เอกสารเผยแพร่

Cloud Shared Responsibility

บริการ GDCC

(Government Data Center and Cloud Service)

เอกสารแสดงบทบาทหน้าที่ความรับผิดชอบ

ระหว่าง ผู้ให้บริการคลาวด์ (Cloud Service Provider) และ

ผู้ใช้บริการคลาวด์ (Cloud Service Customer)

บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)

Version 1.0

สารบัญ

บริการ GDCC

(Government Data Center and Cloud Service)

เอกสารแสดงบทบาทหน้าที่ความรับผิดชอบ

ระหว่าง ผู้ให้บริการคลาวด์ (Cloud Service Provider) และ

ผู้ใช้บริการคลาวด์ (Cloud Service Customer)

1. หลักการและเหตุผล

ปัจจุบันการนำเทคโนโลยีคลาวด์คอมพิวติ้งมาใช้ในการให้บริการระบบสารสนเทศของหน่วยงานภาครัฐ มีบทบาทสำคัญในการเพิ่มประสิทธิภาพ ความยืดหยุ่น และความคุ้มค่าในการบริหารจัดการทรัพยากรด้านเทคโนโลยีสารสนเทศ โดยเฉพาะการใช้บริการคลาวด์ภาครัฐ (Government Data Center and Cloud Service: GDCC) ครอบคลุมแพลตฟอร์ม (Platform) ดังนี้

VMWare Platform เป็นโครงสร้างพื้นฐานที่รองรับการให้บริการระบบสารสนเทศที่มีความสำคัญต่อภารกิจของหน่วยงาน

OpenStack Platform เป็นโครงสร้างพื้นฐานแบบคลาวด์โอเพนซอร์สที่รองรับการให้บริการระบบสารสนเทศที่มีความสำคัญต่อภารกิจของหน่วยงาน และสามารถปรับขยายทรัพยากรได้ตามความต้องการใช้งานอย่างเหมาะสม

อย่างไรก็ตาม การใช้บริการคลาวด์ก่อให้เกิดรูปแบบการแบ่งปันความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศระหว่างผู้ให้บริการคลาวด์ (Cloud Service Provider: CSP) และผู้ใช้บริการคลาวด์ (Cloud Service Customer: CSC) ซึ่งหากไม่มีการกำหนดขอบเขตหน้าที่และความรับผิดชอบที่ชัดเจน อาจก่อให้เกิดความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ ความไม่สอดคล้องกับกฎหมาย ระเบียบ และมาตรฐานที่เกี่ยวข้อง รวมถึงความไม่ชัดเจนในการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศในสภาพแวดล้อมคลาวด์

มาตรฐานสากล **ISO/IEC 27017** ได้กำหนดแนวปฏิบัติด้านการควบคุมความมั่นคงปลอดภัยสารสนเทศสำหรับบริการคลาวด์ โดยเน้นหลักการแบ่งแยกหน้าที่และความรับผิดชอบระหว่าง CSP และ CSC อย่างเหมาะสม ครอบคลุมด้านการบริหารจัดการโครงสร้างพื้นฐานคลาวด์ การควบคุมการเข้าถึงระบบและทรัพยากร การปกป้องข้อมูลสารสนเทศ ความต่อเนื่องในการให้บริการ และการจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ

ดังนั้น เพื่อให้การใช้บริการ **GDCC** เป็นไปอย่างมั่นคงปลอดภัย มีความชัดเจนในการกำกับดูแล และสอดคล้องกับมาตรฐาน ISO/IEC 27017 รวมถึงกฎหมาย ระเบียบ และนโยบายด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้อง จึงมีความจำเป็นต้องจัดทำเอกสารกำหนดหน้าที่และความรับผิดชอบของผู้ให้บริการคลาวด์ (CSP) และผู้ใช้บริการคลาวด์ (CSC) ขึ้น เพื่อใช้เป็นกรอบอ้างอิงในการดำเนินงาน การกำกับดูแล การตรวจประเมิน และการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศอย่างเป็นระบบและมีประสิทธิภาพ

2. คำจำกัดความ

องค์กร คือ บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)

บริการคลาวด์ (Cloud Service) คือ บริการด้านเทคโนโลยีสารสนเทศที่ให้ผู้ใช้สามารถเข้าถึงและใช้ทรัพยากรคอมพิวเตอร์ เช่น ระบบประมวลผล ระบบจัดเก็บข้อมูล เครือข่าย และซอฟต์แวร์ ผ่านโครงข่าย โดยมีความยืดหยุ่นในการปรับขนาดและบริหารจัดการทรัพยากรตามความต้องการ

ผู้ให้บริการคลาวด์ (Cloud Service Provider: CSP) คือ หน่วยงานหรือองค์กรที่ให้บริการคลาวด์แก่ผู้ใช้บริการ โดยรับผิดชอบในการจัดหา บริหารจัดการ และดูแลโครงสร้างพื้นฐานคลาวด์ รวมถึงมาตรการด้านความมั่นคงปลอดภัยสารสนเทศของ GDCC ตามขอบเขตที่กำหนดไว้ โดยมีที่ตั้งทางภูมิศาสตร์ (Geographic location) สำหรับการให้บริการอยู่ที่กรุงเทพมหานครฯ และจังหวัดนนทบุรี ประเทศไทย ดังนั้นการเก็บรวบรวม ใช้ เปิดเผย ประมวลผล รวมถึงการสำรองข้อมูล/ข้อมูลส่วนบุคคลจะเกิดขึ้นภายในราชอาณาจักรไทยเท่านั้น เว้นแต่จะได้รับความยินยอมเป็นอย่างอื่นจากผู้ควบคุมข้อมูลส่วนบุคคลเป็นลายลักษณ์อักษร หรือในสัญญาหลักได้ระบุไว้อย่างชัดเจนแล้วว่าการเก็บรวบรวม ใช้ เปิดเผย ประมวลผลรวมถึงการสำรอง/ข้อมูลส่วนบุคคลเกิดขึ้นในต่างประเทศ

ผู้ใช้บริการคลาวด์ (Cloud Service Customer: CSC) คือ หน่วยงานภาครัฐหรือองค์กรที่ใช้บริการคลาวด์จากผู้ให้บริการคลาวด์ เพื่อประมวลผล จัดเก็บ หรือให้บริการระบบสารสนเทศของตนเอง และมีหน้าที่รับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศในส่วนที่ตนควบคุมได้

แบบจำลองความรับผิดชอบร่วม (Shared Responsibility Model) คือ หลักการแบ่งแยกหน้าที่และความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศระหว่างผู้ให้บริการคลาวด์และผู้ใช้บริการคลาวด์ โดยแต่ละฝ่ายมีความรับผิดชอบในขอบเขตที่แตกต่างกันตามลักษณะของบริการคลาวด์และข้อตกลงที่กำหนดไว้

ความมั่นคงปลอดภัยสารสนเทศ (Information Security) คือ การปกป้องสารสนเทศและระบบสารสนเทศให้มีความมั่นคงปลอดภัยตามหลักการรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งาน (Availability) รวมถึงการป้องกันการเข้าถึง การใช้ การเปิดเผย การแก้ไข หรือการทำลายโดยไม่ได้รับอนุญาต

3. ความรับผิดชอบร่วมของบริการคลาวด์ (Cloud Shared Responsibility)

การใช้บริการคลาวด์ เป็นรูปแบบการให้บริการที่มีการแบ่งปันบทบาท หน้าที่ และความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคลระหว่างผู้ให้บริการคลาวด์ (Cloud Service Provider: CSP) และผู้ใช้บริการคลาวด์ (Cloud Service Customer: CSC) เพื่อให้การใช้งานคลาวด์เป็นไปอย่างมั่นคงปลอดภัย โปร่งใส และสอดคล้องกับมาตรฐานสากล ISO/IEC 27017 และ ISO/IEC 27018 ทั้งสองฝ่ายจึงต้องร่วมกันดำเนินการและประสานความรับผิดชอบในประเด็นสำคัญดังต่อไปนี้

บริการ GDCC (Government Data Center and Cloud Service)

CSP (Cloud Service Provider)	CSC (Cloud Service Customer)
นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Policies) ผู้ให้บริการคลาวด์มีการกำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศสำหรับการประมวลผลบนคลาวด์ให้เป็นนโยบายเฉพาะหัวข้อของผู้ให้บริการคลาวด์ นโยบายความมั่นคงปลอดภัยสารสนเทศสำหรับการประมวลผลบนคลาวด์ของผู้ให้บริการคลาวด์ ต้องสอดคล้องกับระดับความเสี่ยงที่ยอมรับได้ด้านความมั่นคงปลอดภัยสารสนเทศ ที่มีต่อข้อมูลและทรัพย์สินอื่น ๆ ขององค์กร นโยบายคุ้มครองข้อมูลส่วนบุคคลของผู้ให้บริการคลาวด์มีการระบุข้อความเกี่ยวกับข้อตกลงทางสัญญาระหว่างผู้ประมวลผลข้อมูลส่วนบุคคลบนคลาวด์และผู้ใช้บริการคลาวด์	**นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Policies)** ผู้ใช้บริการคลาวด์มีหน้าที่กำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศสำหรับการประมวลผลบนคลาวด์ให้เป็นนโยบายเฉพาะหัวข้อของ ผู้ใช้บริการคลาวด์ นโยบายความมั่นคงปลอดภัยสารสนเทศสำหรับการประมวลผลบนคลาวด์ ของผู้ใช้บริการคลาวด์ ต้องสอดคล้องกับระดับความเสี่ยงที่ยอมรับได้ด้านความมั่นคงปลอดภัยสารสนเทศ ที่มีต่อข้อมูลและทรัพย์สินอื่น ๆ ขององค์กร นโยบายคุ้มครองข้อมูลส่วนบุคคลของผู้ใช้บริการคลาวด์ต้องระบุข้อความเกี่ยวกับข้อตกลงทางสัญญา ระหว่างผู้ประมวลผลข้อมูลส่วนบุคคลบนคลาวด์และผู้ใช้บริการคลาวด์

บริการ GDCC (Government Data Center and Cloud Service)

CSP (Cloud Service Provider)	CSC (Cloud Service Customer)
โครงสร้างองค์กรด้านความมั่นคงปลอดภัยสารสนเทศ (Organization of Information Security) ผู้ให้บริการคลาวด์มีข้อตกลงและบันทึกการแบ่งบทบาทหน้าที่และความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศอย่างเหมาะสมกับ ผู้ใช้บริการคลาวด์, ผู้ให้บริการคลาวด์ และผู้ให้บริการภายนอก ผู้ให้บริการคลาวด์มีการแต่งตั้งผู้ประสานงานด้านการคุ้มครองข้อมูลส่วนบุคคล เพื่อประสานงานกับผู้ใช้บริการคลาวด์ ผู้ให้บริการคลาวด์มีการแจ้งให้ผู้ใช้บริการคลาวด์ทราบถึงที่ตั้งทางภูมิศาสตร์ขององค์กรที่เป็นเจ้าของผู้ให้บริการคลาวด์ และประเทศที่ผู้ให้บริการคลาวด์สามารถจัดเก็บข้อมูล ผู้ใช้บริการคลาวด์ได้ **โดยมีที่ตั้งทางภูมิศาสตร์ (Geographic location) สำหรับการให้บริการอยู่ที่กรุงเทพมหานครฯ และจังหวัดนนทบุรี ประเทศไทย ดังนั้นการเก็บรวบรวม ใช้ เปิดเผย ประมวลผล รวมถึงการสำรองข้อมูล/ข้อมูลส่วนบุคคลจะเกิดขึ้นภายในราชอาณาจักรไทยเท่านั้น เว้นแต่จะได้รับความยินยอมเป็นอย่างอื่นจากผู้ควบคุมข้อมูลส่วนบุคคลเป็นลายลักษณ์อักษร หรือในสัญญาหลักได้ระบุไว้อย่างชัดเจนแล้วว่าการเก็บรวบรวม ใช้ เปิดเผย ประมวลผลรวมถึงการสำรอง/ข้อมูลส่วนบุคคลเกิดขึ้นในต่างประเทศ**	**โครงสร้างองค์กรด้านความมั่นคงปลอดภัยสารสนเทศ (Organization of Information Security)** ผู้ใช้บริการคลาวด์มีหน้าที่ทำข้อตกลงกับผู้ให้บริการคลาวด์เกี่ยวกับการแบ่งบทบาทหน้าที่และความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศอย่างเหมาะสม และยืนยันว่าผู้ใช้บริการคลาวด์ สามารถทำหน้าที่และความรับผิดชอบที่จัดสรรได้ ต้องระบุบทบาทและความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศของทั้งสองฝ่ายไว้ในข้อตกลง ผู้ใช้บริการคลาวด์มีหน้าที่ระบุและจัดการความสัมพันธ์กับส่วนงานที่เกี่ยวกับการสนับสนุนลูกค้าและฟังก์ชันการดูแลของผู้ให้บริการคลาวด์ และมีหน้าที่ระบุหน่วยงานที่เกี่ยวข้องกับการดำเนินการร่วมกันระหว่างผู้ใช้บริการคลาวด์และผู้ให้บริการคลาวด์ ผู้ใช้บริการคลาวด์มีหน้าที่ระบุหน่วยงานที่เกี่ยวข้องกับการดำเนินการร่วมกันระหว่างผู้ใช้บริการคลาวด์และผู้ให้บริการคลาวด์

บริการ GDCC (Government Data Center and Cloud Service)

CSP (Cloud Service Provider)	CSC (Cloud Service Customer)
การบริหารทรัพยากรมนุษย์ (Human Resource Security) ผู้ให้บริการคลาวด์ มีหน้าที่สร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศ และด้านการคุ้มครองข้อมูลส่วนบุคคล การศึกษาและการฝึกอบรมแก่พนักงาน รวมทั้งให้ผู้รับจ้างดำเนินการเช่นเดียวกันเกี่ยวกับการจัดการข้อมูลของผู้ใช้บริการคลาวด์ และข้อมูลที่ได้จากบริการคลาวด์อย่างเหมาะสม โดยข้อมูลนี้อาจมีข้อมูลที่เป็นความลับต่อผู้ใช้บริการคลาวด์หรืออยู่ภายใต้ข้อจำกัดเฉพาะ รวมถึงข้อจำกัดด้านกฎระเบียบในการเข้าถึงและใช้งานโดย ผู้ให้บริการคลาวด์	**การบริหารทรัพยากรมนุษย์ (Human Resource Security)** ผู้ใช้บริการคลาวด์ มีหน้าที่เพิ่มรายการต่อไปนี้ในโปรแกรมสร้างความตระหนักรู้ การศึกษา และการฝึกอบรมสำหรับผู้จัดการธุรกิจบริการคลาวด์ ผู้ดูแลระบบบริการคลาวด์ ผู้ประกอบบริการคลาวด์ และผู้ใช้บริการคลาวด์ รวมถึงพนักงานและผู้รับจ้างที่เกี่ยวข้อง ผู้ใช้บริการคลาวด์ มีหน้าที่จัดให้มีโปรแกรมการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศ การศึกษา และการฝึกอบรมเกี่ยวกับบริการคลาวด์แก่ผู้บริหารและผู้จัดการที่กำกับดูแล รวมถึงหน่วยงานธุรกิจ (Business Units)
การจัดการทรัพย์สิน (Asset Management) • ผู้ให้บริการคลาวด์มีหน้าที่จัดทำบัญชีทรัพย์สินของ infrastructure (servers, storage, network devices, Openstack components) • กำหนดเจ้าของและผู้รับผิดชอบสำหรับทรัพย์สินระดับ infrastructure และ platform services • จัดประเภทและระดับความสำคัญของทรัพย์สิน infrastructure พร้อมกำหนดมาตรการรักษาความปลอดภัยที่เหมาะสม • สอบทาน ติดตามและอัพเดท inventory และสถานะการใช้งานของทรัพยากร hardware/software ในระบบ GDCC ให้เป็นปัจจุบัน • ดูแลรักษาและกำจัดทรัพย์สิน infrastructure อย่างปลอดภัยเมื่อหมดอายุการใช้งาน	**การจัดการทรัพย์สิน (Asset Management)** • ผู้ใช้บริการคลาวด์มีหน้าที่จัดทำบัญชีทรัพย์สินของตนเอง (VMs, volumes, images, snapshots, networks, floating IPs, applications) • กำหนดเจ้าของและผู้รับผิดชอบสำหรับทรัพย์สินแต่ละรายการพร้อมระบุระดับความสำคัญของข้อมูล • จัดหมวดหมู่ทรัพย์สินและข้อมูลตามระดับความลับ เช่น public, internal, confidential, secret เป็นต้น • ทบทวนและลบทรัพย์สินที่ไม่ใช้งาน (unused VMs, old snapshots, orphaned volumes) อย่างสม่ำเสมอ • ลบข้อมูลและทรัพย์สินอย่างปลอดภัยเมื่อไม่ใช้งานหรือสิ้นสุดการใช้บริการคลาวด์ (secure deletion)

บริการ GDCC (Government Data Center and Cloud Service)

CSP (Cloud Service Provider)	CSC (Cloud Service Customer)
การควบคุมการเข้าถึงข้อมูลและระบบ (Access Control) กำหนดและบังคับใช้นโยบายการควบคุมสิทธิ์การเข้าถึงข้อมูลและระบบที่เกี่ยวข้องกับการให้บริการคลาวด์ โดยจำกัดการเข้าถึงเฉพาะผู้ที่มีหน้าที่ความรับผิดชอบ และมีการบันทึกและตรวจสอบการเข้าถึงอย่างเหมาะสม เพื่อจัดการการเข้าถึงบริการคลาวด์โดยผู้ใช้งานของผู้ใช้บริการคลาวด์ ผู้ให้บริการคลาวด์มีหน้าที่จัดเตรียมฟังก์ชันการลงทะเบียนและการยกเลิกการลงทะเบียนผู้ใช้งาน รวมถึงข้อกำหนดสำหรับการใช้งานฟังก์ชันเหล่านี้แก่ ผู้ใช้บริการคลาวด์ ผู้ให้บริการคลาวด์มีหน้าที่ให้ข้อมูลเกี่ยวกับขั้นตอนการจัดการข้อมูลการตรวจสอบความลับ (Secret Authentication Information) ของผู้ใช้บริการคลาวด์ รวมถึงขั้นตอนในการจัดสรรข้อมูลดังกล่าวสำหรับการตรวจสอบสิทธิผู้ใช้งาน ผู้ให้บริการคลาวด์มีหน้าที่จัดให้มีขั้นตอนการเข้าสู่ระบบอย่างปลอดภัยสำหรับบัญชีใด ๆ ที่ผู้ใช้บริการคลาวด์ร้องขอสำหรับผู้ใช้ที่อยู่ภายใต้การควบคุมของผู้ใช้บริการคลาวด์	**การควบคุมสิทธิ์การเข้าถึงของผู้ใช้งาน (Access Control)** กำหนด บริหาร และทบทวนสิทธิ์การเข้าถึงข้อมูลและระบบของผู้ใช้งานภายในองค์กรให้เหมาะสมกับหน้าที่ความรับผิดชอบ พร้อมทั้งป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต นโยบายการควบคุมการเข้าถึงของผู้ใช้บริการคลาวด์สำหรับการใช้บริการเครือข่ายต้องระบุข้อกำหนดสำหรับผู้ใช้งานในการเข้าถึงบริการคลาวด์ตามแต่ละบริการที่ใช้งาน ผู้ใช้บริการคลาวด์มีหน้าที่ใช้เทคนิคการยืนยันตัวตนที่เพียงพอ (เช่น การยืนยันตัวตนแบบหลายปัจจัย) สำหรับการตรวจสอบสิทธิของผู้ดูแลระบบบริการคลาวด์ของ ผู้ใช้บริการคลาวด์ ให้มีความสามารถในการจัดการบริการคลาวด์ที่สอดคล้องตามความเสี่ยงที่ระบุไว้ **โดยเมื่อได้รับรหัสผ่านในครั้งแรก ผู้ใช้งานต้องเปลี่ยนรหัสผ่านใหม่ทันที และต้องเก็บรักษาบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ให้เป็นความลับ**

บริการ GDCC (Government Data Center and Cloud Service)

CSP (Cloud Service Provider)	CSC (Cloud Service Customer)
กฎระเบียบที่เกี่ยวกับมาตรการควบคุมการเข้ารหัสข้อมูล (Cryptographic Controls) ผู้ให้บริการคลาวด์มีหน้าที่ให้คำอธิบายกับ ผู้ใช้บริการคลาวด์เกี่ยวกับมาตรการควบคุมการเข้ารหัสข้อมูลที่ดำเนินการโดยผู้ให้บริการคลาวด์ เพื่อใช้ในการทบทวนการปฏิบัติตามข้อตกลง กฎหมาย และ ข้อบังคับที่เกี่ยวข้อง ผู้ให้บริการคลาวด์มีหน้าที่ให้ข้อมูลแก่ผู้ใช้บริการคลาวด์เกี่ยวกับการเข้ารหัสเพื่อปกป้องข้อมูลและข้อมูลส่วนบุคคล ที่ผู้ให้บริการคลาวด์ประมวลผลนอกจากนี้ ผู้ให้บริการคลาวด์ต้องให้ข้อมูลแก่ผู้ใช้บริการคลาวด์เกี่ยวกับความสามารถใด ๆ ที่ผู้ให้บริการคลาวด์มอบให้ซึ่งสามารถช่วยผู้ใช้บริการคลาวด์ในการใช้การเข้ารหัสดังกล่าว โดยมีการจัดทำแนวทางการเข้ารหัส (Cryptographic) สำหรับผู้ใช้บริการคลาวด์เพื่อนำไปพิจารณาเป็นทางเลือกในการประยุกต์ใช้	**กฎระเบียบที่เกี่ยวกับมาตรการควบคุมการเข้ารหัสข้อมูล (Cryptographic Controls)** ผู้ใช้บริการคลาวด์มีหน้าที่ตรวจสอบให้แน่ใจว่าชุดของมาตรการควบคุมการเข้ารหัสข้อมูลที่ใช้กับการใช้บริการคลาวด์สอดคล้องกับข้อตกลง กฎหมาย และระเบียบข้อบังคับที่เกี่ยวข้อง ผู้ใช้บริการคลาวด์มีหน้าที่ใช้มาตรการควบคุมการเข้ารหัสสำหรับการใช้บริการระบบคลาวด์ที่มีความแข็งแรงเพียงพอ และสอดคล้องตามความเสี่ยงที่ได้ระบุไว้ ไม่ว่าผู้ใช้บริการคลาวด์หรือผู้ให้บริการคลาวด์จะเป็นผู้จัดหามาตรการควบคุมการเข้ารหัสเหล่านั้นก็ตาม
ความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environmental Security) ผู้ให้บริการคลาวด์มีหน้าที่รักษาความปลอดภัยทางกายภาพของ data centers (physical security perimeter, access control, surveillance) ควบคุมการเข้าออกพื้นที่ data centers ด้วยระบบยืนยันตัวตน และบันทึก access logs จัดให้มีระบบสนับสนุนที่จำเป็น (ไฟฟ้าสำรอง, ระบบปรับอากาศ, ระบบดับเพลิง, ระบบตรวจจับควัน) ป้องกันภัยคุกคามทางกายภาพ (fire, flood, earthquake, unauthorized access, theft) รวมถึงการบำรุงรักษาอุปกรณ์และสิ่งอำนวยความสะดวกให้พร้อมใช้งานและตรวจสอบเป็นประจำ	**ความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)** ผู้ใช้บริการคลาวด์มีหน้าที่รักษาความปลอดภัยทางกายภาพของอุปกรณ์ที่ใช้เข้าถึงระบบ GDCC (workstations, laptops, mobile devices) ควบคุมการเข้าถึงอุปกรณ์และสถานที่ทำงานที่มีข้อมูลหรือ credentials สำหรับเข้าถึง GDCC ป้องกันไม่ให้อุปกรณ์ที่ใช้เข้าถึงระบบสูญหายหรือถูกขโมย และรายงานทันทีหากเกิดเหตุ ล็อคหน้าจออุปกรณ์เมื่อไม่ใช้งาน และไม่ทิ้ง credentials หรือข้อมูลสำคัญไว้บนโต๊ะทำงาน (clear desk policy) รวมถึงการทำลายสื่อบันทึกข้อมูล (hard drives, USB, documents) ที่มีข้อมูลสำคัญอย่างปลอดภัยเมื่อไม่ใช้งาน

บริการ GDCC (Government Data Center and Cloud Service)

CSP (Cloud Service Provider)	CSC (Cloud Service Customer)
การรักษาความมั่นคงปลอดภัยในการดำเนินงาน (Operations Security) • ผู้ให้บริการคลาวด์จัดทำและปฏิบัติตามขั้นตอนการดำเนินงานที่มีเอกสารชัดเจนสำหรับ infrastructure และ platform services • ทำการบันทึก event logs ของบริการ GDCC ครอบคลุมโครงสร้างพื้นฐานในการให้บริการ (GDCC Infrastructure) **โดยกำหนดช่องทางการติดต่อสำหรับ CSC ขอข้อมูล event logs ผ่านช่องทางดังนี้** **GDCC Contact Center 02-024-1999** กด 0 ติดต่อ Helpdesk (วัน-เวลาทำการ) กด 1 ติดต่อ Technical Support (ตลอด 24 ชั่วโมง) กด 2 ติดต่อ Migration Support (วัน-เวลาทำการ) กด 3 ติดต่อ Training (วัน-เวลาทำการ) กด 4 ติดต่อ Application Support (วัน-เวลาทำการ) **GDCC Email Address** ศูนย์บริการข้อมูล GDCC: Helpdesk@gdcc.go.th บริการสนับสนุนทางเทคนิค: Support@gdcc.go.th บริการสนับสนุนการย้ายข้อมูล: Migration@gdcc.go.th บริการอบรม: Training@gdcc.go.th บริการสนับสนุนแอปพลิเคชัน: Support_app@gdcc.go.th • ตรวจสอบและแก้ไขช่องโหว่ (vulnerabilities) ของ infrastructure, hypervisors และ platform services อย่างสม่ำเสมอ • สำรองข้อมูล infrastructure configurations, databases และ platform services เป็นประจำ • ควบคุมการติดตั้งและเปลี่ยนแปลง software ในระบบ infrastructure ผ่านกระบวนการ change management	**การรักษาความมั่นคงปลอดภัยในการดำเนินงาน (Operations Security)** • ผู้ใช้บริการคลาวด์มีหน้าที่จัดทำและปฏิบัติตามขั้นตอนการดำเนินงานสำหรับระบบและ applications ของตนเอง • เปิดใช้งานและตรวจสอบ logs ภายใน VMs และ applications เป็นประจำ พร้อมเก็บสำรองข้อมูล logs สำคัญ • ตรวจสอบและแก้ไขช่องโหว่ของ OS, applications และ software ภายใน VMs ด้วยการติดตั้ง security patches • สำรองข้อมูลทั้งหมดภายใน VMs, volumes และ applications ตามนโยบายที่กำหนด พร้อมทดสอบการกู้คืน • ควบคุมการติดตั้ง software และการเปลี่ยนแปลงระบบภายใน VMs ผ่านกระบวนการ change management • ติดตั้งและกำหนดค่า security software (antivirus, host-based firewall, monitoring agents) ภายใน VMs • วางแผนและจัดการ capacity ของทรัพยากรที่ใช้งาน (VMs, storage, network) เพื่อป้องกันการใช้งานเกินโควต้า • แยกสภาพแวดล้อม development, testing และ production ด้วยการสร้าง VMs/networks แยกหรือใช้ projects แยกกัน • ลบข้อมูลและทรัพย์สินที่ไม่ใช้งานอย่างปลอดภัย (secure deletion) รวมถึง VMs, volumes, snapshots ที่ล้าสมัย

บริการ GDCC (Government Data Center and Cloud Service)

CSP (Cloud Service Provider)	CSC (Cloud Service Customer)
• ตรวจสอบและป้องกันการโจมตีทาง network ด้วย firewalls, IDS/IPS ในระดับ infrastructure • จัดการ capacity planning และ monitoring เพื่อให้มั่นใจว่าระบบมีทรัพยากรเพียงพอ • แยกสภาพแวดล้อม development, testing และ production ในระดับ infrastructure	

