ระเบียบสหกรณ์ออมทรัพย์กรมการทหารสื่อสาร จำกัด
ว่าด้วยวิธีปฏิบัติในการควบคุมภายในและการรักษาความปลอดภัย ด้านเทคโนโลยีสารสนเทศของสหกรณ์ พ.ศ. 2566

เพื่อให้การใช้เทคโนโลยีสารสนเทศของสหกรณ์ออมทรัพย์กรมการทหารสื่อสาร จำกัดมีความมั่นคงปลอดภัย และมีความน่าเชื่อถือ รวมทั้งเพื่อป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้เครื่องคอมพิวเตอร์ระบบเครือข่ายคอมพิวเตอร์และระบบสารสนเทศ ประกอบกับสภาวะการณ์ในปัจจุบัน ภัยคุกคามทางไซเบอร์มีหลากหลายรูปแบบ ซึ่งอาจส่งผลต่อการทำธุรกรรมทางการเงินของสหกรณ์อาศัยอำนาจตามความในใจข้อบังคับของสหกรณ์ออมทรัพย์กรมการทหารสื่อสาร จำกัด มติที่ประชุมคณะกรรมการดำเนินการในการประชุมครั้งที่ 10/66 เมื่อวันที่ 27 ต.ค.66 และให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และพระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์พ.ศ.2562 จึงกำหนดระเบียบว่าด้วย วิธีปฏิบัติในการควบคุมภายใน และการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของสหกรณ์ พ.ศ. 2566 ดังต่อไปนี้

หมวด 1
บททั่วไป

ข้อ 1 ระเบียบนี้เรียกว่า “ระเบียบสหกรณ์ออมทรัพย์กรมการทหารสื่อสาร จำกัด ว่าด้วยวิธีปฏิบัติในการควบคุมภายในและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของสหกรณ์พ.ศ. 2565”

ข้อ 2 ระเบียบนี้ให้ใช้บังคับตั้งแต่วันที่ถัดจากวันประกาศเป็นต้นไป

ข้อ 3 ระเบียบนี้ให้ใช้บังคับแก่บุคคลกรในสังกัดสหกรณ์ออมทรัพย์กรมการทหารสื่อสารจำกัด รวมทั้งบุคคลนิติบุคคลอื่นที่เกี่ยวข้องภายใต้ระยะเวลาและเงื่อนไขข้อตกลงที่สหกรณ์กำหนดที่เข้ามาดำเนินการเกี่ยวกับสารสนเทศและระบบสารสนเทศของสหกรณ์ออมทรัพย์กรมการทหารสื่อสาร จำกัด

ข้อ 4 ในระเบียบนี้

“สหกรณ์” หมายความว่า สหกรณ์ออมทรัพย์กรมการทหารสื่อสาร จำกัด

“คณะกรรมการดำเนินการ” หมายความว่า คณะกรรมการดำเนินการสหกรณ์ออมทรัพย์กรมการทหารสื่อสาร จำกัด

“ประธานกรรมการ” หมายความว่า ประธานคณะกรรมการดำเนินการ สหกรณ์ออมทรัพย์กรมการทหารสื่อสาร จำกัด

“ผู้จัดการ” หมายความว่า ผู้จัดการ สหกรณ์ออมทรัพย์กรมการทหารสื่อสาร จำกัด

“เจ้าหน้าที่” หมายความว่า เจ้าหน้าที่สหกรณ์ออมทรัพย์กรมการทหารสื่อสาร จำกัด

“บุคลากร” หมายความว่าคณะกรรมการดำเนินการ กรรมการ อนุกรรมการ คณะทำงานสมาชิก ตลอดจนบุคคลภายนอกที่ได้รับอนุญาตให้ทำงานและเข้าถึงข้อมูลในสหกรณ์ “ผู้ดูแลระบบ” หมายความว่า เจ้าหน้าที่ที่ได้รับมอบหมายจากจากสหกรณ์ให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบ และเครือข่ายคอมพิวเตอร์ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์เพื่อการจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์

“เครื่องคอมพิวเตอร์” หมายความว่า อุปกรณ์หรือเครื่องคอมพิวเตอร์ทั้งหลายซึ่งอาจมีลักษณะเป็นเครื่องคอมพิวเตอร์แบบตั้งโต๊ะ เครื่องคอมพิวเตอร์แบบโน้ตบุ๊ก อุปกรณ์แบบพกพา เช่น โทรศัพท์มือถือแท็ปเล็ต เป็นต้น เครื่องคอมพิวเตอร์แม่ข่าย หรืออุปกรณ์อื่นใด ที่ทำหน้าที่ได้เสมือนเครื่องคอมพิวเตอร์ทั้งที่ใช้งานอยู่ภายในสหกรณ์หรือภายนอกแล้วเชื่อมต่อเข้ากับระบบเครือข่าย

“ระบบคอมพิวเตอร์” หมายความว่า อุปกรณ์ที่ประกอบด้วย ฮาร์ดแวร์และซอฟต์แวร์ ได้แก่ ซอฟต์แวร์ระบบปฏิบัติการ (Operating System) และซอฟต์แวร์ประยุกต์ (Application Software) เพื่อใช้เป็นระบบจัดทำข้อมูล เช่น ตัวเลข ข้อความ รูปภาพ เสียง หรืออยู่ในรูปอื่น ๆ เป็นต้น และใช้ประมวลผลข้อมูลเป็นสารสนเทศที่นำไปใช้ประโยชน์ได้

