and Review)

มีกระบวนการที่มีประสิทธิภาพในการติดตาม และทบทวนความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้อยู่ภายใต้ระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ตามที่กำหนดไว้

๒.๔ การรายงานความเสี่ยง (Risk Reporting)

รายงานระดับความเสี่ยงและผลการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ต่อคณะอนุกรรมการ ตามรอบการประชุมของคณะอนุกรรมการ

มีการทบทวนระเบียบวิธีปฏิบัติและกระบวนการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เช่น กรณีที่มีการเปลี่ยนแปลงของระบบความมั่นคงปลอดภัยไซเบอร์ ความเสี่ยง มาตรฐานสากล อย่างมีนัยสำคัญ เป็นต้น

๓. แผนการรับมือภัยคุกคามทางไซเบอร์

กรมบังคับคดีมีการดำเนินการจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ ดังต่อไปนี้

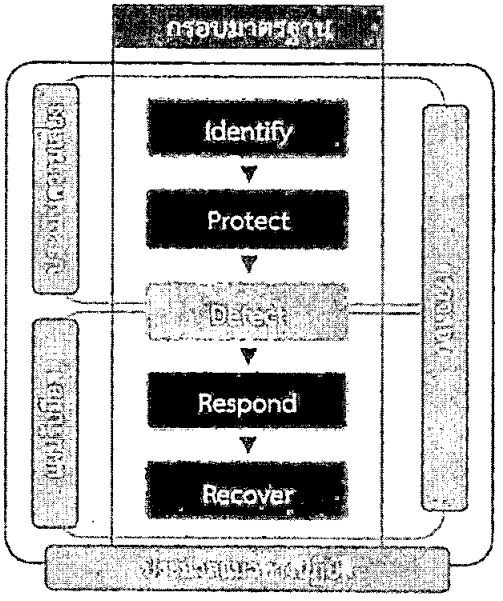
๓.๑ จัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

๓.๒ ตรวจสอบแผนการรับมือภัยคุกคามทางไซเบอร์ได้รับการสื่อสารอย่างมีประสิทธิผลไปยังบุคลากรที่เกี่ยวข้อง

๓.๓ ทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง

๓.๔ ทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ เมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญในสภาพแวดล้อมการปฏิบัติการทางไซเบอร์ของบริการที่สำคัญของกรมบังคับคดี หรือข้อกำหนดในการตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

๓.๕ ฝึกซ้อมการรับมือภัยคุกคามทางไซเบอร์อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง



รูปที่ ๑ ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๔. การรายงานสถานการณ์เกี่ยวกับด้านความมั่นคงปลอดภัยไซเบอร์

กรมบังคับคดีต้องรายงานสถานการณ์เกี่ยวกับด้านความมั่นคงปลอดภัยไซเบอร์ไปยังคณะอนุกรรมการด้านความมั่นคงปลอดภัยไซเบอร์ของกระทรวงยุติธรรมอย่างน้อย ดังนี้

๔.๑ แนวนโยบายหรือแนวปฏิบัติด้านในการรักษาความมั่นคงปลอดภัยไซเบอร์

๔.๒ เหตุการณ์ภัยคุกคามทางไซเบอร์ (Cyber Security Incident) ที่ตรวจพบ และผลดำเนินการในการตรวจสอบเหตุการณ์ภัยคุกคามทางไซเบอร์ (Cyber Security Incident) (ถ้ามี)

๔.๓ การดำเนินการเพื่อทำให้ระบบความมั่นคงปลอดภัยมีความแข็งแกร่ง (Hardening)

๔.๔ การดำเนินการทางกฎหมายที่เกี่ยวข้องในการตอบสนองต่อเหตุการณ์ภัยคุกคามทางไซเบอร์ (Cyber Security Incident)

๔.๕ การพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์

๔.๖ การรายงานปัญหาและอุปสรรคที่เกิดขึ้นในด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อหาแนวทางในการแก้ไขปัญหาที่เกิดขึ้น

ส่วนที่ ๒
มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

หัวข้อที่ ๑ การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล (Identify)

๑.๑ การจัดการทรัพย์สิน (Asset Management)

การจัดเก็บรายละเอียดข้อมูลของอุปกรณ์ด้านเทคโนโลยีสารสนเทศของฮาร์ดแวร์ (Hardware) และซอฟต์แวร์ (Software) ทั้งหมดของระบบเพื่อใช้ในการวางแผนและการบริหารด้านความมั่นคงปลอดภัยไซเบอร์

๑.๑.๑ มีทะเบียนทรัพย์สิน (Inventory) ที่ระบุทรัพย์สินด้านเทคโนโลยีสารสนเทศของฮาร์ดแวร์ (Hardware) และ ซอฟต์แวร์ (Software) และดูแลรักษาทะเบียนทรัพย์สินให้เป็นปัจจุบัน โดยทะเบียนทรัพย์สินแต่ละประเภทต้องมีข้อมูลอย่างน้อย ดังนี้

๑) ชื่อ/คำอธิบายของทรัพย์สิน
๒) ประเภทของอุปกรณ์/ยี่ห้อ
๓) ฟังก์ชันที่สำคัญของทรัพย์สิน
๔) ชื่อระบบปฏิบัติการ (Operation System) และเวอร์ชัน
๕) การระบุลำดับความสำคัญของทรัพย์สิน
๖) เจ้าของและ/หรือผู้ดำเนินการของทรัพย์สิน
๗) ตำแหน่งทางกายภาพของทรัพย์สิน
๘) การขึ้นต่อกันของทรัพย์สิน

๑.๑.๒ มีทะเบียนทรัพย์สินข้อมูล (Data Inventory) ที่ระบุข้อมูลที่เก็บไว้ภายในระบบสารสนเทศ โดยจะต้องมีการกำหนดชั้นความลับของข้อมูล (Data Classification) เพื่อให้สามารถกำหนดสิทธิในการเข้าถึงข้อมูลได้อย่างปลอดภัย โดยทะเบียนทรัพย์สินข้อมูลต้องมีข้อมูลอย่างน้อย ดังนี้

๑) ชื่อ/คำอธิบายของทรัพย์สินข้อมูล
๒) ชั้นความลับของทรัพย์สินข้อมูล
๓) มาตรการตรวจสอบความถูกต้องของทรัพย์สินข้อมูล
๔) มาตรการรักษาสภาพพร้อมใช้งาน
๕) ตำแหน่งทางกายภาพของทรัพย์สินข้อมูล
๖) เจ้าของและ/หรือผู้ดำเนินการของทรัพย์สินข้อมูล
๗) ระดับผลกระทบ

๑.๑.๓ ระบุขอบเขตเครือข่ายของบริการที่สำคัญของกรมบังคับคดีและระบบคอมพิวเตอร์ที่เชื่อมต่อโดยตรงและมีนัยสำคัญ (Direct and Significant Interface)

๑.๑.๔ มีการตรวจสอบทะเบียนทรัพย์สินอย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง หากมีการเปลี่ยนแปลงใดๆ กับทรัพย์สินของบริการที่สำคัญของกรมบังคับคดี กรมบังคับคดีจะดำเนินการปรับปรุงทะเบียนทรัพย์สินดังกล่าว

๑.๑.๕ ดำเนินการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญของกรมบังคับคดีซึ่งรวมถึงรายการทั้งหมดที่ระบุไว้ในทะเบียนทรัพย์สินในข้อ ๑.๑ อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง

๑.๑.๖ มีแผนผังเครือข่าย (Network Diagram) ของกรมบังคับคดีและปรับปรุงให้เป็นปัจจุบัน

๑.๒ การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)

การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์เพื่อเป็นการเตรียมความพร้อมในการรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่อาจจะเกิดขึ้นพร้อมทั้งหาแนวทางในการรับมือเพื่อลดความเสียหายที่จะเกิดขึ้น

๑.๒.๑ ประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง โดยต้องมีข้อมูลอย่างน้อย ดังนี้

๑) กำหนดหน้าที่และความรับผิดชอบในการบริหารและจัดการความเสี่ยง

๒) ระบุความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (IT-related risk)

๓) ประเมินความเสี่ยงที่ครอบคลุมถึงโอกาสหรือความถี่ที่จะเกิดความเสี่ยง และผลกระทบที่จะเกิดขึ้น เพื่อจัดลำดับความสำคัญในการบริหารจัดการความเสี่ยง

๔) กำหนดวิธีการหรือเครื่องมือในการบริหาร และจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

๑.๒.๒ ปรับปรุงทะเบียนความเสี่ยงทุกครั้งหลังการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ทะเบียนความเสี่ยงต้องจัดทำเอกสาร โดยมีรายละเอียดอย่างน้อย ดังนี้

๑) วันที่ระบุความเสี่ยง (Date the Risk is Identified)

๒) คำอธิบายของความเสี่ยง (Description of the Risk)

๓) โอกาสที่จะเกิดขึ้น (Likelihood of Occurrence)

๔) ความรุนแรงของเหตุการณ์ (Severity of the Occurrence)

๕) การจัดการความเสี่ยง (Risk Treatment)

๖) เจ้าของความเสี่ยง (Risk Owner)

๗) สถานะของการจัดการความเสี่ยง (Status of Risk Treatment)

๘) ความเสี่ยงที่เหลือ (Residual Risk)

๑.๓ การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)

เป็นการประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing) ทางด้านความมั่นคงปลอดภัยไซเบอร์ที่ครอบคลุมทั้งฮาร์ดแวร์ (Hardware) และซอฟต์แวร์ (Software) ว่ามีช่องโหว่ใดบ้างที่มีผลกระทบต่อความมั่นคงปลอดภัยไซเบอร์ เพื่อให้หน่วยงานทราบถึงจุดอ่อนด้านความมั่นคงปลอดภัย และแก้ไขก่อนที่จะเกิดเหตุการณ์ที่ส่งผลกระทบต่อระบบสารสนเทศ

๑.๓.๑ ประเมินช่องโหว่ของอุปกรณ์ เพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัย และการควบคุมโดยครอบคลุมบริการที่สำคัญของระบบเทคโนโลยีสารสนเทศ (Information Technology system)

๑.๓.๒ กรมบังคับคดีจะดำเนินการให้แน่ใจว่าขอบเขตของการประเมินช่องโหว่แต่ละรายการประกอบด้วย

๑) การประเมินความมั่นคงปลอดภัยของโฮสต์ (Host Security Assessment)

๒) การประเมินความมั่นคงปลอดภัยของเครือข่าย (Network Security Assessment)

๓) การตรวจสอบความมั่นคงปลอดภัยของสถาปัตยกรรม (Architecture Security Review)

๑.๓.๓ ประเมินช่องโหว่ของบริการที่สำคัญของกรมบังคับคดี เพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัยและควบคุมก่อนที่จะทำการทดสอบระบบใหม่ใดๆ ที่เชื่อมต่อหรือดำเนินการเปลี่ยนแปลงระบบที่สำคัญใดๆ กับบริการที่สำคัญของหน่วยงาน การเปลี่ยนแปลงระบบที่สำคัญ ได้แก่ การเพิ่มโมดูลแอปพลิเคชัน (Adding New Application Module) การปรับปรุงระบบ และการปรับเปลี่ยนเทคโนโลยี

๑.๓.๔ ดำเนินการทดสอบเจาะระบบ (Penetration Testing) บริการที่สำคัญของกรมบังคับคดี โดยเฉพาะอย่างยิ่งระบบเทคโนโลยีสารสนเทศ (Information Technology system) ที่เชื่อมต่อกับระบบเครือข่าย

สื่อสารสาธารณะ (Internet Facing) ให้สอดคล้องกับระดับของความเสี่ยง และพิจารณาผลกระทบหรือความเสี่ยงจากการทดสอบเจาะระบบด้วย

๑.๓.๕ มีการตรวจสอบให้แน่ใจว่าขอบเขตของการทดสอบเจาะระบบ (Scope of a Penetration Test) รวมถึงการทดสอบเจาะระบบของโฮสต์ เครือข่าย และแอปพลิเคชันของบริการที่สำคัญของกรมบังคับคดี โดยเฉพาะอย่างยิ่งทุกระบบที่มีการเชื่อมต่อกับระบบเครือข่ายสื่อสารสาธารณะโดยตรง (Internet Facing)

