ระเบียบสหกรณ์ออมทรัพย์ครูเชียงใหม่ จำกัด
ว่าด้วย วิธีปฏิบัติในการควบคุมภายในและการรักษาความปลอดภัย
ด้านเทคโนโลยีสารสนเทศของสหกรณ์ พ.ศ. 2568

อาศัยอำนาจตามความในข้อ 80 (8) และข้อ 115 (13) แห่งข้อบังคับสหกรณ์ออมทรัพย์ครูเชียงใหม่ จำกัด พ.ศ. 2562 และมติที่ประชุมคณะกรรมการดำเนินการชุดที่ 50/2/2568 เมื่อวันที่ 26 ธันวาคม พ.ศ. 2568 ตามที่นายทะเบียนสหกรณ์ฯ ได้กำหนดระเบียบนายทะเบียนสหกรณ์ว่าด้วยมาตรฐานขั้นต่ำในการควบคุมภายในและการรักษาความปลอดภัยสำหรับสหกรณ์และกลุ่มเกษตรกรที่ใช้โปรแกรมระบบบัญชีคอมพิวเตอร์ประมวลผลข้อมูล พ.ศ.2553 สหกรณ์ออมทรัพย์ครูเชียงใหม่ จำกัด จึงมีมติเห็นชอบให้กำหนดระเบียบว่าด้วยวิธีปฏิบัติในการควบคุมภายในและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของสหกรณ์ พ.ศ. 2568 ซึ่งมีความดังนี้

หมวด 1
บททั่วไป

ข้อ 1. ระเบียบนี้เรียกว่า "ระเบียบสหกรณ์ออมทรัพย์ครูเชียงใหม่ จำกัด ว่าด้วยวิธีปฏิบัติในการควบคุมภายในและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของสหกรณ์ พ.ศ. 2568"

ข้อ 2. ระเบียบนี้ให้ใช้บังคับ ตั้งแต่วันถัดจากวันที่มีมติ เป็นต้นไป

ข้อ 3. ให้ยกเลิกระเบียบสหกรณ์ออมทรัพย์ครูเชียงใหม่ จำกัด ว่าด้วยวิธีปฏิบัติในการควบคุมภายในและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของสหกรณ์พ.ศ. 2558 และที่ได้แก้ไขเพิ่มเติมเสียทั้งหมด บรรดาระเบียบและคำสั่งอื่นใด ในส่วนที่กำหนดไว้แล้วซึ่งขัดหรือแย้งกับระเบียบนี้ให้ใช้ระเบียบนี้แทน

ข้อ 4. ในระเบียบนี้

"สหกรณ์" หมายถึง สหกรณ์ออมทรัพย์ครูเชียงใหม่ จำกัด

"คณะกรรมการ" หมายถึง คณะกรรมการดำเนินการสหกรณ์

"ประธาน" หมายถึง ประธานกรรมการดำเนินการของสหกรณ์

"ผู้จัดการ" หมายถึง ผู้จัดการของสหกรณ์

"เจ้าหน้าที่" หมายถึง เจ้าหน้าที่ของสหกรณ์

"ผู้ดูแลระบบ" หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากสหกรณ์ให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบและเครือข่ายคอมพิวเตอร์ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์เพื่อการจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์

"บุคลากร" หมายถึง ผู้ใช้ประโยชน์จากสินทรัพย์ด้านเทคโนโลยีสารสนเทศของสหกรณ์ ได้แก่ เจ้าหน้าที่ หรือสมาชิกสหกรณ์ได้รับอนุญาตให้ทำงานในสหกรณ์ หรือบุคคลภายนอกที่ได้รับอนุญาตให้ทำงานในสหกรณ์หรือที่เข้ามาดำเนินการด้านเทคโนโลยีสารสนเทศให้กับสหกรณ์ ตามข้อตกลงที่ทำไว้กับสหกรณ์ หรือที่เข้ามาอบรมตามโครงการที่ผ่านความเห็นชอบจากที่ประชุมคณะกรรมการ และเจ้าหน้าที่ของรัฐผู้ดูแลการใช้โปรแกรมระบบบัญชีคอมพิวเตอร์ในการประมวลผลข้อมูล

"ผู้ใช้งาน" หมายถึง บุคลากร สมาชิกที่ได้รับอนุญาต หรือ บุคคลภายนอกที่ได้รับอนุญาต ให้เข้าใช้ระบบสารสนเทศของสหกรณ์

"ระบบเทคโนโลยีสารสนเทศ" หมายถึง สินทรัพย์ด้านเทคโนโลยีสารสนเทศ

"สินทรัพย์ด้านเทคโนโลยีสารสนเทศ" หมายถึง เครื่องคอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่าย ระบบสารสนเทศ ฐานข้อมูล ไฟล์ข้อมูล ซอฟต์แวร์เครื่องมือในการพัฒนา อุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย อุปกรณ์สื่อสาร สื่อบันทึกข้อมูลภายนอก และอุปกรณ์ต่อพ่วงทุกชนิด

"เครื่องคอมพิวเตอร์" หมายถึง อุปกรณ์หรือเครื่องคอมพิวเตอร์ทั้งหลายซึ่งอาจมีลักษณะเป็นเครื่องคอมพิวเตอร์แบบตั้งโต๊ะ เครื่องคอมพิวเตอร์แบบโน้ตบุ๊ก อุปกรณ์แบบพกพา เช่น โทรศัพท์มือถือ แท็ปเล็ต เป็นต้น เครื่องคอมพิวเตอร์แม่ข่าย หรืออุปกรณ์อื่นใด ที่ทำหน้าที่ได้เสมือนเครื่องคอมพิวเตอร์ทั้งที่ใช้งานอยู่ภายในสหกรณ์หรือภายนอกทั้งเชื่อมต่อและไม่เชื่อมต่อเข้ากับระบบเครือข่าย

"อุปกรณ์" หมายถึง อุปกรณ์ทุกประเภทที่ต่อเชื่อมกับคอมพิวเตอร์ และระบบคอมพิวเตอร์เพื่อใช้งาน หรือประมวลผลข้อมูล

"ระบบคอมพิวเตอร์" หมายถึง อุปกรณ์ที่ประกอบด้วย ฮาร์ดแวร์และซอฟต์แวร์ ได้แก่ ซอฟต์แวร์ระบบปฏิบัติการ (Operating System) และซอฟต์แวร์ประยุกต์ (Application Software) เพื่อใช้เป็นระบบจัดทำข้อมูล เช่น ตัวเลข ข้อความ รูปภาพ เสียง หรืออยู่ในรูปอื่น ๆ เป็นต้น โดยมีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดและใช้ประมวลผลข้อมูลเป็นสารสนเทศที่นำไปใช้ประโยชน์ได้