“ระบบเครือข่ายคอมพิวเตอร์” หมายความว่า ระบบคอมพิวเตอร์และอุปกรณ์ที่เชื่อมต่อกันเป็นเครือข่ายด้วยอุปกรณ์เชื่อมต่อเครือข่ายและสื่อการเชื่อมต่อที่สหกรณ์สร้างขึ้น ทั้งที่เป็นสื่อการเชื่อมต่อแบบใช้สายและไร้สาย เพื่อการรับส่งข้อมูลและสารสนเทศระหว่างระบบคอมพิวเตอร์รวมถึงการรับส่งข้อมูลและสารสนเทศภายในระบบสารสนเทศเดียวกัน หรือระหว่างระบบสารสนเทศที่ถูกนำมาใช้งานร่วมกันรวมถึงเครือข่ายอินทราเน็ต (Intranet) ซึ่งเป็นเครือข่ายภายใน และเครือข่ายอินเทอร์เน็ต (Internet) ซึ่งเป็นเครือข่ายภายนอก ของสหกรณ์ด้วย

“ข้อมูล” หมายความว่า สิ่งที่สื่อความหมายให้รู้เรื่องราว ข้อเท็จจริง หรือสิ่งใด ๆ รวมถึงข้อมูลส่วนบุคคล ไม่ว่าจะได้จัดทำไว้ในรูปแบบของเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ รูปภาพการบันทึกภาพหรือเสียง หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้

“สารสนเทศ” หมายความว่า ข้อมูลต่าง ๆ ที่ได้ผ่านการเปลี่ยนแปลงประมวลผลหรือวิเคราะห์สรุปผลด้วยวิธีการต่าง ๆ ที่เก็บรวบรวมไว้เพื่อนำไปใช้ประโยชน์ในการปฏิบัติงาน การบริหาร การวางแผนการตัดสินใจและอื่น ๆ ตามความต้องการ

“ระบบสารสนเทศ” หมายความว่า ระบบที่ใช้จัดเก็บและประมวลผลข้อมูลที่มีการนำเอาฮาร์ดแวร์ซอฟต์แวร์บุคลากร แนวปฏิบัติและข้อมูล ซึ่งทำงานประสานกันเพื่อจัดเตรียมสารสนเทศที่จำเป็นให้กับสหกรณ์

“ไซเบอร์” หมายความว่า ข้อมูลและการ สื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ เครือข่ายอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการระบบเครือข่ายที่ คล้ายคลึงกัน ที่เชื่อมต่อกันเป็นการทั่วไป

“ภัยคุกคาม” หมายความว่า อันตรายที่อาจเกิดขึ้นกับสารสนเทศโดยบุคคล สิ่งต่าง ๆหรือเหตุการณ์ทั้งเจตนาและไม่เจตนา อันเป็นเหตุทำให้ระบบสารสนเทศถูกเปิดเผย เปลี่ยนแปลง บิดเบือน ทำลายปฏิเสธการทำงาน หรือการกระทำอื่นตามความต้องการของภัยคุกคามนั้น

“ภัยคุกคามทางไซเบอร์” หมายความว่า การกระทำหรือการดำเนินการใด ๆ โดยมิชอบที่ใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมประสงค์ร้าย โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ข้อมูลคอมพิวเตอร์หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ระบบคอมพิวเตอร์หรือข้อมูลอื่นที่เกี่ยวข้อง

“ช่องโหว” หมายความว่า จุดอ่อนหรือข้อบกพร่องใด ๆ ของระบบคอมพิวเตอร์และระบบสารสนเทศซึ่งหากมีภัยคุกคามในรูปแบบที่เหมาะกัน สามารถถูกนำไปใช้ประโยชน์ เพื่อก่อให้เกิดความเสียหายต่อสารสนเทศและข้อมูล

“ความเสี่ยง” หมายความว่า โอกาสที่เอื้อให้ภัยคุกคามต่าง ๆ สร้างความเสียหายในรูปแบบที่เหมาะกับช่องโหว่ ที่มีอยู่ในระบบคอมพิวเตอร์และระบบสารสนเทศ

“ประเมินความเสี่ยง” (Risk Assessment) หมายความว่า กระบวนการวิเคราะห์ภัยคุกคามต่างๆ และความอ่อนแอของระบบคอมพิวเตอร์และระบบสารสนเทศ รวมทั้งผลกระทบจากการ สูญเสียสารสนเทศหรือการสูญเสียความสามารถในการรักษาความมั่นคงปลอดภัยของสารสนเทศ การประเมินความเสี่ยงใช้เป็นพื้นฐานในการกำหนดมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมให้สารสนเทศต่อไป

“การรักษาความมั่นคงปลอดภัยสารสนเทศ” หมายความว่า การดำเนินการเพื่อให้สารสนเทศมีคุณสมบัติดังนี้มีการรักษาความลับของข้อมูล (Confidentiality) มีการรักษาความถูกต้องของข้อมูล (Integrity) และมีสภาพความพร้อมใช้งาน (Availability)

“การรักษาความมั่นคงปลอดภัย ไซเบอร์” หมายความว่า มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศ

“เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์” หมายความว่า เหตุการณ์ที่เกิดจากการกระทำหรือการดำเนินการใด ๆ ที่มิชอบซึ่งกระทำผ่านทางคอมพิวเตอร์หรือระบบคอมพิวเตอร์ซึ่งอาจเกิดความเสียหายหรือผลกระทบต่อการรักษาความมั่นคงปลอดภัยไซเบอร์หรือความมั่นคงปลอดภัยไซเบอร์ของคอมพิวเตอร์ข้อมูลคอมพิวเตอร์ระบบคอมพิวเตอร์หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์

“สินทรัพย์ด้านเทคโนโลยีสารสนเทศ” หมายความว่า เครื่องคอมพิวเตอร์เครื่องคอมพิวเตอร์แม่ข่ายระบบสารสนเทศ ฐานข้อมูล ไฟล์ข้อมูล ซอฟต์แวร์เครื่องมือในการพัฒนา อุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย อุปกรณ์สื่อสาร สื่อบันทึกข้อมูลภายนอก และอุปกรณ์ต่อพ่วงทุกชนิด

