(ร่าง)

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

เรื่อง หลักเกณฑ์การให้บริการ Cloud Computing พ.ศ. .....

เนื่องจากมีการใช้บริการ Cloud Computing ในการให้บริการธุรกรรมทางอิเล็กทรอนิกส์อย่างแพร่หลาย เพื่อให้การบริการธุรกรรมทางอิเล็กทรอนิกส์ที่เกี่ยวกับบริการ Cloud Computing มีความมั่นคงปลอดภัย มีความน่าเชื่อถือตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากล

อาศัยอำนาจตามความมาตรา ๓๗ (๕) แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ จึงกำหนดหลักเกณฑ์การให้บริการ Cloud Computing ดังต่อไปนี้

ข้อ ๑ กำหนดให้ผู้ให้บริการ Cloud Computing ควรดำเนินการตามแนวทางหลักเกณฑ์การให้บริการ Cloud Computing ท้ายประกาศนี้

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ประกาศ ณ วันที่ พ.ศ. .....

รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
ประธานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

หลักเกณฑ์การให้บริการ Cloud Computing

๑. บทนำ

เนื่องจากปัจจุบันทั้งภาครัฐและภาคเอกชน มีการให้บริการผ่านช่องทางออนไลน์อย่างแพร่หลาย โดยใช้ Cloud Computing เป็นเทคโนโลยีพื้นฐานในการให้บริการธุรกรรมทางอิเล็กทรอนิกส์ต่างๆ ซึ่งพบว่ายังไม่มีหน่วยงานภาครัฐกำหนดนโยบาย หลักเกณฑ์ หรือแนวทางที่เกี่ยวกับให้บริการ Cloud Computing เพื่อส่งเสริมและพัฒนาการให้บริการ Cloud Computing ที่เกี่ยวข้องกับธุรกรรมทางอิเล็กทรอนิกส์ให้มีความมั่นคงปลอดภัย ความน่าเชื่อถือตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากล คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ จึงเห็นควรกำหนดหลักเกณฑ์การให้บริการ Cloud Computing

๒. คำนิยาม

"บริการ Cloud Computing" หมายถึง

๑) การให้บริการอุปกรณ์ฮาร์ดแวร์ อุปกรณ์จัดเก็บข้อมูล เครือข่าย เป็นต้น หรือ

๒) การให้บริการซอฟต์แวร์ หรือ

๓) การให้บริการสภาพแวดล้อมสำหรับการพัฒนาซอฟต์แวร์ การกระจายข้อมูล การบริหารจัดการซอฟต์แวร์ การใช้ประโยชน์จากข้อมูล เป็นต้น หรือ

๔) การให้บริการใดที่เป็นการรวมกันของบริการสองอย่างขึ้นไป จาก ข้อ ๑) ถึง ๓) หรือ

๕) การให้บริการอื่นที่ประกาศกำหนด

"ผู้ให้บริการ"หมายถึง ผู้ประกอบธุรกิจให้บริการ Cloud Computing

๓. หลักเกณฑ์การให้บริการ Cloud Computing

๓.๑ การจัดทำนโยบายและแนวทางปฏิบัติขององค์กร

เพื่อกำหนดนโยบายและแนวปฏิบัติในองค์กรของผู้ให้บริการ โดยมีสาระสำคัญดังต่อไปนี้

๓.๑.๑ มาตรการป้องกันกระบวนการทำงาน ผู้ให้บริการจะควรมีการจัดทำนโยบายและแนวปฏิบัติว่าด้วยความมั่นคงปลอดภัยสารสนเทศ การพัฒนาทรัพยากรบุคลากรให้มีความรู้ความเข้าใจในเรื่องความมั่นคงปลอดภัยของข้อมูล การประเมินสินทรัพย์ การจัดการเปลี่ยนแปลง การบริหารความเสี่ยง กระบวนการตอบสนองต่อเหตุการณ์ฉุกเฉิน การจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน การติดตามดูแลการให้บริการ กระบวนการจ้างช่วงต่อ (สัญญา) และการปฏิบัติอื่นใดตามที่กฎหมายกำหนด