"ระบบเครือข่ายคอมพิวเตอร์" หมายถึง ระบบคอมพิวเตอร์ คอมพิวเตอร์แม่ข่าย และอุปกรณ์ที่เชื่อมต่อกันเป็นเครือข่ายด้วยอุปกรณ์เชื่อมต่อเครือข่ายและสื่อการเชื่อมต่อที่สหกรณ์สร้างขึ้น ทั้งที่เป็นสื่อการเชื่อมต่อแบบใช้สายและไร้สาย เพื่อการรับส่งข้อมูลและสารสนเทศระหว่างระบบคอมพิวเตอร์ รวมถึงการรับส่งข้อมูลและสารสนเทศภายในระบบสารสนเทศเดียวกันหรือระหว่างระบบสารสนเทศที่ถูกนำมาใช้งานร่วมกัน รวมถึงเครือข่ายอินทราเน็ต (Intranet) ซึ่งเป็นเครือข่ายภายใน และเครือข่ายอินเทอร์เน็ต (Internet) ซึ่งเป็นเครือข่ายภายนอก ของสหกรณ์ด้วย

"ระบบฐานข้อมูล" หมายถึง โครงสร้างของฐานข้อมูลและข้อมูลที่ถูกจัดเก็บและจัดการอย่างเป็นระบบ เพื่อให้ง่ายต่อการเข้าถึง จัดเก็บ และนำไปใช้งาน

"ฐานข้อมูล" หมายถึง ชุดของข้อมูลที่ถูกจัดเก็บรวบรวมอย่างเป็นระบบ เพื่อให้ง่ายต่อการเข้าถึง จัดเก็บ และนำไปใช้งาน

"ข้อมูล" หมายถึง สิ่งที่สื่อความหมายให้รู้เรื่องราว ข้อเท็จจริง ข้อมูล หรือสิ่งใด ๆ ไม่ว่าจะได้จัดทำไว้ในรูปแบบของเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

"สารสนเทศ" หมายถึง ข้อมูลต่าง ๆ ที่ได้ผ่านการเปลี่ยนแปลงประมวลผลหรือวิเคราะห์สรุปผลด้วยวิธีการต่าง ๆ ที่เก็บรวบรวมไว้เพื่อนำไปใช้ประโยชน์ในการปฏิบัติงาน การบริหาร การวางแผน การตัดสินใจและอื่น ๆ ตามความต้องการ

"ระบบสารสนเทศ" หมายถึง ระบบที่ใช้จัดเก็บและประมวลผลข้อมูลที่มีการนำเอาฮาร์ดแวร์ ซอฟต์แวร์ ผู้ใช้งาน แนวปฏิบัติและข้อมูล ซึ่งทำงานประสานกันเพื่อจัดเตรียมสารสนเทศที่จำเป็นให้กับสหกรณ์

"ระบบบัญชีคอมพิวเตอร์" หมายถึง ระบบที่ใช้ในการจัดการ จัดเก็บ ประมวลผล และรายงานข้อมูลทางบัญชีและการเงินของสหกรณ์ในระบบคอมพิวเตอร์

"ไซเบอร์" หมายถึง ข้อมูลและการสื่อสารที่เกิดจากการให้บริการ หรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ เครือข่ายอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการระบบเครือข่ายที่คล้ายคลึงกัน ที่เชื่อมต่อกันเป็นการทั่วไป

"ภัยคุกคาม" หมายถึง อันตรายที่อาจเกิดขึ้นกับสารสนเทศโดยบุคคล สิ่งต่าง ๆ หรือเหตุการณ์ทั้งเจตนาและไม่เจตนา อันเป็นเหตุทำให้ระบบสารสนเทศถูกเปิดเผย เปลี่ยนแปลง บิดเบือน ทำลาย หรือปฏิเสธการทำงาน หรือการกระทำอื่นตามความต้องการของภัยคุกคามนั้น

"ภัยคุกคามทางไซเบอร์" หมายถึง การกระทำหรือการดำเนินการใด ๆ โดยมิชอบ ที่ใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมประสงค์ร้าย โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ข้อมูลคอมพิวเตอร์หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์หรือข้อมูลอื่นที่เกี่ยวข้อง

"ระบบตรวจจับการบุกรุก" หมายถึง ระบบรักษาความปลอดภัยที่ทำหน้าที่ตรวจสอบปริมาณการรับส่งข้อมูลในเครือข่ายหรือกิจกรรมในระบบ เพื่อค้นหาภัยคุกคามทางไซเบอร์

"โปรแกรมป้องกันไวรัส" หมายถึง ซอฟต์แวร์รักษาความปลอดภัยที่ทำหน้าที่ป้องกัน ตรวจจับและกำจัดซอฟต์แวร์ที่เป็นอันตราย

"ช่องโหว่" หมายถึง จุดอ่อนหรือข้อบกพร่องใด ๆ ของระบบคอมพิวเตอร์ และระบบสารสนเทศ ซึ่งหากมีภัยคุกคามในรูปแบบที่เหมาะกัน สามารถถูกนำไปใช้ประโยชน์เพื่อก่อให้เกิดความเสียหายต่อสารสนเทศและข้อมูล

"ความเสี่ยง" หมายถึง โอกาสที่เอื้อให้ภัยคุกคามต่าง ๆ สร้างความเสียหายในรูปแบบที่เหมาะกับช่องโหว่ที่มีอยู่ในระบบคอมพิวเตอร์และระบบสารสนเทศ

"ประเมินความเสี่ยง" (Risk Assessment) หมายถึง กระบวนการวิเคราะห์ภัยคุกคามต่าง ๆ และความอ่อนแอของระบบคอมพิวเตอร์และระบบสารสนเทศ รวมทั้งผลกระทบจากการ สูญเสียสารสนเทศ หรือการสูญเสียความสามารถในการรักษาความมั่นคงปลอดภัยของสารสนเทศ การประเมินความเสี่ยงใช้เป็นพื้นฐานในการกำหนดมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมให้สารสนเทศต่อไป

"การรักษาความมั่นคงปลอดภัยสารสนเทศ" หมายถึง การดำเนินการเพื่อให้สารสนเทศมีคุณสมบัติดังนี้ มีการรักษาความลับของข้อมูล (Confidentiality) มีการรักษาความถูกต้องของข้อมูล (Integrity) และมีสภาพความพร้อมใช้งาน (Availability)

"การรักษาความมั่นคงปลอดภัย ไซเบอร์" หมายถึง มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศ

"เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์" หมายถึง เหตุการณ์ที่เกิดจากการกระทำหรือการดำเนินการใด ๆ ที่มิชอบซึ่งกระทำผ่านทางคอมพิวเตอร์หรือระบบคอมพิวเตอร์ ซึ่งอาจเกิดความเสียหายหรือผลกระทบต่อการรักษาความมั่นคงปลอดภัยไซเบอร์หรือความมั่นคงปลอดภัยไซเบอร์ของคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์

หมวด 2
วัตถุประสงค์

ข้อ 5. วัตถุประสงค์แห่งระเบียบนี้

(1) เพื่อให้ผู้ใช้งานระมัดระวังในการใช้ระบบเทคโนโลยีสารสนเทศ โดยจะไม่ทำให้ประสิทธิภาพของระบบบัญชีคอมพิวเตอร์และระบบเครือข่ายด้อยประสิทธิภาพลงอย่างผิดปกติโดยเจตนาหรือไม่เจตนาก็ตาม และตระหนักถึงความเสี่ยงที่อาจเกิดขึ้นจากการใช้ระบบเทคโนโลยีสารสนเทศ

(2) เพื่อให้ผู้ใช้งานใช้เทคโนโลยีสารสนเทศของสหกรณ์มีความมั่นคง ปลอดภัย สามารถใช้งานได้อย่างมีประสิทธิภาพ อย่างถูกต้องตามบทบาทและหน้าที่ที่ได้รับมอบหมาย

(3) เพื่อให้สหกรณ์ได้มีการควบคุมภายในและรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศที่ใช้คอมพิวเตอร์เป็นไปตามนโยบาย ระเบียบสหกรณ์และระเบียบนายทะเบียนสหกรณ์ เพื่อควบคุม ติดตาม ดูแลและปกป้องระบบเทคโนโลยีสารสนเทศของสหกรณ์ให้สอดคล้องกับการควบคุมภายในที่ดีด้านสารสนเทศ อันหมายรวมถึงข้อมูลคอมพิวเตอร์ ซอฟต์แวร์ และฮาร์ดแวร์ทั้งหมด ผู้ใช้งานต้องปฏิบัติตามระเบียบนี้โดยเคร่งครัดเมื่อเข้าใช้งานคอมพิวเตอร์ผ่านระบบเครือข่ายคอมพิวเตอร์ของสหกรณ์ และเป็นไปตามพระราชบัญญัติความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. 2562

หมวด 3
การรักษาความปลอดภัยทางกายภาพ

ข้อ 6. แนวทางการบริหารจัดการความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศ

(1) จัดทำนโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศ สำหรับระบบเทคโนโลยีสารสนเทศของสหกรณ์ให้เป็นลายลักษณ์อักษร และเอกสารนโยบายดังกล่าว ต้องได้รับการอนุมัติจากประธานกรรมการก่อนนำไปใช้งานและต้องเผยแพร่ให้เจ้าหน้าที่และหน่วยงานภายนอกทั้งหมดที่เกี่ยวข้องได้รับทราบ

(2) ดำเนินการตรวจสอบ ทบทวนนโยบายที่เกี่ยวข้องกับความปลอดภัยด้านเทคโนโลยีสารสนเทศ โดยจะต้องทบทวนตามรอบที่กำหนด หรือเมื่อมีการเปลี่ยนแปลงที่มีผลกระทบต่อการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของสหกรณ์หรืออย่างน้อย 1 ครั้งต่อปี

(3) กำหนดให้มีมาตรการ หรือระบบบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ โดยผ่านการประเมินความเสี่ยง (Risk Management) ช่องโหว่ (Vulnerability) ภัยคุกคาม (Threat) เพื่อให้ได้มาตรการป้องกันที่เหมาะสมกับระบบเทคโนโลยีสารสนเทศของสหกรณ์โดยการจัดทำแผนบริหารจัดการความเสี่ยง (Risk Management Plan) และกำหนดให้มีการปรับปรุงให้ทันสมัยอยู่เสมอ สหกรณ์อาจแต่งตั้งให้ที่ปรึกษาหรือบุคคลที่เหมาะสมด้านระบบเทคโนโลยีสารสนเทศเป็นผู้ประเมินหรือให้คำแนะนำ ปรึกษา และรายงานผลให้คณะกรรมการดำเนินการทราบ

ข้อ 7. สหกรณ์มีการจัดตั้งเครื่องคอมพิวเตอร์ไว้ในที่ที่เหมาะสมกับการใช้งานและให้ใช้งานเครื่องคอมพิวเตอร์ที่ได้รับอนุญาต

สำหรับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ที่เกี่ยวข้อง ไม่อนุญาตให้ถ่ายภาพ หรือวิดีโอในพื้นที่ควบคุม หรือทำกิจกรรมอื่นใดที่เป็นการบันทึกภาพของระบบหรือภาพภายในพื้นที่ควบคุม หากมีความจำเป็นต้องแจ้งเจ้าหน้าที่ผู้กำกับดูแล และ ให้ติดป้ายประกาศข้อความ “ห้ามเข้าก่อนได้รับอนุญาต” และ “ห้ามถ่ายภาพหรือวิดีโอ” บริเวณภายในพื้นที่ควบคุมการปฏิบัติงาน และห้ามผู้ไม่ได้รับอนุญาตเข้ามาใช้เครื่องคอมพิวเตอร์แม่ข่ายของสหกรณ์โดยเด็ดขาด

ข้อ 8. จัดให้มีการติดตั้งอุปกรณ์ดับเพลิงไว้ในที่ที่เหมาะสมและสะดวกต่อการใช้งานเมื่อมีเหตุฉุกเฉิน และจัดทำแผนผังการขนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ รวมทั้งเอกสารที่เกี่ยวข้อง

ข้อ 9. จัดให้มีระบบการควบคุมอุณหภูมิ ให้แก่อุปกรณ์เครื่องคอมพิวเตอร์อย่างเพียงพอและเหมาะสมกับสถานที่รวมทั้งจัดตั้งเครื่องคอมพิวเตอร์ให้อยู่ในสถานที่ที่มีอากาศถ่ายเทได้สะดวก

ข้อ 10. จัดให้มีระบบสำรองไฟเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ที่เกี่ยวข้องอย่างเพียงพอเพื่อลดการหยุดชะงักการทำงานของเครื่องคอมพิวเตอร์แม่ข่ายในกรณีที่มีไฟฟ้าดับหรือไฟตก

หมวด 4
การรักษาความปลอดภัยสำหรับการปฏิบัติงาน

ข้อ 11. การกำหนดขั้นตอนการปฏิบัติงาน

(1) จัดทำคู่มือ หรือขั้นตอนการปฏิบัติงานระบบเทคโนโลยีสารสนเทศ เช่น ขั้นตอนการแจ้งเหตุขัดข้อง ขั้นตอนการกู้คืน ขั้นตอนการบำรุงรักษาและดูแลระบบ ซึ่งประกอบไปด้วยรายละเอียดขั้นตอนการปฏิบัติและเจ้าหน้าที่ผู้รับผิดชอบ เป็นต้น

