นโยบายความมั่นคงปลอดภัยสารสนเทศ สำหรับการประมวลผลบนคลาวด์

ฉบับปี พ.ศ. 2569

งานสารสนเทศ
สถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน)

นโยบายความมั่นคงปลอดภัยสารสนเทศสำหรับการประมวลผลบนคลาวด์
สถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน) ฉบับปี พ.ศ. 2569

นโยบายความมั่นคงปลอดภัยสารสนเทศสำหรับการประมวลผลบนคลาวด์
สถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน)
ฉบับปี พ.ศ. 2569

1. บทนำ

ปัจจุบันเทคโนโลยีการประมวลผลบนคลาวด์ ได้เข้ามามีบทบาทสำคัญอย่างยิ่งต่อการขับเคลื่อนการดำเนินงานและการยกระดับโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศของสถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน) ให้มีความยืดหยุ่นและมีประสิทธิภาพ อย่างไรก็ดี การพึ่งพาบริการคลาวด์สาธารณะและการบริหารจัดการระบบผ่านเครือข่ายภายนอก ย่อมนำมาซึ่งความเสี่ยงและภัยคุกคามทางไซเบอร์รูปแบบใหม่ที่มีความซับซ้อน ซึ่งส่งผลกระทบโดยตรงต่อความมั่นคงปลอดภัยของระบบงานและข้อมูลสารสนเทศของสถาบัน

เพื่อเป็นการป้องกันเชิงรุกต่อความเสี่ยงดังกล่าว รวมถึงการกำหนดเกณฑ์มาตรฐานและคุณลักษณะเฉพาะในการกำกับดูแลหน่วยงานเอกชนผู้รับจ้างหรือผู้ให้บริการคลาวด์ภายนอก และเพื่อให้การดำเนินงานสอดคล้องตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 สถาบันจึงได้จัดทำ “นโยบายความมั่นคงปลอดภัยสารสนเทศสำหรับการประมวลผลบนคลาวด์” ฉบับนี้ขึ้น เพื่อใช้เป็นกรอบเกณฑ์มาตรฐานหลักในการควบคุม บังคับใช้ และบริหารจัดการความมั่นคงปลอดภัยในสภาพแวดล้อมการประมวลผลบนคลาวด์

นโยบายฉบับนี้จัดทำขึ้นโดยมุ่งเน้นการรักษาความลับ การรักษาความถูกต้องครบถ้วน และการรักษาสภาพพร้อมใช้งานของข้อมูลและสินทรัพย์สารสนเทศของสถาบันที่จัดเก็บหรือประมวลผลอยู่บนระบบคลาวด์ พร้อมทั้งมุ่งเน้นการกำหนดเงื่อนไขและมาตรการทางสัญญาที่เด็ดขาดในการควบคุมการปฏิบัติงาน การดูแลรักษา และการแก้ไขปัญหาของผู้ให้บริการคลาวด์ภายนอก ตลอดจนเพื่อให้การใช้งานระบบคลาวด์สอดคล้องตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ อย่างเป็นรูปธรรม

2. วัตถุประสงค์

2.1 เพื่อกำหนดหลักเกณฑ์ มาตรการ และแนวปฏิบัติในการควบคุมดูแลการใช้งานระบบคลาวด์และโครงสร้างพื้นฐานสารสนเทศของสถาบันให้มีความมั่นคงปลอดภัย สอดคล้องตามข้อกำหนดขั้นต่ำด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์

2.2 เพื่อสร้างกลไกและคุณลักษณะเฉพาะด้านความปลอดภัยในการคัดเลือก บริหารจัดการสัญญา และกำกับดูแลการดำเนินงานของหน่วยงานเอกชนผู้รับจ้างหรือผู้ให้บริการคลาวด์ภายนอก ให้ปฏิบัติงานดูแลรักษาและแก้ไขปัญหาเทคนิคอย่างมีประสิทธิภาพ

2.3 เพื่อสร้างความตระหนักรู้ จิตสำนึก และความเข้าใจแก่เจ้าหน้าที่ของสถาบัน รวมถึงบุคลากรของหน่วยงานเอกชนคู่สัญญา เกี่ยวกับความเสี่ยง มาตรฐาน มาตรการควบคุมการเข้าถึง และกระบวนการปกป้องคุ้มครองข้อมูลสารสนเทศบนสภาพแวดล้อมระบบคลาวด์

