ระเบียบสหกรณ์ออมทรัพย์ตำรวจเพชรบุรี จำกัด
ว่าด้วย วิธีปฏิบัติในการควบคุมภายในและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของสหกรณ์
พ.ศ.2568

อาศัยอำนาจตามความในข้อบังคับของสหกรณ์ออมทรัพย์ตำรวจเพชรบุรี จำกัด 79 (8) , ข้อ 107 (10) โดยที่ประชุมคณะกรรมการดำเนินการ ชุดที่ 49 ครั้งที่ 10/2568 วันที่ 29 กรกฎาคม พ.ศ.2568 ได้มีมติกำหนดระเบียบสหกรณ์ออมทรัพย์ตำรวจเพชรบุรี จำกัด ว่าด้วย วิธีปฏิบัติในการควบคุมภายในและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของสหกรณ์ พ.ศ.2568 ดังต่อไปนี้

หมวด 1
บททั่วไป

ข้อ 1. ระเบียบนี้เรียกว่า “ระเบียบสหกรณ์ออมทรัพย์ตำรวจเพชรบุรี จำกัด ว่าด้วยวิธีปฏิบัติในการควบคุมภายในและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของสหกรณ์ พ.ศ. 2568”

ข้อ 2. ระเบียบนี้ให้ใช้บังคับตั้งแต่วันที่ 1 สิงหาคม พ.ศ. 2568 เป็นต้นไป

ข้อ 3. ในระเบียบนี้

“สหกรณ์” หมายถึง สหกรณ์ออมทรัพย์ตำรวจเพชรบุรี จำกัด

“คณะกรรมการ” หมายถึง คณะกรรมการดำเนินการสหกรณ์ออมทรัพย์ตำรวจเพชรบุรี จำกัด

“ประธานกรรมการ” หมายถึง ประธานคณะกรรมการดำเนินการสหกรณ์ออมทรัพย์ตำรวจเพชรบุรี จำกัด

“ผู้จัดการ” หมายถึง ผู้จัดการสหกรณ์ออมทรัพย์ตำรวจเพชรบุรี จำกัด

“เจ้าหน้าที่” หมายถึง เจ้าหน้าที่สหกรณ์ออมทรัพย์ตำรวจเพชรบุรี จำกัด

“บุคลากร” หมายถึง ผู้ใช้ประโยชน์จากทรัพย์สินด้านเทคโนโลยีสารสนเทศของสหกรณ์ ซึ่งครอบคลุมถึงกรรมการ เจ้าหน้าที่ สมาชิกทุกคน ตลอดจนบุคคลภายนอกที่ได้รับอนุญาตให้ทำงานในสหกรณ์ หรือที่เข้ามาดำเนินการด้านเทคโนโลยีสารสนเทศให้กับสหกรณ์ตามข้อตกลงที่ทำไว้กับสหกรณ์ หรือที่เข้ามาอบรมตามโครงการที่ผ่านความเห็นชอบจากที่ประชุมคณะกรรมการ และเจ้าหน้าที่ของรัฐผู้ดูแลการใช้โปรแกรมระบบบัญชีคอมพิวเตอร์ในการประมวลผลข้อมูล[1]

“ระบบคอมพิวเตอร์” หมายถึง เครื่องคอมพิวเตอร์ เครื่องเซิร์ฟเวอร์ อุปกรณ์เครือข่าย อุปกรณ์จัดเก็บข้อมูล หรืออุปกรณ์อื่นใดที่เกี่ยวข้องกับการประมวลผล จัดเก็บ หรือส่งผ่านข้อมูล ทั้งที่ใช้งานอยู่ภายในสหกรณ์หรือภายนอกแล้วเชื่อมต่อเข้ากับระบบเครือข่าย

“ระบบเครือข่าย” หมายถึง ระบบเครือข่ายคอมพิวเตอร์ที่สหกรณ์สร้างขึ้นทั้งแบบมีสาย (Wired Network) และไร้สาย (Wireless Network) รวมถึงการเชื่อมต่ออินเทอร์เน็ต

“ข้อมูล” หมายถึง สิ่งที่สื่อความหมายให้รู้เรื่องราว ข้อเท็จจริง หรือสิ่งใดๆ ไม่ว่าจะได้จัดทำไว้ในรูปแบบของเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยระบบคอมพิวเตอร์ หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้ รวมถึงข้อมูลส่วนบุคคลของสมาชิกและบุคลากร

“ระบบสารสนเทศ” หมายถึง ข้อมูลและสาระต่างๆ ที่เกิดจากการประมวลผลมาจากข้อมูลที่จัดไว้อย่างเป็นระบบ รวมถึงโปรแกรมคอมพิวเตอร์ แอปพลิเคชัน และโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศทั้งหมด