(2) คู่มือและขั้นตอนการปฏิบัติงานต้องได้รับการปรับปรุงเมื่อมีการปรับเปลี่ยนขั้นตอนการปฏิบัติงานนั้น ๆ โดยคู่มือและขั้นตอนการปฏิบัติงานทุกฉบับต้องได้รับการทบทวนอย่างน้อยปีละ 1 ครั้ง

ข้อ 12. การกำหนดการบำรุงรักษาระบบเทคโนโลยีสารสนเทศ

(1) กำหนดให้มีการบำรุงรักษาอย่างถูกต้องและสม่ำเสมอ เช่น จัดให้มีการซ่อมบำรุงอย่างน้อยปีละ 1 ครั้ง

(2) จัดทำสัญญาการบำรุงรักษาสำหรับระบบและอุปกรณ์คอมพิวเตอร์ที่มีความสำคัญ โดยต้องกำหนดเงื่อนไขของการให้บริการในสัญญาการบำรุงรักษาให้ชัดเจน พร้อมทั้งควบคุมและดูแลการปฏิบัติงานของผู้ให้บริการภายนอกให้ปฏิบัติตามสัญญาการจ้างเหมาบำรุงรักษา

ข้อ 13. การบริหารจัดการทะเบียนสินทรัพย์ด้านเทคโนโลยีสารสนเทศ

(1) จัดทำบัญชีหรือทะเบียนสินทรัพย์ประเภทอุปกรณ์คอมพิวเตอร์รวมถึงอุปกรณ์อื่นที่เกี่ยวข้องกับการประมวลผลสารสนเทศของระบบงาน และอุปกรณ์เชื่อมต่อเครือข่ายสารสนเทศ ซึ่งสินทรัพย์ทั้งหมดมีการระบุผู้ถือครองหรือผู้รับผิดชอบ รวมถึงมีหลักฐานเอกสารรับสินทรัพย์ไปถือครองหรือรับผิดชอบ และมีการปรับปรุงบัญชีให้เป็นปัจจุบัน

(2) กำกับดูแลการใช้สินทรัพย์ให้เป็นไปอย่างเหมาะสม เพื่อให้เกิดการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

(3) กำหนดมาตรการหรือเทคนิคในการทำลายข้อมูลสำคัญในสื่อบันทึกข้อมูลก่อนจะจำหน่ายหรือนำกลับมาใช้งานใหม่ทุกครั้ง เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้น

(4) เมื่อสิ้นสุดการใช้งานหรือความรับผิดชอบต่อสินทรัพย์ผู้ถือครองหรือผู้รับผิดชอบสินทรัพย์ต้องส่งคืนสินทรัพย์พร้อมมีเอกสารหลักฐานการส่งคืนสินทรัพย์

(5) กรณีสินทรัพย์เกิดความเสียหายและต้องส่งซ่อม ให้ควบคุมการส่งออกไปซ่อมแซมนอกสถานที่เพื่อป้องกันการสูญหาย หรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต กรณีสินทรัพย์เป็นข้อมูลสำคัญต้องทำการทำลายข้อมูลทิ้งเพื่อไม่ให้ผู้อื่นสามารถเข้าถึงได้

หมวด 5
คณะกรรมการดำเนินการ

ข้อ 14. ต้องพิจารณาจัดให้มีสินทรัพย์ด้านเทคโนโลยีสารสนเทศตามสมควรและเหมาะสมกับสหกรณ์

ข้อ 15. มอบหมายให้มีผู้รับผิดชอบในการติดตามการปฏิบัติตามนโยบายหรือระเบียบปฏิบัติในการควบคุมภายใน และการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของสหกรณ์

ข้อ 16. สื่อสารให้ผู้ใช้งานเข้าใจนโยบายหรือระเบียบปฏิบัติในการควบคุมภายในและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของสหกรณ์

ข้อ 17. ส่งเสริมให้มีการฝึกอบรมหรือให้ความรู้เกี่ยวกับระบบงานและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศแก่คณะกรรมการดำเนินการ ผู้จัดการ และเจ้าหน้าที่สหกรณ์หรือสนับสนุนให้เข้ารับการฝึกอบรมกับหน่วยงานและองค์กรต่าง ๆ ที่มีการจัดอบรมในเรื่องดังกล่าว

ข้อ 18. กำหนดให้ผู้บริการโปรแกรมระบบบัญชีจัดทำคู่มือการใช้โปรแกรมและเอกสารด้านฐานข้อมูล ได้แก่ โครงสร้างข้อมูล (Data Structure) หรือพจนานุกรมข้อมูล (Data Dictionary) ให้กับสหกรณ์ เพื่อประกอบการใช้งานโปรแกรมระบบบัญชี

ข้อ 19. มอบหมายให้มีผู้รับผิดชอบในการเก็บรักษาคู่มือและเอกสารสนับสนุนการปฏิบัติงานให้อยู่ในที่ปลอดภัย และให้เรียกใช้งานได้ทันที

ข้อ 20. พิจารณาคัดเลือกและจัดทำสัญญากับผู้ให้บริการโปรแกรมหรือระบบเทคโนโลยีสารสนเทศ และพิจารณาเกี่ยวกับการรักษาความลับของข้อมูล เงื่อนไขต่าง ๆ และขอบเขตงานของผู้ให้บริการ

ข้อ 21. แต่งตั้งเจ้าหน้าที่เพื่อรับผิดชอบด้านเทคโนโลยีสารสนเทศของสหกรณ์

ข้อ 22. จัดให้มีการทำหรือทบทวนแผนฉุกเฉิน และการประเมินผลของการทดสอบแผนฉุกเฉินตามความเหมาะสม ทั้งนี้ให้เป็นดุลยพินิจของคณะกรรมการดำเนินการ

ข้อ 23. รณรงค์ให้ทุกคนใช้พลังงานไฟฟ้าอย่างประหยัด โดยจัดระดับการทำงานของเครื่องคอมพิวเตอร์และปิดอุปกรณ์ต่อพ่วงทุกครั้งที่ไม่มีการใช้งาน ให้เหมาะสมและมีประสิทธิภาพ รวมทั้ง การใช้มาตรการลดการใช้กระดาษ ให้น้อยลงด้วย

