ธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร
BANK FOR AGRICULTURE AND AGRICULTURAL COOPERATIVES
2346 ถนนพหลโยธิน แขวงเสนานิคม เขตจตุจักร กรุงเทพฯ 10900 โทร. 0 2558 6555 แฟกซ์ : 0 2558 6341
2346 Phaholyothin Rd., Senanikom, Chatuchak, Bangkok 10900 www.baac.or.th
เคียงคู่รู้ค่าประชาชน

ประกาศธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร
ที่ ๖๙๓ /2566
เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

เพื่อให้ระบบเทคโนโลยีสารสนเทศของ ธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร (ธ.ก.ส.) เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหา ที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่าง ๆ ซึ่งอาจก่อให้เกิดความเสียหายแก่ ธ.ก.ส. และส่วนงานในสังกัด เพื่อให้ ธ.ก.ส. สามารถบริหารจัดการการรักษาความมั่นคงปลอดภัยด้านสารสนเทศได้อย่างมีประสิทธิภาพ และครอบคลุมการดำเนินงานของ ธ.ก.ส. ในทุกกิจกรรมที่เกี่ยวข้องกับการใช้เทคโนโลยีสารสนเทศ และเพื่อประกาศใช้และเผยแพร่นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้กับผู้บริหาร พนักงาน และผู้ช่วยพนักงานทุกคน ยึดมั่นเป็นหลักการในการที่จะต้องยอมรับและปฏิบัติตามนโยบายฯ ดังนี้

1. องค์ประกอบของนโยบาย

1.1 บทที่ 1 นโยบายการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Policy)

นโยบายในภาพรวมของการรักษาความมั่นคงปลอดภัย เพื่อสร้างความมั่นใจว่าองค์กรจะได้รับการปกป้องและการรักษาความมั่นคงปลอดภัยจากภาวะคุกคามต่าง ๆ มีการกำหนดทิศทางของนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ที่ชัดเจนที่สนับสนุนและมีการนำไปใช้จริง ให้เกิดความมั่นคงปลอดภัยต่อระบบสารสนเทศ

1.2 บทที่ 2 นโยบายโครงสร้างทางด้านความมั่นคงปลอดภัยสารสนเทศ (Organizational of Information Security)

การบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของ ธ.ก.ส. อย่างเป็นระบบมีการจัดโครงสร้างของหน่วยงานภายใน ที่มีส่วนเกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศ อย่างเหมาะสม ของพนักงาน และลูกจ้าง รวมถึงการกำหนดบทบาทและสิทธิหน้าที่ที่มีต่อข้อมูลของผู้ที่มีส่วนเกี่ยวข้องในฐานะต่าง ๆ ตลอดจนความเข้าใจและตระหนักถึงหน้าที่ด้านความมั่นคงปลอดภัยของข้อมูล

1.3 บทที่ 3 นโยบายการรักษาความปลอดภัยด้านทรัพยากรมนุษย์ (Human Resource Security)

การกำหนดกระบวนการบริหารจัดการทรัพยากรด้านบุคลากร เพื่อให้เข้าใจในหน้าที่ความรับผิดชอบของตนเอง ต้องตระหนักและปฏิบัติตามหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ

1.4 บทที่ 4 นโยบายการบริหารจัดการทรัพย์สิน (Asset Management)

การดูแลรักษา ปกป้องสินทรัพย์หรือทรัพย์สิน รวมถึงข้อมูลด้านสารสนเทศอย่างเหมาะสม โดยการกำหนดกฎระเบียบ หรือหลักเกณฑ์ วิธีปฏิบัติ อย่างเป็นลายลักษณ์อักษรสำหรับการใช้งานสารสนเทศและทรัพย์สินสารสนเทศ ต้องมีการเก็บรักษาทรัพย์สินที่มีความสำคัญอย่างเป็นระเบียบ ในสถานที่ที่ปลอดภัยให้เหมาะสม

1.5 บทที่ 5 นโยบายการควบคุมการเข้าถึง (Access Control)

การกำหนดมาตรการควบคุมการเข้าถึงของบุคคลที่ไม่ได้รับอนุญาตให้เข้าถึงซึ่งระบบสารสนเทศ และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก จากโปรแกรมชุดคำสั่งไม่พึงประสงค์ และภัยคุกคามต่าง ๆ ที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบสารสนเทศให้หยุดชะงัก และทำให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบสารสนเทศได้

1.6 บทที่ 6 นโยบายการเข้ารหัสข้อมูล (Cryptography)

การกำหนดแนวทางมาตรการเข้ารหัสข้อมูลอย่างเหมาะสมเพื่อป้องกันความลับ การปลอมแปลง หรือความถูกต้องเชื่อถือได้ของสารสนเทศ

1.7 บทที่ 7 นโยบายความมั่นคงปลอดภัยทางด้านกายภาพและสภาพแวดล้อม (Physical and Environmental Security)

แนวทางการแก้ไขปัญหาที่เกิดขึ้นจากการสูญหาย การรั่วไหลของระบบสารสนเทศ ในส่วนที่เกี่ยวข้องกับสิ่งซึ่งเป็นรูปธรรมจับต้องได้ในระบบ เช่น อุปกรณ์และสื่อจัดเก็บข้อมูล อาคารที่ตั้งของระบบบริหารจัดการตลอดจนระบบข้อมูล และเทคโนโลยีสารสนเทศที่เกี่ยวข้อง เป็นต้น

1.8 บทที่ 8 นโยบายความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operation Security)

แนวทางการปฏิบัติงานกับอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและมีความมั่นคงปลอดภัย เป็นแนวทางในกำหนดการสำรองข้อมูล เพื่อใช้ในการกู้ระบบในกรณีที่เกิดเหตุต่าง ๆ โดยมีการเก็บหลักฐานหรือบันทึกเหตุการณ์ เพื่อใช้เป็นหลักฐานยืนยัน และเพื่อสร้างความมั่นคงปลอดภัยให้กับซอฟต์แวร์สำหรับระบบสารสนเทศ รวมทั้งสารสนเทศในระบบ ลดความเสี่ยงจากการโจมตีโดยอาศัยช่องโหว่ทางเทคนิคที่มีการเผยแพร่หรือตีพิมพ์ในสถานที่ต่าง ๆ และมีกระบวนการตรวจสอบระบบสารสนเทศทั้งหมด มีผลกระทบน้อยที่สุดต่อการดำเนินงาน

1.9 บทที่ 9 นโยบายความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications Security)

แนวทางในการป้องกันข้อมูลในระบบเครือข่าย และป้องกันโครงสร้างพื้นฐานที่สนับสนุนระบบเครือข่ายของ ธ.ก.ส. ให้มีวิธีการรักษาความมั่นคงปลอดภัยของสารสนเทศที่มีการถ่ายโอนข้อมูลกันภายในและภายนอก

1.10 บทที่ 10 นโยบายการจัดหา พัฒนา และดูแลระบบสารสนเทศ (Systems Acquisition, Development and Maintenance)

แนวทางในการดำเนินการเพื่อให้มั่นใจได้ว่าการพัฒนาระบบงานสนับสนุนธุรกิจ คำนึงถึงความมั่นคงปลอดภัยและการควบคุมที่เพียงพอ ต้องกำหนดให้มีการพิจารณาความต้องการด้านความมั่นคงปลอดภัยของระบบงาน ก่อนที่จะมีการพัฒนาระบบ รวมถึงการกำหนดให้มีการควบคุมภายในระบบงาน

1.11 บทที่ 11 นโยบายความสัมพันธ์กับบุคคลภายนอก (Supplier Relationships)

การป้องกันสินทรัพย์ของ ธ.ก.ส. ที่บุคคลภายนอกสามารถเข้าถึง และมีการรักษาไว้ซึ่งระดับความมั่นคงปลอดภัย และระบบการให้บริการตามที่ตกลงกันไว้ในข้อตกลงการให้บริการของบุคคลภายนอก

1.12 บทที่ 12 นโยบายการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management)

เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยต่อระบบสารสนเทศได้รับการดำเนินการที่ถูกต้องในช่วงระยะเวลาที่เหมาะสม

1.13 บทที่ 13 นโยบายการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ (Information Security - Aspects of Business Continuity Management)

แนวทางเพื่อป้องกันการหยุดชะงักในการดำเนินงานที่เกิดจากความล้มเหลวหรือระบบหยุดทำงาน และเพื่อจัดเตรียมสภาพความพร้อมใช้งานของข้อมูลและอุปกรณ์ประมวลผลระบบสารสนเทศ โดยครอบคลุมการเข้าถึงและการพิสูจน์ตัวตนผู้ใช้ การรักษาความลับของข้อมูล การรักษาความถูกต้องเชื่อถือได้ของระบบสารสนเทศ

1.14 บทที่ 14 นโยบายการปฏิบัติตามข้อกำหนดทางด้านกฎหมาย และบทลงโทษของการละเมิดนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Compliance)

การลดความเสี่ยงที่เกิดจากการละเมิดข้อบังคับทางกฎหมาย ทรัพย์สินทางปัญญา ที่เกี่ยวข้องกับการดำเนินธุรกิจ พนักงาน และลูกจ้างทุกคนต้องทราบถึงข้อกำหนดต่าง ๆ ที่เกี่ยวข้องกับการใช้งานทรัพย์สินด้านสารสนเทศ เป็นการสร้างความตระหนักถึงความเสี่ยงที่อาจเกิดขึ้น

1.15 บทที่ 15 นโยบายการเตรียมความพร้อมด้านการรับมือกับภัยคุกคามด้านไซเบอร์ (Cyber Resilience)

แนวทางการปฏิบัติเพื่อให้มีการบริหารจัดการและกำกับดูแลความเสี่ยงด้านภัยไซเบอร์ รวมทั้งเตรียมความพร้อมที่จะรับมือและแก้ไขได้อย่างเหมาะสม เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ดำเนินการได้อย่างมีประสิทธิภาพ สอดคล้องกับมาตรฐานสากล

ทั้งนี้ จัดเป็นมาตรฐานด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศขององค์กร โดยอ้างอิงรายละเอียดจากเอกสาร “นโยบายและวิธีปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ” เพื่อใช้เป็นแนวทางในการดำเนินงานด้วยวิธีทางอิเล็กทรอนิกส์ให้มีความมั่นคงปลอดภัย เชื่อถือได้ และเป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง ซึ่งผู้บริหาร พนักงาน และผู้ช่วยพนักงานและหน่วยงานภายนอกต้องถือปฏิบัติตามอย่างเคร่งครัดต่อไป

2. ต้องมีการดำเนินการตรวจสอบประเมิน รวมทั้งจัดให้มีการทบทวนนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและวิธีปฏิบัติอย่างน้อยปีละหนึ่งครั้ง หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เพื่อให้มั่นใจว่านโยบายดังกล่าวเหมาะสมกับสภาพแวดล้อมการดำเนินงานขององค์กร

จึงประกาศมาเพื่อทราบทั่วกัน

ประกาศ ณ วันที่ 8 มีนาคม พ.ศ. 2566

(นายจรูญเดช เจนจรัสสกุล)
ประธานอนุกรรมการบริหารเทคโนโลยีดิจิทัล
ธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร