ธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร
2346 ถนนพหลโยธิน แขวงเสนานิคม เขตจตุจักร กรุงเทพมหานคร 10900

ประกาศธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร
ที่ ๒๐๐ /2569
เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
(Information Security Policy)

เพื่อให้ระบบเทคโนโลยีสารสนเทศของ ธ.ก.ส. เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยด้านสารสนเทศที่ครอบคลุมในมิติของการรักษาความลับ (Confidentiality) การรักษาความถูกต้องเชื่อถือได้ (Integrity) และการรักษาสภาพพร้อมใช้งาน (Availability) รวมทั้งป้องกันความเสี่ยง ที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่าง ๆ ซึ่งอาจก่อให้เกิดความเสียหายแก่ ธ.ก.ส. และส่วนงานในสังกัด เพื่อให้ ธ.ก.ส. สามารถบริหารจัดการการรักษาความมั่นคงปลอดภัยด้านสารสนเทศได้อย่างมีประสิทธิภาพ และครอบคลุมการดำเนินงานของ ธ.ก.ส. ในทุกกิจกรรมที่เกี่ยวข้องกับการใช้เทคโนโลยีสารสนเทศ และเพื่อประกาศใช้และเผยแพร่นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้กับผู้บริหาร พนักงาน และผู้ช่วยพนักงานทุกคน ยึดมั่นเป็นหลักการในการที่จะต้องยอมรับและปฏิบัติ ดังนี้

1. นโยบายการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Policy)

ต้องมีการกำหนดนโยบายในภาพรวมของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่ชัดเจนและมีการนำไปใช้จริง เพื่อให้มั่นใจว่า ธ.ก.ส. จะได้รับการปกป้องและการรักษาความปลอดภัยของระบบสารสนเทศจากภาวะภัยคุกคามไซเบอร์ และต้องมีการดำเนินการตรวจสอบและประเมินผล รวมทั้งจัดให้มีการทบทวนนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและวิธีปฏิบัติอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เพื่อให้มั่นใจว่านโยบายดังกล่าวเหมาะสมกับสภาพแวดล้อมการดำเนินงานขององค์กร

2. โครงสร้างทางด้านความมั่นคงปลอดภัยสารสนเทศ (Organizational of Information Security)

ต้องมีการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของ ธ.ก.ส. อย่างเป็นระบบ มีการจัดโครงสร้างของหน่วยงานภายในที่มีส่วนเกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศอย่างเหมาะสม รวมถึงการกำหนดบทบาทและสิทธิหน้าที่พนักงาน ลูกจ้าง ผู้ที่มีส่วนเกี่ยวข้องต่อข้อมูลในฐานะต่าง ๆ ตลอดจนสร้างความเข้าใจและตระหนักถึงหน้าที่ด้านความมั่นคงปลอดภัยของข้อมูล

3. การรักษาความปลอดภัยด้านทรัพยากรมนุษย์ (Human Resource Security)

ต้องมีการกำหนดกระบวนการบริหารจัดการทรัพยากรด้านบุคลากร เพื่อให้เข้าใจในหน้าที่ความรับผิดชอบของตนเอง ต้องตระหนักและปฏิบัติตามหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ

4. การบริหารจัดการทรัพย์สิน (Asset Management)

ต้องมีการดูแลรักษา ปกป้องสินทรัพย์หรือทรัพย์สิน รวมถึงข้อมูลด้านสารสนเทศอย่างเหมาะสม โดยการกำหนดกฎระเบียบ หรือหลักเกณฑ์ วิธีปฏิบัติ อย่างเป็นลายลักษณ์อักษรสำหรับการใช้งานสารสนเทศและทรัพย์สินสารสนเทศ ต้องมีการเก็บรักษาทรัพย์สินที่มีความสำคัญอย่างเป็นระเบียบ ในสถานที่ที่ปลอดภัย ให้เหมาะสมรวมถึงการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ มาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำ และแผนการรักษาความมั่นคงปลอดภัยไซเบอร์แก่ข้อมูลหรือระบบสารสนเทศ

5. การควบคุมการเข้าถึง (Access Control)