2.4 เพื่อรักษาไว้ซึ่งความลับ ความถูกต้องครบถ้วน และสภาพพร้อมใช้งานของข้อมูลสารสนเทศของสถาบัน ตลอดจนควบคุมกระบวนการจัดชั้นความลับ การเข้ารหัสข้อมูล การบริหารจัดการกุญแจเข้ารหัสลับ และการทำลายข้อมูลเมื่อสิ้นสุดสัญญาจ้างให้เป็นไปตามระเบียบและกฎหมายที่เกี่ยวข้อง

3. นิยามศัพท์

3.1 “สถาบัน” หมายถึง สถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน)

3.2 “นโยบาย” หมายความว่า นโยบายความมั่นคงปลอดภัยสารสนเทศสำหรับการประมวลผลบนคลาวด์ สถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน)

3.3 “ระบบคลาวด์ (Cloud Computing)” หมายความว่า รูปแบบการให้บริการและจัดสรรทรัพยากรคอมพิวเตอร์ผ่านระบบเครือข่าย ซึ่งครอบคลุมถึงระบบประมวลผล พื้นที่จัดเก็บข้อมูล เครือข่าย และแอปพลิเคชัน ที่มีความยืดหยุ่นและสามารถปรับขนาดการใช้งานได้ตามความต้องการ

3.4 “ผู้ให้บริการคลาวด์ภายนอก (Cloud Service Provider: CSP)” หมายความว่า นิติบุคคล หรือหน่วยงานเอกชนคู่สัญญา ที่รับจ้างให้บริการทรัพยากรการประมวลผลบนระบบคลาวด์ รวมถึงผู้รับจ้างช่วง (Subcontractor) ที่ดำเนินการในนามของผู้ให้บริการดังกล่าว

3.5 “บริการประเภทโครงสร้างพื้นฐาน (Infrastructure as a Service: IaaS)” หมายความว่า การให้บริการโครงสร้างพื้นฐานทางระบบคอมพิวเตอร์ เช่น หน่วยประมวลผล เครือข่าย และพื้นที่จัดเก็บข้อมูลแบบเสมือนจริง โดยสถาบันมีสิทธิ์ในการควบคุมระบบปฏิบัติการและแอปพลิเคชัน

3.6 “บริการประเภทแพลตฟอร์ม (Platform as a Service: PaaS)” หมายความว่า การให้บริการสภาพแวดล้อมคอมพิวเตอร์และแพลตฟอร์มที่รองรับการพัฒนา ทดสอบ และบริหารจัดการแอปพลิเคชันของสถาบัน

3.7 “บริการประเภทซอฟต์แวร์ (Software as a Service: SaaS)” หมายความว่า การให้บริการแอปพลิเคชันหรือซอฟต์แวร์เบ็ดเสร็จผ่านระบบเครือข่ายอินเทอร์เน็ต โดยสถาบันในฐานะผู้ใช้บริการไม่ต้องบริหารจัดการโครงสร้างพื้นฐานหรือแพลตฟอร์มเบื้องหลัง

3.8 “เจ้าหน้าที่” หมายความว่า ผู้บริหาร พนักงาน ลูกจ้าง ผู้เชี่ยวชาญ หรือบุคคลอื่นใดที่ปฏิบัติงานให้แก่สถาบัน ซึ่งได้รับอนุญาตและได้รับสิทธิ์ให้เข้าถึงข้อมูลและใช้งานระบบคลาวด์ของสถาบัน

3.9 “ทรัพย์สินสารสนเทศ” หมายความว่า ข้อมูล ฐานข้อมูล ซอฟต์แวร์ ระบบเครือข่าย หรือสิ่งอื่นใดที่มีมูลค่าและมีความสำคัญต่อการดำเนินงานของสถาบัน ซึ่งถูกจัดเก็บ ประมวลผล หรือส่งผ่านสภาพแวดล้อมระบบคลาวด์

3.10 “การยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication: MFA)” หมายความว่า มาตรการควบคุมและพิสูจน์ทราบตัวบุคคลในการเข้าถึงระบบ โดยบังคับให้ผู้ใช้งานต้องแสดงหลักฐานยืนยันตัวตนที่แตกต่างกันตั้งแต่สองปัจจัยขึ้นไปประกอบกัน

3.11 “เหตุละเมิดความมั่นคงปลอดภัยไซเบอร์” หมายความว่า เหตุการณ์ผิดปกติ การบุกรุก หรือการกระทำใด ๆ ที่ส่งผลกระทบหรืออาจส่งผลกระทบต่อความลับ ความถูกต้องครบถ้วน หรือสภาพพร้อมใช้งานของระบบคลาวด์และทรัพย์สินสารสนเทศของสถาบัน