บริการ GDCC (Government Data Center and Cloud Service)

CSP (Cloud Service Provider)	CSC (Cloud Service Customer)
การคุ้มครองข้อมูลของผู้ใช้บริการ (Privacy Protection) จัดให้มีมาตรการป้องกันการเข้าถึง การใช้ การเปิดเผย การแก้ไข หรือการทำลายข้อมูลของผู้ใช้บริการโดยไม่ได้รับอนุญาต รวมถึงต้องไม่เข้าถึงข้อมูลของผู้ใช้บริการ เว้นแต่เป็นไปตามขอบเขตที่กฎหมายหรือสัญญาอนุญาต	**การจำแนกและคุ้มครองข้อมูล (Data Classification)** กำหนดระดับความสำคัญและความลับของข้อมูลที่ใช้บริการคลาวด์ และกำหนดมาตรการคุ้มครองข้อมูลให้เหมาะสมกับระดับความเสี่ยง รวมถึงการควบคุมการเข้าถึงและการใช้งานข้อมูล
ผู้ให้บริการคลาวด์มีหน้าที่ให้ข้อมูลแก่ผู้ใช้บริการคลาวด์เกี่ยวกับการปกป้องบันทึกข้อมูลที่รวบรวมและจัดเก็บโดยผู้ให้บริการคลาวด์ที่เกี่ยวข้องกับการใช้บริการคลาวด์ของผู้ใช้บริการคลาวด์	นโยบายคุ้มครองข้อมูลส่วนบุคคลของผู้ใช้บริการคลาวด์มีการระบุข้อความเกี่ยวกับข้อตกลงทางสัญญา ระหว่างผู้ประมวลผลข้อมูลส่วนบุคคลบนคลาวด์และผู้ใช้บริการคลาวด์
การรักษาความมั่นคงปลอดภัยของโครงสร้างพื้นฐานที่รองรับข้อมูล (Infrastructure Security) ผู้ให้บริการคลาวด์มีหน้าที่ดูแลความมั่นคงปลอดภัยของศูนย์ข้อมูล ระบบเครือข่าย ระบบจัดเก็บข้อมูล และแพลตฟอร์มเวอร์ชวลไลเซชัน เพื่อป้องกันความเสี่ยงที่อาจส่งผลกระทบต่อข้อมูลของผู้ใช้บริการ	**การตั้งค่าความมั่นคงปลอดภัยของระบบและแอปพลิเคชัน (Application Security)** ผู้ใช้บริการคลาวด์มีหน้าที่ดำเนินการตั้งค่ามาตรการด้านความมั่นคงปลอดภัย เช่น การกำหนดค่าความปลอดภัยของระบบปฏิบัติการ แอปพลิเคชัน เครือข่าย และการป้องกันมัลแวร์ รวมถึงการอัปเดต Patch และการจัดการช่องโหว่

บริการ GDCC (Government Data Center and Cloud Service)

CSP (Cloud Service Provider)	CSC (Cloud Service Customer)
การบันทึกเหตุการณ์ (Event Logging) จัดให้มีมาตรการเก็บบันทึกกิจกรรมที่เกิดขึ้นในระบบคลาวด์ เพื่อใช้ในการตรวจสอบ วิเคราะห์ และติดตามเหตุการณ์ด้านความมั่นคงปลอดภัย ภายใต้ความรับผิดชอบของผู้ให้บริการคลาวด์ (CSP) ดังนี้ 1. **การบันทึกและจัดเก็บ Log** • บันทึกเหตุการณ์ที่สำคัญในระบบคลาวด์อย่างต่อเนื่อง • จัดเก็บข้อมูล log อย่างปลอดภัยและครบถ้วน • รักษาความสมบูรณ์ของข้อมูล log ไม่ให้ถูกแก้ไขหรือลบโดยไม่ได้รับอนุญาต 2. **การจัดเตรียม Log ตามคำขอ โดยกำหนดช่องทางรับคำขอข้อมูล log ผ่านช่องทางดังนี้** **GDCC Contact Center 02-024-1999** กด 0 ติดต่อ Helpdesk (วัน-เวลาทำการ) กด 1 ติดต่อ Technical Support (ตลอด 24 ชั่วโมง) กด 2 ติดต่อ Migration Support (วัน-เวลาทำการ) กด 3 ติดต่อ Training (วัน-เวลาทำการ) กด 4 ติดต่อ Application Support (วัน-เวลาทำการ) **GDCC Email Address** ศูนย์บริการข้อมูล GDCC: Helpdesk@gdcc.go.th บริการสนับสนุนทางเทคนิค: Support@gdcc.go.th บริการสนับสนุนการย้ายข้อมูล: Migration@gdcc.go.th บริการอบรม: Training@gdcc.go.th บริการสนับสนุนแอปพลิเคชัน: Support_app@gdcc.go.th 3. **จัดเตรียมและส่งมอบข้อมูล log ตามที่ร้องขอภายในระยะเวลาที่กำหนด** 4. **แจ้งสถานะการดำเนินการให้ CSC ทราบ** 5. **การรักษาความปลอดภัย** • เข้ารหัสข้อมูล log ทั้งขณะจัดเก็บและขณะส่งมอบ • ตรวจสอบสิทธิ์การเข้าถึงก่อนให้บริการข้อมูล log	**การบันทึกเหตุการณ์ (Event Logging)** จัดให้มีมาตรการเก็บบันทึกกิจกรรมที่เกิดขึ้นในระบบคลาวด์ เพื่อใช้ในการตรวจสอบ วิเคราะห์ และติดตามเหตุการณ์ด้านความมั่นคงปลอดภัย ภายใต้ความรับผิดชอบของผู้ใช้บริการคลาวด์ (CSC) ดังนี้ 1. ผู้ใช้บริการคลาวด์ สามารถดำเนินการขอ Log ย้อนหลังผ่านขั้นตอนการร้องขอ ดังนี้ • ส่งคำขอผ่านอีเมล ไปยังผู้ให้บริการคลาวด์ (CSP) ตามช่องทางที่กำหนด • ระบุรายละเอียดในอีเมล: o ช่วงเวลาที่ต้องการข้อมูล log (วันที่เริ่มต้น - วันที่สิ้นสุด) o ประเภทของ log ที่ต้องการ (เช่น access log, security log, system log) o เหตุผลในการขอข้อมูล o ข้อมูลติดต่อกลับ • **รอรับการตอบกลับ** จากผู้ให้บริการคลาวด์ (CSP) 2. การจัดเก็บและรักษาความปลอดภัย • จัดเก็บข้อมูล log ที่ได้รับอย่างปลอดภัย • กำหนดสิทธิ์การเข้าถึงข้อมูล log อย่างเหมาะสม • ลบข้อมูล log อย่างปลอดภัยเมื่อหลังพ้นระยะเวลาเก็บรักษาตามนโยบาย **หมายเหตุ: เฉพาะบริการ GDCC บน Openstack Platform** • ผู้ใช้บริการสามารถเข้าถึงและตรวจสอบ Log ผ่าน Self-Service Portal • จัดให้มี self-service portal สำหรับให้ CSC เข้าถึงและดาวน์โหลดข้อมูล log ด้วยตนเอง • ข้อมูล log ที่แสดงใน portal: **ข้อมูลย้อนหลังไม่เกิน 30 วัน ในกรณีที่ต้องการ ข้อมูล log ย้อนหลังเกิน 30 วัน ผู้ใช้บริการสามารถส่งการจัดเตรียม Log ตามคำขอตามช่องทางรับคำขอข้อมูล log ที่ผู้ให้บริการกำหนดไว้**

บริการ GDCC (Government Data Center and Cloud Service)

CSP (Cloud Service Provider)	CSC (Cloud Service Customer)
การสำรองข้อมูล (Information Backup) จัดให้มีมาตรการคัดลอกและจัดเก็บข้อมูลสำคัญไว้ในที่แยกต่างหาก เพื่อให้สามารถกู้คืนข้อมูลได้เมื่อเกิดเหตุการณ์ไม่คาดคิด เช่น ข้อมูลสูญหาย ระบบขัดข้อง หรือถูกโจมตี กำหนดความรับผิดชอบของผู้ให้บริการคลาวด์ (CSP) ดังนี้ • สำรองข้อมูลโครงสร้างพื้นฐานและแพลตฟอร์ม ของบริการ GDCC (infrastructure และ platform services) • สำรองข้อมูล configuration ของ control plane, databases, และ services • จัดเก็บข้อมูลสำรองอย่างปลอดภัยในสถานที่แยกต่างหาก พร้อมเข้ารหัส • จัดทำและทดสอบแผนการกู้คืนระบบในกรณีเกิดภัยพิบัติ • รับรอง RTO และ RPO ของระบบตามที่กำหนดใน SLA	**การสำรองข้อมูล (Information Backup)** 1. การสำรองข้อมูลของตนเอง (Application & Data Layer) สิ่งที่ CSC ต้องสำรองเอง • สำรองข้อมูลทั้งหมดภายใน VMs, volumes, databases และ applications ของตนเอง • กำหนดนโยบายการสำรองข้อมูล (ความถี่, ระยะเวลาเก็บรักษา, RPO/RTO) • เลือกใช้วิธีการสำรองข้อมูลที่เหมาะสม (snapshots, volume backups, application-level backups) • จัดเก็บข้อมูลสำรองอย่างปลอดภัย เข้ารหัสข้อมูลที่อ่อนไหว และควรเก็บสำเนาไว้นอกระบบ GDCC • ทดสอบกระบวนการกู้คืนข้อมูลเป็นประจำและจัดทำเอกสารขั้นตอนการกู้คืน
การจัดการช่องโหว่ด้านเทคนิค (Management of Technical Vulnerabilities) • ตรวจสอบและแก้ไขช่องโหว่ของโครงสร้างพื้นฐานและแพลตฟอร์ม ของบริการ GDCC เช่น infrastructure, hypervisors, และ platform services • ติดตั้ง security patches และ updates สำหรับระบบโครงสร้างพื้นฐานอย่างสม่ำเสมอ • ติดตามประกาศช่องโหว่ (vulnerability advisories) จากผู้ผลิตและชุมชน OpenStack • ทดสอบ patches ก่อนนำไปใช้งานจริง และแจ้งกำหนดการ maintenance ให้ CSC ทราบล่วงหน้า • จัดทำรายงานสถานะการแก้ไขช่องโหว่และแจ้ง CSC เมื่อมีช่องโหว่ที่มีผลกระทบสูง (critical vulnerabilities)	**การจัดการช่องโหว่ด้านเทคนิค (Management of Technical Vulnerabilities)** • ตรวจสอบและแก้ไขช่องโหว่ของ operating systems, applications และ software ภายใน Tenant/VMs ของตนเอง • ติดตั้ง security patches และ updates สำหรับ OS และ applications เป็นประจำ • ใช้เครื่องมือ vulnerability scanning เพื่อตรวจสอบช่องโหว่ในระบบของตนเอง • กำหนดนโยบายการจัดการ patches และระยะเวลาในการแก้ไขช่องโหว่ตามระดับความรุนแรง • ประสานงานกับ CSP เมื่อพบช่องโหว่ที่อาจเกี่ยวข้องกับ infrastructure layer

