

ประกาศที่ 08/2569

เรื่อง รูปแบบความรับผิดชอบร่วมกัน (Shared Responsibility Model)

บริษัท โปร อินไซด์ จำกัด (มหาชน)

1. วัตถุประสงค์ (Purpose)

เอกสารฉบับนี้จัดทำขึ้นเพื่อกำหนดขอบเขตและรูปแบบความรับผิดชอบร่วมกัน (Shared Responsibility Model) ระหว่าง บริษัท โปร อินไซด์ จำกัด (มหาชน) ซึ่งต่อไปในเอกสารนี้เรียกว่า “บริษัทฯ” ในฐานะผู้ให้บริการคลาวด์ (Cloud Service Provider) และ ลูกค้า ในฐานะผู้ใช้บริการคลาวด์ (Cloud Service Customer) ให้มีความชัดเจนและเป็นที่ยอมรับร่วมกัน

ความรับผิดชอบดังกล่าวครอบคลุมการบริหารจัดการระบบ ความมั่นคงปลอดภัยสารสนเทศ การคุ้มครองและกำกับดูแลข้อมูล ตลอดจนการปฏิบัติงานที่เกี่ยวข้องกับการให้บริการและการใช้บริการคลาวด์ เพื่อให้บริษัทฯ และลูกค้าสามารถดำเนินการในส่วนที่อยู่ภายใต้ความรับผิดชอบของตนได้อย่างเหมาะสม

2. ที่ตั้งและการประมวลผลข้อมูล (Data Location)

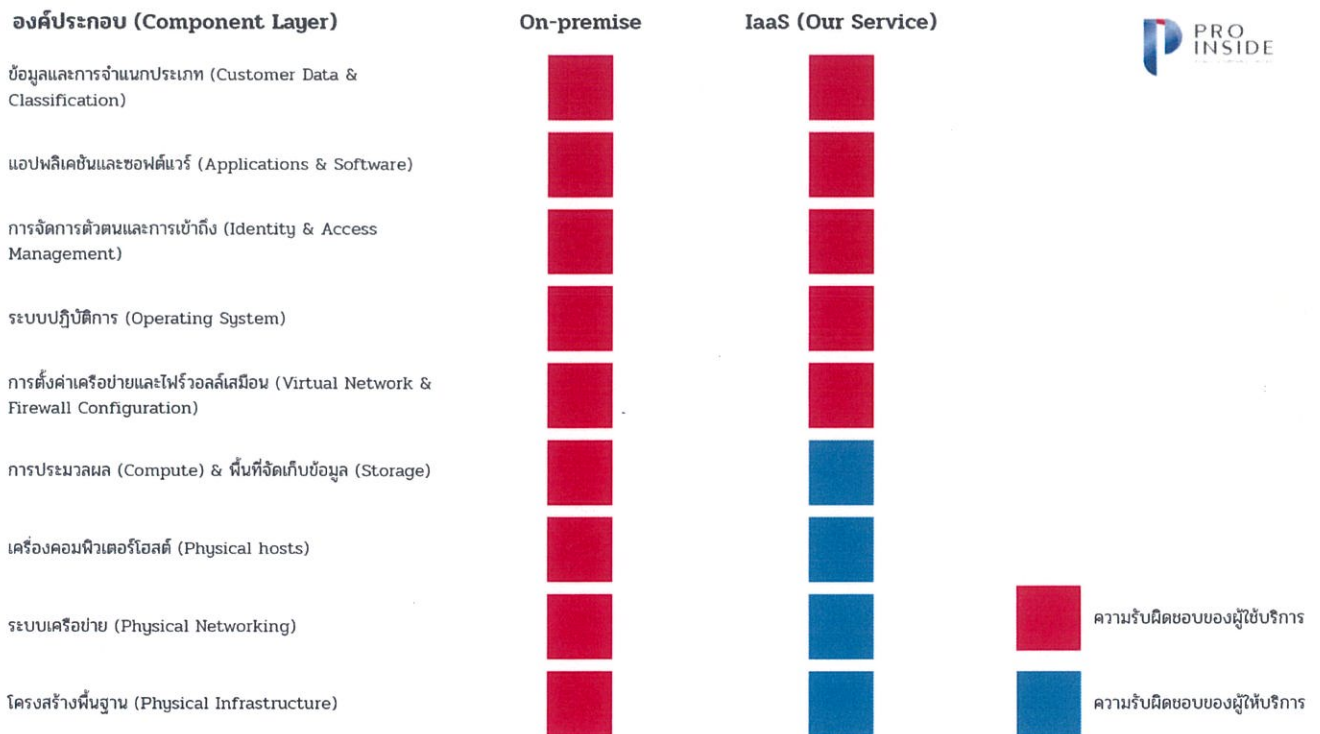
บริษัทฯ ให้บริการโครงสร้างพื้นฐานคลาวด์ (Infrastructure as a Service: IaaS) ผ่านศูนย์ข้อมูลที่ตั้งอยู่ในกรุงเทพมหานครและจังหวัดชลบุรี ประเทศไทย โดยข้อมูลของผู้ใช้บริการ รวมถึงข้อมูลสำรอง (Backup Data) จะถูกจัดเก็บและประมวลผลภายในราชอาณาจักรไทย