หมวด 6
ผู้จัดการสหกรณ์หรือ ผู้ดูแลระบบงาน

ข้อ 24. ควบคุมดูแลการใช้ระบบเทคโนโลยีสารสนเทศให้เป็นไปตามวัตถุประสงค์

ข้อ 25. ดำเนินการให้ระบบเทคโนโลยีสารสนเทศของสหกรณ์ทำงานได้อย่างมีประสิทธิภาพ ทันสมัย และมั่นคงปลอดภัยตามนโยบายการรักษาความปลอดภัยของสหกรณ์

ข้อ 26. ติดตั้งค่าการรักษาความปลอดภัยของระบบบัญชีคอมพิวเตอร์และระบบเครือข่ายให้สามารถป้องกันบุคคลที่ไม่ได้รับอนุญาตเข้าสู่ระบบได้ง่าย ได้แก่ ความยาวของรหัสผ่าน ระยะเวลาการเปลี่ยนแปลงรหัสผ่าน ระยะเวลาการตั้งเวลาพักหน้าจอในกรณีผู้ใช้งานไม่อยู่ที่เครื่อง เป็นต้น

ข้อ 27. มีหน้าที่รับผิดชอบในการบริหารจัดการผู้ใช้งาน เกี่ยวกับการสร้าง/เปลี่ยนแปลง/ลบชื่อผู้ใช้งาน (username) โดยการกำหนดสิทธิการใช้งาน จะต้องเป็นไปตามหน้าที่ความรับผิดชอบของผู้ใช้งาน

ข้อ 28. มีหน้าที่สอบทานสิทธิการใช้งานของเจ้าหน้าที่ในระบบบัญชีคอมพิวเตอร์และระบบเครือข่าย ให้สอดคล้องกับหน้าที่ความรับผิดชอบในแต่ละตำแหน่งเป็นประจำทุกปี

ข้อ 29. จัดทำคู่มือ หรือขั้นตอนการปฏิบัติงานระบบเทคโนโลยีสารสนเทศ ตามหมวด 4 การรักษาความปลอดภัยสำหรับการปฏิบัติงานข้อ 11 (1)

ข้อ 30. บริหารจัดการระบบเครือข่ายให้มีความมั่นคงปลอดภัย มีประสิทธิภาพ ครอบคลุมพื้นที่การทำงานทั้งหมด ได้แก่

(1) กำหนดสิทธิการเข้าถึงระบบเครือข่ายรวมถึงระบบอื่นให้กับผู้ที่ได้รับอนุญาตเท่านั้น

(2) จัดทำการปรับปรุงแผนผังเครือข่ายและอุปกรณ์ที่เกี่ยวข้องให้เป็นปัจจุบัน

(3) มีการตรวจสอบหรือเฝ้าระวังเกี่ยวกับการรักษาความปลอดภัยระบบคอมพิวเตอร์แม่ข่ายอย่างสม่ำเสมอ

(4) ติดตั้งระบบป้องกันไวรัสกับเครื่องคอมพิวเตอร์แม่ข่าย และปรับปรุงระบบป้องกันไวรัส ให้เป็นปัจจุบันสม่ำเสมอ

ข้อ 31. จัดทำตารางแผนการสำรองข้อมูลและวิธีการกู้คืนข้อมูล และให้มีการสำรองข้อมูล และการทดสอบการกู้คืนข้อมูลเป็นไปตามแผนที่กำหนด ได้แก่

(1) กำหนดตารางแผนการสำรองข้อมูลให้เหมาะสมกับการปฏิบัติงานของสหกรณ์

(2) กำหนดให้สำรองข้อมูลจากระบบบัญชีคอมพิวเตอร์ที่สหกรณ์ใช้ในเครื่องคอมพิวเตอร์ที่แยกต่างหากจากเครื่องคอมพิวเตอร์แม่ข่ายหลักของสหกรณ์จำนวน 1 ชุดเป็นประจำทุกวันทำการของสหกรณ์และสำรองข้อมูล ไว้ในสื่อบันทึกข้อมูลจำนวน 1 ชุดเป็นประจำทุกเดือน

(3) กำหนดให้สำรองโปรแกรม ฐานข้อมูลที่เกี่ยวกับระบบปฏิบัติการ ระบบฐานข้อมูล และ ระบบบัญชีคอมพิวเตอร์ไว้ในสื่อบันทึกข้อมูลจำนวน 1 ชุด เป็นประจำทุก 3 เดือน

(4) ให้เจ้าหน้าที่ผู้รับผิดชอบระบบงานสำรองข้อมูลในสื่อบันทึกข้อมูลและติดฉลากที่มีรายละเอียด โปรแกรมระบบงาน วัน เดือน ปี จำนวนหน่วยข้อมูล

(5) จัดเก็บสื่อบันทึกข้อมูลไว้ในที่ปลอดภัยทั้งในและนอกสำนักงานสหกรณ์และให้สามารถนำมา ใช้งานได้ทันทีในกรณีที่มีเหตุฉุกเฉิน

(6) ผู้จัดการหรือผู้ที่ได้รับมอบหมายต้องทดสอบข้อมูลที่สำรองทุก 6 เดือน และเก็บรักษาชุดสำรองข้อมูลไว้อย่างน้อย 10 ปีตามกฎหมาย

(7) จัดทำทะเบียนคุมข้อมูลชุดสำรอง และควบคุมการนำข้อมูลชุดสำรองออกมาใช้งาน

ข้อ 32. จัดทำแผนฉุกเฉินรองรับเมื่อเกิดปัญหากับระบบเทคโนโลยีสารสนเทศ ในกรณีเครื่องคอมพิวเตอร์ได้รับความเสียหายหรือหยุดชะงัก และกำหนดผู้รับผิดชอบที่ชัดเจน

ข้อ 33. ดำเนินการทดสอบแผนฉุกเฉินร่วมกับผู้ใช้งานอย่างน้อยปีละ 1 ครั้งและจัดทำผลการทดสอบ แผนฉุกเฉิน

ข้อ 34. จัดการกับเหตุการณ์ผิดปกติที่เกี่ยวข้องกับความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ โดยทันทีเมื่อได้รับรายงานจากผู้ใช้งาน

หมวด 7

ขอบเขตและความรับผิดชอบของผู้ใช้งาน

ข้อ 35. ผู้ใช้งานต้องใช้ระบบเทคโนโลยีสารสนเทศเพื่อประโยชน์สูงสุดต่อการดำเนินงานของสหกรณ์และ เป็นไปตามวัตถุประสงค์

ข้อ 36. ให้คำนึงถึงการใช้งานอย่างประหยัด ไม่ให้เกิดความเสียหายต่อระบบเทคโนโลยีสารสนเทศ และให้สามารถใช้งานได้ อย่างสมบูรณ์และมีประสิทธิภาพ

