ประกาศสหกรณ์ออมทรัพย์ครูลำปาง จำกัด
เรื่อง มาตรการและวิธีการรักษาความมั่นคงปลอดภัยของระบบฐานข้อมูล
และความพร้อมใช้งานของระบบเครือข่ายคอมพิวเตอร์ที่เกี่ยวข้อง

ด้วยสหกรณ์ออมทรัพย์ครูลำปาง จำกัด ใช้ระบบเครือข่ายคอมพิวเตอร์และระบบฐานข้อมูลในการสนับสนุนการปฏิบัติงานและการให้บริการสมาชิก ซึ่งหากระบบดังกล่าวเกิดเหตุขัดข้อง อาจส่งผลกระทบต่อความต่อเนื่องในการดำเนินงานของสหกรณ์ ดังนั้น เพื่อกำหนดมาตรการรักษาความมั่นคงปลอดภัยของระบบฐานข้อมูล ป้องกันและลดผลกระทบจากเหตุขัดข้อง ตลอดจนทบทวนมาตรการให้เหมาะสมและทันสมัย โดยให้สอดคล้องกับระเบียบสหกรณ์ฯ ว่าด้วยการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ พ.ศ. ๒๕๕๙ สหกรณ์จึงกำหนดมาตรการและวิธีปฏิบัติ ดังต่อไปนี้

ข้อ ๑ วัตถุประสงค์ เพื่อป้องกันและลดผลกระทบจากเหตุขัดข้องของระบบเครือข่ายคอมพิวเตอร์ เครื่องแม่ข่าย และระบบฐานข้อมูลที่เชื่อมโยงกัน รวมทั้งรักษาความมั่นคงปลอดภัยและความพร้อมใช้งานของระบบ เพื่อให้การปฏิบัติงานและการให้บริการของสหกรณ์ดำเนินไปอย่างต่อเนื่องหรือสามารถกลับมาให้บริการได้โดยเร็ว

ข้อ ๒ ขอบเขต ให้ใช้กับระบบเครือข่ายหลัก อุปกรณ์เชื่อมต่อ เครื่องแม่ข่าย ระบบฐานข้อมูล ระบบสำรอง และบริการเชื่อมโยงที่จำเป็นต่อการดำเนินงาน รวมถึงเจ้าหน้าที่ผู้รับผิดชอบและผู้ให้บริการภายนอกที่ได้รับอนุญาต

มาตรการที่ ๑ การควบคุมและรักษาความมั่นคงปลอดภัยของระบบเครือข่ายและฐานข้อมูล

๑. กำหนดผู้รับผิดชอบดูแลระบบเครือข่าย เครื่องแม่ข่าย และระบบฐานข้อมูล พร้อมจัดทำรายการอุปกรณ์และผังการเชื่อมต่อให้เป็นปัจจุบัน

๒. กำหนดสิทธิการเข้าถึงระบบฐานข้อมูลเฉพาะผู้ใช้งานหรือระบบงานที่ได้รับอนุญาตตามความจำเป็น และทบทวนสิทธิเมื่อมีการเปลี่ยนแปลงหน้าที่หรือระบบงาน

๓. จำกัดสิทธิการเปลี่ยนแปลงการตั้งค่าระบบเครือข่ายและระบบฐานข้อมูลเฉพาะผู้ได้รับอนุญาต พร้อมจัดเก็บหลักฐานการเปลี่ยนแปลง

๔. ควบคุมการเชื่อมต่อด้วยระบบรักษาความมั่นคงปลอดภัย เช่น ไฟร์วอลล์ (Firewall) และแบ่งส่วนเครือข่ายเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตและจำกัดผลกระทบต่อระบบงาน

๕. ตรวจสอบการเชื่อมต่อระหว่างระบบงานกับฐานข้อมูล และปิดช่องทางหรือบริการที่ไม่จำเป็น