“ภัยคุกคามทางไซเบอร์” หมายถึง การกระทำใดๆ ที่มุ่งหมายจะทำให้เกิดความเสียหาย ขัดขวางการทำงาน หรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูล หรือระบบเครือข่ายโดยไม่ได้รับอนุญาต

ข้อ 4. วิธีการเผยแพร่ระเบียบ

(1) แจ้งให้ทราบการถือใช้ระเบียบในที่ประชุมคณะกรรมการดำเนินการ

(2) ทำหนังสือเวียนให้เจ้าหน้าที่รับทราบ

(3) ติดประกาศไว้ ณ ที่ทำการสหกรณ์เป็นระยะเวลาอย่างน้อย 60 วันนับแต่วันที่ประกาศถือใช้ระเบียบนี้

(4) เผยแพร่ผ่านช่องทางสื่อสารภายในที่เหมาะสม เช่น ระบบ Intranet, กลุ่ม Line หรือ E-mail

ข้อ 5. ในกรณีที่มีปัญหาเกี่ยวกับการปฏิบัติตามระเบียบนี้ ให้คณะกรรมการดำเนินการเป็นผู้มีอำนาจวินิจฉัย

ข้อ 6. ให้ประธานกรรมการเป็นผู้รักษาการให้เป็นไปตามระเบียบนี้

หมวด 2 วัตถุประสงค์

ข้อ 7. วัตถุประสงค์ของการออกระเบียบนี้

(1) เพื่อให้บุคลากรใช้ระบบคอมพิวเตอร์และระบบเครือข่ายอย่างรับผิดชอบ ป้องกันการกระทำที่อาจทำให้ประสิทธิภาพของระบบด้อยลง หรือก่อให้เกิดความเสียหายโดยเจตนาหรือไม่เจตนาก็ตาม

(2) เพื่อให้บุคลากรใช้เทคโนโลยีสารสนเทศอย่างถูกต้องตามบทบาทและหน้าที่ที่ได้รับมอบหมาย รวมถึงหลักการแบ่งแยกหน้าที่เพื่อความโปร่งใส

(3) เพื่อให้การใช้เทคโนโลยีสารสนเทศของสหกรณ์มีความมั่นคงปลอดภัย มีความพร้อมใช้งาน และสามารถใช้งานได้อย่างมีประสิทธิภาพและต่อเนื่อง

(4) เพื่อให้บุคลากรตระหนักถึงความเสี่ยงที่อาจเกิดขึ้นจากการใช้เทคโนโลยีสารสนเทศภัยคุกคามทางไซเบอร์ และความรับผิดชอบตามกฎหมายที่เกี่ยวข้อง (เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล)

(5) เพื่อให้สหกรณ์ได้มีการควบคุมภายในและรักษาความปลอดภัยระบบสารสนเทศที่ใช้ระบบคอมพิวเตอร์เป็นไปตามนโยบาย ระเบียบสหกรณ์ และระเบียบนายทะเบียนสหกรณ์ รวมถึงมาตรฐานการควบคุมภายในที่ดีและหลักธรรมาภิบาล

หมวด 3

การรักษาความปลอดภัยทางกายภาพและสภาพแวดล้อม

ข้อ 8. สหกรณ์จะต้องจัดตั้งระบบคอมพิวเตอร์และอุปกรณ์สำคัญ (เช่น เซิร์ฟเวอร์) ไว้ในที่ที่เหมาะสม ปลอดภัย และมีการควบคุมการเข้าถึง ห้ามผู้ไม่มีหน้าที่รับผิดชอบเข้าใช้หรือเข้าถึงโดยไม่ได้รับอนุญาต โดยควรพิจารณามาตรการดังนี้:

(1) กำหนดพื้นที่จำกัดการเข้าถึงสำหรับอุปกรณ์สำคัญ

(2) ติดตั้งระบบควบคุมการเข้าออก (Access Control System) เช่น การใช้คีย์การ์ดหรือรหัสผ่าน

(3) ติดตั้งกล้องวงจรปิด (CCTV) ในบริเวณที่มีอุปกรณ์สำคัญและจัดเก็บข้อมูลจากกล้องไว้ตามระยะเวลาที่เหมาะสม

(4) บันทึกประวัติการเข้าออกพื้นที่สำคัญ

ข้อ 9. จัดให้มีการติดตั้งอุปกรณ์ดับเพลิงที่เหมาะสมกับอุปกรณ์อิเล็กทรอนิกส์ไว้ในที่ที่เหมาะสมและสะดวกต่อการใช้งานเมื่อมีเหตุฉุกเฉิน และจัดทำแผนผังการขนย้ายอุปกรณ์คอมพิวเตอร์และเอกสารที่เกี่ยวข้อง