ข้อ 37. จัดทำคู่มือและขั้นตอนการปฏิบัติงานตาม หมวด 4 การรักษาความปลอดภัยสำหรับการปฏิบัติงาน ข้อ 11 (2)

ข้อ 38. ผู้ใช้งานแต่ละคนมีหน้าที่ป้องกันดูแลรักษาข้อมูลชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) ทั้งนี้ต้องห้ามเผยแพร่ให้ผู้อื่นล่วงรู้รหัสผ่าน (password) ของตนเอง

ข้อ 39. การกำหนดรหัสผ่านในการเข้าถึงระบบเทคโนโลยีสารสนเทศอย่างน้อย 6 ตัวอักษร โดยกำหนดให้มี ความยากต่อการคาดเดาและให้มีการเปลี่ยนแปลงรหัสผ่านของผู้ใช้งานทุก ๆ 4 เดือน

ข้อ 40. ผู้ใช้งานแต่ละคนห้ามใช้ชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) ของบุคคลอื่นมาใช้งานไม่ว่าจะได้รับอนุญาตจากผู้ใช้งาน นั้นหรือไม่ก็ตาม

ข้อ 41. การใช้งานเครื่องคอมพิวเตอร์ ผู้ใช้งาน ต้องรับผิดชอบในฐานะเป็นผู้ถือครองเครื่องนั้น ๆ และ ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้นอันเนื่องมาจากการใช้งานที่ผิดปกติ โดยชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) ของผู้ถือครองเครื่องนั้น ๆ

ข้อ 42. เมื่อพบเหตุการณ์ผิดปกติที่เกี่ยวกับความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ให้รีบแจ้งให้ผู้จัดการหรือผู้ดูแลระบบงานของสหกรณ์โดยทันที

ข้อ 43. ผู้ใช้งานจะต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบงานตามความจำเป็นต่อการใช้งานระบบเทคโนโลยีสารสนเทศ

หมวด 8
การพิสูจน์ตัวตน
(Accountability, Identification and Authentication)

ข้อ 44. ผู้ใช้งานมีหน้าที่ในการป้องกันดูแลรักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) โดยผู้ใช้งาน แต่ละคนต้องมีบัญชีชื่อผู้ใช้งาน (Username) ของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่ แจกจ่ายทำให้ผู้อื่นล่วงรู้รหัสผ่าน (Password)

ข้อ 45. ผู้ใช้งานต้องรับผิดชอบต่อการกระทำใด ๆ ที่เกิดจากบัญชีของผู้ใช้งาน (Username) ไม่ว่าการกระทำนั้น จะเกิดจากผู้ใช้งาน หรือไม่ก็ตาม

ข้อ 46. ผู้ใช้งานต้องตั้งรหัสผ่านให้เกิดความปลอดภัย โดยรหัสผ่านต้องประกอบด้วยตัวอักษรตัวพิมพ์ปกติ ตัวพิมพ์ใหญ่ (Character) หรือตัวเลข (Numerical character) และสัญลักษณ์ (Special Characters) เข้าด้วยกัน ไม่น้อยกว่า 6 ตัวอักษร

ข้อ 47. ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) อย่างน้อยทุก ๆ 4 เดือน หรือทุกครั้งเมื่อมีการแจ้งเตือน

ข้อ 48. ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้ง ก่อนที่จะใช้สินทรัพย์ด้านเทคโนโลยีสารสนเทศของสหกรณ์และหากการพิสูจน์ตัวตนนั้นมีปัญหาไม่ว่าจะเกิดจากรหัสผ่าน การถูกล็อค หรือเกิดจากความผิดพลาดใด ๆ ผู้ใช้งาน ต้องแจ้งให้ผู้ดูแลระบบ (System Administrator) ทราบทันที โดย

(1) คอมพิวเตอร์โน๊ตบุ๊ค (Notebook) ต้องทำการพิสูจน์ตัวตนระบบในไบออส (BIOS) ก่อนใช้งาน

(2) คอมพิวเตอร์ทุกประเภท ก่อนการเข้าถึงระบบปฏิบัติการต้องทำการพิสูจน์ตัวตนทุกครั้ง

(3) การใช้งานอินเทอร์เน็ต (Internet) ต้องมีการบันทึกข้อมูลซึ่งสามารถบ่งบอกตัวตนบุคคลผู้ใช้งาน ได้

(4) เมื่อผู้ใช้งาน ไม่อยู่ที่เครื่องคอมพิวเตอร์ เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการปิดระบบโปรแกรมสหกรณ์หรือ ล็อคหน้าจอทุกครั้ง และต้องทำการพิสูจน์ตัวตนก่อนการใช้งานทุกครั้ง

(5) เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการตั้งเวลาพักหน้าจอ (screen saver) โดยตั้งเวลาอย่างน้อย 5 นาที

หมวด 9
การบริหารจัดการสินทรัพย์
(Assets Management)

ข้อ 49. ผู้ใช้งานต้องไม่เข้าถึงเครื่องคอมพิวเตอร์แม่ข่ายโดยเด็ดขาด เว้นแต่ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ 50. ผู้ใช้งานต้องไม่นำเครื่องมือ หรืออุปกรณ์อื่นใด เชื่อมต่อเข้าเครือข่ายโดยเด็ดขาด

ข้อ 51. ผู้ใช้งานต้องไม่ใช้ หรือลบแฟ้มข้อมูลของผู้อื่น ไม่ว่ากรณีใด ๆ

ข้อ 52. ผู้ใช้งานต้องรับผิดชอบต่อสินทรัพย์ของสหกรณ์ที่มอบไว้ให้ใช้งาน หรือหากมีการใช้งานนอกสถานที่ต้องดูแลการรับหรือคืนสินทรัพย์จะถูกบันทึก และตรวจสอบทุกครั้งโดยเจ้าหน้าที่สหกรณ์มอบหมาย

ข้อ 53. ผู้ใช้งานต้องรับผิดชอบต่อสินทรัพย์ของสหกรณ์ที่มอบไว้ให้ใช้งานเสมือนหนึ่งเป็นสินทรัพย์ของผู้ใช้งานเอง โดยชดใช้ค่าเสียหายไม่ว่าสินทรัพย์นั้นจะชำรุดหรือสูญหายตามมูลค่าสินทรัพย์ หากความเสียหายนั้นเกิดจากความประมาทของผู้ใช้งาน

ข้อ 54. ผู้ใช้งานต้องไม่ให้ผู้อื่นยืมคอมพิวเตอร์หรือโน๊ตบุ๊ค (Notebook) ไม่ว่ากรณีใด ๆ เว้นแต่การยืมนั้นได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้มีอำนาจ