บริการ GDCC (Government Data Center and Cloud Service)

CSP (Cloud Service Provider)	CSC (Cloud Service Customer)
สิทธิในทรัพย์สินทางปัญญา (Intellectual Property Rights) • จัดหา licenses ที่ถูกต้องตามกฎหมายสำหรับ software ที่ใช้ใน infrastructure และ platform services • จัดให้มี Windows Server licenses แบบเช่าใช้ (License Mobility) สำหรับ CSC ที่ต้องการใช้งาน • ดูแลให้การใช้ licenses เป็นไปตามข้อตกลงกับผู้ให้สิทธิ์ (license compliance) • คืน licenses เมื่อ CSC ยกเลิกการใช้บริการหรือสิ้นสุดสัญญา • แจ้งข้อมูลและเงื่อนไขการใช้ licenses ให้ CSC ทราบอย่างชัดเจน	**สิทธิในทรัพย์สินทางปัญญา (Intellectual Property Rights)** • ใช้ software licenses ที่ CSP จัดหาให้ตามวัตถุประสงค์และเงื่อนไขที่กำหนดเท่านั้น • จัดหา licenses เองสำหรับ software/applications ที่ติดตั้งเพิ่มเติมภายใน Tenant/VMs (เช่น database, antivirus, applications อื่น ๆ) • ตรวจสอบให้แน่ใจว่า software ที่นำมาใช้งานมี licenses ที่ถูกต้องและไม่ละเมิดลิขสิทธิ์ • ยอมรับว่า licenses ที่เช่าจาก CSP จะสิ้นสุดเมื่อยกเลิกบริการหรือครบกำหนดสัญญา • ส่งคืน licenses และลบ software ที่ได้รับจาก CSP เมื่อสิ้นสุดการใช้บริการ
การจัดการสิทธิ์การเข้าถึงระดับสูง (Management of Privileged Access Rights) • จัดการและควบคุมสิทธิ์ privileged access สำหรับโครงสร้างพื้นฐานและแพลตฟอร์ม ของบริการ GDCC (infrastructure and platform services) • กำหนดนโยบายการใช้งาน admin accounts และ privileged roles ของระบบ GDCC • ทบทวนและตรวจสอบสิทธิ์การเข้าถึงระดับสูงเป็นประจำ รวมถึงยกเลิกสิทธิ์ที่ไม่จำเป็น • บันทึก log การใช้งาน privileged accounts และตรวจสอบกิจกรรมที่ผิดปกติ • จำกัดจำนวนบุคลากรที่มีสิทธิ์ระดับสูงและใช้หลัก least privilege	**การจัดการสิทธิ์การเข้าถึงระดับสูง (Management of Privileged Access Rights)** • จัดการ privileged accounts ภายใน Tenant/VMs และ applications ของตนเอง (เช่น root, administrator) • กำหนดนโยบายการใช้งาน admin/root accounts และจำกัดจำนวนผู้ที่มีสิทธิ์ระดับสูง • ตรวจสอบและทบทวนสิทธิ์การเข้าถึงระดับสูงเป็นประจำ ยกเลิกสิทธิ์เมื่อไม่จำเป็นหรือเมื่อบุคลากรลาออก • เปิดใช้งาน audit logging สำหรับการใช้ privileged accounts และตรวจสอบ log เป็นประจำ • ใช้หลัก separation of duties และ least privilege ในการมอบสิทธิ์ภายในระบบ

บริการ GDCC (Government Data Center and Cloud Service)

CSP (Cloud Service Provider)	CSC (Cloud Service Customer)
การจัดการข้อมูลลับสำหรับการยืนยันตัวตน (Management of Secret Authentication Information of Users) • กำหนดนโยบายความปลอดภัยของ passwords สำหรับ OpenStack accounts (ความยาว, ความซับซ้อน, อายุการใช้งาน) • เข้ารหัสและจัดเก็บ passwords/credentials ของระบบอย่างปลอดภัย (hashing with salt) • ไม่เปิดเผย passwords ของผู้ใช้งานในรูปแบบ plain text และไม่ส่งผ่านช่องทางที่ไม่ปลอดภัย • จัดให้มีกลไก password reset ที่ปลอดภัยและตรวจสอบตัวตนได้ • สนับสนุนการใช้งาน multi-factor authentication (MFA) สำหรับการเข้าถึงระบบ GDCC	**การจัดการข้อมูลลับสำหรับการยืนยันตัวตน (Management of Secret Authentication Information of Users)** • กำหนดและบังคับใช้นโยบาย password policy ภายใน VMs และ applications ของตนเอง • เก็บรักษา passwords, API keys, certificates และข้อมูลลับอื่น ๆ อย่างปลอดภัย ไม่ฝังไว้ใน code หรือ configuration files • เปลี่ยน default passwords ทันทีหลังติดตั้งระบบและเปลี่ยน passwords เป็นประจำตามนโยบาย • ใช้เครื่องมือจัดการ passwords (password manager) หรือ secrets management tools สำหรับเก็บข้อมูลลับ • ไม่แชร์ passwords/credentials และเปลี่ยนทันทีเมื่อบุคลากรที่รู้ข้อมูลลับลาออกหรือมีการเปลี่ยนแปลงโยกย้ายตำแหน่ง
การแยกข้อมูลและสภาพแวดล้อมของผู้ใช้บริการ (Data and Tenant Isolation) ผู้ให้บริการคลาวด์มีหน้าที่จัดให้มีการแยกข้อมูลและทรัพยากรของผู้ใช้บริการแต่ละรายอย่างชัดเจนในระดับโครงสร้างพื้นฐานและแพลตฟอร์ม เพื่อป้องกันการเข้าถึงข้อมูลข้ามกันโดยไม่ได้รับอนุญาต ผู้ให้บริการคลาวด์มีหน้าที่ให้ข้อมูลแก่ผู้ใช้บริการคลาวด์เกี่ยวกับการปกป้องบันทึกข้อมูลที่รวบรวมและจัดเก็บโดยผู้ให้บริการคลาวด์ที่เกี่ยวข้องกับการใช้บริการคลาวด์ของผู้ใช้บริการคลาวด์	**การบริหารจัดการข้อมูลภายในระบบของตน (Data Management)** ผู้ใช้บริการคลาวด์รับผิดชอบต่อข้อมูล ระบบปฏิบัติการ แอปพลิเคชัน และการตั้งค่าภายในสภาพแวดล้อมคลาวด์ที่อยู่ภายใต้การควบคุมของตน รวมถึงการสำรองข้อมูลและการกู้คืนข้อมูลตามความจำเป็น ผู้ใช้บริการคลาวด์สามารถขอข้อมูลจากผู้ให้บริการคลาวด์เกี่ยวกับการปกป้องบันทึกข้อมูลที่รวบรวมและจัดเก็บโดยผู้ให้บริการคลาวด์ที่เกี่ยวข้องกับการใช้บริการคลาวด์ของผู้ใช้บริการคลาวด์

บริการ GDCC (Government Data Center and Cloud Service)

CSP (Cloud Service Provider)	CSC (Cloud Service Customer)
ความมั่นคงปลอดภัยในการสื่อสาร (Communications Security) • ผู้ให้บริการคลาวด์มีหน้าที่จัดการและรักษาความปลอดภัยของ network infrastructure (switches, routers, firewalls, load balancers) แบ่งแยก network segments และควบคุมการเข้าถึงระหว่าง networks ต่าง ๆ ในระดับ infrastructure • ผู้ให้บริการคลาวด์มีการเข้ารหัสการสื่อสารระหว่าง OpenStack components และ management interfaces (APIs, dashboards) • ผู้ให้บริการคลาวด์มีการป้องกันการโจมตีทาง network ในระดับ infrastructure ด้วย DDoS protection, IDS/IPS และจัดให้มี VPN หรือ secure channels สำหรับการเชื่อมต่อเข้าสู่ GDCC management network รวมถึงการตรวจสอบและบันทึก network traffic logs ในระดับ infrastructure • ผู้ให้บริการคลาวด์รักษาความพร้อมใช้งานและความเร็วของ network connectivity ตาม SLA • ผู้ให้บริการคลาวด์จัดให้มี network isolation สำหรับ tenant networks (project networks) ของแต่ละ CSC	**ความมั่นคงปลอดภัยในการสื่อสาร (Communications Security)** • ผู้ใช้บริการคลาวด์มีหน้าที่กำหนดค่า security groups และ network ACLs เพื่อควบคุมการเข้าถึง VMs และ applications และมีการเข้ารหัสข้อมูลที่ส่งผ่าน network โดยใช้ SSL/TLS, VPN หรือโปรโตคอลที่ปลอดภัยสำหรับ applications ปิด ports และ services ที่ไม่จำเป็นภายใน VMs เพื่อลดพื้นที่โจมตี (attack surface) • ผู้ใช้บริการคลาวด์มีหน้าที่แบ่งแยก network zones ภายใน project (เช่น frontend, backend, database networks) ตามความเหมาะสม • ผู้ใช้บริการคลาวด์มีการติดตั้งและกำหนดค่า host-based firewalls ภายใน VMs เพื่อควบคุมการสื่อสารขาเข้าและขาออกตรวจสอบ network traffic และ connection logs ภายใน VMs เพื่อตรวจจับกิจกรรมผิดปกติ เข้ารหัสข้อมูลสำคัญก่อนส่งผ่าน network และเก็บรักษา encryption keys อย่างปลอดภัย • ผู้ใช้บริการคลาวด์ไม่ส่ง credentials, API keys หรือข้อมูลลับผ่านช่องทางที่ไม่ปลอดภัย (plain text email, HTTP)

บริการ GDCC (Government Data Center and Cloud Service)

CSP (Cloud Service Provider)	CSC (Cloud Service Customer)
การจัดหา พัฒนา และบำรุงรักษาระบบ (System Acquisition, Development and Maintenance) • ผู้ให้บริการคลาวด์มีหน้าที่กำหนดและบังคับใช้ข้อกำหนดด้านความมั่นคงปลอดภัยในการจัดหาและพัฒนาระบบโครงสร้างพื้นฐานและแพลตฟอร์ม ของบริการ GDCC • ทดสอบความมั่นคงปลอดภัยของระบบ infrastructure ก่อนนำไปใช้งานจริงและหลังมีการเปลี่ยนแปลงสำคัญ • แยกสภาพแวดล้อม development, testing และ production ในระดับ infrastructure อย่างชัดเจน • ควบคุมการเปลี่ยนแปลงระบบ infrastructure ผ่านกระบวนการ change management ที่เป็นทางการ • ป้องกันข้อมูลทดสอบรั่วไหล โดยไม่ใช้ข้อมูลจริงของ CSC ในสภาพแวดล้อม development/testing • ตรวจสอบและป้องกันช่องโหว่ที่เกิดจาก technical vulnerabilities ใน infrastructure และ platform services • จัดทำเอกสารประกอบระบบ (system documentation) และ security guidelines สำหรับ CSC • ทบทวนและปรับปรุง security baselines สำหรับ infrastructure เป็นประจำ	**การจัดหา พัฒนา และบำรุงรักษาระบบ (System Acquisition, Development and Maintenance)** • ผู้ใช้บริการคลาวด์มีหน้าที่กำหนดข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับ applications และระบบที่พัฒนาหรือจัดหาบน GDCC • ทดสอบความมั่นคงปลอดภัยของ applications (security testing, vulnerability assessment, penetration testing) ก่อนนำไปใช้งานจริง • แยกสภาพแวดล้อม development, testing และ production โดยใช้ Tenant/VMs, networks หรือ projects แยกกัน • ควบคุมการเปลี่ยนแปลงระบบและ applications ผ่านกระบวนการ change management เพื่อป้องกันผลกระทบต่อ production • ไม่ใช้ข้อมูลจริงหรือข้อมูลส่วนบุคคลในสภาพแวดล้อม development/testing หรือทำ data masking ก่อนนำไปใช้ • พัฒนา applications ตามหลัก secure coding practices และตรวจสอบช่องโหว่ (code review, static analysis) • จัดการ dependencies และ third-party libraries อย่างปลอดภัย ตรวจสอบช่องโหว่และอัพเดทเป็นประจำ • จัดทำเอกสารประกอบระบบและคู่มือการใช้งานสำหรับ applications และระบบที่พัฒนา • ปฏิบัติตาม security guidelines และ best practices ที่ CSP จัดทำไว้เมื่อพัฒนาหรือติดตั้งระบบบน GDCC

บริการ GDCC (Government Data Center and Cloud Service)

CSP (Cloud Service Provider)	CSC (Cloud Service Customer)
การจัดการผู้ให้บริการภายนอก (Supplier Relationships) ผู้ให้บริการคลาวด์ มีการระบุมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้อง ซึ่งผู้ให้บริการคลาวด์ จะนำมาใช้เป็นส่วนหนึ่งของข้อตกลงระหว่างผู้ให้บริการคลาวด์และผู้ให้บริการภายนอก ผู้ให้บริการคลาวด์ มีการกำหนดวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศแก่ผู้ให้บริการภายนอก และขอให้ผู้ให้บริการภายนอกแต่ละรายดำเนินกิจกรรมการบริหารความเสี่ยงเพื่อให้บรรลุวัตถุประสงค์ กำกับดูแลให้ผู้ให้บริการปฏิบัติตามข้อตกลงด้านความมั่นคงปลอดภัยและข้อกำหนดในสัญญา (SLA) จัดการความต่อเนื่องของบริการในกรณีที่ผู้ให้บริการหยุดให้บริการหรือเกิดปัญหา ผู้ให้บริการคลาวด์ ควบคุมการเข้าถึงระบบและข้อมูลของผู้ให้บริการภายนอกที่ต้องเข้ามาบำรุงรักษา infrastructure รักษาความลับของข้อมูล CSC และไม่เปิดเผยให้ผู้ให้บริการภายนอกโดยไม่ได้รับอนุญาต	**การจัดการผู้ให้บริการภายนอก (Supplier Relationships)** ผู้ใช้บริการคลาวด์ สามารถระบุได้ว่า ผู้ให้บริการคลาวด์ เป็นผู้ให้บริการภายนอกประเภทหนึ่งในนโยบายความมั่นคงปลอดภัยสารสนเทศสำหรับความสัมพันธ์กับผู้ให้บริการภายนอก ซึ่งจะช่วยลดความเสี่ยงที่เกี่ยวข้องกับการเข้าถึงและจัดการข้อมูลผู้ใช้บริการคลาวด์ ของ ผู้ให้บริการคลาวด์ ผู้ใช้บริการคลาวด์ สามารถยืนยันบทบาทและความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับบริการคลาวด์ ควบคุมและจำกัดสิทธิ์การเข้าถึงของผู้ให้บริการภายนอกให้เท่าที่จำเป็น ตามหลัก least privilege ตรวจสอบและทบทวนการปฏิบัติงานของผู้ให้บริการเป็นประจำ เพื่อให้มั่นใจว่าปฏิบัติตามข้อตกลง ยกเลิกหรือระงับสิทธิ์การเข้าถึงของผู้ให้บริการทันทีเมื่อสิ้นสุดสัญญาหรือไม่จำเป็นต้องใช้งานอีกต่อไป ผู้ใช้บริการคลาวด์ จัดทำแผนสำรองในกรณีที่ผู้ให้บริการหยุดให้บริการหรือเกิดปัญหา เพื่อความต่อเนื่องของธุรกิจของผู้ใช้บริการคลาวด์เอง

บริการ GDCC (Government Data Center and Cloud Service)

CSP (Cloud Service Provider)	CSC (Cloud Service Customer)
การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูล (Incident Management) ผู้ให้บริการคลาวด์ มีการกำหนดกลไกสำหรับรายงานเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ ข้อมูลส่วนบุคคลหรือระบบของผู้ใช้บริการคลาวด์ ต่อ ผู้ใช้บริการคลาวด์ ดังต่อไปนี้ – ผู้ให้บริการคลาวด์ รายงานเหตุการณ์ และแจ้งเตือนผู้ใช้บริการคลาวด์ทันทีเมื่อเกิดเหตุการณ์ที่อาจส่งผลกระทบต่อระบบสารสนเทศ ข้อมูลส่วนบุคคลหรือระบบของผู้ใช้บริการคลาวด์ พร้อมให้ข้อมูลรายละเอียดที่เกี่ยวข้อง – ผู้ให้บริการคลาวด์ รักษาหลักฐานที่เกี่ยวข้องกับเหตุการณ์ (evidence preservation) เพื่อใช้ในการตรวจสอบและดำเนินการทางกฎหมายหากจำเป็น – ผู้ใช้บริการคลาวด์ เพื่อติดตามสถานะของเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ ข้อมูลส่วนบุคคลหรือระบบของผู้ใช้บริการคลาวด์ที่รายงาน โดยผู้ให้บริการคลาวด์ มี**ช่องทางในการรับแจ้งเหตุการณ์ด้านความมั่นคงปลอดภัย หรือการดำเนินการเปลี่ยนแปลงที่มีผลกระทบต่อการใช้บริการ**ของผู้ใช้บริการผ่านทางช่องทางดังนี้ **GDCC Contact Center 02-024-1999** กด 0 ติดต่อ Helpdesk (วัน-เวลาทำการ) กด 1 ติดต่อ Technical Support (ตลอด 24 ชั่วโมง) กด 2 ติดต่อ Migration Support (วัน-เวลาทำการ) กด 3 ติดต่อ Training (วัน-เวลาทำการ) กด 4 ติดต่อ Application Support (วัน-เวลาทำการ) **GDCC Email Address** ศูนย์บริการข้อมูล GDCC: Helpdesk@gdcc.go.th บริการสนับสนุนทางเทคนิค: Support@gdcc.go.th บริการสนับสนุนการย้ายข้อมูล: Migration@gdcc.go.th บริการอบรม: Training@gdcc.go.th บริการสนับสนุนแอปพลิเคชัน: Support_app@gdcc.go.th	**การรายงานและตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัย (Incident Management & Reporting)** แจ้งผู้ให้บริการคลาวด์โดยทันทีเมื่อพบหรือสงสัยว่าเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยที่อาจส่งผลกระทบต่อระบบสารสนเทศ ข้อมูลส่วนบุคคลหรือระบบของผู้ใช้บริการคลาวด์ และร่วมมือกับผู้ให้บริการคลาวด์ในการสืบสวนและแก้ไขเหตุการณ์ดังกล่าว ผู้ใช้บริการคลาวด์ สามารถขอข้อมูลจาก ผู้ให้บริการคลาวด์ เกี่ยวกับกลไกสำหรับ – ผู้ใช้บริการคลาวด์ รายงานเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ ข้อมูลส่วนบุคคลหรือระบบของผู้ใช้บริการคลาวด์ที่ตรวจพบต่อผู้ให้บริการคลาวด์ ประสานงานและให้ข้อมูลที่จำเป็นแก่ผู้ให้บริการคลาวด์ เมื่อเกิดเหตุการณ์ที่ต้องการความช่วยเหลือจาก infrastructure layer – ผู้ให้บริการคลาวด์ เพื่อรับรายงานเกี่ยวกับเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ ข้อมูลส่วนบุคคลหรือระบบของผู้ใช้บริการคลาวด์ที่ตรวจพบโดยผู้ให้บริการคลาวด์ – ผู้ใช้บริการคลาวด์ เพื่อติดตามสถานะของเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศที่รายงาน รักษาหลักฐานที่เกี่ยวข้องกับเหตุการณ์ (evidence preservation) เพื่อใช้ในการตรวจสอบและดำเนินการทางกฎหมายหากจำเป็น – ผู้ใช้บริการคลาวด์ ทดสอบและฝึกซ้อมแผนรับมือเหตุการณ์ของหน่วยงานเป็นประจำ พร้อมประสานกับผู้ให้บริการคลาวด์

บริการ GDCC (Government Data Center and Cloud Service)

CSP (Cloud Service Provider)	CSC (Cloud Service Customer)
การบริหารความต่อเนื่องทางธุรกิจด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Aspects of Business Continuity Management) • ผู้ให้บริการคลาวด์ มีหน้าที่จัดทำและทดสอบแผนความต่อเนื่องทางธุรกิจและแผนกู้คืนจากภัยพิบัติ (BCP/DRP) สำหรับ infrastructure และ platform services รวมถึงประเมินความเสี่ยงและผลกระทบทางธุรกิจ (Business Impact Analysis - BIA) สำหรับระบบ infrastructure อย่างสม่ำเสมอ • จัดให้มีระบบสำรอง (redundancy) และความพร้อมใช้งานสูง (high availability) สำหรับ infrastructure ตาม SLA ที่กำหนด • สำรองข้อมูล infrastructure configurations และ platform databases เป็นประจำ พร้อมเก็บไว้ในสถานที่แยกต่างหาก (offsite backup) • แจ้งให้ผู้ใช้บริการคลาวด์ ทราบล่วงหน้าเกี่ยวกับกิจกรรมที่อาจส่งผลกระทบต่อความพร้อมใช้งาน (planned maintenance, DR testing) • กำหนดและรับรอง Recovery Time Objective (RTO) และ Recovery Point Objective (RPO) สำหรับ infrastructure services • ทดสอบและฝึกซ้อมแผน BCP/DRP เป็นประจำอย่างน้อยปีละ 1 ครั้ง พร้อมทบทวนและปรับปรุงแผน และประสานงานผู้ใช้บริการคลาวด์ ในกรณีเกิดภัยพิบัติหรือเหตุการณ์ที่ต้องเรียกใช้แผน DR เพื่อให้การกู้คืนเป็นไปอย่างราบรื่น	**การบริหารความต่อเนื่องทางธุรกิจด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Aspects of Business Continuity Management)** • ผู้ใช้บริการคลาวด์ มีหน้าที่จัดทำแผนความต่อเนื่องทางธุรกิจและแผนกู้คืนจากภัยพิบัติสำหรับ applications และระบบที่รับผิดชอบบน GDCC รวมถึงประเมินความเสี่ยงและผลกระทบทางธุรกิจของระบบและข้อมูลที่สำคัญของหน่วยงาน พร้อมกำหนดลำดับความสำคัญในการกู้คืน • ผู้ใช้บริการคลาวด์ ออกแบบระบบให้มีความพร้อมใช้งานสูงโดยใช้ความสามารถของ GDCC (multiple Tenant/VMs, load balancers, auto-scaling) • สำรองข้อมูลทั้งหมดภายใน VMs, volumes และ applications ตามนโยบายที่กำหนด พร้อมทดสอบการกู้คืนเป็นประจำ • กำหนด RTO และ RPO ที่เหมาะสมสำหรับแต่ละระบบงานและดำเนินการให้บรรลุเป้าหมายดังกล่าว • เก็บสำเนาข้อมูลสำคัญไว้นอกระบบ GDCC (offsite backup) หรือในพื้นที่แยกต่างหาก • จัดทำเอกสารขั้นตอนการกู้คืนระบบอย่างละเอียดและฝึกซ้อมแผน BCP/DRP กับทีมงานเป็นประจำ • ประสานงานกับผู้ให้บริการคลาวด์ เพื่อทำความเข้าใจ RTO/RPO ของ infrastructure และวางแผนการกู้คืนให้สอดคล้องกัน • แจ้งผู้ให้บริการคลาวด์ ล่วงหน้าหากต้องการทดสอบแผน DR หรือต้องการความช่วยเหลือในการกู้คืนระบบ

บริการ GDCC (Government Data Center and Cloud Service)

CSP (Cloud Service Provider)	CSC (Cloud Service Customer)
การปฏิบัติตามกฎหมายและมาตรฐานที่เกี่ยวข้อง (Legal & Compliance) ผู้ให้บริการคลาวด์มีหน้าที่ดำเนินการให้สอดคล้องกับกฎหมาย ระเบียบ และมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้อง รวมถึงสนับสนุนการตรวจประเมินด้านความมั่นคงปลอดภัยตามข้อตกลงที่กำหนดไว้ ผู้ให้บริการคลาวด์มีการกำหนดให้มีการทบทวน/สอบทานรายการกฎหมายที่เกี่ยวข้องกับองค์กรอย่างน้อยปีละ 1 ครั้ง รวมถึงการกำกับดูแลให้มีการปฏิบัติงานสอดคล้องกับที่กฎหมายกำหนด	**การปฏิบัติตามกฎหมายและนโยบายที่เกี่ยวข้อง (Legal & Compliance)** ผู้ใช้บริการคลาวด์มีหน้าที่ปฏิบัติตามกฎหมาย ระเบียบ และนโยบายด้านความมั่นคงปลอดภัยสารสนเทศและการคุ้มครองข้อมูลที่เกี่ยวข้อง เช่น กฎหมายคุ้มครองข้อมูลส่วนบุคคล และนโยบายภายในขององค์กร ผู้ใช้บริการคลาวด์ผู้ให้บริการคลาวด์พิจารณาประเด็นที่ว่ากฎหมายและข้อบังคับที่เกี่ยวข้องอาจเป็นกฎหมายของเขตอำนาจศาลที่ควบคุมผู้ให้บริการคลาวด์ นอกเหนือจากกฎหมายที่ควบคุมผู้ใช้บริการคลาวด์

บริการ GDCC (Government Data Center and Cloud Service)

CSP (Cloud Service Provider)	CSC (Cloud Service Customer)
การทบทวนด้านการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างเป็นอิสระ (Independent Review of Information Security) ผู้ให้บริการคลาวด์มีหน้าที่ให้หลักฐานที่เป็นเอกสารแก่ผู้ใช้บริการคลาวด์เพื่อยืนยันข้อเรียกร้องของ ผู้ให้บริการคลาวด์ในการนำมาตรการควบคุมความมั่นคงปลอดภัยสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคลไปใช้ ในกรณีที่การตรวจสอบโดยผู้ใช้บริการคลาวด์แต่ละรายการไม่สามารถกระทำได้หรืออาจเพิ่มความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศได้ผู้ให้บริการคลาวด์ต้องแสดงหลักฐานที่เป็นอิสระว่ามีการนำไปปฏิบัติและดำเนินการด้านความมั่นคงปลอดภัยสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคลตามนโยบายและขั้นตอนของผู้ให้บริการคลาวด์ ทั้งนี้ ผู้ให้บริการคลาวด์มีหน้าที่แสดงหลักฐานดังกล่าวให้กับผู้ที่คาดว่าจะเป็น ผู้ใช้บริการคลาวด์ก่อนเข้าทำสัญญา โดยปกติแล้วการตรวจสอบอิสระที่เกี่ยวข้องตามที่ผู้ให้บริการคลาวด์เลือก ควรเป็นวิธีการที่เป็นที่ยอมรับเพื่อตอบสนองความต้องการของ ผู้ใช้บริการคลาวด์ ในการตรวจสอบการดำเนินงานของ ผู้ให้บริการคลาวด์ หากมีความโปร่งใสเพียงพอ เมื่อการตรวจสอบที่เป็นอิสระไม่สามารถทำได้ ผู้ให้บริการคลาวด์ ต้องทำการประเมินตนเอง และเปิดเผยกระบวนการและผลลัพธ์ต่อผู้ใช้บริการคลาวด์	**การทบทวนด้านการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างเป็นอิสระ (Independent Review of Information Security)** ผู้ใช้บริการคลาวด์สามารถขอหลักฐานที่เป็นเอกสารว่ามีการนำมาตรการควบคุมและแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศสำหรับบริการคลาวด์ไปปฏิบัติ และมีความสอดคล้องกับที่ผู้ให้บริการคลาวด์กล่าวอ้าง ทั้งนี้ หลักฐานดังกล่าวอาจรวมถึงการรับรองมาตรฐานที่เกี่ยวข้องด้วย ผู้ใช้บริการคลาวด์สามารถขอหลักฐานว่าผู้ให้บริการคลาวด์ได้ปฏิบัติตามกฎระเบียบและมาตรฐานที่เกี่ยวข้องกับผู้ใช้บริการคลาวด์ โดยหลักฐานดังกล่าวอาจเป็นการรับรองที่จัดทำโดยผู้ตรวจสอบภายนอก

