นโยบาย

ความมั่นคงปลอดภัย ด้านเทคโนโลยีสารสนเทศและข้อมูลส่วนบุคคล

และแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

สหกรณ์ออมทรัพย์กรมการพัฒนาชุมชน จำกัด

มีความมั่นคงปลอดภัย มีความน่าเชื่อถือ และสามารถป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้เครื่องคอมพิวเตอร์ ระบบเครือข่าย และระบบสารสนเทศ

ประกาศ สหกรณ์ออมทรัพย์กรมการพัฒนาชุมชน จำกัด
เรื่อง นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และข้อมูลส่วนบุคคล

****

โดยที่ ระเบียบสหกรณ์ออมทรัพย์กรมการพัฒนาชุมชน จำกัด ว่าด้วยวิธีปฏิบัติการควบคุมภายในและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของสหกรณ์ พ.ศ. 2565 ข้อ 8 (1) สหกรณ์ต้องจัดทำนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศสำหรับระบบสารสนเทศของสหกรณ์ให้เป็นลายลักษณ์อักษร ดังนั้น-เพื่อให้การใช้เทคโนโลยีสารสนเทศของสหกรณ์ออมทรัพย์กรมการพัฒนาชุมชน จำกัด มีความมั่นคงปลอดภัย มีความน่าเชื่อถือ และสามารถป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้เครื่องคอมพิวเตอร์ ระบบเครือข่าย และระบบสารสนเทศ ตามที่กำหนดไว้ในพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 โดยคำนึงถึงความสำคัญของการคุ้มครอง ข้อมูลส่วนบุคคล ซึ่งเป็นข้อมูลที่มีความละเอียดอ่อนและต้องได้รับการดูแลอย่างเข้มงวดตามที่กำหนดไว้ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จึงทบทวนและปรับปรุงนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ เพื่อเสริมสร้างความมั่นคงปลอดภัย ไซเบอร์ของสหกรณ์ฯ ให้เกิดความสมบูรณ์ ทันสมัย และมีประสิทธิภาพสูงสุด และให้สอดคล้องกับปัจจัยสำคัญที่เปลี่ยนแปลงไป ทั้งในด้านกลยุทธ์และทิศทางธุรกิจ ตลอดจนแผนการเปลี่ยนผ่านสู่ดิจิทัลอย่างเหมาะสม และตอบสนองต่อข้อบังคับและกฎหมายที่เปลี่ยนแปลง โดยมุ่งเน้นการปฏิบัติตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) และกฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างเคร่งครัด

อาศัยอำนาจตามข้อบังคับสหกรณ์ออมทรัพย์กรมการพัฒนาชุมชน จำกัด พ.ศ. 2565 แก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ. 2567 และแก้ไขเพิ่มเติม (ฉบับที่ 3) พ.ศ. 2568 ข้อ 81 (24) และระเบียบสหกรณ์ออมทรัพย์กรมการพัฒนาชุมชน จำกัด ว่าด้วยวิธีปฏิบัติการควบคุมภายในและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของสหกรณ์ พ.ศ. 2565 ข้อ 8 (1) ประกอบมติที่ประชุมคณะกรรมการดำเนินการสหกรณ์ ในการประชุม ครั้งที่ 11/2568 เมื่อวันพุธที่ 15 ตุลาคม พ.ศ. 2568 จึงยกเลิกประกาศ เรื่องนโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศ และออกประกาศสหกรณ์ออมทรัพย์กรมการพัฒนาชุมชน จำกัด เรื่อง นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและข้อมูลส่วนบุคคล ดังนี้

ข้อ 1 ประกาศนี้เรียกว่า “ประกาศ สหกรณ์ออมทรัพย์กรมการพัฒนาชุมชน จำกัด เรื่อง นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และข้อมูลส่วนบุคคล ”

ข้อ 2 ประกาศนี้ให้ใช้บังคับตั้งแต่ในวันที่ประกาศ เป็นต้นไป

ข้อ 3 นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและข้อมูลส่วนบุคคล มีวัตถุประสงค์ดังต่อไปนี้

3.1 เพื่อให้เกิดความน่าเชื่อถือ เชื่อมั่น และมีความมั่นคงปลอดภัยในการใช้งานด้านเทคโนโลยีสารสนเทศ ทำให้สามารถดำเนินงานได้อย่างมีประสิทธิภาพ ประสิทธิผล และพร้อมใช้งานอย่างต่อเนื่อง รวมทั้งเพื่อป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้เครื่องคอมพิวเตอร์ ระบบเครือข่ายคอมพิวเตอร์ และระบบสารสนเทศ

3.2 เพื่อกำหนดแนวทางปฏิบัติให้คณะกรรมการดำเนินการ คณะอนุกรรมการ คณะทำงาน ผู้จัดการ เจ้าหน้าที่ ผู้ดูแลระบบ ผู้ให้บริการภายนอก และบุคคลที่เกี่ยวข้อง ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการคุ้มครองข้อมูลส่วนบุคคล และปฏิบัติตามอย่างเคร่งครัด

3.3 เพื่อให้การเก็บ ใช้ เปิดเผย และลบข้อมูลส่วนบุคคลของสมาชิก สหกรณ์ และเจ้าหน้าที่เป็นไปตามหลักการของ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) โดยเฉพาะการขอความยินยอม การแจ้งวัตถุประสงค์ และการรักษาความลับของข้อมูล

3.4 เพื่อกำหนดมาตรการป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต โดยใช้ระบบการพิสูจน์ตัวตนหลายชั้น (Multi-Factor Authentication : MFA) และการควบคุมสิทธิ์ตามหลัก Need-to-Know และ Least Privilege

ข้อ 4 นโยบายในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและข้อมูลส่วนบุคคล กำหนดประเด็นสำคัญดังต่อไปนี้

4.1 การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

4.1.1 การเข้าถึงระบบสารสนเทศ ต้องควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย ทั้งด้านความลับ ความสมบูรณ์ และความพร้อมใช้งาน (Confidentiality, Integrity, Availability) กำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง และกำหนดสิทธิ์อย่างชัดเจน เพื่อให้ผู้ใช้งานในทุกระดับได้รับรู้ เข้าใจ และสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ และการคุ้มครองข้อมูลส่วนบุคคล

4.1.2 การบริหารจัดการการเข้าถึงของผู้ใช้งาน เพื่อควบคุมการเข้าถึงระบบสารสนเทศและป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ต้องกำหนดให้มีการลงทะเบียนผู้ใช้งาน ตรวจสอบบัญชีผู้ใช้งาน อนุมัติ และกำหนดรหัสผ่านหรือวิธีการพิสูจน์ตัวตนที่เหมาะสม โดยให้เฉพาะผู้ใช้งานที่มีสิทธิ์เท่านั้นที่สามารถเข้าใช้ระบบสารสนเทศได้ต้องเก็บบันทึกข้อมูลการเข้าถึงและข้อมูลจราจรทางคอมพิวเตอร์ (Log) อย่างน้อย 90 วัน ต้องบริหารจัดการสิทธิ์การเข้าถึงข้อมูลให้เหมาะสมตามระดับชั้นความลับของผู้ใช้งาน และต้องมีการทบทวนสิทธิ์การใช้งานอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงตำแหน่งงาน พร้อมตรวจสอบการละเมิดความปลอดภัยอย่างสม่ำเสมอ

4.1.3 การควบคุมการเข้าถึงเครือข่าย เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต ต้องกำหนดสิทธิ์ในการเข้าถึงเครือข่าย ให้ผู้ที่จะเข้าใช้งานต้องลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยรหัสผ่านหรือ Multi-Factor Authentication (MFA) สำหรับระบบสำคัญ ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์สำหรับใช้งานอินเทอร์เน็ตโดยผ่านระบบรักษาความปลอดภัย (เช่น Firewall, IDS/IPS) และมีการออกแบบระบบเครือข่ายโดยแบ่งเขต (Zone) การใช้งาน เช่น Zone ภายใน, Zone สาธารณะ (Guest), Zone เซิร์ฟเวอร์ เพื่อควบคุมและป้องกันภัยคุกคามได้อย่างเป็นระบบและมีประสิทธิภาพ

4.1.4 การควบคุมการเข้าถึงระบบปฏิบัติการ เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต ต้องกำหนดให้ผู้ที่จะเข้าใช้งานต้องลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยรหัสผ่านหรือ MFA ต้องกำหนดให้ระบบล็อกอัตโนมัติหลังไม่มีการใช้งานเกิน 15 นาที และจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศ รวมถึงห้ามใช้บัญชีผู้ใช้งานแบบร่วมกัน (Shared Account)

4.1.5 การควบคุมการเข้าถึงโปรแกรมประยุกต์และแอปพลิเคชัน ต้องกำหนดสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศที่สำคัญ โปรแกรมประยุกต์หรือแอปพลิเคชันต่าง ๆ รวมถึง จดหมายอิเล็กทรอนิกส์ (E-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) และระบบงานต่าง ๆ โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่ (Need-to-Know และ Least Privilege) ต้องมีการตรวจสอบและอนุมัติการใช้งานแอปพลิเคชันจากแหล่งภายนอก (เช่น Cloud Services, SaaS) โดยผู้ดูแลระบบก่อนการใช้งาน

4.2 การจัดทำระบบสำรองข้อมูลและการกู้คืน (Backup and Recovery)

เพื่อให้ระบบสารสนเทศของสหกรณ์ฯ สามารถให้บริการได้อย่างต่อเนื่องและมีเสถียรภาพ ต้องจัดทำระบบสารสนเทศและระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน โดยดำเนินการดังนี้

4.2.1 ต้องพิจารณาคัดเลือกระบบสารสนเทศที่สำคัญ (เช่น ระบบการเงิน ระบบสมาชิก ระบบบุคลากร) และจัดลำดับความจำเป็นจากมากไปน้อย

4.2.2 ต้องกำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ในการสำรองข้อมูลอย่างชัดเจน

4.2.3 ต้องกำหนดประเภทของข้อมูลที่ต้องสำรอง ความถี่ในการสำรอง และวิธีการสำรองให้เหมาะสม เช่น ระบบสำคัญ สำรองข้อมูลทุกวัน (Daily Backup) ระบบทั่วไป สำรองข้อมูลรายสัปดาห์ (Weekly Backup)

4.2.4 ต้องจัดเก็บข้อมูลสำรองในสื่อที่ปลอดภัย แยกจากสถานที่ตั้งหลัก (Offsite Backup) และต้องเข้ารหัสข้อมูล (Encrypted) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

4.2.5 ต้องทดสอบการกู้คืนข้อมูล (Recovery Test) อย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่าข้อมูลสามารถกู้คืนได้จริง

4.3 การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างเป็นระบบ ดังนี้

4.3.1 จัดให้มีการตรวจสอบโดยผู้ตรวจสอบภายในของสหกรณ์ฯ หรือผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก อย่างน้อยปีละ 1 ครั้ง

4.3.2 การประเมินความเสี่ยงต้องครอบคลุมทั้งด้านเทคนิค กระบวนการ และข้อมูลส่วนบุคคล โดยพิจารณาความเสี่ยงจากการเข้าถึงโดยไม่ได้รับอนุญาต การสูญหายของข้อมูล การโจมตีทางไซเบอร์ และการไม่ปฏิบัติตาม PDPA

4.3.3 ต้องจัดทำรายงานผลการตรวจสอบและประเมินความเสี่ยง พร้อมข้อเสนอแนะในการปรับปรุง

4.3.4 ต้องมีมาตรการในการตรวจประเมินระบบสารสนเทศ ได้แก่

- กำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นได้ในรูปแบบ "อ่านอย่างเดียว"
- หากจำเป็นต้องใช้ข้อมูลในรูปแบบอื่น ต้องสร้างสำเนา และต้องทำลายหรือลบข้อมูลทันทีหลังการตรวจสอบเสร็จสิ้น หรือเก็บรักษาอย่างปลอดภัย
- ระบุและจัดสรรทรัพยากรที่จำเป็นสำหรับการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย

ข้อ 5 หน้าที่ความรับผิดชอบ

5.1 คณะกรรมการดำเนินการสหกรณ์ฯ คณะอนุกรรมการ คณะทำงานที่เกี่ยวข้อง

5.1.1 สนับสนุนการดำเนินงานด้านเทคโนโลยีสารสนเทศให้มีประสิทธิภาพ รวมทั้งจัดสรรงบประมาณ ทรัพยากร และบุคลากรที่จำเป็นในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและข้อมูลส่วนบุคคล

5.1.2 มอบหมายให้มีผู้รับผิดชอบในการติดตามการปฏิบัติตามระเบียบปฏิบัติในการควบคุมภายใน และการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและข้อมูลส่วนบุคคลของสหกรณ์ฯ อย่างต่อเนื่อง

5.1.3 สื่อสารและสร้างความตระหนักกับบุคลากร ถึงความสำคัญของการปฏิบัติตามระเบียบ และแนวปฏิบัติที่สหกรณ์ฯ กำหนดขึ้นภายใต้ นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและข้อมูลส่วนบุคคล โดยเคร่งครัด

5.1.4 ส่งเสริมให้มีการฝึกอบรมหรือให้ความรู้เกี่ยวกับระบบงาน การรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ และการปฏิบัติตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) แก่คณะกรรมการดำเนินการ ผู้จัดการ และเจ้าหน้าที่สหกรณ์ เป็นประจำทุกปี

5.2 ผู้จัดการ รองผู้จัดการ ผู้ดูแลระบบ และเจ้าหน้าที่สหกรณ์ฯ

5.2.1 ผู้จัดการ หรือรองผู้จัดการที่ได้รับมอบหมาย มีหน้าที่ควบคุมดูแลการใช้งานระบบเทคโนโลยีสารสนเทศภายในสหกรณ์ฯ ให้เป็นไปตามวัตถุประสงค์การใช้งาน และปฏิบัติตามนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและข้อมูลส่วนบุคคลอย่างเคร่งครัด

5.2.2 ผู้ดูแลระบบมีหน้าที่ดำเนินการให้ระบบเทคโนโลยีสารสนเทศของสหกรณ์ฯ ทำงานได้อย่างมีประสิทธิภาพ มั่นคงปลอดภัย ตามระเบียบปฏิบัติในการควบคุมภายใน และการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศและข้อมูลส่วนบุคคลของสหกรณ์ฯ

5.2.3 เจ้าหน้าที่ทุกระดับ มีหน้าที่ปฏิบัติตามคำสั่ง ระเบียบ และแนวปฏิบัติที่สหกรณ์ฯ กำหนดขึ้นภายใต้นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและข้อมูลส่วนบุคคลโดยเคร่งครัด

ข้อ 6 การดำเนินการตามนโยบาย ให้มีผลตามที่กำหนดตั้งแต่วันที่ ประกาศ เรื่อง นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและข้อมูลส่วนบุคคล โดยให้มีการทบทวนอย่างน้อยปีละ 1 ครั้ง

ประกาศ ณ วันที่ 5 พฤศจิกายน พ.ศ. 2568

(นางสาวขนิฏฐา กาญจนรังษีนนท์)
ประธานกรรมการ
สหกรณ์ออมทรัพย์กรมการพัฒนาชุมชน จำกัด

แนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและข้อมูลส่วนบุคคล
สหกรณ์ออมทรัพย์กรมการพัฒนาชุมชน จำกัด

ตามประกาศสหกรณ์ออมทรัพย์กรมการพัฒนาชุมชน จำกัด เรื่อง นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและข้อมูลส่วนบุคคล พ.ศ. 2568 กำหนดให้มีการจัดทำแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้เจ้าหน้าที่ใช้งานระบบเทคโนโลยีสารสนเทศอย่างเหมาะสม มีประสิทธิภาพ มั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง

ทั้งนี้ เพื่อป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและจากการถูกคุกคามจากภัยคุกคามทางไซเบอร์ รวมถึงการรั่วไหลหรือการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต ซึ่งอาจก่อให้เกิดความเสียหายต่อสหกรณ์

หัวข้อที่ 1
การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

วัตถุประสงค์

1. เพื่อควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งาน ความมั่นคงปลอดภัย และการรักษาความลับ ความสมบูรณ์ และความพร้อมใช้งานของข้อมูล

2. เพื่อกำหนดแนวทางที่ชัดเจนในการอนุญาตให้เข้าถึงระบบ และการกำหนดสิทธิ์การใช้งานให้เหมาะสมกับตำแหน่งงานและหน้าที่ของแต่ละคน ไม่ให้มีสิทธิ์เกินความจำเป็น

3. เพื่อให้ผู้ใช้งานได้รับรู้ เข้าใจ และสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการคุ้มครองข้อมูลส่วนบุคคล

แนวปฏิบัติ

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

ข้อ 1 ผู้ดูแลระบบจะอนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศที่ต้องการใช้งานได้ ต่อเมื่อได้รับอนุญาตจากผู้รับผิดชอบ / เจ้าของข้อมูล / เจ้าของระบบและธุรกรรม ตามความจำเป็นต่อการใช้งานเท่านั้น

ข้อ 2 กำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งาน และหน้าที่ความรับผิดชอบในการปฏิบัติงานของผู้ใช้งานระบบสารสนเทศ โดยผู้ดูแลระบบเป็นผู้กำหนดสิทธิ์ตามอนุญาต และต้องมีการ ทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ (อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงตำแหน่งงาน) ดังนี้

(1) กำหนดสิทธิ์ของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง

- อ่านอย่างเดียว
- บันทึกข้อมูล
- แก้ไข
- อนุมัติ
- ไม่มีสิทธิ์

(2) กำหนดเกณฑ์การระงับสิทธิ์ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งานที่ได้กำหนดไว้ โดยเฉพาะเมื่อพนักงานลาออก ย้ายตำแหน่ง หรือหยุดปฏิบัติงาน

(3) ผู้ดูแลระบบมีหน้าที่ควบคุมดูแลการเข้าถึงระบบสารสนเทศ ดังนี้

- อนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศของสหกรณ์ฯ
- กำหนดสิทธิ์ผู้ใช้งานให้เหมาะสมกับการใช้งาน และทบทวนสิทธิ์การเข้าถึงนั้นอย่างสม่ำเสมอ
- ติดตั้งระบบการบันทึกติดตามการใช้งาน (Logging) และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบสารสนเทศของสหกรณ์ฯ
- จัดเก็บ ข้อมูลจราจรทางคอมพิวเตอร์ (Log) อย่างน้อย 90 วัน และจำกัดสิทธิ์การเข้าถึงเฉพาะผู้ที่เกี่ยวข้อง

ข้อ 3 จัดแบ่งประเภทของข้อมูล การจัดลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล ระดับชั้นการเข้าถึง และช่องทางการเข้าถึงข้อมูล โดยกำหนดไว้ดังนี้

(1) จัดแบ่งระดับการเข้าถึง

- ระดับผู้ดูแลระบบ
- ระดับผู้จัดการ
- ระดับรองผู้จัดการ
- ระดับหัวหน้าฝ่าย
- ระดับเจ้าหน้าที่

(2) จัดแบ่งประเภทข้อมูล

- ข้อมูลสมาชิก (รวมถึงข้อมูลส่วนบุคคล เช่น ชื่อ นามสกุล เลขบัตรประชาชน เบอร์โทรศัพท์)
- ข้อมูลหุ้นและหนี้
- ข้อมูลด้านการเงิน
- ข้อมูลด้านการบัญชี
- ข้อมูลบุคลากร
- ข้อมูลสวัสดิการ
- ข้อมูลคำรับรอง
- ข้อมูลด้านการลงทุน
- ข้อมูลวัสดุครุภัณฑ์
- ข้อมูลข่าวสารทั่วไป

ข้อ 4 ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภท ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน ดังนี้

(1) กำหนดบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อใช้ในการพิสูจน์ตัวตนของผู้ใช้งาน

(2) สำหรับระบบสำคัญ ต้องใช้ การพิสูจน์ตัวตนหลายชั้น (Multi-Factor Authentication MFA) เช่น รหัสผ่าน รหัส OTP

(3) การตั้งรหัสผ่านเป็นไปตามหลักเกณฑ์มาตรฐานสากล หรือมาตรฐานที่สหกรณ์ฯ กำหนด ต้องเปลี่ยนรหัสผ่านโดยทันทีเมื่อมีการแจ้งเตือนว่าถูกละเมิด หรือเมื่อมีการเปลี่ยนแปลงบทบาทงาน ไม่จำเป็นต้องเปลี่ยนทุก 180 วัน (ตามแนวทาง NIST)

(4) กรณีนำสินทรัพย์ของสหกรณ์ฯ ออกนอกสำนักงานเพื่อบำรุงรักษาหรือซ่อมแซม ต้องดำเนินการ สำรองข้อมูล และ ลบข้อมูลที่เก็บอยู่ในสื่อบันทึก ก่อนนำออก เพื่อป้องกันการรั่วไหลของข้อมูล

