ระเบียบ สหกรณ์ออมทรัพย์ค่ายสรรพสิทธิประสงค์ จำกัด
ว่าด้วย การรักษาความมั่นคงปลอดภัยสารสนเทศ
พ.ศ. 2567

อาศัยอำนาจตามความในข้อบังคับสหกรณ์ ข้อ 84 ข้อ 120 และมติที่ประชุมคณะกรรมการดำเนินการ ชุดที่ 38 ครั้งที่ 11/2567 เมื่อวันที่ 23 กันยายน 2567 พิจารณาแล้วเห็นว่า เพื่อให้การใช้เทคโนโลยีสารสนเทศของสหกรณ์มีความมั่นคงปลอดภัย และสามารถใช้งานได้อย่างมีประสิทธิภาพ จึงได้กำหนดระเบียบสหกรณ์ออมทรัพย์ค่ายสรรพสิทธิประสงค์ จำกัด ว่าด้วยการรักษาความมั่นคงปลอดภัยสารสนเทศ ดังต่อไปนี้

ข้อ 1 ระเบียบนี้เรียกว่า "ระเบียบ สหกรณ์สหกรณ์ออมทรัพย์ค่ายสรรพสิทธิประสงค์ จำกัด ว่าด้วย การรักษาความมั่นคงปลอดภัยสารสนเทศ พ.ศ. 2567"

ข้อ 2 ระเบียบนี้ให้ใช้บังคับตั้งแต่ถัดจากวันประกาศ เป็นต้นไป

ข้อ 3 ในระเบียบนี้

"สหกรณ์" หมายถึง สหกรณ์ออมทรัพย์ค่ายสรรพสิทธิประสงค์ จำกัด

"คณะกรรมการ" หมายถึง คณะกรรมการดำเนินการ สหกรณ์ออมทรัพย์ค่ายสรรพสิทธิประสงค์ จำกัด

"ประธานกรรมการ" หมายถึง ประธานคณะกรรมการดำเนินการ สหกรณ์ออมทรัพย์ค่ายสรรพสิทธิประสงค์ จำกัด

"ผู้จัดการ" หมายถึง ผู้จัดการ สหกรณ์ออมทรัพย์ค่ายสรรพสิทธิประสงค์ จำกัด

"ผู้ดูแลระบบ" หมายถึง เจ้าหน้าที่ สหกรณ์ออมทรัพย์ค่ายสรรพสิทธิประสงค์ จำกัด ที่ได้รับมอบหมายให้ดูแลระบบเทคโนโลยีสารสนเทศและการสื่อสารในภาพรวม

"ผู้ใช้งาน" หมายถึง ผู้ใช้ประโยชน์ด้านเทคโนโลยีสารสนเทศของสหกรณ์ ได้แก่ เจ้าหน้าที่ สมาชิก สมาชิกสมทบ รวมถึงบุคคลภายนอกที่ได้รับอนุญาตจากสหกรณ์

"เครื่องคอมพิวเตอร์" หมายถึง เครื่องคอมพิวเตอร์ทั้งหลาย เครื่องเซิร์ฟเวอร์ หรืออุปกรณ์อื่นใด ที่ทำหน้าที่ได้เสมือนเครื่องคอมพิวเตอร์ ทั้งที่ใช้งานอยู่ภายในสหกรณ์ หรือภายนอกแล้วเชื่อมต่อเข้ากับระบบเครือข่าย

"ระบบเครือข่าย" หมายถึง ระบบเครือข่ายคอมพิวเตอร์ที่สหกรณ์สร้างขึ้นทั้งแบบมีสาย และไร้สาย

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

"สารสนเทศ" หมายถึง ข้อมูลที่ผ่านการประมวลผลแล้วจัดระเบียบให้ข้อมูลซึ่งอยู่ในรูปของตัวเลขข้อความหรือกราฟิกให้อยู่ในลักษณะที่ผู้ให้สามารถเข้าใจได้ง่ายและสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจและอื่นๆ

"ความลับ" (Confidentiality)" หมายถึง การรับรองว่าจะมีการรักษาข้อมูลไว้เป็นความลับและจะมีเพียงผู้มีสิทธิเท่านั้นที่จะเข้าถึงข้อมูลเหล่านั้นได้

"ความถูกต้อง (Integrity)" หมายถึง การรับรองว่าข้อมูลจะต้องไม่ถูกกระทำการใดใดอันมีผลให้เกิดความเปลี่ยนแปลงหรือแก้ไขโดยผู้ไม่มีสิทธิ ไม่ว่าการกระทำนั้นจะมีสมาชิก หรือไม่ก็ตาม

"สภาพพร้อมใช้งาน (Availability)" หมายถึง การรับรองว่าข้อมูลหรือระบบเทคโนโลยีสารสนเทศทั้งหลายพร้อมที่จะให้บริการในเวลาที่ต้องใช้งาน

"ช่องโหว่" หมายถึง จุดอ่อนของระบบสารสนเทศที่ทำให้ผู้ไม่พงประสงค์เข้าโจมตีระบบทำให้ประสิทธิภาพของการทำงานที่ลดลง

"ภัยคุกคามทางไซเบอร์" หมายถึง การกระทำหรือการดำเนินการใดใด โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายทำให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ข้อมูลคอมพิวเตอร์หรือข้อมูลอื่นที่เกี่ยวข้อง

"ข้อมูลส่วนบุคคล" หมายถึง ข้อมูลเกี่ยวกับบุคคลที่สามารถระบุตัวบุคคลนั้นได้ทั้งทางตรงหรือทางอ้อม แต่จะไม่นับรวมข้อมูลของผู้ที่เสียชีวิตไปแล้ว