๑.๓.๖ มีการดำเนินการทดสอบเจาะระบบอย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง ตามความจำเป็น เพื่อตรวจสอบความถูกต้องของระบบรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญของกรมบังคับคดี ก่อนที่จะทำการทดสอบระบบใหม่หรือการเปลี่ยนแปลงระบบที่สำคัญ เช่น โมดูลเสริม การปรับปรุงระบบ และการปรับเปลี่ยนเทคโนโลยี เป็นต้น

๑.๔ การจัดการผู้ให้บริการภายนอก (Third Party Management)

การจัดให้มีการกำกับดูแลการบริหารจัดการความเสี่ยงจากการใช้บริการการเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก โดยประกอบด้วยการกำหนดบทบาทหน้าที่และความรับผิดชอบของผู้ให้บริการภายนอก

๑.๔.๑ ต้องรับผิดชอบ (Responsible) และมีภาระรับผิดชอบ (Accountable) ต่อการดูแลรักษาความมั่นคงปลอดภัยไซเบอร์ แม้ว่าผู้ให้บริการภายนอกจะดำเนินงานใดๆ ก็ตามในส่วนของบริการที่สำคัญของหน่วยงาน

๑.๔.๒ มีข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์เพื่อลดความเสี่ยงที่เกี่ยวข้องกับการเข้าถึง กระบวนการจัดเก็บ การสื่อสาร และการดำเนินการ ของผู้ให้บริการภายนอกในข้อตกลงระดับการให้บริการ (Service Level Agreement) หรือเงื่อนไขของสัญญากับผู้ให้บริการภายนอก ข้อกำหนดต้องคำนึงถึงรายละเอียดอย่างน้อย ดังนี้

๑) ประเภทของผู้ให้บริการภายนอกที่เข้าถึงทรัพย์สินของบริการที่สำคัญของกรมบังคับคดี ตามความต้องการทางธุรกิจขององค์กร และโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๒) ภาระหน้าที่ของผู้ให้บริการภายนอก ในการปกป้องบริการที่สำคัญของกรมบังคับคดี จากภัยคุกคามทางไซเบอร์

๓) ความเสี่ยงที่เกี่ยวข้องกับบริการและห่วงโซ่อุปทานผลิตภัณฑ์

๔) สิทธิ์ของกรมบังคับคดีในการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการภายนอก

๑.๔.๓ มีการสร้างกระบวนการตรวจสอบความถูกต้องของผู้ให้บริการภายนอกว่าสอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ในเงื่อนไขของสัญญา ตัวอย่างเช่น การตรวจสอบโดยบุคคลที่สาม และการตรวจสอบผลิตภัณฑ์ เป็นต้น

๑.๔.๔ มีการดำเนินการเจรจาต่อรองเงื่อนไขของสัญญาจ้างให้สอดคล้องกับกรณีที่มีข้อกำหนดทางกฎหมายหรือข้อบังคับใหม่

หัวข้อที่ ๒ มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)

๒.๑ การควบคุมการเข้าถึง (Access Control)

การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอกในการเข้าถึงบริการที่สำคัญของหน่วยงาน

๒.๑.๑ กรมบังคับคดีมีการควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัยอย่างน้อย ดังนี้

๑) การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

๒) การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

๓) การควบคุมการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ระบบเครือข่าย

๔) การควบคุมการเข้าถึงระบบงานและแอปพลิเคชัน

๕) การบริหารจัดการการเข้าถึงด้านระบบเทคโนโลยีสารสนเทศของผู้ใช้งาน

๒.๑.๒ กรมบังคับคดีมีการกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง โดยกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาตการกำหนดสิทธิหรือการมอบอำนาจของหน่วยงาน ให้สอดคล้องกับหน้าที่ความรับผิดชอบของเจ้าหน้าที่

๒.๑.๓ กรมบังคับคดีมีการกำหนดเกี่ยวกับประเภทของข้อมูล ลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึงและช่องทางการเข้าถึง

๒.๑.๔ กรมบังคับคดีมีการตรวจสอบให้แน่ใจว่าการเข้าถึงอินเทอร์เฟซ (Interface) ของบริการที่สำคัญของกรมบังคับคดี (เช่น USB, พอร์ตอนุกรม) และการเข้าถึงทางลอจิคอล (Logical) มีการกำกับดูแลโดยทางศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเท่านั้น

๒.๑.๕ กรมบังคับคดีมีการเก็บรักษาบันทึกข้อมูลการเข้าถึงทั้งหมด (Logs of All Access) และความพยายามทั้งหมดในการเข้าถึงบริการที่สำคัญของกรมบังคับคดี

๒.๑.๖ ในการเข้าถึงระบบสารสนเทศของกรมบังคับคดีต้องมีการเข้ารหัส Transaction ที่มีความปลอดภัย เช่น Secure Socket Layer (SSL) หรือ Transport Layer Security (TLS) เป็นต้น โดยต้องใช้ใบรับรอง (Certificate) ที่มีความปลอดภัย

๒.๒ การทำให้ระบบมีความแข็งแกร่ง (System Hardening)

๒.๒.๑ กรมบังคับคดีมีการสร้างมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) สำหรับระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่ายทั้งหมดของบริการที่สำคัญของกรมบังคับคดี

๒.๒.๒ กรมบังคับคดีมีการจัดทำมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ต้องมีหลักการรักษาความมั่นคงปลอดภัยอย่างน้อย ดังนี้

๑) สิทธิพิเศษในการเข้าถึงน้อยที่สุด (Least Access Privilege)

๒) การแบ่งแยกหน้าที่ (Separation of Duties)

๓) การบังคับใช้นโยบายความซับซ้อนของรหัสผ่าน

๔) การลบบัญชีที่ไม่ได้ใช้

๕) การลบบริการและแอปพลิเคชันที่ไม่จำเป็น เช่น การลบคอมไพเลอร์ (Removal of Compiler) และแอปพลิเคชันสนับสนุนผู้ให้บริการภายนอก (Vendor Support Application)

๖) การปิดพอร์ตเครือข่ายที่ไม่ได้ใช้งาน

๗) การป้องกันมัลแวร์ (Malware)

๘) การปรับปรุงซอฟต์แวร์และแพตช์ (Patch) ความมั่นคงปลอดภัยของระบบ อย่างทันการณ์และเหมาะสม

๒.๒.๓ กรมบังคับคดีมีการตรวจสอบให้แน่ใจว่ามีการใช้มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ตามที่ระบุไว้ก่อนที่จะมีอุปกรณ์ใดๆ เชื่อมต่อหรือเมื่อมีการเปลี่ยนแปลงหรือปรับปรุงบริการที่สำคัญของกรมบังคับคดี

๒.๒.๔ กรมบังคับคดีมีการตรวจสอบมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standard) ของบริการที่สำคัญอย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง เพื่อให้แน่ใจว่ามาตรฐานเหล่านี้ยังคงมีประสิทธิภาพต่อภัยคุกคามทางไซเบอร์

๒.๒.๕ กรมบังคับคดีมีการจัดทำกระบวนการจัดการเปลี่ยนแปลง (Change Management Process) เพื่ออนุญาตและตรวจสอบความถูกต้องของการเปลี่ยนแปลงระบบทั้งหมดที่มีต่อบริการที่สำคัญของกรมบังคับคดี

๒.๓ การเชื่อมต่อระยะไกล (Remote Control)

๒.๓.๑ กรมบังคับคดีมีการตรวจสอบให้แน่ใจว่าการเชื่อมต่อระยะไกลทั้งหมดมายังบริการที่สำคัญของกรมบังคับคดีมีมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพ เพื่อป้องกันและตรวจจับการเข้าถึงโดยไม่ได้รับอนุญาต

๒.๓.๒ สำหรับการเชื่อมต่อระยะไกลกับบริการที่สำคัญของกรมบังคับคดีต้องปฏิบัติตามแนวทางปฏิบัติ ดังนี้

๑) เปิดใช้งานการเชื่อมต่อระยะไกล เมื่อจำเป็นและได้รับการอนุญาตเท่านั้น

๒) ควรใช้งานโปรโตคอลที่ปลอดภัย เช่น Internet Protocol Security (IPSEC)

๓) ต้องทำการเชื่อมต่อระยะไกลผ่านช่องทางระบบเครือข่ายเสมือน Virtual Private Network (VPN)

๔) มีเทคนิคการพิสูจน์ตัวตน (Authentication Techniques) ที่มีความมั่นคงปลอดภัยในการส่ง (Transmission Security) และความสมบูรณ์ของข้อความ (Message Integrity) ที่แข็งแกร่ง เช่น การยืนยันตัวตนแบบสองปัจจัย (Two-Factor Authentication) กำหนดระยะเวลาในการเปลี่ยนรหัสผ่านตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างสม่ำเสมอ

๕) ใช้การเข้ารหัสสำหรับการเชื่อมต่อเครือข่ายทั้งหมด เช่น https, ssh, scp เป็นต้น

๖) ไม่อนุญาตให้เชื่อมต่อระยะไกลจากการใช้คำสั่งระบบ (Issuing System Commands) ที่จะส่งผลกระทบต่อการดำเนินการบริการที่สำคัญของกรมบังคับคดีเว้นแต่จะได้รับอนุญาต

๗) จำกัดการไหลของข้อมูลเฉพาะฟังก์ชันขั้นต่ำที่จำเป็นสำหรับการเชื่อมต่อ

๒.๔ สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)

๒.๔.๑ กรมบังคับคดีมีการตรวจสอบให้แน่ใจว่ามีการใช้การควบคุมอย่างเข้มงวดในการเชื่อมต่อสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์แบบพกพา เช่น แล็ปท็อป กับบริการที่สำคัญของกรมบังคับคดีโดยใช้มาตรการอย่างน้อย ดังนี้

๑) ในกรณีที่มีฟังก์ชันให้ปิดใช้งานพอร์ตการเชื่อมต่อภายนอกทั้งหมด เช่น พอร์ต USB ที่รองรับสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์แบบพกพา และเปิดใช้งานเมื่อจำเป็นเท่านั้น

๒) ใช้สื่อบันทึกข้อมูลที่ได้รับอนุญาตเท่านั้น

๓) ตรวจสอบว่าสื่อบันทึกข้อมูลแบบถอดได้และอุปกรณ์คอมพิวเตอร์พกพาทั้งหมดไม่มีมัลแวร์ก่อนที่จะเชื่อมต่อกับบริการที่สำคัญของกรมบังคับคดี

๒.๔.๒ กรมบังคับคดีมีการเข้ารหัสข้อมูลที่ละเอียดอ่อนทั้งหมดของบริการที่สำคัญของกรมบังคับคดีบนสื่อบันทึกข้อมูลแบบถอดได้

๒.๔.๓ กรมบังคับคดีมีการกำหนดวิธีการที่ปลอดภัยในการทำลายสื่อบันทึกข้อมูลแบบถอดได้เพื่อป้องกันการรั่วไหลของข้อมูล

๒.๕ การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)

๒.๕.๑ กรมบังคับคดีมีการเผยแพร่ ประชาสัมพันธ์ เกี่ยวกับแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์และสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับผู้ใช้งาน ในลักษณะเกร็ดความรู้หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย

๒.๕.๒ กรมบังคับคดีมีการจัดทำ ปรับปรุงคู่มือการใช้งานระบบสารสนเทศให้เป็นปัจจุบัน และมีการเผยแพร่ผ่านช่องทางที่เหมาะสม

๒.๕.๓ กรมบังคับคดีมีการจัดฝึกอบรมการใช้งานระบบสารสนเทศให้มีความปลอดภัยอย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง หรือเมื่อมีการปรับปรุงและเปลี่ยนแปลงการใช้งานของระบบสารสนเทศ

๒.๕.๔ กรมบังคับคดีมีการสร้างความตระหนัก (Awareness Program) เรื่องการรักษาความมั่นคงปลอดภัยไซเบอร์ ความเสี่ยงด้านเทคโนโลยีสารสนเทศ การใช้งานระบบอย่างปลอดภัย ให้แก่บุคลากรทุกระดับ