ส่วนที่ 1 การกำกับดูแลด้านความมั่นคงปลอดภัยระบบคลาวด์

1. วัตถุประสงค์ของนโยบาย

1.1 เพื่อกำหนดขอบเขตและแนวทางปฏิบัติในการใช้บริการคลาวด์ของสถาบันให้มีความมั่นคงปลอดภัย และสอดคล้องกับระดับความเสี่ยงที่ยอมรับได้

1.2 เพื่อใช้เป็นข้อกำหนดมาตรฐานและคุณลักษณะเฉพาะด้านความปลอดภัยในการคัดเลือก และควบคุมการดำเนินงานของหน่วยงานเอกชน ผู้รับจ้างหรือผู้ให้บริการคลาวด์ภายนอก

1.3 เพื่อกำหนดบทบาทหน้าที่ ความรับผิดชอบ และแนวทางการประสานงานร่วมกันระหว่างเจ้าหน้าที่ของสถาบันและผู้ให้บริการคลาวด์ภายนอกในการดูแลรักษาและการแก้ไขปัญหาเมื่อเกิดเหตุคุกคามไซเบอร์

2. แนวทางปฏิบัติในการกำกับดูแลด้านความมั่นคงปลอดภัยระบบคลาวด์

2.1 การกำหนดข้อกำหนดทางสัญญาและการควบคุมผู้ให้บริการคลาวด์ภายนอก

2.1.1 สถาบันต้องจัดทำข้อตกลงทางสัญญาที่ระบุขอบเขตความรับผิดชอบร่วมกันระหว่างสถาบัน ผู้ให้บริการคลาวด์ภายนอก และผู้รับจ้างช่วงอย่างชัดเจน โดยแยกแยะตามประเภทของบริการคลาวด์ที่เลือกใช้ ไม่ว่าจะเป็น บริการประเภทโครงสร้างพื้นฐาน (IaaS) บริการประเภทแพลตฟอร์ม (PaaS) หรือบริการประเภทซอฟต์แวร์ (SaaS) เพื่อให้การควบคุมความปลอดภัยในระดับแอปพลิเคชันและโครงสร้างพื้นฐานมีความชัดเจน

2.1.2 ข้อกำหนดในสัญญาต้องระบุให้ผู้ให้บริการคลาวด์ภายนอกมีนโยบายและมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศที่มีประสิทธิภาพในการออกแบบและการดำเนินงานด้านบริการคลาวด์ รวมถึงต้องมีมาตรการบริหารจัดการเพื่อลดความเสี่ยงที่อาจเกิดขึ้นจากบุคคลภายในของผู้ให้บริการเองที่ได้รับสิทธิ์ในการเข้าถึงระบบ

2.1.3 การประมวลผลข้อมูลบนระบบคลาวด์ต้องกำหนดให้ผู้ให้บริการคลาวด์ภายนอกจัดทำข้อตกลงและปฏิบัติตามแนวทางการคุ้มครองข้อมูลส่วนบุคคลของสถาบันอย่างเคร่งครัด โดยครอบคลุมถึงมาตรการการเข้าถึงและปกป้องข้อมูลของสถาบัน และการจำกัดสิทธิ์มิให้เข้าใช้งานข้อมูลโดยมิได้รับอนุญาต

2.2 มาตรฐานทางเทคนิคและการจัดการความปลอดภัยของผู้ให้บริการคลาวด์ภายนอก

2.2.1 ผู้ให้บริการคลาวด์ภายนอกต้องมีมาตรฐานเทคโนโลยีในการแยกแยะผู้ใช้บริการคลาวด์แต่ละรายออกจากกันอย่างเด็ดขาดในสภาพแวดล้อมที่มีการเช่าใช้ระบบร่วมกันหลายราย รวมถึงระบบการจำลองเสมือน เพื่อป้องกันการรั่วไหลหรือความเสียหายของข้อมูลระหว่างหน่วยงาน

2.2.2 ผู้ให้บริการคลาวด์ภายนอกต้องกำหนดขั้นตอนการควบคุมการเข้าถึงทรัพย์สินสารสนเทศของสถาบันอย่างเข้มงวด โดยเฉพาะการกำหนดให้ผู้ดูแลระบบของผู้ให้บริการคลาวด์ต้องใช้เทคนิคการยืนยันตัวตนที่เข้มงวดในการเข้าถึงระบบเพื่อปฏิบัติงานดูแลรักษา