ข้อ 5 การกำหนดระบบและอุปกรณ์สนับสนุนการปฏิบัติงาน ดังนี้

(1) มีระบบสนับสนุนการทำงานของระบบสารสนเทศของหน่วยงานที่เพียงพอต่อความต้องการใช้งาน ระบบรักษาความปลอดภัย (Security System) ระบบสำรองกระแสไฟฟ้า (UPS) ระบบสำรองข้อมูล (Backup System) และแผนผังเครือข่าย (Network Diagram)

(2) ตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างสม่ำเสมอ (อย่างน้อยทุก 6 เดือน) เพื่อให้มั่นใจได้ว่าทำงานได้ปกติ และลดความเสี่ยงจากความล้มเหลวในการทำงาน

(3) จัดวางอุปกรณ์ในพื้นที่หรือบริเวณที่เหมาะสม เพื่อหลีกเลี่ยงการเข้าถึงจากบุคคลภายนอก และให้แยกอุปกรณ์ที่มีความสำคัญเก็บไว้อีกพื้นที่หนึ่งที่มีความมั่นคงปลอดภัยเพียงพอ

(4) การเดินสายไฟ สายสัญญาณเครือข่าย และสายเคเบิลอื่นที่จำเป็นต้องวางผ่านบริเวณที่บุคคลภายนอกเข้าถึงได้ ให้ร้อยท่อสายสัญญาณเพื่อป้องกัน สัตว์กัดกินสาย การดักจับสัญญาณ (Eavesdropping) การตัดสายสัญญาณ

(5) ต้องจัดทำ แผนผังสายสัญญาณสื่อสาร ให้ครบถ้วนถูกต้อง โดยแยกสายสัญญาณสื่อสารและสายไฟฟ้าออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนสัญญาณ จัดเก็บสายสัญญาณต่าง ๆ ไว้ในตู้ Rack และปิดใส่สลักกุญแจให้สนิท เพื่อป้องกันการเข้าถึงจากบุคคลภายนอกหรือผู้ที่ไม่มีส่วนเกี่ยวข้อง

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

ข้อ 1 กำหนดให้มีการลงทะเบียนเจ้าหน้าที่หรือผู้ใช้งานใหม่ (User Registration) เพื่อรับสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศและระบบสารสนเทศ ตามตำแหน่งงานหรือหน้าที่ที่ได้รับมอบหมาย

ข้อ 2 กำหนดให้มีการบริหารจัดการสิทธิ์ของผู้ใช้งาน (User Management) อย่างรัดกุม โดยมีการควบคุม จำกัด และเปลี่ยนแปลงสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศ และระบบสารสนเทศ ตามตำแหน่งงานหรือหน้าที่ที่ได้รับมอบหมาย ต้องมีการทบทวนสิทธิ์ของผู้ใช้งาน และปรับปรุงบัญชีของผู้ใช้งานอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงตำแหน่งงาน โยกย้าย ลาออก หรือสิ้นสุดการจ้าง ห้ามใช้บัญชีผู้ใช้งานแบบร่วมกัน (Shared Account)

ข้อ 3 กำหนดกระบวนการสำหรับยกเลิกสิทธิ์การใช้งานทันทีเมื่อมีการเปลี่ยนแปลงตำแหน่งงาน โยกย้าย ลาออก หรือสิ้นสุดการจ้าง ต้องดำเนินการภายใน 24 ชั่วโมง นับจากวันที่ทราบและมีการยืนยันการปิดบัญชีผู้ใช้งานจากผู้ดูแลระบบ

ข้อ 4 กำหนดให้มีการบริหารจัดการรหัสผ่าน (User Password Management) อย่างรัดกุม ดังนี้

(1) ต้องเปลี่ยนหรือยกเลิกรหัสผ่าน (Password) ทันทีเมื่อผู้ใช้งานลาออก พ้นจากตำแหน่งหรือยกเลิกการใช้งาน

(2) ห้ามบันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ หรือในรูปแบบที่ไม่ได้รับการป้องกัน เช่น ไฟล์ข้อความ โน้ต สมุดจด

(3) สำหรับระบบสำคัญ ต้องใช้ Multi-Factor Authentication (MFA) เช่น รหัสผ่าน รหัส OTP หรือแอปยืนยันตัวตน

(4) ห้ามใช้รหัสผ่านที่คาดเดาได้ง่าย เช่น ชื่อผู้ใช้ วันเกิด หรือรหัสผ่านซ้ำกันในหลายระบบ

(5) หากมีการกระทำความผิดเกิดขึ้นจากชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของบุคคลใด บุคคลนั้นต้องเป็นผู้รับผิดชอบต่อการกระทำนั้น เว้นแต่จะสามารถพิสูจน์ได้ว่าถูกละเมิดโดยไม่ใช่ความผิดของตนเอง

ข้อ 5 ระบบงานสารสนเทศทางธุรกิจที่เชื่อมโยงกัน ให้ผู้จัดการพิจารณาประเด็นต่าง ๆ ทางด้านความมั่นคงปลอดภัย และข้อมูลละเอียดอ่อนต่าง ๆ ก่อนตัดสินใจใช้ข้อมูลร่วมกันในระบบงาน หรือระบบเทคโนโลยีสารสนเทศที่จะเชื่อมโยงเข้าด้วยกัน เช่น ระหว่างสหกรณ์ฯ กับหน่วยงานอื่นที่มาขอเชื่อมโยง โดยต้องพิจารณาดังนี้

(1) จำกัดหรือไม่อนุญาตการเข้าถึง ข้อมูลส่วนบุคคล โดยเฉพาะข้อมูลที่ละเอียดอ่อน (Sensitive Data) เช่น เลขบัตรประจำตัวประชาชน เลขบัญชีธนาคาร เว้นแต่จะมีเหตุผลจำเป็นและได้รับความยินยอม

(2) จัดทำแผนผังการไหลของข้อมูล (Data Flow Diagram) เพื่อแสดงเส้นทางการเคลื่อนย้ายข้อมูลตั้งแต่จุดเริ่มต้นจนถึงปลายทาง

(3) พิจารณาว่ามีบุคลากรใดบ้างที่มีสิทธิ์หรือได้รับอนุญาตให้เข้าใช้งาน และต้องมีการบันทึกไว้ในทะเบียนการประมวลผลข้อมูล (ROPA)

(4) มีมาตรการป้องกันที่เหมาะสมและเพียงพอในการใช้ข้อมูล

ส่วนที่ 3 การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

ข้อ 1 การใช้งานรหัสผ่าน ผู้ใช้งานต้องปฏิบัติดังนี้

(1) ผู้ใช้งานมีหน้าที่ในการป้องกัน ดูแล และรักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) อย่างเคร่งครัด โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งานของตนเอง ห้ามใช้ร่วมกับผู้อื่น ห้ามเผยแพร่ แจกจ่าย หรือทำให้ผู้อื่นล่วงรู้รหัสผ่าน สำหรับระบบสำคัญ ต้องใช้ Multi-Factor Authentication (MFA) เช่น รหัสผ่าน รหัส OTP

(2) หลีกเลี่ยงการตั้งรหัสผ่านที่คาดเดาได้ง่าย เช่น ชื่อ นามสกุล วันเกิด หรือรหัสผ่านทั่วไป (เช่น 123456, password) รหัสผ่านควรมีความยาวไม่น้อยกว่า 12 ตัวอักษร และประกอบด้วยตัวพิมพ์ใหญ่ เลข และสัญลักษณ์

(3) เมื่อจำเป็นต้องใช้เว็บเบราว์เซอร์ บนเครื่องคอมพิวเตอร์ที่ไม่ใช่ส่วนตัว หรือที่ใช้ร่วมกับผู้อื่น ห้าม“จดจำรหัสผ่านอัตโนมัติ” (Save Password)

(4) ห้ามจดหรือบันทึกรหัสผ่านไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็น เช่น กระดาษเหนือโต๊ะ ใต้แป้นพิมพ์ หรือไฟล์ข้อความในเครื่อง

(5) ต้องเปลี่ยนรหัสผ่านโดยทันทีเมื่อมีการแจ้งเตือนว่าถูกละเมิด หรือเมื่อมีการเปลี่ยนแปลงบทบาทงาน ไม่จำเป็นต้องเปลี่ยนทุก 180 วัน (ตามแนวทาง NIST)

ข้อ 2 การกระทำใด ๆ ที่เกิดจากการใช้บัญชีของผู้ใช้งาน (Username) อันมีกฎหมายกำหนดให้เป็นความผิด ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานโดยตรงหรือไม่ก็ตาม ให้ถือว่าเป็นความรับผิดชอบส่วนบุคคล ผู้ใช้งานต้องรับผิดชอบต่อการกระทำที่เกิดขึ้นจากบัญชีของตน หากพบว่าบัญชีถูกใช้งานโดยไม่ได้รับอนุญาต ต้องรายงานทันทีให้ผู้ดูแลระบบและเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

ข้อ 3 ห้ามใช้สินทรัพย์ของหน่วยงานเพื่อการรบกวน ก่อให้เกิดความเสียหาย หรือใช้ในการโจรกรรมข้อมูล หรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมาย ศีลธรรม หรือกระทบต่อภารกิจของสหกรณ์ฯ รวมถึงห้ามใช้เพื่อเก็บแชร์ หรือเผยแพร่ข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต

ข้อ 4 ห้ามกระทำการใด ๆ เพื่อการดักข้อมูล (Sniffing) ไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใดในเครือข่ายระบบสารสนเทศของสหกรณ์ฯ โดยเด็ดขาด ไม่ว่าจะด้วยวิธีการใด ๆ ก็ตาม

ข้อ 5 ห้ามกระทำการรบกวน ทำลาย หรือทำให้ระบบสารสนเทศของหน่วยงานต้องหยุดชะงัก

ข้อ 6 ห้ามกระทำการใด ๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลของผู้อื่น ไม่ว่าจะเป็นกรณีใด ๆ เพื่อประโยชน์ในการเข้าถึงข้อมูล หรือเพื่อการใช้ทรัพยากรของสหกรณ์ฯ

ส่วนที่ 4 การบริหารจัดการสินทรัพย์ (Assets Management)

ข้อ 1 ผู้ใช้งานต้องไม่เข้าไปในศูนย์คอมพิวเตอร์ ซึ่งหมายถึง พื้นที่ที่ใช้จัดวางเครื่องคอมพิวเตอร์แม่ข่าย (Server), ระบบจัดเก็บข้อมูลภายนอก (Storage), ระบบเครือข่ายคอมพิวเตอร์ และอุปกรณ์สื่อสารต่าง ๆ ของสหกรณ์ ซึ่งเป็นศูนย์กลางในการประมวลผลข้อมูลสารสนเทศเพื่อใช้ปฏิบัติงานของสหกรณ์ฯ และถือเป็น เขตหวงห้าม เว้นแต่ได้รับอนุญาตจากผู้ดูแลระบบ ต้องมีการติดตั้งระบบควบคุมการเข้าออก (เช่น บัตรผ่าน, เครื่องสแกนลายนิ้วมือ) และกล้องวงจรปิด (CCTV) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

ข้อ 2 ผู้ใช้งานต้องไม่นำอุปกรณ์หรือชิ้นส่วนใด ๆ ออกจากห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ ห้ามถอดหรือเปลี่ยนแปลงส่วนประกอบของอุปกรณ์ภายในศูนย์คอมพิวเตอร์โดยไม่ได้รับอนุญาต เว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ 3 กรณีทำงานนอกสถานที่ ผู้ใช้งานต้องดูแลและรับผิดชอบสินทรัพย์ของหน่วยงานที่ได้รับมอบหมายอย่างเข้มงวด โดยต้องปฏิบัติดังนี้

(1) ต้องไม่ทิ้งอุปกรณ์ไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย โจรกรรม หรือความเสียหาย

(2) กรณีอุปกรณ์สูญหายหรือถูกโจรกรรม ต้องรายงานให้ผู้ดูแลระบบและเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ทันทีเพื่อประเมินความเสี่ยงและดำเนินการแจ้งเหตุละเมิดข้อมูล (Data Breach Notification) ตาม PDPA

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

ข้อ 1 ผู้ใช้งานจะนำเครื่องคอมพิวเตอร์หรืออุปกรณ์ใด ๆ มาเชื่อมต่อกับเครื่องคอมพิวเตอร์ ระบบ หรือเครือข่ายของสหกรณ์ฯ ต้องได้รับอนุญาตจากผู้ดูแลระบบก่อน ต้องมีการตรวจสอบความปลอดภัยของอุปกรณ์ก่อนเชื่อมต่อ มีการติดตั้ง Antivirus ที่เป็นปัจจุบัน ห้ามเชื่อมต่ออุปกรณ์ส่วนตัว (BYOD) โดยไม่ได้รับอนุญาต

ข้อ 2 ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติม หรือดำเนินการใดๆ ต่ออุปกรณ์ส่วนกลาง โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลัก การเปลี่ยนแปลงการตั้งค่าใดๆ ต้องมีการบันทึกและอนุมัติล่วงหน้า

ข้อ 3 ผู้ดูแลระบบต้องควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ ดังนี้

(1) จำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น

(2) จำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน โดยใช้เทคโนโลยี Network Segmentation เพื่อแยกเครือข่ายภายในออกจากกัน

(3) จำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่าย (Server) เพื่อไม่ให้ผู้ใช้งานสามารถใช้เส้นทางอื่น ๆ ได้

(4) ติดตั้งและดูแลระบบป้องกันเครือข่ายคอมพิวเตอร์ (Firewall) เพื่อตรวจสอบและบล็อกการใช้งานที่ผิดปกติ รวมถึงป้องกันภัยคุกคามจากภายนอก

(5) การเข้าสู่ระบบเครือข่ายภายในหน่วยงานผ่านทางอินเทอร์เน็ต ต้องมีการลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยรหัสผ่าน

(6) ต้องจัดทำ แผนผังระบบเครือข่าย (Network Diagram) ที่มีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและภายนอก อุปกรณ์ต่าง ๆ และการเชื่อมต่ออย่างชัดเจน พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

(7) กำหนดระยะเวลาผู้ใช้งานที่อยู่ในระบบเครือข่ายให้ออกจากระบบเครือข่าย เมื่อเว้นว่างจากการใช้งานเป็นระยะเวลาไม่เกิน 15 นาที

ข้อ 4 ผู้ดูแลระบบต้องบริหารควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) และรับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่าต่าง ๆ ของซอฟต์แวร์ระบบ (Systems Software)

ข้อ 5 การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบงานต้องมีการขออนุมัติจากผู้ดูแลระบบก่อนดำเนินการ ต้องมั่นใจว่าซอฟต์แวร์มีลิขสิทธิ์ และไม่ก่อให้เกิดช่องโหว่ด้านความปลอดภัย

ข้อ 6 การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์มีความถูกต้องครบถ้วน และสามารถระบุตัวบุคคลที่เข้าถึงระบบได้ ต้องเก็บ Log อย่างน้อย 90 วัน ห้ามแก้ไข ลบ หรือปลอมแปลง Log จำกัดสิทธิ์การเข้าถึง Log ให้เฉพาะผู้ดูแลระบบและเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

ส่วนที่ 6 การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

ข้อ 1 กำหนดขั้นตอนการปฏิบัติเพื่อเข้าใช้งาน ดังนี้

(1) ผู้ใช้งานต้องกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ รหัสผ่านต้องมีความซับซ้อนและปลอดภัยสูงตามหลักเกณฑ์มาตรฐานสากล หรือมาตรฐานที่สหกรณ์ฯ กำหนด (ไม่น้อยกว่า 8-16 ตัวอักษร) และไม่ควรใช้คำที่คาดเดาได้ง่าย สำหรับเครื่องที่เก็บข้อมูลส่วนบุคคลหรือข้อมูลสำคัญ ต้องมีการ เข้ารหัสดิสก์ (Full Disk Encryption)

(2) ผู้ใช้งานต้องตั้งค่าล็อกหน้าจออัตโนมัติเมื่อไม่มีการใช้งาน ระยะเวลาไม่เกิน 15 นาที สำหรับเครื่องทั่วไป เมื่อต้องการใช้งานอีกครั้ง ต้องใส่รหัสผ่านหรือใช้วิธีพิสูจน์ตัวตนที่ได้รับอนุญาต

(3) ห้ามเปิดหรือใช้งานโปรแกรมที่มีความเสี่ยง เช่น โปรแกรมแชทส่วนตัว โปรแกรมดาวน์โหลดไฟล์แบบ P2P หรือโปรแกรมที่ไม่ผ่านการตรวจสอบความปลอดภัย เว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบ

(4) ซอฟต์แวร์ที่สหกรณ์ฯ ใช้ต้องมีลิขสิทธิ์ครบถ้วน ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น ห้ามติดตั้งหรือใช้งานซอฟต์แวร์ใด ๆ ที่ไม่มีลิขสิทธิ์ หรือเป็นซอฟต์แวร์ไม่ถูกลิขสิทธิ์

(5) ซอฟต์แวร์ที่สหกรณ์ฯ จัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นทรัพยากรที่จำเป็นต่อการปฏิบัติงาน ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น ห้ามคัดลอกหรือแจกจ่ายซอฟต์แวร์ให้บุคคลภายนอก หรือใช้ในกิจกรรมส่วนตัว

6) ห้ามผู้ใช้งานนำเสนอ แชร์ หรือเผยแพร่ข้อมูลใด ๆ ที่ละเมิดลิขสิทธิ์ มีเนื้อหารุนแรง ลามก หรือไม่เหมาะสม ขัดต่อศีลธรรม หรืออาจก่อให้เกิดความเสียหายต่อชื่อเสียงของสหกรณ์ฯ โดยเฉพาะข้อมูลส่วนบุคคลของสมาชิกหรือเจ้าหน้าที่ ต้องไม่เปิดเผยโดยเด็ดขาด

ส่วนที่ 7 การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control)

ข้อ 1 ผู้ดูแลระบบต้องกำหนดสิทธิ์การใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์ โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิ์เฉพาะตามหน้าที่งาน ต้องได้รับความเห็นชอบจากผู้ดูแลระบบหรือเจ้าของข้อมูลก่อนอนุมัติ ต้องมีการทบทวนสิทธิ์การเข้าถึงอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงตำแหน่งงาน

ข้อ 2 ผู้ดูแลระบบต้องบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่านของบุคลากร ดังนี้

(1) ต้องเปลี่ยนหรือยกเลิกรหัสผ่าน (Password) ทันทีเมื่อผู้ใช้งานลาออก พ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

(2) ห้ามให้ผู้ใช้งานบันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้รับการป้องกัน เช่น ไฟล์ข้อความ โน้ต หรือสมุดจด

(3) ต้องมั่นใจว่าชื่อผู้ใช้งาน (Username) ไม่ซ้ำกันในระบบ และต้องไม่ใช้ชื่อที่คาดเดาได้ง่าย

(4) สำหรับระบบสำคัญ ต้องใช้ Multi-Factor Authentication (MFA) เช่น รหัสผ่าน รหัส OTP

ข้อ 3 ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภท ดังนี้

(1) ควบคุมการเข้าถึงข้อมูลแต่ละระดับความลับอย่างเคร่งครัด ทั้งการเข้าถึงโดยตรง และผ่านระบบงาน

(2) กำหนดให้ใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) หรือวิธีพิสูจน์ตัวตนอื่นเพื่อยืนยันตัวตนจริงของผู้ใช้งานในแต่ละระดับความลับ

(3) ต้องเปลี่ยนรหัสผ่านเมื่อมีการแจ้งเตือนว่าถูกละเมิด หรือเมื่อมีการเปลี่ยนแปลงบทบาทงาน ไม่จำเป็นต้องเปลี่ยนทุก 180 วัน (ตามแนวทาง NIST)

(4) ต้องสำรองข้อมูลและระบบอย่างสม่ำเสมอ และทดสอบการกู้คืนข้อมูลและระบบอย่างน้อยปีละ 1 ครั้ง โดยกำหนดความถี่การสำรองข้อมูลอย่างชัดเจน

ข้อ 4 การใช้งานอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องปฏิบัติดังต่อไปนี้

(1) ตรวจสอบความพร้อมของคอมพิวเตอร์และอุปกรณ์ที่จะนำไปใช้งานว่าอยู่ในสภาพพร้อมใช้งาน และตรวจสอบว่าโปรแกรมที่ติดตั้งมีลิขสิทธิ์ถูกต้อง

(2) ระมัดระวังไม่ให้บุคคลภายนอกคัดลอกข้อมูลจากอุปกรณ์ที่นำไปใช้ เว้นแต่ข้อมูลนั้นจะได้รับการเผยแพร่เป็นการทั่วไป

(3) เมื่อหมดความจำเป็นต้องใช้อุปกรณ์ ให้รีบนำส่งคืนเจ้าหน้าที่ที่รับผิดชอบทันที

(4) เจ้าหน้าที่ผู้รับผิดชอบในการรับคืนต้องตรวจสอบสภาพความพร้อมใช้งานของอุปกรณ์ที่รับคืน

(5) หากความเสียหายที่เกิดขึ้นเกิดจากความประมาทอย่างร้ายแรงของผู้นำไปใช้ ผู้ใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

(6) หากอุปกรณ์สูญหายหรือถูกโจรกรรม ต้องรายงานทันทีให้ผู้ดูแลระบบและ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) เพื่อประเมินความเสี่ยงและพิจารณาการแจ้งเหตุละเมิดข้อมูล (Data Breach Notification)

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

ข้อ 1 สหกรณ์ฯให้ความสำคัญอย่างยิ่งต่อเรื่องทรัพย์สินทางปัญญาและสิทธิ์ในซอฟต์แวร์ ผู้ใช้งานสามารถขอใช้งานซอฟต์แวร์ที่หน่วยงานได้รับอนุญาตหรือมีลิขสิทธิ์ ตามหน้าที่และความจำเป็นในการปฏิบัติงาน ห้ามติดตั้งหรือใช้งานซอฟต์แวร์ใด ๆ ที่ไม่มีลิขสิทธิ์หรือเป็นซอฟต์แวร์เถื่อน

ข้อ 2 ซอฟต์แวร์ที่สหกรณ์ฯ จัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นทรัพยากรที่จำเป็นต่อการปฏิบัติงาน ห้ามถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น ห้ามคัดลอกหรือแจกจ่ายซอฟต์แวร์ให้บุคคลภายนอก หรือใช้ในกิจกรรมส่วนตัว การติดตั้งซอฟต์แวร์เพิ่มเติมต้องได้รับอนุญาตจากผู้ดูแลระบบเท่านั้น

ข้อ 3 คอมพิวเตอร์ทุกเครื่องต้องติดตั้งโปรแกรมป้องกันไวรัส (Antivirus) ตามที่สหกรณ์ฯ กำหนด ต้องเปิดใช้งานการสแกนแบบเรียลไทม์ (Real-time Scanning) และอัปเดตฐานข้อมูลไวรัสอัตโนมัติ ห้ามปิดหรือถอนการติดตั้ง Antivirus โดยไม่ได้รับอนุญาต

ข้อ 4 ข้อมูล ไฟล์ ซอฟต์แวร์ หรือสิ่งอื่นใด ที่ได้รับจากผู้ใช้งานอื่น หรือดาวน์โหลดจากภายนอก (เช่น อีเมล, USB, อินเทอร์เน็ต) ต้องได้รับการตรวจสอบไวรัสและโปรแกรมไม่ประสงค์ดี (Malware) ก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง

ข้อ 5 ผู้ใช้งานต้องดำเนินการปรับปรุงระบบปฏิบัติการ (Operating System) และซอฟต์แวร์ต่าง ๆ อย่างสม่ำเสมอ ต้องเปิดใช้งานการอัปเดตอัตโนมัติ (Automatic Update) เพื่อลดความเสี่ยงจากช่องโหว่ด้านความปลอดภัย หากใช้ระบบอัปเดตแบบกำหนดเอง ต้องตรวจสอบและติดตั้ง Patch ล่าสุดเสมอ

ข้อ 6 ผู้ใช้งานต้องระมัดระวังภัยคุกคามจากไวรัสและโปรแกรมไม่ประสงค์ดี (Malware) อยู่เสมอ หลีกเลี่ยงการคลิกลิงก์หรือเปิดไฟล์แนบจากแหล่งที่ไม่น่าเชื่อถือ เมื่อพบสิ่งผิดปกติ เช่น เครื่องทำงานช้า โปรแกรมผิดพลาด หรือมีการแจ้งเตือนผิดปกติ ต้องรายงานทันทีให้ผู้ดูแลระบบ

ข้อ 7 เมื่อผู้ใช้งานพบว่าเครื่องคอมพิวเตอร์ติดไวรัสหรือมัลแวร์ ต้องดำเนินการดังนี้ทันที ไม่เชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่เครือข่าย เพื่อป้องกันการแพร่กระจาย แจ้งผู้ดูแลระบบหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ทันที

ข้อ 8 ห้ามเผยแพร่ กระจาย หรือส่งต่อไวรัสคอมพิวเตอร์ มัลแวร์ หรือโปรแกรมอันตรายใด ๆ ที่อาจก่อให้เกิดความเสียหายต่อสินทรัพย์ไอทีของสหกรณ์ฯ ไม่ว่าจะโดยเจตนาหรือประมาท

ข้อ 9 การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก (Outsourced Software Development) ต้องดำเนินการอย่างเคร่งครัด ดังนี้

(1) ต้องมีการควบคุมโครงการพัฒนาซอฟต์แวร์โดยผู้รับจ้างจากภายนอก ทั้งในด้านเวลา คุณภาพ และความปลอดภัย

(2) ต้องระบุอย่างชัดเจนในสัญญาว่า สหกรณ์ฯ เป็นผู้มีสิทธิ์ในทรัพย์สินทางปัญญา (Intellectual Property) และซอร์สโค้ดของซอฟต์แวร์ที่พัฒนาขึ้น

(3) ต้องมีการจัดทำ ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement - DPA) เพื่อกำหนดบทบาทระหว่างสหกรณ์ฯ

(3) ต้องสงวนสิทธิ์ในการตรวจสอบคุณภาพ ความถูกต้อง และความปลอดภัยของซอฟต์แวร์ก่อนนำไปใช้งานจริง และระบุไว้ในสัญญาจ้าง

(4) ต้องมีการตรวจสอบโปรแกรมประสงค์ร้าย (Malware Scan) และการวิเคราะห์ช่องโหว่ (Vulnerability Assessment) ก่อนติดตั้งซอฟต์แวร์

(5) ผู้พัฒนาระบบจากภายนอก (Outsource) ต้องปฏิบัติตามนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยของสหกรณ์ฯ อย่างเคร่งครัด

(6) สำหรับซอฟต์แวร์ที่เกี่ยวข้องกับข้อมูลส่วนบุคคล ต้องมีการประเมินความเสี่ยงด้านความเป็นส่วนตัว (Privacy Impact Assessment: PIA) ก่อนเริ่มโครงการ

(7) ต้องมีข้อกำหนดในสัญญาเรื่องการแจ้งเหตุละเมิดข้อมูล (Breach Notification) และการรักษาความลับของข้อมูล

ส่วนที่ 9 การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

ข้อ 1 ผู้ดูแลระบบต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายน้อยที่สุด หลีกเลี่ยงการติดตั้ง Access Point ใกล้บริเวณที่เปิดเผย เช่น หน้าอาคาร หรือบริเวณที่บุคคลภายนอกสามารถเข้าถึงได้ง่าย

ข้อ 2 ผู้ดูแลระบบต้องกำหนดค่าความปลอดภัยของเครือข่ายไร้สาย (Wireless Security) ดังนี้ ห้ามใช้ WEP เนื่องจากเป็นมาตรฐานที่ล้าสมัยและมีช่องโหว่ด้านความปลอดภัย ต้องใช้มาตรฐาน WPA3-Personal หรือ WPA3-Enterprise สำหรับการเข้ารหัสข้อมูลระหว่างเครื่องลูกข่าย (Wireless LAN Client) และอุปกรณ์กระจายสัญญาณ (Access Point) หากยังไม่สามารถใช้ WPA3 ได้

ข้อ 3 ผู้ดูแลระบบต้องติดตั้งและใช้ ไฟร์วอลล์ (Firewall) แยกระหว่างระบบเครือข่ายไร้สายกับเครือข่ายภายในหน่วยงาน ต้องกำหนดนโยบายการเข้าถึง (Access Policy) อย่างเคร่งครัด เช่น ห้ามเข้าถึงเซิร์ฟเวอร์ภายในโดยตรง

ข้อ 4 ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานในระบบเครือข่ายไร้สายติดต่อสื่อสารกับเครือข่ายภายในหน่วยงานผ่านทาง VPN (Virtual Private Network) เท่านั้น

ข้อ 5 ผู้ดูแลระบบต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สาย (Wireless Intrusion Detection/Prevention System: WIDS/WIPS) แจ้งเตือนผู้ดูแลระบบเมื่อตรวจพบภัยคุกคาม

ข้อ 6 ผู้ดูแลระบบต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาตใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบเครือข่ายและระบบสารสนเทศภายในหน่วยงาน ต้องแยกเครือข่ายสำหรับผู้ใช้ภายนอก (Guest Network) ออกจากเครือข่ายภายใน เครือข่ายภายนอกต้องไม่สามารถเข้าถึงระบบภายในหรือข้อมูลส่วนบุคคลได้

<u>ส่วนที่ 10 การควบคุมการใช้งานอุปกรณ์ป้องกันเครือข่าย (Firewall Control)</u>

ข้อ 1 ทุกบริการ (Services) และเส้นทางเชื่อมต่ออินเทอร์เน็ตที่ไม่อนุญาตตามนโยบาย ต้องถูกบล็อก (Block) โดย Firewall อย่างเด็ดขาด ห้ามเปิดพอร์ตหรือบริการใด ๆ โดยไม่ผ่านกระบวนการขออนุญาตและประเมินความเสี่ยง

ข้อ 2 การกำหนดค่าบริการและการเชื่อมต่อที่อนุญาต ต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง หากมีการเปลี่ยนแปลงค่าต่าง ๆ ของ Firewall ต้องได้รับการอนุมัติจากผู้ดูแลระบบก่อนดำเนินการ

ข้อ 3 การเข้าถึงตัวอุปกรณ์ Firewall ต้องจำกัดเฉพาะผู้ที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น ต้องใช้บัญชีผู้ใช้งานเฉพาะสำหรับการดูแลระบบ (Privileged Account) ห้ามใช้บัญชีร่วมกัน (Shared Account)

ข้อ 4 ข้อมูลจราจรทางคอมพิวเตอร์ (Log) ที่เข้าออกอุปกรณ์ Firewall ต้องถูกส่งไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (SIEM หรือ Log Server) ต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า 90 วัน

ข้อ 5 การกำหนดนโยบายในการให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่าย อนุญาตให้เปิดพอร์ตการเชื่อมต่อพื้นฐานของโปรแกรมทั่วไป (เช่น HTTP, HTTPS, SMTP) เท่านั้น หากมีความจำเป็นต้องใช้งานพอร์ตอื่นนอกเหนือจากที่กำหนด ต้องได้รับความยินยอมจากผู้ดูแลระบบก่อน ต้องมีการประเมินความเสี่ยงหากพอร์ตดังกล่าวเกี่ยวข้องกับข้อมูลส่วนบุคคล

ข้อ 6 การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่าย (Server) ในแต่ละส่วนของเครือข่ายต้องอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้นการกำหนดค่าต้องขออนุญาตจากผู้ดูแลระบบ โดยต้องระบุข้อมูลดังนี้

(1) หมายเลข Port ที่ต้องการขอให้เปิด

(2) หมายเลข IP Address ของปลายทางที่ต้องการติดต่อสื่อสาร

(3) วัตถุประสงค์ หรือชื่อแอปพลิเคชันที่ต้องการใช้งานผ่าน Port นั้น ๆ

ข้อ 7 เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศภายในหน่วยงาน (Intranet) ห้ามเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ตโดยตรง เว้นแต่มีความจำเป็น

ข้อ 8 สหกรณ์ฯ มีสิทธิ์ที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายทันที หากพบพฤติกรรมการใช้งานที่ผิดหรือเสี่ยงต่อความปลอดภัยของระบบเครือข่ายส่วนรวม เช่น การส่งข้อมูลจำนวนมาก (DDoS), การติดตั้งมัลแวร์, หรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต การระงับจะดำเนินการจนกว่าจะได้รับการแก้ไขและยืนยันความปลอดภัย

ข้อ 9 การเชื่อมต่อในลักษณะของการควบคุมระยะไกล (Remote Login) จากภายนอกมายังเครื่องแม่ข่ายหรืออุปกรณ์เครือข่ายภายใน ต้องได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ 10 ผู้ละเมิดนโยบายด้านความปลอดภัยของ Firewall จะถูกระงับการให้บริการทันที จนกว่าจะได้รับการแก้ไข และอาจถูกลงโทษตามระเบียบวินัยของสหกรณ์ฯ

ข้อ 11 ต้องตรวจสอบและปิดพอร์ตของระบบหรืออุปกรณ์ที่ไม่มีความจำเป็นในการเข้าใช้งานอย่างสม่ำเสมอ อย่างน้อยสัปดาห์ละ 1 ครั้ง

<u>ส่วนที่ 11 การควบคุมการใช้อินเทอร์เน็ต (Internet)</u>

ข้อ 1 ผู้ดูแลระบบต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ตต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่สหกรณ์ฯ จัดสรรไว้เท่านั้น

ข้อ 2 เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา ก่อนทำการเชื่อมต่ออินเทอร์เน็ตผ่านเว็บเบราว์เซอร์ (Web Browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส (Antivirus) ที่ทันสมัย อุดช่องโหว่ของระบบปฏิบัติการ (Operating System) โดยติดตั้ง Patch อัปเดตล่าสุด และตรวจสอบว่าไม่มีมัลแวร์หรือซอฟต์แวร์ที่ไม่ได้รับอนุญาตก่อนเชื่อมต่อ

ข้อ 3 ในการรับส่งข้อมูลผ่านทางอินเทอร์เน็ต ต้องมีการตรวจจับไวรัส (Virus Scanning)โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง รวมถึงไฟล์แนบในอีเมล ดาวน์โหลดไฟล์ และการอัปโหลดข้อมูล ต้องมีระบบตรวจจับมัลแวร์อัตโนมัติ (Malware Detection) บนเซิร์ฟเวอร์พร็อกซีหรืออีเมลเซิร์ฟเวอร์

ข้อ 4 ห้ามใช้เครือข่ายอินเทอร์เน็ตของสหกรณ์ฯ เพื่อกระทำการต่อไปนี้

(1) หาประโยชน์ในเชิงธุรกิจส่วนตัว

(2) เพื่อความบันเทิง เช่น การเล่นเกม การดูภาพยนตร์ การฟังเพลง หรือการเข้าชมเว็บไซต์ที่ไม่เกี่ยวข้องกับงาน

(3) กระทำการที่ก่อให้เกิดความเสียหายต่อภาพลักษณ์และชื่อเสียงของสหกรณ์ฯ เช่น การเผยแพร่ข้อมูลที่อาจก่อความเสียหายต่อสหกรณ์ฯ การเปิดเผยข้อมูลสำคัญหรือข้อมูลลับของสหกรณ์ฯ ผ่านช่องทางสาธารณะ การโพสต์ข้อความในโซเชียลมีเดียในนามองค์กรโดยไม่ได้รับอนุญาต

ข้อ 5 ห้ามกระทำการใด ๆ ที่ผิดกฎหมาย หรือขัดต่อศีลธรรม

(1) นำเข้าหรือเผยแพร่ข้อมูลหรือชุดโปรแกรมที่ละเมิดลิขสิทธิ์

(2) แพร่กระจายโปรแกรมไม่ประสงค์ดี (Malware) เช่น ไวรัสคอมพิวเตอร์ ม้าโทรจัน แรนซัมแวร์

(3) กระทำการที่ไม่เหมาะสมขัดต่อศีลธรรม เช่น การเล่นพนันออนไลน์ การนำเข้าหรือเผยแพร่สื่อลามก อนาจาร

(4) กระทำการที่ส่งผลร้ายต่อความมั่นคงของชาติ ศาสนา พระมหากษัตริย์ เช่น การก่อการร้าย การเผยแพร่ข้อมูลเท็จเพื่อยุยง

(5) กระทำการข่มขู่ คุกคาม หรือละเมิดสิทธิ์ของผู้อื่น

(6) กระทำการเป็นภัยต่อสังคม เช่น การเผยแพร่ข้อมูลเท็จ (Fake News) เพื่อสร้างความสับสนวุ่นวาย การหลอกลวง (Scam) หรือการโจมตีแบบฟิชชิ่ง (Phishing) ผ่านเว็บไซต์หรืออีเมล

ข้อ 6 ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของสหกรณ์ฯ ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต โดยเฉพาะข้อมูลส่วนบุคคลของสมาชิก พนักงาน หรือข้อมูลทางการเงิน การเผยแพร่ข้อมูลต้องผ่านกระบวนการอนุมัติจากผู้มีอำนาจ และต้องปฏิบัติตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA)

ข้อ 7 ระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากระบบอินเทอร์เน็ต ต้องดาวน์โหลดเฉพาะจากแหล่งที่น่าเชื่อถือ และมีลิขสิทธิ์ถูกต้อง ห้ามติดตั้งซอฟต์แวร์ที่ไม่ผ่านการตรวจสอบความปลอดภัย การอัปเดตโปรแกรมต่าง ๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์

ส่วนที่ 12 การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล

ข้อ 1 แนวทางปฏิบัติการใช้งานทั่วไป

(1) เครื่องคอมพิวเตอร์ที่สหกรณ์ฯ อนุญาตให้ใช้งาน เป็นสินทรัพย์ของสหกรณ์ฯ เพื่อใช้ในงานสหกรณ์เท่านั้น ห้ามนำเครื่องไปใช้เพื่อประโยชน์ส่วนตัว หรือกิจกรรมที่ไม่เกี่ยวข้องกับงาน

(2) โปรแกรมที่ติดตั้งลงบนเครื่องคอมพิวเตอร์ของสหกรณ์ฯ ต้องเป็นโปรแกรมที่สหกรณ์ฯ ได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ห้ามคัดลอก แก้ไข หรือนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว ห้ามแจกจ่ายหรือเผยแพร่ซอฟต์แวร์ให้ผู้อื่นโดยไม่ได้รับอนุญาต

(2) โปรแกรมที่ติดตั้งลงบนเครื่องคอมพิวเตอร์ของสหกรณ์ฯ ต้องเป็นโปรแกรมที่สหกรณ์ฯ ได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ห้ามคัดลอก แก้ไข หรือนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว ห้ามแจกจ่ายหรือเผยแพร่ซอฟต์แวร์ให้ผู้อื่นโดยไม่ได้รับอนุญาต

(3) ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้ง หรือแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ของสหกรณ์ฯ โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

(4) ผู้ใช้งานมีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์ ต้องไม่ปล่อยเครื่องทิ้งไว้โดยไม่ล็อกหน้าจอ ต้องรายงานทันทีหากพบความผิดปกติ หากมีโปรแกรมแปลกปลอม

(5) ต้องปิดเครื่องคอมพิวเตอร์ที่ตนเองใช้งานเมื่อเลิกปฏิบัติงานประจำวัน หรือตั้งค่าให้ล็อกหน้าจออัตโนมัติเมื่อไม่มีการใช้งานเกิน 15 นาที

ข้อ 2 การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

(1) ผู้ใช้งานต้องตรวจสอบสื่อภายนอก (เช่น Flash Drive, External Hard Disk) ด้วยโปรแกรมป้องกันไวรัส ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์ ห้ามใช้สื่อที่ไม่ผ่านการสแกนไวรัส

(2) ผู้ใช้งานต้องตรวจสอบไฟล์แนบในอีเมล หรือไฟล์ที่ดาวน์โหลดจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัส ก่อนเปิดใช้งานทุกครั้ง

(3) ผู้ใช้งานต้องระมัดระวังไม่ให้เครื่องคอมพิวเตอร์ติดตั้งโปรแกรมไม่พึงประสงค์ (Malware) ที่อาจทำให้ข้อมูลสูญหาย ถูกทำลาย ถูกแก้ไข หรือระบบทำงานผิดปกติ หากพบความผิดปกติ ต้องหยุดใช้งานและแจ้งผู้ดูแลระบบทันที

ข้อ 3 การสำรองข้อมูลและการกู้คืน

(1) ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลสำคัญจากเครื่องคอมพิวเตอร์ ไปยังสื่อจัดเก็บที่ปลอดภัย เช่น เซิร์ฟเวอร์ภายใน (Network Drive) ระบบสำรองข้อมูลกลาง (Central Backup System) External Hard Disk ที่เข้ารหัส (Encrypted) Cloud Storage ที่ได้รับอนุญาตจากสหกรณ์ฯ

(2) ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่ปลอดภัย

(3) ผู้ใช้งานต้องประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ภายในเครื่องไม่ควรเป็นข้อมูลสำคัญหรือข้อมูลส่วนบุคคล เพราะหากฮาร์ดดิสก์เสียหาย อาจทำให้ข้อมูลสูญหาย

ส่วนที่ 13 การใช้งานเครื่องคอมพิวเตอร์แบบพกพา

ข้อ 1 แนวทางปฏิบัติการใช้งานทั่วไป

(1) เครื่องคอมพิวเตอร์แบบพกพาที่สหกรณ์ฯ อนุญาตให้ใช้งาน เป็นสินทรัพย์ของสหกรณ์ฯ เพื่อใช้ในงานสหกรณ์เท่านั้น ห้ามนำเครื่องไปใช้เพื่อประโยชน์ส่วนตัวหรือกิจกรรมที่ไม่เกี่ยวข้องกับงาน

(2) โปรแกรมที่ติดตั้งลงบนเครื่องคอมพิวเตอร์แบบพกพาของสหกรณ์ฯ ต้องเป็นโปรแกรมที่สหกรณ์ฯ ได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ห้ามคัดลอก แก้ไข หรือนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว ห้ามแจกจ่ายหรือเผยแพร่ซอฟต์แวร์ให้ผู้อื่นโดยไม่ได้รับอนุญาต

(3) ห้ามดัดแปลงหรือแก้ไขส่วนประกอบต่าง ๆ ของเครื่องคอมพิวเตอร์แบบพกพา ต้องรักษาสภาพของเครื่องให้เป็นไปตามสภาพเดิม ห้ามถอดเปลี่ยนฮาร์ดแวร์ เช่น RAM, SSD, หรือติดตั้งอุปกรณ์ภายนอกโดยไม่ได้รับอนุญาต

(4) ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ต้องใส่ใน กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา (Laptop Bag) ที่มีการกันกระแทก เพื่อป้องกันความเสียหายจากการตก กระทบ หรือหลุดมือ

(5) หลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่น ปลายปากกา กดหรือขีดข่วนหน้าจอ LCD ควรใช้ สไตลัสที่ออกแบบมาโดยเฉพาะ หากจำเป็นต้องสัมผัสหน้าจอ

(6) ห้ามวางของหนักหรือของมีคมทับบนหน้าจอและแป้นพิมพ์ เพื่อป้องกันการบีบอัดหรือทำให้จอภาพเสียหาย

(7) การเช็ดทำความสะอาดหน้าจอภาพ ต้องใช้ผ้าไมโครไฟเบอร์แห้งหรือเปียกหมาดเล็กน้อย ต้องเช็ดในทิศทางเดียวกัน ห้ามเช็ดแบบหมุนวน เพื่อป้องกันรอยขีดข่วน

ข้อ 2 ความปลอดภัยทางด้านกายภาพ

(1) ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหายหรือโจรกรรมของเครื่องคอมพิวเตอร์แบบพกพา ต้องล็อกหน้าจอทันทีเมื่อไม่ใช้งาน ห้ามวางเครื่องทิ้งไว้ในที่สาธารณะ เช่น ร้านกาแฟ สนามบิน หรือห้องประชุม หากต้องทิ้งไว้ชั่วคราว ต้องเก็บในล็อกเกอร์หรือพื้นที่ปลอดภัย

(2) ผู้ใช้งานต้องหลีกเลี่ยงการใช้งานหรือเก็บรักษาเครื่องคอมพิวเตอร์แบบพกพาในสถานที่ที่มีอุณหภูมิสูง (เช่น ใต้แสงแดด หรือในรถที่จอดตากแดด) ความชื้นสูง (เช่น ห้องน้ำ หรือบริเวณที่มีฝนรั่ว) ฝุ่นละอองมาก (เช่น ไซต์งานก่อสร้าง) และต้องระวังไม่ให้เครื่องตกหรือกระแทกแรง

ข้อ 3 การควบคุมการเข้าถึงระบบปฏิบัติการ

(1) ผู้ใช้งานต้องกำหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์แบบพกพา

(2) รหัสผ่านต้องมีความยาวไม่น้อยกว่า 8-16 ตัวอักษร ประกอบด้วยตัวพิมพ์ใหญ่ เลข และสัญลักษณ์ สำหรับเครื่องที่มีข้อมูลส่วนบุคคล ต้องใช้ Multi-Factor Authentication (MFA) หรือ การเข้ารหัสดิสก์ (Full Disk Encryption)

(3) ผู้ใช้งานต้องทำการ Logout หรือ ล็อกหน้าจอ ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน ระยะเวลาไม่เกิน 15 นาที สำหรับเครื่องทั่วไป

ข้อ 4 การสำรองข้อมูลและการกู้คืน

(1) ผู้ใช้งานต้องทำการสำรองข้อมูลจากเครื่องคอมพิวเตอร์แบบพกพา อย่างสม่ำเสมอ โดยใช้วิธีการและสื่อที่ปลอดภัย เช่น ระบบสำรองข้อมูลกลาง (Central Backup System) External Hard Disk

(2) ผู้ใช้งานต้องเก็บรักษาสื่อสำรองข้อมูล (Backup Media) ไว้ในสถานที่ที่ปลอดภัย ไม่เสี่ยงต่อการสูญหาย โจรกรรม หรือความเสียหาย หากสื่อสำรองมีข้อมูลส่วนบุคคล ต้องมีการ เข้ารหัสข้อมูล และจำกัดการเข้าถึง

(3) ผู้ใช้งานต้องประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ภายในเครื่องไม่ควรเป็นข้อมูลสำคัญหรือข้อมูลส่วนบุคคล เพราะหากฮาร์ดดิสก์เสียหาย อาจทำให้ข้อมูลสูญหาย ข้อมูลสำคัญควรสำรองข้อมูล

ส่วนที่ 14 การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log)

ข้อ 1 ต้องจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้อง และแท้จริง ต้องสามารถระบุตัวบุคคลที่เข้าถึงระบบ รวมถึงกิจกรรมที่กระทำ เช่น การเข้าสู่ระบบ การเข้าถึงข้อมูล การเปลี่ยนแปลงข้อมูล หรือการส่งออกข้อมูล

ข้อ 2 ห้ามแก้ไข เปลี่ยนแปลง หรือลบข้อมูลจราจรคอมพิวเตอร์ (Log) ที่เก็บรักษาไว้ ห้ามลบหรือปิดการใช้งานฟีเจอร์การบันทึก Log โดยไม่ได้รับอนุญาต หากพบการแก้ไขหรือลบ Log โดยไม่ได้รับอนุญาต ถือเป็นความผิดร้ายแรงและอาจเข้าข่ายการปกปิดการละเมิดความปลอดภัย

ข้อ 3 ต้องมีมาตรการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ อย่างเข้มงวด และจำกัดสิทธิ์การเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น ผู้ที่มีสิทธิ์เข้าถึง Log ได้แก่ ผู้ดูแลระบบ (System Administrator) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ผู้ตรวจสอบภายในหรือภายนอก (เมื่อมีการตรวจสอบ) ต้องมีการบันทึกการเข้าถึง Log ของผู้ที่มีสิทธิ์ (Audit Trail) เพื่อป้องกันการใช้ในทางที่ผิด ต้องมีการตรวจสอบความสมบูรณ์ของ Log อย่างสม่ำเสมอ

หัวข้อที่ 2
การจัดทำระบบสำรองข้อมูล

วัตถุประสงค์

1. เพื่อให้ระบบสารสนเทศของสหกรณ์ฯ สามารถให้บริการได้อย่างต่อเนื่อง และมีความมั่นคงปลอดภัย แม้เกิดเหตุขัดข้องหรือภัยพิบัติ เช่น ไฟไหม้ น้ำท่วม หรือการโจมตีทางไซเบอร์

2. เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติ และความรับผิดชอบของผู้ดูแลระบบ ในการจัดทำระบบสำรองข้อมูลอย่างเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการคุ้มครองข้อมูลส่วนบุคคล

3. เพื่อให้ผู้ใช้งานได้รับรู้ เข้าใจ และสามารถปฏิบัติตามแนวทางที่กำหนดได้อย่างถูกต้อง รวมทั้งตระหนักถึงความสำคัญของการสำรองข้อมูลในการป้องกันการสูญหายของข้อมูลสำคัญ

<u>แนวปฏิบัติการสำรองข้อมูล</u>

ข้อ 1 ต้องพิจารณาคัดเลือกระบบสารสนเทศที่สำคัญ และจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน โดยจัดลำดับความสำคัญจากมากไปน้อย ต้องมีการประเมินความเสี่ยงของระบบแต่ละประเภทเพื่อกำหนดความถี่และความต้องการในการสำรองข้อมูล

ข้อ 2 ต้องกำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ในการสำรองข้อมูลอย่างชัดเจน ระบุชื่อผู้รับผิดชอบ (Owner) และผู้ปฏิบัติงาน (Operator) สำหรับแต่ละระบบ ต้องมีการบันทึกการสำรองข้อมูล (Backup Log) และลงนามยืนยันการดำเนินการทุกครั้ง

ข้อ 3 ต้องจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของสหกรณ์ กำหนดระบบที่ต้องจัดทำระบบสำรองข้อมูล และจัดทำ แผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) อย่างน้อยปีละ 1 ครั้ง

ข้อ 4 ต้องกำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ และกำหนดความถี่ในการสำรองข้อมูล หากระบบที่มีการเปลี่ยนแปลงบ่อย ต้องเพิ่มความถี่ในการสำรองข้อมูล ต้องมีวิธีการสำรองข้อมูลดังนี้

(1) กำหนดประเภทของข้อมูลที่ต้องสำรองเก็บไว้ และความถี่ในการสำรอง

(2) กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะสำรอง

(3) จัดเก็บข้อมูลที่สำรองในสื่อจัดเก็บข้อมูล โดยต้องติดฉลากหรือบันทึกข้อมูลอย่างชัดเจน

(4) ต้องจัดเก็บข้อมูลสำรองไว้ นอกสถานที่ ระยะทางระหว่างสถานที่จัดเก็บกับสำนักงานหลักต้องเพียงพอ เพื่อป้องกันความเสียหายจากภัยพิบัติ

(5) ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่จัดเก็บข้อมูลนอกสถานที่

(6) จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้

(7) ตรวจสอบและทดสอบประสิทธิภาพของขั้นตอนการกู้คืนข้อมูลอย่างสม่ำเสมอ

ข้อ 5 มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงระบบ โครงสร้าง หรือกฎหมายที่เกี่ยวข้อง

หัวข้อที่ 3
การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ และข้อมูลส่วนบุคค

วัตถุประสงค์

1. เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศหรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดได้

2. เพื่อเป็นการป้องกันและลดระดับความเสี่ยงที่อาจจะเกิดขึ้นได้กับระบบสารสนเทศ

3. เพื่อเป็นแนวทางในการปฏิบัติหากเกิดความเสี่ยงที่เป็นอันตรายต่อระบบสารสนเทศ

4. เพื่อให้หน่วยงานสามารถระบุช่องโหว่และจุดอ่อนของระบบได้อย่างเป็นระบบ และดำเนินการแก้ไขอย่างทันท่วงที

