ประกาศ สหกรณ์ออมทรัพย์กรมการพัฒนาชุมชน จำกัด
เรื่อง นโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศ

****

โดยที่ระเบียบสหกรณ์ออมทรัพย์กรมการพัฒนาชุมชน จำกัด ว่าด้วยวิธีปฏิบัติการควบคุมภายในและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของสหกรณ์ พ.ศ.2565 ข้อ 8 (1) สหกรณ์ต้องจัดทำนโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศสำหรับระบบสารสนเทศของสหกรณ์ให้เป็นลายลักษณ์อักษรและเอกสารนโยบายดังกล่าว เพื่อให้การใช้เทคโนโลยีสารสนเทศของสหกรณ์ออมทรัพย์กรมการพัฒนาชุมชน จำกัด มีความมั่นคงปลอดภัย และมีความน่าเชื่อถือ รวมทั้งเพื่อป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้เครื่องคอมพิวเตอร์ ระบบเครือข่ายคอมพิวเตอร์ และระบบสารสนเทศ

อาศัยอำนาจตามข้อบังคับสหกรณ์ออมทรัพย์กรมการพัฒนาชุมชน จำกัด พ.ศ.2565 ข้อ 81(24) และระเบียบสหกรณ์ออมทรัพย์กรมการพัฒนาชุมชน จำกัด ว่าด้วยวิธีปฏิบัติการควบคุมภายในและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของสหกรณ์ พ.ศ.2565 ข้อ 8 (1) ประกอบมติที่ประชุมคณะกรรมการดำเนินการสหกรณ์ ครั้งที่ 9/2566 เมื่อวันพุธที่ 16 สิงหาคม พ.ศ.2566 จึงได้ออกประกาศสหกรณ์ออมทรัพย์กรมการพัฒนาชุมชน จำกัด เรื่อง นโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศ ดังนี้

ข้อ 1. ประกาศนี้เรียกว่า “ประกาศ สหกรณ์ออมทรัพย์กรมการพัฒนาชุมชน จำกัด เรื่อง นโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศ ”

ข้อ 2. ประกาศนี้ให้ใช้บังคับตั้งแต่ในวันที่ประกาศ เป็นต้นไป

ข้อ 3. นโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศ มีวัตถุประสงค์ ดังต่อไปนี้

3.1 เพื่อให้เกิดความน่าเชื่อถือ เชื่อมั่น และมีความมั่นคงปลอดภัยในการใช้งานด้านสารสนเทศ ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล พร้อมใช้งานอย่างต่อเนื่อง รวมทั้งเพื่อป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้เครื่องคอมพิวเตอร์ ระบบเครือข่ายคอมพิวเตอร์ และระบบสารสนเทศ

3.2 เพื่อกำหนดแนวทางปฏิบัติ ให้คณะกรรมการดำเนินการ คณะอนุกรรมการ คณะทำงาน ผู้จัดการ เจ้าหน้าที่ ผู้ดูแลระบบ และหน่วยงานอื่นหรือบุคคลภายนอกที่เกี่ยวข้อง ที่ปฏิบัติงานให้กับสหกรณ์ฯ ตระหนักถึงความสำคัญของการรักษาความมั่นคงในการใช้งานด้านสารสนเทศและปฏิบัติตามอย่างเคร่งครัด

ข้อ 4. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กำหนดประเด็นสำคัญดังต่อไปนี้

4.1 การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

4.1.1 การเข้าถึงระบบสารสนเทศ ต้องควบคุมการเข้าถึงข้อมูลและอุปกรณ์ ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศ กำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง กำหนดสิทธิ์ เพื่อให้ผู้ใช้งานในทุกระดับได้รับรู้เข้าใจและ สามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคง ปลอดภัยของระบบสารสนเทศ

4.1.2 การบริหารจัดการการเข้าถึงของผู้ใช้งาน เพื่อควบคุมการเข้าถึงระบบสารสนเทศและป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ต้องกำหนดให้มีการลงทะเบียนผู้ใช้งาน ตรวจสอบบัญชีผู้ใช้งาน อนุมัติและกำหนดรหัสผ่านการลงทะเบียนผู้ใช้งาน เพื่อให้ผู้ใช้งานที่มีสิทธิ์เท่านั้นที่สามารถเข้าใช้ระบบสารสนเทศได้ และต้องเก็บบันทึกข้อมูลการเข้าถึงและข้อมูลจราจรทางคอมพิวเตอร์ตลอดจนบริหารจัดการสิทธิ์การเข้าถึงข้อมูลให้เหมาะสมตามระดับชั้นความลับของผู้ใช้งาน ต้องมีการทบทวนสิทธิ์การใช้งานและตรวจสอบการละเมิดความปลอดภัยเสมอ

4.1.3 การควบคุมการเข้าถึงเครือข่าย เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต ต้องกำหนดสิทธิ์ในการเข้าถึงเครือข่าย ให้ผู้ที่จะเข้าใช้งานต้องลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่านก่อนการเข้าใช้งาน ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์สำหรับใช้งานอินเทอร์เน็ตโดยผ่านระบบรักษาความปลอดภัย และมีการออกแบบระบบเครือข่ายโดยแบ่งเขต (Zone) การใช้งาน เพื่อทำให้การควบคุมและป้องกันภัยคุกคามได้อย่างเป็นระบบและมีประสิทธิภาพ

4.1.4 การควบคุมการเข้าถึงระบบปฏิบัติการ เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต ต้องกำหนดให้ผู้ที่จะเข้าใช้งานต้องลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่านก่อนการเข้าใช้งานต้องกำหนดระยะเวลาเพื่อยุติการใช้งานเมื่อว่างเว้นจากการใช้งาน และจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศ

4.1.5 การควบคุมการเข้าถึงโปรแกรมประยุกต์และแอปพลิเคชัน ต้องกำหนดสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศที่สำคัญ โปรแกรมประยุกต์หรือแอปพลิเคชันต่าง ๆ รวมถึง จดหมายอิเล็กทรอนิกส์ (E-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) และระบบงานต่าง ๆ โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่

4.2 การจัดทำระบบสำรองข้อมูล เพื่อให้ระบบสารสนเทศของหน่วยงานสามารถให้บริการได้อย่างต่อเนื่องและมีเสถียรภาพ ต้องจัดทำระบบสารสนเทศและระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน โดยคัดเลือกระบบสารสนเทศที่สำคัญ เรียงลำดับความจำเป็นมากไปน้อย พร้อมทั้งกำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ในการสำรองข้อมูล และจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ อย่างน้อยปีละหนึ่งครั้ง เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

4.3 การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยจัดให้มีการตรวจสอบจากผู้ตรวจสอบภายในของสหกรณ์ฯ หรือผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก อย่างน้อยปีละหนึ่งครั้ง เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