2.2.3 ผู้ให้บริการคลาวด์ภายนอกต้องมีกระบวนการสื่อสารและแจ้งเตือนสถาบันในระหว่างการบริหารจัดการความเปลี่ยนแปลงของระบบคลาวด์ เพื่อให้เจ้าหน้าที่ของสถาบันสามารถเตรียมการรองรับและประเมินผลกระทบด้านความปลอดภัยได้อย่างทันท่วงที

2.3 การแก้ไขปัญหา การสืบสวน และการประสานงานร่วมกัน

2.3.1 ข้อกำหนดในสัญญาต้องระบุเงื่อนไขให้ผู้ให้บริการคลาวด์ภายนอกมีหน้าที่สื่อสารและแจ้งเตือนสถาบันโดยทันทีเมื่อเกิดเหตุละเมิดความมั่นคงปลอดภัยไซเบอร์ และต้องสนับสนุนแนวทางการแบ่งปัน

ข้อมูลเพื่อช่วยในการสืบสวนและการพิสูจน์หลักฐานดิจิทัลทางนิติเวชไซเบอร์เมื่อเกิดปัญหากระทบต่อระบบของสถาบัน

2.3.2 สถาบันต้องตกลงและบันทึกการแบ่งบทบาทหน้าที่ด้านความมั่นคงปลอดภัยสารสนเทศกับผู้ให้บริการคลาวด์ภายนอกเป็นลายลักษณ์อักษร เพื่อยืนยันว่าสถาบันและเจ้าหน้าที่สามารถทำหน้าที่ตามสิทธิ์ที่จัดสรรได้อย่างสมบูรณ์ และผู้ให้บริการคลาวด์ภายนอกต้องแต่งตั้งผู้ประสานงานด้านการคุ้มครองข้อมูลส่วนบุคคลเพื่อปฏิบัติงานร่วมกับสถาบันโดยเฉพาะ

2.3.3 เจ้าหน้าที่ของสถาบันต้องระบุและจัดการความสัมพันธ์กับหน่วยงานสนับสนุนลูกค้าและฟังก์ชันการดูแลระบบของผู้ให้บริการคลาวด์ภายนอกอย่างชัดเจน รวมถึงกำหนดให้ผู้ให้บริการแจ้งข้อมูลที่ตั้งทางภูมิศาสตร์ขององค์กรและประเทศที่ใช้จัดเก็บข้อมูลของสถาบัน เพื่อให้สถาบันสามารถประเมินขอบเขตการกำกับดูแลและการดำเนินการร่วมกันเมื่อเกิดเหตุฉุกเฉิน

ส่วนที่ 2 การบริหารทรัพยากรมนุษย์และการจัดการทรัพย์สินระบบคลาวด์

1. วัตถุประสงค์ของนโยบาย

1.1 เพื่อให้เจ้าหน้าที่และผู้ให้บริการคลาวด์ภายนอกมีความตระหนักรู้และเข้าใจในความเสี่ยง มาตรฐาน และขั้นตอนการใช้งานระบบคลาวด์อย่างปลอดภัยตามกฎหมายและระเบียบที่เกี่ยวข้อง

1.2 เพื่อควบคุมการบริหารจัดการทรัพยากรบุคคลของสถาบันและคู่สัญญาให้มีจิตสำนึกด้านความมั่นคงปลอดภัยสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคล

1.3 เพื่อกำหนดหลักเกณฑ์ในการจัดทำทะเบียนบัญชีทรัพย์สินสารสนเทศบนระบบคลาวด์ รวมถึงระบุสถานที่จัดเก็บข้อมูลทางภูมิศาสตร์อย่างชัดเจนและตรวจสอบได้

1.4 เพื่อควบคุมการบ่งชี้ชั้นความลับของข้อมูลของสถาบันที่จัดเก็บอยู่บนระบบคลาวด์ให้ถูกต้องตามระเบียบที่กำหนด และบังคับให้ผู้ให้บริการคลาวด์ภายนอกจัดเตรียมเครื่องมือรองรับการดำเนินงานดังกล่าว

2. แนวทางปฏิบัติในการบริหารทรัพยากรมนุษย์และการจัดการทรัพย์สินระบบคลาวด์

2.1 การบริหารทรัพยากรมนุษย์และความตระหนักรู้ด้านความปลอดภัยระบบคลาวด์

2.1.1 สถาบันต้องจัดให้มีกระบวนการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศ การศึกษา และการฝึกอบรมเกี่ยวกับบริการคลาวด์แก่ผู้บริหารและเจ้าหน้าที่ของสถาบันอย่างสม่ำเสมอ

