ประกาศ สหกรณ์ออมทรัพย์กรมการพัฒนาชุมชน จำกัด
เรื่อง นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และข้อมูลส่วนบุคคล

****

โดยที่ ระเบียบสหกรณ์ออมทรัพย์กรมการพัฒนาชุมชน จำกัด ว่าด้วยวิธีปฏิบัติการควบคุมภายในและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของสหกรณ์ พ.ศ. 2565 ข้อ 8 (1) สหกรณ์ต้องจัดทำนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศสำหรับระบบสารสนเทศของสหกรณ์ให้เป็นลายลักษณ์อักษร ดังนั้น-เพื่อให้การใช้เทคโนโลยีสารสนเทศของสหกรณ์ออมทรัพย์กรมการพัฒนาชุมชน จำกัด มีความมั่นคงปลอดภัย มีความน่าเชื่อถือ และสามารถป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้เครื่องคอมพิวเตอร์ ระบบเครือข่าย และระบบสารสนเทศ ตามที่กำหนดไว้ในพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 โดยคำนึงถึงความสำคัญของการคุ้มครอง ข้อมูลส่วนบุคคล ซึ่งเป็นข้อมูลที่มีความละเอียดอ่อนและต้องได้รับการดูแลอย่างเข้มงวดตามที่กำหนดไว้ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จึงทบทวนและปรับปรุงนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ เพื่อเสริมสร้างความมั่นคงปลอดภัย ไซเบอร์ของสหกรณ์ฯ ให้เกิดความสมบูรณ์ ทันสมัย และมีประสิทธิภาพสูงสุด และให้สอดคล้องกับปัจจัยสำคัญที่เปลี่ยนแปลงไป ทั้งในด้านกลยุทธ์และทิศทางธุรกิจ ตลอดจนแผนการเปลี่ยนผ่านสู่ดิจิทัลอย่างเหมาะสม และตอบสนองต่อข้อบังคับและกฎหมายที่เปลี่ยนแปลง โดยมุ่งเน้นการปฏิบัติตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) และกฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างเคร่งครัด

อาศัยอำนาจตามข้อบังคับสหกรณ์ออมทรัพย์กรมการพัฒนาชุมชน จำกัด พ.ศ. 2565 แก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ. 2567 และแก้ไขเพิ่มเติม (ฉบับที่ 3) พ.ศ. 2568 ข้อ 81 (24) และระเบียบสหกรณ์ออมทรัพย์กรมการพัฒนาชุมชน จำกัด ว่าด้วยวิธีปฏิบัติการควบคุมภายในและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของสหกรณ์ พ.ศ. 2565 ข้อ 8 (1) ประกอบมติที่ประชุมคณะกรรมการดำเนินการสหกรณ์ ในการประชุม ครั้งที่ 11/2568 เมื่อวันพุธที่ 15 ตุลาคม พ.ศ. 2568 จึงยกเลิกประกาศ เรื่องนโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศ และออกประกาศสหกรณ์ออมทรัพย์กรมการพัฒนาชุมชน จำกัด เรื่อง นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและข้อมูลส่วนบุคคล ดังนี้

ข้อ 1 ประกาศนี้เรียกว่า “ประกาศ สหกรณ์ออมทรัพย์กรมการพัฒนาชุมชน จำกัด เรื่อง นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และข้อมูลส่วนบุคคล ”

ข้อ 2 ประกาศนี้ให้ใช้บังคับตั้งแต่ในวันที่ประกาศ เป็นต้นไป

ข้อ 3 นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและข้อมูลส่วนบุคคล มีวัตถุประสงค์ดังต่อไปนี้

3.1 เพื่อให้เกิดความน่าเชื่อถือ เชื่อมั่น และมีความมั่นคงปลอดภัยในการใช้งานด้านเทคโนโลยีสารสนเทศ ทำให้สามารถดำเนินงานได้อย่างมีประสิทธิภาพ ประสิทธิผล และพร้อมใช้งานอย่างต่อเนื่อง รวมทั้งเพื่อป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้เครื่องคอมพิวเตอร์ ระบบเครือข่ายคอมพิวเตอร์ และระบบสารสนเทศ

3.2 เพื่อกำหนดแนวทางปฏิบัติให้คณะกรรมการดำเนินการ คณะอนุกรรมการ คณะทำงาน ผู้จัดการ เจ้าหน้าที่ ผู้ดูแลระบบ ผู้ให้บริการภายนอก และบุคคลที่เกี่ยวข้อง ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการคุ้มครองข้อมูลส่วนบุคคล และปฏิบัติตามอย่างเคร่งครัด

3.3 เพื่อให้การเก็บ ใช้ เปิดเผย และลบข้อมูลส่วนบุคคลของสมาชิก สหกรณ์ และเจ้าหน้าที่เป็นไปตามหลักการของ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) โดยเฉพาะการขอความยินยอม การแจ้งวัตถุประสงค์ และการรักษาความลับของข้อมูล