ข้อ 5 หน้าที่ความรับผิดชอบ

5.1 คณะกรรมการดำเนินการสหกรณ์ฯ คณะอนุกรรมการ คณะทำงาน ที่เกี่ยวข้อง

5.1.1 สนับสนุนการดำเนินงานด้านเทคโนโลยีสารสนเทศให้มีประสิทธิภาพ

5.1.2 มอบหมายให้มีผู้รับผิดชอบในการติดตามการปฏิบัติตามระเบียบปฏิบัติในการควบคุมภายใน และการรักษา ความปลอดภัยด้านเทคโนโลยีสารสนเทศของสหกรณ์ฯ

5.1.3 สื่อสารและสร้างความตระหนักกับบุคลากร ถึงการปฏิบัติตามระเบียบและแนวปฏิบัติที่สหกรณ์ฯ กำหนดขึ้นภายใต้นโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศโดยเคร่งครัด

5.1.4. ส่งเสริมให้มีการฝึกอบรมหรือให้ความรู้เกี่ยวกับระบบงานและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศแก่คณะกรรมการดำเนินการ ผู้จัดการ และเจ้าหน้าที่สหกรณ์เป็นประจำทุกปี

5.2 ผู้จัดการ รองผู้จัดการ ผู้ดูแลระบบ และเจ้าหน้าที่สหกรณ์ฯ

5.2.1 ผู้จัดการ หรือรองผู้จัดการที่ได้รับมอบหมาย มีหน้าที่ควบคุมดูแลการใช้งานระบบเทคโนโลยีสารสนเทศภายในสหกรณ์ฯ ให้เป็นไปตามวัตถุประสงค์การใช้งาน

5.2.2 ผู้ดูแลระบบมีหน้าที่ดำเนินการให้ระบบเทคโนโลยีสารสนเทศของสหกรณ์ฯ ทำงานได้อย่างมีประสิทธิภาพ มั่นคงปลอดภัยตามระเบียบปฏิบัติในการควบคุมภายใน และการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของสหกรณ์ฯ

5.2.3 เจ้าหน้าที่ทุกระดับ มีหน้าที่ปฏิบัติตามคำสั่ง ระเบียบ และแนวปฏิบัติที่สหกรณ์ฯ กำหนดขึ้นภายใต้นโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศโดยเคร่งครัด

ข้อ 6 การดำเนินการตามนโยบาย ให้มีผลตามที่กำหนดตั้งแต่วันที่ ประกาศ เรื่อง นโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศ โดยมีการประเมินอย่างน้อยปีละ 1 ครั้ง

ประกาศ ณ วันที่ 16 สิงหาคม พ.ศ. 2566

(นางสาวขนิฏฐา กาญจนรังษีนนท์)
ประธานกรรมการ
สหกรณ์ออมทรัพย์กรมการพัฒนาชุมชน จำกัด

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
สหกรณ์ออมทรัพย์กรมการพัฒนาชมชน จำกัด

แนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
สหกรณ์ออมทรัพย์กรมการพัฒนาชมชน จำกัด

ตามประกาศสหกรณ์ออมทรัพย์กรมการพัฒนาชุมชน จำกัด เรื่อง นโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศ พ.ศ.2566 กำหนดให้มีการจัดทำ**แนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ** เพื่อให้เจ้าหน้าที่ใช้งานระบบเทคโนโลยีสารสนเทศ อย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะ เกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และจากการถูกคุกคามจากภัยต่าง ๆ ซึ่งอาจก่อให้เกิดความเสียหาย

หัวข้อที่ 1
การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

วัตถุประสงค์

1. เพื่อควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลโดยคำนึงถึงการใช้งานและ ความมั่นคงปลอดภัย

2. เพื่อกำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึงการกำหนดสิทธิ์

3. เพื่อให้ผู้ใช้งานได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

แนวปฏิบัติ

<u>ส่วนที่ 1 การควบคุมการเข้าถึงสารสนเทศ (Access Control)</u>

ข้อ 1 ผู้ดูแลระบบจะอนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศที่ต้องการใช้งานได้ต่อเมื่อได้รับ อนุญาตจากผู้รับผิดชอบ/เจ้าของข้อมูล/เจ้าของระบบและธุรกรรมตามความจำเป็นต่อการใช้งานเท่านั้น

ข้อ 2 กำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งาน และ หน้าที่ความรับผิดชอบในการปฏิบัติงานของผู้ใช้งานระบบสารสนเทศรวมทั้งมีการทบทวนสิทธิ์การเข้าถึง อย่างสม่ำเสมอ โดยผู้ดูแลระบบจะเป็นผู้กำหนดสิทธิ์ตามอนุญาตนั้น ดังนี้

(1) กำหนดสิทธิ์ของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง

- อ่านอย่างเดียว
- บันทึกข้อมูล
- แก้ไข
- อนุมัติ
- ไม่มีสิทธิ์

(2) กำหนดเกณฑ์ การระงับสิทธิ์ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งานที่ได้กำหนดไว้

(3) ผู้ดูแลระบบมีหน้าที่ควบคุมดูแลการเข้าถึงระบบสารสนเทศ ดังนี้

- อนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศของสหกรณ์ฯ
- กำหนดสิทธิ์ผู้ใช้งานให้เหมาะสมกับการใช้งาน และทบทวนสิทธิ์การเข้าถึงนั้นอย่างสม่ำเสมอ
- ติดตั้งระบบการบันทึกติดตามการใช้งานและตรวจตราการละเมิด ความปลอดภัยที่มีต่อระบบสารสนเทศของสหกรณ์ฯ

ข้อ 3 จัดแบ่งประเภทของข้อมูล การจัดลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล ระดับชั้นการเข้าถึง และช่องทางการเข้าถึงข้อมูล โดยกำหนดไว้ดังนี้

(1) จัดแบ่งระดับการเข้าถึง

- ระดับผู้ดูแลระบบ
- ระดับผู้จัดการ
- ระดับรองผู้จัดการ
- ระดับหัวหน้าฝ่าย
- ระดับเจ้าหน้าที่

(2) จัดแบ่งประเภทข้อมูล

- ข้อมูลสารสนเทศด้านการบริหาร เป็นข้อมูลสมาชิก ข้อมูลหุ้นและหนี้ ข้อมูลด้านการเงิน ข้อมูลด้านการบัญชี ข้อมูลบุคลากร ข้อมูลสวัสดิการ ข้อมูลคำรับรอง ข้อมูลด้านการลงทุน ข้อมูลวัสดุครุภัณฑ์ ข้อมูลข่าวสารทั่วไป

ข้อ 4 ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน ดังนี้

(1) กำหนดบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อใช้ในการพิสูจน์ ตัวตนของผู้ใช้งานข้อมูลในแต่ละชั้นความลับ

(2) การกำหนดให้เปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนด

(3) กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำสินทรัพย์ของ หน่วยงานออกนอกสำนักงานสหกรณ์ฯ บำรุงรักษาตรวจซ่อมให้ดำเนินการสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน

ข้อ 5 การกำหนดระบบและอุปกรณ์สนับสนุนการปฏิบัติงาน ดังนี้

(1) มีระบบสนับสนุนการทำงานของระบบสารสนเทศของหน่วยงานที่เพียงพอต่อความต้องการใช้งาน ดังนี้ระบบรักษาความปลอดภัย (Security) ระบบสำรองกระแสไฟฟ้า (UPS)

(2) ตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่าทำงานได้ปกติและลดความเสี่ยงจากความล้มเหลวในการทำงาน

(3) จัดวางอุปกรณ์ในพื้นที่หรือบริเวณที่เหมาะสมเพื่อหลีกเลี่ยงการเข้าถึงจากบุคคลภายนอก และให้แยกอุปกรณ์ที่มีความสำคัญเก็บไว้อีกพื้นที่หนึ่งที่มีความมั่นคงปลอดภัยเพียงพอ

(4) การเดินสายไฟสายสัญญาณเครือข่ายของหน่วยงานและสายเคเบิลอื่นที่จำเป็นต้องทำการวางผ่านเข้าไปในบริเวณที่บุคคลภายนอกเข้าถึงได้นั้นให้ร้อยท่อสายสัญญาณต่าง ๆ เพื่อป้องกัน หนูนกกระรอก แมลงสาบ หรือสัตว์อื่นกัดสายไฟ ป้องกันการดักจับ สัญญาณ การตัดสายสัญญาณ อันจะทำให้เกิดความเสียหายต่อระบบเครือข่ายใช้งานไม่ได้

(5) ต้องจัดทำแผนผังสายสัญญาณสื่อสารต่าง ๆ ให้ครบถ้วนถูกต้อง โดยสายสัญญาณ สื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณ ซึ่งกันและกัน แล้วให้จัดเก็บสายสัญญาณต่าง ๆ ไว้ในตู้ Rack และปิดใส่สลักกุญแจให้สนิท เพื่อป้องกันการเข้าถึงจากบุคคลภายนอกหรือผู้ที่ไม่มีส่วนเกี่ยวข้อง

<u>ส่วนที่ 2 การบริหารจัดการการเข้าถึงของผู้ใช้งาน(User Access Management)</u>

ข้อ 1 กำหนดให้มีการลงทะเบียนเจ้าหน้าที่หรือผู้ใช้งานใหม่ (User Registration) เพื่อรับการเข้าถึงระบบเทคโนโลยีสารสนเทศและระบบสารสนเทศตามตำแหน่งงาน หรือหน้าที่ที่ได้รับมอบหมาย

ข้อ 2 กำหนดให้มีการบริหารจัดการสิทธิ์ของผู้ใช้งาน (User Management) อย่างรัดกุมโดยมีการควบคุมจำกัด และเปลี่ยนแปลงสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศ และระบบสารสนเทศ ตามตำแหน่งงาน หรือหน้าที่ที่ได้รับมอบหมาย รวมถึงทบทวนสิทธิ์ของผู้ใช้งาน และปรับปรุงบัญชีของผู้ใช้งาน อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงตำแหน่งงาน โยกย้าย ลาออก หรือสิ้นสุดการจ้าง

ข้อ 3 กำหนดกระบวนการสำหรับยกเลิกสิทธิ์การใช้งานเมื่อมีการเปลี่ยนแปลงตำแหน่งงาน โยกย้าย ลาออก หรือสิ้นสุดการจ้าง

ข้อ 4 กำหนดให้มีการบริหารจัดการรหัสผ่าน (User Password Management) อย่างรัดกุม ดังนี้

(1) กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

(2) กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

(3) กำหนดให้ผู้ใช้งานต้องมีการทบทวนความเหมาะสมของสิทธิ์ในการเข้าถึงข้อมูลของ ผู้ใช้งานอย่างน้อย 180 วัน

(4) หากมีการกระทำความผิดเกิดขึ้นจากชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของบุคคลใดบุคคลนั้น ต้องเป็นผู้รับผิดชอบต่อการกระทำความผิดนั้น

ข้อ 5 ระบบงานสารสนเทศทางธุรกิจที่เชื่อมโยงกันให้ผู้จัดการพิจารณาประเด็นต่างๆทางด้านความมั่นคงปลอดภัย และจุดอ่อนต่าง ๆ ก่อนตัดสินใจ ใช้ข้อมูลร่วมกันในระบบงาน หรือระบบเทคโนโลยีสารสนเทศที่จะเชื่อมโยงเข้าด้วยกัน เช่น ระหว่างสหกรณ์ฯ หรือหน่วยงานอื่นที่มาขอเชื่อมโยง

(1) พิจารณาจำกัดหรือไม่อนุญาตการเข้าถึงข้อมูลส่วนบุคคล

(2) พิจารณาว่ามีบุคลากรใดบ้างที่มีสิทธิ์หรือได้รับอนุญาตให้เข้าใช้งาน

(3) ไม่อนุญาตให้มีการใช้งานข้อมูลสำคัญหรือข้อมูลลับร่วมกันในกรณีที่ระบบไม่มี มาตรการป้องกันเพียงพอ

ส่วนที่ 3 การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

ข้อ 1 การใช้งานรหัสผ่าน ผู้ใช้งานต้องปฏิบัติ ดังนี้

(1) ผู้ใช้งานมีหน้าที่ในการป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และ รหัสผ่าน (Password) โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งาน (Username) ของ ตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่ แจกจ่าย ทำให้ผู้อื่นล่วงรู้ รหัสผ่าน (Password)

(2) หลีกเลี่ยงการตั้งรหัสผ่านที่อยู่บนพื้นฐานที่สามารถเดาได้ง่าย เช่น ชื่อหรือนามสกุลของตนเอง

(3) ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ(Save Password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่ผู้ใช้งานครอบครองอยู่

(4) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

(5) ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) ไม่เกิน 180 วันหรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน

ข้อ 2 การกระทำใด ๆ ที่เกิดจากการใช้บัญชีของผู้ใช้งาน (Username) อันมีกฎหมายกำหนดให้ เป็นความผิด ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม ให้ถือว่าเป็นความรับผิดชอบส่วนบุคคล ซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

ข้อ 3 ห้ามใช้สินทรัพย์ของหน่วยงาน เพื่อการรบกวน ก่อให้เกิดความเสียหาย หรือใช้ในการ โจรกรรมข้อมูล หรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรม หรือกระทบต่อภารกิจของสหกรณ์ฯ

ข้อ 4 ห้ามกระทำการใด ๆ เพื่อการดักข้อมูล ไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใด ในเครือข่ายระบบสารสนเทศของสหกรณ์ฯ โดยเด็ดขาด ไม่ว่าจะด้วยวิธีการใด ๆ ก็ตาม

ข้อ 5 ห้ามกระทำการรบกวน ทำลาย หรือทำให้ระบบสารสนเทศของหน่วยงานต้องหยุดชะงัก

ข้อ 6 ห้ามกระทำการใด ๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลของผู้อื่น ไม่ว่าจะเป็นกรณีใด ๆ เพื่อประโยชน์ในการเข้าถึงข้อมูล หรือเพื่อการใช้ทรัพยากรก็ตาม

ส่วนที่ 4 การบริหารจัดการสินทรัพย์ (Assets Management)

