



เคียงคู่ผู้กำกับประชาชน

ประกาศธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร
ที่ ๒๑๒ /2566

เรื่อง นโยบายการบริหารจัดการบุคคลภายนอกด้านสารสนเทศ (Third Party Management)

เพื่อให้การบริหารจัดการบุคคลภายนอกด้านสารสนเทศ ของธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร (ธ.ก.ส.) เป็นไปอย่างเหมาะสม มีประสิทธิภาพ เพิ่มขีดความสามารถในการแข่งขันซึ่งจะช่วยสร้างความพึงพอใจต่อผลิตภัณฑ์และบริการให้กับลูกค้า และผู้รับบริการที่ดีขึ้น รวมถึงการสร้างประสิทธิภาพการดำเนินงานที่ดี และเพื่อประกาศใช้และเผยแพร่ นโยบายการบริหารจัดการบุคคลภายนอกด้านสารสนเทศ (Third Party Management) ให้กับผู้บริหาร พนักงาน และผู้ช่วยพนักงานทุกคน ยึดมั่นเป็นหลักการในการที่จะต้องยอมรับและปฏิบัติตามนโยบายฯ ดังนี้

1. องค์ประกอบของนโยบาย

1.1 นโยบายทั่วไป

นโยบายในภาพรวมการบริหารจัดการบุคคลภายนอกด้านสารสนเทศ เพื่อสร้างความมั่นใจว่ามีแนวปฏิบัติการบริหารจัดการบุคคลภายนอกด้านสารสนเทศ รวมทั้งมีการติดตามผล ได้อย่างชัดเจน

1.2 ประเภทการให้บริการจากบุคคลภายนอก

กำหนดประเภทของการให้บริการจากบุคคลภายนอก เพื่อให้ใช้ในการพิจารณาประเภทของบุคคลภายนอก

1.3 การบริหารความเสี่ยง

กำหนดแนวทาง และวิธีการบริหารจัดการความเสี่ยงที่อาจเกิดขึ้นจากการให้บริการจากบุคคลภายนอก รวมทั้งมีการกำกับดูแล ติดตาม และบริหารจัดการความเสี่ยงจากการให้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก

1.4 การนำเทคโนโลยีมาใช้หรือการเปลี่ยนแปลงระบบเทคโนโลยี

กำหนดแนวทางการดำเนินการหากมีการนำเทคโนโลยี หรือเมื่อมีการเปลี่ยนแปลงระบบเทคโนโลยี

1.5 การบริหารจัดการบุคคลภายนอกด้านสารสนเทศ (Third Party Management)

กำหนดแนวทางการบริหารจัดการบุคคลภายนอกด้านสารสนเทศ มีกระบวนการและหลักเกณฑ์ในการคัดเลือกที่ชัดเจน

1.6 การรักษาความลับของระบบและข้อมูล (Confidentiality)

แนวทางการกำกับดูแล เพื่อให้บุคคลภายนอกมีและจัดทำแนวทางหรือมาตรฐานในการรักษาความปลอดภัยและความลับ รวมทั้งต้องมีการติดตาม ตรวจสอบเพื่อให้มั่นใจว่าบุคคลภายนอกสามารถดำเนินการได้ตามแนวทางหรือมาตรฐาน ด้านการรักษาความปลอดภัยและความลับของระบบงานและข้อมูล

1.7 การรักษาความถูกต้องเชื่อถือได้ของระบบงานและข้อมูล (Integrity)

การดำเนินงานให้มั่นใจว่าบุคคลภายนอกมีแนวทางหรือมาตรฐานในการรักษาความถูกต้องเชื่อถือได้ของระบบงานและข้อมูล ซึ่งครอบคลุมตั้งแต่การพัฒนาหรือการเปลี่ยนแปลงแก้ไขระบบงาน การควบคุม ทั้งในส่วนของการบันทึกข้อมูลเข้าสู่ระบบ (Input Validation) การประมวลผล (Processing Control) และการนำข้อมูลออกจากระบบ (Output Control)

11

1.8 ความพร้อมใช้ของงานเทคโนโลยีสารสนเทศที่ใช้บริการ (Availability)

กระบวนการ ขั้นตอน หรือระบบในการติดตาม ประเมินผล และตรวจสอบบุคคลภายนอก เพื่อให้มั่นใจว่า บุคคลภายนอกสามารถดำเนินการได้ตามแนวทางหรือมาตรฐานด้านความพร้อมใช้ของงานเทคโนโลยีสารสนเทศที่ใช้บริการที่ได้ตกลงไว้กับ ธ.ก.ส.

