ธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร
2346 ถนนพหลโยธิน แขวงเสนานิคม เขตจตุจักร กรุงเทพมหานคร 10900

ประกาศธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร
ที่ 199 /2569
เรื่อง นโยบายการบริหารจัดการบุคคลภายนอก
(Third Party Management Policy)

เพื่อให้การบริหารจัดการบุคคลภายนอก ในที่นี้หมายถึง บุคคลภายนอกซึ่งเป็นผู้ให้บริการด้านเทคโนโลยีสารสนเทศของ ธ.ก.ส. ตามนิยามในประกาศของธนาคารแห่งประเทศไทย เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยด้านสารสนเทศที่ครอบคลุมในมิติของการรักษาความลับ (Confidentiality) การรักษาความถูกต้องเชื่อถือได้ (Integrity) และการรักษาสภาพพร้อมใช้งาน (Availability) เพิ่มขีดความสามารถในการแข่งขันซึ่งจะช่วยสร้างความพึงพอใจต่อผลิตภัณฑ์และบริการให้กับลูกค้า และผู้รับบริการที่ดีขึ้น รวมถึงการสร้างประสิทธิผลการดำเนินงานที่ดี และเพื่อประกาศ ใช้และเผยแพร่นโยบายการบริหารจัดการบุคคลภายนอก (Third Party Management) ให้กับผู้บริหาร พนักงาน และผู้ช่วยพนักงานทุกคน ยึดมั่นเป็นหลักการในการที่จะต้องยอมรับและปฏิบัติ ดังนี้

1. นโยบายการบริหารจัดการบุคคลภายนอก

ต้องมีการกำหนดนโยบายในภาพรวมการบริหารจัดการบุคคลภายนอก เพื่อสร้างความมั่นใจว่ามีแนวปฏิบัติการบริหารจัดการบุคคลภายนอก รวมทั้งมีการติดตามผล ได้อย่างชัดเจน รวมทั้งจัดให้มีการทบทวนนโยบายการบริหารจัดการบุคคลภายนอกสารสนเทศและวิธีปฏิบัติอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เพื่อให้มั่นใจว่านโยบายดังกล่าวเหมาะสมกับสภาพแวดล้อมการดำเนินงานขององค์กร

2. ประเภทการใช้บริการจากบุคคลภายนอก

ต้องมีการกำหนดประเภทของการใช้บริการจากบุคคลภายนอก เพื่อให้ใช้ในการพิจารณาประเภทของบุคคลภายนอก

3. การบริหารความเสี่ยง

ต้องมีการกำหนดแนวทาง และวิธีการบริหารจัดการความเสี่ยงที่อาจเกิดขึ้นจากการใช้บริการจากบุคคลภายนอก รวมทั้งมีการกำกับดูแล ติดตาม และบริหารจัดการความเสี่ยงจากการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก

4. การนำเทคโนโลยีมาใช้หรือการเปลี่ยนแปลงระบบเทคโนโลยี

ต้องมีการกำหนดแนวทางการดำเนินการหากมีการนำเทคโนโลยีมาใช้ หรือเมื่อมีการเปลี่ยนแปลงระบบเทคโนโลยี

5. การบริหารจัดการบุคคลภายนอก (Third Party Management)

ต้องมีการกำหนดแนวทางการบริหารจัดการบุคคลภายนอก มีกระบวนการและหลักเกณฑ์ในการคัดเลือกที่ชัดเจน

6. การรักษาความลับของระบบและข้อมูล (Confidentiality)

ต้องมีการกำหนดแนวทางการกำกับดูแล เพื่อให้บุคคลภายนอกมีและจัดทำแนวทางหรือมาตรฐานในการรักษาความปลอดภัยและความลับ รวมทั้งต้องมีการติดตาม ตรวจสอบเพื่อให้มั่นใจว่าบุคคลภายนอกสามารถดำเนินการได้ตามแนวทางหรือมาตรฐาน ด้านการรักษาความปลอดภัยและความลับของระบบงานและข้อมูล

7. การรักษาความถูกต้องเชื่อถือได้ของระบบงานและข้อมูล (Integrity)

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

8. การรักษาความพร้อมใช้ของงานเทคโนโลยีสารสนเทศที่ใช้บริการ (Availability)

ต้องมีการกำหนดกระบวนการ ขั้นตอน หรือระบบในการติดตาม ประเมินผล และตรวจสอบบุคคลภายนอก เพื่อให้มั่นใจว่า บุคคลภายนอกสามารถดำเนินการได้ตามแนวทางหรือมาตรฐานด้านความพร้อมใช้ของงานเทคโนโลยีสารสนเทศที่ให้บริการที่ได้ตกลงไว้กับ ธ.ก.ส.