3.4 เพื่อกำหนดมาตรการป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต โดยใช้ระบบการพิสูจน์ตัวตนหลายชั้น (Multi-Factor Authentication : MFA) และการควบคุมสิทธิ์ตามหลัก Need-to-Know และ Least Privilege

ข้อ 4 นโยบายในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและข้อมูลส่วนบุคคล กำหนดประเด็นสำคัญดังต่อไปนี้

4.1 การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

4.1.1 การเข้าถึงระบบสารสนเทศ ต้องควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย ทั้งด้านความลับ ความสมบูรณ์ และความพร้อมใช้งาน (Confidentiality, Integrity, Availability) กำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง และกำหนดสิทธิ์อย่างชัดเจน เพื่อให้ผู้ใช้งานในทุกระดับได้รับรู้ เข้าใจ และสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ และการคุ้มครองข้อมูลส่วนบุคคล

4.1.2 การบริหารจัดการการเข้าถึงของผู้ใช้งาน เพื่อควบคุมการเข้าถึงระบบสารสนเทศและป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ต้องกำหนดให้มีการลงทะเบียนผู้ใช้งาน ตรวจสอบบัญชีผู้ใช้งาน อนุมัติ และกำหนดรหัสผ่านหรือวิธีการพิสูจน์ตัวตนที่เหมาะสม โดยให้เฉพาะผู้ใช้งานที่มีสิทธิ์เท่านั้นที่สามารถเข้าใช้ระบบสารสนเทศได้ต้องเก็บบันทึกข้อมูลการเข้าถึงและข้อมูลจราจรทางคอมพิวเตอร์ (Log) อย่างน้อย 90 วัน ต้องบริหารจัดการสิทธิ์การเข้าถึงข้อมูลให้เหมาะสมตามระดับชั้นความลับของผู้ใช้งาน และต้องมีการทบทวนสิทธิ์การใช้งานอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงตำแหน่งงาน พร้อมตรวจสอบการละเมิดความปลอดภัยอย่างสม่ำเสมอ

4.1.3 การควบคุมการเข้าถึงเครือข่าย เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต ต้องกำหนดสิทธิ์ในการเข้าถึงเครือข่าย ให้ผู้ที่จะเข้าใช้งานต้องลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยรหัสผ่านหรือ Multi-Factor Authentication (MFA) สำหรับระบบสำคัญ ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์สำหรับใช้งานอินเทอร์เน็ตโดยผ่านระบบรักษาความปลอดภัย (เช่น Firewall, IDS/IPS) และมีการออกแบบระบบเครือข่ายโดยแบ่งเขต (Zone) การใช้งาน เช่น Zone ภายใน, Zone สาธารณะ (Guest), Zone เซิร์ฟเวอร์ เพื่อควบคุมและป้องกันภัยคุกคามได้อย่างเป็นระบบและมีประสิทธิภาพ

4.1.4 การควบคุมการเข้าถึงระบบปฏิบัติการ เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต ต้องกำหนดให้ผู้ที่จะเข้าใช้งานต้องลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยรหัสผ่านหรือ MFA ต้องกำหนดให้ระบบล็อกอัตโนมัติหลังไม่มีการใช้งานเกิน 15 นาที และจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศ รวมถึงห้ามใช้บัญชีผู้ใช้งานแบบร่วมกัน (Shared Account)

4.1.5 การควบคุมการเข้าถึงโปรแกรมประยุกต์และแอปพลิเคชัน ต้องกำหนดสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศที่สำคัญ โปรแกรมประยุกต์หรือแอปพลิเคชันต่าง ๆ รวมถึง จดหมายอิเล็กทรอนิกส์ (E-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) และระบบงานต่าง ๆ โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่ (Need-to-Know และ Least Privilege) ต้องมีการตรวจสอบและอนุมัติการใช้งานแอปพลิเคชันจากแหล่งภายนอก (เช่น Cloud Services, SaaS) โดยผู้ดูแลระบบก่อนการใช้งาน

4.2 การจัดทำระบบสำรองข้อมูลและการกู้คืน (Backup and Recovery)

เพื่อให้ระบบสารสนเทศของสหกรณ์ฯ สามารถให้บริการได้อย่างต่อเนื่องและมีเสถียรภาพ ต้องจัดทำระบบสารสนเทศและระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน โดยดำเนินการดังนี้

4.2.1 ต้องพิจารณาคัดเลือกระบบสารสนเทศที่สำคัญ (เช่น ระบบการเงิน ระบบสมาชิก ระบบบุคลากร) และจัดลำดับความจำเป็นจากมากไปน้อย

4.2.2 ต้องกำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ในการสำรองข้อมูลอย่างชัดเจน

4.2.3 ต้องกำหนดประเภทของข้อมูลที่ต้องสำรอง ความถี่ในการสำรอง และวิธีการสำรองให้เหมาะสม เช่น ระบบสำคัญ สำรองข้อมูลทุกวัน (Daily Backup) ระบบทั่วไป สำรองข้อมูลรายสัปดาห์ (Weekly Backup)

