ประกาศกรมปศุสัตว์
เรื่อง นโยบายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ของกรมปศุสัตว์
พ.ศ. ๒๕๖๗

ตามที่ได้มีประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. ๒๕๖๗ โดยอาศัยอำนาจตามความในมาตรา ๙ (๔) แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ โดยหน่วยงานของรัฐต้องดำเนินการตามนโยบายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ เพื่อลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่มีต่อการใช้บริการคลาวด์สาธารณะให้กับหน่วยงานของรัฐ

เพื่อให้การดำเนินการด้านระบบคลาวด์ของกรมปศุสัตว์ มีความมั่นคงปลอดภัย มีมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์เป็นที่ยอมรับในระดับสากล กรมปศุสัตว์จึงกำหนดนโยบายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ของกรมปศุสัตว์ พ.ศ. ๒๕๖๗ เพื่อให้ผู้ใช้งาน ผู้ดูแลระบบงาน และผู้เกี่ยวข้องกับระบบเครือข่ายคอมพิวเตอร์และระบบเทคโนโลยีสารสนเทศของกรมปศุสัตว์ใช้เป็นแนวทางในการดูแลรักษาความมั่นคงปลอดภัยทางไซเบอร์ระบบคลาวด์ และสนับสนุนการดำเนินงานของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ กรมปศุสัตว์จึงออกประกาศไว้ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศกรมปศุสัตว์ เรื่อง นโยบายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ของกรมปศุสัตว์ พ.ศ. ๒๕๖๗”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

ข้อ ๓ ประกาศนี้ให้ใช้บังคับแก่ ข้าราชการ พนักงานราชการ เจ้าหน้าที่ พนักงานของรัฐ ลูกจ้าง ผู้บริหารองค์กร ผู้รับบริการ ผู้รับจ้างทำของ เจ้าหน้าที่ของหน่วยงานภายนอก ที่ปฏิบัติงานอยู่ภายในหน่วยงานสังกัดกรมปศุสัตว์ และผู้ใช้งานที่ใช้บริการระบบเทคโนโลยีสารสนเทศของกรมปศุสัตว์

ข้อ ๔ ในประกาศนี้

“หน่วยงาน” หมายความว่า หน่วยงานที่อยู่ภายใต้การควบคุมหรือกำกับดูแลของกรมปศุสัตว์

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

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

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

(๒) การให้...

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

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

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

(๕) การให้บริการอื่นที่สำนักงานประกาศกำหนด

"คลาวด์สาธารณะ" (Public Cloud) หมายความว่า รูปแบบการใช้คลาวด์ที่บริการคลาวด์สามารถใช้ได้กับผู้ใช้บริการคลาวด์ใด ๆ และทรัพยากรถูกควบคุมโดยผู้ให้บริการคลาวด์

"ผู้ใช้บริการคลาวด์" (Cloud Service Customer : CSC) หมายความว่า หน่วยงานที่มีข้อตกลงทางสัญญาอย่างเป็นทางการในการใช้บริการคลาวด์ที่ให้บริการโดยผู้ให้บริการคลาวด์

"ผู้ให้บริการคลาวด์" (Cloud Service Provider : CSP) หมายความว่า หน่วยงานของรัฐหรือเอกชนที่ทำให้บริการคลาวด์สามารถใช้ได้กับผู้ใช้บริการคลาวด์ รวมถึงจัดการทรัพยากรเหล่านี้เพื่อให้มั่นใจว่ามีความพร้อมใช้งานความมั่นคงปลอดภัย และความสามารถในการขยายตัวสำหรับผู้ใช้บริการคลาวด์ของตน

"ข้อมูลส่วนบุคคล" หมายความว่า ข้อมูลส่วนบุคคลตามที่กำหนดไว้ในมาตรา ๖ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

ข้อ ๕ นโยบายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ของกรมปศุสัตว์ พ.ศ. ๒๕๖๗ มีวัตถุประสงค์ ดังต่อไปนี้

(๑) เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานด้านสารสนเทศของกรมปศุสัตว์ ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

(๒) เพื่อกำหนดกรอบมาตรฐาน แนวทางปฏิบัติ และวิธีการปฏิบัติให้ผู้บริหาร ผู้ใช้งาน ผู้ดูแลระบบ และผู้เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศของกรมปศุสัตว์ ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบคลาวด์สาธารณะ และปฏิบัติตามอย่างเคร่งครัด โดยจะต้องมีการทบทวนนโยบายปีละ ๑ ครั้ง

(๓) เพื่อเผยแพร่ประกาศนโยบายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ของกรมปศุสัตว์ พ.ศ. ๒๕๖๗ ให้เจ้าหน้าที่ทุกระดับของหน่วยงานในสังกัดกรมปศุสัตว์ และผู้ที่เกี่ยวข้องทั้งหมดได้รับทราบ และถือปฏิบัติตามนโยบายอย่างเคร่งครัด

ข้อ ๖ ให้หน่วยงานที่ใช้บริการคลาวด์สาธารณะดำเนินการตามนโยบายนี้ โดยคำนึงถึงระดับผลกระทบของข้อมูลหรือระบบสารสนเทศ ตามที่กำหนดไว้ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๖ และดำเนินการไม่น้อยกว่าข้อกำหนดขั้นต่ำท้ายประกาศนี้

ข้อ ๗ การดำเนิน...