มาตรการที่ ๒ การป้องกันภัยคุกคามและการเปลี่ยนแปลงระบบ

๑. ตรวจสอบและปรับปรุงระบบปฏิบัติการ ระบบจัดการฐานข้อมูล อุปกรณ์เครือข่าย และโปรแกรมป้องกันภัยคุกคามตามระดับความเสี่ยง

๒. เฝ้าระวังเหตุการณ์ผิดปกติที่อาจกระทบต่อความปลอดภัยหรือความพร้อมใช้งานของระบบ และแจ้งผู้รับผิดชอบโดยเร็ว

๓. การเปลี่ยนแปลงการตั้งค่าระบบที่สำคัญต้องได้รับอนุมัติ มีการประเมินผลกระทบ ทดสอบตามความเหมาะสม และกำหนดวิธีคืนค่าระบบเดิมเมื่อเกิดข้อผิดพลาด

๔. บันทึกและตรวจสอบเหตุการณ์สำคัญเกี่ยวกับการเข้าถึงฐานข้อมูล การเปลี่ยนแปลงค่ากำหนด และความผิดปกติของการเชื่อมต่อ พร้อมจัดเก็บหลักฐานให้ตรวจสอบย้อนหลังได้

มาตรการที่ ๓ การรักษาความพร้อมใช้งานของระบบ

๑. ตรวจสอบสถานะเครื่องแม่ข่าย อุปกรณ์เครือข่าย ระบบฐานข้อมูล พื้นที่จัดเก็บข้อมูล และระบบไฟฟ้าตามรอบที่กำหนด พร้อมบันทึกผลและแก้ไขข้อบกพร่อง

๒. กำหนดลำดับความสำคัญของระบบงานในการแก้ไขเหตุขัดข้อง พร้อมระบุผู้รับผิดชอบและผู้ประสานงาน

๓. ตรวจสอบและประเมินความเสี่ยงของอุปกรณ์หรือจุดเชื่อมต่อสำคัญที่อาจทำให้ระบบหยุดทำงานเมื่อเกิดเหตุขัดข้อง พร้อมกำหนดแนวทางรองรับและบันทึกผลการพิจารณา

๔. จัดทำแผนบำรุงรักษาและตรวจสอบความพร้อมใช้งานของอุปกรณ์ พร้อมบันทึกผลการดำเนินงาน

มาตรการที่ ๔ การสำรองข้อมูลและการกู้คืนระบบ

๑. กำหนดข้อมูลและระบบสำคัญที่ต้องสำรอง พร้อมระบุความถี่ วิธีการ สถานที่จัดเก็บ และผู้รับผิดชอบตามความสำคัญของระบบงาน

๒. จัดเก็บข้อมูลสำรองอย่างปลอดภัย แยกจากระบบหลัก และเก็บรักษาในสถานที่อื่นที่ปลอดภัย

๓. ตรวจสอบผลการสำรองข้อมูลตามรอบที่กำหนด พร้อมบันทึกผลและแก้ไขเมื่อพบข้อผิดพลาด

๔. จัดทำขั้นตอนการกู้คืนระบบฐานข้อมูลและระบบเครือข่าย โดยกำหนดลำดับการกู้คืนและผู้รับผิดชอบให้ชัดเจน

๕. สำรองข้อมูลการตั้งค่าของอุปกรณ์เครือข่ายที่สำคัญ และปรับปรุงให้เป็นปัจจุบัน เมื่อมีการเปลี่ยนแปลงเพื่อใช้กู้คืนระบบเมื่อเกิดเหตุขัดข้อง

๖. กำหนดระยะเวลาเป้าหมายในการกู้คืนระบบ (RTO) และระยะเวลาของข้อมูลที่ยอมให้สูญหายได้ (RPO) ตามความสำคัญของระบบงาน พร้อมจัดทำเป็นเอกสาร

๗. ทดสอบการกู้คืนข้อมูลหรือระบบสำคัญอย่างน้อยปีละ ๑ ครั้ง พร้อมตรวจสอบความถูกต้องของข้อมูลและบันทึกผลการทดสอบ