๒.๕.๕ กรมบังคับคดีมีการจัดให้มีการฝึกอบรมและพัฒนาความรู้ความเชี่ยวชาญให้ครอบคลุมและเพียงพอต่อการปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์กับเจ้าหน้าที่ที่ดูแลระบบสารสนเทศ

๒.๖ การแบ่งปันข้อมูล (Information Sharing)

กรมบังคับคดีมีการกำหนดขั้นตอนเพื่อแบ่งปันข้อมูลเกี่ยวกับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์และภัยคุกคามทางไซเบอร์ โดยต้องรายงานต่อคณะอนุกรรมการด้านความมั่นคงปลอดภัยไซเบอร์ กระทรวงยุติธรรม

หัวข้อที่ ๓ มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Treat Detection and Monitoring) การตรวจสอบการกระทำหรือการดำเนินการใดๆ โดยมิชอบ โดยใช้เครื่องคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมที่ไม่พึงประสงค์ ซึ่งมีจุดมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลที่เกี่ยวข้อง เพื่อให้อยู่ภายใต้ระดับความเสี่ยงด้านไซเบอร์ที่ยอมรับได้ตามที่กำหนดไว้ โดยกรมบังคับคดีมีกระบวนการในการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ ดังนี้

๓.๑ มีกระบวนการในการตรวจจับเหตุการณ์ผิดปกติที่กระทบต่อความมั่นคงปลอดภัยไซเบอร์

๓.๒ มีกระบวนการในการจัดประเภทและวิเคราะห์เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ

๓.๓ มีกระบวนการในการระบุว่ามีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับบริการที่สำคัญของกรมบังคับคดี

๓.๔ ต้องดำเนินการตรวจสอบกลไกและกระบวนการเฝ้าระวังภัยคุกคามทางไซเบอร์อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง เพื่อให้แน่ใจว่ากลไกและกระบวนการต่าง ๆ ยังคงมีประสิทธิภาพ

หัวข้อที่ ๔ มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)

มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond) ซึ่งมีแผนเกี่ยวข้องกับการตรวจพบภัยคุกคามทางไซเบอร์ จำนวน ๒ แผน ดังนี้

๔.๑ แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

กรมบังคับคดีมีการจัดทำการสื่อสาร ฝึกซ้อม ทบทวน และปรับปรุง แผนการรับมือภัยคุกคามทางไซเบอร์ตามที่ระบุไว้ในประมวลแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างน้อย ปีละ

๑ (หนึ่ง) ครั้ง เพื่อให้แน่ใจว่าแผนการรับมือภัยคุกคามทางไซเบอร์สามารถดำเนินการได้อย่างมี ประสิทธิภาพและประสิทธิผล

๔.๒ แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)

๔.๒.๑ กรมบังคับคดีมีการจัดทำแผนการสื่อสารในภาวะวิกฤตเพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

๔.๒.๒ กรมบังคับคดีมีการตรวจสอบแผนการสื่อสารในภาวะวิกฤต

๑) จัดตั้งทีมสื่อสารในภาวะวิกฤตเพื่อเปิดใช้งานในช่วงวิกฤต

๒) ระบุสถานการณ์จำลองเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เป็นไปได้และแผนการดำเนินการที่เกี่ยวข้อง

๓) ระบุกลุ่มเป้าหมาย และผู้มีส่วนได้ส่วนเสียสำหรับสถานการณ์จำลองเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์แต่ละประเภท

๔) ระบุโฆษกหลักและผู้เชี่ยวชาญด้านเทคนิคที่จะเป็นตัวแทนขององค์กรเมื่อกล่าวแถลงกับสื่อมวลชน

๕) ระบุแพลตฟอร์มหรือช่องทางการเผยแพร่ที่เหมาะสม เช่น สื่อดั้งเดิมและโซเชียลมีเดียสำหรับการเผยแพร่ข้อมูล

๔.๒.๓ กรมบังคับคดีมีการตรวจสอบแผนการสื่อสารในภาวะวิกฤต รวมถึงการประสานงานระหว่างทุกฝ่ายที่ได้รับผลกระทบเพื่อให้แน่ใจว่ามีการตอบสนองที่ประสานกันและสอดคล้องกันในช่วงวิกฤต

๔.๒.๔ กรมบังคับคดีมีการดำเนินการฝึกซ้อมแผนการสื่อสารในภาวะวิกฤตอย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง เพื่อให้แน่ใจว่าสามารถสื่อสารและเผยแพร่ข้อมูลได้อย่างทันท่วงทีและมีประสิทธิผล ในช่วงวิกฤตอันเนื่องมาจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

หัวข้อที่ ๕ มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery)

การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery) เมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือเมื่อหน่วยงานได้รับแจ้งเตือนการเกิดภัยคุกคามทางไซเบอร์ หน่วยงานควรกำหนดแนวทางการดำเนินมาตรการเพื่อระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ (containment, eradication, and recovery) โดยการดำเนินการดังกล่าวควรกำหนดให้สอดคล้องกับความรุนแรงและระดับของภัยคุกคามทางไซเบอร์แต่ละระดับจนกระทั่งสามารถกู้คืนทรัพย์สินสำคัญทางสารสนเทศให้กลับมาดำเนินงานหรือให้บริการได้ตามปกติ ซึ่งการดำเนินการในขั้นตอนนี้ อาจต้องกระทำควบคู่ไปกับการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ที่อาจมีการลุกลามหรือทวีความรุนแรงมากขึ้น

๕.๑ กรมบังคับคดีมีการจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) เพื่อให้แน่ใจว่าบริการที่สำคัญของกรมบังคับคดี สามารถให้บริการที่จำเป็นต่อไปได้ในกรณีที่เกิดการหยุดชะงักเนื่องจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ เพื่อให้สามารถใช้ปฏิบัติงานได้จริงเพื่อพิจารณาความสอดคล้องกับแผนของหน่วยงาน เช่น ความสอดคล้องกันของขอบเขตคำนิยามและการกำหนดระยะเวลาที่สำคัญ Maximum Tolerable Period of Disruption (MTPD), Recovery Time Objective (RTO) และ Recovery Point Objective (RPO) เป็นต้น โดยมีรายละเอียดอย่างน้อย ดังนี้

๕.๑.๑ จัดลำดับความสำคัญของความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์และระบบสารสนเทศโดยต้องพิจารณาจากปัจจัยที่สำคัญ เช่น ผลกระทบของการหยุดชะงัก ระยะเวลาที่ยอมรับได้ของการหยุดชะงัก ลำดับความสำคัญในการกู้คืนระบบ เป็นต้น

๕.๑.๒ จัดทำแผนกู้คืนภาวะวิกฤต สำหรับกระบวนการดำเนินงานของหน่วยงานที่ใช้ทรัพย์สินสารสนเทศที่มีระดับการป้องกันความมั่นคงปลอดภัย "สูง" หรือ "สูงสุด" เพื่อให้มั่นใจว่าสามารถดำเนินงานได้อย่างต่อเนื่อง มีการควบคุมดูแล การแก้ไขและกู้คืนระบบ เมื่อเกิดเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์และระบบสารสนเทศ

๕.๒ กรมบังคับคดีมีการตรวจสอบให้แน่ใจว่ามีการฝึกซ้อมแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง เพื่อประเมินประสิทธิภาพของแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) ต่อภัยคุกคามทางไซเบอร์และเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

๕.๓ ในกรณีตรวจพบภัยคุกคามทางไซเบอร์ (Cyber Security Incident) กรมบังคับคดีจะดำเนินการจัดทำรายงานภัยคุกคามทางไซเบอร์ (Incident Report) โดยรายงานความคืบหน้าของการดำเนินการให้คณะอนุกรรมการด้านความมั่นคงปลอดภัยไซเบอร์ของกระทรวงยุติธรรมทราบทุกระยะ

หัวข้อที่ ๖ มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์

มาตรฐานฉบับนี้กำหนดความเสี่ยงจากการใช้บริการระบบคลาวด์เป็น ๒ ประเภท ได้แก่ ความเสี่ยงจากผู้ใช้บริการคลาวด์ (Cloud Service Customer : CSC) และความเสี่ยงจากผู้ให้บริการคลาวด์ (Cloud Service Provider : CSP) เนื่องจากความเสี่ยงจากการใช้บริการคลาวด์มาจาก ๒ ส่วนคือ ความเสี่ยงอันเกิดจากผู้ใช้บริการคลาวด์ และความเสี่ยงอันเกิดจากผู้ให้บริการคลาวด์ ดังนั้น มาตรฐานฉบับนี้จึงอาศัยหลักการเรื่องความร่วมรับผิดชอบ (Share Responsibilities) ให้กับทั้งผู้ใช้บริการคลาวด์ (CSC) และผู้ให้บริการคลาวด์ (CSP) ซึ่งจะทำให้สามารถลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่มีต่อระบบคลาวด์ได้อย่างครอบคลุม และมีประสิทธิภาพ นอกจากนี้ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญ ทางสารสนเทศ ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มีการใช้งานระบบ สารสนเทศและข้อมูลสารสนเทศซึ่งมีระดับผลกระทบ (Criticality) และระดับความอ่อนไหว(Sensitivity) ที่แตกต่างกัน ประกอบกับประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๖ กำหนดให้หน่วยงานดังกล่าวมีการประเมินและจัดระดับผลกระทบที่อาจเกิดขึ้นตามวัตถุประสงค์ ด้านความมั่นคงปลอดภัยไซเบอร์ (Security Objectives) ดังนั้น มาตรฐานฉบับนี้จึงกำหนดให้มีข้อกำหนดขั้นต่ำ ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Baseline) เป็น ๓ ระดับ คือ ระดับต่ำ ระดับกลาง และระดับสูง เพื่อให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐาน สำคัญทางสารสนเทศ สามารถปฏิบัติตามมาตรฐานฉบับนี้ได้อย่างมีประสิทธิภาพ โดยมีค่าใช้จ่ายที่เหมาะสมกับประโยชน์ที่จะได้รับ นอกจากนี้ ผู้ให้บริการคลาวด์ (Cloud Service Provider : CSP) ที่จะให้บริการกับหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ มีหน้าที่ต้องดำเนินการให้เป็นไปตามที่หน่วยงานดังกล่าวร้องขอด้วย

๖.๑ กระบวนการตรวจรับรองมาตรฐาน

๖.๑.๑ ประเภทของการตรวจรับรอง

- การประเมินตนเอง (Self-assessment) เป็นการประเมินหน่วยงานของตนตามรูปแบบที่สำนักงานกำหนด พร้อมแนบหลักฐานและขออนุมัติไปยังผู้บริหารสูงสุดของหน่วยงาน โดยเก็บรักษาไว้ที่หน่วยงานและส่งให้สำนักงานด้วย

- การตรวจรับรองโดยหน่วยงานควบคุมหรือกำกับดูแล (Attestation) เป็นการตรวจให้การรับรองโดยหน่วยงานควบคุมหรือกำกับดูแลตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมายการควบคุมและกำกับดูแล

- การตรวจรับรองโดยหน่วยงานให้บริการตรวจรับรอง (Certify Body) เป็นการตรวจให้การรับรองโดยหน่วยงานให้บริการตรวจรับรองในระดับขั้นก้าวหน้าหรือสูงกว่า ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๖ ทั้งนี้ ในช่วงแรกของการดำเนินการที่สำนักงานยังมิได้ให้การรับรองหน่วยงานให้บริการตรวจรับรอง อาจดำเนินการโดยหน่วยงานให้บริการตรวจรับรองตามมาตรฐานสากลที่สำนักงานประกาศกำหนดก็ได้

๖.๑.๒ ความถี่ในการตรวจรับรอง

๖.๑.๒.๑ กรณีของผู้ใช้บริการคลาวด์

- ผลกระทบระดับต่ำ : ให้ดำเนินการประเมินตนเอง (Self-assessment) รวมทั้งมีการทบทวน อย่างน้อยปีละ 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 และการตรวจสำรวจในปีที่ ๒ และ ๓