ข้อ ๗ การดำเนินการตามข้อ ๖ กรณีเป็นข้อมูลส่วนบุคคล ให้จัดระดับผลกระทบด้านการรักษาความลับระดับกลางเป็นอย่างน้อย ตามที่กำหนดไว้ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๖ และดำเนินการไม่น้อยกว่าข้อกำหนดขั้นต่ำท้ายประกาศนี้

ข้อ ๘ นโยบายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ของกรมปศุสัตว์ พ.ศ. ๒๕๖๗ จัดเป็นมาตรฐานด้านการรักษาความปลอดภัยในการใช้งานระบบคลาวด์สาธารณะของกรมปศุสัตว์ เพื่อใช้เป็นแนวทางในการดำเนินงานอย่างปลอดภัย เชื่อถือได้ เป็นไปตามกฎหมาย และระเบียบที่เกี่ยวข้อง จึงให้ใช้แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ของกรมปศุสัตว์ ตามเอกสารแนบท้ายประกาศนี้ ซึ่งเจ้าหน้าที่ของหน่วยงานในสังกัดกรมปศุสัตว์และผู้เกี่ยวข้องจะต้องปฏิบัติตามอย่างเคร่งครัด

ข้อ ๙ กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศของกรมปศุสัตว์เกิดความเสียหายหรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือที่ฝ่าฝืนการปฏิบัติตามนโยบายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ของกรมปศุสัตว์ พ.ศ. ๒๕๖๗ ตามประกาศนี้ กรมปศุสัตว์จะพิจารณาดำเนินการทางวินัย และทางกฎหมาย แก่ผู้ที่กระทำความผิดนั้น ตามกฎหมาย ระเบียบหรือประกาศที่เกี่ยวข้อง

ประกาศ ณ วันที่ ๒๑ ตุลาคม พ.ศ. ๒๕๖๗

(นายสมชวน รัตนมังคลานนท์)
อธิบดีกรมปศุสัตว์

แนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์
ของ
กรมปศุสัตว์

โดย
ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
กรมปศุสัตว์

สารบัญ

บทนำ

หลักการ

ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 ข้อ 5 ที่อาศัยอำนาจตามความในมาตรา 9 (4) แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 โดยกำหนดให้หน่วยงานของรัฐต้องดำเนินการตามนโยบายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์อันเป็นข้อกำหนดขั้นต่ำเพื่อลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่มีต่อการใช้บริการคลาวด์สาธารณะให้กับหน่วยงานของรัฐ รวมทั้งใช้เป็นแนวทางในการดำเนินงานอย่างปลอดภัย เชื่อถือได้ เป็นไปตามกฎหมาย และระเบียบที่เกี่ยวข้อง และสามารถปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ และเป็นไปในทิศทางเดียวกัน สอดคล้องกับมาตรฐานสากล และสนับสนุนการดำเนินงานของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

วัตถุประสงค์

เพื่อลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่มีต่อการใช้บริการคลาวด์สาธารณะให้กับกรมปศุสัตว์

ขอบเขตการใช้

ใช้ภายในหน่วยงานทั้งหมดภายใต้สังกัดกรมปศุสัตว์

คำนิยาม

คณะกรรมการ	หมายถึง	คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
กกม.	หมายถึง	คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์
หน่วยงาน	หมายถึง	หน่วยงานทั้งหมดภายใต้สังกัดกรมปศุสัตว์
บริการคลาวด์ (Cloud Service)	หมายถึง	ความสามารถ (Capability) ในการประมวลผลคลาวด์ ซึ่งถูกเรียกใช้โดยอินเทอร์เฟซที่กำหนดให้
ประเภทบริการคลาวด์ (Cloud Service Category)	หมายถึง	กลุ่มของบริการคลาวด์ ที่มีคุณสมบัติร่วมกันบางอย่าง โดยมีรูปแบบดังนี้ (1) การให้บริการโครงสร้างพื้นฐานหลัก (Infrastructure as a Service: IaaS) ประกอบด้วย ระบบประมวลผลข้อมูล ระบบการจัดเก็บข้อมูล ระบบเครือข่าย และทรัพยากรพื้นฐานอื่นๆ ที่เกี่ยวข้อง กับระบบประมวลผล ผู้ใช้บริการสามารถใช้งานซอฟต์แวร์บนโครงสร้างพื้นฐานและทรัพยากรที่ผู้ให้บริการจัดหาให้ได้อย่างมีประสิทธิภาพ โดยไม่ต้องบริหารจัดการโครงสร้างพื้นฐานที่จำเป็นด้วยตนเอง หรือ (2) การให้บริการแพลตฟอร์ม (Platform as a Service: PaaS) ประกอบด้วย ระบบโปรแกรม งานคอมพิวเตอร์ ระบบฐานข้อมูล และระบบจัดการหรืองานบริการจากคอมพิวเตอร์ ผู้ใช้บริการสามารถพัฒนาติดตั้ง และปรับแต่งซอฟต์แวร์ได้โดยไม่ต้องบริหารจัดการในส่วนที่เกี่ยวข้องกับโครงสร้างพื้นฐาน เครือข่ายระบบปฏิบัติการ และระบบจัดการฐานข้อมูล หรือ

(3) การให้...