"การพิสูจน์ตัวตน (Authentication)" หมายถึง การทำให้มั่นใจว่าสิทธิการเข้าใช้งานระบบคอมพิวเตอร์และข้อมูลสารสนเทศต้องผ่านกระบวนการยืนยันตัวตนที่สมบูรณ์แล้วเท่านั้น

"ทดสอบการเจาะระบบ (Penetration Testing)" หมายถึง การประเมินความเสี่ยงด้วยการทดสอบเจาะระบบเพื่อค้นหาจุดอ่อนในการเข้าถึงระบบต่างๆ พร้อมแจ้งผลว่ามีความเสี่ยงจุดใด เพื่อเตรียมการป้องกันไว้ก่อน

หมวด 1
บททั่วไป

ข้อ 4 สหกรณ์ออมทรัพย์ค่ายสรรพสิทธิประสงค์ จำกัด ได้ประกาศใช้แผนการพัฒนาและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของ สหกรณ์ออมทรัพย์ค่ายสรรพสิทธิประสงค์ จำกัด ระยะ 3 ปี (พ.ศ. 2566-2568) เป็นกรอบกำหนดทิศทางการดำเนินงานด้านเทคโนโลยีสารสนเทศได้อย่างมีประสิทธิภาพ บริการสมาชิกได้อย่างรวดเร็ว ฉับไว โปร่งใสและพึงพอใจ อีกทั้งเพื่อให้เป็นไปตามความในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ 2550 และที่แก้ไขเพิ่มเติม พระราชบัญญัติรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ข้อ 5 ด้วยเหตุผลดังกล่าวข้อ 4 จึงกำหนดให้มีระเบียบว่าด้วยการรักษาความมั่นคงปลอดภัยสารสนเทศของสหกรณ์ออมทรัพย์ค่ายสรรพสิทธิประสงค์ จำกัด เพื่อเป็นกรอบในการปฏิบัติงานได้อย่างถูกต้องตามกฎหมายและมีประสิทธิภาพตามหลักมาตรฐานสากลด้านความมั่นคงปลอดภัยของสารสนเทศ (ISO/IEC 27001:2013) โดยให้ครอบคลุมด้านการรักษาความลับ(Confidentiality) ความถูกต้อง (Integrity) และสภาพพร้อมใช้งานของสารสนเทศ (Availability)

หมวด 2

ความมั่นคงปลอดภัยสำหรับบุคลากร

ข้อ 6 การจัดการบุคลากรก่อนจ้างงาน สหกรณ์ต้องทำการตรวจสอบคุณสมบัติของผู้สมัครงานทุกคนต้องไม่มีประวัติในการบุกรุก แก้ไข ทำลายหรือ โจรกรรม ข้อมูลในระบบเทคโนโลยีสารสนเทศของหน่วยงานใดมาก่อน

ข้อ 7 จัดให้มีการลงนามนสัญญาระหว่าง "เจ้าหน้าที่"และสหกรณ์ว่าจะไม่เปิดเผยความลับของหน่วยงาน (Non-Disclosure Agreement : NDA) โครงการลงนามนี้จะเป็นส่วนหนึ่งของการว่าจ้างเจ้าหน้าที่นั้นๆ ทั้งนี้ต้องมีผลผูกพันทั้งในขณะที่ทำงานและผูกพันต่อเนื่องเป็นเวลาไม่น้อยกว่า 1 ปี ภายหลังจากที่สิ้นสุดการว่าจ้างแล้ว

ข้อ 8 กำหนดและเงื่อนไขของการจ้างงานต้องกำหนดเงื่อนไขการจ้างงานที่รวมถึงหน้าที่ความรับผิดชอบทางด้านความมั่นคงปลอดภัยทางด้านสารสนเทศ

ข้อ 9 สหกรณ์ต้องกำหนดให้เจ้าหน้าที่ที่ว่าจ้างาปฏิบัติงานรับทราบและปฏิบัติตามนโยบาย กฎระเบียบ และขั้นตอนการทำงานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสาสรสนเทศของสหกรณ์ด้วย

ข้อ 10 เจ้าหน้าที่ต้องได้รับการอบรมเกี่ยวกับนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อสร้างความตระหนักและความเข้าใจในความมั่นคงปลอดภัยสารสนเทศภายใน 30 วัน นับจากเข้าทำงานสหกรณ์

ข้อ 11 มีกำหนดบทลงโทษทางวินัย สำหรับผู้ที่ฝ่าฝืน นโยบายกฎ และ/หรือ ระเบียบการปฏิบัติ แต่หากเป็นการละเมิดข้อกฎหมายบทลงโทษจะเป็นไปตามฐานความผิด ที่ได้กระทามที่ระบุในแต่ละข้อกฎหมายนั้นๆ

ข้อ 12 เมื่อมีการสิ้นสุดหรือเปลี่ยนหน้าที่ความรับผิดชอบของการจ้างงาน มีกำหนดและสื่อสารให้เจ้าหน้าที่ผู้ทำสัญญาได้ทราบ รวมทั้งมีการควบคุมให้ปฏิบัติตามข้อกำหนดในสัญญา

ข้อ 13 เจ้าหน้าที่ที่สิ้นสุดสภาพการว่าจ้างหรือเปลี่ยนหน้าที่ความรับผิดชอบ ให้ปฏิบัติตามคู่มือการปฏิบัติงานเรื่องการลงทะเบียนใช้งานระบบสารสนเทศเพื่อดำเนินการเพิกถอนสิทธิ์หรือเปลี่ยนแปลงสิทธิ์

หมวด 3

ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม

ข้อ 14 สหกรณ์ต้องจัดตั้งคอมพิวเตอร์ไว้ในที่เหมาะสมและห้ามผู้ไม่มีหน้าที่รับผิดชอบเข้ามาใช้เครื่องคอมพิวเตอร์โดยไม่ได้รับอนุญาต

ข้อ 15 จัดให้มีการติดตั้งอุปกรณ์ดับเพลิงไว้ในที่เหมาะสมและสะดวกต่อการใช้งาน และจัดทำแผนผังการขนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ รวมทั้งเอกสารที่เกี่ยวข้องเมื่อมีเหตุฉุกเฉินความปลอดภัยด้านเทคโนโลยีสารสนเทศของสหกรณ์

ข้อ 16 จัดให้มีระบบการควบคุมอุณหภูมิ ให้แก่อุปกรณ์เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ที่เกี่ยวข้องอย่างเพียงพอและเหมาะสมกับสาถนที่ รวมทั้งจัดตั้งเครื่องคอมพิวเตอร์ให้อยู่ในสถานที่ที่มีอากาศถ่ายเทได้สะดวกตลอดจนจัดให้ระบบสำรองไฟ เพื่อให้สามารถใช้งานได้อย่างต่อเนื่อง

ข้อ 17 จัดทำให้มีระบบรักษาความปลอดภัยทางกายภาพที่เพียงพอแก่การป้องกนมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าถึงอุปกรณ์คอมพิวเตอร์ที่สำคัญและจัดทำให้มีระบบป้องกันความเสียหายจากสภาพแวดล้อมหรือภัยพิบัติต่างๆ ให้แก่อุปกรณ์คอมพิวเตอร์ที่สำคัญ

ข้อ 18 ประเมินความเสี่ยงและกำหนดระดับความสำคัญของทรัพย์สินสารสนเทศให้สอดคล้องกับนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ พร้อมทั้งกำหนดพื้นที่การจัดวางทรัพย์สินสารสนเทศดังกล่าวที่มีความสำคัญให้เป็นพื้นที่หวงห้าม (Physical Security Perimeter)

ข้อ 19 กำหนดสิทธิ์การเข้าพื้นที่หวงห้ามให้เฉพาะบุคคลที่มีหน้าที่เกี่ยวข้องภายใต้หลักความจำเป็นในการรับรู้ข้อมูล (Need-to-know basis) รวมทั้งต้องจัดให้มีระบบการควบคุมการเข้า-ออกอย่างรัดกุมและทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

ข้อ 20 จัดให้มีการติดตั้งกล้องวงจรปิด ทั้งภายในห้องคอมพิวเตอร์และบริเวณภายนอกเพื่อติดตามสถานการณ์แบบ Real Time ซึ่งจะทำให้เกิดความรวดเร็วในการแก้ปัญหา พร้อมทั้งเป็นหลักฐานสำคัญสำหรับการก่ออาชญากรรมที่ไม่พึงประสงค์

ข้อ 21 เจ้าหน้าที่ควรตรวจสอบความมั่นคงปลอดภัยของพื้นที่ทำงานของตนเองเป็นประจำทุกวันหลังเลิกงาน เพื่อให้มั่นใจว่าตู้เอกสารลิ้นชัก และอุปกรณ์ต่างๆได้รับการปิดล็อคอย่างเหมาะสมและกุญแจถูกเก็บรักษาไว้อย่างปลอดภัย

หมวด 4
การบริหารจัดการทรัพย์สินสารสนเทศ

ข้อ 22 สหกรณ์ต้องจัดทำระเบียบเก็บสินทรัพย์ ซึ่งรวมถึงสินทรัพย์ข้อมูล เอกสาร ซอฟแวร์ เพื่อให้ได้รับการป้องกันและปกป้องอย่างเหมาะสม ตลอดจนประเมินความเสี่ยงอันอาจจะเกิดขึ้น

ข้อ 23 จัดให้มีการตรวจสอบบัญชีสินทรัพย์ทุกประเภทตามระยะเวลาที่กำหนดไว้ เช่น ปีละ 1 ครั้ง

ข้อ 24 ผู้ใช้งานต้องไม่เข้าไปในห้องคอมพิวเตอร์แม่ข่าย (Sever) ทางสหกรณ์เว้นแต่ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ 25 ผู้ใช้งานต้องไม่นำเครื่องมือหรืออุปกรณ์อื่นใดเชื่อมต่อเข้ากับเครื่องคอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์ของสหกรณ์เพื่อประโยชน์ส่วนตน

ข้อ 26 ผู้ใช้งานต้องไม่คัดลอกหรือทำสำเนาแฟ้มข้อมูลที่มีลิขสิทธิ์กำกับของการใช้งานก่อนได้รับอนุญาต

ข้อ 27 ห้ามมิให้ผู้ใช้งานกระทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำหรือทำลายข้อมูลระบบงานสหกรณ์และระบบเครือข่าย เว้นแต่ได้รับอนุญาตจากคณะกรรมการ

ข้อ 28 ห้ามติดตั้งอุปกรณ์หรือกระทำการใดเพื่อให้สามารถเข้าถึงข้อมูลด้านเทคโนโลยีสารสนเทศของสหกรณ์โดยไม่ได้อนุญาต

ข้อ 29 เครื่องคอมพิวเตอร์แม่ข่าย เครื่องคอมพิวเตอร์ลูกข่ายและเครื่องคอมพิวเตอร์ทั้งหมดของสหกรณ์ต้องได้รับการปกป้องด้วยรหัสผ่านของระบบปฏิบัติการทุกครั้งเมื่อต้องเข้าใช้

ข้อ 30 ห้ามเจ้าหน้าที่ทำการติดตั้งหรือเผยแพร่ซอฟแวร์ที่ละเมิดลิขสิทธิ์บนระบบคอมพิวเตอร์ของสหกรณ์

ข้อ 31 ซอฟต์แวร์ที่นำมาใช้ในการประมวลผลและจัดเก็บข้อมูลลับหรือข้อมูลสำคัญของสหกรณ์ต้องได้รับการตรวจสอบ ควบคุมและอนุมัติตามความเหมาะสม

ข้อ 32 ห้ามผู้ใช้งานคลิ๊กหน้าอ่านโฆษณาแบบป๊อปอัพหรือเข้าสู่เว็ปไซต์ใดๆ ที่โฆษณาโดยสแปม เนื่องจากเว็ปไซต์เหล่านี้อาจมีโปรแกรมมุ่งร้ายแฝงอยู่

ข้อ 33 E-mail Account ต้องได้รับการปกป้องด้วยรหัสผ่านเพื่อป้องกันการถูกล่วงละเมิดและการนำอีเมล์ไปใช้ในทางที่ผิด

ข้อ 34 ซอฟแวร์สำหรับใช้งานอีเมล์ต้องได้รับการตั้งค่าให้อีเมล์ออกทุกฉบับมีลายเซ็นของผู้สั่งเสมอ

ข้อ 35 ผู้ใช้งานต้องไม่ยินยอมให้บุคคลอื่นทำการส่งอีเมล์โดยใช้ E-mail Account ของตนเองโดยเด็ดขาดไม่ว่าบุคคลนั้นจะสำคัญแค่ไหน

ข้อ 36 สารสนเทศต้องมีการจัดชั้นความลับโดยพิจารณาจากความต้องการด้านกฎหมาย คุณค่า ระดับความสำคัญ และระดับความอ่อนไหวหากถูกเปิดเผยหรือเปลี่ยนแปลงโดยไม่ได้รับอนุญาต

ข้อ 37 จัดทำระเบียบวิธีปฏิบัติงานสำหรับการทำลายสื่อที่ใช้ในการบันทึกข้อมูลอย่างเป็นลายลักษณ์อักษร

ข้อ 38 ควรทำลายสื่อที่ใช้ในการบันทึกข้อมูล เอกสารและอุปกรณ์สำนักงานภายใต้สิ่งแวดล้อมที่ได้มีการควบคุม

หมวด 5

การควบคุมการเข้าถึง

ข้อ 39 สหกรณ์ควรกำหนดให้มีการควบคุมการใช้งานข้อมูลและระบบสรสนเทศ เพื่อควบคุมการเข้าถึงให้เข้าได้เฉพาะผู้ใช้ที่ได้รับอนุญาตเท่านั้น

ข้อ 40 กำหนดสิทธิการเข้าถึงข้อมูลและระบบสารสนเทศให้เหมาะสมกับการเข้าใช้งานและหน้าที่ความรับผิดชอบของผู้ใช้งาน

ข้อ 41 ผู้ดูแลระบบเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิเข้าถึงข้อมูลและระบบสารสนเทศ

ข้อ 42 ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้มีรหัสใช้งาน (User Account) และมีกำหนดรหัสผ่าน (User ID) ในการเข้าใช้ระบบงานโดยกำหนด รวมถึงการยกเลิกรหัสผู้ใช้ของเจ้าหน้าที่ที่ลาออกและกำหนดรหัสผู้ใช้ให้แก่เจ้าหน้าที่ที่เข้ามาปฏิบัติงานใหม่

ข้อ 43 ผู้ดูแลระบบต้องกำกับดูแลให้ผู้ใช้งานต้องมีการเปลี่ยนรหัสผ่านทุกๆ 6 เดือน เป็นอย่างน้อย

ข้อ 44 ผู้ใช้งานต้องเก็บรหัสผ่านเป็นความลับ มิให้ผู้ใดล่วงรู้ หากพิสูจน์ได้ว่าเกิดความเสียหายจากระบบและข้อมูลจากรหัสนั้น ผู้ใช้งานนั้นต้องเป็นผู้รับผิดชอบในความเสียหายที่เกิดขึ้น

ข้อ 45 เมื่อผู้ใช้งานพบเหตุการณ์ผิดปกติที่เกี่ยวกับความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ให้รีบแจ้งผู้ดูแลระบบหรือผู้บังคับบัญชาตามลำดับชั้นทราบโดยทันที

ข้อ 46 การพัฒนาการเปลี่ยนแปลงแก้ไขโปรแกรมประมวลผลต้องมีหนังสือแสดงความต้องการเปลี่ยนแปลงระบบและได้รับอนุมัติจากผู้ดูแลระบบก่อน

ข้อ 47 ต้องจัดให้มีขั้นตอนการบริหารการจัดการเรื่อง การกำหนดรหัสผ่าน (User Password Management) อย่างเหมาะสม

ข้อ 48 จัดให้มีการลงทะเบียนบัญชีผู้ใช้ระบบงานสารสนเทศและยกเลิกบัญชีผู้ใช้งานอย่างเป็นทางการ เพื่อควบคุมการให้สิทธิและการยกเลิกสิทธิในการเข้าถึง

ข้อ 49 จัดให้มีการติดตาม ทบทวนระดับสิทธิการเข้าถึงอย่างสม่ำเสมอ และยกเลิกสิทธิการเข้าถึงโดยทันที เมื่อบุคคลที่ได้รับสิทธิลาออกหรือเปลี่ยนแปลงหน้าที่การปฏิบัติงาน

ข้อ 50 จัดให้มีระบบการริหารการจัดการสถานที่มีความมั่นคงปลอดภัยโดยขั้นต่ำต้องมีกระบวนการดังนี้

(1) กำหนดให้มีผู้ใช้งานแต่ละรายต้องรับผิดชอบบัญชีผู้ใช้งานและรหัสผ่านของตนเอง
(2) ให้ผู้ใช้งานสามารถตั้งค่าหรือเปลี่ยนแปลงรหัสผ่านได้ด้วยตนเอง และระบบต้องมีขั้นตอนให้ยืนยันความถูกต้อง
(3) บังคับให้ผู้ใช้งานเปลี่ยนแปลงรหัสผ่านทันทีที่ได้รับรหัสผ่านครั้งแรกและควรเปลี่ยนรหัสผ่านอย่างน้อยทุก 6 เดือน
(4) ในการเปลี่ยนแปลงรหัสผ่านแต่ละครั้งไม่ควรกำหนดรหัสผ่านใหม่ซ้ำกันกับรหัสผ่านที่ใช้ในครั้งล่าสุด
(5) ควรกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิด ซึ่งในทางปฏิบัติโดยทั่วไปไม่ควรเกิน 10 ครั้ง
(6) ควรมีวิธีใช้การจัดส่งรหัสผ่านให้แก่ผู้ที่ใช้งานอย่างรัดกุมและปลอดภัย เช่น การใส่ซองปิดผนึก เป็นต้น

หมวด 6
การพิสูจน์ตัวตน

ข้อ 51 ผู้ใช้งานแต่ละคนต้องมีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนเองและมีหน้าที่ป้องกัน ดูแลรักษาข้อมูลชื่อผู้ใช้งาน และรหัสผ่านของตนเอง ทั้งนี้ห้ามมิให้ใช้ร่วมกับผู้อื่นรวมทั้งห้ามเผยแพร่ แจกจ่าย หรือ กระทำการใดๆ อันทำให้ผู้อื่นร่วงรู้รหัสผ่านของตนเอง

ข้อ 52 ผู้ใช้งานต้องรับผิดชอบต่อการกระทำใดๆ ที่เกิดจากผู้ใช้งาน (Username) ไม่ว่าการกระทำนั้นเกิดจากผู้ใช้งานหรือไม่ก็ตาม

ข้อ 53 ผู้ใช้งานต้องตั้งรหัสผ่านให้เกิดความปลอดภัย โดยรหัสผ่านต้องประกอบด้วยตัวเลขและหรือตัวอักษรรวมกันไม่น้อยกว่า 8 ตัว

ข้อ 54 การใช้งานระบบสหกรณ์ ผู้ใช้งานซึ่งเป็นเจ้าหน้าที่ต้องเปลี่ยนรหัสผ่านทุกๆ 120 วัน หรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน

ข้อ 55 ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งในการใช้งานอินเตอร์เน็ต การเข้าถึงระบบผู้ปฏิบัติการและการใช้งานระบบคอมพิวเตอร์

หมวด 7
ความมั่นคงปลอดภัยของเครือข่าย

ข้อ 56 ผู้ดูแลระบบของสหกรณ์ ต้องควบคุมและกำหนดหลักเกณฑ์ผู้มีสิทธิการเข้าใช้งานระบบเครือข่ายของสหกรณ์ให้มีความปลอดภัยและประสิทธิภาพสูงสุด

ข้อ 57 ห้ามมิให้นำเครื่องคอมพิวเตอร์ที่ใช้งานระบบงานสหกรณ์เชื่อมต่อกับเครือข่ายภายนอก (Internet) ก่อนได้รับอนุญาต

ข้อ 58 การนำอุปกรณ์จัดเก็บข้อมูลเชื่อมต่อกับเครื่องคอมพิวเตอร์ต้องได้รับการตรวจสอบและอนุญาตจากผู้ดูแลระบบ

ข้อ 59 ผู้ดูแลระบบควรติดตั้งไฟล์วอล (Firewall) ระหว่างระบบเครือข่ายไร้สายกับระบบเครือข่ายภายในสหกรณ์เพื่อป้องกันการโจมตีการรักษาความปลอดภัยเครือข่ายหรือการโจมตีของแฮกเกอร์

ข้อ 60 กำหนดการป้องกันภัยคุกคามต่างๆทางเครือข่ายและกำหนดสิทธิผู้ใช้งานผ่านเครือข่าย โดยอนุญาตเฉพาะผู้ที่มีสิทธิเท่านั้น

ข้อ 61 กำหนดให้บัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนเอง สำหรับการใช้งานระบบเครือข่ายภายนอก (Internet)

ข้อ 62 ผู้ดูแลระบบ ต้องมีการบันทึกและจัดเก็บหลักฐาน (logs) เพื่อติดตามตรวจสอบ การทำงานที่เกี่ยวข้องหรืออาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบเครือข่ายคอมพิวเตอร์

ข้อ 63 ควรระมัดระวังการดาวน์โหลด (Download) ไฟล์ข้อมูลหรือโปรแกรมต่างๆจากระบบเครือข่ายภายนอก (Internet) เพราะอาจเป็นการละเมิดทรัพย์สินทางปัญญา หรืออาจทำให้มีไวรัสคอมพิวเตอร์ บุกรุกข้อมูลระบบคอมพิวเตอร์และระบบสารสนเทศ

ข้อ 64 การใช้งานจดหมายอเล็กทรอนิกส์ (E-mail) ต้องตรวจสอบชื่อผู้ส่งจดหมายอิเล็กทรอนิกส์ (Sender) ก่อนเปิดจดหมาย เพื่อป้องกันการเปิดไฟล์อันตรายที่อาจมีไวรัสคอมพิวเตอร์

ข้อ 65 การใช้งานเครือข่ายไร้สาย (WiFi) ผู้ใช้งาน (User) ต้องใช้บัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพราะเข้าใช้งานเครือข่ายไร้สาย (WiFi)

ข้อ 66 การใช้งานต้องปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติมโดยเคร่งครัด

หมวด 8
ความมั่นคงปลอดภัยสำหรับการดำเนินงาน

ข้อ 68 สหกรณ์ควรจัดทำคู่มือหรือขั้นตอนการปฏิบัติงานสารสนเทศเพื่อให้การปฏิบัติงานกับอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและมีความมั่นคงปลอดภัย