“ศูนย์คอมพิวเตอร์” หมายความว่า พื้นที่ที่ใช้จัดวางเครื่องคอมพิวเตอร์แม่ข่าย ระบบจัดเก็บข้อมูลภายนอก ระบบเครือข่ายคอมพิวเตอร์และอุปกรณ์สื่อสารต่าง ๆ ของสหกรณ์ไว้เป็นศูนย์กลางในการประมวลผลข้อมูลสารสนเทศสำหรับใช้ปฏิบัติงานของสหกรณ์

ข้อ 5 ให้ประธานกรรมการเป็นผู้รักษาการให้เป็นไปตามระเบียบนี้ในกรณีที่มีปัญหาเกี่ยวกับการปฏิบัติตามระเบียบนี้ประธานกรรมการอาจใช้ข้อมูลจากคณะกรรมการ กรรมการ อนุกรรมการหรือคณะทำงาน ในการวินิจฉัยชี้ขาดและให้ถือเป็นที่สิ้นสุด

หมวด 2
วัตถุประสงค์

ข้อ 6 วัตถุประสงค์ของระเบียบนี้

(1) เพื่อให้บุคลากรระมัดระวังในการใช้เครื่องคอมพิวเตอร์และตระหนักถึงความเสี่ยงที่อาจเกิดขึ้นกับการใช้เทคโนโลยีสารสนเทศ โดยเจตนาหรือไม่เจตนาก็ตาม

(2) เพื่อให้บุคลากรใช้เทคโนโลยีสารสนเทศอย่างถูกต้องตามบทบาทและหน้าที่ที่ได้รับมอบหมาย

(3) เพื่อให้การใช้งานเทคโนโลยีสารสนเทศของสหกรณ์มีความมั่นคงปลอดภัย และสามารถใช้งานได้อย่างมีประสิทธิภาพ

(4) เพื่อเสริมสร้างความน่าเชื่อถือให้กับสมาชิกและลูกค้าของสหกรณ์ในด้านความสามารถในการให้บริการ รวมทั้งการรักษาความลับของข้อมูลและระบบเทคโนโลยีสารสนเทศ

(5) เพื่อเป็นแนวทางกำหนดในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศของสหกรณ์ให้สอดคล้องกับการควบคุมภายในที่ดีด้านสารสนเทศ และให้เป็นไปตามพระราชบัญญัติความมั่นคงปลอดภัยทางไซเบอร์พ.ศ. 2562

หมวด 3
ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม

ข้อ 7 แนวทางการบริหารจัดการความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศ

(1) ต้องจัดทำนโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศ สำหรับระบบสารสนเทศของสหกรณ์ให้เป็นลายลักษณ์อักษร และเอกสารนโยบายดังกล่าว ต้องได้รับการอนุมัติจากประธานกรรมการก่อนนำไปใช้งานและต้องเผยแพร่ให้เจ้าหน้าที่และหน่วยงานภายนอกทั้งหมดที่เกี่ยวข้องได้รับทราบ

(2) ต้องดำเนินการตรวจสอบ ทบทวนนโยบายที่เกี่ยวข้องกับความปลอดภัยด้านเทคโนโลยีสารสนเทศ โดยจะต้องทบทวนตามรอบที่กำหนด หรือเมื่อมีการเปลี่ยนแปลงที่มีผลกระทบต่อการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของสหกรณ์หรืออย่างน้อย 1 ครั้งต่อปี

(3) การกำหนดมาตรการ หรือระบบบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ต้องผ่านการประเมินความเสี่ยง (Risk Management) ช่องโหว่ (Vulnerability) ภัยคุกคาม (Threat) เพื่อให้ได้มาตรการป้องกันที่เหมาะสมกับระบบเทคโนโลยีสารสนเทศของสหกรณ์โดยการจัดทำแผนบริหารจัดการความเสี่ยง (Risk Management Plan) และกำหนดให้มีการปรับปรุงให้ทันสมัยอยู่เสมอทั้งนี้ประธานกรรมการอาจมอบหมายให้คณะทำงานบริหารระบบเทคโนโลยีสารสนเทศเป็นผู้สนับสนุนการดำเนินงานข้างต้น และรายงานผลให้ทราบ

ข้อ 8 สถานที่ซึ่งติดตั้งระบบเทคโนโลยีสารสนเทศและการสื่อสารหลักของสหกรณ์ต้องมีการควบคุมการเข้าถึงทางกายภาพ โดยกำหนดมาตรการเกี่ยวกับการอนุญาตให้มีการเข้าออกสถานที่ การกำหนดสิทธิ์ในการเข้าออกสถานที่การบันทึกข้อมูลการเข้าออกเพื่อการตรวจสอบ การทบทวนรายชื่อผู้ได้รับอนุญาตและสิทธิ์ ในการเข้าออกสถานที่ เพื่อจุดประสงค์ในการเฝ้าระวัง ควบคุม การรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิด ขึ้นได้

ข้อ 9 ต้องมีการจำแนกและกำหนดพื้นที่ของระบบเทคโนโลยีสารสนเทศและการสื่อสารอย่างเหมาะสม มีการแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารให้ชัดเจนพื้นที่สำนักงาน พื้นที่จัดส่งและรับของ พื้นที่ทำงานของผู้ดูแลระบบ พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยแบ่งแยกพื้นที่ปลอดภัย การใช้งานพื้นที่ใช้งานเครือข่ายไร้สาย มีการแยกสถานที่ซึ่งติดตั้งระบบเทคโนโลยีสารสนเทศและการสื่อสารออกจากสถานที่ทำงานทั่วไป มีกระบวนการควบคุมการเข้าออกพื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัยให้เข้าออกได้เฉพาะผู้ที่มีหน้าที่รับผิดชอบและผู้ที่ได้รับอนุญาตอย่างเป็นลายลักษณ์อักษร รวมทั้งจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งาน และประกาศให้ทราบทั่วกัน