๓.๑.๒ มาตรการป้องกันทางกายภาพ ผู้ให้บริการควรจัดให้มีมาตรการในการป้องกันสำหรับความมั่นคงปลอดภัยและสิ่งอำนวยความสะดวกในการประมวลผลข้อมูลทางกายภาพ เช่น การกำหนดควบคุมพื้นที่ ความปลอดภัยในพื้นที่หวงห้าม การควบคุมการเข้าออกพื้นที่

๓.๑.๓ มาตรการป้องกันทางเทคนิค ผู้ให้บริการควรจัดให้มีมาตรการในป้องกันสำหรับความมั่นคงปลอดภัยและความน่าเชื่อถือทางเทคนิค เช่น โครงสร้างระบบเสมือน (Virtual infrastructure) และสภาพแวดล้อมของระบบ การควบคุมการเข้าถึง การยืนยันตัวตน การตรวจสอบสิทธิของผู้ใช้งานระบบ ความมั่นคงปลอดภัยเครือข่าย การคุ้มครองข้อมูลและการเข้ารหัส การวิเคราะห์ ออกแบบจัดทำระบบตามวัฏจักรการพัฒนาระบบงาน (System development Life Cycle : SDLC) แนวทางการรักษาความปลอดภัยในการพัฒนาซอฟต์แวร์และ Application Programming Interface (API) และแนวทางในการรักษาความปลอดภัยการจ้างบุคคลภายนอก (Outsourcing)

๓.๒ ประสิทธิภาพการให้บริการ

เพื่อกำหนดหลักเกณฑ์การให้บริการ ผู้ให้บริการควรคำนึงถึงคุณภาพการให้บริการเป็นสำคัญ และควรแสดงรายละเอียดการให้บริการในข้อตกลงระดับการให้บริการ (Service Level Agreement : SLA) โดยมีสาระสำคัญดังต่อไปนี้

๓.๒.๑ ความพร้อมใช้งาน (Availability) ผู้ให้บริการควรแสดงให้ผู้ใช้บริการมั่นใจถึงบริการที่ได้รับ เช่น ร้อยละของเวลาที่พร้อมให้บริการ (Uptime)

๓.๒.๒ ระยะเวลาการตอบสนอง (Response Time) ผู้ให้บริการควรระบุระยะเวลาการตอบสนองต่อเหตุการณ์ ซึ่งเป็นระยะเวลานับแต่ผู้ใช้บริการแจ้งความประสงค์และผู้ให้บริการได้ดำเนินการต่อความประสงค์นั้น โดยระยะเวลาการตอบสนองเป็นหลักการพิจารณาที่สำคัญของผู้ใช้บริการ บางกรณีการตอบสนองล่าช้ากว่ากำหนดส่งผลให้เกิดความเสียหาย

๓.๒.๓ ความสามารถรองรับปริมาณงาน ผู้ให้บริการควรระบุ จำนวนปริมาณการเชื่อมต่อสูงสุดพร้อมกัน จำนวนปริมาณการใช้งานของผู้ใช้บริการพร้อมกัน จำนวนปริมาณทรัพยากรของระบบที่รองรับการใช้งาน และจำนวนงาน (Throughput) เพื่อเป็นข้อมูลสำคัญแก่ผู้ใช้บริการ

๓.๒.๔ การบริการสนับสนุน ผู้ให้บริการควรจัดให้มีช่องทางและกำหนดช่วงเวลาที่ผู้ใช้บริการสามารถแจ้งปัญหา หรือติดต่อสอบถามจากผู้ให้บริการได้ เช่น การกำหนดให้ผู้ใช้บริการสามารถติดต่อผู้ให้บริการได้ตลอด ๒๔ ชั่วโมง และระยะเวลาในการแก้ไขปัญหาการใช้งานตั้งแต่เริ่มต้นจนปัญหานั้นสิ้นสุด

๓.๒.๕ กระบวนการยุติสัญญา กรณีผู้ใช้บริการ หรือผู้ให้บริการต้องการยุติข้อตกลงการให้บริการ ผู้ให้บริการควรดำเนินการตามขั้นตอนที่ได้แจ้งให้ผู้ใช้บริการทราบไว้ก่อนล่วงหน้า เช่น ระยะเวลาสำหรับการเข้าถึงข้อมูลของผู้ใช้บริการ และระยะเวลาการเก็บรักษาข้อมูลของผู้ให้บริการ

๓.๓ การรักษาความมั่นคงปลอดภัย

เพื่อกำหนดหลักเกณฑ์การรักษาความมั่นคงปลอดภัยในระบบสารสนเทศ ผู้ให้บริการควรแสดงรายละเอียดในข้อตกลงระดับการให้บริการ (Service Level Agreement : SLA) โดยมีสาระสำคัญดังต่อไปนี้

๓.๓.๑ ความน่าเชื่อถือของบริการ ผู้ให้บริการควรจัดให้มีการควบคุมความมั่นคงปลอดภัยการบริหารจัดการความต่อเนื่องทางธุรกิจ และการจัดให้มีระบบฉุกเฉินสำรอง โดยอ้างอิงตามมาตรฐานสากล

๓.๓.๒ การพิสูจน์ตัวตนและการอนุญาต ผู้ให้บริการควรจัดให้มีกระบวนการพิสูจน์ตัวตนเพื่อเป็นการตรวจสอบความเป็นตัวตนของผู้มีสิทธิในการเข้าใช้งาน ระยะเวลาเวลาในการดำเนินการเพิ่มหรือถอนสิทธิ์ผู้ใช้งานที่เหมาะสม การป้องกันการเข้าใช้งานจากผู้ที่ไม่มีสิทธิ์ การกำหนด Authentication Level และการควบคุมการอนุญาตการเข้าถึงการใช้งานจากบุคคลภายนอกที่สนับสนุนการให้บริการ (Outsourcing)

๓.๓.๓ การเข้ารหัส ผู้ให้บริการควรจัดให้มีการเข้ารหัสในการแปลงข้อมูลเพื่อปกปิดข้อมูลป้องการเข้าถึง การแก้ไข และการใช้งานโดยไม่ได้รับอนุญาต การกำหนดการเข้ารหัสให้สอดคล้องกับ Data Classification และจัดให้มีนโยบายการควบคุมกุญแจสำหรับการเข้ารหัส (Key Access Control Policy) ตามความเหมาะสม

๓.๓.๔ การรายงานเหตุการณ์และการจัดการรักษาความมั่นคงปลอดภัย เนื่องจากการเกิดเหตุการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูลอาจจะส่งผลต่อความมั่นคงทางธุรกิจ โดยการจัดการเหตุการณ์และการรักษาความมั่นคงปลอดภัยของข้อมูล เริ่มตั้งแต่กระบวนการตรวจพบเหตุการณ์ การรายงานเหตุการณ์ การประเมิน การตอบสนอง การแก้ปัญหา และการเรียนรู้จากเหตุการณ์ความปลอดภัยที่เกิดขึ้น

๓.๓.๕ การบันทึกและการตรวจสอบข้อมูลการใช้งานระบบ ผู้ให้บริการควรจัดให้มีการบันทึกข้อมูลที่เกี่ยวข้องกับการดำเนินการและการใช้งานบริการ Cloud Computing เพื่อให้สามารถตรวจสอบข้อมูลย้อนหลังได้

๓.๓.๖ การตรวจสอบขั้นตอนกระบวนการทำงานและความปลอดภัย ผู้ให้บริการควรจัดให้มีการตรวจสอบกระบวนการทำงานและความปลอดภัยอย่างเป็นระบบ มีความเป็นอิสระ มีขั้นตอนการทำงานที่มีเอกสารหลักฐาน และกำหนดสิทธิของผู้ตรวจสอบภายใน ผู้ตรวจสอบภายนอก เป็นประจำอย่างสม่ำเสมอ โดยหลักฐานการตรวจสอบที่ใช้และหลักเกณฑ์ถูกกำหนดตามข้อกำหนด หรือตามการรับรองในแต่ละประเภทการให้บริการ

๓.๓.๗ การจัดการช่องโหว่ ผู้ให้บริการควรจัดให้มีการตรวจสอบ ประเมิน และบริหารจัดการช่องโหว่ หรือจุดเสี่ยงในระบบ กระบวนการรักษาความปลอดภัยของระบบ การควบคุมภายใน หรือการใช้งานที่อาจถูกนำไปใช้หรือถูกเรียกใช้โดยภัยคุกคาม รวมถึง การทดสอบระบบความปลอดภัย Vulnerability Assessments และ Penetration Testing โดยจะต้องดำเนินการตามมาตรการ และวิธีการที่เหมาะสมเพื่อลดความเสี่ยงในการเกิดความเสียหาย

๓.๓.๘ ธรรมาภิบาล กรณีการเปลี่ยนการให้บริการอันเนื่องมากจากการปรับปรุง อัพเดตซอฟต์แวร์ที่อาจส่งผลกระทบกระบวนการทำงาน ช่องทางการให้บริการหรือรายละเอียดในข้อตกลงการให้บริการผู้ให้บริการควรจัดให้มีการแจ้งให้ผู้ใช้บริการทราบล่วงหน้าในระยะเวลาที่เหมาะสมเพื่อให้ผู้ใช้บริการเตรียมพร้อมในการเปลี่ยนแปลงดังกล่าว

๓.๔ การจัดการข้อมูล

เพื่อกำหนดหลักเกณฑ์ในการบริการจัดการข้อมูล ผู้ให้บริการควรแสดงรายละเอียดในข้อตกลงระดับการให้บริการ (Service Level Agreement : SLA) โดยมีสาระสำคัญดังต่อไปนี้

๓.๔.๑ การจัดประเภทข้อมูล ข้อมูลที่ใช้ใน Cloud Computing ประกอบด้วย ๓ ประเภท ได้แก่ ข้อมูลของผู้ใช้บริการ ข้อมูลของผู้ให้บริการ และข้อมูลที่เกิดจากการประมวลผลข้อมูลของผู้ใช้บริการโดยผู้ให้บริการ (Derived Data) ผู้ให้บริการควรจัดให้มีนโยบายที่เกี่ยวข้องกับการใช้ข้อมูลของผู้ใช้บริการและการกำหนดขอบเขตและแนวปฏิบัติต่อข้อมูลที่ถูกสร้างขึ้นจากข้อมูลของผู้ใช้บริการโดยผู้ให้บริการ และกำหนดสิทธิในการตรวจสอบข้อมูลที่เกิดขึ้นของผู้ใช้บริการ

๓.๔.๒ การจัดเก็บ สำรองข้อมูล และการเรียกคืนข้อมูล ผู้ให้บริการควรจัดให้มีการจัดเก็บสำรองข้อมูลให้อยู่ในสภาพพร้อมใช้งาน โดยกำหนดระยะเวลา ความถี่การดำเนินการ วิธีการ และการเก็บรักษาที่เหมาะสม ในกรณีที่ข้อมูลปัจจุบันถูกทำลายหรือได้รับความเสียหายส่งผลทำให้ไม่สามารถใช้งานได้ ผู้ให้บริการจะต้องดำเนินการเรียกคืนข้อมูลเพื่อให้เกิดความพร้อมในการใช้งานตามที่ระบุไว้ในข้อตกลงการให้บริการ

๓.๔.๓ วงจรชีวิตของข้อมูล ผู้ให้บริการควรจัดให้มีนโยบายและแนวปฏิบัติที่เหมาะสมในการบริหารจัดการข้อมูลอย่างมีประสิทธิภาพและการทำลายข้อมูล

๓.๔.๔ การโอนย้ายข้อมูล กรณียุติข้อตกลงการให้บริการ ผู้ให้บริการควรมีนโยบายและแนวปฏิบัติในการส่งออกข้อมูล โดยกำหนดรูปแบบ กระบวนการส่งออก และอัตราความเร็วขั้นต่ำในการโอนย้ายข้อมูลตามความเหมาะสม การกำหนด Existing Plan

๓.๕ การคุ้มครองข้อมูลส่วนบุคคล

เพื่อกำหนดหลักเกณฑ์และแนวทางการคุ้มครองข้อมูลส่วนบุคคล ผู้ให้บริการควรแสดงรายละเอียดในข้อตกลงระดับการให้บริการ (Service Level Agreement : SLA) โดยมีสาระสำคัญดังต่อไปนี้

๓.๕.๑ แนวปฏิบัติตามมาตรฐานสากล ผู้ให้บริการควรจัดให้มีนโยบาย แนวทางปฏิบัติ มาตรการหรือมาตรฐานที่สอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล

๓.๕.๒ การระบุวัตถุประสงค์ ผู้ให้บริการไม่สามารถดำเนินการกับข้อมูลส่วนบุคคลที่ปราศจากความยินยอมของเจ้าของข้อมูลได้ ทั้งนี้ผู้ให้บริการควรระบุวัตถุประสงค์และความยินยอมในการรวบรวม เก็บรักษา การใช้ และการเปิดเผยข้อมูล ให้ชัดเจน

๓.๕.๓ การเก็บรักษาข้อมูลเท่าที่จำเป็น ผู้ให้บริการควรกำหนดระยะเวลาในการเก็บรักษาข้อมูลชั่วคราวที่เหมาะสม และการกำหนดระยะเวลาในการเก็บรักษาข้อมูลหลังจากมีการแจ้งให้ทำลายข้อมูล โดยควรระบุให้ชัดเจนในข้อตกลงการให้บริการ ทั้งนี้ ผู้ใช้บริการมีหน้าที่รับผิดชอบต้องตรวจสอบว่าข้อมูลส่วนบุคคลที่ถูกทำลายแล้ว (ทั้งผู้ให้บริการ และผู้รับจ้างต่อ) กรณีข้อมูลชั่วคราวที่ถูกสร้างระหว่างการให้บริการและอาจจะไม่ถูกทำลายในทันที เนื่องจากเหตุผลทางเทคนิค อาจจะต้องตรวจสอบระยะเวลาในการทำลายข้อมูลชั่วคราวด้วย

๓.๕.๔ การใช้ เก็บรักษา และการเปิดเผย ผู้ให้บริการควรแจ้งให้ผู้ใช้บริการทราบว่าผู้ให้บริการจะไม่เปิดเผยข้อมูลส่วนบุคคลที่มีการจัดเก็บ รวบรวมไว้ เว้นแต่ได้รับความยินยอมจากผู้ใช้บริการหรือเป็นกรณีที่กฎหมายกำหนดหรือเป็นการเปิดเผยแก่หน่วยงานที่มีอำนาจตามกฎหมาย หรือตามคำสั่งศาล

๓.๕.๕ ความโปร่งใส และการแจ้งเตือน ผู้ให้บริการควรแจ้งให้ผู้ใช้บริการทราบและให้ข้อมูลที่เพียงพอเกี่ยวกับความโปรงใสในการดำเนินการกับข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด

๓.๕.๖ ความรับผิดชอบต่อข้อมูล เนื่องจากความรับผิดชอบด้านสารสนเทศจะเป็นส่วนสำคัญในการตรวจสอบการละเมิดข้อมูลส่วนบุคคล ผู้ให้บริการควรมีนโยบายและแนวปฏิบัติในกรณีการละเมิดข้อมูลและจะต้องมีกระบวนการ เอกสารหลักฐานที่ได้ดำเนินการที่สอดคล้องกับแนวทางการคุ้มครองข้อมูลส่วนบุคคล

๓.๕.๗ สถานที่จัดเก็บข้อมูล การประมวลผลข้อมูลส่วนบุคคลอาจจะถูกโอนย้ายข้อมูลไปยังต่างประเทศซึ่งอาจจะมีกฎหมาย กฎระเบียบหรือระดับความการคุ้มครองข้อมูลส่วนบุคคลที่แตกต่างกัน เพื่อเป็นการลดความเสี่ยงในการถูกละเมิด ผู้ให้บริการควรแสดงให้ผู้ใช้บริการทราบสถานที่ในการจัดเก็บข้อมูลหรือกำหนดให้ผู้ใช้บริการสามารถเลือกสถานที่จัดเก็บข้อมูลได้

๓.๕.๘ การอำนวยความสะดวกในการเข้าถึงข้อมูล ผู้ให้บริการควรอำนวยความสะดวกแก่ผู้ใช้บริการในระยะเวลาที่เหมาะสมและมีประสิทธิภาพ ทั้งนี้ ห้ามมิให้ผู้ให้บริการใช้ข้อกำหนดทางเทคนิคหรือข้อกำหนดขององค์กรเป็นอุปสรรคในการปฏิเสธสิทธิของเจ้าของข้อมูล