ข้อ 1 ผู้ใช้งานต้องไม่เข้าไปในศูนย์คอมพิวเตอร์ หมายถึง พื้นที่ที่ใช้จัดวางเครื่องคอมพิวเตอร์แม่ข่าย ระบบจัดเก็บข้อมูลภายนอก ระบบเครือข่ายคอมพิวเตอร์และอุปกรณ์สื่อสารต่าง ๆ ของสหกรณ์ไว้เป็นศูนย์กลางในการประมวลผลข้อมูลสารสนเทศสำหรับใช้ปฏิบัติงานของสหกรณ์ฯ ที่เป็นเขตหวงห้าม โดยเด็ดขาด เว้นแต่ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ 2 ผู้ใช้งานต้องไม่นำอุปกรณ์หรือชิ้นส่วนใดออกจากห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ เว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ 3 กรณีทำงานนอกสถานที่ผู้ใช้งานต้องดูแลและรับผิดชอบสินทรัพย์ของหน่วยงานที่ได้รับ มอบหมาย

<u>ส่วนที่ 5 การควบคุมการเข้าถึงเครือข่าย (Network Access Control)</u>

ข้อ 1 ผู้ใช้งานจะนำเครื่องคอมพิวเตอร์ อุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์ ระบบ เครือข่ายของหน่วยงาน ต้องได้รับอนุญาตจากผู้ดูและระบบ

ข้อ 2 ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใด ๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลัก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ 3 ผู้ดูแลระบบ ต้องควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการระบบเครือข่าย ได้อย่างมีประสิทธิภาพ ดังต่อไปนี้

(1) ต้องจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะระบบเครือข่าย ที่ได้รับอนุญาตเท่านั้น

(2) ต้องจำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน

(3) ต้องจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่าย เพื่อไม่ให้ผู้ใช้งานสามารถใช้เส้นทางอื่น ๆ ได้

(4) จัดให้มีระบบป้องกันเครือข่ายคอมพิวเตอร์ (Firewall) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งาน ระบบเครือข่ายของหน่วยงานในลักษณะที่ผิดปกติ

(5) การเข้าสู่ระบบเครือข่ายภายในหน่วยงาน โดยผ่านทางระบบอินเทอร์เน็ตจำเป็นต้องมี การลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน เพื่อตรวจสอบความถูกต้องของ ผู้ใช้งานก่อนทุกครั้ง

(6) ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับ ขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

(7) กำหนดระยะเวลาผู้ใช้งานที่อยู่ในระบบเครือข่ายให้ออกจากระบบเครือข่าย เมื่อเว้นว่างจากการใช้งานเป็นเวลานาน

ข้อ 4 ผู้ดูแลระบบ ต้องบริหารควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) และรับผิดชอบในการ ดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่าง ๆ ของซอฟต์แวร์ระบบ (Systems Software)

ข้อ 5 การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบงานต้องมีการขออนุมัติจากผู้ดูแลระบบให้ ติดตั้งก่อนดำเนินการ

ข้อ 6 การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์ มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้

ส่วนที่ 6 การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

ข้อ 1 กำหนดขั้นตอนการปฏิบัติเพื่อเข้าใช้งาน

(1) ผู้ใช้งานต้องกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ

(2) ผู้ใช้งานต้องตั้งค่า ล็อกหน้าจอภาพเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งาน ผู้ใช้งานต้องใส่ รหัสผ่าน (Password) เพื่อเข้าใช้งาน

(3) ห้ามเปิดหรือใช้งานโปรแกรมที่มีความเสี่ยง เว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบ

(4) ซอฟต์แวร์ที่สหกรณ์ฯ ใช้มีลิขสิทธิ์ผู้ใช้งานสามารถขอใช้งานได้ตาม หน้าที่ความจำเป็น และห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใด ที่ไม่มีลิขสิทธิ์หากตรวจพบ ถือว่าเป็นความผิดส่วนบุคคลผู้ใช้งานรับผิดชอบแต่เพียง ผู้เดียว

(5) ซอฟต์แวร์ที่สหกรณ์ฯ จัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็น ห้ามมิให้ ผู้ใช้งานทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนา เพื่อนำไปใช้งาน ที่อื่น

(6) ห้ามผู้ใช้งานนำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์แสดงข้อความรูปภาพ ไม่เหมาะสม หรือขัดต่อศีลธรรม

ส่วนที่ 7 การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control)

ข้อ 1 ผู้ดูแลระบบ ต้องกำหนดสิทธิ์การใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์ โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์(E-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากผู้ดูแลระบบ รวมทั้งต้องทบทวนสิทธิ์ดังกล่าว อย่างสม่ำเสมอ

ข้อ 2 ผู้ดูแลระบบ ต้องบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่านของบุคลากรดังต่อไปนี้

(1) กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบ ลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

(2) กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

(3) กำหนดชื่อผู้ใช้งานหรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

ข้อ 3 ผู้ดูแลระบบ ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุม การเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลาย ข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

(1) ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและ การเข้าถึงผ่านระบบงาน

(2) ต้องกำหนดรายชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อใช้ในการ ตรวจสอบตัวตนจริงของผู้ใช้งานข้อมูล ในแต่ละชั้นความลับของข้อมูล

(3) กำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของระดับ ความสำคัญของข้อมูล

(4) ต้องสำรองข้อมูลและระบบ และทดสอบการกู้คืนข้อมูลและระบบอย่างสม่ำเสมอ โดยกำหนดความถี่ในการดำเนินงานอย่างชัดเจนในแต่ละระบบ

ข้อ 4 การใช้งานอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องปฏิบัติดังต่อไปนี้

(1) ตรวจสอบความพร้อมของคอมพิวเตอร์ และอุปกรณ์ที่จะนำไปใช้งานว่าอยู่ในสภาพ พร้อมใช้งานหรือไม่ และตรวจสอบโปรแกรมมาตรฐานว่าถูกต้องตามลิขสิทธิ์

(2) ระมัดระวังไม่ให้บุคคลภายนอกคัดลอกข้อมูลจากคอมพิวเตอร์ที่นำไปใช้ได้ เว้นแต่ ข้อมูลที่ได้มีการเผยแพร่เป็นการทั่วไป

(3) เมื่อหมดความจำเป็นต้องใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่แล้ว ให้รีบนำ ส่งคืนเจ้าหน้าที่ที่รับผิดชอบทันที

(4) เจ้าหน้าที่ผู้รับผิดชอบในการรับคืนต้องตรวจสอบสภาพความพร้อมใช้งานของ อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ที่รับคืนด้วย

(5) หากปรากฏว่าความเสียหายที่เกิดขึ้นนั้นเกิดจากความประมาทอย่างร้ายแรงของ ผู้นำไปใช้ ผู้นำไปใช้ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

ส่วนที่ 8 การบริหารจัดการซอฟต์แวร์และลิขสิทธิ์และการป้องกันโปรแกรมไม่ประสงค์ดี (Software Licensing and intellectual property and Preventing Malware)