4.2.4 ต้องจัดเก็บข้อมูลสำรองในสื่อที่ปลอดภัย แยกจากสถานที่ตั้งหลัก (Offsite Backup) และต้องเข้ารหัสข้อมูล (Encrypted) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

4.2.5 ต้องทดสอบการกู้คืนข้อมูล (Recovery Test) อย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่าข้อมูลสามารถกู้คืนได้จริง

4.3 การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างเป็นระบบ ดังนี้

4.3.1 จัดให้มีการตรวจสอบโดยผู้ตรวจสอบภายในของสหกรณ์ฯ หรือผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก อย่างน้อยปีละ 1 ครั้ง

4.3.2 การประเมินความเสี่ยงต้องครอบคลุมทั้งด้านเทคนิค กระบวนการ และข้อมูลส่วนบุคคล โดยพิจารณาความเสี่ยงจากการเข้าถึงโดยไม่ได้รับอนุญาต การสูญหายของข้อมูล การโจมตีทางไซเบอร์ และการไม่ปฏิบัติตาม PDPA

4.3.3 ต้องจัดทำรายงานผลการตรวจสอบและประเมินความเสี่ยง พร้อมข้อเสนอแนะในการปรับปรุง

4.3.4 ต้องมีมาตรการในการตรวจประเมินระบบสารสนเทศ ได้แก่

- กำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นได้ในรูปแบบ "อ่านอย่างเดียว"
- หากจำเป็นต้องใช้ข้อมูลในรูปแบบอื่น ต้องสร้างสำเนา และต้องทำลายหรือลบข้อมูลทันทีหลังการตรวจสอบเสร็จสิ้น หรือเก็บรักษาอย่างปลอดภัย
- ระบุและจัดสรรทรัพยากรที่จำเป็นสำหรับการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย

ข้อ 5 หน้าที่ความรับผิดชอบ

5.1 คณะกรรมการดำเนินการสหกรณ์ฯ คณะอนุกรรมการ คณะทำงานที่เกี่ยวข้อง

5.1.1 สนับสนุนการดำเนินงานด้านเทคโนโลยีสารสนเทศให้มีประสิทธิภาพ รวมทั้งจัดสรรงบประมาณ ทรัพยากร และบุคลากรที่จำเป็นในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและข้อมูลส่วนบุคคล

5.1.2 มอบหมายให้มีผู้รับผิดชอบในการติดตามการปฏิบัติตามระเบียบปฏิบัติในการควบคุมภายใน และการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและข้อมูลส่วนบุคคลของสหกรณ์ฯ อย่างต่อเนื่อง

5.1.3 สื่อสารและสร้างความตระหนักกับบุคลากร ถึงความสำคัญของการปฏิบัติตามระเบียบ และแนวปฏิบัติที่สหกรณ์ฯ กำหนดขึ้นภายใต้ นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและข้อมูลส่วนบุคคล โดยเคร่งครัด

5.1.4 ส่งเสริมให้มีการฝึกอบรมหรือให้ความรู้เกี่ยวกับระบบงาน การรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ และการปฏิบัติตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) แก่คณะกรรมการดำเนินการ ผู้จัดการ และเจ้าหน้าที่สหกรณ์ เป็นประจำทุกปี

5.2 ผู้จัดการ รองผู้จัดการ ผู้ดูแลระบบ และเจ้าหน้าที่สหกรณ์ฯ

5.2.1 ผู้จัดการ หรือรองผู้จัดการที่ได้รับมอบหมาย มีหน้าที่ควบคุมดูแลการใช้งานระบบเทคโนโลยีสารสนเทศภายในสหกรณ์ฯ ให้เป็นไปตามวัตถุประสงค์การใช้งาน และปฏิบัติตามนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและข้อมูลส่วนบุคคลอย่างเคร่งครัด

5.2.2 ผู้ดูแลระบบมีหน้าที่ดำเนินการให้ระบบเทคโนโลยีสารสนเทศของสหกรณ์ฯ ทำงานได้อย่างมีประสิทธิภาพ มั่นคงปลอดภัย ตามระเบียบปฏิบัติในการควบคุมภายใน และการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศและข้อมูลส่วนบุคคลของสหกรณ์ฯ

5.2.3 เจ้าหน้าที่ทุกระดับ มีหน้าที่ปฏิบัติตามคำสั่ง ระเบียบ และแนวปฏิบัติที่สหกรณ์ฯ กำหนดขึ้นภายใต้นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและข้อมูลส่วนบุคคลโดยเคร่งครัด

ข้อ 6 การดำเนินการตามนโยบาย ให้มีผลตามที่กำหนดตั้งแต่วันที่ ประกาศ เรื่อง นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและข้อมูลส่วนบุคคล โดยให้มีการทบทวนอย่างน้อยปีละ 1 ครั้ง

ประกาศ ณ วันที่ 5 พฤศจิกายน พ.ศ. 2568

(นางสาวขนิฏฐา กาญจนรังษีนนท์)
ประธานกรรมการ
สหกรณ์ออมทรัพย์กรมการพัฒนาชุมชน จำกัด