ข้อ 69 มาตรการป้องกันโปรแกรมไม่ประสงค์ดีให้กับเครื่องคอมพิวเตอร์ลูกขายและเครื่องคอมพิวเตอร์แบบพกพาต้องได้รับการติดตั้งโปรแกรมป้องกันไวรัสและปฏิบัติตามเอกสารวิธีปฏิบัติงานเรื่องการจัดการควบคุมซอฟต์แวร์ไม่ประสงค์ดี

ข้อ 70 การสำรองข้อมูลเพื่อใช้ในการกู้ระบบในกรณีที่เกิดเหตุต่างๆเช่นภัยธรรมชาติ ระบบเสียหาย ฯลฯ ต้องกำหนด ความถี่ในการสำรองข้อมูลขึ้นอยู่กับความสำคัญของระบบข้อมูลและการยอมรับความเสี่ยงกำหนดโดยเจ้าของข้อมูลหรือระบบโดยปฏิบัติตามเอกสารวิธีปฏิบัติงานเรื่องการจัดการสำรองข้อมูลสารสนเทศน์

ข้อ 71 จัดให้มีการทดสอบข้อมูลสำรองและกระบวนการกู้คืนข้อมูลอย่างน้อยปีละ 1 ครั้งเพื่อให้มั่นใจได้ว่าข้อมูลรวมทั้งโปรแกรมระบบต่างๆ ที่ได้สำรองไว้มีความถูกต้องครบถ้วนและสามารถใช้งานได้ภายในระยะเวลาที่กำหนด

ข้อ 72 การบันทึกข้อมูลล็อกและการเฝ้าระวัง(Logging and Monitoring)เพื่อให้มีการเก็บหลักฐานหรือบันทึกเหตุการณ์ใช้เป็นหลักฐานยืนยันต้องกำหนดให้การบันทึกกิจกรรมการใช้งานของผู้ใช้ปฏิเสธการให้บริการของระบบและเหตุการณ์ต่างๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยอย่างสม่ำเสมอตามระยะเวลาที่กำหนดไว้

ข้อ 73 การป้องกันข้อมูลล็อกต้องกำหนดให้มีการป้องกันข้อมูลบันทึกกิจกรรมหรือเหตุการณ์ต่างๆที่เกี่ยวข้องกับการใช้งานสาระสนเทศน์เพื่อป้องกันการเปลี่ยนแปลงหรือการแก้ไขโดยไม่ได้รับอนุญาต

ข้อ 74 การตั้งเวลาให้ถูกต้อง (Lock Synchronization) ผู้ใช้งานต้องตั้งเวลาของเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ในสหกรณ์ให้ตรงกันโดยอ้างอิงจากแหล่งเวลาที่ถูกระบุตามระบบตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์เพื่อช่วยในการตรวจสอบช่วงเวลาหากเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ถูกบุกรุก

หมวด 9
การรักษาความมั่นคงปลอดภัยไซเบอร์

ข้อ 75 การรักษาความมั่นคงปลอดภัยไซเบอร์ของสหกรณ์ออมทรัพย์ค่ายสรรพสิทธิประสงค์จำกัดมีวัตถุประสงค์เพื่อดำเนินการผ่านมาตรการแก้ไขปัญหาโดยใช้บุคลากรกระบวนการและเทคโนโลยีที่กำหนดขึ้นเพื่อป้องกันรับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์อันกระทบต่อการปฏิบัติงานของสหกรณ์โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์ เพื่อมุ่งหมายให้เกิดการประทุษร้ายและความเสียหายต่อระบบคอมพิวเตอร์ข้อมูลคอมพิวเตอร์และข้อมูลอื่นๆที่เกี่ยวข้อง

ข้อ 76 จัดให้มีคณะกรรมการติดตามและแก้ไขปัญหาภัยคุกคามจากไซเบอร์หรือเรียกว่า "ทีมไซเบอร์" ของสหกรณ์ออมทรัพย์ค่ายสรรพสิทธิประสงค์จำกัดเพื่อดำเนินการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

ข้อ 77 ให้คณะกรรมการตามข้อ 76 จัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อันเป็นข้อกำหนดขั้นต่ำในการดำเนินการด้านรักษาความปลอดภัยไซเบอร์รวมทั้งกำหนดมาตรการให้การประเมินความเสี่ยงการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์เพื่อให้การรักษาความมั่นคงปลอดภัยทางไซเบอร์ปฏิบัติได้อย่างรวดเร็วมีประสิทธิภาพและเป็นไปในทิศทางเดียวกัน

ข้อ 78 กรอบการทำงานด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber security Framework) เป็นแนวทางปฏิบัติที่สหกรณ์ออมทรัพย์ค่ายสรรพสิทธิประสงค์จำกัดนำมาใช้บริการการจัดการความเสี่ยงเพื่อยกระดับความมั่นคงปลอดภัยสามารถวางแผนป้องกันตรวจจับและตอบสนองต่อภัยคุกคามไซเบอร์ได้อย่างรวดเร็วและเป็นระบบซึ่งมีห้าขั้นตอนดังนี้

ขั้นที่ 1 : การระบุความเสี่ยงที่อาจเกิดขึ้นแก่คอมพิวเตอร์ข้อมูลคอมพิวเตอร์ระบบคอมพิวเตอร์และข้อมูลที่เกี่ยวข้องระบบคอมพิวเตอร์ (identify)