ต้องมีการกำหนดมาตรการควบคุมการเข้าถึงของบุคคลที่ไม่ได้รับอนุญาตให้เข้าถึงระบบสารสนเทศและป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก จากโปรแกรมชุดคำสั่งไม่พึงประสงค์ และภัยคุกคามต่าง ๆ ที่จะสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบสารสนเทศให้หยุดชะงัก และทำให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบสารสนเทศได้

6. การเข้ารหัสข้อมูล (Cryptography)

ต้องมีการกำหนดแนวทางมาตรการเข้ารหัสข้อมูลอย่างเหมาะสม เพื่อป้องกันความลับ การปลอมแปลง หรือความถูกต้องเชื่อถือได้ของสารสนเทศ

7. ความมั่นคงปลอดภัยทางด้านกายภาพและสภาพแวดล้อม (Physical and Environmental Security)

ต้องมีการกำหนดแนวทางการแก้ไขปัญหาที่เกิดขึ้นจากการสูญหาย การรั่วไหลของระบบสารสนเทศ ในส่วนที่เกี่ยวข้องกับสิ่งซึ่งเป็นรูปธรรมจับต้องได้ในระบบ เช่น อุปกรณ์และสื่อจัดเก็บข้อมูล อาคารที่ตั้งของระบบบริหารจัดการ ตลอดจนระบบข้อมูล และเทคโนโลยีสารสนเทศที่เกี่ยวข้อง เป็นต้น

8. ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operation Security)

ต้องมีการกำหนดแนวทางการปฏิบัติงานกับอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและมีความมั่นคงปลอดภัย มีแนวทางในกำหนดการสำรองข้อมูล เพื่อใช้ในการกู้ระบบในกรณีที่เกิดเหตุต่าง ๆ โดยมีการเก็บหลักฐานหรือบันทึกเหตุการณ์ เพื่อใช้เป็นหลักฐานยืนยัน และเพื่อสร้างความมั่นคงปลอดภัยให้กับซอฟต์แวร์สำหรับระบบสารสนเทศ รวมทั้งสารสนเทศในระบบ ลดความเสี่ยงจากการโจมตีโดยอาศัยช่องโหว่ทางเทคนิคที่มีการเผยแพร่หรือตีพิมพ์ในสถานที่ต่าง ๆ และมีกระบวนการตรวจสอบระบบสารสนเทศทั้งหมดมีผลกระทบน้อยที่สุดต่อการดำเนินงาน

9. ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications Security)

ต้องมีแนวทางในการป้องกันข้อมูลในระบบเครือข่าย และป้องกันโครงสร้างพื้นฐานที่สนับสนุนระบบเครือข่ายของ ธ.ก.ส. ให้มีวิธีการรักษาความมั่นคงปลอดภัยของสารสนเทศที่มีการถ่ายโอนข้อมูลกันทั้งภายในและภายนอก

10. การจัดหา พัฒนา และดูแลระบบสารสนเทศ (Systems Acquisition, Development and Maintenance)

ต้องมีแนวทางในการดำเนินการเพื่อให้มั่นใจได้ว่าการพัฒนาระบบงานสนับสนุนธุรกิจคำนึงถึงความมั่นคงปลอดภัยและการควบคุมที่เพียงพอ ต้องกำหนดให้มีการพิจารณาความต้องการด้านความมั่นคงปลอดภัยของระบบงาน ก่อนที่จะมีการพัฒนาระบบ รวมถึงการกำหนดให้มีการควบคุมภายในระบบงาน

11. ความสัมพันธ์กับบุคคลภายนอก (Supplier Relationships)

ต้องมีการป้องกันสินทรัพย์ของ ธ.ก.ส. ที่บุคคลภายนอกสามารถเข้าถึง และมีการรักษาไว้ซึ่งระดับความมั่นคงปลอดภัย และระบบการให้บริการตามที่ตกลงกันไว้ในข้อตกลงการให้บริการของบุคคลภายนอก

12. การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management)

ต้องมีการกำหนดแนวทางในการบริการจัดการเหตุการณ์ผิดปกติที่เกี่ยวข้องกับความมั่นคงปลอดภัยต่อระบบสารสนเทศ ให้ได้รับการดำเนินการที่ถูกต้องในช่วงระยะเวลาที่เหมาะสม และมีการรายงานต่อธนาคารแห่งประเทศไทย (ธปท.) หากปัญหาหรือเหตุการณ์ด้านเทคโนโลยีสารสนเทศซึ่งส่งผลกระทบต่อการให้บริการ ระบบงาน หรือชื่อเสียง ที่มีนัยสำคัญ

13. การบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ (Information Security-Aspects of Business Continuity Management)

ต้องมีการกำหนดแนวทางเพื่อป้องกันการหยุดชะงักในการดำเนินงานที่เกิดจากความล้มเหลวหรือระบบหยุดทำงาน และเพื่อจัดเตรียมสภาพความพร้อมใช้งานของข้อมูลและอุปกรณ์ประมวลผลระบบสารสนเทศ โดยครอบคลุมการเข้าถึงและการพิสูจน์ตัวตนผู้ใช้ การรักษาความลับของข้อมูล การรักษาความถูกต้องเชื่อถือได้ของระบบสารสนเทศ

14. การปฏิบัติตามข้อกำหนดทางด้านกฎหมาย และบทลงโทษของการละเมิดนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Compliance)

ต้องมีการกำหนดแนวทางเพื่อลดความเสี่ยงที่เกิดจากการละเมิดข้อบังคับทางกฎหมาย ทรัพย์สินทางปัญญา ที่เกี่ยวข้องกับการดำเนินธุรกิจ พนักงาน และลูกจ้างทุกคนต้องทราบถึงข้อกำหนดต่าง ๆ ที่เกี่ยวข้องกับการใช้งานทรัพย์สินด้านสารสนเทศ รวมถึงการสร้างความตระหนักถึงความเสี่ยงที่อาจเกิดขึ้น

15. การเตรียมความพร้อมด้านการรับมือกับภัยคุกคามด้านไซเบอร์ (Cyber Resilience)

ต้องมีแนวทางการปฏิบัติเพื่อให้มีการบริหารจัดการและกำกับดูแลความเสี่ยงด้านภัยไซเบอร์ รวมทั้งเตรียมความพร้อมที่จะรับมือและแก้ไขได้อย่างเหมาะสม เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ดำเนินการได้อย่างมีประสิทธิภาพ สอดคล้องกับมาตรฐานสากล รวมถึงการปฏิบัติตามกฎหมายและประกาศที่เกี่ยวข้อง

16. การรักษาความมั่นคงปลอดภัยระบบปัญญาประดิษฐ์

ต้องมีการรักษาความมั่นคงปลอดภัยตลอดวงจรชีวิตของระบบปัญญาประดิษฐ์ ตั้งแต่การออกแบบ การพัฒนา การติดตั้งใช้งาน การดำเนินงานและบำรุงรักษา จนถึงการกำจัดและทำลาย โดยมุ่งเน้นที่การป้องกันระบบปัญญาประดิษฐ์จากการถูกโจมตี การรักษาความมั่นคงปลอดภัยของข้อมูล โมเดล แอปพลิเคชันและโครงสร้างพื้นฐานการใช้ระบบปัญญาประดิษฐ์ ปฏิบัติตามกฎหมาย กฎระเบียบข้อบังคับที่เกี่ยวข้อง และการเสริมสร้างความตระหนักรู้และความเข้าใจในการใช้งานระบบปัญญาประดิษฐ์ให้มีความปลอดภัย

17. การรักษาความมั่นคงปลอดภัยเว็บไซต์

ต้องมีการกำหนดคุณลักษณะความมั่นคงปลอดภัยให้กับข้อมูลหรือสารสนเทศของเว็บไซต์ และกำหนดมาตรการและแนวทางการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ให้สอดคล้องกับกฎระเบียบข้อบังคับที่เกี่ยวข้อง มีการประเมินตนเองเพื่อตรวจสอบสถานะความมั่นคงปลอดภัยสำหรับเว็บไซต์ อย่างน้อยปีละ 1 ครั้ง และให้รายงานผลต่อฝ่ายจัดการและหน่วยงานควบคุมกำกับดูแลที่เกี่ยวข้อง

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

ธ.ก.ส. จัดให้มีการทบทวนนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างน้อยปีละครั้ง หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เพื่อให้มั่นใจว่านโยบายดังกล่าวเหมาะสมกับสภาพแวดล้อมการดำเนินงานขององค์กร

จึงประกาศมาเพื่อทราบทั่วกัน

ประกาศ ณ วันที่ ๕ มกราคม ๒๕๖๑

(นายฉัตรชัย ศิริไล)
ผู้จัดการ
ธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร