

นโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ (Information Security Policy)

การรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ เป็นการจัดทำขึ้นเพื่อกำหนดแนวทางไว้เป็นกรอบและเป็นแผนที่นำทางในระดับกลยุทธ์ เพื่อยกระดับมาตรฐานการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของสหกรณ์ ให้อยู่ระดับมาตรฐานสากล โดยอ้างอิงจากกรอบมาตรฐานสากล ISO/IEC 27001 อีกทั้งต้องการลดผลกระทบจากเหตุ ตลอดจนการกู้คืนระบบอย่างรวดเร็วหลังจากการโจมตีสิ้นสุดลงแล้ว เป็นแนวทางปฏิบัติของผู้ใช้งานด้านเทคโนโลยีสารสนเทศของสหกรณ์

นโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของสหกรณ์ ประกอบด้วย 8 หมวด โดยมีรายละเอียดดังต่อไปนี้

หมวด 1 ว่าด้วยการพิสูจน์ตัวตน

(Accountability, Identification and Authentication)

ข้อ 1 ผู้ใช้งานมีหน้าที่ในการป้องกัน ดูแลรักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งาน (Username) ของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่ แจกจ่าย ทำให้ผู้อื่นล่วงรู้รหัสผ่าน (Password)

ข้อ 2 ผู้ใช้งานต้องรับผิดชอบต่อการกระทำใดๆ ที่เกิดจากบัญชีชื่อผู้ใช้งาน (Username) ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม

ข้อ 3 ผู้ใช้งานต้องตั้งรหัสผ่านให้เกิดความปลอดภัย โดยรหัสผ่านประกอบด้วยตัวอักษรไม่น้อยกว่า 8 ตัวอักษร ซึ่งต้องประกอบด้วยตัวเลข (Numerical character) ตัวอักษร (Alphabet) และตัวอักษรพิเศษ (Special character)

ข้อ 4 ผู้ใช้งานต้องไม่ใช้งานรหัสผ่านซึ่งเคยใช้มาแล้ว อย่างน้อย 5 รหัสผ่าน

ข้อ 5 ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) ทุก ๆ 6 เดือนหรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน

ข้อ 6 ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้ทรัพยากรหรือด้านเทคโนโลยีสารสนเทศของสหกรณ์ และหากการพิสูจน์ตัวตนนั้นมีปัญหา ไม่ว่าจะเกิดจากรหัสผ่าน การโดนล๊อคกั๊ต หรือเกิดจากความผิดพลาดใด ๆ ก็ดี ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันที โดย

(1) คอมพิวเตอร์โน้ตบุ๊ก (Notebook) ต้องทำการพิสูจน์ตัวตนในระดับไบออส (BIOS) ก่อนการใช้งาน

(2) คอมพิวเตอร์ทุกประเภท ก่อนการเข้าถึงระบบปฏิบัติการต้องทำการพิสูจน์ตัวตนทุกครั้ง

(3) การใช้งานระบบคอมพิวเตอร์อื่นในเครือข่ายจะต้องทำการพิสูจน์ตัวตนทุกครั้ง

(4) การใช้งานอินเทอร์เน็ต (Internet) ต้องทำการพิสูจน์ตัวตนและต้องมีการบันทึกข้อมูล ซึ่งสามารถบอกตัวตนบุคคลผู้ใช้งานได้

(5) เมื่อผู้ใช้งานไม่อยู่ที่เครื่องคอมพิวเตอร์ เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการล็อกหน้าจอทุกครั้ง และต้องทำการพิสูจน์ตัวตนก่อนการใช้งานทุกครั้ง

(6) เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการตั้งเวลาพักหน้าจอ (screen saver) โดยตั้งเวลาอย่างน้อย 5 นาที

หมวด 2 ว่าด้วยการบริหารจัดการทรัพย์สิน (Assets Management)

ข้อ 7 ผู้ใช้งานต้องไม่นำเครื่องมือ หรืออุปกรณ์อื่นใด เชื่อมเข้าเครือข่ายเพื่อการประกอบธุรกิจส่วนบุคคล

ข้อ 8 ผู้ใช้งานต้องไม่ใช้ หรือลบเพิ่มข้อมูลของผู้อื่น ไม่ว่ากรณีใด ๆ

ข้อ 9 ผู้ใช้งานต้องไม่คัดลอกหรือทำสำเนาเพิ่มข้อมูลที่มีลิขสิทธิ์กำกับการใช้งาน ก่อนได้รับอนุญาต

ข้อ 10 ผู้ใช้งานมีหน้าที่ต้องรับผิดชอบต่อทรัพย์สินที่สหกรณ์มอบไว้ให้ใช้งานเสมือนหนึ่งเป็นทรัพย์สินของผู้ใช้งานเอง โดยบรรดารายการทรัพย์สิน (Asset lists) ที่ผู้ใช้งานต้องรับผิดชอบจะอยู่แนบท้ายเอกสารข้อบังคับนี้การรับหรือคืนทรัพย์สินจะถูกบันทึกและตรวจสอบทุกครั้งโดยเจ้าหน้าที่ที่สหกรณ์มอบหมาย

ข้อ 11 กรณีทำงานนอกสถานที่ผู้ใช้งานต้องดูแลและรับผิดชอบทรัพย์สินของสหกรณ์ที่ได้รับมอบหมาย

ข้อ 12 ผู้ใช้งานมีหน้าที่ต้องชดเชยค่าเสียหายไม่ว่าทรัพย์สินนั้นจะชำรุด หรือสูญหายตามมูลค่าทรัพย์สิน หากความเสียหายนั้นเกิดจากความประมาทของผู้ใช้งาน

ข้อ 13 ผู้ใช้งานต้องไม่ให้ผู้อื่นยืม คอมพิวเตอร์ หรือโน้ตบุ๊ก ไม่ว่าในกรณีใด ๆ เว้นแต่การยืมนั้นได้รับ การอนุมัติเป็นลายลักษณ์อักษรจากผู้ดูแลระบบ

ข้อ 14 ทรัพย์สินและด้านเทคโนโลยีสารสนเทศต่าง ๆ ที่สหกรณ์ จัดเตรียมไว้ให้ใช้งาน มีวัตถุประสงค์เพื่อการใช้งานของสหกรณ์เท่านั้น ห้ามมิให้ผู้ใช้งานนำทรัพย์สินและด้านเทคโนโลยีสารสนเทศต่าง ๆ ไปใช้ในกิจกรรมที่สหกรณ์ไม่ได้กำหนด หรือทำให้เกิดความเสียหายต่อสหกรณ์

ข้อ 15 ความเสียหายใด ๆ ที่เกิดจากการละเมิดตามข้อ 16 ข้อ 18 ให้ถือเป็นความผิดส่วนบุคคลโดยผู้ใช้งาน ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

หมวด 3 ว่าด้วยการบริหารจัดการข้อมูลองค์กร (Corporate Management)

ข้อ 16 ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูล ไม่ว่าข้อมูลนั้นจะเป็นของสหกรณ์ หรือเป็นข้อมูลของบุคคลภายนอก

ข้อ 17 ข้อมูลทั้งหลายที่อยู่ภายในทรัพย์สินของสหกรณ์ ถือเป็นทรัพย์สินของสหกรณ์ ห้ามมิให้ทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย โดยไม่ได้รับอนุญาตจากผู้บริหารสหกรณ์

ข้อ 18 ผู้ใช้งานมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลของสหกรณ์ หรือข้อมูลของผู้รับบริการ หากเกิดการสูญหาย โดยนำไปใช้ในทางที่ผิด การเผยแพร่โดยไม่รับอนุญาต ผู้ใช้งานต้องมีส่วนร่วม ในการรับผิดชอบต่อความเสียหายนั้นด้วย

ข้อ 19 ผู้ใช้งานต้องป้องกัน ดูแล รักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูล

ข้อ 20 ผู้ใช้งานมีสิทธิโดยชอบธรรมที่จะเก็บ รักษา ใช้งานและป้องกันข้อมูลส่วนบุคคลตามเห็นสมควร สหกรณ์จะให้การสนับสนุนและเคารพต่อสิทธิส่วนบุคคล และไม่อนุญาตให้บุคคลหนึ่งบุคคลใดทำการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้น ยกเว้นในกรณีที่สหกรณ์ ต้องการตรวจสอบข้อมูลหรือ คาดว่าข้อมูลนั้นเกี่ยวข้องกับสหกรณ์ ซึ่งสหกรณ์อาจแต่งตั้งให้ผู้ทำหน้าที่ตรวจสอบ ทำการตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลา โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

หมวด 4 ว่าด้วยซอฟต์แวร์และลิขสิทธิ์

(Software Licensing and intellectual property)

ข้อ 21 สหกรณ์ได้ให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญา ดังนั้นซอฟต์แวร์ที่สหกรณ์อนุญาตให้ใช้งานหรือที่สหกรณ์มีลิขสิทธิ์ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และสหกรณ์ห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากมีการตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ์ สหกรณ์ถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงผู้เดียว

ข้อ 22 ซอฟต์แวร์ (Software) ที่สหกรณ์ได้จัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็นต่อการทำงาน ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น

หมวด 5 ว่าด้วยการป้องกันโปรแกรมไม่ประสงค์ดี

(Preventing MalWare)

ข้อ 23 คอมพิวเตอร์ของผู้ใช้งานติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Antivirus) ตามที่สหกรณ์ ได้ประกาศให้ใช้ เว้นแต่คอมพิวเตอร์นั้นเป็นเครื่องเพื่อการศึกษา พัฒนา ระบบป้องกัน โดยต้องได้รับอนุญาตจากผู้บริหารสหกรณ์

ข้อ 24 บรรดาข้อมูล ไฟล์ ซอฟต์แวร์ หรือสิ่งอื่นใด ที่ได้รับจากผู้ใช้งานอื่นต้องได้รับการตรวจสอบไวรัสคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดีก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง

ข้อ 25 ผู้ใช้งานต้องทำการปรับปรุงข้อมูล สำหรับตรวจสอบและปรับปรุงระบบปฏิบัติการ (Update patch) ให้ใหม่เสมอ เพื่อเป็นการป้องกันความเสียหายที่อาจเกิดขึ้น

ข้อ 26 ผู้ใช้งานต้องพึงระวังไวรัสและโปรแกรมไม่ประสงค์ดีตลอดเวลา รวมทั้งเมื่อพบสิ่งผิดปกติ ผู้ใช้งานต้องแจ้งเหตุแก่ผู้ดูแลระบบ เมื่อผู้ใช้งานพบว่าเครื่องคอมพิวเตอร์ติดไวรัส ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่เครือข่าย และต้องแจ้งแก่ผู้ดูแลระบบ

ข้อ 27 ห้ามลักลอบทำสำเนา เปลี่ยนแปลง ลบทิ้ง ซึ่งข้อมูล ข้อความ เอกสาร หรือสิ่งใด ๆ ที่เป็นทรัพย์สินของสหกรณ์หรือของผู้อื่น โดยไม่ได้รับอนุญาตจากผู้มีอำนาจ ห้ามทำการเผยแพร่ไวรัสคอมพิวเตอร์มัลแวร์ หรือโปรแกรมอันตรายใด ๆ ที่อาจก่อให้เกิดความเสียหายมาสู่ทรัพย์สินของสหกรณ์

ประกาศ ณ วันที่ 28 เดือน ตุลาคม พ.ศ. 2565

(นายพิเชษฐ์ จั่นแก้ว)

ประธานกรรมการ

สหกรณ์ออมทรัพย์สาธารณสุขสมุทรสงคราม จำกัด ชุดที่ 41

นโยบายการรักษาความปลอดภัยของเครือข่ายไร้สาย (Wireless Policy)

ข้อ 1 ผู้ดูแลระบบ (System Administrator) ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access Point) ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายน้อยที่สุด

ข้อ 2 ผู้ดูแลระบบ (System Administrator) ควรทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าโดยปริยาย (Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ (Access Point) มาใช้งาน

ข้อ 3 ผู้ดูแลระบบ (System Administrator) ต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาต ใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในต่างๆ ของหน่วยงาน

ประกาศ ณ วันที่ 28 เดือน ตุลาคม พ.ศ. 2565



(นายพิเชษฐ์ จันแก้ว)

ประธานกรรมการ

สหกรณ์ออมทรัพย์สาธารณสุขสมุทรสงคราม จำกัด ชุดที่ 41

นโยบายการรักษาความปลอดภัยของอีเมล(E-mail Policy)

- ข้อ 1 ในการลงทะเบียนบัญชีผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ (e-mail) ต้องทำการกรอกข้อมูลคำขอเข้าใช้บริการจดหมายอิเล็กทรอนิกส์ (e-mail) ของหน่วยงานโดยยื่นคำขอกับเจ้าหน้าที่สหกรณ์
- ข้อ 2 เมื่อได้รับรหัสผ่าน (Password) ครั้งแรกในการเข้าระบบจดหมายอิเล็กทรอนิกส์ (e-mail) และเมื่อมีการเข้าสู่ระบบในครั้งแรกนั้น ควรเปลี่ยนรหัสผ่าน (Password) โดยทันที
- ข้อ 3 ไม่ควรบันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์
- ข้อ 4 ควรเปลี่ยนรหัสผ่าน (Password) ทุก 3 - 6 เดือน
- ข้อ 5 ไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail address) ของผู้อื่นเพื่ออ่านหรือรับหรือส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้บริการและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์ (e-mail) เป็นผู้รับผิดชอบต่อการใช้งานในจดหมายอิเล็กทรอนิกส์ (e-mail) ของตน
- ข้อ 6 หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (e-mail) เสร็จสิ้นควรลงบันทึกออก (Logout) ทุกครั้ง
- ข้อ 7 การส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์ (e-mail)

ประกาศ ณ วันที่ 28 เดือน ตุลาคม พ.ศ. 2565



(นายพิเชษฐ์ จั่นแก้ว)

ประธานกรรมการ

สหกรณ์ออมทรัพย์สาธารณสุขสมุทรสงคราม จำกัด ชุดที่ 41

นโยบายการรักษาความปลอดภัยของอินเทอร์เน็ต (Internet Security Policy)

ข้อ 1 ไม่ใช้ระบบอินเทอร์เน็ต (Internet) ของหน่วยงาน เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อการรักษาความต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคมหรือละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับหน่วยงาน

ข้อ 2 ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงานที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต (Internet)

ข้อ 3 ระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากระบบอินเทอร์เน็ต (Internet) การดาวน์โหลดการอัปเดต (Update) โปรแกรมต่าง ๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์

ข้อ 4 ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของหน่วยงาน

ข้อ 5 ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน การทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่น ๆ

ข้อ 6 หลังจากใช้งานระบบอินเทอร์เน็ต (Internet) เสร็จแล้ว ให้ปิดเว็บเบราว์เซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ

ประกาศ ณ วันที่ 28 เดือน ตุลาคม พ.ศ. 2565

(นายพิเชษฐ์ จั่นแก้ว)

ประธานกรรมการ

สหกรณ์ออมทรัพย์สาธารณสุขสมุทรสงคราม จำกัด ชุดที่ 41

นโยบายการรักษาความปลอดภัยของการควบคุมการเข้าถึงระบบ (Access control Policy)

หมวด 1

การควบคุมการเข้าถึงด้านเทคโนโลยีสารสนเทศ

ข้อ 1 สหกรณ์กำหนดมาตรการควบคุมการเข้าใช้งาน ด้านเทคโนโลยีสารสนเทศของหน่วยงานเพื่อดูแลรักษาความปลอดภัย โดยที่บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานด้านเทคโนโลยีสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษรต่อผู้บัญชาการสำนักงานสหกรณ์

ข้อ 2 ผู้ดูแลระบบ (System Administrator) ต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งานระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อน เข้าใช้ด้านเทคโนโลยีสารสนเทศ รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ

ข้อ 3 ผู้ดูแลระบบ (System Administrator) ควรจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานด้านเทคโนโลยีสารสนเทศของหน่วยงาน และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบข้อมูล

ข้อ 4 ผู้ดูแลระบบ (System Administrator) ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบการแก้ไขเปลี่ยนแปลงสิทธิ์ต่าง ๆ และการผ่านเข้า-ออกสถานที่ตั้งของระบบของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาตเพื่อเป็นหลักฐานในการตรวจสอบ

หมวด 2

การบริหารจัดการการเข้าถึงด้านเทคโนโลยีสารสนเทศ

ข้อ 1 ผู้ดูแลระบบ (System Administrator) ต้องกำหนดการลงทะเบียนบุคลากรใหม่ของสหกรณ์ ควรกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการเพื่อให้มีสิทธิ์ต่างๆ ในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เช่น การลาออก หรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น

