ประกาศ

สหกรณ์ออมทรัพย์ข้าราชการกระทรวงศึกษาธิการ จำกัด

เรื่อง นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

(Information Security Policy)

****

โดยที่ระเบียบสหกรณ์ออมทรัพย์ข้าราชการกระทรวงศึกษาธิการ จำกัด ว่าด้วยวิธีปฏิบัติในการควบคุมภายในและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของสหกรณ์ พ.ศ. 2563 ข้อ 8(5) กำหนดให้สหกรณ์มีการควบคุมภายในและรักษาความปลอดภัยระบบสารสนเทศที่ใช้คอมพิวเตอร์เป็นไปตามนโยบาย ระเบียบสหกรณ์และระเบียบนายทะเบียนสหกรณ์ ดังนั้นเพื่อให้การใช้เทคโนโลยีสารสนเทศของสหกรณ์ออมทรัพย์ข้าราชการกระทรวงศึกษาธิการ จำกัด มีความมั่นคงปลอดภัย มีความน่าเชื่อถือ และสามารถป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้เครื่องคอมพิวเตอร์ระบบเครือข่าย และระบบสารสนเทศ ตามที่กำหนดไว้ในพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 โดยคำนึงถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคล ซึ่งเป็นข้อมูลที่มีความละเอียดอ่อนและต้องได้รับการดูแลอย่างเข้มงวดตามที่กำหนดไว้ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 อย่างเคร่งครัด ทันสมัยและมีประสิทธิภาพสูงสุด

อาศัยอำนาจตามข้อบังคับสหกรณ์ออมทรัพย์ข้าราชการกระทรวงศึกษาธิการ จำกัด พ.ศ. 2569 ข้อ 79 (3) และระเบียบสหกรณ์ออมทรัพย์ข้าราชการกระทรวงศึกษาธิการ จำกัด ว่าด้วยวิธีปฏิบัติในการควบคุมภายในและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของสหกรณ์ พ.ศ. 2563 ข้อ 8 (5) ประกอบมติที่ประชุมคณะกรรมการดำเนินการสหกรณ์ในการประชุม ครั้งที่ 6/2569 เมื่อวันพุธที่ 24 มิถุนายน 2569 จึงออกประกาศดังต่อไปนี้

ข้อ 1 ประกาศนี้เรียกว่า “ประกาศ สหกรณ์ออมทรัพย์ข้าราชการกระทรวงศึกษาธิการ จำกัด เรื่อง นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ”

ข้อ 2 ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศ เป็นต้นไป

ข้อ 3 นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ มีวัตถุประสงค์ดังต่อไปนี้

3.1 เพื่อกำหนดให้เกิดความน่าเชื่อถือ เชื่อมั่น และมีความมั่นคงปลอดภัยในการใช้งานด้านเทคโนโลยีสารสนเทศ ทำให้สามารถดำเนินงานได้อย่างมีประสิทธิภาพ ประสิทธิผล และพร้อมใช้งานอย่างต่อเนื่อง ในแนวทางมีความสอดคล้องกับกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง รวมทั้งเพื่อป้องกันหรือจัดการปัญหาที่อาจเกิดขึ้นจากการใช้เครื่องคอมพิวเตอร์ ระบบเครือข่ายคอมพิวเตอร์และระบบสารสนเทศได้อย่างมีประสิทธิภาพ

/3.2 เพื่อกำหนด...

3.2 เพื่อกำหนดแนวทางปฏิบัติให้คณะกรรมการดำเนินการสหกรณ์ฯ คณะกรรมการอื่น คณะอนุกรรมการ คณะทำงาน ผู้จัดการ เจ้าหน้าที่ ผู้ดูแลระบบ ผู้ให้บริการภายนอก และบุคคลที่เกี่ยวข้อง ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการคุ้มครองข้อมูลส่วนบุคคล และให้ถือปฏิบัติตามอย่างเคร่งครัด

3.3 เพื่อกำหนดให้มีการเก็บ ใช้ เปิดเผย และลบข้อมูลส่วนบุคคลของสมาชิกสหกรณ์และเจ้าหน้าที่ เป็นไปตามหลักการของ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) โดยเฉพาะการขอความยินยอม การแจ้งวัตถุประสงค์และการรักษาความลับของข้อมูล

3.4 เพื่อกำหนดมาตรการป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต โดยใช้ระบบการพิสูจน์ตัวตน (Authentication) และการควบคุมสิทธิ์ตามหลักการจัดการข้อมูลที่อนุญาตให้บุคคลเข้าถึงข้อมูลได้เฉพาะส่วนที่จำเป็นต่อการปฏิบัติหน้าที่ตนเองเท่านั้น (Need-to-Know) และทำงานตามหลักการด้านความปลอดภัยที่กำหนดผู้ใช้ระบบได้รับ “สิทธิขั้นต่ำสุด” เท่าที่จำเป็นต่อการปฏิบัติงานเท่านั้น (Least Privilege) โดยแบ่งแยกอำนาจหน้าที่ความรับผิดชอบ (Segregation of Duties) ในกระบวนการทำงานอย่างเหมาะสม เพื่อไม่ให้บุคคลใดบุคคลหนึ่งมีอำนาจเข้าถึงระบบมากเกินไปเพื่อจำกัดความเสียหาย และมีการรักษาความมั่นคงปลอดภัยแบบหลายระดับการควบคุม (Defense in Depth) ได้แก่ ด้านกายภาพ (Physical Control) ด้านเทคนิค (Technical Control) และด้านการบริหารจัดการ (Administrative Control) เพื่อป้องกันไม่ให้ผู้โจมตีเข้าถึงเครือข่ายหรือทรัพยากรภายในองค์กรที่ได้รับการป้องกัน

ข้อ 4 นโยบายในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและข้อมูลส่วนบุคคลกำหนดประเด็นสำคัญดังต่อไปนี้

4.1 การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

4.1.1 การควบคุมการเข้าถึงระบบสารสนเทศ ต้องควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย ทั้งด้านความลับ ความสมบูรณ์และความพร้อมใช้งาน (Confidentiality, Integrity, Availability) กำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึงและกำหนดสิทธิอย่างชัดเจน เพื่อให้ผู้ใช้งานในทุกระดับได้รับรู้เข้าใจ และสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคล

4.1.2 การควบคุมการบริหารจัดการการเข้าถึงของผู้ใช้งาน ต้องควบคุมการเข้าถึงระบบสารสนเทศและป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ต้องกำหนดให้มีการลงทะเบียนผู้ใช้งานตรวจสอบบัญชีผู้ใช้งาน อนุมัติและกำหนดรหัสผ่านหรือวิธีการพิสูจน์ตัวตนที่เหมาะสม โดยให้เฉพาะผู้ใช้งานที่มีสิทธิ์เท่านั้นที่สามารถเข้าใช้ระบบสารสนเทศได้ ต้องเก็บบันทึกข้อมูลการเข้าถึงและข้อมูลจราจรทางคอมพิวเตอร์ (Log) อย่างน้อย 90 วัน ต้องบริหารจัดการสิทธิ์การเข้าถึงข้อมูลให้เหมาะสมตามระดับชั้นความลับของผู้ใช้งานและต้องมีการทบทวนสิทธิ์การใช้งานอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงตำแหน่งงานพร้อมตรวจสอบการละเมิดความปลอดภัยอย่างสม่ำเสมอ

/4.1.3 การควบคุม...

4.1.3 การควบคุมการเข้าถึงเครือข่าย เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต ต้องกำหนดสิทธิ์ในการเข้าถึงเครือข่าย ให้ผู้ที่จะเข้าใช้งานต้องลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยรหัสผ่าน สำหรับระบบสำคัญ ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์สำหรับใช้งานอินเทอร์เน็ตโดยผ่านระบบรักษาความปลอดภัยและมีการออกแบบระบบเครือข่ายโดยแบ่งเขต (Zone) การใช้งาน เช่น Zone ภายใน, Zone สาธารณะ (Guest) เพื่อควบคุมและป้องกันภัยคุกคามได้อย่างเป็นระบบและมีประสิทธิภาพ

4.1.4 การควบคุมการเข้าถึงระบบปฏิบัติการ เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต ต้องกำหนดให้ผู้ที่จะเข้าใช้งานต้องลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยรหัสผ่าน ต้องกำหนดให้ระบบล็อกอัตโนมัติหรือเครื่องคอมพิวเตอร์จะเข้าสู่โหมดพักหน้าจอและกลับไปสู่หน้าจอให้ลงชื่อเข้าใช้งานใหม่ภายหลัง ไม่มีการใช้งานเกินเวลาที่กำหนดและจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศรวมถึงห้ามใช้บัญชีผู้ใช้งานแบบร่วมกัน (Shared Account)

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

4.2 การจัดทำระบบสำรองข้อมูลและการกู้คืน (Backup and Recovery) เพื่อให้ระบบสารสนเทศของสหกรณ์ฯ สามารถให้บริการได้อย่างต่อเนื่องและมีเสถียรภาพต้องจัดทำระบบสารสนเทศและระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน โดยดำเนินการดังนี้

4.2.1 ต้องพิจารณาคัดเลือกระบบสารสนเทศที่สำคัญ เช่น ระบบการเงิน ระบบสมาชิก ระบบบุคลากร และจัดลำดับความจำเป็นจากมากไปน้อย

4.2.2 ต้องกำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ในการสำรองข้อมูลอย่างชัดเจน

4.2.3 ต้องกำหนดประเภทของข้อมูลที่ต้องสำรอง ความถี่ในการสำรองและวิธีการสำรองให้เหมาะสม เช่น ระบบสำคัญและมีการเปลี่ยนแปลงบ่อย สำรองข้อมูลทุกวัน (Daily Backup), ระบบสำคัญแต่ไม่มีการเปลี่ยนแปลงบ่อย สำรองข้อมูลเมื่อมีการเปลี่ยนแปลง ระบบทั่วไป สำรองข้อมูลรายสัปดาห์ (Weekly Backup)

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

4.2.5 ต้องทดสอบการกู้คืนข้อมูล (Recovery Test) อย่างน้อยปีละ 1ครั้งเพื่อให้มั่นใจว่าข้อมูลสามารถกู้คืนได้จริง

/4.3 การตรวจสอบ...

4.3 การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างเป็นระบบ ดังนี้

4.3.1 จัดให้มีการตรวจสอบโดยผู้ตรวจสอบภายในของสหกรณ์ฯ หรือผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก อย่างน้อยปีละ 1 ครั้ง

4.3.2 การประเมินความเสี่ยงต้องครอบคลุมทั้งด้านเทคนิค กระบวนการและข้อมูลส่วนบุคคล โดยพิจารณาความเสี่ยงจากการเข้าถึงโดยไม่ได้รับอนุญาต การสูญหายของข้อมูล การโจมตีทางไซเบอร์และการไม่ปฏิบัติตาม PDPA

4.3.3 ต้องจัดทำรายงานผลการตรวจสอบและประเมินความเสี่ยง พร้อมข้อเสนอแนะในการปรับปรุง

4.3.4 ต้องมีมาตรการในการตรวจประเมินระบบสารสนเทศ ได้แก่

(1) กำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นได้ในรูปแบบ "อ่านอย่างเดียว"

(2) หากจำเป็นต้องใช้ข้อมูลในรูปแบบอื่น ต้องสร้างสำเนา และต้องทำลายหรือลบข้อมูลทันทีหลังการตรวจสอบเสร็จสิ้น หรือเก็บรักษาอย่างปลอดภัย

(3) ระบุและจัดสรรทรัพยากรที่จำเป็นสำหรับการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย

ข้อ 5 หน้าที่และความรับผิดชอบ

5.1 คณะกรรมการดำเนินการสหกรณ์ฯ คณะกรรมการอื่น คณะอนุกรรมการ คณะทำงานที่เกี่ยวข้อง

5.1.1 สนับสนุนการดำเนินงานด้านเทคโนโลยีสารสนเทศให้มีประสิทธิภาพรวมทั้งจัดสรรงบประมาณ ทรัพยากร และบุคลากรที่จำเป็นในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและข้อมูลส่วนบุคคล

5.1.2 มอบหมายให้มีผู้รับผิดชอบในการติดตามการปฏิบัติตามระเบียบปฏิบัติในการควบคุมภายใน และการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและข้อมูลส่วนบุคคลของสหกรณ์ฯ อย่างต่อเนื่อง

5.1.3 สื่อสารและสร้างความตระหนักกับบุคลากร ถึงความสำคัญของการปฏิบัติตามระเบียบ และแนวปฏิบัติที่สหกรณ์ฯ กำหนดขึ้นภายใต้นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศโดยเคร่งครัด

5.1.4 ส่งเสริมให้มีการฝึกอบรมหรือให้ความรู้เกี่ยวกับระบบงานการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ และการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) แก่คณะกรรมการดำเนินการสหกรณ์ฯ ผู้จัดการ และเจ้าหน้าที่สหกรณ์เป็นประจำทุกปี

/5.2 ผู้จัดการ...

5.2 ผู้จัดการ รองผู้จัดการ ผู้ช่วยผู้จัดการ ผู้ดูแลระบบ และเจ้าหน้าที่สหกรณ์ฯ

5.2.1 ผู้จัดการ หรือรองผู้จัดการ หรือผู้ช่วยผู้จัดการที่ได้รับมอบหมาย มีหน้าที่ควบคุมดูแลการใช้งานระบบเทคโนโลยีสารสนเทศภายในสหกรณ์ฯ ให้เป็นไปตามวัตถุประสงค์การใช้งาน และปฏิบัติตามนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศอย่างเคร่งครัด

5.2.2 ผู้ดูแลระบบมีหน้าที่ดำเนินการให้ระบบเทคโนโลยีสารสนเทศของสหกรณ์ฯทำงานได้อย่างมีประสิทธิภาพ มั่นคงปลอดภัยตามระเบียบปฏิบัติในการควบคุมภายใน และการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของสหกรณ์ฯ

5.2.3 เจ้าหน้าที่ทุกระดับ มีหน้าที่ปฏิบัติตามคำสั่ง ระเบียบ และแนวปฏิบัติที่สหกรณ์ฯ กำหนดขึ้นภายใต้นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศโดยเคร่งครัด

ข้อ 6 การดำเนินการตามนโยบาย ให้มีผลตามที่กำหนดตั้งแต่วันที่ ประกาศ เรื่อง นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ โดยให้มีการทบทวนอย่างน้อยปีละ 1 ครั้ง

ประกาศ ณ วันที่ 2 เดือน กรกฎาคม พ.ศ. 2569

ว่าที่ร้อยตรี

(จรูญ ชูลาภ)

ประธานกรรมการสหกรณ์

ข้าราชการกระทรวงศึกษาธิการ จำกัด