การเก็บรวบรวม ใช้ เปิดเผย ประมวลผล และสำรองข้อมูล รวมถึงข้อมูลส่วนบุคคล จะดำเนินการภายในราชอาณาจักรไทยเท่านั้น เว้นแต่จะได้รับความยินยอมเป็นลายลักษณ์อักษรจากผู้ควบคุมข้อมูลส่วนบุคคล หรือมีการระบุไว้เป็นอย่างอื่นในสัญญาการให้บริการ

3. รูปแบบความรับผิดชอบร่วมกัน (Shared Responsibility Model)

การให้บริการคลาวด์เป็นความรับผิดชอบร่วมกันระหว่างบริษัทฯ และผู้ใช้บริการ โดยบริษัทฯ รับผิดชอบการรักษาความมั่นคงปลอดภัยและการบริหารจัดการโครงสร้างพื้นฐานที่ใช้ในการให้บริการคลาวด์ (Security of the Cloud) ขณะที่ผู้ใช้บริการรับผิดชอบการรักษาความมั่นคงปลอดภัยของระบบ ทรัพยากร และข้อมูลที่นำมาใช้งานบนบริการคลาวด์ (Security in the Cloud) ตามขอบเขตการควบคุมของแต่ละฝ่าย แสดงดังภาพที่ 1

2/แผนภาพที่ 1 รูปแบบความรับผิดชอบร่วมกัน.....



แผนภาพที่ 1 รูปแบบความรับผิดชอบร่วมกัน (Shared Responsibility Model)

ความรับผิดชอบในบางด้านอาจเป็นความรับผิดชอบร่วมกันระหว่างบริษัทฯ และผู้ให้บริการ ทั้งนี้ ขอบเขตความรับผิดชอบของแต่ละฝ่ายมีรายละเอียดตามแผนภาพและข้อกำหนดในหัวข้อต่อไป

3.1 หน้าที่และความรับผิดชอบของผู้ให้บริการ (Cloud Service Provider Responsibilities)

ผู้ให้บริการรับผิดชอบการบริหารจัดการและรักษาความมั่นคงปลอดภัยของโครงสร้างพื้นฐานที่ใช้ในการให้บริการคลาวด์ (Security of the Cloud) ตั้งแต่โครงสร้างพื้นฐานทางกายภาพ ระบบเครือข่าย เครื่องคอมพิวเตอร์โฮสต์ ตลอดจนทรัพยากรด้านการประมวลผลและพื้นที่จัดเก็บข้อมูล โดยมีหน้าที่และความรับผิดชอบดังนี้

องค์ประกอบ	หน้าที่และความรับผิดชอบของผู้ให้บริการ
โครงสร้างพื้นฐาน (Physical Infrastructure)	จัดให้มีและดูแลโครงสร้างพื้นฐานทางกายภาพที่รองรับการให้บริการคลาวด์ รวมถึงมาตรการควบคุมการเข้าถึงทางกายภาพ ระบบไฟฟ้า ระบบปรับอากาศ และระบบสนับสนุนที่จำเป็น เพื่อให้บริการมีความมั่นคงปลอดภัยและพร้อมใช้งาน
ระบบเครือข่าย (Physical Networking)	บริหารจัดการและรักษาความมั่นคงปลอดภัยของโครงสร้างพื้นฐานเครือข่ายที่ใช้ในการให้บริการ รวมถึงอุปกรณ์เครือข่ายและอุปกรณ์รักษาความมั่นคงปลอดภัยที่อยู่ภายใต้การควบคุมของผู้ให้บริการ
เครื่องคอมพิวเตอร์โฮสต์ (Physical Hosts)	บริหารจัดการเครื่องคอมพิวเตอร์โฮสต์และระบบ Virtualization ที่รองรับการให้บริการ รวมถึงการกำหนดค่าความมั่นคงปลอดภัย การติดตั้ง Patch และการแก้ไขช่องโหว่ของระบบที่อยู่ภายใต้การควบคุมของผู้ให้บริการ

3/การประมวลผลและพื้นที่จัดเก็บข้อมูล.....