(1) จัดทำทะเบียนทรัพย์สินและมีการตรวจสอบทะเบียนอย่างน้อยปีละ1 ครั้ง

(2) จัดการประเมินความเสี่ยงและกำหนดกลยุทธ์การจัดการความเสี่ยง

(3) มีการ ประเมินช่องโหว่ (Vulnerability assessment) ของบริการที่สำคัญเพื่อระบุจุดอ่อนตัวความมั่นคงปลอดภัย

(4) ดำเนินการทดสอบเจาะระบบ (Penetration testing) สำหรับการบริการที่สำคัญโดยเฉพาะอย่างยิ่งระบบสาระสนเทศน์ที่เชื่อมต่อกับอินเตอร์เน็ตโดยตรงเพื่อให้สอดคล้องกับระบบเพราะของความเสี่ยงอย่างน้อยควรทดสอบเจาะระบบปีละ 1 ครั้ง

(5) เคร่งครัดในเรื่องการจัดการผู้ให้บริการภายนอก(Third party management) โดยแจ้งผู้ให้บริการภายนอกได้รับทราบถึงความรับผิดชอบและภาระรับผิดชอบต่อการดูแลรักษาความมั่นคงปลอดภัยไซเบอร์ของโครงสร้างพื้นฐานสำคัญของสาระสนเทศน์

ขั้นที่ 2 : มาตรการป้องกันความเสี่ยงที่อาจเกิดขึ้น (Protect)

(1) การควบคุมการเข้าถึง access control บริการที่สำคัญระบบสาระสนเทศน์ผู้ใช้งานและข้อมูลความข้อมูลตามระดับชั้นความลับ

(2) การทำให้ระบบมีความแข็งแกร่ง (System hardening) โครงการสร้างมาตรฐานการกำหนดถ้าขั้นต่ำด้านความมั่นคงปลอดภัย

(3) ตรวจสอบให้แน่ใจว่าการเชื่อมต่อระยะไกล remote connection ทั้งหมดมายังบริการที่สำคัญได้จัดให้มีมาตรการรักษาความปลอดภัยไซเบอร์ที่มีประสิทธิภาพเพื่อป้องกันและตรวจจับการเข้าถึงโดยไม่ได้รับอนุญาต

(4) สร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ cyber security, awareness ให้กับกรรมการฝ่ายจัดการและสมาชิกสหกรณ์ได้ทราบอย่างน้อยปีละหนึ่งครั้ง

ขั้นที่ 3 : มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามไซเบอร์ (Detect)

(1) มีการตรวจสอบและเฝ้าระวังภัยพุกคามทางไซเบอร์โดยมีการทบทวนกลไกและกระบวนการอย่างน้อยปีละ1 ครั้ง

ขั้นที่ 4 : มาตรการเผชิญเหตุเมื่อมีการตรวจสอบพบภัยคุกคามไซเบอร์ (Respond)

(1) จัดทำแผนการสร้างรับมือภัยคุกคามไซเบอร์ เพื่อกำหนดวิธีการตรวจสอบควบคุมป้องกันแก้ไขปัญหาและลดความเสี่ยงที่เกิดขึ้นจากภัยคุกคามไซเบอร์

(2) เตรียมแผนการสื่อสารในภาวะวิกฤตเพื่อสร้างความเข้าใจกับทุกฝ่ายที่เกี่ยวข้องในสถานการณ์ของสหกรณ์ได้อย่างรวดเร็วทันต่อเหตุการณ์ได้อย่างเป็นเอกภาพ

(3) ทำการฝึกซ้อมและการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละหนึ่งครั้ง

ขั้นที่ 5 : มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)

(1) การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์โดยจัดทำแผนตามต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) เพื่อให้แน่ใจว่าบริการที่สำคัญของสหกรณ์สามารถให้บริการที่จำเป็นต่อไปได้

ข้อ 79 ในการรับมือและบรรเทาความเสียหายจากภัยคุกคามทางไซเบอร์ในระดับร้ายแรงให้ผู้เกี่ยวที่เกี่ยวข้องดำเนินการดังนี้

(1) เฝ้าระวังคอมพิวเตอร์หรือระบบคอมพิวเตอร์ในช่วงระยะเวลาใดเวลาหนึ่ง

(2) ตรวจสอบคอมพิวเตอร์หรือระบบคอมพิวเตอร์เพื่อหาข้อบกพร่องที่กระทบต่อการรักษาความมั่นคงปลอดภัยไซเบอร์วิเคราะห์สถานการณ์และประเมินผลกระทบจากภัยคุกคามไซเบอร์

(3) ดำเนินมาตรการแก้ไขภัยคุกคามทางไซเบอร์เพื่อจัดการข้อบกพร่องหรือจำกัดชุดคำสั่งที่ไม่พึงประสงค์หรือระงับบรรเทาภัยคุกคามทางไซเบอร์ที่ดำเนินการอยู่

(4) รักษาสถานะของข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ด้วยวิธีการใดใดเพื่อดำเนินการทางนิติวิทยาศาตทางคอมพิวเตอร์

(5) เข้าถึงข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ที่เกี่ยวข้องเฉพาะเท่าที่จำเป็นเพื่อป้องกันภัยคุกคามไซเบอร์ไซเบอร์

ข้อ 80 เมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยยะสำคัญต่อระบบของหน่วยงานโดยโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศเท่านั้นรายงานต่อสำนักงานและหน่วยงานควบคุมเพื่อกำกับดูแล

ข้อ 81 ให้ปฏิบัติตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์พ.ศ. 2562 โดยประสานรายละเอียดการปฏิบัติกับสำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

หมวด 10

การคุ้มครองข้อมูลส่วนบุคคล

ข้อ 82 สหกรณ์จัดให้มีนโยบายการคุ้มครองข้อมูลส่วนบุคคลและแจ้งให้ผู้มีส่วนเกี่ยวข้องได้ทราบทั่วกัน