(3) การให้บริการซอฟต์แวร์ (Software as a Service: SaaS) ผู้ให้บริการจัดเตรียมซอฟต์แวร์สำเร็จรูปแล้ว โดยผู้ใช้บริการสามารถกำหนดค่าความต้องการ พารามิเตอร์ ปริมาณหน่วยประมวลผลข้อมูลหน่วยเก็บข้อมูล และบริหารจัดการเพื่อให้ได้บริการตามวัตถุประสงค์ หรือ

(4) การให้บริการใดที่เป็นการรวมกันของสองบริการขึ้นไป จากข้อ (1) ถึง (3) หรือ

(5) การให้บริการอื่นที่สำนักงานประกาศกำหนด

คลาวด์สาธารณะ (Public Cloud)	หมายถึง	รูปแบบการใช้คลาวด์ที่บริการคลาวด์สามารถใช้ได้กับผู้ใช้บริการคลาวด์ใด ๆ และทรัพยากรถูกควบคุมโดยผู้ให้บริการคลาวด์
ผู้ใช้บริการคลาวด์ (Cloud Service Customer : CSC)	หมายถึง	หน่วยงานที่มีข้อตกลงทางสัญญาอย่างเป็นทางการในการใช้บริการคลาวด์ที่ให้บริการโดยผู้ให้บริการคลาวด์
ผู้ให้บริการคลาวด์ (Cloud Service Provider : CSP)	หมายถึง	หน่วยงานของรัฐหรือเอกชนที่ทำให้บริการคลาวด์สามารถใช้ได้กับผู้ใช้บริการคลาวด์ รวมถึงจัดการทรัพยากรเหล่านี้เพื่อให้มั่นใจว่ามีความพร้อมใช้งานความมั่นคงปลอดภัย และความสามารถในการขยายตัวสำหรับผู้ใช้บริการคลาวด์ของตน
ข้อมูลส่วนบุคคล	หมายถึง	ข้อมูลส่วนบุคคลตามที่กำหนดไว้ในมาตรา 6 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ความเสี่ยงจากการใช้บริการคลาวด์

กำหนดความเสี่ยงจากการใช้บริการระบบคลาวด์เป็น 2 ประเภท ได้แก่ ความเสี่ยงจาก ผู้ใช้บริการคลาวด์ (Cloud Service Customer : CSC) และความเสี่ยงจากผู้ให้บริการคลาวด์ (Cloud Service Provider : CSP)

ข้อกำหนดขั้นต่ำและการตรวจรับรองสำหรับผู้ใช้บริการคลาวด์

อ้างอิงตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566 และ ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567

ประเภทของข้อมูลหรือระบบสารสนเทศ	ข้อกำหนดขั้นต่ำ	การตรวจรับรองสำหรับผู้ใช้บริการคลาวด์
ผลกระทบระดับต่ำ	ข้อกำหนดส่วนที่ 1 - เฉพาะข้อ 1.1.1, 1.1.2 ข้อกำหนดส่วนที่ 2 - เฉพาะข้อ 1.2.1, 1.2.2, 1.2.3, 1.2.4, 1.2.8, 1.2.9	ประเมินตนเอง (Self-assessment) พร้อมแนบหลักฐาน และขออนุมัติไปยังผู้บริหารสูงสุดของหน่วยงาน โดยเก็บรักษาไว้ที่หน่วยงานและส่งให้สำนักงานด้วย
ผลกระทบระดับกลาง	ข้อกำหนดส่วนที่ 1 - ทุกข้อ ข้อกำหนดส่วนที่ 2 - เฉพาะข้อ 1.2.1, 1.2.2, 1.2.3, 1.2.4, 1.2.7, 1.2.8, 1.2.9, 1.2.10	ได้รับการรับรองโดยหน่วยงานควบคุมหรือกำกับดูแล(Attestation) หรือ ได้รับการรับรองโดยหน่วยงานให้บริการตรวจรับรอง (Certify Body) ตามวงรอบ 3 ปี ประกอบด้วย การตรวจรับรองในปีที่ 1 และการตรวจสำรวจในปีที่ 2 และ 3
ผลกระทบระดับสูง	ข้อกำหนดส่วนที่ 1 - ทุกข้อ ข้อกำหนดส่วนที่ 2 - ทุกข้อ	ได้รับการรับรองโดยหน่วยงานให้บริการตรวจรับรอง (Certify Body) ตามวงรอบ 3 ปี ประกอบด้วย การตรวจรับรองในปีที่ 1 และการตรวจสำรวจในปีที่ 2 และ 3

มาตรการ...

มาตรการการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์

1.1 การกำกับดูแลด้านความมั่นคงปลอดภัยระบบคลาวด์ (Cloud Security Governance)

1.1.1 นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Policies)

ก) ผู้ใช้บริการคลาวด์ต้องกำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศสำหรับการประมวลผลบนคลาวด์ให้เป็นนโยบายเฉพาะหัวข้อของผู้ใช้บริการคลาวด์นโยบายความมั่นคงปลอดภัยสารสนเทศสำหรับการประมวลผลบนคลาวด์ของผู้ใช้บริการคลาวด์ต้องสอดคล้องกับระดับความเสี่ยงที่ยอมรับได้ด้านความมั่นคงปลอดภัยสารสนเทศที่มีต่อข้อมูลและทรัพย์สินอื่นๆ ขององค์กร

ข) เมื่อกำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศสำหรับการประมวลผลบนคลาวด์ ผู้ใช้บริการคลาวด์ต้องคำนึงถึงสิ่งต่อไปนี้

- ข้อมูลที่จัดเก็บในสภาพแวดล้อมการประมวลผลบนคลาวด์อาจอยู่ภายใต้การเข้าถึงและการจัดการโดยผู้ให้บริการคลาวด์
- ทรัพย์สินขององค์กรอาจจะได้รับการดูแลรักษาในสภาพแวดล้อมการประมวลผลบนคลาวด์ เช่น โปรแกรมแอปพลิเคชัน
- กระบวนการต่าง ๆ สามารถทำงานบนบริการคลาวด์เสมือนจริงที่มีผู้ใช้หลายราย
- ผู้ใช้บริการคลาวด์และบริบทที่ใช้บริการคลาวด์
- ผู้ดูแลระบบบริการคลาวด์ของผู้ใช้บริการคลาวด์ที่ได้รับสิทธิพิเศษในการเข้าถึง
- ตำแหน่งทางภูมิศาสตร์ขององค์กรของผู้ให้บริการคลาวด์และประเทศที่ผู้ให้บริการคลาวด์สามารถจัดเก็บข้อมูลผู้ใช้บริการคลาวด์ได้ (แม้จะเป็นการชั่วคราว)