องค์ประกอบ	หน้าที่และความรับผิดชอบของผู้ให้บริการ
การประมวลผลและพื้นที่จัดเก็บข้อมูล (Compute & Storage)	จัดสรรและบริหารจัดการทรัพยากรด้านการประมวลผลและพื้นที่จัดเก็บข้อมูลให้เพียงพอต่อการให้บริการ รวมถึงติดตามการใช้ทรัพยากรและบริหาร Capacity เพื่อรักษาประสิทธิภาพและความพร้อมใช้งานของบริการตามระดับที่กำหนด
การเฝ้าระวังและบันทึกเหตุการณ์ (Monitoring & Logging)	เฝ้าระวังการทำงานและเหตุการณ์ด้านความมั่นคงปลอดภัยของโครงสร้างพื้นฐาน คลาวด์อย่างต่อเนื่อง รวมถึงจัดเก็บ Log ที่เกี่ยวข้องกับโครงสร้างพื้นฐานคลาวด์ เป็นระยะเวลาไม่น้อยกว่า 90 วัน เพื่อใช้ในการตรวจสอบความผิดปกติและดำเนินการแก้ไขอย่างเหมาะสม โดยมีการควบคุมการเข้าถึงและการใช้งาน Log ให้เป็นไปตามวัตถุประสงค์ที่กำหนด และดำเนินการลบ Log เมื่อพ้นระยะเวลาการจัดเก็บในกรณีที่ผู้ใช้บริการประสงค์จะขอข้อมูล Log ผู้ใช้บริการสามารถส่งคำร้อง พร้อมระบุวัตถุประสงค์ในการขอข้อมูลผ่านทาง cloud.services@proinside.co.th
การสำรองและกู้คืนข้อมูล (Backup & Recovery)	สำรองข้อมูลตามขอบเขตและเงื่อนไขของบริการที่กำหนด โดยดำเนินการสำรองข้อมูล ทุก 24 ชั่วโมง และจัดเก็บข้อมูลสำรองเป็นระยะเวลา 30 วัน โดยมีค่า RPO ไม่เกิน 24 ชั่วโมง RTO ไม่เกิน 2 ชั่วโมง เพื่อรองรับการกู้คืนข้อมูลและการให้บริการเมื่อเกิดเหตุขัดข้อง ข้อมูลสำรองจะได้รับการจัดเก็บแยกจากระบบที่ให้บริการหลักทางทางตรรกะตามความเหมาะสม พร้อมมีมาตรการควบคุมการเข้าถึงและการรักษาความมั่นคงปลอดภัย และจะถูกลบเมื่อพ้นระยะเวลาการจัดเก็บที่กำหนด รวมถึงมีการทบทวนและทดสอบกระบวนการสำรองและกู้คืนข้อมูลตามรอบที่กำหนด เพื่อให้มั่นใจว่าสามารถกู้คืนข้อมูลได้เมื่อจำเป็น
การจัดการเหตุการณ์และการเปลี่ยนแปลง (Incident & Change Management)	ผู้ให้บริการจะบริหารจัดการเหตุการณ์และการเปลี่ยนแปลงที่เกี่ยวข้องกับโครงสร้างพื้นฐานคลาวด์ และแจ้งผู้ใช้บริการเมื่อมีเหตุการณ์หรือการเปลี่ยนแปลงที่อาจส่งผลกระทบต่อการใช้บริการผ่านทาง cloud.services@proinside.co.th
การจัดการช่องโหว่และการทดสอบความมั่นคงปลอดภัย (Vulnerability Management & Security Testing)	ดำเนินการตรวจสอบและจัดการช่องโหว่ของโครงสร้างพื้นฐานคลาวด์ที่อยู่ภายใต้ความรับผิดชอบ โดยดำเนินการ VA และทดสอบเจาะระบบ (Penetration Testing) ตามรอบที่กำหนด และเมื่อมีการเปลี่ยนแปลงระบบอย่างมีนัยสำคัญ (Major Change) ทั้งนี้ ในกรณีที่การดำเนินการอาจส่งผลกระทบต่อการใช้บริการ บริษัทฯ จะแจ้งผู้ใช้บริการก่อนดำเนินการตามกระบวนการบริหารการเปลี่ยนแปลงที่กำหนด
การคุ้มครองข้อมูลและการปฏิบัติตามข้อกำหนด (Data Protection & Compliance)	ดำเนินมาตรการคุ้มครองข้อมูลและปฏิบัติตามกฎหมาย ข้อกำหนด และมาตรฐานที่เกี่ยวข้องกับการให้บริการ รวมถึงดำเนินการต่อข้อมูลส่วนบุคคลตามขอบเขตหน้าที่ และเงื่อนไขที่กำหนดไว้ในสัญญาหรือข้อตกลงที่เกี่ยวข้อง