ข้อ 10 ต้องมีการสร้างความมั่นคงปลอดภัยทางกายภาพต่อสำนักงาน ห้องทำงาน และสินทรัพย์อื่นๆและต้องจัดให้มีการป้องกันภัยคุกคามต่าง ๆ เช่น ไฟไหม้ น้ำท่วม แผ่นดินไหว การก่อความไม่สงบ โรคระบาดเป็นต้น รวมถึงการปฏิบัติงานในพื้นที่ที่ต้องรักษาความมั่นคงปลอดภัยต้องมีการจัดการป้องกันที่เพียงพอ

ข้อ 11 การปฏิบัติงานในพื้นที่ควบคุมการปฏิบัติงาน

(1) ต้องมีการควบคุมการปฏิบัติงานของหน่วยงานภายนอกในบริเวณพื้นที่ควบคุมได้แก่ ไม่อนุญาตให้ถ่ายภาพหรือวีดีโอในพื้นที่ควบคุม หรือทำกิจกรรมอื่นใดที่เป็นการบันทึกภาพของระบบหรือภาพภายในพื้นที่ควบคุม หากมีความจำเป็นต้องแจ้งเจ้าหน้าที่ผู้กำกับดูแล (2) ต้องมีป้ายประกาศข้อความ “ห้ามเข้าก่อนได้รับอนุญาต” และ “ห้ามถ่ายภาพหรือวีดีโอ”บริเวณภายในพื้นที่ควบคุมการปฏิบัติงาน

ข้อ 12 ข้อกำหนดด้านความมั่นคงปลอดภัยของอุปกรณ์

(1) ต้องจัดวางและป้องกันอุปกรณ์ของสหกรณ์ เพื่อลดความเสี่ยงจากภัยคุกคามทางด้านสิ่งแวดล้อมและอันตรายต่าง ๆ รวมทั้งความเสี่ยงในการเข้าถึงอุปกรณ์โดยไม่ได้รับอนุญาต และต้องมีการควบคุมการนำอุปกรณ์เข้าออกในบริเวณพื้นที่ควบคุม

(2) อุปกรณ์ที่มีความสำคัญต่อระบบสารสนเทศ ต้องได้รับการปิดล็อคและป้องกันการเข้าถึง

(3) ต้องมีกลไกการป้องกันการล้มเหลวของระบบและอุปกรณ์สนับสนุน ต่าง ๆ อาทิ ระบบไฟฟ้า ระบบไฟฟ้าสำรอง ระบบตรวจจับและดับเพลิง ระบบควบคุมอุณหภูมิและความชื้น

(4) ต้องกำหนดให้มีการบำรุงรักษาอุปกรณ์ต่าง ๆ อย่างสม่ำเสมอ เพื่อให้อุปกรณ์ทำงานได้อย่างต่อเนื่องและอยู่ในสภาพที่มีความสมบูรณ์ต่อการใช้งาน เป็นไปตามมาตรฐานหรือคุณสมบัติของอุปกรณ์แต่ละระบบ ตามระยะเวลาและขั้นตอนที่อุปกรณ์แต่ละประเภทกำหนดหรือตามแผนการบำรุงรักษาระบบคอมพิวเตอร์นั้น ๆ

(5) ต้องกำหนดแนวทางปฏิบัติให้มีวิธีการในการตรวจสอบอุปกรณ์ซึ่งมีข้อมูลสำคัญเก็บไว้เพื่อป้องกันการรั่วไหล หรือการเปิดเผยข้อมูลดังกล่าว ก่อนนำอุปกรณ์ไปแจกจ่ายหรือการนำกลับมาใช้งานใหม่

(6) ต้องกำหนดการควบคุมเอกสาร ข้อมูล หรือสื่อต่าง ๆ ที่มีข้อมูลสำคัญจัดเก็บไม่ให้วางทิ้งไว้บนโต๊ะทำงาน หรือในสถานที่ที่ไม่ปลอดภัยในขณะที่ไม่ได้นำมาใช้งาน ตลอดจนการควบคุมหน้าจอคอมพิวเตอร์ไม่ให้มีข้อมูลสำคัญปรากฏในขณะที่ไม่ได้ใช้งาน

ข้อ 13 จัดทำแผนป้องกันภัยคุกคามทางไซเบอร์เป็น 3 ระดับ คือ

ระดับไม่ร้ายแรง หมายถึง ภัยคุกคามทางไซเบอร์ที่มีความเสี่ยงอย่างนัยสำคัญถึงระดับที่ทำให้ระบบคอมพิวเตอร์ของสหกรณ์โครงสร้างพื้นฐานสำคัญของสหกรณ์ หรือการให้บริการของสหกรณ์ด้อยประสิทธิภาพลง

ระดับร้ายแรง หมายถึง ภัยคุกคามที่มีลักษณะการเพิ่มขึ้นอย่างมีนัยสำคัญของการโจมตีระบบคอมพิวเตอร์คอมพิวเตอร์ หรือข้อมูลคอมพิวเตอร์โดยมุ่งหมายเพื่อโจมตีโครงสร้างพื้นฐานสำคัญของสหกรณ์ และการโจมตีดังกล่าวมีผลทำให้ระบบคอมพิวเตอร์ หรือความมั่นคงของสหกรณ์จนไม่สามารถทำงานหรือให้บริการได้

