



ระเบียบสหกรณ์ออมทรัพย์มหาวิทยาลัยสงขลานครินทร์ จำกัด
ว่าด้วย การควบคุมภายในและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ
พ.ศ. 2561

อาศัยอำนาจตามความในข้อบังคับสหกรณ์ออมทรัพย์มหาวิทยาลัยสงขลานครินทร์ จำกัด ข้อ 78(8) และข้อ 110(10) ที่ประชุมคณะกรรมการดำเนินการ ชุดที่ 45 ครั้งที่ 6 เมื่อวันที่ 13 มิถุนายน 2561 มีมติกำหนดระเบียบสหกรณ์ออมทรัพย์มหาวิทยาลัยสงขลานครินทร์ จำกัด ว่าด้วยการควบคุมภายในและการรักษาความปลอดภัย ด้านเทคโนโลยีสารสนเทศ พ.ศ. 2561 ดังต่อไปนี้

ข้อ 1 ระเบียบนี้เรียกว่า “ระเบียบสหกรณ์ออมทรัพย์มหาวิทยาลัยสงขลานครินทร์ จำกัด ว่าด้วยการควบคุมภายใน และการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ พ.ศ. 2561”

ข้อ 2 ระเบียบนี้ให้ใช้บังคับตั้งแต่วันที่ 14 มิถุนายน 2561 เป็นต้นไป

ข้อ 3 ให้ยกเลิกบรรดาระเบียบ คำสั่ง และคำแนะนำต่างๆ ในส่วนที่ได้กำหนดไว้แล้ว ที่ขัดหรือแย้งกับระเบียบนี้ให้ใช้ระเบียบนี้แทน

ข้อ 4 ในระเบียบนี้

สหกรณ์ หมายถึง สหกรณ์ออมทรัพย์มหาวิทยาลัยสงขลานครินทร์ จำกัด

คณะกรรมการ หมายถึง คณะกรรมการดำเนินการสหกรณ์

ประธานกรรมการ หมายถึง ประธานกรรมการดำเนินการสหกรณ์

ผู้จัดการใหญ่ หมายถึง ผู้จัดการใหญ่สหกรณ์

รองผู้จัดการใหญ่ หมายถึง รองผู้จัดการใหญ่สหกรณ์

ผู้จัดการฝ่ายพัฒนาระบบสารสนเทศ หมายถึง ผู้จัดการฝ่ายพัฒนาระบบสารสนเทศสหกรณ์

ผู้ดูแลระบบ หมายถึง ผู้จัดการใหญ่หรือรองผู้จัดการใหญ่ที่ได้รับมอบหมาย

ผู้ควบคุมระบบ หมายถึง ผู้จัดการฝ่ายพัฒนาระบบสารสนเทศหรือผู้ได้รับมอบหมาย

ผู้ใช้งาน หมายถึง เจ้าหน้าที่สหกรณ์ผู้ปฏิบัติงานเกี่ยวกับโปรแกรมระบบงานสหกรณ์ออมทรัพย์ และโปรแกรมอื่นๆที่เกี่ยวข้อง

เครื่องคอมพิวเตอร์ หมายถึง เครื่องคอมพิวเตอร์ทั้งหลาย เครื่องเซิร์ฟเวอร์ หรืออุปกรณ์อื่นใดที่ทำหน้าที่ได้เสมือนเครื่องคอมพิวเตอร์ทั้งที่ใช้งานอยู่ในสหกรณ์หรือภายนอกแล้วเชื่อมต่อเข้ากับระบบเครือข่าย

ระบบเครือข่าย หมายถึง ระบบเครือข่ายคอมพิวเตอร์ที่สหกรณ์จัดให้มีขึ้นทั้งแบบมีสายและไร้สาย

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

ระบบสารสนเทศ หมายถึง ข้อมูล และสาระต่างๆที่เกิดจากการประมวลผลมาจากข้อมูล ที่จัดไว้อย่างเป็นระบบ

หมวด 1

นโยบายการควบคุมภายในและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ

ข้อ 5 สหกรณ์มีการนำระบบโปรแกรมคอมพิวเตอร์มาใช้ในการประมวลผลข้อมูล และจัดทำการเงินซึ่งอาจจะก่อให้เกิดความเสี่ยง และความเสียหายต่อข้อมูลที่สำคัญของสหกรณ์ได้ จึงต้องมีการเตรียมมาตรการในการป้องกันความเสี่ยงระบบสารสนเทศไว้ และมีการบริหารจัดการ การควบคุมงานด้านคอมพิวเตอร์อย่างมีระบบ และประสิทธิภาพรวมทั้งให้เหมาะสมตามสภาพแวดล้อมที่ได้เปลี่ยนแปลงไปในการประมวลผลข้อมูลด้วยคอมพิวเตอร์

ข้อ 6 การรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ เป็นการจัดทำขึ้นเพื่อกำหนดแนวทางเป็นกรอบและเป็นแผนที่นำทางในระดับกลยุทธ์เพื่อยกระดับมาตรฐานการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของสหกรณ์ให้อยู่ระดับมาตรฐานสากล อีกทั้งต้องการลดผลกระทบจากเหตุการณ์โจมตี ตลอดจนการกู้คืนระบบอย่างรวดเร็วหลังจากการโจมตีสิ้นสุดลง เป็นแนวทางปฏิบัติของผู้ใช้งานด้านเทคโนโลยีสารสนเทศของสหกรณ์

ข้อ 7 การปฏิบัติในการควบคุมภายในและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศมีดังนี้

(1) จัดให้มีระบบการรักษาความปลอดภัยทางกายภาพที่เพียงพอแก่การป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่ที่เกี่ยวข้องเข้าถึงอุปกรณ์คอมพิวเตอร์ที่สำคัญและจัดให้มีระบบป้องกันความเสียหายจาก สภาวะแวดล้อม หรือภัยพิบัติต่างๆ ให้แก่อุปกรณ์คอมพิวเตอร์ที่สำคัญ

(2) จัดให้มีระบบการรักษาความปลอดภัยของข้อมูลในระบบคอมพิวเตอร์และระบบเครือข่ายที่เพียงพอแก่การป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่ที่เกี่ยวข้องได้เข้าถึง ล้วงรู้ใช้ประโยชน์หรือแก้ไขเปลี่ยนแปลง ข้อมูลหรือระบบดังกล่าวได้

(3) จัดให้มีมาตรการควบคุมการพัฒนาหรือแก้ไขเปลี่ยนแปลงที่เพียงพอ เพื่อให้ระบบโปรแกรม คอมพิวเตอร์มีการประมวลผลที่ถูกต้องครบถ้วนและเป็นไปตามความต้องการของผู้ใช้งาน รวมทั้งต้องมีการสื่อสาร หรือฝึกอบรมเกี่ยวกับระบบบัญชีคอมพิวเตอร์ให้ผู้เกี่ยวข้องได้รับทราบอย่างทั่วถึง เพื่อให้สามารถใช้งานได้อย่างถูกต้อง

(4) จัดให้มีและควบคุมดูแลเอกสารสนับสนุนการปฏิบัติงานสำหรับโปรแกรมคอมพิวเตอร์ โดยมี รายละเอียด ดังนี้

ก. เอกสารสนับสนุนการปฏิบัติงาน

1) เอกสารด้านข้อมูลของระบบบัญชีคอมพิวเตอร์เป็นเอกสารแสดงรายละเอียดการจัดเก็บข้อมูลที่เป็นสาระสำคัญทางบัญชีทั้งนี้เพื่อให้สหกรณ์สามารถเข้าใจถึงโครงสร้างการจัดเก็บข้อมูลของระบบ บัญชีคอมพิวเตอร์ที่ใช้งานอยู่และใช้อ้างอิงเพื่อแก้ไขปัญหาได้โดยเอกสารด้านฐานข้อมูลของระบบโปรแกรมคอมพิวเตอร์ที่จำเป็นจะต้องมีคือผังการไหลของข้อมูล (Data Flow Diagram) และพจนานุกรมข้อมูล (Data Dictionary) หรือตารางแสดงรายละเอียดข้อมูลตามแบบที่กรมตรวจบัญชีสหกรณ์กำหนด

2) คู่มือการใช้ระบบโปรแกรมคอมพิวเตอร์เพื่อเป็นเอกสารประกอบการทำงานของผู้ใช้งานในการบันทึกข้อมูล ประมวลผลข้อมูล และออกรายงานได้อย่างถูกต้อง

ข. การควบคุมดูแลเอกสารสนับสนุนการปฏิบัติงาน โดยจัดให้มีสถานที่เก็บและปรับปรุงเอกสารให้ถูกต้องและทันสมัยอยู่เสมอ

(5) จะต้องสามารถเข้าถึงฐานข้อมูลของระบบโปรแกรมคอมพิวเตอร์ได้และสามารถนำข้อมูลออกจากฐานข้อมูลในรูปแบบที่อ่านเข้าใจได้

(6) จัดให้มีการสำรองข้อมูลของระบบโปรแกรมคอมพิวเตอร์เพื่อให้สามารถรองรับการดำเนินงานได้อย่างต่อเนื่อง มีประสิทธิภาพและทันเหตุการณ์ตลอดจนจัดให้มีการดูแลรักษาข้อมูลชุดสำรองให้มีความปลอดภัยรวมทั้งจัดให้มีการป้องกันมิให้มีการนำข้อมูลชุดสำรองมาใช้โดยไม่ถูกต้อง

หมวด 2

การควบคุมภายในด้านเทคโนโลยีสารสนเทศ

ข้อ 8 การควบคุมการเข้าถึงระบบงาน

(1) ให้ผู้ควบคุมระบบการเข้าถึงระบบงานและข้อมูล เป็นผู้กำหนดสิทธิและควบคุมการเข้าถึงระบบงานและข้อมูลให้เป็นไปตามความรับผิดชอบของเจ้าหน้าที่ของแต่ละระบบงานที่มีการมอบหมายตามมติคณะกรรมการหรือคำสั่งปฏิบัติงาน รวมถึงการสอบถามสิทธิการใช้งานให้สอดคล้องตามภาระงานให้เป็นปัจจุบันเสมอ

(2) ผู้ควบคุมระบบต้องจัดที่ตั้งอุปกรณ์คอมพิวเตอร์อยู่ในส่วนที่ไม่อนุญาตให้บุคคลภายนอกที่ไม่มีหน้าที่เกี่ยวข้องเข้ามาในส่วนการทำงานของเจ้าหน้าที่

(3) ผู้ควบคุมระบบต้องจัดให้มีผู้รับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์และผู้ใช้งานต้องมีการกำหนดรหัสในการอนุญาตใช้งาน

(4) ผู้ควบคุมระบบต้องกำหนดให้ผู้ใช้มีรหัสใช้งาน (User account) และมีการกำหนดรหัสผ่าน (User ID) ในการเข้าใช้ระบบงานโดยกำหนด รวมถึงการยกเลิกรหัสผู้ใช้ของเจ้าหน้าที่ที่ลาออก และกำหนดรหัสผู้ใช้ให้แก่เจ้าหน้าที่ที่เข้ามาปฏิบัติงานใหม่

(5) ผู้ควบคุมระบบต้องกำกับดูแลให้ผู้ใช้งานต้องมีการเปลี่ยนรหัสผ่านทุกๆ 6 เดือน เป็นอย่างน้อย

(6) ผู้ใช้งานต้องเก็บรักษารหัสผ่านเป็นความลับ มิให้ผู้ใดล่วงรู้หากพิสูจน์ได้ว่าเกิดความเสียหายกับระบบ และข้อมูลจากรหัสผู้ใช้งานนั้น ผู้ใช้งานนั้นต้องเป็นผู้รับผิดชอบในความเสียหายที่เกิดขึ้น

(7) ผู้ใช้งานต้องใช้งานคอมพิวเตอร์เพื่อประโยชน์สูงสุดต่อการดำเนินงานของสภกรณ์และเป็นไปตามวัตถุประสงค์

(8) ต้องคำนึงถึงการใช้งานอย่างประหยัด และหมั่นตรวจสอบเครื่องคอมพิวเตอร์ให้สามารถใช้งานได้อย่างสมบูรณ์และมีประสิทธิภาพ

(9) เมื่อผู้ใช้งานพบเหตุการณ์ผิดปกติที่เกี่ยวกับความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศให้รีบแจ้งให้ผู้ควบคุมระบบหรือผู้บังคับบัญชาตามลำดับชั้นทราบโดยทันที

ข้อ 9 การควบคุมการประมวลผลและเพิ่มข้อมูลคอมพิวเตอร์

(1) การพัฒนาการเปลี่ยนแปลงแก้ไขโปรแกรมประมวลผล ให้มีการปฏิบัติให้เป็นไปตามขั้นตอนที่กำหนดดังนี้

ก. ต้องมีหนังสือเป็นลายลักษณ์อักษรแจ้งความต้องการของผู้ใช้งานในการเปลี่ยนแปลงระบบ

ข. ต้องได้รับอนุมัติจากผู้ดูแลระบบ

ค. กำหนดผู้รับผิดชอบในการพัฒนาซึ่งต้องไม่เป็นผู้ที่ทำหน้าที่ใช้งานระบบแต่อย่างใด

ง. มีการทดสอบระบบงานที่พัฒนาเพื่อมั่นใจว่าระบบสามารถประมวลผลได้อย่างถูกต้องและเป็นไปตามความต้องการ

จ. จัดให้มีการฝึกอบรมแก่ผู้ใช้งาน เพื่อให้เกิดความเข้าใจและทำงานได้อย่างถูกต้อง

(2) ในกรณีที่มีการเปลี่ยนแปลงข้อมูลหลักที่สำคัญ เช่น อัตราดอกเบี้ย เงื่อนไขการให้สินเชื่อ และอื่น ๆ ต้องมีการสั่งการของผู้มีอำนาจเป็นลายลักษณ์อักษร

ข้อ 10 การควบคุมดูแลเอกสารสนับสนุนการปฏิบัติงานสำหรับระบบโปรแกรมคอมพิวเตอร์

(1) ผู้ควบคุมระบบต้องจัดให้มีเอกสารด้านฐานข้อมูลที่เป็นได้แก่ ผังการไหลของข้อมูล (Data Flow Diagram) และ พจนานุกรมข้อมูล (Data Dictionary) รวมถึงคู่มือการใช้งานระบบงานและต้องปรับปรุงให้เป็นปัจจุบันเสมอ

(2) ผู้ควบคุมระบบต้องจัดเก็บเอกสารสนับสนุนการปฏิบัติงานในสถานที่ที่ปลอดภัยและสามารถเรียกใช้งานได้

หมวด 3

การรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ

ข้อ 11 การพิสูจน์ตัวตน

(1) ผู้ใช้งานมีหน้าที่ในการป้องกัน ดูแลรักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งาน (Username) ของตนเอง ห้ามใช้ร่วมกับผู้อื่นรวมทั้งห้ามทำการเผยแพร่แจกจ่ายทำให้ผู้อื่นล่วงรู้รหัสผ่าน (Password)

(2) ผู้ใช้งานต้องรับผิดชอบต่อการกระทำใด ๆ ที่เกิดจากบัญชีของผู้ใช้งาน (Username) ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม

(3) ผู้ใช้งานต้องตั้งรหัสผ่านให้เกิดความปลอดภัย

(4) ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) ทุก ๆ 6 เดือน หรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่านและความยาวขั้นต่ำของรหัสผ่านไม่ต่ำกว่า 8 ตัวอักษร เป็นตัวอักษรและตัวเลข

(5) ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งในการใช้งานอินเทอร์เน็ต (Internet) การเข้าถึงระบบปฏิบัติการ การใช้งานระบบคอมพิวเตอร์อื่นใด

(6) ผู้ใช้งานต้องทำการพิสูจน์ตัวตนในการใช้งานเครื่องคอมพิวเตอร์ทุกครั้ง และต้องทำการล็อก(Lock)หน้าจอทุกครั้ง เมื่อผู้ใช้งานไม่อยู่ที่เครื่องคอมพิวเตอร์

ข้อ 12 การบริหารจัดการทรัพย์สิน

(1) ผู้ใช้งานต้องไม่เข้าไปในห้องคอมพิวเตอร์แม่ข่าย (Sever) สหกรณ์ที่เป็นเขตหวงห้ามโดยเด็ดขาด เว้นแต่ได้รับอนุญาตจากผู้ควบคุมระบบ

(2) ผู้ใช้งานต้องไม่นำอุปกรณ์หรือชิ้นส่วนใดออกจากห้องคอมพิวเตอร์แม่ข่าย (Sever) เว้นแต่จะได้รับอนุญาตจากผู้ควบคุมระบบ

(3) ผู้ใช้งานต้องไม่นำเครื่องมือ หรืออุปกรณ์อื่นใด เชื่อมเข้าเครือข่ายที่ไม่ได้เกี่ยวข้องกับกิจการของสหกรณ์

(4) ผู้ใช้งานต้องไม่ใช้หรือลบเพิ่มข้อมูลของผู้อื่น ไม่ว่ากรณีใด ๆ

(5) ผู้ใช้งานต้องไม่คัดลอกหรือทำสำเนาเพิ่มข้อมูลที่มีลิขสิทธิ์ก้ำกับการใช้งานก่อนได้รับ

อนุญาต

(6) ผู้ใช้งานมีหน้าที่ต้องรับผิดชอบต่อทรัพย์สินที่สหกรณ์มอบไว้ให้ใช้งาน โดยบรรดารายการทรัพย์สิน (Asset lists) ที่ผู้ใช้งานต้องรับผิดชอบจะต้องบันทึกในบัญชีรายการทรัพย์สินและชื่อผู้ใช้งานทรัพย์สินนั้น การรับหรือคืนทรัพย์สินจะถูกบันทึกและตรวจสอบทุกครั้งโดยเจ้าหน้าที่ที่สหกรณ์มอบหมาย