4/การส่งคืนและลบข้อมูลเมื่อสิ้นสุดบริการ.....

องค์ประกอบ	หน้าที่และความรับผิดชอบของผู้ให้บริการ
การส่งคืนและลบข้อมูลเมื่อสิ้นสุดบริการ (Data Portability & Deletion)	เมื่อสิ้นสุดหรือยกเลิกการใช้บริการ บริษัทฯ จะเปิดให้ผู้ให้บริการสามารถเข้าถึงและนำข้อมูลออกจากระบบภายในระยะเวลา 30 วันนับจากวันที่สิ้นสุดบริการ โดยผู้ให้บริการสามารถนำข้อมูลออกในรูปแบบมาตรฐานหรือรูปแบบที่ระบบรองรับ เช่น Virtual Machine Image, Backup File หรือ Data Export ตามเทคโนโลยีของบริการ ผู้ให้บริการมีหน้าที่ดำเนินการนำข้อมูลที่ต้องการเก็บรักษาออกจากระบบ และตรวจสอบความครบถ้วนและความสามารถในการนำข้อมูลไปใช้งานต่อภายในระยะเวลาดังกล่าวเมื่อพ้นระยะเวลา 30 วัน บริษัทฯ จะดำเนินการลบข้อมูลของผู้ให้บริการออกจากระบบที่ให้บริการ และข้อมูลสำรองจะถูกเก็บตามรอบการเก็บรักษาข้อมูลสำรอง (Backup Retention) ที่กำหนด โดยในช่วงระหว่างรอการลบ ข้อมูลจะยังคงได้รับการควบคุมการเข้าถึงและมาตรการรักษาความมั่นคงปลอดภัยตามที่กำหนด

3.2 หน้าที่และความรับผิดชอบของผู้ใช้บริการ (Cloud Service Customer Responsibilities)

ผู้ให้บริการรับผิดชอบการรักษาความมั่นคงปลอดภัยของทรัพยากร ระบบงาน และข้อมูลที่นำมาใช้งานบนบริการคลาวด์ (Security in the Cloud) ตั้งแต่การกำหนดค่าเครือข่ายเสมือน ระบบปฏิบัติการ การบริหารจัดการตัวตนและสิทธิ์การเข้าถึง แอปพลิเคชันและซอฟต์แวร์ ตลอดจนข้อมูลของผู้ใช้บริการ โดยมีหน้าที่และความรับผิดชอบ ดังนี้

องค์ประกอบ	หน้าที่และความรับผิดชอบของผู้ใช้บริการ
การตั้งค่าเครือข่ายและไฟร์วอลล์เสมือน (Virtual Network & Firewall Configuration)	กำหนดและบริหารจัดการเครือข่ายเสมือน Firewall Rule และการเชื่อมต่อของ Virtual Machine ในส่วนที่อยู่ภายใต้การควบคุมของผู้ให้บริการให้มีความมั่นคงปลอดภัย รวมถึงเลือกใช้ Protocol ที่มีการเข้ารหัสสำหรับการบริหารจัดการจากระยะไกลและการรับส่งข้อมูลสำคัญ เช่น HTTPS, SFTP และ SSH
ระบบปฏิบัติการ (Operating System)	ดูแลรักษาความมั่นคงปลอดภัยของระบบปฏิบัติการภายใน Virtual Machine รวมถึงการกำหนดค่า Security Hardening การติดตั้ง Security Patch การป้องกัน Malware และการแก้ไขช่องโหว่ โดยหลีกเลี่ยงการใช้งานระบบปฏิบัติการที่สิ้นสุดการสนับสนุนด้านความมั่นคงปลอดภัย (End of Support) หรือดำเนินการจัดการความเสี่ยงที่เหมาะสมในกรณีที่มีความจำเป็นต้องใช้งาน
ผู้มีอำนาจในการร้องขอบริการ (Authorized Person & Incident Requester)	ผู้ให้บริการต้องกำหนดผู้มีอำนาจ (Authorized Person) และลงทะเบียนเป็น Incident Requester สำหรับการแจ้งเหตุหรือร้องขอให้บริษัทฯ ดำเนินการเกี่ยวกับบริการ โดยสามารถลงทะเบียนได้สูงสุด 3 ท่าน บริษัทฯ จะดำเนินการอนุมัติหรือปรับปรุงรายชื่อภายใน 24 ชั่วโมงนับจากได้รับคำขอ และจะขอให้ผู้ให้บริการทบทวนรายชื่อทุก 3 เดือน ทั้งนี้ การเปลี่ยนแปลงรายชื่อผู้มีสิทธิ์สามารถแจ้งได้ที่ cloud.services@proinside.co.th