๖.๑.๒.๒ กรณีของผู้ให้บริการคลาวด์

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

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

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

๖.๑.๔ ในกรณีที่ผู้ให้บริการคลาวด์ ได้รับการรับรองตามมาตรฐาน CSA STAR Level ๒/CCM แล้วก็ไม่จำเป็นต้องดำเนินการตรวจรับรองตามมาตรฐาน CSA STAR Level ๑/CCM Lite

๖.๒ ข้อกำหนดขั้นต่ำและการตรวจรับรองสำหรับผู้ใช้บริการคลาวด์และผู้ให้บริการคลาวด์

ตารางข้อกำหนดขั้นต่ำและการตรวจรับรองสำหรับผู้ใช้บริการคลาวด์และผู้ให้บริการคลาวด์

ประเภทข้อมูลหรือระบบสารสนเทศ	ข้อกำหนดขั้นต่ำ	การตรวจรับรองสำหรับผู้ใช้บริการคลาวด์	การตรวจรับรองสำหรับผู้ให้บริการคลาวด์
ผลกระทบระดับต่ำ	ข้อกำหนดส่วนที่ ๑ - เฉพาะข้อ ๖.๓.๑.๑, ๖.๓.๑.๒ ข้อกำหนดส่วนที่ ๒ - เฉพาะข้อ ๖.๓.๒.๑, ๖.๓.๒.๒, ๖.๓.๒.๓, ๖.๓.๒.๔, ๖.๓.๒.๘, ๖.๓.๒.๙	ประเมินตนเอง (Self-assessment) พร้อมแนบหลักฐานและขออนุมัติไปยังผู้บริหารสูงสุดของหน่วยงาน โดยเก็บรักษาไว้ที่หน่วยงานและส่งให้สำนักงานด้วย	ได้รับการรับรองโดยหน่วยงานให้บริการตรวจรับรอง (Certify Body) ตามวงรอบ ๓ ปี ประกอบด้วยการตรวจรับรองในปีที่ ๑ และการตรวจสำรวจในปีที่ ๒ และ ๓ และได้รับการรับรองตามมาตรฐาน ISO/IEC ๒๗๐๐๑ Certification และ CSA STAR Level ๑/CCM Lite เป็นอย่างน้อย
ผลกระทบระดับกลาง	ข้อกำหนดส่วนที่ ๑ - ทุกข้อ ข้อกำหนดส่วนที่ ๒ - เฉพาะข้อ ๖.๓.๒.๑, ๖.๓.๒.๒, ๖.๓.๒.๓, ๖.๓.๒.๔, ๖.๓.๒.๗, ๖.๓.๒.๘, ๖.๓.๒.๙, ๖.๓.๒.๑๐	ได้รับการรับรองโดยหน่วยงานควบคุมหรือกำกับดูแล (Attestation) หรือได้รับการรับรองโดยหน่วยงานให้บริการตรวจรับรอง (Certify Body) ตามวงรอบ ๓ ปี ประกอบด้วยการตรวจรับรองในปีที่ ๑ , ๒ และ ๓	ได้รับการรับรองโดยหน่วยงานให้บริการตรวจรับรอง (Certify Body) ตามวงรอบ ๓ ปี ประกอบด้วยการตรวจรับรองในปีที่ ๑ , ๒ และ ๓ และได้รับการ รับรองตามมาตรฐาน CSA STAR Level ๒/CCM และ ISO/IEC๒๗๗๐๑ Certification เป็นอย่างน้อย
ผลกระทบระดับสูง	ข้อกำหนดส่วนที่ ๑ - ทุกข้อ ข้อกำหนดส่วนที่ ๒ - ทุกข้อ	ได้รับการรับรองโดหน่วยงานให้บริการตรวจรับรอง (Certify Body) ตามวงรอบ ๓ ปี ประกอบด้วยการตรวจรับรองในปีที่ ๑ , ๒ และ ๓	ได้รับการรับรองโดยหน่วยงาน ให้บริการตรวจรับรอง (Certify Body) ตามวงรอบ ๓ ปี ประกอบด้วย การตรวจรับรองในปีที่ ๑ , ๒ และ ๓ และได้รับการรับรอง

ประเภทข้อมูลหรือระบบสารสนเทศ	ข้อกำหนดขั้นต่ำ	การตรวจรับรองสำหรับผู้ใช้บริการคลาวด์	การตรวจรับรองสำหรับผู้ให้บริการคลาวด์
			ตามมาตรฐาน ISO/IEC ๒๗๐๑๗ Certification หรือ CSA STAR Level ๒/CCM และ ISO/IEC ๒๗๐๑๘ Certification และ ISO/IEC ๒๗๗๐๑ Certification เป็นอย่างน้อย

๖.๓. มาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์

๖.๓.๑ การกำกับดูแลด้านความมั่นคงปลอดภัยระบบคลาวด์ (Cloud Security Governance)

๖.๓.๑.๑ นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Policies)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ต้องกำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศสำหรับการประมวลผลบนคลาวด์ให้เป็นนโยบายเฉพาะหัวข้อของผู้ใช้บริการคลาวด์นโยบายความมั่นคงปลอดภัยสารสนเทศสำหรับการประมวลผลบนคลาวด์ของผู้ใช้บริการคลาวด์ต้องสอดคล้องกับระดับความเสี่ยงที่ยอมรับได้ด้านความมั่นคงปลอดภัยสารสนเทศที่มีต่อข้อมูลและทรัพย์สินอื่นๆ ขององค์กร ข) เมื่อกำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศสำหรับการประมวลผลบนคลาวด์ ผู้ใช้บริการคลาวด์ต้องคำนึงถึงสิ่งต่อไปนี้ - ข้อมูลที่จัดเก็บในสภาพแวดล้อมการประมวลผลบนคลาวด์อาจอยู่ภายใต้การเข้าถึงและการจัดการโดยผู้ให้บริการคลาวด์ - ทรัพย์สินขององค์กรอาจจะได้รับการดูแลรักษาในสภาพแวดล้อมการประมวลผลบนคลาวด์ เช่น โปรแกรมแอปพลิเคชัน - กระบวนการต่างๆ สามารถทำงานบนบริการคลาวด์เสมือนจริงที่มีผู้ใช้หลายราย - ผู้ใช้บริการคลาวด์และบริบทที่ใช้บริการคลาวด์ - ผู้ดูแลระบบบริการคลาวด์ของผู้ใช้บริการคลาวด์ที่ได้รับสิทธิพิเศษในการเข้าถึง	ก) ผู้ให้บริการคลาวด์ต้องเพิ่มนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศเพื่อจัดการกับการจัดหาและใช้บริการคลาวด์โดยคำนึงถึงสิ่งต่อไปนี้ - ข้อกำหนดขั้นต่ำด้านความมั่นคงปลอดภัยสารสนเทศที่ใช้กับการออกแบบและการใช้งานบริการคลาวด์ - ความเสี่ยงจากบุคคลภายในที่ได้รับอนุญาต - การเช่าหลายราย และการแยกผู้ใช้บริการคลาวด์ (รวมถึงการจำลองเสมือน) - การเข้าถึงทรัพย์สินของผู้ใช้บริการคลาวด์โดยเจ้าหน้าที่ของผู้ให้บริการคลาวด์ - ขั้นตอนการควบคุมการเข้าถึง เช่น การยืนยันตัวตนที่เข้มงวดสำหรับการเข้าถึงบริการคลาวด์ของผู้ดูแลระบบ - การสื่อสารกับผู้ใช้บริการคลาวด์ระหว่างการจัดการการเปลี่ยนแปลง - ความปลอดภัยของการจำลองเสมือน - การเข้าถึงและปกป้องข้อมูลของผู้ใช้บริการคลาวด์ - การจัดการวงจรชีวิตของบัญชีผู้ใช้บริการคลาวด์ - การสื่อสารกรณีเกิดเหตุละเมิดและแนวทางการแบ่งปันข้อมูลเพื่อช่วยในการสืบสวนและนิติเวช

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
- ตำแหน่งทางภูมิศาสตร์ขององค์กรของผู้ให้บริการคลาวด์ และประเทศที่ผู้ให้บริการคลาวด์สามารถจัดเก็บข้อมูลผู้ใช้บริการคลาวด์ได้ (แม้จะเป็นการชั่วคราว) ค) นโยบายคุ้มครองข้อมูลส่วนบุคคลของผู้ใช้บริการคลาวด์ต้องระบุข้อความเกี่ยวกับข้อตกลงทางสัญญาระหว่างผู้ประมวลผลข้อมูลส่วนบุคคลบนคลาวด์ และผู้ใช้บริการคลาวด์ ง) ข้อตกลงทางสัญญาต้องกำหนดความรับผิดชอบระหว่างผู้ประมวลผลข้อมูลส่วนบุคคลบนคลาวด์ ผู้รับจ้างช่วง(Sub-contractors) และผู้ใช้บริการคลาวด์อย่างชัดเจน โดยพิจารณาจากประเภทของบริการคลาวด์ (เช่น บริการประเภท IaaS, PaaS หรือ SaaS) ตัวอย่างเช่น การกำหนดความรับผิดชอบในการควบคุมระดับแอปพลิเคชันอาจแตกต่างกันขึ้นอยู่กับว่าผู้ประมวลผลข้อมูลส่วนบุคคลบนคลาวด์นั้นให้บริการ SaaS หรือ PaaS หรือ IaaS	

๖.๓.๑.๒ โครงสร้างองค์กรด้านความมั่นคงปลอดภัยสารสนเทศ (Organization of Information Security)

๖.๓.๑.๒.๑ บทบาทและความรับผิดชอบด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security Roles and Responsibilities)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ต้องมีการตกลงกับผู้ให้บริการคลาวด์เกี่ยวกับการแบ่งบทบาทหน้าที่และความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศอย่างเหมาะสม และยืนยันว่าผู้ใช้บริการคลาวด์สามารถทำหน้าที่และความรับผิดชอบที่จัดสรรได้ต้องระบุบทบาทและความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศของทั้งสองฝ่ายไว้ในข้อตกลง ข) ผู้ใช้บริการคลาวด์ต้องระบุและจัดการความสัมพันธ์กับส่วนงานที่เกี่ยวกับการสนับสนุนลูกค้าและฟังก์ชันการดูแลของผู้ให้บริการคลาวด์	ก) ผู้ให้บริการคลาวด์ต้องตกลงและบันทึกการแบ่งบทบาทหน้าที่และความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศอย่างเหมาะสมกับผู้ใช้บริการคลาวด์ผู้ให้บริการคลาวด์ และผู้ให้บริการภายนอก ข) ผู้ให้บริการคลาวด์ต้องแต่งตั้งผู้ประสานงานด้าน การคุ้มครองข้อมูลส่วนบุคคลเพื่อประสานงานกับผู้ใช้บริการคลาวด์

๖.๓.๑.๒.๒ การติดต่อกับเจ้าหน้าที่ (Contact with Authorities)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ต้องระบุหน่วยงานที่เกี่ยวข้องกับการดำเนินการร่วมกันระหว่างผู้ใช้บริการคลาวด์และผู้ให้บริการคลาวด์	ก) ผู้ให้บริการคลาวด์ควรแจ้งให้ผู้ใช้บริการคลาวด์ทราบถึงที่ตั้งทางภูมิศาสตร์ขององค์กรที่เป็นเจ้าของผู้ให้บริการคลาวด์ และประเทศที่ผู้ให้บริการคลาวด์สามารถจัดเก็บข้อมูล ผู้ใช้บริการคลาวด์ได้

๖.๓.๑.๓ การปฏิบัติตามกฎ ระเบียบ ข้อบังคับ (Compliance)