2.1.2 เจ้าหน้าที่ที่มีหน้าที่ดูแลระบบคลาวด์ ผู้บริหารจัดการธุรกิจคลาวด์ และเจ้าหน้าที่ผู้ใช้งานระบบคลาวด์ รวมถึงพนักงานและผู้รับจ้างที่เกี่ยวข้อง ต้องได้รับการฝึกอบรมในหัวข้อที่ครอบคลุมถึงมาตรฐานและขั้นตอนการใช้บริการคลาวด์ ความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศและวิธีการจัดการความเสี่ยง ความเสี่ยงด้านสภาพแวดล้อมของระบบและเครือข่าย การคุ้มครองข้อมูลส่วนบุคคล ตลอดจนข้อพิจารณาทางกฎหมายและข้อบังคับที่เกี่ยวข้อง

2.1.3 ข้อกำหนดในสัญญาจ้างต้องบังคับให้ผู้ให้บริการคลาวด์ภายนอกดำเนินการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคล การศึกษา และการฝึกอบรมแก่พนักงานรวมถึงผู้รับจ้างช่วงของผู้ให้บริการคลาวด์เกี่ยวกับการจัดการข้อมูลของสถาบันอย่างเหมาะสม โดยต้องปฏิบัติตามข้อจำกัดเฉพาะและข้อจำกัดทางกฎหมายในการเข้าถึงและใช้งานข้อมูลอย่างเคร่งครัด

2.2 การจัดการทะเบียนทรัพย์สินและการบ่งชี้ข้อมูลบนระบบคลาวด์

2.2.1 ฝ่ายเทคโนโลยีสารสนเทศต้องจัดทำและปรับปรุงทะเบียนทรัพย์สินสารสนเทศที่จัดเก็บหรือประมวลผลในสภาพแวดล้อมการประมวลผลบนคลาวด์ให้เป็นปัจจุบัน โดยในบันทึกทะเบียนทรัพย์สินต้องระบุสถานที่จัดเก็บทรัพย์สินทางภูมิศาสตร์และชื่อของผู้ให้บริการคลาวด์ไว้อย่างชัดเจน

2.2.2 ข้อกำหนดในสัญญาจ้างต้องระบุให้ผู้ให้บริการคลาวด์ภายนอกจัดทำเอกสารระบุในทะเบียนทรัพย์สินของตนเองอย่างชัดเจนเกี่ยวกับข้อมูลของสถาบันในฐานะผู้ใช้บริการ และข้อมูลทั้งหมดที่เกิดขึ้นจากการใช้บริการคลาวด์ของสถาบัน

2.2.3 เจ้าหน้าที่ผู้รับผิดชอบต้องดำเนินการบ่งชี้ข้อมูลและทรัพย์สินของสถาบันที่ใช้งานหรือเก็บรักษาไว้บนระบบคลาวด์ตามขั้นตอนปฏิบัติสำหรับการบ่งชี้และจัดชั้นความลับข้อมูลของสถาบัน เพื่อแยกแยะข้อมูลตามระดับความสำคัญและสอดคล้องกับแนวทางการจัดโซนระบบสารสนเทศ

2.2.4 ผู้ให้บริการคลาวด์ภายนอกต้องจัดทำเอกสารและเปิดเผยฟังก์ชันการทำงานของบริการคลาวด์ใด ๆ ที่สถาบันสามารถนำไปใช้เพื่อวัตถุประสงค์ในการบ่งชี้ข้อมูลและทรัพย์สินที่เกี่ยวข้อง เพื่อให้สถาบันสามารถควบคุมชั้นความลับของข้อมูลได้อย่างมีประสิทธิภาพ

ส่วนที่ 3 การควบคุมการเข้าถึงและการเข้ารหัสข้อมูลบนระบบคลาวด์

1. **วัตถุประสงค์ของนโยบาย**

1.1 เพื่อกำหนดหลักเกณฑ์ มาตรการทางเทคนิค และวิธีปฏิบัติในการควบคุมการเข้าถึงระบบคลาวด์และสารสนเทศของสถาบันให้เป็นไปตามสิทธิ์ที่จำเป็นและมีความปลอดภัยสูงสุด

1.2 เพื่อยกระดับความมั่นคงปลอดภัยในกระบวนการพิสูจน์ตัวตนและการยืนยันตัวตนสำหรับเจ้าหน้าที่ผู้ใช้งานทั่วไปและเจ้าหน้าที่ผู้ดูแลระบบ

1.3 เพื่อกำหนดแนวทางการเลือกใช้เทคโนโลยีการเข้ารหัสข้อมูลและการบริหารจัดการกุญแจเข้ารหัสลับที่มีความแข็งแกร่งในการรักษาความลับและความถูกต้องครบถ้วนของข้อมูลบนระบบคลาวด์