5/การจัดการตัวตนและการเข้าถึง.....

องค์ประกอบ	หน้าที่และความรับผิดชอบของผู้ให้บริการ
การจัดการตัวตนและการเข้าถึง (Identity & Access Management)	บริหารจัดการบัญชีใช้งาน การพิสูจน์ตัวตน และสิทธิ์การเข้าถึง Virtual Machine และทรัพยากรคลาวด์ที่อยู่ภายใต้การควบคุมของตน รวมถึงกำหนดรหัสผ่านที่มีความมั่นคงปลอดภัย และ เปลี่ยนรหัสผ่านที่ได้รับจากผู้ให้บริการทันทีเมื่อเริ่มใช้งาน ตลอดจนทบทวน เปลี่ยนแปลง และยกเลิกสิทธิ์เมื่อไม่มีความจำเป็น
แอปพลิเคชันและซอฟต์แวร์ (Applications & Software)	รับผิดชอบการติดตั้ง กำหนดค่า ดูแลรักษา และปรับปรุงแอปพลิเคชันและซอฟต์แวร์ภายใน Virtual Machine รวมถึงการติดตั้ง Security Patch การจัดการช่องโหว่ และในกรณีที่มีการพัฒนาระบบงาน ต้องคำนึงถึงหลักการพัฒนาระบบอย่างมั่นคงปลอดภัยตลอดวงจรการพัฒนาระบบ (Secure SDLC)
การบริหารจัดการทรัพยากรใน VM (VM Resource Management)	รับผิดชอบในการติดตามความเพียงพอของทรัพยากร Virtual Machine และสามารถร้องขอปรับเปลี่ยนทรัพยากรผ่านทาง cloud.services@proinside.co.th โดยบริษัทฯ จะตรวจสอบสิทธิ์ผู้ร้องขอและ Capacity ตามขอบเขตของสัญญาก่อนดำเนินการ ทั้งนี้ กรณีเกินโควตาหรือขอบเขตบริการอาจมีค่าใช้จ่ายเพิ่มเติมและบริษัทฯ จะรายงานการใช้ทรัพยากรของ VM ให้ผู้ให้บริการทราบเป็นประจำทุกเดือน
ข้อมูลและการจำแนกประเภท (Customer Data & Classification)	รับผิดชอบการรักษาความมั่นคงปลอดภัยของข้อมูลที่จัดเก็บหรือประมวลผลภายใน VM รวมถึงการจำแนกประเภทและระดับความอ่อนไหวของข้อมูล การกำหนดสิทธิ์การเก็บรักษา การส่งต่อ และการลบข้อมูลให้สอดคล้องกับกฎหมาย ข้อกำหนด และวัตถุประสงค์ในการประมวลผลที่เกี่ยวข้อง
การคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection)	ในกรณีที่มีการประมวลผลข้อมูลส่วนบุคคล ผู้ให้บริการรับผิดชอบการกำหนดวัตถุประสงค์และขอบเขตการประมวลผล การจัดทำและทบทวนข้อมูลที่เกี่ยวข้อง เช่น Data Inventory และ RoPA การพิจารณาจัดทำ DPIA ตามความเหมาะสม การรองรับการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล ตลอดจนการกำหนดระยะเวลาการเก็บรักษาและการลบข้อมูลให้สอดคล้องกับกฎหมายและข้อกำหนดที่เกี่ยวข้อง
การเข้ารหัสและการบริหารจัดการกุญแจ (Encryption & Key Management)	ผู้ให้บริการรับผิดชอบการเลือกใช้การเข้ารหัสและบริหารจัดการกุญแจให้เหมาะสมกับข้อมูล รวมถึงสามารถนำกุญแจของตนเองมาใช้ (Bring Your Own Key: BYOK) ทั้งนี้ KMS ไม่รวมอยู่ในบริการมาตรฐาน หากมีความประสงค์ใช้งาน สามารถติดต่อบริษัทฯ เพื่อจัดหาเทคโนโลยีและกำหนดขอบเขตการให้บริการร่วมกัน
การสำรองและกู้คืนข้อมูล (Backup & Recovery)	กำหนดความต้องการด้านการสำรองและกู้คืนข้อมูลให้เหมาะสมกับระบบงานและความสำคัญของข้อมูล และเลือกใช้บริการ Backup ตามขอบเขตที่ผู้ให้บริการจัดให้ ทั้งนี้ ผู้ให้บริการจะรับผิดชอบการสำรองข้อมูลเฉพาะส่วนที่ได้ตกลงกับผู้ให้บริการไว้เท่านั้น
การบันทึกและเฝ้าระวังเหตุการณ์ (Logging & Monitoring)	จัดเก็บ ปกป้อง และตรวจสอบ Log ที่เกิดขึ้นภายใน Virtual Machine ระบบปฏิบัติการ และแอปพลิเคชันที่อยู่ภายใต้การควบคุมของตน รวมถึงจัดให้มีพื้นที่จัดเก็บ Log ที่เพียงพอ การควบคุมการเข้าถึง และระยะเวลาการเก็บรักษาให้สอดคล้องกับกฎหมายและข้อกำหนดที่เกี่ยวข้อง ตลอดจนจัดให้มีการเทียบเวลาของระบบกับแหล่งเวลามาตรฐานที่เชื่อถือได้ (Time Synchronization)