ข้อ 2 ผู้ดูแลระบบ (System Administrator) ต้องกำหนดการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงาน ในหน้าที่และต้องได้รับความเห็นชอบจากผู้บริหารสหกรณ์เป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ ดังกล่าวอย่างสม่ำเสมอ

ข้อ 3 ผู้ดูแลระบบ (System Administrator) ต้องบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่านของบุคลากรดังต่อไปนี้

(1) กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

(2) ส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้บริการด้วยวิธีการที่ปลอดภัย คว หลีกเลี่ยงการให้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (e-mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน (Password)

(3) ควรกำหนดให้ผู้ให้บริการตอบยืนยันการได้รับรหัสผ่าน (Password)

(4) ควรกำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

(5) กำหนดชื่อผู้ใช้หรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

(6) ในกรณี...



(6) ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บริหารสหกรณ์ โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

ข้อ 4 ผู้ดูแลระบบ (System Administrator) ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ ในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

(1) ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

(2) ต้องกำหนดรายชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

(3) ควรกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

(4) การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL VPN หรือ XML Encryption เป็นต้น

(5) ควรกำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

(6) ควรกำหนดมาตรการรักษาการรักษาความปลอดภัยของข้อมูลในกรณีที่น่าเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

ประกาศ ณ วันที่ 28 เดือน ตุลาคม พ.ศ. 2565

(นายพิเชษฐ์ จันแก้ว)

ประธานกรรมการ

สหกรณ์ออมทรัพย์สาธารณสุขสุพรรณบุรี จำกัด ชุดที่ 41

นโยบายการรักษาความปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Network and Server Policy)

ข้อ 1 ผู้ใช้บริการจะนำเครื่องคอมพิวเตอร์และอุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงาน ต้องได้รับอนุญาตจากผู้บัญชาการสหกรณ์ และต้องปฏิบัติตามนโยบายนี้โดยเคร่งครัด

ข้อ 2 การขออนุญาตใช้งานพื้นที่ Web Server และชื่อโดเมนย่อย (Sub Domain Name) ที่หน่วยงานรับผิดชอบอยู่ จะต้องทำหนังสือขออนุญาตต่อผู้บัญชาการสหกรณ์ และจะต้องไม่ติดตั้งโปรแกรมใดๆ ที่ส่งผลกระทบต่อการทำงานของระบบและผู้ใช้บริการอื่นๆ

ข้อ 3 ผู้ดูแลระบบ (System Administrator) ต้องควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ ดังต่อไปนี้

(1) การเข้าสู่ระบบเครือข่ายภายในสหกรณ์ โดยผ่านทางอินเทอร์เน็ตจำเป็นต้องมีการลงบันทึกเข้า และต้องมีการพิสูจน์ยืนยันตัวตน เพื่อตรวจสอบความถูกต้องของผู้ใช้บริการ

(2) เลขที่อยู่ไอพีภายในของระบบเครือข่ายภายในของสหกรณ์ จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้

(3) ต้องจัดทำแผนผังระบบเครือข่าย ซึ่งรายละเอียดเกี่ยวข้องกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

(4) การใช้เครื่องมือต่างๆ เพื่อการตรวจสอบระบบเครือข่าย ควรได้รับการอนุมัติจากผู้ดูแลระบบ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

ข้อ 4 สหกรณ์กำหนดมาตรการควบคุมการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์ แม่ข่าย เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอกตามแนวทาง ดังต่อไปนี้

(1) บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการใช้งานระบบเครือข่าย และเครื่องคอมพิวเตอร์แม่ข่ายของสหกรณ์ จะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุญาตจากผู้บริหารสหกรณ์

(2) มีการควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

(3) วิธีการใดๆ ที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้จากระยะไกลต้องได้รับการอนุญาตจากผู้บัญชาการสหกรณ์

(4) การเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐาน ระบุเหตุผลหรือความจำเป็น ในการดำเนินงานกับหน่วยงานอย่างเพียงพอ

(5) การใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจากระบบของหน่วยงาน

ประกาศ ณ วันที่ 28 เดือน ตุลาคม พ.ศ. 2565

(นายพิเชษฐ์ จันแก้ว)

ประธานกรรมการ

สหกรณ์ออมทรัพย์สาธารณสุขสมุทรสงคราม จำกัด ชุดที่ 41