1.4 เพื่อใช้เป็นเกณฑ์มาตรฐานทางเทคนิคในการบังคับให้ผู้ให้บริการคลาวด์ภายนอกจัดเตรียมกลไกการควบคุมการเข้าถึงและการเข้ารหัสข้อมูลที่สอดคล้องกับข้อกำหนดและกฎหมายที่เกี่ยวข้อง

2. แนวทางปฏิบัติในการควบคุมการเข้าถึงและการเข้ารหัสข้อมูลบนระบบคลาวด์

2.1 การบริหารจัดการสิทธิ์และการควบคุมการเข้าถึงระบบคลาวด์

2.1.1 สถาบันต้องกำหนดสิทธิ์การเข้าถึงระบบคลาวด์และสารสนเทศตามบทบาทหน้าที่และความจำเป็นในการปฏิบัติงาน โดยใช้หลักการให้สิทธิ์เท่าที่จำเป็นขั้นต่ำ และการแบ่งแยกหน้าที่ความรับผิดชอบเพื่อป้องกันการเข้าถึงข้อมูลโดยมิชอบ

2.1.2 ฝ่ายเทคโนโลยีสารสนเทศต้องจัดให้มีขั้นตอนปฏิบัติในการลงทะเบียน การเปลี่ยนแปลง และการยกเลิกสิทธิ์ของผู้ใช้งานและผู้ดูแลระบบคลาวด์อย่างเป็นระบบ และต้องดำเนินการเพิกถอนสิทธิ์โดยทันทีเมื่อเจ้าหน้าที่พ้นสภาพการปฏิบัติงานหรือมีการปรับเปลี่ยนหน้าที่ความรับผิดชอบ

2.1.3 ฝ่ายเทคโนโลยีสารสนเทศต้องดำเนินการทบทวนสิทธิ์การเข้าถึงระบบคลาวด์และสารสนเทศของเจ้าหน้าที่ทุกระดับอย่างสม่ำเสมออย่างน้อยปีละหนึ่งครั้ง เพื่อให้มั่นใจว่าสิทธิ์การเข้าใช้งานมีความเหมาะสมและเป็นปัจจุบัน

2.1.4 ข้อกำหนดในสัญญาจ้างต้องระบุให้ผู้ให้บริการคลาวด์ภายนอกจัดเตรียมเครื่องมือและฟังก์ชันการทำงานที่จำเป็น เพื่อให้สถาบันสามารถควบคุม กำกับดูแล และจัดสรรสิทธิ์การเข้าถึงระบบและข้อมูลที่จัดเก็บไว้บนระบบคลาวด์ได้อย่างมีประสิทธิภาพ

2.2 การพิสูจน์ตัวตนและการรักษาความปลอดภัยระดับระบบ

2.2.1 การเข้าใช้งานระบบคลาวด์และสารสนเทศของสถาบัน ต้องผ่านกระบวนการพิสูจน์ตัวตนที่มั่นคงปลอดภัย โดยให้เจ้าหน้าที่กำหนดรหัสผ่านตามเกณฑ์มาตรฐานความปลอดภัยที่สถาบันประกาศกำหนด

2.2.2 เจ้าหน้าที่ที่ได้รับสิทธิ์พิเศษหรือผู้ดูแลระบบ รวมถึงเจ้าหน้าที่ของผู้ให้บริการคลาวด์ภายนอกที่มีสิทธิ์เข้าถึงโครงสร้างพื้นฐานระบบคลาวด์ในส่วนที่เกี่ยวข้องกับสถาบัน ต้องใช้เทคนิคการยืนยันตัวตนแบบหลายปัจจัยในการเข้าสู่ระบบเพื่อปฏิบัติงานทุกครั้ง

2.2.3 สถาบันและผู้ให้บริการคลาวด์ภายนอกต้องร่วมกันจำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์ที่มีขีดความสามารถในการข้ามมาตรการควบคุมความปลอดภัยของระบบคลาวด์ โดยจะอนุญาตให้ใช้เฉพาะในกรณีที่มีความจำเป็นอย่างยิ่งยวดและต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้มีอำนาจเท่านั้น

2.3 การเข้ารหัสข้อมูลและการบริหารจัดการกุญแจเข้ารหัสลับ

2.3.1 ข้อมูลของสถาบันที่มีความสำคัญหรือถูกจัดจำแนกอยู่ในชั้นความลับตามที่ระเบียบกำหนด ต้องได้รับการเข้ารหัสข้อมูลทั้งในขณะจัดเก็บและในระหว่างการรับส่งข้อมูลผ่านเครือข่าย เพื่อป้องกันการรั่วไหลและการดักรับข้อมูลจากผู้ไม่มีสิทธิ์

2.3.2 ฝ่ายเทคโนโลยีสารสนเทศและผู้ให้บริการคลาวด์ภายนอกต้องร่วมกันกำหนดมาตรการและกระบวนการบริหารจัดการกุญแจเข้ารหัสลับตลอดวงจรชีวิต ตั้งแต่การสร้าง การจัดเก็บ การแจกจ่าย การใช้งาน การเปลี่ยนทดแทน และการทำลายกุญแจเข้ารหัสลับ เพื่อมิให้บุคคลที่ไม่ได้รับอนุญาตสามารถเข้าถึงกุญแจดังกล่าวได้

2.3.3 ข้อกำหนดในสัญญาจ้างต้องบังคับให้ผู้ให้บริการคลาวด์ภายนอกเปิดเผยและชี้แจงเทคโนโลยีอัลกอริทึมที่ใช้ในการเข้ารหัสข้อมูล และแนวทางการบริหารจัดการกุญแจเข้ารหัสลับให้สถาบันทราบ เพื่อให้สถาบันสามารถประเมินความแข็งแกร่งและความสอดคล้องกับมาตรฐานสากลก่อนการลงนามในสัญญา

ส่วนที่ 4 การจัดหาและการจัดการผู้ให้บริการคลาวด์ภายนอก

1. วัตถุประสงค์ของนโยบาย

1.1 เพื่อกำหนดหลักเกณฑ์ มาตรการ และขั้นตอนปฏิบัติในการประเมินและคัดเลือกผู้ให้บริการคลาวด์ภายนอกให้สอดคล้องกับข้อกำหนดความมั่นคงปลอดภัยสารสนเทศของสถาบันก่อนการจัดซื้อจัดจ้าง

1.2 เพื่อบังคับใช้ข้อตกลงระดับการให้บริการและมาตรการควบคุมทางสัญญาในการกำกับดูแลการดำเนินงาน การบำรุงรักษา และการแก้ไขปัญหาทางเทคนิคของผู้ให้บริการคลาวด์ภายนอก

1.3 เพื่อกำหนดแนวทางการจัดการเหตุการณ์ผิดปกติและการประสานงานร่วมกับคู่สัญญาเอกชนเมื่อเกิดภัยคุกคามไซเบอร์กระทบต่อระบบคลาวด์ของสถาบัน

1.4 เพื่อควบคุมกระบวนการส่งคืน การโอนย้าย และการทำลายข้อมูลของสถาบันอย่างปลอดภัยเมื่อสิ้นสุดสัญญาจ้างหรือการยกเลิกใช้บริการคลาวด์

2. แนวทางปฏิบัติในการจัดหาและการจัดการผู้ให้บริการคลาวด์ภายนอก

2.1 การจัดหาและกำหนดคุณลักษณะเฉพาะด้านความมั่นคงปลอดภัย

2.1.1 ฝ่ายเทคโนโลยีสารสนเทศต้องจัดทำข้อกำหนดคุณลักษณะเฉพาะด้านความมั่นคงปลอดภัยสารสนเทศและเกณฑ์การประมวลผลบนระบบคลาวด์ บรรจุไว้ในเอกสารเชิญชวนประกวดราคาหรือขอบเขตงานจ้างอย่างชัดเจนก่อนการจัดหาบริการคลาวด์ทุกครั้ง

2.1.2 สถาบันต้องดำเนินการประเมินความสามารถและสอดคล้องตามเกณฑ์มาตรฐานของผู้ให้บริการคลาวด์ภายนอก โดยผู้ให้บริการต้องแสดงหลักฐานการรับรองมาตรฐานสากลด้านความปลอดภัยคลาวด์ หรือรายงานผลการตรวจประเมินจากหน่วยงานภายนอกที่เป็นอิสระ เพื่อให้สถาบันมั่นใจว่าผู้ให้บริการสามารถปฏิบัติตามข้อกำหนดที่สถาบันกำหนดได้จริง

2.1.3 ฝ่ายเทคโนโลยีสารสนเทศต้องขอข้อมูลและตรวจสอบแนวทางการพัฒนาที่ปลอดภัย นโยบายการทดสอบระบบ และการบริหารจัดการช่องโหว่ของผู้ให้บริการคลาวด์ภายนอก เพื่อประเมินความเสี่ยงด้านสถาปัตยกรรมระบบคลาวด์ก่อนการลงนามในสัญญา