ค) นโยบายคุ้มครองข้อมูลส่วนบุคคลของผู้ใช้บริการคลาวด์ต้องระบุข้อความเกี่ยวกับข้อตกลงทางสัญญาระหว่างผู้ประมวลผลข้อมูลส่วนบุคคลบนคลาวด์และผู้ใช้บริการคลาวด์

ง) ข้อตกลงทางสัญญาต้องกำหนดความรับผิดชอบระหว่างผู้ประมวลผลข้อมูลส่วนบุคคลบนคลาวด์ผู้รับจ้างช่วง (Sub-contractors) และผู้ใช้บริการคลาวด์อย่างชัดเจน โดยพิจารณาจากประเภทของบริการคลาวด์ (เช่น บริการประเภท IaaS, PaaSหรือ SaaS) ตัวอย่างเช่น การกำหนดความรับผิดชอบในการควบคุมระดับแอปพลิเคชันอาจแตกต่างกันขึ้นอยู่กับว่าผู้ประมวลผลข้อมูลส่วนบุคคลบนคลาวด์นั้นให้บริการ SaaS หรือ PaaS หรือ IaaS

1.1.2 โครงสร้างองค์กรด้านความมั่นคงปลอดภัยสารสนเทศ (Organization of Information Security)

1.1.2.1 บทบาทและความรับผิดชอบด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security Roles and Responsibilities)

ก) ผู้ใช้บริการคลาวด์ต้องมีการตกลงกับผู้ให้บริการคลาวด์เกี่ยวกับการแบ่งบทบาทหน้าที่และความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศอย่างเหมาะสม และยืนยันว่าผู้ใช้บริการคลาวด์สามารถทำหน้าที่และความรับผิดชอบที่จัดสรรได้ต้องระบุบทบาทและความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศของทั้งสองฝ่ายไว้ในข้อตกลง

ข) ผู้ใช้บริการคลาวด์ต้องระบุและจัดการความสัมพันธ์กับส่วนงานที่เกี่ยวกับการสนับสนุนลูกค้าและฟังก์ชันการดูแลของผู้ให้บริการคลาวด์

1.1.3 การปฏิบัติ....

1.1.3 การปฏิบัติตามกฎ ระเบียบ ข้อบังคับ (Compliance)

1.1.3.1 การระบุกฎหมายที่บังคับใช้และข้อกำหนดตามสัญญา (Identification of Applicable Legislation and Contractual Requirements)

ก) ผู้ใช้บริการคลาวด์ต้องพิจารณาประเด็นที่ว่ากฎหมายและข้อบังคับที่เกี่ยวข้องอาจเป็นกฎหมายของเขตอำนาจศาลที่ควบคุมผู้ให้บริการคลาวด์นอกเหนือจากกฎหมายที่ควบคุมผู้ใช้บริการคลาวด์

ข) ผู้ใช้บริการคลาวด์ต้องขอหลักฐานว่าผู้ให้บริการคลาวด์ได้ปฏิบัติตามกฎระเบียบและมาตรฐานที่เกี่ยวข้องกับผู้ใช้บริการคลาวด์โดยหลักฐานดังกล่าวอาจเป็นการรับรองที่จัดทำโดยผู้ตรวจสอบภายนอก

1.1.3.2 สิทธิในทรัพย์สินทางปัญญา (Intellectual Property Rights)

ก) การติดตั้งซอฟต์แวร์ที่ได้รับอนุญาตในเชิงพาณิชย์ในบริการคลาวด์อาจทำให้เกิดการละเมิดเงื่อนไขการอนุญาตให้ใช้สิทธิสำหรับซอฟต์แวร์ได้ ผู้ใช้บริการคลาวด์ต้องมีขั้นตอนในการระบุข้อกำหนดในการให้สิทธิการใช้งานเฉพาะระบบคลาวด์ก่อนที่จะอนุญาตให้ติดตั้งซอฟต์แวร์ที่ได้รับอนุญาตในบริการคลาวด์ และต้องให้ความสนใจเป็นพิเศษกับกรณีที่บริการคลาวด์มีความยืดหยุ่นและสามารถปรับขนาดได้และสามารถใช้งานซอฟต์แวร์บนระบบหรือแกนประมวลผลได้มากกว่าที่อนุญาตโดยเงื่อนไขการอนุญาตให้ใช้สิทธิ

1.1.3.3 การปกป้องบันทึกข้อมูล (Protection of Records)

ก) ผู้ใช้บริการคลาวด์ต้องขอข้อมูลจากผู้ให้บริการคลาวด์เกี่ยวกับการปกป้องบันทึกข้อมูลที่รวบรวมและจัดเก็บโดยผู้ให้บริการคลาวด์ที่เกี่ยวข้องกับการใช้บริการคลาวด์ของผู้ใช้บริการคลาวด์

1.1.3.4 กฎระเบียบที่เกี่ยวกับมาตรการควบคุมการเข้ารหัสข้อมูล (Regulation of Cryptographic Controls)

ก) ผู้ใช้บริการคลาวด์ต้องตรวจสอบให้แน่ใจว่าชุดของมาตรการควบคุมการเข้ารหัสข้อมูลที่ใช้กับการใช้บริการคลาวด์สอดคล้องกับข้อตกลงกฎหมายและระเบียบข้อบังคับที่เกี่ยวข้อง

1.1.3.5 การทบทวนด้านการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างเป็นอิสระ (Independent Review of Information Security)

ก) ผู้ใช้บริการคลาวด์ต้องขอหลักฐานที่เป็นเอกสารว่ามีการนำมาตรการควบคุมและแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศสำหรับบริการคลาวด์ไปปฏิบัติและมีความสอดคล้องกับที่ผู้ให้บริการคลาวด์กล่าวอ้าง ทั้งนี้ หลักฐานดังกล่าวอาจรวมถึงการรับรองมาตรฐานที่เกี่ยวข้องด้วย

1.2 การปฏิบัติการและการรักษาความมั่นคงปลอดภัยโครงสร้างพื้นฐานระบบคลาวด์ (Cloud Infrastructure Security and Operation)

1.2.1 การบริหารทรัพยากรมนุษย์ (Human Resource Security)

1.2.1.1 การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศการศึกษาและการฝึกอบรม (Information Security Awareness, Education and Training)

ก) ผู้ใช้บริการคลาวด์ต้องเพิ่มรายการต่อไปนี้ในโปรแกรมสร้างความตระหนักรู้การศึกษาและการฝึกอบรมสำหรับผู้จัดการธุรกิจบริการคลาวด์ ผู้ดูแลระบบบริการคลาวด์ ผู้ประกอบบริการคลาวด์ และผู้ใช้บริการคลาวด์ รวมถึงพนักงานและผู้รับจ้างที่เกี่ยวข้อง

- มาตรฐานและขั้นตอนการใช้บริการคลาวด์
- ความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ ที่เกี่ยวข้องกับบริการคลาวด์และวิธีการจัดการความเสี่ยงเหล่านั้น

- ความเสี่ยงด้านสภาพแวดล้อมของระบบและเครือข่ายจากการใช้บริการคลาวด์
- การคุ้มครองข้อมูลส่วนบุคคล
- ข้อพิจารณาทางกฎหมายและข้อบังคับที่เกี่ยวข้อง

ข) ต้องจัดให้มีโปรแกรมการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศ การศึกษา และการฝึกอบรมเกี่ยวกับบริการคลาวด์แก่ผู้บริหารและผู้จัดการที่กำกับดูแล รวมถึงหน่วยงานธุรกิจ (Business Units)

1.2.2 การจัดการทรัพย์สิน (Asset Management)

1.2.2.1 ทะเบียนทรัพย์สิน (Inventory of Assets)

ก) ทะเบียนทรัพย์สินของผู้ใช้บริการคลาวด์ต้องคำนึงถึงข้อมูลและทรัพย์สินที่เกี่ยวข้องซึ่งจัดเก็บในสภาพแวดล้อมการประมวลผลบนคลาวด์ ทั้งนี้บันทึกทะเบียนทรัพย์สินต้องระบุสถานที่จัดเก็บทรัพย์สิน เช่น ชื่อของผู้ให้บริการคลาวด์

1.2.2.2 การบ่งชี้ข้อมูล (Labelling of Information)

ก) ผู้ใช้บริการคลาวด์ต้องบ่งชี้ข้อมูลและทรัพย์สินขององค์กรที่ใช้งานหรือเก็บรักษาไว้บนระบบคลาวด์ตามขั้นตอนปฏิบัติสำหรับการบ่งชี้ข้อมูลขององค์กร

1.2.3 การควบคุมการเข้าถึง (Access Control)

1.2.3.1 การควบคุมเข้าถึงเครือข่ายและบริการเครือข่าย (Access to Networks and Network Services)

ก) นโยบายการควบคุมการเข้าถึงของผู้ใช้บริการคลาวด์สำหรับการใช้บริการเครือข่ายต้องระบุข้อกำหนดสำหรับผู้ใช้งานในการเข้าถึงบริการคลาวด์ตามแต่ละบริการที่ใช้งาน

1.2.3.2 การลงทะเบียนและยกเลิกการลงทะเบียนสำหรับผู้ใช้(User Registration and Deregistration)

ก) ขั้นตอนการลงทะเบียนและยกเลิกการลงทะเบียนสำหรับผู้ใช้ต้องครอบคลุมถึงสถานการณ์ที่การควบคุมการเข้าถึงของผู้ใช้ถูกคุกคาม เช่น การที่รหัสผ่านหรือข้อมูลการลงทะเบียนผู้ใช้อื่น ๆ (ยกตัวอย่างเช่น จากการเปิดเผยโดยไม่ได้ตั้งใจ) ถูกทำให้เสียหายหรือถูกคุกคาม

1.2.3.3 การจัดการสิทธิการเข้าถึงที่ได้รับสิทธิพิเศษ (Management of Privileged Access Rights)

ก) ผู้ใช้บริการคลาวด์ต้องใช้เทคนิคการยืนยันตัวตนที่เพียงพอ (เช่น การยืนยันตัวตนแบบหลายปัจจัย) สำหรับการตรวจสอบสิทธิของผู้ดูแลระบบบริการคลาวด์ของผู้ใช้บริการคลาวด์ให้มีความสามารถในการจัดการบริการคลาวด์ที่สอดคล้องตามความเสี่ยงที่ระบุไว้

1.2.3.4 การจัดการข้อมูลการพิสูจน์ตัวตนที่เป็นความลับของผู้ใช้ (Management of Secret Authentication Information of Users)

ก) ผู้ใช้บริการคลาวด์ต้องตรวจสอบว่ากระบวนการจัดการของผู้ให้บริการคลาวด์สำหรับการจัดสรรข้อมูลการตรวจสอบความลับ (Secret Authentication Information) เช่น รหัสผ่านเป็นไปตามข้อกำหนดของผู้ใช้บริการคลาวด์

1.2.3.5 การจำกัดการเข้าถึงข้อมูล (Information Access Restriction)

ก) ผู้ใช้บริการคลาวด์ต้องตรวจสอบให้แน่ใจว่าสามารถจำกัดการเข้าถึงข้อมูลในบริการคลาวด์ได้ตามนโยบายการควบคุมการเข้าถึงและปฏิบัติตามข้อจำกัดดังกล่าว ซึ่งรวมถึงการจำกัดการเข้าถึงบริการต่าง ๆ บนระบบคลาวด์และข้อมูล ผู้ใช้บริการคลาวด์ที่เก็บไว้ในบริการ

1.2.3.6 การใช้...

1.2.3.6 การใช้โปรแกรมอรรถประโยชน์พิเศษ (Use of Privilege Utility Programs)

ก) หากอนุญาตให้ใช้โปรแกรมอรรถประโยชน์ได้ ผู้ใช้บริการคลาวด์ต้องระบุโปรแกรมอรรถประโยชน์ที่จะใช้ในสภาพแวดล้อมการประมวลผลบนคลาวด์และตรวจสอบให้มั่นใจว่าโปรแกรมเหล่านั้นไม่รบกวนการควบคุมของบริการคลาวด์

1.2.3.7 ขั้นตอนการเข้าสู่ระบบอย่างปลอดภัย (Secure Log-on Procedures)

ก) ผู้ใช้บริการคลาวด์ต้องกำหนดให้ผู้ใช้ที่อยู่ภายใต้การควบคุมของผู้ใช้บริการคลาวด์ปฏิบัติตามขั้นตอนการเข้าสู่ระบบอย่างปลอดภัยสำหรับบัญชีใด ๆ

1.2.4 การเข้ารหัส (Cryptography)

1.2.4.1 นโยบายเกี่ยวกับการใช้มาตรการควบคุมการเข้ารหัส (Policy on the Use of Cryptographic Controls)

ก) ผู้ใช้บริการคลาวด์ต้องใช้มาตรการควบคุมการเข้ารหัสสำหรับการใช้บริการระบบคลาวด์ที่มีความแข็งแรงเพียงพอและสอดคล้องตามความเสี่ยงที่ได้ระบุไว้ไม่ว่าผู้ใช้บริการคลาวด์หรือผู้ให้บริการคลาวด์จะเป็นผู้จัดหามาตรการควบคุมการเข้ารหัสเหล่านั้นก็ตาม

ข) เมื่อผู้ให้บริการคลาวด์นำเสนอการเข้ารหัสใดๆ ผู้ใช้บริการคลาวด์ต้องตรวจสอบข้อมูลที่ผู้ให้บริการคลาวด์จัดหาให้เพื่อยืนยันว่ามีความสามารถในการเข้ารหัสดังนี้หรือไม่

- ปฏิบัติตามข้อกำหนดด้านนโยบายของผู้ใช้บริการคลาวด์
- เข้ากันได้กับการป้องกันการเข้ารหัสลับอื่นๆ ที่ใช้โดยผู้ใช้บริการคลาวด์
- ใช้กับข้อมูลขณะจัดเก็บและระหว่างโอนถ่ายภายในบริการคลาวด์และนอกระบบคลาวด์

1.2.4.2 การจัดการกุญแจ (Key Management Use of Cryptographic Controls)

ก) ผู้ใช้บริการคลาวด์ต้องระบุกุญแจสำหรับการเข้ารหัสในแต่ละบริการคลาวด์และดำเนินการตามขั้นตอนสำหรับการจัดการกุญแจ

ข) ในกรณีที่บริการคลาวด์มีฟังก์ชันการจัดการกุญแจสำหรับการใช้งานโดยผู้ใช้บริการคลาวด์ ผู้ใช้บริการคลาวด์ต้องขอข้อมูลดังต่อไปนี้เกี่ยวกับขั้นตอนที่ใช้ในการจัดการกุญแจสำหรับการเข้ารหัสที่เกี่ยวข้องกับบริการคลาวด์

- ประเภทของกุญแจ
- ข้อกำหนดเฉพาะของระบบการจัดการ รวมถึงขั้นตอนต่าง ๆ ตลอดอายุการใช้งานของกุญแจเข้ารหัส เช่น การสร้าง เปลี่ยนแปลง หรือปรับปรุงจัดเก็บ หมดอายุการใช้งาน เรียกคืน เก็บรักษาและทำลาย
- ขั้นตอนการจัดการกุญแจที่แนะนำสำหรับการใช้งานโดยผู้ใช้บริการคลาวด์

ค) ผู้ใช้บริการคลาวด์ต้องไม่อนุญาตให้ผู้ให้บริการคลาวด์จัดเก็บและจัดการกุญแจสำหรับการเข้ารหัสเมื่อผู้ใช้บริการคลาวด์ใช้กุญแจเข้ารหัสของตนเอง

1.2.5 การรักษาความปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environment Security)

1.2.5.1 ตำแหน่งของศูนย์ข้อมูล (Data Center Location)

ก) ต้องใช้ศูนย์ข้อมูลหลักในประเทศไทย (Data Localization)

1.2.5.2 การกำจัดหรือนำอุปกรณ์กลับมาใช้ใหม่อย่างปลอดภัย (Secure Disposal or Reuse of Equipment)

ก) ผู้ใช้บริการคลาวด์ต้องร้องขอการยืนยันว่าผู้ให้บริการคลาวด์มีนโยบายและขั้นตอนในการกำจัดหรือนำทรัพยากรกลับมาใช้ใหม่อย่างปลอดภัย

1.2.6 การรักษาความมั่นคงปลอดภัยการปฏิบัติการ (Operations Security)

1.2.6.1 การจัดการการเปลี่ยนแปลง (Change Management)