(7) กรณีทำงานนอกสถานที่ผู้ใช้งานต้องดูแล และรับผิดชอบทรัพย์สินของสหกรณ์ที่ได้รับมอบหมาย

(8) ผู้ใช้งานมีหน้าที่ต้องชดเชยค่าเสียหายไม่ว่าทรัพย์สินนั้นจะชำรุด หรือสูญหายตามมูลค่าทรัพย์สิน หากความเสียหายนั้นเกิดจากความประมาทของผู้ใช้งาน

(9) ผู้ใช้งานต้องไม่ให้ผู้อื่นยืมคอมพิวเตอร์หรือโน้ตบุ๊ก ไม่ว่าในกรณีใดๆ เว้นแต่การยืมนั้นได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้มีอำนาจ

(10) ทรัพย์สิน และอุปกรณ์ด้านเทคโนโลยีสารสนเทศต่าง ๆ ที่สหกรณ์จัดเตรียมไว้ให้ใช้งานมีวัตถุประสงค์เพื่อการใช้งานของสหกรณ์เท่านั้น ห้ามมิให้ผู้ใช้งานนำทรัพย์สินและอุปกรณ์ด้านเทคโนโลยีสารสนเทศต่างๆ ไปใช้ในกิจกรรมที่สหกรณ์ไม่ได้กำหนดหรือทำให้เกิดความเสียหายต่อสหกรณ์

(11) ความเสียหายใดๆ ที่เกิดจากการกระทำตาม (10) ให้ถือเป็นความผิดส่วนบุคคลโดยผู้ใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

(12) สหกรณ์จะต้องจัดตั้งเครื่องคอมพิวเตอร์ไว้ในที่ที่เหมาะสม และห้ามผู้ที่ไม่มีหน้าที่รับผิดชอบเข้ามาใช้เครื่องคอมพิวเตอร์ของสหกรณ์โดยไม่ได้รับอนุญาต

(13) สหกรณ์จะต้องจัดให้มีการติดตั้งอุปกรณ์ดับเพลิงไว้ในที่เหมาะสมและสะดวกต่อการใช้งานเมื่อมีเหตุฉุกเฉิน และจัดทำแผนผังการขนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ รวมทั้งเอกสารที่เกี่ยวข้อง

(14) สหกรณ์จะต้องจัดให้มีระบบการควบคุมอุณหภูมิ ให้แก่อุปกรณ์เครื่องคอมพิวเตอร์อย่างเพียงพอและเหมาะสมกับสถานที่รวมทั้งจัดตั้งเครื่องปรับอากาศให้อยู่ในสถานที่ที่มีอากาศถ่ายเทได้สะดวก

(15) สหกรณ์จะต้องจัดให้มีระบบสำรองไฟเครื่องแม่ข่ายและอุปกรณ์ที่เกี่ยวข้องอย่างพอเพียง เพื่อลดการหยุดชะงักการทำงานของเครื่องแม่ข่ายในกรณีที่มีไฟฟ้าดับหรือไฟตก

ข้อ 13 การบริหารจัดการข้อมูลองค์กร

(1) ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูล ไม่ว่าข้อมูลนั้นจะเป็นของสหกรณ์หรือเป็นข้อมูลของบุคคลภายนอก

(2) ข้อมูลทั้งหลายที่อยู่ภายในทรัพย์สินของสหกรณ์ถือเป็นทรัพย์สินของสหกรณ์ห้ามไม่ให้ทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย โดยไม่ได้รับอนุญาตจากสหกรณ์

(3) ผู้ใช้งานมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลของสหกรณ์หรือข้อมูลของผู้รับบริการ หากเกิดการสูญหาย โดยนำไปใช้ในทางที่ผิด การเผยแพร่โดยไม่ได้รับอนุญาต ผู้ใช้งานต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้นด้วย

(4) ผู้ใช้งานต้องป้องกัน ดูแล รักษาไว้ซึ่งความลับ ความถูกต้องและความพร้อมใช้ของข้อมูล

(5) ผู้ใช้งานมีสิทธิโดยชอบธรรมที่จะเก็บรักษา ใช้งานและป้องกันข้อมูลส่วนบุคคลตามสมควร สหกรณ์จะให้การสนับสนุนและเคารพต่อสิทธิส่วนบุคคล และไม่อนุญาตให้บุคคลหนึ่งบุคคลใดทำการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้น ยกเว้นในกรณีที่สหกรณ์ต้องการตรวจสอบข้อมูล หรือคาดว่าข้อมูลนั้นเกี่ยวข้องกับสหกรณ์ ซึ่งสหกรณ์อาจแต่งตั้งให้ผู้ทำหน้าที่ตรวจสอบทำการตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลา โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

ข้อ 14 การบริหารจัดการด้านเทคโนโลยีสารสนเทศ

(1) ผู้ใช้งานมีสิทธิที่จะพัฒนาโปรแกรมหรือเครื่องคอมพิวเตอร์ใด ๆ แต่ต้องไม่ดำเนินการดังนี้

ก. พัฒนาโปรแกรมหรือเครื่องคอมพิวเตอร์ใด ๆ ที่จะทำลายกลไกรักษาความปลอดภัยระบบรวมทั้งการกระทำในลักษณะเป็นการแอบใช้รหัสผ่าน การลักลอบทำสำเนาข้อมูลบุคคลอื่นหรือแกะรหัสผ่านของบุคคลอื่น

ข. พัฒนาโปรแกรมหรือเครื่องคอมพิวเตอร์ใด ๆ ซึ่งทำให้ผู้ใช้สิทธิและลำดับความสำคัญในการครอบครองทรัพยากรระบบมากกว่าผู้อื่น

ค. พัฒนาโปรแกรมใดที่จะทำซ้ำตัวโปรแกรมหรือแผ่ตัวโปรแกรมไปกับโปรแกรมอื่นในลักษณะเช่นเดียวกับมัลแวร์ หรือไวรัสคอมพิวเตอร์

ง. พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ที่จะทำลายระบบจำกัดสิทธิการใช้ (License) ซอฟต์แวร์

จ. นำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ แสดงข้อความ รูปภาพไม่เหมาะสม หรือขัดต่อศีลธรรมประเพณีอันดีงามของประเทศไทย กรณีที่ผู้ใช้สร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์

(2) ห้ามติดตั้งอุปกรณ์หรือกระทำการใดเพื่อให้สามารถเข้าถึงอุปกรณ์ด้านเทคโนโลยีสารสนเทศของสหกรณ์โดยไม่ได้รับอนุญาตจากผู้มีอำนาจ

ข้อ 15 ซอฟต์แวร์ และลิขสิทธิ์

(1) สหกรณ์ได้ให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญา ดังนั้นซอฟต์แวร์ที่สหกรณ์อนุญาตให้ใช้งาน หรือที่สหกรณ์มีลิขสิทธิ์ผู้ใช้งานสามารถใช้งานได้ตามหน้าที่ความจำเป็น และสหกรณ์ห้ามไม่ให้ผู้ใช้งาน ทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์หากมีการตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ์

(2) ซอฟต์แวร์ (Software) ที่สหกรณ์ได้จัดเตรียมไว้ให้ผู้ใช้งานถือเป็นสิ่งจำเป็นต่อการทำงานห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น

ข้อ 16 การป้องกันโปรแกรมไม่ประสงค์ดี

(1) คอมพิวเตอร์ของผู้ใช้งานติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Antivirus) ตามที่ สหกรณ์ได้ประกาศให้ใช้เว้นแต่คอมพิวเตอร์นั้นเป็นเครื่องเพื่อการศึกษา พัฒนา ระบบป้องกัน โดยต้อง ได้รับ อนุญาตจากสหกรณ์

(2) บรรดาข้อมูลไฟล์ซอฟต์แวร์หรือสิ่งใด ที่ได้รับจากผู้ใช้งานอื่นต้องได้รับการ ตรวจสอบไวรัสคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดีก่อนนำมาใช้งาน หรือเก็บบันทึกทุกครั้ง

(3) ผู้ใช้งานต้องทำการปรับปรุงข้อมูล สำหรับตรวจสอบและปรับปรุงระบบปฏิบัติการ (Update patch) ให้ใหม่เสมอ เพื่อเป็นการป้องกันความเสียหายที่อาจเกิดขึ้น

(4) ผู้ใช้งานต้องพึงระวังไวรัสและโปรแกรมไม่ประสงค์ดีตลอดเวลา รวมทั้งเมื่อพบสิ่ง ผิดปกติผู้ใช้งานต้องแจ้งเหตุแก่ผู้ควบคุมระบบ

(5) เมื่อผู้ใช้งานพบว่าเครื่องคอมพิวเตอร์ติดไวรัสผู้ใช้งานต้องไม่เชื่อมต่อเครื่อง คอมพิวเตอร์เข้าสู่เครือข่าย และต้องแจ้งแก่ผู้ควบคุมระบบ

(6) ห้ามลักลอบทำสำเนา เปลี่ยนแปลง ลบทิ้ง ซึ่งข้อมูล ข้อความ เอกสาร หรือสิ่งใด ๆ ที่ เป็นทรัพย์สินของสหกรณ์หรือของผู้อื่น โดยไม่ได้รับอนุญาตจากผู้มีอำนาจ

(7) ห้ามทำการเผยแพร่ไวรัสคอมพิวเตอร์มัลแวร์หรือโปรแกรมอันตรายใด ๆ ที่อาจ ก่อให้เกิดความเสียหายมาสู่ทรัพย์สินของสหกรณ์

ข้อ 17 การรักษาความปลอดภัยของการควบคุมการเข้าถึงระบบ

(1) การควบคุมการเข้าถึงด้านเทคโนโลยีสารสนเทศ

ก. สหกรณ์กำหนดมาตรการควบคุมการเข้าใช้งาน ด้านเทคโนโลยีสารสนเทศของ สหกรณ์เพื่อดูแลรักษาความปลอดภัย โดยที่บุคคลภายนอกที่ต้องการสิทธิในการเข้าใช้งานด้านเทคโนโลยี สารสนเทศของสหกรณ์จะต้องขออนุญาตเป็นลายลักษณ์อักษรต่อประธานกรรมการสหกรณ์

ข. ผู้ควบคุมระบบ ต้องกำหนดสิทธิการเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสม กับการใช้งานของผู้ใช้งานระบบและเจ้าหน้าที่ ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้า ใช้ด้านเทคโนโลยีสารสนเทศ รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ

ค. ผู้ควบคุมระบบ ควรจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานด้าน เทคโนโลยีสารสนเทศของสหกรณ์ และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบข้อมูล

ง. ผู้ควบคุมระบบ ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบการแก้ไข เปลี่ยนแปลงสิทธิ์ต่าง ๆ และการผ่านเข้า – ออก สถานที่ตั้งของระบบของทั้งผู้ที่ได้รับอนุญาตและ ไม่ได้รับ อนุญาตเพื่อเป็นหลักฐานในการตรวจสอบ

(2) การบริหารจัดการการเข้าถึงด้านเทคโนโลยีสารสนเทศ

ก. ผู้ควบคุมระบบ ต้องกำหนดการลงทะเบียนบุคลากรใหม่ของสหกรณ์ กำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการเพื่อให้มีสิทธิ์ต่าง ๆ ในการใช้งานตามความจำเป็นรวมทั้ง ขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เช่น การลาออก หรือการเปลี่ยนตำแหน่งงานภายใน สหกรณ์ เป็นต้น