มาตรการที่ ๕ การจัดการเมื่อเกิดเหตุขัดข้อง

๑. เมื่อพบเหตุขัดข้อง ให้บันทึกวัน เวลา ลักษณะเหตุขัดข้อง ระบบที่ได้รับผลกระทบ ผู้แจ้งเหตุ และการดำเนินการเบื้องต้น พร้อมรายงานผู้รับผิดชอบตามลำดับ

๒. ผู้รับผิดชอบต้องตรวจสอบสาเหตุ จำกัดผลกระทบ และดำเนินการแก้ไขหรือประสานผู้ให้บริการภายนอกตามความจำเป็น

๓. ก่อนเปิดให้ใช้งานตามปกติ ต้องตรวจสอบการเชื่อมต่อ การทำงานของระบบงาน และความถูกต้องและความพร้อมใช้งานของฐานข้อมูลที่เกี่ยวข้อง

๔. หลังเกิดเหตุการณ์สำคัญ ให้สรุปสาเหตุ ระยะเวลาหยุดชะงัก ผลกระทบ และมาตรการป้องกันการเกิดซ้ำ

มาตรการที่ ๖ การติดตาม ตรวจสอบ และทบทวนมาตรการ

๑. ตรวจสอบและทบทวนมาตรการรักษาความมั่นคงปลอดภัยและความพร้อมใช้งานของระบบอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงระบบสำคัญหรือเกิดเหตุขัดข้องที่ส่งผลกระทบอย่างมีนัยสำคัญ

๒. ทบทวนความเหมาะสมของการควบคุมสิทธิ การรักษาความมั่นคงปลอดภัย การตรวจสอบระบบและการสำรองและกู้คืนข้อมูล

๓. กำหนดแนวทางแก้ไขข้อบกพร่อง ผู้รับผิดชอบ และระยะเวลาดำเนินการ พร้อมติดตามผลการแก้ไข

๔. รายงานผลการดำเนินงาน ปัญหา อุปสรรค และข้อเสนอแนะต่อผู้จัดการหรือคณะกรรมการที่เกี่ยวข้องตามอำนาจหน้าที่

การบังคับใช้และความรับผิดชอบ

ข้อ ๓ ให้ผู้จัดการกำกับดูแลการดำเนินงานตามประกาศนี้ และให้ฝ่ายที่รับผิดชอบด้านเทคโนโลยีสารสนเทศดำเนินการตามมาตรการที่กำหนด พร้อมจัดเก็บหลักฐานเพื่อให้สามารถตรวจสอบได้ ทั้งนี้ ผู้ใช้งานระบบและผู้ให้บริการภายนอกต้องปฏิบัติตามมาตรการที่เกี่ยวข้องภายใต้หน้าที่และสิทธิที่ได้รับอนุญาต

ข้อ ๔ ประกาศนี้เป็นมาตรการปฏิบัติเพิ่มเติมภายใต้ระเบียบสหกรณ์ออมทรัพย์ครูลำปาง จำกัด ว่าด้วยการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ พ.ศ. ๒๕๕๙ โดยไม่เป็นการแก้ไขหรือยกเลิกระเบียบดังกล่าว ทั้งนี้ หากมีข้อความใดขัดหรือแย้งกับระเบียบสหกรณ์ ให้ถือปฏิบัติตามระเบียบ และเสนอผู้มีอำนาจพิจารณาปรับปรุงแก้ไขตามขั้นตอนต่อไป

ข้อ ๕ ให้ประกาศนี้มีผลใช้บังคับตั้งแต่วันประกาศเป็นต้นไป

ประกาศ ณ วันที่ ๒๘ ตุลาคม พ.ศ. ๒๕๖๙

(นายสมศักดิ์ สลีวงศ์)
ประธานกรรมการ
สหกรณ์ออมทรัพย์ครูลำปาง จำกัด