ข้อ 83 จัดให้มีระบบการจัดเก็บการใช้การเปิดเผยข้อมูลส่วนบุคคลให้มั่นคงและปลอดภัย

เข้า 84 จัดให้มีผู้ควบคุมข้อมูลผู้ประมวลผลข้อมูลและเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลเพื่อให้มั่นใจว่าข้อมูลส่วนบุคคลมีการใช้ตรงตามวัตถุประสงค์

ข้อ 85 การส่งข้อมูลส่วนบุคคลไปหน่วยงานภายนอกต้องมีข้อตกลงกับหน่วยงานภายนอกให้ทำการคุ้มครองที่มั่นคงปลอดภัยหรือทำตามกฎหมายกำหนดอย่างเคร่งครัด

ข้อ 86 ข้อมูลส่วนบุคคลสหกรณ์จะรักษาเสมือนหนึ่งเป็นทรัพย์สินสหกรณ์เองห้ามมิให้ผู้ใดละเมิดเปิดเผยเข้าถึงนำไปหาประโยชน์ส่วนตัวหรือทำลายข้อมูลนี้โดยไม่ได้รับอนุมัติจากผู้ควบคุมข้อมูลผู้ฝ่าฝืนจะถูกลงโทษและชดใช้ความเสียหาย

ข้อ 87 จัดให้มีวิธีการเก็บและสถานที่เก็บข้อมูลทั้งในรูปแบบสื่ออิเล็กทรอนิกส์และเป็นเอกสาร

ข้อ 88 จัดให้มีกำหนดพาสเวิร์ดหรือผู้รับผิดชอบการเก็บการใช้การเปิดเผยที่ชัดเจนเฉพาะคนเพื่อป้องกัน ไม่ให้มีการละเมิดเข้าถึงข้อมูลที่ไม่เกี่ยวข้อง

ข้อ 89 การเปลี่ยนแปลงข้อมูลส่วนบุคคลที่สหกรณ์คุ้มครองไว้ต้องจัดให้มีผู้มีอำนาจทำการทบทวนอนุมัติก่อนการเปลี่ยนแปลงเพื่อให้มั่นใจว่าข้อมูลที่คุ้มครองไว้นั้นได้รับการจัดเก็บใช้งานอย่างมั่นคงและปลอดภัย

ข้อ 90 จัดให้มีการตรวจสอบเป็นระยะและให้มีการทบทวนทั้งระบบอย่างน้อยปีละหนึ่งครั้งเพื่อให้มั่นใจว่าข้อมูลส่วนบุคคลที่เก็บใช้งานได้รับการคุ้มครองตามนโยบายและกฎหมายที่เกี่ยวข้องสถานที่เกมให้เป็นไปตามสหกรณ์กำหนด

ข้อ 91 ข้อมูลที่ใช้ในการทำงานจะเก็บไว้ตลอดเวลาและหลังจากพ้นสภาพไปแล้วไม่น้อยกว่า 10 ปี โดยเก็บไว้ในสื่ออิเล็กทรอนิกส์หรือเป็นเอกสารที่ปลอดภัย

ข้อ 92 ข้อมูลที่ไม่ได้ใช้งานจะเก็บไว้ไม่เกินสามเดือนจะทำลายโดยการย่อยหรือทำลายไม่ให้มีการนำกลับมาใช้ใหม่หรือป้องกันการนำกลับมาใช้ผิด

ข้อ 93 ข้อมูลใดที่เก็บไว้ในสื่ออิเล็กทรอนิกส์หรือซอฟต์แวร์ที่สามารถตรวจสอบได้ถูกต้องตามจริงแล้ว สหกรณ์อาจทำลายข้อมูลที่เป็นกระดาษได้ เพื่อไม่ให้เป็นภาระในการจัดเก็บ

ข้อ 94 สหกรณ์ให้ความเคารพสิทธิ์เสรีภาพของเจ้าของข้อมูลและจัดให้เจ้าของข้อมูลมีสิทธิ์ดังต่อไปนี้

(1) ขอตรวจสอบวิธีการเก็บการใช้และการเปิดเผยข้อมูล

(2) ขอคัดค้านขอระงับการใช้ได้

(3) ขอถอนความยินยอมได้

(4) ขอให้ลบออกจากการเก็บการใช้การเปิดเผยได้

(5) ขอให้เปลี่ยนแปลงแก้ไขให้ถูกต้องได้

ข้อ 95 เจ้าของข้อมูลหากมีการเปลี่ยนแปลงข้อมูลส่วนบุคคลให้แจ้งผู้เกี่ยวข้องทราบทันทีหรือภายในไม่เกินเจ็ดวัน

ข้อ 96 เจ้าของข้อมูลหากพบเหตุผิดปกติหรือเหตุการณ์ละเมิดข้อมูลส่วนบุคคลอันอาจทำให้เกิดความเสียหายให้แจ้งจากกรทราบทันทีเพื่อระงับได้ทันเหตุการณ์

ข้อ 97 หากมีการนำข้อมูลส่วนบุคคลที่สหกรณ์คุ้มครองไว้ไปเปิดเผยหาประโยชน์ นอกจากวัตถุประสงค์ที่เจ้าของข้อมูลยินยอมทำให้เจ้าของข้อมูลเสียหายและทำผิดตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลพ.ศ. 2562 อาจจะถูกลงโทษขั้นสูงสุดหรือดำเนินคดีตามกฎหมายกำหนดไว้สูงสุด

ประกาศ ณ วันที่ ๒๐ ตุลาคม พ.ศ.2567

พลตรี

(อัครพนธ์ มูลประดับ)

ประธานกรรมการ

สหกรณ์ออมทรัพย์ค่ายสรรพสิทธิประสงค์ จำกัด