ก) กระบวนการจัดการการเปลี่ยนแปลงของผู้ใช้บริการคลาวด์ต้องคำนึงถึงผลกระทบของการเปลี่ยนแปลงใด ๆ ที่เกิดขึ้นจากผู้ให้บริการคลาวด์

1.2.6.2 การบริหารจัดการความจุ (Capacity Management)

ก) ผู้ใช้บริการคลาวด์ต้องตรวจสอบให้แน่ใจว่าขีดความสามารถของทรัพยากรที่ตกลงกันไว้ในบริการคลาวด์นั้นตรงตามข้อกำหนดของ ผู้ใช้บริการคลาวด์

ข) ผู้ใช้บริการคลาวด์ต้องตรวจสอบการใช้บริการคลาวด์และคาดการณ์ความต้องการด้านขีดความสามารถของทรัพยากรของบริการคลาวด์ เพื่อให้มั่นใจในประสิทธิภาพของบริการคลาวด์เมื่อเวลาผ่านไป

1.2.6.3 การสำรองข้อมูล (Information Backup)

ก) ในกรณีที่ผู้ให้บริการคลาวด์ มีความสามารถในการสำรองข้อมูลซึ่งเป็นส่วนหนึ่งของบริการคลาวด์ ผู้ใช้บริการคลาวด์ต้องขอข้อมูลจำเพาะของความสามารถในการสำรองข้อมูลจากผู้ให้บริการคลาวด์ นอกจากนี้ ผู้ใช้บริการคลาวด์ต้องทำการตรวจสอบเพื่อให้แน่ใจว่าเป็นไปตามข้อกำหนดในการสำรองข้อมูลหรือไม่

ข) ผู้ใช้บริการคลาวด์มีหน้าที่รับผิดชอบในการดำเนินการสำรองข้อมูลเมื่อผู้ให้บริการคลาวด์ไม่ได้ให้บริการนี้

1.2.6.4 การบันทึกเหตุการณ์ (Event Logging)

ก) ผู้ใช้บริการคลาวด์ต้องจัดทำข้อกำหนดสำหรับการบันทึกเหตุการณ์และตรวจสอบว่าบริการคลาวด์ตรงตามข้อกำหนดเหล่านั้นหรือไม่

1.2.6.5 การปกป้องข้อมูลในบันทึกเหตุการณ์ (Protection of Log information)

ก) ข้อมูลที่บันทึกไว้ในบันทึกเหตุการณ์เพื่อวัตถุประสงค์ต่าง ๆ เช่น การตรวจสอบความปลอดภัยและการวินิจฉัยการทำงานอาจมีข้อมูลส่วนบุคคลอยู่ด้วยจึงต้องมีมาตรการ เช่น การควบคุมการเข้าถึง เพื่อให้มั่นใจว่าข้อมูลที่บันทึกไว้ในบันทึกเหตุการณ์จะถูกนำไปใช้ตามวัตถุประสงค์ที่ตั้งไว้เท่านั้น

ข) ต้องมีขั้นตอนการดำเนินการซึ่งดีที่สุดคือเป็นระบบอัตโนมัติเพื่อให้มั่นใจว่าข้อมูลที่บันทึกไว้ในบันทึกเหตุการณ์จะถูกลบภายในระยะเวลาที่กำหนด (Log Retention) และเอกสารระบุไว้

1.2.6.7 บันทึกเหตุการณ์ของผู้ดูแลระบบและผู้ปฏิบัติงาน (Administrator and Operator Logs)

ก) หากมีการให้สิทธิพิเศษให้แก่ผู้ใช้บริการคลาวด์การใช้สิทธิพิเศษนั้นต้องมีการบันทึกเหตุการณ์และประสิทธิภาพของการดำเนินการเหล่านั้น ผู้ใช้บริการคลาวด์ต้องพิจารณาว่าความสามารถในการบันทึกเหตุการณ์ที่ผู้ให้บริการคลาวด์จัดหาให้นั้นเหมาะสมหรือไม่ หรือผู้ใช้บริการคลาวด์ต้องใช้ความสามารถในการบันทึกเหตุการณ์เพิ่มเติมหรือไม่

1.2.6.8 การซิงโครไนซ์นาฬิกา (Clock Synchronization)

ก) ผู้ใช้บริการคลาวด์ต้องขอข้อมูลเกี่ยวกับการซิงโครไนซ์นาฬิกาที่ใช้ในระบบของผู้ให้บริการคลาวด์

1.2.6.9 การจัดการช่องโหว่ทางเทคนิค (Management of Technical Vulnerabilities)

ก) ผู้ใช้บริการคลาวด์ต้องขอข้อมูลจากผู้ให้บริการคลาวด์เกี่ยวกับการจัดการช่องโหว่ทางเทคนิคที่อาจส่งผลกระทบต่อบริการคลาวด์ที่ให้บริการผู้ใช้บริการคลาวด์ต้องระบุช่องโหว่ทางเทคนิคที่ผู้ใช้บริการคลาวด์จะเป็นผู้รับผิดชอบในการจัดการและกำหนดกระบวนการในการจัดการให้ชัดเจน

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

ก) ในกรณีที่ไม่สามารถหลีกเลี่ยงการใช้ข้อมูลส่วนบุคคลสำหรับวัตถุประสงค์ในการทดสอบได้ ต้องมีการประเมินความเสี่ยงมาตรการด้านเทคนิคและการจัดการองค์กรต้องถูกนำมาใช้เพื่อลดความเสี่ยงที่ระบุไว้ให้น้อยที่สุด

1.2.7 การรักษาความมั่นคงปลอดภัยเครือข่าย (Communication Security)

1.2.7.1 นโยบายและขั้นตอนปฏิบัติในการถ่ายโอนข้อมูล (Information Transfer Policies and Procedures)

ก) เมื่อใดก็ตามที่มีการใช้สื่อทางกายภาพสำหรับการถ่ายโอนข้อมูลต้องมีระบบที่จะบันทึกสื่อทางกายภาพที่เข้ามาและออกไปซึ่งมีข้อมูลส่วนบุคคลรวมถึงประเภทของสื่อทางกายภาพผู้ส่ง/ผู้รับที่ได้รับอนุญาต วันที่และเวลาและจำนวนสื่อทางกายภาพ

ข) ผู้ใช้บริการคลาวด์ต้องขอให้ผู้ให้บริการคลาวด์ใช้มาตรการเพิ่มเติม (เช่น การเข้ารหัส) เพื่อให้มั่นใจว่าข้อมูลสามารถเข้าถึงได้เฉพาะจุดปลายทางเท่านั้นไม่ใช่ระหว่างทาง

1.2.7.2 การแบ่งแยกในเครือข่าย (Segregation in Networks)

ก) ผู้ใช้บริการคลาวด์ต้องจัดทำข้อกำหนดสำหรับการแยกเครือข่ายเพื่อให้เกิดการแยกผู้เช่า (Tenant) ในสภาพแวดล้อมที่เป็นการใช้บริการคลาวด์ร่วมกันและตรวจสอบว่าผู้ให้บริการคลาวด์มีคุณสมบัติตรงตามข้อกำหนดเหล่านั้นหรือไม่

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

1.2.8.1 การวิเคราะห์และข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Requirements Analysis and Specification)

ก) ผู้ใช้บริการคลาวด์ต้องกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศสำหรับการใช้บริการคลาวด์จากนั้นประเมินว่าบริการของผู้ให้บริการคลาวด์สามารถตอบสนองความต้องการเหล่านี้ได้หรือไม่

ข) สำหรับการประเมินนี้ผู้ใช้บริการคลาวด์ต้องขอข้อมูลเกี่ยวกับความสามารถในการรักษาความมั่นคงปลอดภัยสารสนเทศจาก ผู้ให้บริการคลาวด์

1.2.8.2 นโยบายการพัฒนาที่ปลอดภัย (Secure Development Policy)

ก) ผู้ใช้บริการคลาวด์ต้องขอข้อมูลจากผู้ให้บริการคลาวด์เกี่ยวกับการใช้ขั้นตอนและวิธีปฏิบัติในการพัฒนาที่ปลอดภัยของผู้ให้บริการคลาวด์

1.2.9 การจัดการผู้ให้บริการภายนอก (Supplier Relationships)

1.2.9.1 นโยบายความมั่นคงปลอดภัยสารสนเทศสำหรับความสัมพันธ์กับผู้ให้บริการภายนอก (Information Security Policy for Supplier Relationships)

ก) ผู้ใช้บริการคลาวด์ต้องระบุว่าผู้ให้บริการคลาวด์เป็นผู้ให้บริการภายนอกประเภทหนึ่งในนโยบายความมั่นคงปลอดภัยสารสนเทศสำหรับความสัมพันธ์กับผู้ให้บริการภายนอกซึ่งจะช่วยลดความเสี่ยงที่เกี่ยวข้องกับการเข้าถึงและจัดการข้อมูลผู้ใช้บริการคลาวด์ของผู้ให้บริการคลาวด์

1.2.9.2 การจัดการ...

1.2.9.2 การจัดการกับการรักษาความมั่นคงปลอดภัยภายในข้อตกลงของผู้ให้บริการภายนอก (Addressing Security within Supplier Agreements)

ก) ผู้ใช้บริการคลาวด์ต้องยืนยันบทบาทและความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับบริการคลาวด์ดังที่อธิบายไว้ในข้อตกลงการให้บริการสิ่งเหล่านี้อาจรวมถึงกระบวนการต่อไปนี้

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

1.2.10 การจัดการเหตุภัยคุกคามทางสารสนเทศ (Information Security Incident Management)

1.2.10.1 ความรับผิดชอบและขั้นตอน (Responsibilities and Procedures)

ก) ผู้ใช้บริการคลาวด์ต้องตรวจสอบการจัดสรรความรับผิดชอบสำหรับการจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศและต้องตรวจสอบให้แน่ใจว่าเป็นไปตามข้อกำหนดของผู้ใช้บริการคลาวด์

ข) เหตุภัยคุกคามทางสารสนเทศต้องนำไปสู่การทบทวนโดยผู้ใช้บริการคลาวด์หรือทบทวนร่วมกันระหว่างผู้ให้บริการคลาวด์และผู้ใช้บริการคลาวด์ในฐานะที่เป็นส่วนหนึ่งของกระบวนการจัดการเหตุภัยคุกคามทางสารสนเทศของตนเพื่อพิจารณาว่าได้มีการละเมิดข้อมูลที่เกี่ยวข้องกับข้อมูลส่วนบุคคลเกิดขึ้นหรือไม่

1.2.10.2 การรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Reporting Information Security Events)

ก) ผู้ใช้บริการคลาวด์ต้องขอข้อมูลจากผู้ให้บริการคลาวด์เกี่ยวกับกลไกสำหรับ

- ผู้ใช้บริการคลาวด์รายงานเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศที่ตรวจพบต่อผู้ให้บริการคลาวด์
- ผู้ให้บริการคลาวด์เพื่อรับรายงานเกี่ยวกับเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศที่ตรวจพบโดยผู้ให้บริการคลาวด์
- ผู้ใช้บริการคลาวด์เพื่อติดตามสถานะของเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศที่รายงาน