ระดับวิกฤต หมายถึง เป็นภัยคุกคามทางไซเบอร์ที่เกิดจากการโจมตีระบบคอมพิวเตอร์คอมพิวเตอร์ข้อมูลคอมพิวเตอร์ในระดับที่สูงกว่าระดับภัยคุกคามทางไซเบอร์ และระดับร้ายแรงโดยส่งผลกระทบรุนแรง ต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศของสหกรณ์ในลักษณะที่เป็นวงกว้าง จนทำให้การทำงานของสหกรณ์หรือการให้บริการโครงสร้างพื้นฐานสำคัญของสหกรณ์ล้มเหลวทั้งระบบ รวมทั้งให้จัดทำแผนรับสถานการณ์ฉุกเฉินต่าง ๆ เช่น แผนป้องกันอัคคีภัยของระบบสารสนเทศ แผนบริหารความต่อเนื่องทางธุรกิจ (Contingency Plan) แผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ เป็นต้น

หมวด 4
ความมั่นคงปลอดภัยสำหรับการปฏิบัติงาน

ข้อ 14 การกำหนดขั้นตอนการปฏิบัติงาน

(1) ต้องจัดทำคู่มือ หรือขั้นตอนการปฏิบัติงานสารสนเทศ เช่น ขั้นตอนการแจ้งเหตุขัดข้อง ขั้นตอนการกู้คืน ขั้นตอนการบำรุงรักษาและดูแลระบบ ซึ่งประกอบไปด้วยรายละเอียดขั้นตอนการปฏิบัติและเจ้าหน้าที่หรือหน่วยงานผู้รับผิดชอบ เป็นต้น

(2) คู่มือและขั้นตอนการปฏิบัติงานต้องได้รับการปรับปรุงเมื่อมีการปรับเปลี่ยนขั้นตอนการปฏิบัติงานนั้น ๆ โดยคู่มือและขั้นตอนการปฏิบัติงานทุกฉบับต้องได้รับการทบทวนอย่างน้อยปีละ 1 ครั้ง การกำหนดการบำรุงรักษาระบบสารสนเทศ ต้องกำหนดให้มีการบำรุงรักษาอย่างถูกต้องและสม่ำเสมอ เช่น จัดให้มีการซ่อมบำรุงอย่างน้อยปีละ 1 ครั้ง จัดทำสัญญาการบำรุงรักษาสำหรับระบบและอุปกรณ์คอมพิวเตอร์

ข้อ 16 การบริหารจัดการทะเบียนสินทรัพย์ด้านเทคโนโลยีสารสนเทศ

(1) ต้องจัดทำบัญชีหรือทะเบียนสินทรัพย์ประเภทอุปกรณ์คอมพิวเตอร์รวมถึงอุปกรณ์อื่นที่เกี่ยวข้องกับการประมวลผลสารสนเทศของหน่วยงานหรือระบบงาน และอุปกรณ์เชื่อมต่อเครือข่ายสารสนเทศซึ่งสินทรัพย์ทั้งหมดต้องมีการระบุผู้ถือครองหรือผู้รับผิดชอบ รวมถึงมีหลักฐานเอกสารรับสินทรัพย์ไปถือครองหรือรับผิดชอบ และมีการปรับปรุงบัญชีให้เป็นปัจจุบัน

(2) ต้องกำกับดูและการใช้สินทรัพย์ให้เป็นไปอย่างเหมาะสม เพื่อให้เกิดการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

(3) กำหนดมาตรการหรือเทคนิคในการทำลายข้อมูลสำคัญในสื่อบันทึกข้อมูลก่อนจะจำหน่ายหรือนำกลับมาใช้งานใหม่ทุกครั้ง เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้น

(4) เมื่อสิ้นสุดการใช้งานหรือความรับผิดชอบต่อสินทรัพย์ผู้ถือครองหรือผู้รับผิดชอบสินทรัพย์ต้องส่งคืนสินทรัพย์พร้อมมีเอกสารหลักฐานการส่งคืนสินทรัพย์

(5) กรณีสินทรัพย์เกิดความเสียหายและต้องส่งซ่อม ให้ควบคุมการส่งออกไปซ่อมแซมนอกสถานที่เพื่อป้องกันการสูญหาย หรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต กรณีสินทรัพย์เป็นข้อมูลสำคัญต้องทำการทำลายข้อมูลทิ้งเพื่อไม่ให้ผู้อื่นสามารถเข้าถึงได้

ข้อ 17 การควบคุมการใช้งานและบริหารจัดการอุปกรณ์คอมพิวเตอร์แบบพกพา

(1) ต้องนำอุปกรณ์คอมพิวเตอร์แบบพกพาส่วนตัว หรืออุปกรณ์คอมพิวเตอร์แบบพกพาของสหกรณ์ที่ได้รับอนุมัติจากผู้บังคับบัญชาให้เชื่อมต่อระบบเครือข่ายภายในและเข้าถึงระบบสารสนเทศของสหกรณ์ที่ฝ่ายเทคโนโลยีสารสนเทศ และปฏิบัติตามขั้นตอนที่ฝ่ายเทคโนโลยีสารสนเทศกำหนดเพื่อป้องกันการเข้าถึงระบบสารสนเทศด้วยอุปกรณ์คอมพิวเตอร์แบบพกพาโดยไม่ได้รับอนุญาต

(2) ต้องกำหนดมาตรการระบุและพิสูจน์ตัวตนก่อนเข้าถึงอุปกรณ์คอมพิวเตอร์แบบพกพาด้วยบัญชีผู้ใช้งานและรหัสผ่าน เพื่อป้องกันการเข้าถึงจากผู้อื่นและระมัดระวังมิให้ผู้อื่นเข้าถึงอุปกรณ์แบบพกพาของตน