ข้อ 1 สหกรณ์ฯ ได้ให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญา ดังนั้นซอฟต์แวร์ ที่หน่วยงานอนุญาตให้ใช้งานหรือที่หน่วยงานมีลิขสิทธิ์ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์หากมีการตรวจสอบพบความผิด ฐานละเมิดลิขสิทธิ์ถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงผู้เดียว

ข้อ 2 ซอฟต์แวร์ (Software) ที่หน่วยงานได้จัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็นต่อการทำงาน ห้ามมิให้ผู้ใช้งานทำการ ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น ๆ ยกเว้นได้รับการอนุญาตจากผู้ดูแลระบบ

ข้อ 3 คอมพิวเตอร์ของผู้ใช้งานติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Antivirus) ตามที่ สหกรณ์ฯ กำหนด

ข้อ 4 บรรดาข้อมูล ไฟล์ ซอฟต์แวร์ หรือสิ่งอื่นใด ที่ได้รับจากผู้ใช้งานอื่นต้องได้รับการตรวจสอบ ไวรัสคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดีก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง

ข้อ 5 ผู้ใช้งานต้องทำการปรับปรุงข้อมูล สำหรับตรวจสอบและปรับปรุงระบบปฏิบัติการ (Update Patch) ให้ใหม่เสมอ เพื่อเป็นการป้องกันความเสียหายที่อาจเกิดขึ้น

ข้อ 6 ผู้ใช้งานต้องพึงระวังไวรัสและโปรแกรมไม่ประสงค์ดีตลอดเวลา รวมทั้งเมื่อพบสิ่งผิดปกติ ผู้ใช้งานต้องแจ้งเหตุแก่ผู้ดูแลระบบ

ข้อ 7 เมื่อผู้ใช้งานพบว่าเครื่องคอมพิวเตอร์ติดไวรัส ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์ เข้าสู่เครือข่ายและต้องแจ้งแก่ผู้ดูแลระบบ

ข้อ 8 ห้ามทำการเผยแพร่ไวรัสคอมพิวเตอร์ มัลแวร์ หรือโปรแกรมอันตรายใด ๆ ที่อาจก่อให้เกิดความเสียหายมาสู่สินทรัพย์ของสหกรณ์ฯ

ข้อ 9 การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก (Outsourced Software Development)

(1) จัดให้มีการควบคุมโครงการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

(2) พิจารณาระบุว่าใครจะเป็นผู้มีสิทธิ์ในทรัพย์สินทางปัญญาสำหรับซอร์สโค้ดในการ พัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

(3) พิจารณากำหนดเรื่องการสงวนสิทธิ์ที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้ให้บริการภายนอก โดยระบุไว้ในสัญญาจ้าง ที่ทำกับผู้ให้บริการภายนอกนั้น

(4) ให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดี ในซอฟต์แวร์ต่าง ๆ ที่จะทำการติดตั้ง ก่อนดำเนินการติดตั้ง

(5) ผู้พัฒนาระบบจากภายนอก (Outsource) ต้องถือปฏิบัติตามแนวนโยบาย และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ส่วนที่ 9 การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

ข้อ 1 ผู้ดูแลระบบ ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายน้อยที่สุด

ข้อ 2 ผู้ดูแลระบบ ต้องกำหนดค่า Wireless Security เป็นแบบ WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) หรือ ที่ดีกว่า ในการเข้ารหัสข้อมูลระหว่างเครื่องลูกข่าย (Wireless LAN Client) และอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) และกำหนดค่าโดยไม่ให้ แสดงชื่อระบบเครือข่ายไร้สาย

ข้อ 3 ผู้ดูแลระบบ ต้องมีการติดตั้งไฟร์วอลล์ (Firewall) ระหว่างระบบเครือข่ายไร้สายกับระบบ เครือข่ายภายในหน่วยงาน

ข้อ 4 ผู้ดูแลระบบ ควรกำหนดให้ผู้ใช้งานในระบบเครือข่ายไร้สายติดต่อสื่อสารกับเครือข่าย ภายในหน่วยงานผ่านทาง VPN (Virtual Private Network) เพื่อช่วยป้องกันการบุกรุกในระบบเครือข่าย ไร้สาย

ข้อ 5 ผู้ดูแลระบบ ต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบ เครือข่ายไร้สายเพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย

ข้อ 6 ผู้ดูแลระบบ ต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาต ใช้งาน ระบบเครือข่ายไร้สายในการเข้าสู่ระบบเครือข่ายและระบบสารสนเทศภายในหน่วยงาน

ส่วนที่ 10 การควบคุมการใช้งานอุปกรณ์ป้องกันเครือข่าย (Firewall Control)

ข้อ 1 ทุกบริการ (Services) และเส้นทางเชื่อมต่ออินเทอร์เน็ตที่ไม่อนุญาตตาม Policy จะต้อง ถูกบล็อก (Block) โดย Firewall

ข้อ 2 การกำหนดค่าบริการและการเชื่อมต่อที่อนุญาต จะต้องมีการบันทึกการเปลี่ยนแปลง ทุกครั้ง หากมีการเปลี่ยนแปลงค่าต่าง ๆ ของ Firewall

ข้อ 3 การเข้าถึงตัวอุปกรณ์ Firewall จะต้องสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับมอบหมายให้ดูแล จัดการเท่านั้น

ข้อ 4 ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์Firewall จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์ จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า 90 วัน

ข้อ 5 การกำหนดนโยบายในการให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่ายจะ เปิดพอร์ตการเชื่อมต่อพื้นฐานของโปรแกรมทั่วไป ที่อนุญาตให้ใช้งาน ซึ่งหากมีความจำเป็นที่จะใช้งานพอร์ต การเชื่อมต่อนอกเหนือที่กำหนด จะต้องได้รับความยินยอมจากผู้ดูแลระบบก่อน

ข้อ 6 การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่าย จะต้องกำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น โดยข้อนโยบายจะต้องถูกระบุ ให้กับเครื่องคอมพิวเตอร์แม่ข่ายเป็นรายเครื่องที่ให้บริการจริง และการกำหนดค่าการให้บริการของ เครื่องคอมพิวเตอร์แม่ข่ายหรืออุปกรณ์ในเครือข่าย ต้องขออนุญาตจากผู้ดูแลระบบ โดยต้องระบุข้อมูล ดังนี้

(1) หมายเลข Port ที่ต้องการขอให้เปิด

(2) หมายเลข IP Address ของปลายทางที่ต้องการติดต่อสื่อสาร

(3) วัตถุประสงค์ หรือชื่อแอปพลิเคชันที่ต้องการใช้งานผ่าน Port นั้น ๆ

ข้อ 7 เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่าง ๆ ภายในหน่วยงานที่มี ลักษณะที่เป็นอินทราเน็ตจะต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็น โดยจะต้องกำหนดเป็นกรณีไป

ข้อ 8 สหกรณ์ฯ มีสิทธิ์ที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มี พฤติกรรมการใช้งานที่ผิดหรือเสี่ยงต่อความปลอดภัยของระบบเครือข่ายส่วนรวม หรือเกิดจากการทำงานของ โปรแกรมที่มีความเสี่ยงต่อความปลอดภัยจนกว่าจะได้รับการแก้ไข