6/การจัดการช่องโหว่.....

องค์ประกอบ	หน้าที่และความรับผิดชอบของผู้ให้บริการ
การจัดการช่องโหว่ (Vulnerability Management)	ติดตามและตรวจสอบช่องโหว่ของระบบปฏิบัติการ แอปพลิเคชัน และซอฟต์แวร์ภายใน VM พร้อมดำเนินการแก้ไขหรือใช้มาตรการลดความเสี่ยงภายในระยะเวลาที่เหมาะสม ทั้งนี้ หากผู้ให้บริการต้องการ บริการตรวจสอบช่องโหว่เพิ่มเติม (Vulnerability Assessment Service) สามารถติดต่อบริษัทฯ ผ่านช่องทางที่กำหนดเพื่อพิจารณาขอบเขตและเงื่อนไขการให้บริการเพิ่มเติมได้
การจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยและหลักฐานทางคอมพิวเตอร์ (Security Incident & Digital Evidence)	ตรวจสอบและตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยในส่วนที่อยู่ภายใต้การควบคุมของตน และประสานบริษัทฯ เมื่อเหตุการณ์เกี่ยวข้องกับโครงสร้างพื้นฐานคลาวด์ กรณีต้องการหลักฐานทางคอมพิวเตอร์ในส่วนที่อยู่ภายใต้ความรับผิดชอบของบริษัทฯ ผู้ให้บริการสามารถร้องขอผ่าน cloud.services@proinside.co.th 02-029-7878 โดยบริษัทฯ จะให้ข้อมูลเฉพาะส่วนที่เกี่ยวข้องกับผู้ให้บริการรายนั้นเท่านั้น
การบริหารการเปลี่ยนแปลง (Change Management)	ควบคุมการเปลี่ยนแปลง Virtual Machine ระบบปฏิบัติการ แอปพลิเคชัน และการกำหนดค่าที่อยู่ภายใต้การควบคุมของตน และประสานผู้ให้บริการก่อนดำเนินการในกรณีที่การเปลี่ยนแปลงอาจส่งผลกระทบต่อโครงสร้างพื้นฐานหรือบริการคลาวด์
ผู้ให้บริการภายนอกของผู้ให้บริการ (Customer's Third-party)	รับผิดชอบและควบคุมการเข้าถึงหรือการดำเนินการของบุคคลภายนอกที่ผู้ให้บริการอนุญาตให้เข้าถึง Virtual Machine ระบบงาน หรือข้อมูลของตน โดยการดำเนินการของบุคคลดังกล่าวถือเป็นส่วนหนึ่งของความรับผิดชอบของผู้ให้บริการ
อุปกรณ์ปลายทาง (Endpoint Security)	ดูแลอุปกรณ์ปลายทางที่ใช้เข้าถึงหรือบริหารจัดการบริการคลาวด์ให้มีความมั่นคงปลอดภัย โดยใช้มาตรการที่เหมาะสม เช่น การควบคุมการเข้าถึง การติดตั้ง Security Patch การป้องกัน Malware และการเข้ารหัสข้อมูล
การปฏิบัติตามกฎหมายและข้อกำหนด (Compliance)	พิจารณาและดำเนินการให้การนำข้อมูลและระบบงานมาใช้บนบริการคลาวด์สอดคล้องกับกฎหมาย ข้อกำหนดตามสัญญา และข้อกำหนดภายในองค์กรที่เกี่ยวข้องกับผู้ให้บริการ