๖.๓.๑.๓.๑ การระบุกฎหมายที่บังคับใช้และข้อกำหนดตามสัญญา (Identification of Applicable Legislation and Contractual Requirements)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ต้องพิจารณาประเด็นที่ว่ากฎหมายและข้อบังคับที่เกี่ยวข้องอาจเป็นกฎหมายของเขตอำนาจศาลที่ควบคุมผู้ให้บริการคลาวด์นอกเหนือจากกฎหมายที่ควบคุมผู้ใช้บริการคลาวด์ ข) ผู้ใช้บริการคลาวด์ต้องขอหลักฐานว่าผู้ให้บริการคลาวด์ได้ปฏิบัติตามกฎระเบียบและมาตรฐานที่เกี่ยวข้องกับผู้ใช้บริการคลาวด์ โดยหลักฐานดังกล่าวอาจเป็นการรับรองที่จัดทำโดยผู้ตรวจสอบภายนอก	ก) ผู้ให้บริการคลาวด์ต้องแจ้งให้ผู้ใช้บริการคลาวด์ทราบถึงเขตอำนาจศาลทางกฎหมายที่ควบคุมบริการคลาวด์ ข) ผู้ให้บริการคลาวด์ต้องระบุข้อกำหนดทางกฎหมายที่เกี่ยวข้องของตนเอง (เช่น เกี่ยวกับการเข้ารหัสเพื่อปกป้องข้อมูลส่วนบุคคล) และต้องให้ข้อมูลนี้แก่ผู้ใช้บริการคลาวด์เมื่อได้รับการร้องขอ ค) ผู้ให้บริการคลาวด์ต้องแสดงหลักฐานให้ผู้ใช้บริการคลาวด์ทราบถึงการปฏิบัติตามกฎหมาย ที่บังคับใช้ในปัจจุบันและข้อกำหนดตามสัญญา

๖.๓.๑.๓.๒ สิทธิในทรัพย์สินทางปัญญา (Intellectual Property Rights)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) การติดตั้งซอฟต์แวร์ที่ได้รับอนุญาตในเชิงพาณิชย์ใน บริการคลาวด์อาจทำให้เกิดการละเมิดเงื่อนไขการอนุญาตให้ใช้สิทธิสำหรับซอฟต์แวร์ได้ ผู้ใช้บริการคลาวด์ต้องมีขั้นตอนในการระบุข้อกำหนดในการ ให้สิทธิการใช้งานเฉพาะระบบคลาวด์ก่อนที่จะอนุญาต ให้ติดตั้งซอฟต์แวร์ที่ได้รับอนุญาตในบริการคลาวด์ และต้องให้ความสนใจเป็นพิเศษกับกรณีที่บริการคลาวด์มีความยืดหยุ่นและสามารถปรับขนาดได้ และ สามารถใช้งานซอฟต์แวร์บนระบบหรือแกนประมวลผล ได้มากกว่าที่อนุญาตโดยเงื่อนไขการอนุญาตให้ใช้สิทธิ	ก) ผู้ให้บริการคลาวด์ต้องกำหนดกระบวนการในการตอบสนองต่อการร้องเรียนเรื่องสิทธิในทรัพย์สินทางปัญญา

๖.๓.๑.๓.๓ การปกป้องบันทึกข้อมูล (Protection of Records)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ต้องขอข้อมูลจากผู้ให้บริการคลาวด์เกี่ยวกับการปกป้องบันทึกข้อมูลที่รวบรวมและจัดเก็บโดยผู้ให้บริการคลาวด์ที่เกี่ยวข้องกับการใช้บริการคลาวด์ของผู้ใช้บริการคลาวด์	ก) ผู้ให้บริการคลาวด์ต้องให้ข้อมูลแก่ผู้ใช้บริการคลาวด์เกี่ยวกับการปกป้องบันทึกข้อมูลที่รวบรวม และจัดเก็บโดยผู้ให้บริการคลาวด์ที่เกี่ยวข้องกับ การใช้บริการคลาวด์ของผู้ใช้บริการคลาวด์

๖.๓.๑.๓.๔ การทบทวนด้านการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างเป็นอิสระ (Independent Review of Information Security)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ต้องขอหลักฐานที่เป็นเอกสารว่ามีการนำมาตรการควบคุมและแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศสำหรับบริการคลาวด์ไปปฏิบัติ และมีความสอดคล้องกับผู้ที่ให้บริการคลาวด์กล่าวอ้างทั้งนี้ หลักฐานดังกล่าวอาจรวมถึงการรับรองมาตรฐานที่เกี่ยวข้องด้วย	ก) ผู้ให้บริการคลาวด์ต้องให้หลักฐานที่เป็นเอกสารแก่ผู้ใช้บริการคลาวด์เพื่อยืนยันข้อเรียกร้องของผู้ให้บริการคลาวด์ในการนำมาตรการควบคุมความมั่นคงปลอดภัยสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคลไปใช้ ข) ในกรณีที่การตรวจสอบโดยผู้ใช้บริการคลาวด์แต่ละรายการไม่สามารถกระทำได้หรืออาจเพิ่มความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศได้ ผู้ให้บริการคลาวด์ต้องแสดงหลักฐานที่เป็นอิสระว่ามีการนำไปปฏิบัติและดำเนินการด้านความมั่นคงปลอดภัยสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคลตามนโยบายและขั้นตอนของผู้ให้บริการคลาวด์ ทั้งนี้ผู้ให้บริการคลาวด์ต้องแสดงหลักฐานดังกล่าวให้กับผู้ที่คาดว่าจะเป็นผู้ใช้บริการคลาวด์ก่อนเข้าทำสัญญาโดยปกติแล้วการตรวจสอบอิสระที่เกี่ยวข้องตามที่ผู้ให้บริการคลาวด์เลือกควรเป็นวิธีการที่เป็นที่ยอมรับเพื่อตอบสนองความต้องการของผู้ใช้บริการคลาวด์ในการตรวจสอบการดำเนินงานของผู้ให้บริการคลาวด์หากมีความโปร่งใสเพียงพอเมื่อการตรวจสอบที่เป็นอิสระไม่สามารถทำได้ผู้ให้บริการคลาวด์ต้องทำการประเมินตนเอง และเปิดเผยกระบวนการและผลลัพธ์ต่อผู้ใช้บริการคลาวด์

๖.๓.๑.๓.๕ กฎระเบียบที่เกี่ยวกับมาตรการควบคุมการเข้ารหัสข้อมูล (Regulation of Cryptographic Controls)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ต้องตรวจสอให้แน่ใจว่าชุดของมาตรการควบคุมการเข้ารหัสข้อมูลที่ใช้กับการใช้บริการคลาวด์สอดคล้องกับข้อตกลงกฎหมายและระเบียบข้อบังคับที่เกี่ยวข้อง	ก) ผู้ให้บริการคลาวด์ต้องให้คำอธิบายกับผู้ใช้บริการคลาวด์เกี่ยวกับมาตรการควบคุมการเข้ารหัสข้อมูลที่ดำเนินการโดยผู้ให้บริการคลาวด์เพื่อใช้ในการทบทวนการปฏิบัติตามข้อตกลงกฎหมายและข้อบังคับที่เกี่ยวข้อง

๖.๓.๒ การปฏิบัติการและการรักษาความมั่นคงปลอดภัยโครงสร้างพื้นฐานระบบคลาวด์ (Cloud Infrastructure Security and Operation)

๖.๓.๒.๑ การบริหารทรัพยากรมนุษย์(Human Resource Security)

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

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ต้องเพิ่มรายการต่อไปนี้ในโปรแกรมสร้างความตระหนักรู้ การศึกษาและการฝึกอบรมสำหรับผู้จัดการธุรกิจบริการคลาวด์ ผู้ดูแลระบบบริการคลาวด์ผู้ประกอบบริการคลาวด์และผู้ใช้บริการคลาวด์รวมถึงพนักงานและผู้รับจ้างที่เกี่ยวข้อง - มาตรฐานและขั้นตอนการใช้บริการคลาวด์ - ความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับบริการคลาวด์และวิธีการจัดการความเสี่ยงเหล่านั้น - ความเสี่ยงด้านสภาพแวดล้อมของระบบและเครือข่ายจากการใช้บริการคลาวด์ - การคุ้มครองข้อมูลส่วนบุคคล - ข้อพิจารณาทางกฎหมายและข้อบังคับที่เกี่ยวข้อง ข) ต้องจัดให้มีโปรแกรมการสร้างความตระหนักรู้ด้าน ความมั่นคงปลอดภัยสารสนเทศ การศึกษาและการฝึกอบรมเกี่ยวกับบริการคลาวด์แก่ผู้บริหารและผู้จัดการที่กำกับดูแลรวมถึงหน่วยงานธุรกิจ (Business Units)	ก) ผู้ให้บริการคลาวด์ต้องสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศ และด้านการคุ้มครองข้อมูลส่วนบุคคล การศึกษาและการฝึกอบรมแก่พนักงานรวมทั้งให้ผู้รับจ้างดำเนินการเช่นเดียวกันเกี่ยวกับการจัดการข้อมูลของผู้ใช้บริการคลาวด์ และข้อมูลที่ได้จากบริการคลาวด์อย่างเหมาะสมโดยข้อมูลนี้อาจมีข้อมูลที่เป็นความลับต่อผู้ใช้บริการคลาวด์หรืออยู่ภายใต้ข้อจำกัดเฉพาะรวมถึงข้อจำกัดด้านกฎระเบียบในการเข้าถึง และใช้งานโดยผู้ให้บริการคลาวด์

๖.๓.๒.๒ การจัดการทรัพย์สิน (Asset Management)

๖.๓.๒.๒.๑ ทะเบียนทรัพย์สิน (Inventory of Assets)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ทะเบียนทรัพย์สินของผู้ใช้บริการคลาวด์ต้องคำนึงถึงข้อมูลและทรัพย์สินที่เกี่ยวข้องซึ่งจัดเก็บในสภาพแวดล้อมการประมวลผลบนคลาวด์ทั้งนี้ บันทึกทะเบียนทรัพย์สินต้องระบุสถานที่จัดเก็บทรัพย์สิน เช่นชื่อของผู้ให้บริการคลาวด์	ก) ทะเบียนทรัพย์สินของผู้ให้บริการคลาวด์ต้องระบุอย่างชัดเจนในเรื่อง - ข้อมูลของผู้ใช้บริการคลาวด์ - ข้อมูลที่เกิดจากการใช้บริการคลาวด์

๖.๓.๒.๒.๒ การบ่งชี้ข้อมูล (Labelling of Information)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ต้องบ่งชี้ข้อมูลและทรัพย์สินขององค์กรที่ใช้งานหรือเก็บรักษาไว้บนระบบคลาวด์ตามขั้นตอนปฏิบัติสำหรับการบ่งชี้ข้อมูลขององค์กร	ก) ผู้ให้บริการคลาวด์ต้องจัดทำเอกสารและเปิดเผยฟังก์ชันการทำงานของบริการใดๆ ที่ผู้ใช้บริการคลาวด์สามารถนำไปใช้เพื่อการบ่งชี้ข้อมูลและทรัพย์สินที่เกี่ยวข้องได้

๖.๓.๒.๓ การควบคุมการเข้าถึง (Access Control)

๖.๓.๒.๓.๑ การควบคุมเข้าถึงเครือข่ายและบริการเครือข่าย (Access to Networks and Network Services)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) นโยบายการควบคุมการเข้าถึงของผู้ใช้บริการคลาวด์สำหรับการใช้บริการเครือข่ายต้องระบุข้อกำหนดสำหรับผู้ใช้งานในการเข้าถึงบริการคลาวด์ตามแต่ละบริการที่ใช้งาน	

๖.๓.๒.๓.๒ การลงทะเบียนและยกเลิกการลงทะเบียนสำหรับผู้ใช้ (User Registration and Deregistration)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ขั้นตอนการลงทะเบียนและยกเลิกการลงทะเบียนสำหรับผู้ใช้ต้องครอบคลุมถึงสถานการณ์ที่การควบคุมการเข้าถึงของผู้ใช้ถูกคุกคามเช่น การที่รหัสผ่านหรือข้อมูลการลงทะเบียนผู้ใช้อื่นๆ (ยกตัวอย่างเช่นจากการเปิดเผยโดยไม่ได้ตั้งใจ) ถูกทำให้เสียหายหรือถูกคุกคาม	ก) เพื่อจัดการการเข้าถึงบริการคลาวด์โดยผู้ใช้งานของผู้ใช้บริการคลาวด์ผู้ให้บริการคลาวด์ต้องจัดเตรียมฟังก์ชันการลงทะเบียนและการยกเลิกการลงทะเบียนผู้ใช้งานรวมถึงข้อกำหนดสำหรับการใช้งานฟังก์ชันเหล่านี้แก่ผู้ใช้บริการคลาวด์