(3) ต้องดูแลรักษาข้อมูลองค์กรในอุปกรณ์คอมพิวเตอร์แบบพกพาให้สอดคล้องกับข้อกำหนดการบริหารจัดการข้อมูลขององค์กรข้างต้น

ข้อ 18 การควบคุมการใช้งานสารสนเทศ

(1) ผู้ดูแลระบบ มีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิ์ในการผ่านเข้าสู่ระบบ ได้แก่ผู้ใช้งานในการขออนุญาตเข้าระบบงานนั้น จะต้องมีการทำเป็นเอกสารเพื่อขอสิทธิ์ในการเข้าสู่ระบบและกำหนดให้มีการลงนามอนุมัติเอกสารดังกล่าวต้องมีการจัดเก็บไว้เป็นหลักฐาน และให้การส่งมอบสิทธิ์การเข้าถึงข้อมูลสารสนเทศ ให้กำหนดในรูปแบบเนื้อหาภายในสหกรณ์

(2) เจ้าของข้อมูลและเจ้าของระบบงานจะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้น เนื่องจากการให้สิทธิ์เกินความจำเป็นในการใช้งาน จะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่ดังนั้น การกำหนดสิทธิ์ในการเข้าถึงระบบงานต้องกำหนดตามความจำเป็นขั้นต่ำเท่านั้น

(3) ผู้ใช้งานจะต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบงานตามความจำเป็นต่อการใช้งานระบบเทคโนโลยีสารสนเทศ

ข้อ 19 การบริหารจัดการความปลอดภัยเครือข่าย

ผู้ดูแลระบบสารสนเทศต้องบริหารจัดการ การควบคุมเครือข่ายคอมพิวเตอร์เครือข่ายสื่อสารเพื่อป้องกันภัยคุกคาม และมีการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ และแอพพลิเคชัน ที่ทำงานบนเครือข่ายคอมพิวเตอร์รวมทั้งข้อมูลสารสนเทศที่มีการแลกเปลี่ยนบนเครือข่าย ตามกฎหมาย ระเบียบคำสั่งหลักเกณฑ์และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของสหกรณ์ที่ประกาศใช้ในปัจจุบัน

ข้อ 20 การบริหารจัดการผู้ใช้งานในการเข้าถึงระบบสารสนเทศ

(1) การลงทะเบียนผู้ใช้งานใหม่ต้องกำหนดให้มีระเบียบปฏิบัติอย่างเป็นทางการสำหรับการลงทะเบียนผู้ใช้งานใหม่เพื่อให้มีสิทธิ์การเข้าถึงระบบสารสนเทศตามความจำเป็น รวมทั้งระเบียบปฏิบัติสำหรับการยกเลิกสิทธิ์เช่น เมื่อลาออก เกษียณอายุ หรือเมื่อเปลี่ยนตำแหน่งงาน เป็นต้น โดยผู้ใช้งานต้องได้รับการพิจารณาอนุมัติตามขั้นตอน อย่างเคร่งครัด

(2) การจัดการสิทธิ์ผู้ใช้งาน ต้องมีการกำหนดวิธีการในการบริหารจัดการสิทธิ์ทั้งการให้สิทธิ์และการยกเลิกสิทธิ์สำหรับผู้ใช้งานทุกประเภท

(3) การบริหารจัดการสิทธิ์การเข้าถึงระบบสารสนเทศ

(3.1) ต้องกำหนดสิทธิ์ของผู้ใช้งานในการเข้าถึงสารสนเทศและระบบสารสนเทศแต่ละส่วนอย่างชัดเจน รวมทั้งกำหนดสิทธิ์แยกตามหน้าที่ที่รับผิดชอบ

(3.2) ผู้ใช้งานต้องได้รับการตรวจพิสูจน์ตัวตนทุกครั้งก่อนเข้าถึงระบบสารสนเทศ

(3.3) การเข้าสู่ระบบ (Log in) ที่มีความมั่นคงปลอดภัย ต้องกำหนดกระบวนการในการเข้าถึงระบบให้มีความมั่นคงปลอดภัย โดยกำหนดให้ระบบปฏิเสธการให้บริการ หากผู้ใช้งานพิมพ์รหัสผ่านผิดพลาดเกิน 3 ครั้ง

(3.4) ต้องจัดให้มีระบบบริหารจัดการรหัสผ่าน (Password) หรือวิธีการในการตรวจสอบคุณภาพของรหัสผ่าน และมีวิธีการควบคุมดูแลให้ผู้ใช้งานเปลี่ยนรหัสผ่านทุก ๆ 180 วันหรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน

(4) การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน ต้องมีกระบวนการจัดการซึ่งเป็นความลับ

(5) การทบทวนสิทธิ์ในการเข้าถึงระบบสารสนเทศของผู้ใช้งาน ต้องดำเนินการตามระยะเวลาที่กำหนดไว้

(6) การถอนหรือการปรับปรุงสิทธิ์การเข้าถึงของเจ้าหน้าที่และบุคคลภายนอกต่อระบบสารสนเทศ ต้องถูกยกเลิกสิทธิ์เมื่อสิ้นสุดสถานภาพการปฏิบัติงาน การจ้างงานหมดสัญญา หรือสิ้นสุดข้อตกลงการจ้าง และต้องได้รับการปรับปรุงสิทธิ์ให้ถูกต้องอยู่เสมอ