ข้อ 9 การเชื่อมต่อในลักษณะของการควบคุมระยะไกล (Remote Login) จากภายนอกมายัง เครื่องแม่ข่ายหรืออุปกรณ์เครือข่ายภายในต้องได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ 10 ผู้ละเมิดนโยบายด้านความปลอดภัยของ Firewall จะถูกระงับการให้บริการทันทีจนกว่าจะได้รับการแก้ไข

ข้อ 11 ต้องตรวจสอบและปิดพอร์ตของระบบหรืออุปกรณ์ที่ไม่มีความจำเป็นในการเข้าใช้งาน อย่างสม่ำเสมออย่างน้อยสัปดาห์ละ 1 ครั้ง

ส่วนที่ 11 การควบคุมการใช้อินเทอร์เน็ต (Internet)

ข้อ 1 ผู้ดูแลระบบ ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งาน อินเทอร์เน็ต ที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่หน่วยงานจัดสรรไว้เท่านั้น

ข้อ 2 เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา ก่อนทำการเชื่อมต่อ อินเทอร์เน็ต ผ่านเว็บเบราว์เซอร์ (Web Browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดช่องโหว่ของระบบปฏิบัติการ

ข้อ 3 ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ตจะต้องมีการตรวจจับไวรัส (Virus Scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง

ข้อ 4 ห้ามใช้เครือข่ายอินเทอร์เน็ตของสหกรณ์ฯ เพื่อกระทำการต่อไปนี้

(1) หาประโยชน์ในเชิงธุรกิจส่วนตัว

(2) เพื่อความบันเทิง ได้แก่ การเล่นเกม ดูภาพยนตร์ฟังเพลง

(3) กระทำการที่ก่อให้เกิดความเสียหายต่อภาพลักษณ์ และชื่อเสียงของสหกรณ์ฯ เช่น การเผยแพร่ข้อมูลที่อาจก่อความเสียหายต่อสหกรณ์ฯ หรือข้อมูลสำคัญที่เป็น ความลับของสหกรณ์ฯ

ข้อ 5 กระทำผิดกฎหมาย เช่น

(1) นำเข้าหรือเผยแพร่ ข้อมูลหรือชุดโปรแกรมที่ละเมิดลิขสิทธิ์

(2) แพร่กระจายโปรแกรมไม่ประสงค์ดี (Malware) เช่น ไวรัสคอมพิวเตอร

(3) กระทำการที่ไม่เหมาะสมขัดต่อศีลธรรม เช่น การเล่นพนันออนไลน์ การนำเข้า หรือเผยแพร่สื่อลามก อนาจาร

(4) กระทำการที่ส่งผลร้าย กระทบกับความมั่นคงของชาติ ศาสนา พระมหากษัตริย์ เช่น การก่อการร้าย

(5) กระทำการข่มขู่ คุกคาม หรือละเมิดสิทธิ์ของผู้อื่นให้ได้รับความเสียหาย เช่น การนำเข้าหรือเผยแพร่ภาพ เสียง สื่อผสมภาพและเสียง (Multimedia) ของผู้อื่น ทั้งที่เป็นข้อมูลจริง หรือข้อมูลเท็จอันเกิดจากการสร้าง ตัดต่อ แต่งเติม หรือ ดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ที่ทำให้ผู้อื่นนั้นเสีย ชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

(6) กระทำการเป็นภัยต่อสังคม เช่น การนำเข้าหรือเผยแพร่ ข้อมูลที่มีลักษณะ อันเป็นเท็จเพื่อสร้างความสับสนวุ่นวาย หรือเพื่อการหลอกลวงให้เกิด ความเสียหายต่าง ๆ

ข้อ 6 ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงานที่ยังไม่ได้ประกาศ อย่างเป็นทางการผ่านระบบอินเทอร์เน็ต (Internet)

ข้อ 7 ระมัดระวังการดาวน์โหลด โปรแกรมใช้งานจากระบบอินเทอร์เน็ต (Internet) การอัปเดต (Update) โปรแกรมต่าง ๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์

ส่วนที่ 12 การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล

ข้อ 1 แนวทางปฏิบัติการใช้งานทั่วไป

(1) เครื่องคอมพิวเตอร์ที่หน่วยงานอนุญาตให้ใช้งาน เป็นสินทรัพย์ของสหกรณ์ฯ เพื่อใช้ ในงานสหกรณ์ฯ

(2) โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของสหกรณ์ฯ ต้องเป็นโปรแกรม ที่หน่วยงานได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอก โปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือ นำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

(3) ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคลของสหกรณ์ฯ

(4) ผู้ใช้งาน มีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์

(5) ปิดเครื่องคอมพิวเตอร์ส่วนบุคคลที่ตนเองครอบครองใช้งานอยู่ เมื่อใช้งาน ประจำวันเสร็จสิ้น

ข้อ 2 การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

(1) ผู้ใช้งานต้องตรวจสอบหาไวรัสจากสื่อต่าง ๆ เช่น Floppy Disk, Flash Drive และ Data Storage อื่น ๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

(2) ผู้ใช้งานต้องตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลด มาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัส ก่อนใช้งาน

(3) ผู้ใช้งานต้องตรวจสอบข้อมูลคอมพิวเตอร์ใดที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

ข้อ 3 การสำรองข้อมูลและการกู้คืน

(1) ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่น ๆ เช่น CD, DVD, External Hard Disk เป็นต้น

(2) ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้ อย่างสม่ำเสมอ

(3) ผู้ใช้งานต้องประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ไม่ควรจะเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน เพราะหาก Hard Disk เสียไป ก็ไม่กระทบต่อ การดำเนินการของหน่วยงาน

ส่วนที่ 13 การใช้งานเครื่องคอมพิวเตอร์แบบพกพา

ข้อ 1 แนวทางปฏิบัติการใช้งานทั่วไป

(1) เครื่องคอมพิวเตอร์แบบพกพาที่สหกรณ์ฯ อนุญาตให้ใช้งาน เป็นสินทรัพย์ของ สหกรณ์ฯ เพื่อใช้ในงานสหกรณ์ฯ

(2) โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์แบบพกพาของสหกรณ์ฯ ต้องเป็น โปรแกรมที่สหกรณ์ฯ ได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งาน คัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

(3) ไม่ดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของคอมพิวเตอร์และรักษาสภาพของ คอมพิวเตอร์ให้มีสภาพเดิม

(4) ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ควรใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงาน หรือหลุดมือเป็นต้น

(5) หลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่น ปลายปากกา กดสัมผัสหน้าจอ LCD ให้เป็น รอยขีดข่วนหรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้

(6) ไม่วางของทับบนหน้าจอและแป้นพิมพ์

(7) การเช็ดทำความสะอาดหน้าจอภาพต้องเช็ดอย่างเบามือที่สุด และต้องเช็ดไปใน แนวทางเดียวกันห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วนได้

ข้อ 2 ความปลอดภัยทางด้านกายภาพ

(1) ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรล็อกเครื่องขณะที่ ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อ การสูญหาย