๖.๓.๒.๓.๓ การจัดสรรการเข้าถึงของผู้ใช้ (User Access Provisioning)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
	ก) ผู้ให้บริการคลาวด์ต้องจัดเตรียมฟังก์ชันสำหรับการจัดการสิทธิการเข้าถึงของผู้ใช้บริการคลาวด์รวมถึงข้อกำหนดสำหรับการใช้งานฟังก์ชันเหล่านี้

๖.๓.๒.๓.๔ การจัดการสิทธิการเข้าถึงที่ได้รับสิทธิพิเศษ (Management of Privileged Access Rights)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ให้บริการคลาวด์ต้องมีเทคนิคการยืนยันตัวตนที่เพียงพอ (เช่นการยืนยันตัวตนแบบหลายปัจจัย) สำหรับการตรวจสอบสิทธิของผู้ดูแลระบบบริการคลาวด์ของผู้ใช้บริการคลาวด์ให้มีความสามารถในการบริหารจัดการระบบคลาวด์ที่สอดคล้องตามความเสี่ยงที่ระบุไว้	ก) ผู้ให้บริการคลาวด์ต้องมีเทคนิคการยืนยันตัวตนที่เพียงพอ (เช่นการยืนยันตัวตนแบบหลายปัจจัย) สำหรับการตรวจสอบสิทธิของผู้ดูแลระบบบริการคลาวด์ของผู้ใช้บริการคลาวด์ให้มีความสามารถในการบริหารจัดการระบบคลาวด์ที่สอดคล้องตามความเสี่ยงที่ระบุไว้

๖.๓.๒.๓.๕ การจัดการข้อมูลการพิสูจน์ตัวตนที่เป็นความลับของผู้ใช้ (Management of Secret Authentication Information of Users)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ต้องตรวจสอบว่ากระบวนการจัดการของผู้ให้บริการคลาวด์สำหรับการจัดสรรข้อมูลการตรวจสอบความลับ (Secret Authentication Information) เช่นรหัสผ่านเป็นไปตามข้อกำหนดของผู้ใช้บริการคลาวด์	ก) ผู้ให้บริการคลาวด์ต้องให้ข้อมูลเกี่ยวกับขั้นตอนการจัดการข้อมูลการตรวจสอบความลับ (Secret Authentication Information) ของผู้ใช้บริการคลาวด์รวมถึงขั้นตอนในการจัดสรรข้อมูลดังกล่าวสำหรับการตรวจสอบสิทธิผู้ใช้งาน

๖.๓.๒.๓.๖ การจำกัดการเข้าถึงข้อมูล (Information Access Restriction)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ต้องตรวจสอบให้แน่ใจว่าสามารถจำกัดการเข้าถึงข้อมูลในบริการคลาวด์ได้ตามนโยบายการควบคุมการเข้าถึงและปฏิบัติตามข้อจำกัดดังกล่าวซึ่งรวมถึงการจำกัดการเข้าถึงบริการต่างๆ บนระบบคลาวด์ และข้อมูลผู้ใช้บริการคลาวด์ที่เก็บไว้ในบริการ	ก) ผู้ให้บริการคลาวด์ต้องให้การควบคุมการเข้าถึง ที่อนุญาตให้กับผู้ใช้บริการคลาวด์เพื่อจำกัดการเข้าถึงบริการต่างๆ บนระบบคลาวด์ และข้อมูลผู้ใช้บริการคลาวด์ที่เก็บไว้ในบริการ

๖.๓.๒.๓.๗ การใช้โปรแกรมอรรถประโยชน์พิเศษ (Use of Privilege Utility Programs)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) หากอนุญาตให้ใช้โปรแกรมอรรถประโยชน์ได้ ผู้ใช้บริการคลาวด์ต้องระบุโปรแกรมอรรถประโยชน์ที่จะใช้ในสภาพแวดล้อมการประมวลผลบนคลาวด์และตรวจสอบให้มั่นใจว่าโปรแกรมเหล่านั้นไม่รบกวนการควบคุมของบริการคลาวด์	ก) ผู้ให้บริการคลาวด์ต้องระบุข้อกำหนดสำหรับโปรแกรมอรรถประโยชน์ใดๆที่ใช้ในบริการคลาวด์ ผู้ให้บริการคลาวด์ต้องตรวจสอบให้มั่นใจว่าการใช้โปรแกรมอรรถประโยชน์ใดๆที่สามารถข้ามขั้นตอนการทำงานตามปกติหรือการรักษาความปลอดภัยนั้นจำกัดเฉพาะบุคลากรที่ได้รับอนุญาตเท่านั้น และต้องมีการทบทวนและตรวจสอบการใช้โปรแกรมดังกล่าวอย่างสม่ำเสมอ

๖.๓.๒.๓.๘ ขั้นตอนการเข้าสู่ระบบอย่างปลอดภัย (Secure Log-on Procedures)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ต้องกำหนดให้ผู้ใช้ที่อยู่ภายใต้การควบคุมของผู้ใช้บริการคลาวด์ปฏิบัติตามขั้นตอนการเข้าสู่ระบบอย่างปลอดภัยสำหรับบัญชีใดๆ	ก) ในกรณีที่จำเป็นผู้ให้บริการคลาวด์ต้องจัดให้มีขั้นตอนการเข้าสู่ระบบอย่างปลอดภัยสำหรับบัญชีใดๆ ที่ผู้ใช้บริการคลาวด์ร้องขอสำหรับผู้ใช้ที่อยู่ภายใต้การควบคุมของผู้ใช้บริการคลาวด์

๖.๓.๒.๔ การเข้ารหัส(Cryptography)

๖.๓.๒.๔.๑ นโยบายเกี่ยวกับการใช้มาตรการควบคุมการเข้ารหัส (Policy on the Use of Cryptographic Controls)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ต้องใช้มาตรการควบคุมการเข้ารหัสสำหรับการใช้บริการระบบคลาวด์ที่มีความแข็งแรงเพียงพอ และสอดคล้องตามความเสี่ยงที่ได้ระบุไว้ไม่ว่าผู้ใช้บริการคลาวด์หรือผู้ให้บริการคลาวด์จะเป็นผู้จัดหามาตรการควบคุมการเข้ารหัสเหล่านั้นก็ตาม ข) เมื่อผู้ให้บริการคลาวด์นำเสนอการเข้ารหัสใดๆผู้ใช้บริการคลาวด์ต้องตรวจสอบข้อมูลที่ผู้ให้บริการคลาวด์จัดหาให้เพื่อยืนยันว่ามีความสามารถในการเข้ารหัสดังนี้หรือไม่ - ปฏิบัติตามข้อกำหนดด้านนโยบายของผู้ใช้บริการคลาวด์ - เข้ากันได้กับการป้องกันการเข้ารหัสลับอื่นๆ ที่ใช้โดยผู้ใช้บริการคลาวด์ - ใช้กับข้อมูลขณะจัดเก็บและระหว่างโอนถ่ายภายในบริการคลาวด์และนอกระบบคลาวด์	ก) ผู้ให้บริการคลาวด์ต้องให้ข้อมูลแก่ผู้ใช้บริการคลาวด์เกี่ยวกับการเข้ารหัสเพื่อปกป้องข้อมูลและข้อมูลส่วนบุคคลที่ผู้ให้บริการคลาวด์ประมวลผลนอกจากนี้ผู้ให้บริการคลาวด์ต้องให้ข้อมูลแก่ผู้ใช้บริการคลาวด์เกี่ยวกับความสามารถที่ผู้ให้บริการคลาวด์มอบให้ซึ่งสามารถช่วยผู้ใช้บริการคลาวด์ในการใช้กาเข้ารหัสดังกล่าว

๖.๓.๒.๔.๒ การจัดการกุญแจ (Key Management)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ต้องระบุกุญแจสำหรับการเข้ารหัสในแต่ละบริการคลาวด์ และดำเนินการตามขั้นตอนสำหรับการจัดการกุญแจ ข) ในกรณีที่บริการคลาวด์มีฟังก์ชันการจัดการกุญแจสำหรับการใช้งานโดยผู้ใช้บริการคลาวด์ผู้ใช้บริการคลาวด์ต้องขอข้อมูลดังต่อไปนี้เกี่ยวกับขั้นตอนที่ใช้ในการจัดการกุญแจสำหรับการเข้ารหัสที่เกี่ยวข้องกับบริการคลาวด์ ประเภทของกุญแจ	

ผู้ใช้บริการคลาวด์	**ผู้ให้บริการคลาวด์**
- ข้อกำหนดเฉพาะของระบบการจัดการรวมถึงขั้นตอนต่างๆ ตลอดอายุการใช้งานของกุญแจเข้ารหัสเช่นการสร้างเปลี่ยนแปลงหรือปรับปรุงจัดเก็บหมดอายุการใช้งาน เรียกคืน เก็บรักษาและทำลาย - ขั้นตอนการจัดการกุญแจที่แนะนำสำหรับการใช้งานโดยผู้ใช้บริการคลาวด์ ค) ผู้ใช้บริการคลาวด์ต้องไม่อนุญาตให้ผู้ให้บริการคลาวด์จัดเก็บ และจัดการกุญแจสำหรับการเข้ารหัสเมื่อผู้ใช้บริการคลาวด์ใช้กุญแจเข้ารหัสของตนเอง	

๖.๓.๒.๕ การรักษาความปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environment Security)

๖.๓.๒.๕.๑ ตำแหน่งของศูนย์ข้อมูล (Data Center Location)

ผู้ใช้บริการคลาวด์	**ผู้ให้บริการคลาวด์**
ก) ต้องใช้ศูนย์ข้อมูลหลักในประเทศไทย (Data Localization)	ก) ต้องจัดตั้งศูนย์ข้อมูลหลักในประเทศไทย (Data Localization) ข) ต้องจัดตั้งศูนย์ข้อมูลสำรองในประเทศไทย (Data Localization) หรืออยู่ในภูมิภาคเอเชียตะวันออกเฉียงใต้ที่ใกล้กับการใช้งานหลักของผู้ใช้บริการคลาวด์ให้มากที่สุดรวมถึงสิงคโปร์ และเขตปกครอง พิเศษฮ่องกง

๖.๓.๒.๕.๒ การกำจัดหรือนำอุปกรณ์กลับมาใช้ใหม่อย่างปลอดภัย (Secure Disposal or Reuse of Equipment)

ผู้ใช้บริการคลาวด์	**ผู้ให้บริการคลาวด์**
ก) ผู้ใช้บริการคลาวด์ต้องร้องขอการยืนยันว่าผู้ให้บริการคลาวด์มีนโยบายและขั้นตอนในการกำจัดหรือนำทรัพยากรกลับมาใช้ใหม่อย่างปลอดภัย	ก) ผู้ให้บริการคลาวด์ต้องตรวจสอบให้แน่ใจว่ามีการเตรียมการสำหรับการกำจัดหรือนำทรัพยากร (เช่นอุปกรณ์ที่เก็บข้อมูล ไฟล์ หน่วยความจำ) กลับมาใช้ใหม่อย่างปลอดภัย และทันท่วงที ข) เพื่อวัตถุประสงค์ในการกำจัดหรือนำกลับมาใช้ใหม่อย่างมั่นคงปลอดภัย และไม่สามารถกู้คืนข้อมูลกลับมาได้อุปกรณ์ที่มีสื่อจัดเก็บข้อมูลที่อาจมีข้อมูลส่วนบุคคลต้องได้รับการปฏิบัติเสมือนว่ามีข้อมูลส่วนบุคคลจริง

๖.๓.๒.๖ การรักษาความมั่นคงปลอดภัยการปฏิบัติการ (Operations Security)