1.9 การคุ้มครองผู้ใช้บริการของ ธ.ก.ส. (Consumer Protection)

กำหนดแนวทางหรือมาตรฐานในการดูแลและป้องกันข้อมูลสำคัญของผู้ใช้บริการของ ธ.ก.ส. โดยควรสอดคล้องกับกฎหมาย ข้อบังคับที่เกี่ยวข้องของทางการ และมาตรฐานสากลที่เกี่ยวข้องกับงานเทคโนโลยีสารสนเทศ รวมทั้ง กำหนดกระบวนการ ขั้นตอน หรือระบบในการติดตาม ประเมินผล และตรวจสอบบุคคลภายนอก เพื่อให้มั่นใจว่าบุคคลภายนอกสามารถดำเนินการได้ตามแนวทางที่ตกลง

1.10 การคุ้มครองข้อมูลส่วนบุคคล (Data Protection)

กำหนดให้บุคคลภายนอกต้องปฏิบัติตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล และนโยบายการคุ้มครองข้อมูลส่วนบุคคลกำหนดให้ผู้ให้บริการภายนอกต้องไม่เปิดเผยข้อมูลส่วนบุคคลที่มีการจัดเก็บรวบรวมไว้ เว้นแต่ได้รับความยินยอมจากผู้ให้บริการหรือเป็นไปตามที่ กฎหมายกำหนด หรือเป็นการเปิดเผยแก่หน่วยงานที่มีอำนาจตามกฎหมาย หรือตามคำสั่งศาล

1.11 การใช้บริการ Cloud Computing

กำหนดข้อตกลงให้บุคคลภายนอกดำเนินการเกี่ยวกับประสิทธิภาพการให้บริการ และมาตรการรักษาความมั่นคงปลอดภัย หากมีการใช้บริการ Cloud Computing

1.12 การกำกับดูแลเพิ่มเติม

แนวทางที่กำหนดเพิ่มเติม กรณีการใช้บริการจากบุคคลภายนอกประเภทที่มีความสำคัญอย่างยิ่ง และประเภทใช้บริการ Cloud Computing เพื่อให้มั่นใจว่าเป็นไปตามกรอบหลักการด้านเทคโนโลยีสารสนเทศ ที่สำคัญ 3 ประการ คือ การรักษาความลับของระบบและข้อมูล (Confidentiality) ความถูกต้อง เชื่อถือได้ของระบบงานและข้อมูล (Integrity) และความพร้อมใช้ของงานเทคโนโลยีสารสนเทศที่ใช้บริการ (Availability)

1.13 การรายงานและการตรวจสอบ

แนวทางการรายงานต่อธนาคารแห่งประเทศไทย (ธปท.) เช่น การรายงานโครงการด้านเทคโนโลยีสารสนเทศที่มีนัยสำคัญ เป็นรายไตรมาส และรายปี รวมทั้งรายงานการนำเทคโนโลยีมาใช้ หรือการเปลี่ยนแปลงระบบหรือเทคโนโลยี ที่มีนัยสำคัญ

ทั้งนี้ จัดเป็นมาตรฐานด้านการบริหารจัดการบุคคลภายนอกด้านสารสนเทศขององค์กร โดยอ้างอิงรายละเอียดจากเอกสาร “นโยบายและวิธีปฏิบัติการบริหารจัดการบุคคลภายนอกด้านสารสนเทศ (Third Party Management)” เพื่อใช้เป็นแนวทางในการดำเนินการเกี่ยวกับการกำกับดูแล การบริหารจัดการ ความเสี่ยง และการควบคุมความเสี่ยงที่อาจเกิดขึ้น เนื่องจากบุคคลภายนอกที่มีการเชื่อมต่อกับระบบเทคโนโลยีสารสนเทศของ ธ.ก.ส. หรือสามารถเข้าถึงข้อมูลสำคัญของ ธ.ก.ส. ได้ ซึ่งให้ผู้บริหาร พนักงาน และผู้ช่วยพนักงานและหน่วยงานภายนอกต้องถือปฏิบัติตามอย่างเคร่งครัดต่อไป

2. ต้องมีการดำเนินการตรวจสอบประเมิน รวมทั้งจัดให้มีการทบทวนนโยบายการบริหารจัดการบุคคลภายนอก และวิธีปฏิบัติอย่างน้อยปีละหนึ่งครั้ง หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เพื่อให้มั่นใจว่านโยบายดังกล่าวเหมาะสมกับสภาพแวดล้อมการดำเนินงานขององค์กร

จึงประกาศมาเพื่อทราบทั่วกัน

ประกาศ ณ วันที่ ๕ มีนาคม พ.ศ. 2566



(นายจรรยเดช เจนจรัสกุล)

ประธานอนุกรรมการบริหารเทคโนโลยีดิจิทัล
ธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร