ระเบียบสหกรณ์ออมทรัพย์กรมที่ดิน จำกัด
ว่าด้วยการควบคุมภายในและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของสหกรณ์
พ.ศ. 2564

เพื่อให้การใช้ระบบเทคโนโลยีสารสนเทศในการปฏิบัติงานและการให้บริการสมาชิกของสหกรณ์มีความมั่นคงปลอดภัยและน่าเชื่อถือ รวมทั้งเพื่อป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้เครื่องคอมพิวเตอร์ ระบบเครือข่ายคอมพิวเตอร์และระบบสารสนเทศ และสอดคล้องกับระเบียบนายทะเบียนสหกรณ์ว่าด้วยมาตรฐานขั้นต่ำในการควบคุมภายในและการรักษาความปลอดภัยสำหรับสหกรณ์และกลุ่มเกษตรกรที่ใช้โปรแกรมระบบบัญชีคอมพิวเตอร์ประมวลผลข้อมูล พ.ศ. 2553 และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

อาศัยอำนาจตามความใน ข้อ 58 (9) และข้อ 77 (10) ของข้อบังคับสหกรณ์ออมทรัพย์กรมที่ดิน จำกัด และมติที่ประชุมคณะกรรมการดำเนินการ ครั้งที่ 12/2564 วันที่ 23 กันยายน 2564 จึงได้กำหนดระเบียบว่าด้วยการควบคุมภายในและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของสหกรณ์ไว้ดังต่อไปนี้

หมวด 1
บททั่วไป

ข้อ 1 ระเบียบนี้เรียกว่า “ระเบียบสหกรณ์ออมทรัพย์กรมที่ดิน จำกัด ว่าด้วยการควบคุมภายในและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของสหกรณ์ พ.ศ. 2564”

ข้อ 2 ระเบียบนี้ให้ใช้บังคับตั้งแต่วันที่ 1 ตุลาคม 2564 เป็นต้นไป

ข้อ 3 บรรดาระเบียบ ประกาศ คำสั่ง มติ หรือข้อตกลงอื่นใด ซึ่งขัดหรือแย้งกับระเบียบนี้ให้ใช้ระเบียบนี้แทน

ข้อ 4 ในระเบียบนี้

“สหกรณ์” หมายความว่า สหกรณ์ออมทรัพย์กรมที่ดิน จำกัด

“คณะกรรมการ” หมายความว่า คณะกรรมการดำเนินการสหกรณ์ออมทรัพย์กรมที่ดิน จำกัด

“ประธานกรรมการ” หมายความว่า ประธานคณะกรรมการดำเนินการสหกรณ์ออมทรัพย์กรมที่ดิน จำกัด

“ผู้จัดการ” หมายความว่า ผู้จัดการสหกรณ์ออมทรัพย์กรมที่ดิน จำกัด

/“เจ้าหน้าที่”...

"เจ้าหน้าที่" หมายความว่า เจ้าหน้าที่สหกรณ์ออมทรัพย์กรมที่ดิน จำกัด

"สมาชิก" หมายความว่า สมาชิกและสมาชิกสมทบสหกรณ์ออมทรัพย์กรมที่ดิน จำกัด

"ผู้ใช้งาน" หมายความว่า เจ้าหน้าที่ สมาชิกทุกคน ตลอดจนบุคคลภายนอกที่ได้รับอนุญาตให้ทำงานในสหกรณ์หรือที่เข้ามาดำเนินการด้านเทคโนโลยีสารสนเทศให้กับสหกรณ์ตามข้อตกลงที่ทำไว้กับสหกรณ์ หรือที่เข้ามาอบรมตามโครงการที่ผ่านความเห็นชอบจากที่ประชุมคณะกรรมการ

"ผู้ดูแลระบบ" หมายความว่า ผู้จัดการหรือผู้ที่ได้รับมอบหมายจากผู้จัดการ

"เครื่องคอมพิวเตอร์" หมายความว่า เครื่องคอมพิวเตอร์ทั้งหลาย เครื่องเซิร์ฟเวอร์ หรืออุปกรณ์อื่นใด ที่ทำหน้าที่ได้เสมือนเครื่องคอมพิวเตอร์ ทั้งที่ใช้งานอยู่ภายในสหกรณ์หรือภายนอกแล้วเชื่อมต่อเข้ากับระบบเครือข่าย

"ระบบเครือข่าย" หมายความว่า ระบบเครือข่ายคอมพิวเตอร์ที่สหกรณ์สร้างขึ้นทั้งแบบมีสาย (Wire) แบบไร้สาย (Wireless) และเครือข่ายเสมือนส่วนตัว (Virtual Private Network)

"ข้อมูล" หมายความว่า สิ่งที่สื่อความหมายให้รู้เรื่องราว ข้อเท็จจริง ข้อมูล หรือสิ่งใด ๆ ไม่ว่าจะได้จัดทำไว้ในรูปแบบของเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้

"ระบบสารสนเทศ" หมายความว่า ข้อมูล และสาระต่าง ๆ ที่เกิดจากการประมวลผลมาจากข้อมูล ที่จัดไว้อย่างเป็นระบบ

ข้อ 5 ให้ประธานกรรมการรักษาการตามระเบียบนี้

หมวด 2
การควบคุมภายในและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ

ข้อ 6 การควบคุมภายในและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ มีดังนี้

(1) จัดให้มีระบบรักษาความปลอดภัยทางกายภาพที่เพียงพอแก่การป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่ที่เกี่ยวข้องเข้าถึงอุปกรณ์คอมพิวเตอร์ที่สำคัญ และจัดให้มีระบบป้องกันความเสียหายจากสภาพแวดล้อมหรือภัยพิบัติต่าง ๆ ให้แก่อุปกรณ์คอมพิวเตอร์ที่สำคัญ

(2) จัดให้มีระบบการรักษาความปลอดภัยของข้อมูลในระบบคอมพิวเตอร์และระบบเครือข่ายที่เพียงพอต่อการป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่ที่เกี่ยวข้องได้เข้าถึง ล่วงรู้ ใช้ประโยชน์ หรือแก้ไขเปลี่ยนแปลงหรือลักลอบทำสำเนาข้อมูลหรือระบบดังกล่าวได้

(3) จัดให้มีมาตรการควบคุมการพัฒนาหรือแก้ไขเปลี่ยนแปลงที่เพียงพอ เพื่อให้ระบบโปรแกรมคอมพิวเตอร์มีการประมวลผลที่ถูกต้อง ครบถ้วน เป็นไปตามความต้องการของผู้ใช้งาน รวมทั้งต้องมีการสื่อสารหรือฝึกอบรมเกี่ยวกับระบบคอมพิวเตอร์ให้ผู้เกี่ยวข้องทราบอย่างทั่วถึงเพื่อให้สามารถใช้งานได้อย่างถูกต้อง

/(4) จัดให้มี...

(4) จัดให้มีเอกสารด้านข้อมูลของระบบคอมพิวเตอร์เป็นเอกสารแสดงรายละเอียดการจัดเก็บข้อมูลที่เป็นสาระสำคัญ เพื่อให้สามารถเข้าใจถึงโครงสร้างการจัดเก็บข้อมูลของระบบและใช้อ้างอิงเพื่อแก้ไขปัญหาได้ โดยเอกสารด้านฐานข้อมูลของระบบโปรแกรมคอมพิวเตอร์ที่จำเป็นจะต้องมีคือผังการไหลของข้อมูล (Data Flow Diagram) และพจนานุกรมข้อมูล (Data Dictionary) และคู่มือการใช้งาน ซึ่งมีการปรับปรุงเอกสารให้ถูกต้องและทันสมัยอยู่เสมอ

(5) จัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง ลบหรือถ่ายโอนข้อมูล ให้สอดคล้องเหมาะสมกับวิธีการและสื่อที่ใช้ในการเก็บรวบรวมใช้หรือเปิดเผยข้อมูล

(6) จัดให้มีการสำรองข้อมูลของระบบงานทุกสัปดาห์ เพื่อให้สามารถรองรับการดำเนินงานได้อย่างต่อเนื่อง มีประสิทธิภาพและทันเหตุการณ์ตลอดจนการดูแลรักษาข้อมูลชุดสำรองให้มีความปลอดภัยรวมทั้งป้องกันมิให้มีการนำข้อมูลชุดสำรองมาใช้อย่างไม่ถูกต้อง

ข้อ 7 การควบคุมทางกายภาพ

(1) จัดตั้งเครื่องคอมพิวเตอร์ไว้ในที่ที่เหมาะสม และห้ามผู้ไม่มีหน้าที่รับผิดชอบเข้ามาใช้เครื่องคอมพิวเตอร์ของสหกรณ์โดยไม่ได้รับอนุญาต

(2) จัดให้มีการติดตั้งอุปกรณ์ดับเพลิงไว้ในที่ที่เหมาะสมและสะดวกต่อการใช้งานเมื่อมีเหตุฉุกเฉิน และจัดทำแผนผังการขนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ รวมทั้งเอกสารที่เกี่ยวข้อง

(3) จัดให้มีระบบการควบคุมอุณหภูมิให้แก่อุปกรณ์เครื่องคอมพิวเตอร์อย่างเพียงพอและเหมาะสมกับสถานที่รวมทั้งจัดตั้งเครื่องคอมพิวเตอร์ให้อยู่ในสถานที่ที่มีอากาศถ่ายเทได้สะดวก

(4) จัดให้มีระบบสำรองไฟเครื่องแม่ข่ายและอุปกรณ์ที่เกี่ยวข้องอย่างเพียงพอเพื่อลดการหยุดชะงักการทำงานของเครื่องแม่ข่าย ในกรณีที่มีไฟฟ้าดับหรือไฟตก

ข้อ 8 การควบคุมการเข้าถึงระบบงาน

(1) ให้ผู้ดูแลระบบเป็นผู้กำหนดสิทธิและควบคุมการเข้าถึงระบบงานและข้อมูลให้เป็นไปตามความรับผิดชอบของเจ้าหน้าที่ของแต่ละระบบงานที่มีการมอบหมายตามคำสั่งปฏิบัติงาน รวมถึงการสอบทานสิทธิการใช้งานให้สอดคล้องตามภาระงานให้เป็นปัจจุบันเสมอ

(2) ผู้ดูแลระบบต้องจัดที่ตั้งอุปกรณ์คอมพิวเตอร์อยู่ในส่วนที่ไม่อนุญาตให้บุคคลภายนอกที่ไม่มีหน้าที่เกี่ยวข้องเข้ามาในส่วนการทำงานของเจ้าหน้าที่และจัดให้มีผู้รับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์ รวมทั้งผู้ใช้งานต้องมีการกำหนดรหัสในการอนุญาตใช้งาน

(3) ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้มีรหัสใช้งาน (User account) และมีการกำหนดรหัสผ่าน (User ID) ในการเข้าใช้ระบบงานรวมถึงการยกเลิกรหัสผู้ใช้ของเจ้าหน้าที่ที่ลาออกและกำหนดรหัสผู้ใช้ให้แก่เจ้าหน้าที่ที่เข้ามาปฏิบัติงานใหม่ รวมทั้งต้องกำกับดูแลให้ผู้ใช้งานมีการเปลี่ยนรหัสผ่านทุก ๆ 6 เดือน เป็นอย่างน้อย

(4) ผู้ใช้งานต้องเก็บรักษารหัสผ่านเป็นความลับ มิให้ผู้ใดล่วงรู้หากพิสูจน์ได้ว่าเกิดความเสียหายกับระบบและข้อมูลจากรหัสผู้ใช้งานนั้น ผู้ใช้งานนั้นต้องเป็นผู้รับผิดชอบในความเสียหายที่เกิดขึ้น

/(5) ผู้ใช้งาน...

(5) ผู้ใช้งานต้องใช้งานคอมพิวเตอร์ เพื่อประโยชน์สูงสุดต่อการดำเนินงานของสหกรณ์ และเป็นไปตามวัตถุประสงค์ รวมทั้งหมั่นตรวจสอบเครื่องคอมพิวเตอร์ให้สามารถใช้งานได้อย่างสมบูรณ์ และมีประสิทธิภาพหากพบเหตุการณ์ผิดปกติที่เกี่ยวกับความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ให้รีบแจ้งให้ผู้ดูแลระบบหรือผู้บังคับบัญชาตามลำดับชั้นทราบโดยทันที

ข้อ 9 การควบคุมการประมวลผลและแฟ้มข้อมูลคอมพิวเตอร์

(1) การเปลี่ยนแปลงแก้ไขโปรแกรมประมวลผลต้องจัดทำเป็นหนังสือแจ้งความต้องการของผู้ใช้งานในการเปลี่ยนแปลงแก้ไขให้ผู้ดูแลระบบพิจารณาอนุมัติและส่งต่อให้ผู้รับจ้างบำรุงรักษาโปรแกรมระบบงานดำเนินการและต้องตรวจสอบผลการแก้ไขของผู้รับจ้างให้ตรงกับความต้องการทุกครั้ง

(2) การเปลี่ยนแปลงข้อมูลหลักที่สำคัญ เช่น อัตราดอกเบี้ย เงื่อนไขการให้สินเชื่อ เงื่อนไขการรับฝากเงินและอื่น ๆ ต้องเป็นไปตามมติคณะกรรมการ

ข้อ 10 การควบคุมดูแลเอกสารสนับสนุนการปฏิบัติงานสำหรับระบบโปรแกรมคอมพิวเตอร์

(1) ผู้ดูแลระบบต้องจัดให้มีเอกสารด้านฐานข้อมูลที่จำเป็น ได้แก่ ผังการไหลของข้อมูล (Data Flow Diagram) และพจนานุกรมข้อมูล (Data Dictionary) รวมถึงคู่มือการใช้ระบบงานและต้องปรับปรุงให้เป็นปัจจุบันเสมอ

(2) ผู้ดูแลระบบต้องจัดเก็บเอกสารสนับสนุนการปฏิบัติงานในสถานที่ปลอดภัยและสามารถเรียกใช้งานได้

ข้อ 11 การพิสูจน์ตัวตน

(1) ผู้ใช้งานมีหน้าที่ในการดูแลรักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนเองมิให้ผู้อื่นล่วงรู้ หรือห้ามใช้ร่วมกับผู้อื่น รวมทั้งต้องเปลี่ยนรหัสผ่านทุก ๆ 6 เดือนเป็นอย่างน้อย

(2) ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งที่เข้าใช้งานคอมพิวเตอร์ และต้องทำการล็อคหน้าจอทุกครั้งหรือตั้งเวลาพักหน้าจอเมื่อไม่อยู่ที่เครื่องคอมพิวเตอร์

ข้อ 12 ผู้ใช้งานมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลของสหกรณ์หรือข้อมูลของผู้รับบริการหากเกิดการสูญหาย โดยนำไปใช้ในทางที่ผิด การเผยแพร่โดยไม่ได้รับอนุญาต ผู้ใช้งานต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้นด้วย

ข้อ 13 การป้องกันโปรแกรมไม่ประสงค์ดี

(1) เครื่องคอมพิวเตอร์ต้องติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ทุกเครื่อง รวมถึงอัพเดทระบบปฏิบัติการที่ใช้งานอยู่ให้เป็นปัจจุบันอยู่เสมอโดยเฉพาะในด้านความปลอดภัย

(2) บรรดาข้อมูลไฟล์ ซอฟต์แวร์ หรือสิ่งอื่นใดที่ได้รับจากผู้ใช้งานอื่นต้องได้รับการตรวจสอบไวรัสคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดีก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง

(3) ผู้ใช้งานต้องพึงระวังไวรัสและโปรแกรมไม่ประสงค์ดีตลอดเวลา หากพบว่าติดไวรัสต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่ระบบเครือข่าย และต้องแจ้งแก่ผู้ดูแลระบบ

/ข้อ 14 การ...

ข้อ 14 การรักษาความปลอดภัยของเครือข่ายไร้สาย

ผู้ดูแลระบบต้องควบคุมผู้ใช้บริการที่มีสิทธิเข้าใช้งานระบบเครือข่ายไร้สาย โดยอนุญาตเฉพาะชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ตามที่กำหนดไว้เท่านั้น

ข้อ 15 การรักษาความปลอดภัยของไฟร์วอลล์

(1) ผู้ดูแลระบบมีหน้าที่ในการบริหารจัดการ การติดตั้ง และกำหนดค่าของไฟร์วอลล์ทั้งหมด

(2) การกำหนดค่าเริ่มต้นพื้นฐานของทุกเครือข่ายจะต้องเป็นการปฏิเสธทั้งหมด

(3) ทุกเส้นทางเชื่อมต่ออินเตอร์เน็ตและบริการอินเตอร์เน็ตที่ไม่อนุญาตตามนโยบายจะต้องถูกบล็อก (Block) โดยไฟร์วอลล์

(4) ผู้ใช้งานอินเตอร์เน็ตจะต้องมีการ Login Account ก่อนการใช้งานทุกครั้ง

(5) ค่าเปลี่ยนแปลงทั้งหมดในไฟร์วอลล์ เช่น ค่าพารามิเตอร์ การกำหนดค่าใช้บริการและการเชื่อมต่อที่อนุญาต จะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง

(6) การเข้าถึงตัวอุปกรณ์ไฟร์วอลล์ จะต้องสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น

(7) ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ไฟร์วอลล์ จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า 90 วัน

(8) การเชื่อมต่อในลักษณะของการ Remote login จากภายนอกมายังเครื่องแม่ข่ายหรืออุปกรณ์เครือข่ายภายในจะต้องบันทึกรายการขออนุญาตดำเนินการเกี่ยวกับเครื่องแม่ข่ายและอุปกรณ์เครือข่าย และต้องได้รับความเห็นชอบจากผู้ดูแลระบบก่อน

(9) ต้องติดตั้งไฟร์วอลล์ (Firewall) ระหว่างระบบคลาวด์กับระบบเครือข่ายภายในสหกรณ์

(10) ต้องกำหนดให้ติดตั้งช่องทางการสื่อสารแบบเฉพาะ VPN (Virtual Private Network) เพื่อช่วยป้องกันการบุกรุกระหว่างระบบเครือข่ายและระบบคลาวด์

ข้อ 16 การรักษาความปลอดภัยของการสำรองข้อมูล

(1) จัดทำสำเนาข้อมูลเก็บไว้ทุกสัปดาห์ให้จัดเรียงตามลำดับความจำเป็นของการสำรองข้อมูลจากจำเป็นมากไปหาน้อย โดยจัดเก็บข้อมูลในสื่อเก็บข้อมูล พิมพ์ชื่อข้อมูล วันที่ เวลาที่สำรองข้อมูลไว้อย่างชัดเจน จัดเก็บในสถานที่อื่นและต้องมีการทดสอบสื่อเก็บข้อมูลสำรองอย่างสม่ำเสมอ

(2) ต้องมีการจัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาที่เหมาะสม

ประกาศ ณ วันที่ 15 ตุลาคม พ.ศ. 2564

(นายนิสิต จันทร์สมวงศ์)

ประธานกรรมการ

สหกรณ์ออมทรัพย์กรมที่ดิน จำกัด