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

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

10. การคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection)

กำหนดให้บุคคลภายนอกต้องปฏิบัติตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล และนโยบายการคุ้มครองข้อมูลส่วนบุคคลกำหนดให้ผู้ให้บริการภายนอกต้องไม่เปิดเผยข้อมูลส่วนบุคคลที่มีการจัดเก็บรวบรวมไว้ เว้นแต่ได้รับความยินยอมจากผู้ใช้บริการหรือเป็นไปตามที่กฎหมายกำหนด หรือเป็นการเปิดเผยแก่หน่วยงานที่มีอำนาจตามกฎหมาย หรือตาม คำสั่งศาล

11. การใช้บริการคลาวด์ (Cloud Computing)

หากมีการใช้บริการ Cloud Computing ต้องมีการกำหนดข้อตกลงให้บุคคลภายนอกดำเนินการเกี่ยวกับประสิทธิภาพการให้บริการ และมาตรการรักษาความมั่นคงปลอดภัย รวมถึงการปฏิบัติตามมาตรฐานการรักษาความมั่นคงปลอดภัยที่กฎหมายกำหนด

12. การกำกับดูแลเพิ่มเติม

ต้องมีการกำหนดแนวทางเพิ่มเติม กรณีการใช้บริการจากบุคคลภายนอกประเภทที่มีความสำคัญอย่างยิ่ง และประเภทใช้บริการ Cloud Computing เพื่อให้มั่นใจว่าเป็นไปตามกรอบหลักการด้านเทคโนโลยีสารสนเทศ ที่สำคัญ 3 ประการ คือ การรักษาความลับของระบบและข้อมูล (Confidentiality) ความถูกต้องเชื่อถือได้ของระบบงานและข้อมูล (Integrity) และความพร้อมใช้ของงานเทคโนโลยีสารสนเทศที่ใช้บริการ (Availability)

13. การรายงานและการตรวจสอบ

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

14. การใช้บริการระบบปัญญาประดิษฐ์ของบุคคลภายนอก

ใช้ระบบปัญญาประดิษฐ์ของบุคคลภายนอกที่รับความเห็นชอบอย่างเป็นทางการเท่านั้น ต้องมีการกำหนดแนวทางการใช้ระบบปัญญาประดิษฐ์ของบุคคลภายนอก อย่างมั่นคงปลอดภัย เหมาะสม มีประสิทธิภาพ และปฏิบัติตามกฎหมาย กฎระเบียบข้อบังคับที่เกี่ยวข้อง และต้องมีการเสริมสร้างความตระหนักรู้และความเข้าใจเกี่ยวกับการใช้ระบบปัญญาประดิษฐ์ของบุคคลภายนอกให้สามารถใช้งานได้อย่างถูกต้องเหมาะสมและเป็นไปตามแนวทาง ธ.ก.ส. กำหนด

ทั้งนี้ จัดเป็นมาตรฐานด้านการบริหารจัดการบุคคลภายนอกขององค์กร โดยอ้างอิงรายละเอียดจากเอกสาร “นโยบายและวิธีปฏิบัติการบริหารจัดการบุคคลภายนอก (Third Party Management)” เพื่อใช้เป็นแนวทางในการดำเนินการเกี่ยวกับการกำกับดูแล การบริหารจัดการความเสี่ยง และการควบคุมความเสี่ยงที่อาจเกิดขึ้น เนื่องจากบุคคลภายนอกที่มีการเชื่อมต่อกับระบบเทคโนโลยีสารสนเทศของ ธ.ก.ส. หรือสามารถเข้าถึงข้อมูลสำคัญของ ธ.ก.ส. ได้ ซึ่งให้ผู้บริหาร พนักงาน และผู้ช่วยพนักงานและหน่วยงานภายนอกต้องถือปฏิบัติตามอย่างเคร่งครัดต่อไป

ธ.ก.ส. จัดให้มีการทบทวนนโยบายการบริหารจัดการบุคคลภายนอกอย่างน้อยปีละครั้ง หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เพื่อให้มั่นใจว่านโยบายดังกล่าวเหมาะสมกับสภาพแวดล้อมการดำเนินงานขององค์กร

จึงประกาศมาเพื่อทราบทั่วกัน

ประกาศ ณ วันที่ ๕ มกราคม ๒๕๖๙

(นายฉัตรชัย ศิริไล)
ผู้จัดการ
ธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร

สำนักรักษาความมั่นคงปลอดภัยเทคโนโลยีและสารสนเทศ