บริการ GDCC (Government Data Center and Cloud Service)

CSP (Cloud Service Provider)	CSC (Cloud Service Customer)
การควบคุมเพิ่มเติมสำหรับการปกป้องข้อมูลส่วนบุคคลใน Public Cloud (Public Cloud PII Processor Extended Control Set for PII Protection) • ผู้ให้บริการคลาวด์ไม่นำข้อมูลส่วนบุคคล (PII) ของ CSC ไปใช้เพื่อการตลาดหรือโฆษณาโดยไม่ได้รับความยินยอมอย่างชัดเจน • ผู้ให้บริการคลาวด์แจ้งให้ CSC ทราบเกี่ยวกับสถานที่เก็บข้อมูล (data location) และการใช้ sub-processors ภายนอกก่อนเริ่มให้บริการหรือเมื่อมีการเปลี่ยนแปลง • ผู้ให้บริการคลาวด์จัดให้มีกลไกสำหรับ CSC ในการคืนหรือลบข้อมูลส่วนบุคคลเมื่อสิ้นสุดการให้บริการหรือตามที่ร้องขอ • ผู้ให้บริการคลาวด์แจ้งเตือน CSC ทันทีเมื่อเกิดเหตุการณ์การรั่วไหลของข้อมูลส่วนบุคคล (PII breach) พร้อมให้รายละเอียดที่จำเป็นสำหรับการดำเนินการ • ผู้ให้บริการคลาวด์มีช่องทางให้ CSC สามารถตรวจสอบ (audit) การปฏิบัติตามมาตรการคุ้มครอง PII ผ่านรายงาน third-party audit หรือ certification • ผู้ให้บริการคลาวด์แยกข้อมูลและทรัพยากรของแต่ละ CSC อย่างชัดเจนด้วย multi-tenancy isolation เพื่อป้องกันการเข้าถึงข้อมูลระหว่าง tenants • ผู้ให้บริการคลาวด์กำหนดให้บุคลากรที่เข้าถึง PII ลงนามในข้อตกลงรักษาความลับ (NDA) และได้รับการอบรมด้านการคุ้มครองข้อมูลส่วนบุคคล ปฏิบัติตามกฎหมายและข้อกำหนดด้านการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้อง (PDPA, GDPR ฯลฯ) เมื่อประมวลผล PII ในฐานะ processor	**การควบคุมเพิ่มเติมสำหรับการปกป้องข้อมูลส่วนบุคคลใน Public Cloud (Public Cloud PII Processor Extended Control Set for PII Protection)** • ผู้ใช้บริการคลาวด์กำหนดวัตถุประสงค์และขอบเขตการประมวลผล PII อย่างชัดเจน และสั่งการให้ CSP ประมวลผล PII ตามวัตถุประสงค์เท่านั้น (acting as PII controller) • ผู้ใช้บริการคลาวด์จัดประเภทและระบุข้อมูลส่วนบุคคลที่เก็บไว้ในระบบ GDCC พร้อมกำหนดมาตรการคุ้มครองที่เหมาะสมตามระดับความอ่อนไหว • ผู้ใช้บริการคลาวด์ขอความยินยอมจากเจ้าของข้อมูล (data subjects) ก่อนเก็บรวบรวมและประมวลผล PII ตามที่กฎหมายกำหนด • ผู้ใช้บริการคลาวด์เข้ารหัสข้อมูลส่วนบุคคลที่มีความอ่อนไหวสูงทั้งขณะจัดเก็บ (at rest) และขณะส่งผ่าน (in transit) • ผู้ใช้บริการคลาวด์จัดให้มีกลไกสำหรับเจ้าของข้อมูลในการเข้าถึง แก้ไข หรือลบข้อมูลส่วนบุคคลของตนตามสิทธิที่กฎหมายกำหนด • ผู้ใช้บริการคลาวด์กำหนดระยะเวลาการเก็บรักษา PII และลบข้อมูลอย่างปลอดภัยเมื่อหมดความจำเป็นหรือครบกำหนดเวลา • ผู้ใช้บริการคลาวด์รายงานเหตุการณ์การรั่วไหลของข้อมูลส่วนบุคคลต่อหน่วยงานกำกับดูแล (สคส., PDPC) ตามที่กฎหมายกำหนด • ผู้ใช้บริการคลาวด์ตรวจสอบและทบทวนว่า CSP ปฏิบัติตามข้อตกลงและมาตรการคุ้มครอง PII อย่างเหมาะสม • ผู้ใช้บริการคลาวด์แจ้ง CSP เมื่อต้องการคืนหรือลบข้อมูลส่วนบุคคลทั้งหมดเมื่อสิ้นสุดการใช้บริการหรือโครงการ

4. อ้างอิงกฎหมาย นโยบาย และมาตรฐานที่เกี่ยวข้อง

4.1 นโยบายและกฎหมายที่เกี่ยวข้องกับ Cloud First Policy

4.1.1. นโยบาย Cloud First Policy ของภาครัฐ เป็นแนวทางที่ภาครัฐกำหนดให้หน่วยงานพิจารณาใช้บริการคลาวด์เป็นลำดับแรกในการพัฒนาหรือปรับปรุงระบบสารสนเทศ เพื่อเพิ่มประสิทธิภาพ ลดความซ้ำซ้อนในการลงทุน และยกระดับความมั่นคงปลอดภัยของระบบสารสนเทศภาครัฐ โดยส่งเสริมการใช้บริการคลาวด์ภาครัฐ (Government Data Center and Cloud Service: GDCC) และคลาวด์ที่มีมาตรฐานความมั่นคงปลอดภัยเหมาะสมกับระดับความสำคัญของข้อมูล

4.1.2. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 กำหนดให้หน่วยงานของรัฐและโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องมีมาตรการป้องกัน ตรวจสอบ และรับมือกับภัยคุกคามทางไซเบอร์ ซึ่งรวมถึงระบบที่ให้บริการผ่านโครงสร้างพื้นฐานคลาวด์ โดยต้องมีการบริหารจัดการความเสี่ยงและการจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยอย่างเหมาะสม

4.1.3. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) กำหนดให้หน่วยงานที่ประมวลผลข้อมูลส่วนบุคคลต้องมีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม ทั้งในด้านเทคนิคและการบริหารจัดการ ซึ่งครอบคลุมถึงการใช้บริการคลาวด์ โดยต้องกำหนดหน้าที่และความรับผิดชอบระหว่างผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลให้ชัดเจน

4.2 มาตรฐานสากลที่เกี่ยวข้องกับบริการคลาวด์ (Private Cloud)

4.2.1. ISO/IEC 27001 – Information Security Management System (ISMS)

เป็นมาตรฐานสากลด้านระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ใช้เป็นกรอบในการกำหนดนโยบาย การประเมินความเสี่ยง และการควบคุมด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ รวมถึงระบบ Private Cloud

4.2.2. ISO/IEC 27017 – Code of Practice for Information Security Controls for Cloud Services

เป็นมาตรฐานที่ให้แนวปฏิบัติเพิ่มเติมจาก ISO/IEC 27002 สำหรับบริการคลาวด์ โดยเน้นการกำหนดหน้าที่และความรับผิดชอบระหว่างผู้ให้บริการคลาวด์ (CSP) และผู้ใช้บริการคลาวด์ (CSC) ตามหลัก Shared Responsibility Model ซึ่งเหมาะสำหรับการนำมาใช้กำกับดูแล Private Cloud เช่น GDCC VMware Platform

4.2.3. ISO/IEC 27701 – Privacy Information Management System (PIMS)

เป็นมาตรฐานขยายจาก ISO/IEC 27001 และ ISO/IEC 27002 เพื่อรองรับการบริหารจัดการข้อมูลส่วนบุคคล ช่วยให้การใช้บริการ Private Cloud สอดคล้องกับข้อกำหนดด้านความเป็นส่วนตัวและกฎหมายคุ้มครองข้อมูลส่วนบุคคล

4.2.4. ISO/IEC 20000-1 – IT Service Management System (ITSMS)

เป็นมาตรฐานด้านการบริหารจัดการบริการเทคโนโลยีสารสนเทศ ช่วยสนับสนุนการให้บริการคลาวด์ให้มีคุณภาพสอดคล้องกับ SLA และการบริหารจัดการเหตุการณ์และความต่อเนื่องของบริการ