ข. ผู้ควบคุมระบบ ต้องกำหนดการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่าย ไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องใช้สิทธิ์เฉพาะการ ปฏิบัติงานใน หน้าที่และต้องได้รับความเห็นชอบจากสหกรณ์เป็นลายลักษณ์อักษร รวมทั้งต้องทบทวน สิทธิ์ดังกล่าว อย่างสม่ำเสมอ

ค. ผู้ควบคุมระบบ ต้องบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่านของ บุคลากรดังต่อไปนี้

1) กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อ ผู้ใช้งานระบบลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

2) ส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ให้บริการด้วยวิธีการที่ ปลอดภัยควรหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (e-mail) ที่ไม่มีการป้องกันใน การส่งรหัสผ่าน (Password)

3) กำหนดชื่อผู้ใช้หรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

ง. ผู้ควบคุมระบบ ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ ใน การควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

1) ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึง โดยตรงและการเข้าถึงผ่านระบบงาน

2) ต้องกำหนดรายชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อ ใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

3) การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการ เข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล

4) กำหนดมาตรการรักษาการรักรักษาความปลอดภัยของข้อมูลในกรณีที่ นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของสหกรณ์

ข้อ 18 การรักษาความปลอดภัยของเครือข่ายไร้สาย

- (1) ผู้ควบคุมระบบ ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access Point) ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายน้อยที่สุด
- (2) ผู้ควบคุมระบบ ควรทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าโดยปริยาย (Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ (Access Point) มาใช้งาน
- (3) ผู้ควบคุมระบบ ต้องการเข้ารหัสข้อมูลอุปกรณ์ Wireless ให้เป็นไปตามมาตรฐานสากล
- (4) ผู้ควบคุมระบบ ต้องควบคุมผู้ให้บริการที่มีสิทธิ์ในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ตามที่กำหนดไว้เท่านั้นให้เข้าใช้ระบบเครือข่ายไร้สายได้อย่างถูกต้อง
- (5) ผู้ควบคุมระบบ ต้องติดตั้งไฟร์วอลล์ (Firewall) ระหว่างระบบเครือข่ายไร้สายกับระบบเครือข่ายภายในสหกรณ์
- (6) ผู้ควบคุมระบบ ควรกำหนดให้ผู้ให้บริการในระบบเครือข่ายไร้สายติดต่อสื่อสารได้เฉพาะกับ VPN (Virtual Private Network) เพื่อช่วยป้องกันการบุกรุกในระบบเครือข่ายไร้สาย
- (7) ผู้ควบคุมระบบ ควรใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบการรักษาความปลอดภัยของระบบเครือข่ายไร้สายเพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย และจัดส่งรายงานผลการตรวจสอบทุก 3 เดือน และในกรณีที่ตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติให้ผู้ควบคุมระบบ รายงานต่อประธานกรรมการทราบทันที
- (8) ผู้ควบคุมระบบ ต้องควบคุมดูแลไม่ให้บุคคล หรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาตใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูล ภายในต่าง ๆ ของสหกรณ์

ข้อ 19 การรักษาความปลอดภัยของไฟร์วอลล์

- (1) ผู้ควบคุมระบบมีหน้าที่ในการบริหารจัดการ การติดตั้งและกำหนดค่าของไฟร์วอลล์ทั้งหมด
- (2) การกำหนดค่าเริ่มต้นพื้นฐานของทุกเครือข่ายจะต้องเป็นการปฏิเสธทั้งหมด
- (3) ทุกเส้นทางเชื่อมต่ออินเทอร์เน็ตและบริการอินเทอร์เน็ตที่ไม่อนุญาตตามนโยบายจะต้องถูกบล็อก (Block) โดยไฟร์วอลล์
- (4) ผู้ใช้งานอินเทอร์เน็ตจะต้องมีการ Login account ก่อนการใช้งานทุกครั้ง
- (5) ค่าการเปลี่ยนแปลงทั้งหมดในไฟร์วอลล์เช่น ค่าพารามิเตอร์การกำหนดค่าใช้บริการ และการเชื่อมต่อที่อนุญาต จะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง

(6) การเข้าถึงตัวอุปกรณ์ไฟร์วอลล์จะต้องสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น

(7) ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ไฟร์วอลล์จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บ ข้อมูลจราจรทางคอมพิวเตอร์โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า 90 วัน

(8) การกำหนดนโยบายในการให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่ายจะเปิดพอร์ตการเชื่อมต่อพื้นฐานของโปรแกรมทั่วไปที่สภกรณ์จะอนุญาตให้ใช้งาน ซึ่งหากมีความจำเป็นที่จะใช้งานพอร์ตการเชื่อมต่อ นอกเหนือที่กำหนดจะต้องได้รับความยินยอมจากสภกรณ์ก่อน

(9) การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่าย จะต้อง กำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น โดยข้อนโยบาย จะต้องถูกระบุให้กับเครื่อง คอมพิวเตอร์แม่ข่ายเป็นรายชื่อเครื่องที่ให้บริการจริง

(10) จะต้องมีการสำรองข้อมูลการกำหนดค่าต่าง ๆ ของอุปกรณ์ไฟร์วอลล์เป็นประจำทุกสัปดาห์หรือทุกครั้งที่มีการเปลี่ยนแปลงค่า

(11) เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่าง ๆ จะต้องไม่อนุญาตให้มีการ เชื่อมต่อเพื่อใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็นโดยจะต้องกำหนดเป็นกรณีไป

(12) สภกรณ์มีสิทธิที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้ งานที่ผิดนโยบาย หรือเกิดจากการทำงานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัย จนกว่าจะได้รับการแก้ไข

(13) การเชื่อมต่อในลักษณะของการ Remote Login จากภายนอกมายังเครื่องแม่ข่าย หรืออุปกรณ์ เครือข่ายภายใน จะต้องบันทึกรายการของการดำเนินการตามแบบการขออนุญาตดำเนินการ เกี่ยวกับเครื่องคอมพิวเตอร์ แม่ข่ายและอุปกรณ์เครือข่าย และจะต้องได้รับความเห็นชอบจากสภกรณ์ก่อน

(14) ผู้ละเมิดนโยบายด้านความปลอดภัยของไฟร์วอลล์จะถูกะงับการใช้งานอินเทอร์เน็ตทันที

ข้อ 20 ในกรณีที่สภกรณ์จัดให้มีบริการจดหมายอิเล็กทรอนิกส์ของสภกรณ์(e-mail) การรักษาความปลอดภัยของจดหมายอิเล็กทรอนิกส์(e-mail) ต้องปฏิบัติ ดังนี้

(1) ในการลงทะเบียนบัญชีผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ (e-mail) ต้องทำการกรอกข้อมูลค่าขอเข้าใช้บริการจดหมายอิเล็กทรอนิกส์ (e-mail) ของสภกรณ์โดยยื่นคำขอกับผู้ควบคุมระบบ

(2) เมื่อได้รับรหัสผ่าน (Password) ครั้งแรกในการเข้าระบบจดหมายอิเล็กทรอนิกส์ (e-mail) และเมื่อมีการเข้าสู่ระบบในครั้งแรกนั้น ควรเปลี่ยนรหัสผ่าน (Password) โดยทันที

(3) ไม่ควรบันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์

(4) ควรเปลี่ยนรหัสผ่าน (Password) ทุก 3 - 6 เดือน

(5) ไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail address) ของผู้อื่นเพื่ออ่าน หรือรับ หรือส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ให้บริการ และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์ (e-mail) เป็นผู้รับผิดชอบต่อการใช้งานในจดหมายอิเล็กทรอนิกส์ (e-mail) ของตน

(6) หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (e-mail) เสร็จสิ้นควรลงบันทึกออก (Logout) ทุกครั้ง

(7) การส่งข้อมูลที่เป็นความลับไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์ (e-mail)

ข้อ 21 การรักษาความปลอดภัยของอินเทอร์เน็ต

(1) ไม่ใช้ระบบอินเทอร์เน็ต (Internet) ของสหกรณ์เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อการรักษาความต่อชาติ ศาสนา พระมหากษัตริย์หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิของผู้อื่นหรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับหน่วยงาน

(2) ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของสหกรณ์ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต (Internet)

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

(4) ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของสหกรณ์

(5) ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วเย้าให้ร้ายที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของสหกรณ์ การทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่น ๆ

(6) หลังจากใช้งานระบบอินเทอร์เน็ต (Internet) เสร็จแล้ว ให้ปิดเว็บเบราว์เซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ

ข้อ 22 การรักษาความปลอดภัยของการตรวจจับการบุกรุก (Intrusion Detection System / Intrusion Prevention System Policy : IDS/IPS Policy)

(1) IDS/IPS Policy เป็นนโยบายการติดตั้งระบบตรวจสอบการบุกรุก และตรวจสอบความปลอดภัยของเครือข่ายเพื่อป้องกันทรัพยากรด้านเทคโนโลยีสารสนเทศ และข้อมูลบนเครือข่ายภายในสหกรณ์ให้มีการรักษาความปลอดภัย เป็นแนวทางการปฏิบัติเกี่ยวกับการตรวจสอบการบุกรุกเครือข่ายพร้อมกับบทบาทและความรับผิดชอบที่เกี่ยวข้อง

(2) IDS/IPS Policy ครอบคลุมทุกโฮสต์ (Host) ในเครือข่ายของสหกรณ์และเครือข่ายข้อมูลทั้งหมด รวมถึงเส้นทางที่ข้อมูลอาจเดินทางซึ่งไม่อยู่ในเครือข่ายอินเทอร์เน็ตทุกเส้นทาง

- (3) ระบบทั้งหมดที่สามารถเข้าถึงได้จากอินเทอร์เน็ต หรือสาธารณะจะต้องผ่านการตรวจสอบจากระบบ IDS/IPS
- (4) ระบบทั้งหมดใน DMZ จะต้องได้รับการตรวจสอบรูปแบบการให้บริการก่อนการติดตั้งและเปิดให้บริการ
- (5) โสภต์และเครือข่ายทั้งหมดที่มีการส่งผ่านข้อมูลผ่าน IDS/IPS จะต้องมีการบันทึกผลการตรวจสอบ
- (6) มีการตรวจสอบและ Update Patch/Signature ของ IDS/IPS เป็นประจำ
- (7) มีการตรวจสอบเหตุการณ์ข้อมูลจราจร พฤติกรรมการใช้งาน กิจกรรม และบันทึกปริมาณข้อมูลเข้าใช้งานเครือข่ายเป็นประจำทุกวันโดยผู้ควบคุมระบบ
- (8) IDS/IPS จะทำงานภายใต้กฎควบคุมพื้นฐานของไฟร์วอลล์ที่ใช้ในการเข้าถึงเครือข่ายของด้านเทคโนโลยีสารสนเทศตามปกติ
- (9) เครื่องแม่ข่ายที่มีการติดตั้ง host-based IDS จะต้องมีการตรวจสอบข้อมูลประจำวัน
- (10) พฤติกรรมการใช้งาน กิจกรรม หรือเหตุการณ์ทั้งหมดที่มีความเสี่ยงต่อการบุกรุก การโจมตีระบบ พฤติกรรมที่น่าสงสัย หรือการพยายามเข้าระบบทั้งที่ประสบความสำเร็จและไม่ประสบความสำเร็จจะต้องมีการรายงานให้ผู้บริหารสหกรณ์ทราบทันทีที่ตรวจพบ
- (11) การตรวจสอบการบุกรุกทั้งหมดจะต้องเก็บบันทึกข้อมูลไว้ไม่น้อยกว่า 90 วัน

ข้อ 23 การรักษาความปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Network and Server Policy)