2.2 การกำกับดูแลและการบริหารจัดการผู้ให้บริการคลาวด์ภายนอก

2.2.1 ข้อกำหนดในสัญญาจ้างต้องระบุข้อตกลงระดับการให้บริการที่ครอบคลุมถึงดัชนีวัดผลการดำเนินงาน มาตรการการป้องกันมัลแวร์ การสำรองข้อมูล การจัดการช่องโหว่ทางเทคนิค และสิทธิ์ในการเข้าตรวจประเมินระบบโดยสถาบันหรือผู้ตรวจสอบที่ได้รับมอบหมาย

2.2.2 ฝ่ายเทคโนโลยีสารสนเทศต้องดำเนินการเฝ้าระวัง ตรวจสอบ และทบทวนผลการดำเนินงานของผู้ให้บริการคลาวด์ภายนอกอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าบริการคลาวด์และการประมวลผลข้อมูลเป็นไปตามเงื่อนไขความมั่นคงปลอดภัยที่ระบุไว้ในสัญญาจ้าง

2.2.3 ในกรณีที่มีการเปลี่ยนแปลงสถาปัตยกรรมระบบคลาวด์ ซอฟต์แวร์ หรือมาตรการควบคุมความปลอดภัยที่มีนัยสำคัญ ผู้ให้บริการคลาวด์ภายนอกต้องแจ้งให้สถาบันทราบล่วงหน้าเป็นลายลักษณ์อักษร เพื่อให้สถาบันร่วมประเมินผลกระทบก่อนการอนุมัติให้ดำเนินการเปลี่ยนแปลง

2.3 การจัดการและแก้ไขปัญหาเมื่อเกิดเหตุการณ์ผิดปกติ

2.3.1 ข้อกำหนดในสัญญาจ้างต้องบังคับให้ผู้ให้บริการคลาวด์ภายนอกจัดเตรียมกระบวนการและช่องทางการสื่อสารในการแจ้งเหตุละเมิดความมั่นคงปลอดภัยสารสนเทศหรือภัยคุกคามไซเบอร์ต่อสถาบันโดยทันทีเมื่อเกิดเหตุ

2.3.2 ผู้ให้บริการคลาวด์ภายนอกต้องส่งมอบข้อมูล บันทึกเหตุการณ์ผิดปกติ และเอกสารรายละเอียดเกี่ยวกับขั้นตอนการจัดการปัญหา รวมถึงมาตรการเยียวยาความเสียหายให้แก่สถาบัน เพื่อใช้เป็นข้อมูลในการแก้ไขปัญหาและวิเคราะห์หาสาเหตุร่วมกัน

2.3.3 เมื่อเกิดภัยคุกคามสารสนเทศที่ส่งผลกระทบต่อสถาบัน ฝ่ายเทคโนโลยีสารสนเทศและผู้ให้บริการคลาวด์ภายนอกต้องร่วมกันจัดกิจกรรมทบทวนและประเมินเหตุการณ์ เพื่อพิจารณาว่ามีการรั่วไหลหรือการละเมิดข้อมูลที่เกี่ยวข้องกับข้อมูลส่วนบุคคลของสถาบันเกิดขึ้นหรือไม่ เพื่อดำเนินการตามกฎหมายที่เกี่ยวข้องต่อไป

2.4 การจัดการสินทรัพย์และการยกเลิกการใช้บริการคลาวด์

2.4.1 ข้อกำหนดในสัญญาจ้างต้องระบุขั้นตอนปฏิบัติอย่างชัดเจนเมื่อสิ้นสุดสัญญาจ้างหรือการยกเลิกการใช้บริการ โดยผู้ให้บริการคลาวด์ภายนอกต้องดำเนินการส่งคืนข้อมูลและสินทรัพย์สารสนเทศทั้งหมดให้แก่สถาบัน หรือทำการโอนย้ายไปยังผู้ให้บริการรายใหม่ตามที่สถาบันมอบหมาย

2.4.2 ผู้ให้บริการคลาวด์ภายนอกต้องมีกระบวนการลบหรือทำลายข้อมูล สำเนาข้อมูล และไฟล์สำรองของสถาบันที่ยังคงค้างอยู่ในระบบประมวลผลคลาวด์และสื่อบันทึกข้อมูลของผู้ให้บริการอย่างปลอดภัยและถาวร โดยต้องจัดทำหนังสือยืนยันและหลักฐานการทำลายข้อมูลส่งมอบให้แก่สถาบันเพื่อตรวจสอบ