ข้อ 55. สินทรัพย์ด้านเทคโนโลยีสารสนเทศต่าง ๆ ที่สหกรณ์จัดเตรียมไว้ให้ใช้งานมีวัตถุประสงค์เพื่อการใช้งานของสหกรณ์เท่านั้น ห้ามมิให้ผู้ใช้งาน นำสินทรัพย์ด้านเทคโนโลยีสารสนเทศต่าง ๆ ไปใช้ในกิจกรรมที่สหกรณ์ไม่ได้กำหนด หรือทำให้เกิดความเสียหายต่อสหกรณ์

ข้อ 56. ความเสียหายใด ๆ ที่เกิดจากการละเมิดข้อ 55 ให้ถือเป็นความผิดส่วนบุคคลโดยผู้ใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

หมวด 10
การบริหารจัดการข้อมูลสหกรณ์
(Corporate Management)

ข้อ 57. ผู้ใช้งาน ต้องป้องกัน ดูแล รักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูล รวมถึงระมัดระวังต่อการใช้งานของข้อมูล ทั้งข้อมูลของสหกรณ์หรือข้อมูลส่วนบุคคล หากเกิดความสูญหาย โดยนำไปใช้ในทางที่ผิด การเผยแพร่โดยไม่ได้รับอนุญาต ผู้ใช้งาน ต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้น

ข้อ 58. ข้อมูลทั้งหมดที่อยู่ภายในสินทรัพย์ของสหกรณ์ถือเป็นสินทรัพย์ของสหกรณ์ห้ามเผยแพร่ แก้ไขเปลี่ยนแปลง หรือทำลาย โดยไม่ได้รับอนุมัติจากสหกรณ์

ข้อ 59. ผู้ใช้งาน มีส่วนร่วมและมีสิทธิโดยชอบธรรม ที่จะเก็บ ดูแลรักษา ใช้งานและป้องกันข้อมูลของสหกรณ์ หรือข้อมูลส่วนบุคคลตามเห็นสมควร และไม่อนุญาตให้บุคคลหนึ่งบุคคลใดละเมิดต่อข้อมูลส่วนบุคคล โดยไม่ได้รับอนุญาตจากผู้ใช้งาน หากเกิดการสูญหาย โดยนำไปใช้ในทางที่ผิด การเผยแพร่โดยไม่ได้รับอนุญาตผู้ใช้งานต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้นด้วย เว้นแต่กรณีสหกรณ์ต้องการตรวจสอบ โดยแต่งตั้งผู้ทำหน้าที่ทำการตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลา โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

หมวด 11
การบริหารจัดการด้านเทคโนโลยีสารสนเทศ
(IT Infrastructure Management)

ข้อ 60. ผู้ใช้งาน ที่จะทำการพัฒนา ปรับปรุงหรือแก้ไข เปลี่ยนแปลง ระบบฐานข้อมูลหรือระบบเทคโนโลยีสารสนเทศของสหกรณ์ ให้เหมาะสมและเพียงพอ ต้องแจ้งให้ผู้ดูแลระบบพิจารณาร่วมกับกลุ่มงานเทคโนโลยีสารสนเทศและกลุ่มงานอื่นที่เกี่ยวข้องก่อน เพื่อให้ระบบบัญชีคอมพิวเตอร์ มีความเชื่อมโยงและประมวลผลได้ถูกต้อง ครบถ้วน และให้เป็นไปตามมติของคณะกรรมการดำเนินการ

สำหรับการพัฒนา ปรับปรุงหรือแก้ไข เปลี่ยนแปลง ระบบฐานข้อมูลหรือระบบเทคโนโลยีสารสนเทศของสหกรณ์ต้องไม่ดำเนินการที่จะก่อให้เกิดผลกระทบ ดังนี้

(1) กระทบหรือทำลายโครงสร้างของระบบเทคโนโลยีสารสนเทศของสหกรณ์ และระบบฐานข้อมูลของสหกรณ์ที่มีอยู่ในปัจจุบัน

(2) ทำลายกลไกการควบคุมและรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศของสหกรณ์ รวมทั้งการกระทำในลักษณะที่เป็นการแอบใช้รหัสผ่าน การลักลอบทำสำเนาข้อมูลบุคคลอื่น หรือแกะรหัสผ่านของบุคคลอื่น

(3) กระทำซ้ำโปรแกรมหรือแฝงตัวโปรแกรมไปกับโปรแกรมอื่น ในลักษณะเช่นเดียวกับภัยคุกคามทางไซเบอร์

(4) ทำลายระบบจำกัดสิทธิ์การใช้ ระบบเทคโนโลยีสารสนเทศหรือก่อเกิดสิทธิ หรือมีความสำคัญในการเข้าถึงข้อมูลหรือครอบครองทรัพยากรระบบมากกว่าผู้ใช้อื่น

(5) สร้างเว็บเพจ บนเครือข่าย เสนอข้อมูลผิดกฎหมาย ละเมิดลิขสิทธิ์ แสดงข้อความรูปภาพที่ไม่เหมาะสม หรือขัดต่อศีลธรรมประเพณีอันดีงามของประเทศ

ข้อ 61. ห้ามติดตั้งอุปกรณ์อื่นหรือกระทำการใด ๆ เพื่อให้เข้าถึงระบบเทคโนโลยีสารสนเทศของสหกรณ์โดยไม่ได้รับอนุญาตจากสหกรณ์

ข้อ 62. ห้ามต่อพ่วงเครื่องคอมพิวเตอร์แม่ข่ายร่วมกับเครื่องที่ใช้ต่อ INTERNET โดยเด็ดขาด

หมวด 12
ซอฟต์แวร์และลิขสิทธิ์
(Software Licensing and intellectual Property)

ข้อ 63. สหกรณ์ให้ความสำคัญ เรื่องสินทรัพย์ทางปัญญา ทั้งนี้ ระบบคอมพิวเตอร์ที่สหกรณ์ใช้อนุญาตให้ใช้งานหรือที่สหกรณ์มีลิขสิทธิ์ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และห้ามไม่ให้ผู้ใช้งาน ทำการติดตั้งหรือใช้งาน ระบบคอมพิวเตอร์อื่นที่ไม่มีลิขสิทธิ์ หากตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ์ ให้ถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานต้องรับผิดชอบผู้เดียว

ข้อ 64. ระบบคอมพิวเตอร์ที่สหกรณ์จัดเตรียมไว้ให้ผู้ใช้งาน ถือว่าเป็นสิ่งจำเป็นในการปฏิบัติงาน ห้ามมิให้ผู้ใช้งาน ทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไขหรือทำสำเนาเพื่อนำไปใช้งานที่อื่น

หมวด 13
การป้องกันโปรแกรมที่ไม่ประสงค์ดี
(Preventing Malware)