๖.๓.๒.๖.๑ การจัดการการเปลี่ยนแปลง (Change Management)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) กระบวนการจัดการการเปลี่ยนแปลงของผู้ใช้บริการคลาวด์ต้องคำนึงถึงผลกระทบของการเปลี่ยนแปลงใดๆ ที่เกิดขึ้นจากผู้ให้บริการคลาวด์	ก) ผู้ให้บริการคลาวด์ต้องให้ข้อมูลแก่ผู้ใช้บริการคลาวด์เกี่ยวกับการเปลี่ยนแปลงในบริการคลาวด์ที่อาจส่งผลเสียต่อบริการคลาวด์ข้อมูลต่อไปนี้จะช่วยให้ผู้ใช้บริการคลาวด์ระบุถึงผลกระทบของการเปลี่ยนแปลงที่อาจมีผลต่อความมั่นคงปลอดภัยสารสนเทศ - ประเภทของการเปลี่ยนแปลง - วันที่และเวลาที่วางแผนไว้ของการเปลี่ยนแปลง - คำอธิบายทางเทคนิคเกี่ยวกับการเปลี่ยนแปลงของบริการคลาวด์ และระบบที่เกี่ยวข้อง (Underlying Systems) - การแจ้งเตือนการเริ่มต้นและการเปลี่ยนแปลงที่เสร็จสมบูรณ์ ข) เมื่อผู้ให้บริการคลาวด์ให้บริการคลาวด์ที่ขึ้นอยู่กับผู้ให้บริการรายย่อยของผู้ให้บริการคลาวด์ผู้ให้บริการคลาวด์อาจจำเป็นต้องแจ้งการเปลี่ยนแปลงที่เกิดขึ้นให้ผู้ใช้บริการคลาวด์ทราบ

๖.๓.๒.๖.๒ การบริหารจัดการความจุ (Capacity Management)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ต้องตรวจสอบให้แน่ใจว่าขีดความสามารถของทรัพยากรที่ตกลงกันไว้ในบริการคลาวด์นั้นตรงตามข้อกำหนดของผู้ใช้บริการคลาวด์ ข) ผู้ใช้บริการคลาวด์ต้องตรวจสอบการใช้บริการคลาวด์และคาดการณ์ความต้องการด้านขีดความสามารถของทรัพยากรของบริการคลาวด์เพื่อให้มั่นใจในประสิทธิภาพของบริการคลาวด์เมื่อเวลาผ่านไป	ก) ผู้ให้บริการคลาวด์ต้องตรวจสอบขีดความสามารถของทรัพยากรทั้งหมดเพื่อป้องกันไม่ให้เกิดเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่เกิดจากการขาดแคลนทรัพยากร

๖.๓.๒.๖.๓ การสำรองข้อมูล (Information Backup)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ในกรณีที่ผู้ให้บริการคลาวด์มีความสามารถในการสำรองข้อมูลซึ่งเป็นส่วนหนึ่งของบริการคลาวด์ ผู้ใช้บริการคลาวด์ต้องขอข้อมูลจำเพาะของความสามารถในการสำรองข้อมูลจากผู้ให้บริการคลาวด์นอกจากนี้ผู้ใช้บริการคลาวด์ต้องทำการตรวจสอบเพื่อให้แน่ใจว่าเป็นไปตามข้อกำหนดในการสำรองข้อมูลหรือไม่ ข) ผู้ใช้บริการคลาวด์มีหน้าที่รับผิดชอบในการดำเนินการสำรองข้อมูลเมื่อผู้ให้บริการคลาวด์ไม่ได้ให้บริการสำรองข้อมูลหรือเมื่อเกิดเหตุการณ์ที่อยู่นอกเหนือการควบคุมของผู้ให้บริการ	ก) ผู้ให้บริการคลาวด์ต้องให้ข้อมูลจำเพาะของความสามารถในการสำรองข้อมูลแก่ผู้ใช้บริการคลาวด์ข้อมูลจำเพาะควรมีข้อมูลต่อไปนี้ตามความเหมาะสม - ขอบเขตและกำหนดการของการสำรองข้อมูล - วิธีการสำรองข้อมูลและรูปแบบข้อมูลรวมถึงวิธีการเข้ารหัสหากมีความเกี่ยวข้อง - ระยะเวลาเก็บรักษาข้อมูลสำรอง - ขั้นตอนการตรวจสอบความสมบูรณ์ของข้อมูลสำรอง - ขั้นตอนและระยะเวลาที่เกี่ยวข้องกับการกู้คืนข้อมูลจากการสำรองข้อมูล - ขั้นตอนในการทดสอบความสามารถในการสำรองข้อมูล - สถานที่จัดเก็บข้อมูลสำรอง ข) ผู้ให้บริการคลาวด์ต้องให้บริการการเข้าถึงข้อมูลสำรองที่ปลอดภัยและแยกออกจากกันหากบริการดังกล่าวมีการนำเสนอให้ผู้ใช้บริการคลาวด์

๖.๓.๒.๖.๔ การบันทึกเหตุการณ์ (Event Logging)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ต้องจัดทำข้อกำหนดสำหรับการบันทึกเหตุการณ์และตรวจสอบว่าบริการคลาวด์ตรงตามข้อกำหนดเหล่านั้นหรือไม่	ก) ผู้ให้บริการคลาวด์ต้องให้ผู้ใช้บริการสามารถบันทึกเหตุการณ์ ข) ในกรณีที่เป็นไปได้บันทึกเหตุการณ์ควรบันทึกว่าข้อมูลส่วนบุคคลได้รับการเปลี่ยนแปลงหรือไม่ (เพิ่มแก้ไข หรือลบ) จากเหตุการณ์นั้นและโดยใคร (Audit Log) ในกรณีที่มีผู้ให้บริการหลายรายเข้ามาเกี่ยวข้องในการให้บริการจากหลากหลายประเภทบริการของสถาปัตยกรรมอ้างอิงประมวลผลคลาวด์อาจมีบทบาทที่แตกต่างหรือแบ่งปันกันในการปฏิบัติตามข้อนี้

๖.๓.๒.๖.๕ การปกป้องข้อมูลในบันทึกเหตุการณ์ (Protection of Log information)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ข้อมูลที่บันทึกไว้ในบันทึกเหตุการณ์เพื่อวัตถุประสงค์ต่างๆ เช่นการตรวจสอบความปลอดภัยและการวินิจฉัยการทำงานอาจมีข้อมูลส่วนบุคคลอยู่ด้วยจึงต้องมีมาตรการเช่นการควบคุมการเข้าถึงเพื่อให้มั่นใจว่าข้อมูลที่บันทึกไว้ในบันทึกเหตุการณ์จะถูกนำไปใช้ตามวัตถุประสงค์ที่ตั้งไว้เท่านั้น ข) ต้องมีขั้นตอนการดำเนินการซึ่งดีที่สุดคือเป็นระบบอัตโนมัติเพื่อให้มั่นใจว่าข้อมูลที่บันทึกไว้ในบันทึกเหตุการณ์จะถูกลบภายในระยะเวลาที่กำหนด (Log Retention) และเอกสารระบุไว้	ก) ข้อมูลที่บันทึกไว้ในบันทึกเหตุการณ์เพื่อวัตถุประสงค์ต่างๆ เช่นการตรวจสอบความปลอดภัยและการวินิจฉัยการทำงานอาจมีข้อมูลส่วนบุคคลอยู่ด้วยจึงต้องมีมาตรการเช่นการควบคุมการเข้าถึงเพื่อให้มั่นใจว่าข้อมูลที่บันทึกไว้ในบันทึกเหตุการณ์จะถูกนำไปใช้ตามวัตถุประสงค์ที่ตั้งไว้เท่านั้น ข) ต้องมีขั้นตอนการดำเนินการซึ่งดีที่สุดคือเป็นระบบอัตโนมัติเพื่อให้มั่นใจว่าข้อมูลที่บันทึกไว้ในบันทึกเหตุการณ์จะถูกลบภายในระยะเวลาที่กำหนด (Log Retention) และเอกสารระบุไว้

๖.๓.๒.๖.๖ บันทึกเหตุการณ์ของผู้ดูแลระบบและผู้ปฏิบัติงาน (Administrator and Operator Logs)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) หากมีการให้สิทธิพิเศษให้แก่ผู้ใช้บริการคลาวด์การใช้สิทธิพิเศษนั้นต้องมีการบันทึกเหตุการณ์และ ประสิทธิภาพของการดำเนินการเหล่านั้น ผู้ใช้บริการคลาวด์ต้องพิจารณาว่าความสามารถในการบันทึก เหตุการณ์ที่ผู้ให้บริการคลาวด์จัดหาให้นั้นเหมาะสมหรือไม่หรือผู้ใช้บริการคลาวด์ต้องใช้ความสามารถในการบันทึกเหตุการณ์เพิ่มเติมหรือไม่	

๖.๓.๒.๖.๗ การซิงโครไนซ์นาฬิกา (Clock Synchronization)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ต้องขอข้อมูลเกี่ยวกับการซิงโครไนซ์นาฬิกาที่ใช้ในระบบของผู้ให้บริการคลาวด์	ก) ผู้ให้บริการคลาวด์ต้องให้ข้อมูลแก่ผู้ใช้บริการคลาวด์เกี่ยวกับนาฬิกาที่ระบบของผู้ให้บริการคลาวด์ใช้ และข้อมูลเกี่ยวกับวิธีที่ผู้ใช้บริการคลาวด์สามารถซิงโครไนซ์นาฬิกาภายในกับนาฬิกาในบริการคลาวด์

๖.๓.๒.๖.๘ การจัดการช่องโหว่ทางเทคนิค (Management of Technical Vulnerabilities)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ต้องขอข้อมูลจากผู้ให้บริการคลาวด์เกี่ยวกับการจัดการช่องโหว่ทางเทคนิคที่อาจส่งผลกระทบต่อบริการคลาวด์ที่ให้บริการ ผู้ใช้บริการคลาวด์ต้องระบุช่องโหว่ทางเทคนิคที่ผู้ใช้บริการคลาวด์จะเป็นผู้รับผิดชอบในการจัดการ และกำหนดกระบวนการในการจัดการให้ชัดเจน	ก) ผู้ให้บริการคลาวด์ต้องให้ข้อมูลผู้ใช้บริการคลาวด์เกี่ยวกับการจัดการช่องโหว่ทางเทคนิคที่อาจส่งผลกระทบต่อบริการคลาวด์ที่ให้บริการ

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

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ในกรณีที่ไม่สามารถหลีกเลี่ยงการใช้ข้อมูลส่วนบุคคลสำหรับวัตถุประสงค์ในการทดสอบได้ ต้องมีการประเมินความเสี่ยงมาตรการด้านเทคนิคและการจัดการองค์กรต้องถูกนำมาใช้เพื่อลดความเสี่ยงที่ระบุไว้ให้น้อยที่สุด	ก) ในกรณีที่ไม่สามารถหลีกเลี่ยงการใช้ข้อมูลส่วนบุคคลสำหรับวัตถุประสงค์ในการทดสอบได้ ต้องมีการประเมินความเสี่ยงมาตรการด้านเทคนิคและการจัดการองค์กรต้องถูกนำมาใช้เพื่อลดความเสี่ยงที่ระบุไว้ให้น้อยที่สุด

๖.๓.๒.๗ การรักษาความมั่นคงปลอดภัยเครือข่าย (Communication Security)

๖.๓.๒.๗.๑ นโยบายและขั้นตอนปฏิบัติในการถ่ายโอนข้อมูล (Information Transfer Policies and Procedures)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) เมื่อใดก็ตามที่มีการใช้สื่อทางกายภาพสำหรับการถ่ายโอนข้อมูลต้องมีระบบที่จะบันทึกสื่อทางกายภาพที่เข้ามาและออกไปซึ่งมีข้อมูลส่วนบุคคลรวมถึงประเภทของสื่อทางกายภาพ ผู้ส่ง/ผู้รับ ที่ได้รับอนุญาตวันที่และเวลา และจำนวนสื่อทางกายภาพ ข) ผู้ใช้บริการคลาวด์ต้องขอให้ผู้ให้บริการคลาวด์ใช้มาตรการเพิ่มเติม (เช่นการเข้ารหัส) เพื่อให้มั่นใจว่าข้อมูลสามารถเข้าถึงได้เฉพาะจุดปลายทางเท่านั้นไม่ใช่ระหว่างทาง	ก) เมื่อใดก็ตามที่มีการใช้สื่อทางกายภาพสำหรับการถ่ายโอนข้อมูลต้องมีระบบที่จะบันทึกสื่อทางกายภาพที่เข้ามาและออกไปซึ่งมีข้อมูลส่วนบุคคลรวมถึงประเภทของสื่อทางกายภาพ ผู้ส่ง/ผู้รับ ที่ได้รับอนุญาตวันที่และเวลา และจำนวนสื่อทางกายภาพ ข) หากเป็นไปได้ต้องขอให้ผู้ใช้บริการคลาวด์ใช้มาตรการเพิ่มเติม (เช่นการเข้ารหัส) เพื่อให้มั่นใจว่าข้อมูลสามารถเข้าถึงได้เฉพาะจุดปลายทางเท่านั้นไม่ใช่ระหว่างทาง