4. แนวปฏิบัติที่ดีเพื่อความมั่นคงปลอดภัยสำหรับผู้ให้บริการ (Customer Best Practices)

ผู้ให้บริการควรพิจารณานำแนวทางปฏิบัติด้านความมั่นคงปลอดภัยต่อไปนี้มาใช้ โดยปรับให้เหมาะสมกับลักษณะระบบงาน ข้อมูล และระดับความเสี่ยงของตน โดยมีแนวทางปฏิบัติดังนี้

- เปิดใช้งาน Multi-Factor Authentication (MFA) สำหรับบัญชีที่รองรับ โดยเฉพาะบัญชีผู้ดูแลระบบ กำหนดสิทธิ์ตามหลัก Least Privilege แยกบัญชี Administrator ออกจากบัญชีใช้งานทั่วไป และปิดหรือลบ Account ที่ไม่ใช้งาน
- เปิดเฉพาะ Port และ Protocol ที่จำเป็น จำกัด Source IP สำหรับ Management Port เช่น SSH/RDP หลีกเลี่ยงการเปิด Management Interface สู่ Internet โดยตรง และแบ่ง Network Segment ตามความสำคัญของระบบงาน

7/ปิด Service.....

- ปิด Service และ Default Account ที่ไม่จำเป็น เปลี่ยน Default Credential ติดตั้ง Security Patch อย่างสม่ำเสมอ ใช้ OS ที่ยังอยู่ในช่วง Support และติดตั้ง Anti-malware/EDR ตามความเหมาะสม
- เข้ารหัสข้อมูลสำคัญทั้ง Data at Rest และ Data in Transit ใช้ Protocol ที่ปลอดภัย เช่น HTTPS, SSH และ SFTP จำกัดสิทธิ์เข้าถึง Cryptographic Key และหลีกเลี่ยงการจัดเก็บ Password, API Key หรือ Secret ใน Source Code หรือ Configuration File ที่ไม่มีการป้องกัน
- เปิด Logging สำหรับ Login/Logout, Failed Login, Privileged Activity, Configuration Change และ Security Event ที่สำคัญ และกำหนด Time Synchronization ให้ VM ใช้แหล่งเวลาที่เชื่อถือได้ และกำหนด Alert สำหรับเหตุการณ์ผิดปกติหรือมีความเสี่ยงสูง
- กำหนด Backup ให้เหมาะสมกับความสำคัญของระบบและข้อมูล แยก Backup ออกจาก Production Environment จำกัดสิทธิ์เข้าถึง Backup และ ทดสอบ Restore เป็นระยะ เพื่อยืนยันว่าสามารถกู้คืนข้อมูลได้จริง
- ควรจัดเก็บและบริหารกุญแจเข้ารหัสด้วยระบบที่เหมาะสม เช่น Key Management System (KMS), HSM หรือ Secrets Vault และไม่จัดเก็บกุญแจร่วมกับข้อมูลที่ถูกเข้ารหัสหรือฝังไว้ใน Source Code/Configuration File ควรจำกัดสิทธิ์การเข้าถึงตามหลัก Least Privilege แยกหน้าที่ผู้ดูแลกุญแจออกจากผู้ใช้งาน (Separation of Duties) และจัดให้มีการ สร้าง เปลี่ยนหมุนเวียน (Key Rotation) สำรอง เพิกถอน และทำลายกุญแจ ตามวงจรชีวิตที่กำหนด รวมถึงจัดเก็บ Log การใช้งานและการเปลี่ยนแปลงกุญแจเพื่อให้สามารถตรวจสอบย้อนหลังได้