ข้อ 65. ติดตั้งระบบตรวจจับการบุกรุก (Intrusion Detection System) เพื่อตรวจสอบการใช้งาน ที่มีลักษณะที่ผิดปกติและภัยคุกคามทางไซเบอร์

ข้อ 66. คอมพิวเตอร์ของผู้ใช้งาน ต้องติดตั้งโปรแกรมป้องกันไวรัส (Antivirus) ตามที่สหกรณ์ได้ประกาศให้ใช้ เว้นแต่คอมพิวเตอร์นั้นเป็นเครื่องเพื่อการศึกษา พัฒนา ระบบป้องกัน โดยต้องได้รับอนุญาตจากผู้ดูแลระบบของสหกรณ์

ข้อ 67. ระบบคอมพิวเตอร์ในส่วนของซอฟต์แวร์ (Software) ที่ได้รับอนุญาตจากผู้ใช้งาน ต้องทำการตรวจสอบภัยคุกคามทางไซเบอร์ โดยโปรแกรมป้องกันไวรัส (Antivirus) ก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง

ข้อ 68. ผู้ใช้งาน ต้องพึงระวังภัยคุกคามทางไซเบอร์ อยู่ตลอดเวลา หากพบสิ่งที่ผิดปกติ ใช้งานต้องไม่ทำการเผยแพร่โปรแกรมอันตรายใดๆ ที่อาจก่อให้เกิดความเสียหายมาสู่สินทรัพย์ของสหกรณ์ และต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่เครือข่าย ทั้งนี้ต้องแจ้งให้ผู้ดูแลระบบทราบทันที

ข้อ 69. ผู้ใช้งาน ต้องปรับปรุงข้อมูล สำหรับตรวจสอบและปรับปรุงระบบปฏิบัติการ (Update patch) ให้ใหม่อยู่เสมอ เพื่อป้องกันความเสียหายที่อาจเกิดขึ้น

ข้อ 70. จัดทำแผนป้องกันภัยคุกคามทางไซเบอร์เป็น 3 ระดับ คือ

(1) ระดับไม่ร้ายแรง หมายถึง ภัยคุกคามทางไซเบอร์ที่มีความเสี่ยงอย่างนัยสำคัญถึงระดับที่ทำให้ระบบคอมพิวเตอร์ของสหกรณ์โครงสร้างพื้นฐานสำคัญของสหกรณ์หรือการให้บริการของสหกรณ์ด้อยประสิทธิภาพลง

(2) ระดับร้ายแรง หมายถึง ภัยคุกคามที่มีลักษณะการเพิ่มขึ้นอย่างมีนัยสำคัญของการโจมตีระบบคอมพิวเตอร์ คอมพิวเตอร์ หรือข้อมูลคอมพิวเตอร์ โดยมุ่งหมายเพื่อโจมตีโครงสร้างพื้นฐานสำคัญของสหกรณ์และการโจมตีดังกล่าวมีผลทำให้ระบบคอมพิวเตอร์หรือความมั่นคงของสหกรณ์จนไม่สามารถทำงานหรือให้บริการได้

(3) ระดับวิกฤต หมายถึง เป็นภัยคุกคามทางไซเบอร์ที่เกิดจากการโจมตีระบบคอมพิวเตอร์ คอมพิวเตอร์ หรือข้อมูลคอมพิวเตอร์ ในระดับที่สูงกว่าระดับภัยคุกคามทางไซเบอร์และระดับร้ายแรง โดยส่งผลกระทบรุนแรง ต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศของสหกรณ์ในลักษณะที่เป็นวงกว้าง จนทำให้การทำงานของสหกรณ์หรือการให้บริการโครงสร้างพื้นฐานสำคัญของสหกรณ์ล้มเหลวทั้งระบบ

รวมทั้งให้จัดทำแผนรับสถานการณ์ฉุกเฉินต่าง ๆ เช่น แผนป้องกันอัคคีภัยของระบบสารสนเทศ แผนบริหารความต่อเนื่องทางธุรกิจ (Contingency Plan) แผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติ แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ เป็นต้น

หมวด 14
การรักษาความปลอดภัยของข้อมูลคอมพิวเตอร์
(Data Security)

ข้อ 71. กระทำการสำรองข้อมูลคอมพิวเตอร์ของแต่ละระบบงานเป็นประจำในเวลาปิดงาน ทุกวันทำการ

ข้อ 72. กระทำการสำรองฐานข้อมูลคอมพิวเตอร์ของแต่ละระบบงานเป็นประจำในเวลาปิดงาน ทุกวันทำการ

ข้อ 73. ผู้สำรองฐานข้อมูลที่ได้รับมอบหมาย ทำการจัดเก็บข้อมูลชุดสำรองไว้ในสื่อภายนอก ได้แก่ CD, DVD หรือ External Hard disk หรือ Cloud อย่างน้อยสัปดาห์ละ 3 วัน และส่งมอบให้ผู้เก็บรักษาความปลอดภัยชุดสำรองฐานข้อมูล อย่างน้อยเดือนละ 1 ครั้ง

ข้อ 74. ติดฉลากบอกรายละเอียดบนสื่อเก็บข้อมูลโดยระบุวัน เวลาที่สำรองข้อมูลให้ชัดเจน

ข้อ 75. มีการทดสอบสื่อเก็บข้อมูลที่สำรองโดยการเรียกคืนข้อมูล อย่างน้อยเดือนละ 1 ครั้ง

ข้อ 76. มอบหมายผู้เก็บรักษาความปลอดภัยชุดสำรองฐานข้อมูล เพื่อป้องกันเหตุฉุกเฉินและเพื่อให้สามารถกู้ระบบกลับคืนได้ภายในระยะเวลาที่เหมาะสม ไว้ดังนี้

(1) ผู้จัดการสหกรณ์หรือผู้ดูแลระบบ จำนวน 1 ชุด

(2) เหรัญญิก จำนวน 1 ชุด

(3) ผู้สำรองฐานข้อมูล จำนวน 1 ชุด

ข้อ 77. ในกรณีที่มีปัญหาเกี่ยวกับการปฏิบัติตามระเบียบนี้ ให้คณะกรรมการดำเนินการเป็นผู้มีอำนาจวินิจฉัย

ข้อ 78. ให้ประธานกรรมการเป็นผู้รักษาการให้เป็นไปตามระเบียบนี้

ประกาศ ณ วันที่ 29 ธันวาคม พ.ศ. 2568

ลงชื่อ 

(นายสุทัศน์ ประสาธน์สุวรรณ์)

ประธานกรรมการ

สหกรณ์ออมทรัพย์ครูเชียงใหม่ จำกัด