(2) ผู้ใช้งานไม่เก็บหรือใช้งานคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อน/ความชื้น/ฝุ่นละอองสูง และต้องระวังป้องกันการตกกระทบ

ข้อ 3 การควบคุมการเข้าถึงระบบปฏิบัติการ

(1) ผู้ใช้งานต้องกำหนดชื่อผู้ใช้งาน (User name) และรหัสผ่าน (Password) ในการ เข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์แบบพกพา

(2) ผู้ใช้งานต้องกำหนดรหัสผ่านให้มีคุณภาพดีอย่างน้อยตามที่ระบุไว้ในเอกสาร “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน”

(3) ผู้ใช้งานต้องทำการ Logout ออกจากระบบทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอ เป็นเวลานาน

ข้อ 4 การสำรองข้อมูลและการกู้คืน

(1) ผู้ใช้งานต้องทำการสำรองข้อมูลจากเครื่องคอมพิวเตอร์แบบพกพา โดยวิธีการและ สื่อต่าง ๆ เพื่อป้องกันการสูญหายของข้อมูล

(2) ผู้ใช้งานต้องจะเก็บรักษาสื่อสำรองข้อมูล (Backup Media) ไว้ในสถานที่ ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล

(3) ผู้ใช้งานต้องประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ไม่ควรจะเป็น ข้อมูลสำคัญเกี่ยวข้องกับการทำงาน เพราะหาก Hard Disk เสียไป ก็ไม่กระทบ ต่อการดำเนินการของสหกรณ์ฯ

ส่วนที่ 14 การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log)

ข้อ 1 จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษา ความครบถ้วน ถูกต้อง แท้จริง ระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ และข้อมูลที่ใช้ในการจัดเก็บต้องกำหนด ชั้นความลับในการเข้าถึง

ข้อ 2 ห้ามแก้ไขข้อมูลจราจรคอมพิวเตอร์ (Log) ที่เก็บรักษาไว้

ข้อ 3 ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ และจำกัดสิทธิ์การเข้าถึงบันทึก เหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

หัวข้อที่ 2
การจัดทำระบบสำรองข้อมูล

วัตถุประสงค์

1. เพื่อให้ระบบสารสนเทศของสหกรณ์ฯ สามารถให้บริการได้อย่างต่อเนื่อง

2. เพื่อให้เป็นมาตรฐาน แนวทางปฏิบัติและความรับผิดชอบของผู้ดูแลระบบในการปฏิบัติงานให้กับสหกรณ์ฯ อย่างเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

3. เพื่อให้ผู้ใช้งานได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

<u>แนวปฏิบัติการสำรองข้อมูล</u>

ข้อ 1 ต้องพิจารณาคัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ ในสภาพพร้อมใช้งาน โดยเรียงลำดับความจำเป็นมากไปน้อย

ข้อ 2 ต้องกำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ในการสำรองข้อมูล

ข้อ 3 ต้องจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของสหกรณ์ พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง และจัดทำระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ 1 ครั้ง

ข้อ 4 ต้องกำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ และกำหนดความถี่ในการสำรองข้อมูล หากระบบใดที่มีการเปลี่ยนแปลงบ่อยกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น โดยให้มี วิธีการสำรองข้อมูล ดังนี้

(1) กำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้ และความถี่ในการสำรอง

(2) กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรองข้อมูล

(3) จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้น ให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูล และผู้รับผิดชอบในการ สำรองข้อมูลไว้อย่างชัดเจน

(4) จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับหน่วยงานต้องห่างกันเพียงพอ เพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้ นอกสถานที่นั้น ในกรณีที่เกิดภัยพิบัติกับสหกรณ์ฯ

(5) ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูล นอกสถานที่

(6) จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้

(7) ตรวจสอบและทดสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง หรือตามความเหมาะสมโดยคำนึงถึง ความเสี่ยงต่างๆ ที่จะเกิดขึ้น

ข้อ 5 มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ 1 ครั้ง

หัวข้อที่ 3
การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

วัตถุประสงค์

1. เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศหรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดได้

2. เพื่อเป็นการป้องกันและลดระดับความเสี่ยงที่อาจจะเกิดขึ้นได้กับระบบสารสนเทศ

3. เพื่อเป็นแนวทางในการปฏิบัติหากเกิดความเสี่ยงที่เป็นอันตรายต่อระบบสารสนเทศ

แนวปฏิบัติ

<u>ส่วนที่ 1 การตรวจสอบและประเมินความเสี่ยง</u>

ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศหรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิดได้ ที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ โดยผู้ตรวจสอบภายในของหน่วยงาน (Internal Auditor) อย่างน้อยปีละ 1 ครั้ง เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคง ปลอดภัยสารสนเทศ โดยมีแนวทางในตรวจสอบและประเมินความเสี่ยงที่ต้องคำนึงถึง ดังนี้

ข้อ 1 จัดลำดับความสำคัญของความเสี่ยง

ข้อ 2 ค้นหาวิธีการดำเนินการเพื่อลดความเสี่ยง

ข้อ 3 ศึกษาข้อดีข้อเสียของวิธีการดำเนินการเพื่อลดความเสี่ยง

ข้อ 4 สรุปผลข้อเสนอแนะและแนวทางแก้ไขเพื่อลดความเสี่ยงที่ตรวจสอบได้

ข้อ 5 มีการตรวจสอบและประเมินความเสี่ยงและให้จัดทำรายงานพร้อมข้อเสนอแนะ

ข้อ 6 มีมาตรการในการตรวจประเมินระบบสารสนเทศ อย่างน้อย ดังนี้

(1) กำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านได้ อย่างเดียว

(2) ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่น ๆ ให้สร้างสำเนาสำหรับข้อมูลนั้น เพื่อให้ผู้ตรวจสอบใช้งาน รวมทั้งต้องทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือต้อง จัดเก็บไว้โดยมีการป้องกันเป็นอย่างดี

(3) กำหนดให้มีการระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย

(4) กำหนดให้มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้งบันทึก Log แสดง การเข้าถึงนั้น ซึ่งรวมถึงวันและเวลาที่เข้าถึงระบบงานที่สำคัญ ๆ

ส่วนที่ 2 ความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ

จากการติดตามตรวจสอบความเสี่ยงต่าง ๆ รวมถึงเหตุการณ์ด้านความมั่นคงปลอดภัยในระบบ เทคโนโลยีสารสนเทศ สามารถแยกเป็นภัยต่าง ๆ ได้ 4 ประเภท ดังนี้

ประเภทที่ 1 ภัยที่เกิดจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน (Human Error) เช่น เจ้าหน้าที่ หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในเครื่องมืออุปกรณ์คอมพิวเตอร์ ทั้งด้าน Hardware และ Software ซึ่งอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย ใช้งานไม่ได้ เกิดการชะงักงัน หรือหยุดทำงาน และส่งผลให้ไม่สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้อย่างเต็มประสิทธิภาพ ได้กำหนดแนวทางการ ดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศไว้ ดังนี้

(1) จัดหลักสูตรอบรมเจ้าหน้าที่ของสหกรณ์ฯ ให้มีความรู้ความเข้าใจในด้าน Hardware และ Software เบื้องต้น เพื่อลดความเสี่ยงด้าน Human Error ให้น้อยที่สุด ทำให้ เจ้าหน้าที่มีความรู้ความเข้าใจการใช้และบริหารจัดการเครื่องมืออุปกรณ์ทางด้าน สารสนเทศ ทั้งทางด้าน Hardware และ Software ได้มีประสิทธิภาพยิ่งขึ้น ทำให้ ความเสี่ยงที่เกิดจาก Human Error ลดน้อยลง

(2) จัดทำหนังสือแจ้ง เรื่อง การใช้และ การประหยัดพลังงานให้กับเครื่องคอมพิวเตอร์และอุปกรณ์ เพื่อเป็นแนวทางปฏิบัติ ได้อย่างถูกต้อง

ประเภทที่ 2 ภัยที่เกิดจาก Software ที่สร้างความเสียหายให้แก่เครื่องคอมพิวเตอร์หรือ ระบบเครือข่ายคอมพิวเตอร์ประกอบด้วย ไวรัสคอมพิวเตอร์ (Computer Virus) หนอนอินเทอร์เน็ต (Internet Worm) ม้าโทรจัน (Trojan Horse) และข่าวไวรัสหลอกลวง (Hoax) พวก Software เหล่านี้ อาจรบกวนการทำงาน และก่อให้เกิดความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ ถึงขั้นทำให้ระบบ เครือข่ายคอมพิวเตอร์ใช้งานไม่ได้ ได้กำหนดแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ภัยจาก Software ดังนี้

(1) ติดตั้ง Firewall ที่เครื่องคอมพิวเตอร์แม่ข่าย ทำหน้าที่ในการกำหนดสิทธิ์การเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่าย และป้องกันการบุกรุกจากภายนอก

(2) ติดตั้งซอฟต์แวร์ Antivirus ดักจับไวรัสที่เข้ามาในระบบเครือข่าย และสามารถ ตรวจสอบได้ว่ามีไวรัสชนิดใดเข้ามาทำความเสียหายกับระบบเครือข่ายคอมพิวเตอร์

ประเภทที่ 3 ภัยจากไฟไหม้ หรือ ระบบไฟฟ้า จัดเป็นภัยร้ายแรงที่ทำความเสียหายให้แก่ ระบบเทคโนโลยีสารสนเทศ ได้กำหนดแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ดังนี้

(1) ติดตั้งอุปกรณ์สำรองไฟฟ้า (UPS) เพื่อควบคุมการจ่ายกระแสไฟฟ้าให้กับระบบเครื่องแม่ข่าย (Server) ในกรณีเกิดกระแสไฟฟ้าขัดข้อง ระบบเครือข่ายคอมพิวเตอร์จะสามารถ ให้บริการได้ในระยะเวลาที่สามารถจัดเก็บและสำรองข้อมูลไว้อย่างปลอดภัย

(2) ติดตั้งอุปกรณ์ดับเพลิง ที่ห้องควบคุมระบบคอมพิวเตอร์เพื่อไว้ใช้ในกรณี เหตุฉุกเฉิน (ไฟไหม้) โดยมีการตรวจสอบความพร้อมของอุปกรณ์และทดลองใช้งาน โดยสม่ำเสมอ

ประเภทที่ 4 ภัยจากน้ำท่วม (อุทกภัย) ความเสี่ยงต่อความเสียหายจากน้ำท่วม จัดเป็นภัยร้ายแรงที่ทำความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ ได้กำหนดแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ดังนี้

(1) เจ้าหน้าที่ช่วยกันเคลื่อนย้ายเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่ายไว้ในที่สูง

(2) กรณีน้ำลดลงเรียบร้อยแล้วให้ช่างไฟฟ้าตรวจสอบระบบไฟฟ้าในห้องควบคุมเครือข่าย ว่าสามารถใช้งานได้ปกติหรือไม่ และเตรียมความพร้อมห้องควบคุมระบบเครือข่าย สำหรับติดตั้งเครื่องคอมพิวเตอร์ แม่ข่ายและอุปกรณ์เครือข่าย

(3) ทำการติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย พร้อมทั้งทดสอบการใช้งานของเครื่องคอมพิวเตอร์แม่ข่ายแต่ละเครื่องว่าสามารถให้บริการได้ตามปกติหรือไม่ ตรวจสอบระบบ Network ว่าสามารถเชื่อมต่อและให้บริการกับเครื่องคอมพิวเตอร์ลูกข่าย ได้หรือไม่

(4) เมื่อตรวจสอบแล้วว่าเครื่องคอมพิวเตอร์แม่ข่ายและระบบเครือข่ายสามารถให้บริการ ข้อมูลได้เรียบร้อยแล้ว แจ้งให้หน่วยงานที่เกี่ยวข้องทราบ เพื่อเข้ามาใช้บริการได้ ตามปกติ

หัวข้อที่ 4
การบริหารจัดการ การใช้บริการจากหน่วยงานภายนอก

วัตถุประสงค์

เพื่อให้หน่วยงานภายนอก ได้ปฏิบัติตามนโยบายรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ สหกรณ์ฯ ออมทรัพย์กรมการพัฒนาชุมชน จำกัด ทำให้ระบบสารสนเทศดำเนินไปได้อย่างต่อเนื่องและมีประสิทธิภาพ

แนวปฏิบัติ

ข้อ 1 ต้องมีการประเมินความเสี่ยงจากการเข้าถึงข้อมูล และระบบสารสนเทศหรืออุปกรณ์ที่ใช้ในการประมวลผลโดยหน่วยงานภายนอก และกำหนดมาตรการควบคุมที่เหมาะสมก่อนที่จะอนุญาตให้เข้าถึงข้อมูลและระบบสารสนเทศ หรืออุปกรณ์ดังกล่าวได้

ข้อ 2 การเข้าใช้งานระบบสารสนเทศหรือเข้าถึงข้อมูลของหน่วยงานจากหน่วยงานภายนอก ต้องมีการขออนุญาตจากสหกรณ์ และได้รับอนุญาตจากผู้จัดการ หรือผู้ดูแลระบบ ที่ได้รับมอบหมายก่อนเสมอ

ข้อ 3 การบริการ และการดำเนินงานจากหน่วยงานภายนอก จะต้องปฏิบัติตาม นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ แนวทางการปฏิบัติงาน มาตรฐาน และกฎข้อบังคับต่าง ๆ

ข้อ 4 ผู้ดูแลระบบต้องให้สิทธิ์การเข้าถึงข้อมูลต่อหน่วยงานภายนอกที่ขออนุญาตแล้วเท่านั้น

ข้อ 5 ต้องมีข้อตกลงในการเก็บรักษาความลับขององค์กร ระหว่างสหกรณ์ฯ และหน่วยงานภายนอกที่เข้ามาปฏิบัติงานก่อนเปิดให้ใช้บริการระบบเสมอ...