ข้อ 21 การสำรองและกู้คืนข้อมูลสารสนเทศ

(1) ต้องกำหนดการกู้คืนข้อมูลสารสนเทศ ให้สามารถนำกลับมาใช้ได้ในภายหลัง ในกรณีที่เกิดเหตุต่าง ๆ ที่ทำให้ข้อมูลสูญหายหรือถูกทำลายเช่น ภัยจากการโจมตีทางไซเบอร์ระบบล้มเหลวภัยจากธรรมชาติเป็นต้น

(2) กำหนดความถี่ในการทำการสำรองข้อมูล

(3) มีการควบคุมการเข้าถึงทางกายภาพ (Physical Access Control) ของสถานที่ที่เก็บข้อมูลสำรอง สื่อเก็บข้อมูลต้องได้รับการป้องกันสอดคล้องกับระดับความสำคัญของระบบสารสนเทศ

(4) มีการทำเอกสารกระบวนการสำรองข้อมูล และมีการตรวจสอบเป็นวงรอบปฏิบัติประจำ

(5) จัดให้มีทะเบียนการบันทึกข้อมูลที่ทำการสำรองไว้และการเรียกคืนข้อมูลในแต่ละครั้ง

(6) ข้อมูลสำรองต้องได้รับการทดสอบตามห้วงเวลาที่กำหนด เพื่อให้มั่นใจว่าข้อมูลที่สำรองไว้สามารถกู้ข้อมูลกลับมาได้อย่างสมบูรณ์

(7) ลงบันทึกการเก็บสื่อสำรองข้อมูลและสถานที่จัดเก็บต้องได้รับการตรวจสอบเป็นประจำทุกปี

หมวด 5
แนวปฏิบัติพัฒนา และบำรุงระบบสารสนเทศ

ข้อ 22 แนวปฏิบัติด้านความมั่นคงปลอดภัยของระบบสารสนเทศ เป็นส่วนประกอบสำคัญในการบริหารจัดการระบบสารสนเทศตลอดวงจรของการพัฒนาระบบ ทั้งนี้รวมถึงระบบสารสนเทศที่ให้บริการบนเครือข่ายสาธารณะด้วย

(1) การจัดทำข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศจะต้องถูกระบุไว้ในข้อกำหนดในการพัฒนาระบบใหม่หรือการปรับปรุงระบบที่มีอยู่เดิม การพิสูจน์ตัวตนและการกำหนดสิทธิ์ของ

ใช้งานระบบบทบาทหน้าที่ของผู้ใช้งานระบบและเจ้าหน้าที่ดูแลระบบ แนวทางในการป้องกันสินทรัพย์ที่เกี่ยวข้องโดยเฉพาะในด้านการรักษาความลับ การรักษาความสมบูรณ์และความพร้อมใช้

(2) การป้องกันบริการแอปพลิเคชันบนเครือข่ายสาธารณะ สารสนเทศของบริการแอปพลิเคชันต่าง ๆ ที่มีการส่งผ่านทางเครือข่ายสาธารณะต้องมีการป้องกันจากการฉ้อโกง การปฏิเสธ การเปิดเผยและการเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต

ข้อ 23 แนวปฏิบัติด้านความมั่นคงปลอดภัยในการพัฒนาระบบและกระบวนการสนับสนุนเป็นองค์ประกอบสำคัญในการออกแบบและพัฒนาระบบสารสนเทศ

(1) แนวปฏิบัติการพัฒนาระบบอย่างปลอดภัย ระบบสารสนเทศต้องได้รับการพัฒนาในสภาพแวดล้อมที่มีความมั่นคงปลอดภัยทั้งทางกายภาพ และทางตรรกะ เช่น สถานที่ที่ใช้ในการพัฒนาระบบต้องไม่สามารถเข้าถึงโดยผู้ไม่เกี่ยวข้องได้โดยง่าย เป็นต้น

(2) ขั้นตอนการปฏิบัติงานในการควบคุมการเปลี่ยนแปลง การเปลี่ยนแปลงระบบงานใดๆ จะต้องมีการควบคุมเพื่อไม่ให้มีผลกระทบต่อซอฟต์แวร์ประยุกต์(Application Software) ซอฟต์แวร์ระบบ(System Software) ระบบเครือข่าย (Network System) หรือการเปลี่ยนแปลงอื่น ๆ ที่เกิดจากการเปลี่ยนแปลงระบบงาน เช่น การพัฒนาระบบการทดสอบระบบ จะต้องอยู่ภายใต้การควบคุมที่เหมาะสมและเพียงพอ โดยวิธีการดังกล่าวจะช่วยให้ระบบสารสนเทศนั้น ๆ สามารถทำงานเข้ากันได้ทั้งด้านฮาร์ดแวร์และซอฟต์แวร์การเปลี่ยนแปลงแก้ไขควรมีคำขอการเปลี่ยนแปลงอย่างเป็นทางการซึ่งมีการอนุมัติในส่วนที่มีอำนาจอนุมัติการเปลี่ยนแปลงระบบงานนั้น ๆ

(3) การตรวจสอบระบบสารสนเทศทั้งหมดที่เกี่ยวข้อง การจ้างพัฒนาระบบต้องตรวจสอบระบบสารสนเทศที่เกี่ยวข้อง ภายหลังที่ได้ติดตั้งระบบใหม่เพื่อให้ทราบถึงผลกระทบจากการพัฒนาระบบและเป็นไปตามเงื่อนไขในการว่าจ้าง พร้อมทั้งมีการตรวจสอบจากหน่วยงานที่เกี่ยวข้องหลังจากการติดตั้งระบบใหม่หรือการปรับปรุง