- (1) ผู้ควบคุมระบบกำหนดมาตรการควบคุมการเข้า – ออกห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server)
- (2) ผู้ให้บริการจะนำเครื่องคอมพิวเตอร์และอุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์และระบบเครือข่ายของสหกรณ์ต้องได้รับอนุญาตจากประธานกรรมการ และต้องปฏิบัติตามนโยบายนี้โดยเคร่งครัด
- (3) การขออนุญาตใช้งานพื้นที่ Web Server และชื่อโดเมนย่อย (Sub Domain Name) ที่สหกรณ์รับผิดชอบอยู่ จะต้องทำหนังสือขออนุญาตต่อประธานกรรมการ และจะต้องไม่ติดตั้งโปรแกรมใดๆ ที่ส่งผลกระทบต่อการทำงานของระบบและผู้ให้บริการอื่น ๆ
- (4) ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใด ๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลักโดยไม่ได้รับอนุญาตจากผู้ควบคุมระบบ
- (5) ผู้ควบคุมระบบ ต้องควบคุมการเข้าถึงระบบเครือข่ายเพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ ดังต่อไปนี้

ก. ต้องมีวิธีการจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น

ข. ต้องมีวิธีการจำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน

ค. ต้องกำหนดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่อง

คอมพิวเตอร์ไป

ยังเครื่องคอมพิวเตอร์แม่ข่าย เพื่อไม่ให้ผู้ใช้บริการสามารถใช้เส้นทางอื่น ๆ ได้

ง. ระบบเครือข่ายทั้งหมดของสหกรณ์ที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมีความสามารถในการตรวจจับ โปรแกรมประสงค์ร้าย (Malware) ด้วย

จ. ระบบเครือข่ายต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System/Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของสหกรณ์ในลักษณะที่ผิดปกติ

ฉ. การเข้าสู่ระบบเครือข่ายภายในสหกรณ์ โดยผ่านทางระบบอินเทอร์เน็ต จำเป็นต้องมีการบันทึกเข้า (Login) และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้องของผู้ใช้บริการ

ช. เลขที่อยู่ไอพี (IP Address) ภายในของระบบเครือข่ายภายในของสหกรณ์ จำเป็นต้องมีการป้องกันมิให้บุคคลภายนอกที่เชื่อมต่อสามารถมองเห็นได้

ซ. ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอกและอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

ณ. การใช้เครื่องมือต่าง ๆ เพื่อการตรวจสอบระบบเครือข่ายควรได้รับการอนุมัติจากผู้ควบคุมระบบ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

6) ผู้ควบคุมระบบ ต้องบริหารควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) และรับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่างๆ ของซอฟต์แวร์ระบบ (System Software)

(7) สหกรณ์กำหนดมาตรการควบคุมการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์ (Log) มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ตามแนวทางดังต่อไปนี้

ก. ควรจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้อง แท้จริง และระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้และข้อมูลที่ใช้ในการจัดเก็บต้องกำหนดชั้นความลับในการเข้าถึงข้อมูล และผู้ควบคุมระบบไม่ได้รับอนุญาตในการแก้ไขข้อมูลที่เก็บรักษาไว้ยกเว้นผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศของสหกรณ์ (IT Auditor) หรือบุคคลที่สหกรณ์มอบหมาย

ข. ควรกำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุกเช่น บันทึกการเข้า – ออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน Command Line และ Firewall Log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย 90 วัน นับตั้งแต่การให้บริการสิ้นสุดลง

ค. ควรตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานระบบอย่างสม่ำเสมอ

ง. ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ และจำกัดสิทธิการเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

(8) สหกรณ์กำหนดมาตรการควบคุมการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอกตามแนวทาง ดังต่อไปนี้

ก. บุคคลภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) ของสหกรณ์จะต้องขออนุญาตเป็นลายลักษณ์อักษรจากประธานกรรมการ

ข. มีการควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

ค. วิธีการใด ๆ ที่สามารถเข้าสู่ข้อมูล หรือระบบข้อมูลได้จากกระยะไกลต้องได้รับการอนุญาตจากประธานกรรมการ

ง. การเข้าสู่ระบบจากกระยะไกล ผู้ใช้งานต้องแสดงหลักฐาน ระบุเหตุผลหรือความจำเป็นในการเข้าสู่ระบบกับสหกรณ์อย่างเพียงพอ

จ. การเข้าใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจากระบบของสหกรณ์

ข้อ 24 การรักษาความปลอดภัยของการสำรองข้อมูล

(1) จัดทำสำเนาข้อมูลและซอฟต์แวร์เก็บไว้โดยจัดเรียงตามลำดับความจำเป็นของการสำรองข้อมูลด้านเทคโนโลยีสารสนเทศของสหกรณ์จากจำเป็นมากไปหาน้อย

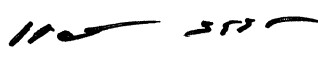
(2) มีขั้นตอนการปฏิบัติการจัดทำสำรองข้อมูลและการกู้คืนข้อมูลอย่างถูกต้องทั้งระบบซอฟต์แวร์และข้อมูลในด้านเทคโนโลยีสารสนเทศโดยขั้นตอนปฏิบัติแยกตามด้านเทคโนโลยีสารสนเทศแต่ละระบบ

(3) จัดเก็บข้อมูลที่สำคัญนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์วันที่ เวลา ที่สำคัญข้อมูลและผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน ข้อมูลที่สำคัญควรจัดเก็บไว้ในสถานที่เก็บข้อมูลสำรองซึ่งติดตั้งอยู่ที่สถานที่อื่น และต้องมีการทดสอบสื่อเก็บข้อมูลสำรองอย่างสม่ำเสมอ

(4) ต้องมีการจัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาที่เหมาะสม

ข้อ 25 ให้ประธานกรรมการเป็นผู้รักษาการตามระเบียบนี้

ประกาศ ณ วันที่ 13 มิถุนายน 2561



(ผู้ช่วยศาสตราจารย์ ดร.เมธี สรรพพานิช)

ประธานกรรมการ

สภามหาวิทยาลัยสงขลานครินทร์ จำกัด