๖.๓.๒.๗.๒ การแบ่งแยกในเครือข่าย (Segregation in Networks)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ต้องจัดทำข้อกำหนดสำหรับการแยกเครือข่ายเพื่อให้เกิดการแยกผู้เช่า (Tenant) ในสภาพแวดล้อมที่เป็นการใช้บริการคลาวด์ร่วมกัน และตรวจสอบว่าผู้ให้บริการคลาวด์มีคุณสมบัติตรงตามข้อกำหนดเหล่านั้นหรือไม่	ก) ผู้ให้บริการคลาวด์ต้องบังคับใช้การแยกการเข้าถึงเครือข่ายในกรณีต่อไปนี้ - การแบ่งแยกระหว่างผู้เช่าในสภาพแวดล้อมที่มีผู้เช่าหลายราย - การแยกระหว่างสภาพแวดล้อมการดูแลระบบภายในของผู้ให้บริการคลาวด์ และสภาพแวดล้อมการประมวลผลบนคลาวด์ของผู้ใช้บริการคลาวด์ ข) ผู้ให้บริการคลาวด์ต้องช่วยผู้ใช้บริการคลาวด์ตรวจสอบการแบ่งแยกที่ดำเนินการโดยผู้ให้บริการคลาวด์

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

๖.๓.๒.๘.๑ การวิเคราะห์และข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Requirements Analysis and Specification)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ต้องกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศสำหรับการใช้บริการคลาวด์จากนั้นประเมินว่าบริการของผู้ให้บริการคลาวด์สามารถตอบสนองความต้องการเหล่านี้ได้หรือไม่ ข) สำหรับการประเมินนี้ผู้ใช้บริการคลาวด์ต้องขอข้อมูลเกี่ยวกับความสามารถในการรักษาความมั่นคงปลอดภัยสารสนเทศจาก ผู้ให้บริการคลาวด์	ก) ผู้ให้บริการคลาวด์ต้องให้ข้อมูลแก่ผู้ใช้บริการคลาวด์เกี่ยวกับความสามารถในการรักษาความมั่นคงปลอดภัยสารสนเทศที่ตนใช้ข้อมูลนี้ต้องเป็นข้อมูลโดยไม่เปิดเผยข้อมูลที่อาจเป็นประโยชน์ต่อบุคคลที่มีเจตนาร้าย

๖.๓.๒.๘.๒ นโยบายการพัฒนาที่ปลอดภัย (Secure Development Policy)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ต้องขอข้อมูลจากผู้ให้บริการคลาวด์เกี่ยวกับการใช้ขั้นตอนและวิธีปฏิบัติในการ พัฒนาที่ปลอดภัยของผู้ให้บริการคลาวด์	ก) ผู้ให้บริการคลาวด์ต้องให้ข้อมูลเกี่ยวกับการใช้ขั้นตอน และวิธีปฏิบัติในการพัฒนาความปลอดภัยของตนในขอบเขตที่สอดคล้องกับนโยบายในการเปิดเผยข้อมูล

๖.๓.๒.๙ การจัดการผู้ให้บริการภายนอก (Supplier Relationships)

๖.๓.๒.๙.๑ นโยบายความมั่นคงปลอดภัยสารสนเทศสำหรับความสัมพันธ์กับผู้ให้บริการภายนอก (Information Security Policy for Supplier Relationships)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ต้องระบุว่าผู้ให้บริการคลาวด์เป็นผู้ให้บริการภายนอกประเภทหนึ่งในนโยบายความมั่นคงปลอดภัยสารสนเทศสำหรับความสัมพันธ์กับผู้ให้บริการภายนอกซึ่งจะช่วยลดความเสี่ยงที่เกี่ยวข้องกับการเข้าถึงและจัดการข้อมูลผู้ใช้บริการคลาวด์ของผู้ให้บริการคลาวด์	

๖.๓.๒.๙.๒ การจัดการกับการรักษาความมั่นคงปลอดภัยภายในข้อตกลงของผู้ให้บริการภายนอก (Addressing Security within Supplier Agreements)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ต้องยืนยันบทบาทและความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับบริการคลาวด์ดังที่อธิบายไว้ในข้อตกลงการให้บริการสิ่งเหล่านี้อาจรวมถึงกระบวนการต่อไปนี้ - การป้องกันมัลแวร์ - การสำรองข้อมูล - มาตรการควบคุมการเข้ารหัส - การจัดการช่องโหว่ - การจัดการเหตุการณ์ - การตรวจสอบการปฏิบัติตามข้อกำหนดทาง เทคนิค – การทดสอบความปลอดภัย - การตรวจสอบ - การรวบรวมการบำรุงรักษาและการปกป้องหลักฐาน รวมถึงบันทึกและเส้นทางการตรวจสอบ - การปกป้องข้อมูลเมื่อสิ้นสุดข้อตกลงการให้บริการ - การยืนยันตัวตน และการควบคุมการเข้าถึง - การจัดการข้อมูลประจำตัวและการเข้าถึง	ก) ผู้ให้บริการคลาวด์ต้องระบุมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องซึ่งผู้ให้บริการคลาวด์จะนำมาใช้เป็นส่วนหนึ่งของข้อตกลงเพื่อให้แน่ใจว่าจะไม่เกิดความเข้าใจผิดระหว่างผู้ให้ บริการคลาวด์ และผู้ใช้บริการคลาวด์สิ่งเหล่านี้อาจรวมถึงกระบวนการต่อไปนี้ - การป้องกันมัลแวร์ - การสำรองข้อมูล - มาตรการควบคุมการเข้ารหัส - การจัดการช่องโหว่ - การจัดการเหตุการณ์ - การตรวจสอบการปฏิบัติตามข้อกำหนดทางเทคนิค - การทดสอบความปลอดภัย - การตรวจสอบ - การรวบรวมการบำรุงรักษาและการปกป้องหลักฐานรวมถึงบันทึกและเส้นทางการตรวจสอบ - การปกป้องข้อมูลเมื่อสิ้นสุดข้อตกลงการให้บริการ - การยืนยันตัวตน และการควบคุมการเข้าถึง - การจัดการข้อมูลประจำตัวและการเข้าถึง ข) มาตรการรักษาความมั่นคงปลอดภัยสารสนเทศที่ให้บริการคลาวด์จะใช้อาจแตกต่างกันออกไปตามประเภทของบริการคลาวด์ที่ผู้ใช้บริการคลาวด์ใช้งานอยู่

๖.๓.๒.๙.๓ ห่วงโซ่อุปทานของเทคโนโลยีสารสนเทศและการสื่อสาร (Information and Communication Technology Supply Chain)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
	ก) หากผู้ให้บริการคลาวด์ใช้บริการคลาวด์ของผู้ให้บริการรายย่อยผู้ให้บริการคลาวด์ต้องตรวจสอบให้แน่ใจว่าระดับความมั่นคงปลอดภัยสารสนเทศของผู้ให้บริการรายย่อยนั้นได้รับการดูแลไม่น้อยกว่าผู้ใช้บริการคลาวด์ ข) เมื่อผู้ให้บริการคลาวด์ให้บริการคลาวด์ตามห่วงโซ่อุปทานผู้ให้บริการคลาวด์ต้องกำหนดวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศแก่ผู้ให้บริการภายนอก และขอให้ผู้ให้บริการภายนอกแต่ละรายดำเนินกิจกรรมการบริหารความเสี่ยงเพื่อให้บรรลุวัตถุประสงค์

๖.๓.๒.๑๐ การจัดการเหตุภัยคุกคามทางสารสนเทศ (Information Security Incident Management)

๖.๓.๒.๑๐.๑ ความรับผิดชอบและขั้นตอน (Responsibilities and Procedures)

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ก) ผู้ใช้บริการคลาวด์ต้องตรวจสอบการจัดสรรความรับผิดชอบสำหรับการจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ และต้องตรวจสอบให้แน่ใจว่าเป็นไปตามข้อกำหนดของผู้ใช้บริการคลาวด์ ข) เหตุภัยคุกคามทางสารสนเทศต้องนำไปสู่การทบทวนโดยผู้ใช้บริการคลาวด์หรือทบทวนร่วมกันระหว่างผู้ให้บริการคลาวด์ และผู้ใช้บริการคลาวด์ในฐานะที่เป็นส่วนหนึ่งของกระบวนการจัดการเหตุภัยคุกคามทางสารสนเทศของตนเพื่อพิจารณาว่าได้มีการละเมิดข้อมูลที่เกี่ยวข้องกับข้อมูลส่วนบุคคลเกิดขึ้นหรือไม่	ก) ผู้ให้บริการคลาวด์ ต้องกำหนดขอบเขตความรับผิดชอบและขั้นตอนการจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศระหว่างผู้ใช้บริการคลาวด์ และผู้ให้บริการคลาวด์โดยเป็นส่วนหนึ่งของข้อกำหนดบริการ ข) ผู้ให้บริการคลาวด์ต้องจัดเตรียมเอกสารให้ผู้ใช้บริการคลาวด์ครอบคลุม – ขอบเขตของเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่ผู้ให้บริการคลาวด์จะรายงานต่อผู้ใช้บริการคลาวด์ – ระดับการเปิดเผยการตรวจพบเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศและการตอบสนองที่เกี่ยวข้อง – กรอบเวลาเป้าหมายที่จะมีการแจ้งเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศเกิดขึ้น – ขั้นตอนการแจ้งเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ – ข้อมูลติดต่อสำหรับการจัดการปัญหาที่เกี่ยวข้องกับเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ

ผู้ใช้บริการคลาวด์	**ผู้ให้บริการคลาวด์**
	– การเยียวยาใดๆที่สามารถนำไปใช้ได้หากเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศบางอย่างขึ้น ค) เหตุภัยคุกคามทางสารสนเทศต้องนำไปสู่การทบทวนโดยผู้ใช้บริการคลาวด์หรือทบทวนร่วมกันระหว่างผู้ให้บริการคลาวด์ และผู้ใช้บริการคลาวด์ในฐานะที่เป็นส่วนหนึ่งของกระบวนการจัดการเหตุภัยคุกคามทางสารสนเทศของตนเพื่อพิจารณาว่าได้มีการละเมิดข้อมูลที่เกี่ยวข้องกับข้อมูลส่วนบุคคลเกิดขึ้นหรือไม่

๖.๓.๒.๑๐.๒ การรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Reporting Information Security Events)

ผู้ใช้บริการคลาวด์	**ผู้ให้บริการคลาวด์**
ก) ผู้ใช้บริการคลาวด์ต้องขอข้อมูลจากผู้ให้บริการคลาวด์เกี่ยวกับกลไกสำหรับ – ผู้ใช้บริการคลาวด์รายงานเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศที่ตรวจพบต่อผู้ให้บริการคลาวด์ – ผู้ให้บริการคลาวด์เพื่อรับรายงานเกี่ยวกับเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศที่ตรวจพบโดยผู้ให้บริการคลาวด์ – ผู้ใช้บริการคลาวด์เพื่อติดตามสถานะของเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศที่รายงาน	ก) ผู้ให้บริการคลาวด์ต้องมีกลไกสำหรับ – ผู้ใช้บริการคลาวด์รายงานเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศต่อผู้ให้บริการคลาวด์ – ผู้ให้บริการคลาวด์เพื่อรายงานเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศต่อผู้ใช้บริการคลาวด์ – ผู้ใช้บริการคลาวด์เพื่อติดตามสถานะของเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศที่รายงาน