ข้อ 24 แนวปฏิบัติด้านข้อมูลในการทดสอบระบบ (Test Data) เพื่อใช้ในการป้องกันข้อมูลที่ใช้ระหว่างการ ทดสอบระบบ หลักการป้องกันข้อมูลจริงที่ใช้ในการทดสอบระบบ (Protection of Test Data)ข้อมูลจริงที่จะนำใช้ทดสอบระบบต้องได้รับอนุญาตจากหน่วยงานที่รับผิดชอบในการรักษาข้อมูลนั้นๆก่อนเมื่อใช้งานเสร็จจะต้องลบข้อมูลจริงออกจากระบบทดสอบทันทีและบันทึกไว้เป็นหลักฐานว่าได้นำข้อมูลจริงไปใช้ทดสอบอะไรบ้าง รวมถึงวันเวลาและหน่วยงานที่ทดสอบแจ้งไปยังหน่วยงานที่รับผิดชอบในการรักษาข้อมูลนั้นอีกครั้ง

หมวด 6
แนวปฏิบัติของผู้จัดการ รองผู้จัดการ และเจ้าหน้าที่

ข้อ 25 ผู้จัดการ และรองผู้จัดการมีหน้าที่ควบคุมดูแลการใช้งานระบบเทคโนโลยีสารสนเทศให้เป็นไปตามวัตถุประสงค์

ข้อ 26 ผู้ดูแลระบบมีหน้าที่ดำเนินการให้ระบบเทคโนโลยีสารสนเทศของสหกรณ์ทำงานได้อย่างมีประสิทธิภาพ ทันสมัย และมั่นคงปลอดภัยตามนโยบายการรักษาความปลอดภัยของสหกรณ์ติดตั้งการรักษาความปลอดภัยของระบบบัญชีคอมพิวเตอร์และระบบเครือข่ายให้สามารถป้องกันบุคคลที่ไม่ได้รับอนุญาตเข้าสู่ ระบบได้ง่าย สอบทานสิทธิการใช้งานของเจ้าหน้าที่ให้สอดคล้องกับหน้าที่ความรับผิดชอบในแต่ละตำแหน่งเป็นประจำ ทุกปีจัดทำตารางแผนการสำรองข้อมูลและวิธีการกู้คืนข้อมูล และให้มีการสำรองข้อมูลและการทดสอบการกู้คืนข้อมูลให้เป็นไปตามแผนที่กำหนด จัดทำทะเบียนคุมข้อมูลชุดสำรองและควบคุมการนำข้อมูลชุดสำรองออกมาใช้งาน

ข้อ 27 ผู้ใช้งานมีหน้าที่รับผิดชอบในการบริหารจัดการข้อมูลที่เกี่ยวกับ การสร้าง เปลี่ยนแปลงข้อมูลโดยการกำหนดสิทธิ์การใช้งานจะต้องเป็นไปตามหน้าที่ความรับผิดชอบของผู้ใช้งาน ป้องกันดูแลรักษาข้อมูลชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) ทั้งนี้ต้องห้ามเผยแพร่ให้ผู้อื่นล่วงรู้รหัสผ่านของตนเองห้ามใช้ชื่อผู้ใช้งาน และรหัสผ่านของบุคคลอื่นมาใช้งานไม่ว่าจะได้รับอนุญาตจากผู้ใช้งานนั้นหรือไม่ก็ตามการใช้งานเครื่องคอมพิวเตอร์ต้องรับผิดชอบในฐานะเป็นผู้ถือครองเครื่องนั้น ๆ และต้องรับผิดชอบต่อความเสียหายที่ เกิดขึ้นอันเนื่องมาจากการใช้งานที่ผิดปกติเมื่อพบเหตุการณ์ผิดปกติที่เกี่ยวกับความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ให้รีบแจ้งให้ผู้จัดการ และผู้ดูแลระบบงานของสหกรณ์โดยทันที

หมวด 7
แนวปฏิบัติของคณะกรรมการ

ข้อ 28 สนับสนุนการดำเนินงานด้านเทคโนโลยีสารสนเทศให้มีประสิทธิภาพ

ข้อ 29 มอบหมายให้มีผู้รับผิดชอบในการติดตามการปฏิบัติตามนโยบาย และระเบียบปฏิบัติในการควบคุมภายใน และการรักษา ความปลอดภัยด้านเทคโนโลยีสารสนเทศของสหกรณ์

ข้อ 30 สื่อสารและสร้างความตระหนักกับบุคลากร ให้เข้าใจนโยบายและระเบียบปฏิบัติในการควบคุมภายใน และการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของสหกรณ์ส่งเสริมให้มีการฝึกอบรมหรือให้ความรู้เกี่ยวกับระบบงาน และการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศแก่คณะกรรมการดำเนินการ ผู้จัดการ และเจ้าหน้าที่สหกรณ์ เป็นประจำทุกปีรวมทั้งสนับสนุนให้เข้ารับการฝึกอบรม กับหน่วยงานและองค์กรต่าง ๆ ที่มีการจัดอบรมในเรื่องดังกล่าว

ข้อ 31 กำหนดให้ผู้ให้บริการโปรแกรมระบบสารสนเทศจัดทำคู่มือการใช้โปรแกรม และเอกสารด้านฐานข้อมูล ได้แก่ โครงสร้างข้อมูล (Data Structure) หรือพจนานุกรมข้อมูล (Data Dictionary) ให้กับสหกรณ์เพื่อ ประกอบการใช้งานโปรแกรม ระบบบัญชี

ข้อ 32 จัดให้มีการทบทวนแผนดำเนินการตาม ข้อ 14 และมีการซักซ้อมแผนฉุกเฉินเป็นประจำทุกปี

ประกาศ ณ วันที่ ๒๗ เดือน ตุลาคม พ.ศ. 2566

พลโท

(ภาณุภัสสร์ ลิมปะสุวัณณะ)

ประธานกรรมการ

สหกรณ์ออมทรัพย์กรมการทหารสื่อสาร จำกัด