สำหรับระบบที่มีความสำคัญหรือประมวผลข้อมูลส่วนบุคคล/ข้อมูลอ่อนไหว ผู้ให้บริการควรพิจารณาเพิ่มมาตรการ เช่น Vulnerability Scanning, Secure SDLC, การแยก Production และ Non-production และหลีกเลี่ยงการใช้ข้อมูลจริงในระบบทดสอบ

5. ผู้ให้บริการภายนอกที่เกี่ยวข้อง (Third-party Service Provider)

บริษัทฯ ใช้บริการจากผู้ให้บริการภายนอกเพื่อสนับสนุนการให้บริการคลาวด์ โดยบริษัทฯ จะดำเนินการคัดเลือก ประเมิน และกำกับดูแลผู้ให้บริการภายนอกให้มีมาตรการด้านความมั่นคงปลอดภัยและการคุ้มครองข้อมูลที่เหมาะสมกับขอบเขตของบริการ ผู้ให้บริการภายนอกที่เกี่ยวข้องกับการให้บริการ มีดังนี้

ผู้ให้บริการ	บริการที่เกี่ยวข้อง	การเข้าถึง/ประมวผลข้อมูล
บริษัท โทรคมนาคม แห่งชาติ จำกัด (มหาชน) (NT)	ให้บริการพื้นที่ศูนย์ข้อมูล (Data Center / Colocation) สำหรับ ติดตั้งโครงสร้างพื้นฐานคลาวด์ที่ กรุงเทพมหานครและจังหวัดชลบุรี	ให้บริการศูนย์ข้อมูลสำหรับระบบหลักและระบบสำรอง รวมถึงการ เชื่อมต่อเครือข่าย โดยมีการเข้าถึงเฉพาะในระดับ Physical Infrastructure และ Network Service และ ไม่มีสิทธิ์เข้าถึงระบบ Cloud Infrastructure ในระดับ Logical Access หรือข้อมูลของ ผู้ให้บริการ
บริษัท วีเอสที อีซี เอส (ประเทศไทย) จำกัด (VST ECS)	การให้คำปรึกษาและสนับสนุน ด้านเทคโนโลยีคลาวด์ และ โครงสร้างพื้นฐาน	จัดให้มีบุคลากรผู้เชี่ยวชาญด้านเทคโนโลยี Huawei Cloud เพื่อ สนับสนุนการดูแล บำรุงรักษา และแก้ไขปัญหาด้าน Cloud Infrastructure โดยบุคลากรอาจได้รับสิทธิ์ระดับสูงในการเข้าถึง ระบบตามความจำเป็น ซึ่งอาจทำให้สามารถเข้าถึงข้อมูลของ ผู้ให้บริการ รวมถึงข้อมูลส่วนบุคคลได้ ทั้งนี้ การเข้าถึงต้องเป็นไปตาม ขอบเขต สิทธิ์ และมาตรการควบคุมที่บริษัทฯ กำหนด

8/บริษัทฯ ยังคงรับผิดชอบ.....

บริษัทฯ ยังคงรับผิดชอบในการกำกับดูแลผู้ให้บริการภายนอกที่เกี่ยวข้องกับการให้บริการคลาวด์ตามขอบเขตความรับผิดชอบของบริษัทฯ รวมถึงข้อกำหนดตามสัญญา กฎหมาย และข้อกำหนดด้านความมั่นคงปลอดภัยและการคุ้มครองข้อมูลที่เกี่ยวข้อง

ในกรณีที่มีการเปลี่ยนแปลงผู้ให้บริการภายนอกซึ่งอาจส่งผลกระทบต่อให้บริการหรือการประมวลผลข้อมูล/ข้อมูลส่วนบุคคลของผู้ใช้บริการ บริษัทฯ จะแจ้งให้ผู้ให้บริการทราบตามช่องทางและเงื่อนไขที่กำหนด

รูปแบบความรับผิดชอบร่วมกันฯ นี้มีผลบังคับใช้ตั้งแต่วันที่ 31 กรกฎาคม 2569

จึงเรียนมาเพื่อทราบโดยทั่วกัน

ประกาศ ณ วันที่ 31 กรกฎาคม พ.ศ. 2569



(นางสาวเบญญาภา เฉลิมวัฒน์)
ประธานเจ้าหน้าที่บริหาร
บริษัท โปร อินไซด์ จำกัด (มหาชน)