แนวปฏิบัติ

<u>ส่วนที่ 1 การตรวจสอบและประเมินความเสี่ยง</u>

ต้องดำเนินการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ หรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดได้ ที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ โดยดำเนินการอย่างน้อยปีละ 1 ครั้ง โดยผู้ตรวจสอบภายในของสหกรณ์ฯ หรือผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยของระบบสารสนเทศ การตรวจสอบและประเมินความเสี่ยง ต้องคำนึงถึงแนวทางดังนี้

ข้อ 1 จัดลำดับความสำคัญของความเสี่ยง

ข้อ 2 ค้นหาวิธีการดำเนินการเพื่อลดความเสี่ยง

ข้อ 3 ศึกษาข้อดีข้อเสียของวิธีการดำเนินการเพื่อลดความเสี่ยง

ข้อ 4 สรุปผล ข้อเสนอแนะ และแนวทางแก้ไขเพื่อลดความเสี่ยงที่ตรวจสอบได้

ข้อ 5 มีการตรวจสอบและประเมินความเสี่ยง และให้จัดทำรายงานพร้อมข้อเสนอแนะ

ข้อ 6 มีมาตรการในการตรวจประเมินระบบสารสนเทศ อย่างน้อย ดังนี้

(1) กำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้ในรูปแบบ "อ่านอย่างเดียว" (Read-Only Access) เพื่อป้องกันการเปลี่ยนแปลงข้อมูล

(2) ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในรูปแบบอื่น (เช่น การทดสอบระบบ) ให้สร้างสำเนาข้อมูล (Data Copy) สำหรับการตรวจสอบ ต้องทำลายหรือลบข้อมูลทันทีหลังการตรวจสอบเสร็จสิ้น

(3) กำหนดให้มีการระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย

(4) กำหนดให้มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้งบันทึก Log แสดงการเข้าถึงนั้น

<u>ส่วนที่ 2 ความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ</u>

จากการติดตามตรวจสอบความเสี่ยงต่าง ๆ รวมถึงเหตุการณ์ด้านความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ สามารถแยกเป็นภัยคุกคามหลักได้ 4 ประเภท ดังนี้

ประเภทที่ 1 ภัยที่เกิดจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน (Human Error) เช่น การคลิกลิงก์ฟิชชิ่ง การเปิดไฟล์แนบมัลแวร์ การตั้งรหัสผ่านอ่อนแอ การสูญหายของอุปกรณ์ หรือการส่งข้อมูลส่วนบุคคลผิดที่ ซึ่งอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย ใช้งานไม่ได้ เกิดการชะงักงัน หรือหยุดทำงาน และส่งผลให้ไม่สามารถใช้งานระบบได้อย่างเต็มประสิทธิภาพ

แนวทางการป้องกันและลดความเสี่ยง

(1) จัดหลักสูตรเสริมสร้างความรู้ ความเข้าใจ และความตระหนักรู้ด้านไซเบอร์ (Cybersecurity Awareness) อย่างต่อเนื่อง ให้เจ้าหน้าที่ทุกคนสามารถระบุภัยคุกคาม ป้องกันตนเอง และรายงานเหตุผิดปกติได้อย่างทันท่วงที

(2) จัดหลักสูตรอบรมด้านความปลอดภัยไซเบอร์และ PDPA ให้กับเจ้าหน้าที่ของสหกรณ์ฯ อย่างสม่ำเสมอ การใช้งาน Hardware และ Software อย่างถูกต้อง, การรับรู้ภัยคุกคาม, การจัดการข้อมูลส่วนบุคคล

(3) จัดทำหนังสือแจ้งหรือคู่มือปฏิบัติงาน (Guideline) เรื่องการใช้เครื่องคอมพิวเตอร์และอุปกรณ์ รวมถึงแนวทางการล็อกเครื่องเมื่อไม่ใช้งาน การไม่เปิดไฟล์จากแหล่งที่ไม่น่าเชื่อถือ และการรายงานเหตุผิดปกติ

ประเภทที่ 2 ภัยที่เกิดจากซอฟต์แวร์ไม่ประสงค์ดี (Malicious Software) ไวรัสคอมพิวเตอร์ (Computer Virus) หนอนอินเทอร์เน็ต (Internet Worm) ม้าโทรจัน (Trojan Horse) แรนซัมแวร์ (Ransomware) ข่าวหลอกลวง (Hoax) ซอฟต์แวร์เหล่านี้อาจรบกวนการทำงาน ก่อให้เกิดความเสียหาย หรือทำให้ระบบเครือข่ายใช้งานไม่ได้

แนวทางการป้องกันและลดความเสี่ยง

(1) ติดตั้งและดูแลบำรุกรักษาระบบ ไฟร์วอลล์ (Firewall) ที่เครื่องคอมพิวเตอร์แม่ข่าย (Server) เพื่อกำหนดสิทธิ์การเข้าใช้งาน และป้องกันการบุกรุกจากภายนอก

(2) ติดตั้งซอฟต์แวร์ Antivirus และ Anti-Malware ที่เป็นปัจจุบัน พร้อมเปิดใช้งานการสแกนแบบเรียลไทม์และอัปเดตอัตโนมัติ

ประเภทที่ 3 ภัยจากไฟไหม้ หรือระบบไฟฟ้าขัดข้อง เป็นภัยร้ายแรงที่อาจทำให้สูญเสียข้อมูลถาวรและระบบหยุดให้บริการ

แนวทางการป้องกันและลดความเสี่ยง

(1) ติดตั้งอุปกรณ์สำรองไฟฟ้า (UPS) สำหรับเซิร์ฟเวอร์ ระบบเครือข่าย และอุปกรณ์สำคัญ ต้องมีการทดสอบการทำงานของ UPS

(2) ติดตั้งอุปกรณ์ดับเพลิงชนิดที่เหมาะสมสำหรับห้องเครื่อง (เช่น ระบบดับเพลิงแบบก๊าซ) ต้องมีการตรวจสอบความพร้อมของอุปกรณ์อย่างสม่ำเสมอ และจัดฝึกซ้อมดับเพลิงประจำปี

(3) ติดตั้งระบบแจ้งเตือนควันและอุณหภูมิสูงในห้องควบคุมระบบคอมพิวเตอร์

ประเภทที่ 4 ภัยจากน้ำท่วม (อุทกภัย) ความเสี่ยงต่อความเสียหายจากน้ำท่วม จัดเป็นภัยร้ายแรงที่อาจทำให้อุปกรณ์เสียหายถาวร

แนวทางการป้องกันและลดความเสี่ยง

(1) เจ้าหน้าที่ต้องดำเนินการ เคลื่อนย้ายเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายไปยังที่สูง หรือพื้นที่ปลอดภัยทันทีเมื่อมีการแจ้งเตือนอุทกภัย

(2) เมื่อน้ำลดลง ต้องให้ ช่างไฟฟ้าตรวจสอบระบบไฟฟ้า ก่อนเปิดใช้งานอุปกรณ์ เพื่อป้องกันการช็อตหรือความเสียหายเพิ่มเติม

(3) ตรวจสอบสภาพอุปกรณ์ และทำความสะอาดอย่างเหมาะสมก่อนนำกลับมาใช้งาน หากอุปกรณ์เปียกน้ำ ต้องส่งให้ผู้เชี่ยวชาญตรวจสอบก่อนใช้งาน

(4) ทำการติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย พร้อมทั้ง ทดสอบการใช้งาน ของแต่ละเครื่องและระบบเครือข่ายอย่างละเอียด

(5) เมื่อยืนยันว่าระบบสามารถให้บริการได้เรียบร้อยแล้ว ต้องแจ้งให้หน่วยงานที่เกี่ยวข้องทราบเพื่อเข้ามาใช้งานตามปกติ

หัวข้อที่ 4
การบริหารจัดการ การใช้บริการจากหน่วยงานภายนอก

วัตถุประสงค์

เพื่อให้หน่วยงานภายนอกหรือผู้ให้บริการภายนอก (Third-Party) ที่เข้ามาปฏิบัติงานหรือให้บริการกับสหกรณ์ฯ ได้ปฏิบัติตามนโยบายรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและข้อมูลส่วนบุคคลของสหกรณ์ออมทรัพย์กรมการพัฒนาชุมชน จำกัด อย่างเคร่งครัด ทำให้ระบบสารสนเทศดำเนินไปได้อย่างต่อเนื่อง มีประสิทธิภาพ และปลอดภัยจากการละเมิดข้อมูล

แนวปฏิบัติ

ข้อ 1 ต้องมีการประเมินความเสี่ยงจากการเข้าถึงข้อมูล และระบบสารสนเทศหรืออุปกรณ์ที่ใช้ในการประมวลผลโดยหน่วยงานภายนอกต้องประเมินทั้งด้านเทคนิค กระบวนการ และความเสี่ยงด้าน ข้อมูลส่วนบุคคล ต้องกำหนดมาตรการควบคุมที่เหมาะสม (เช่น การเข้ารหัสข้อมูล การใช้ MFA) ก่อนอนุญาตให้เข้าถึงข้อมูล ระบบสารสนเทศ หรืออุปกรณ์ดังกล่าว

ข้อ 2 การเข้าใช้งานระบบสารสนเทศหรือเข้าถึงข้อมูลของสหกรณ์ฯ จากหน่วยงานภายนอก ต้องมีการขออนุญาตล่วงหน้าจากสหกรณ์ฯ และต้องได้รับอนุญาตจาก ผู้จัดการ หรือผู้ดูแลระบบ ที่ได้รับมอบหมายก่อนเสมอ ต้องระบุวัตถุประสงค์ ระยะเวลาการใช้งาน และข้อมูลที่ต้องการเข้าถึง

ข้อ 3 การให้บริการและการดำเนินงานจากหน่วยงานภายนอกจะต้องปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและข้อมูลส่วนบุคคลของสหกรณ์ฯ รวมถึงแนวทางการปฏิบัติงาน มาตรฐาน และกฎข้อบังคับต่าง ๆ ต้องไม่ส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบหรือข้อมูลส่วนบุคคล

ข้อ 4 ผู้ดูแลระบบต้องให้สิทธิ์การเข้าถึงข้อมูลต่อหน่วยงานภายนอกที่ขออนุญาตและได้รับอนุมัติแล้วเท่านั้น ต้องให้สิทธิ์ตามหลัก

ข้อ 5 ต้องมีข้อตกลงในการเก็บรักษาความลับขององค์กร (Non-Disclosure Agreement: NDA) และข้อกำหนดด้านความปลอดภัยระหว่างสหกรณ์ฯ กับหน่วยงานภายนอก ก่อนเปิดให้ใช้บริการระบบเสมอ