ข้อ 10. จัดให้มีระบบการควบคุมอุณหภูมิและความชื้นที่เหมาะสมและเพียงพอสำหรับอุปกรณ์ระบบคอมพิวเตอร์ และจัดตั้งอุปกรณ์ให้อยู่ในสถานที่ที่มีอากาศถ่ายเทได้สะดวก

ข้อ 11. จัดให้มีระบบสำรองไฟฟ้า (UPS) สำหรับเครื่องแม่ข่ายและอุปกรณ์สำคัญที่เกี่ยวข้องอย่างเพียงพอ เพื่อลดการหยุดชะงักการทำงานในกรณีที่มีไฟฟ้าดับหรือไฟตก และควรพิจารณาระบบเครื่องกำเนิดไฟฟ้า (Generator) สำหรับระบบที่สำคัญยิ่ง

หมวด 4

คณะกรรมการดำเนินการ

ข้อ 12. ต้องพิจารณาจัดให้มีทรัพยากรด้านเทคโนโลยีสารสนเทศ (บุคลากร งบประมาณและอุปกรณ์) ตามสมควรและเหมาะสมกับขนาดและความเสี่ยงของสหกรณ์ และทบทวนความเพียงพอของทรัพยากรเป็นประจำทุกปี

ข้อ 13. มอบหมายให้มีผู้รับผิดชอบในการกำกับ ติดตาม และประเมินผลการปฏิบัติตามนโยบายหรือระเบียบปฏิบัติในการควบคุมภายในและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ ของสหกรณ์อย่างสม่ำเสมอ

ข้อ 14. สื่อสารให้บุคลากรและสมาชิกเข้าใจนโยบายหรือระเบียบปฏิบัติในการควบคุมภายในและ การรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของสหกรณ์อย่างต่อเนื่อง รวมถึงการสร้างความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น

ข้อ 15. ส่งเสริมและสนับสนุนให้กรรมการ ผู้จัดการ และเจ้าหน้าที่ได้รับการฝึกอบรมหรือให้ความรู้เกี่ยวกับการป้องกันความเสี่ยงด้านเทคโนโลยีสารสนเทศ การใช้งานระบบอย่างปลอดภัยการบริหารจัดการข้อมูลส่วนบุคคล และการรักษาความลับของข้อมูลสมาชิกอย่างน้อยปีละ 1 ครั้ง หรือสนับสนุนให้เข้ารับการฝึกอบรมกับหน่วยงานและองค์กรต่างๆ ที่มีการจัดอบรมในเรื่องดังกล่าวอย่างสม่ำเสมอเพื่อสร้างวัฒนธรรมองค์กรที่ตระหนักรู้และป้องกันภัยคุกคามจากเทคโนโลยีสารสนเทศ

ข้อ 16. ต้องกำหนดให้ผู้บริการโปรแกรมระบบบัญชีจัดทำคู่มือการใช้โปรแกรมและเอกสารด้านฐานข้อมูล ได้แก่ โครงสร้างข้อมูล (Data Structure) หรือพจนานุกรมข้อมูล (Data Dictionary) และเอกสารที่เกี่ยวข้องกับการติดตั้งและการบำรุงรักษาให้กับสหกรณ์เพื่อประกอบการใช้งานโปรแกรมระบบบัญชี

ข้อ 17. มอบหมายให้มีผู้รับผิดชอบในการเก็บรักษาคู่มือและเอกสารสนับสนุนการปฏิบัติงานและเอกสารทางเทคนิคให้อยู่ในที่ปลอดภัย และให้เรียกใช้งานได้ทันทีเมื่อจำเป็น

ข้อ 18. พิจารณาคัดเลือกและจัดทำสัญญากับผู้ให้บริการโปรแกรมหรือระบบเทคโนโลยีสารสนเทศภายนอกอย่างรัดกุม โดยต้องระบุเกี่ยวกับสิทธิ์ในการเข้าถึงข้อมูลของสหกรณ์ การรักษาความลับข้อมูล (รวมถึงข้อกำหนดตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล) ขอบเขตงาน เงื่อนไขในการให้บริกา รมาตรฐานความปลอดภัยทางเทคนิค และบทลงโทษหรือแนวทางดำเนินคดีหากผู้ให้บริการไม่ปฏิบัติตามสัญญาและหลักเกณฑ์ที่เกี่ยวข้อง

ข้อ 19. แต่งตั้งเจ้าหน้าที่ หรือบุคลากรที่มีความรู้ความเชี่ยวชาญเพื่อรับผิดชอบ ด้านเทคโนโลยีสารสนเทศของสหกรณ์อย่างชัดเจน และอาจพิจารณาการแต่งตั้งคณะทำงานด้าน IT Security ตามความเหมาะสม

ข้อ 20. จัดให้มีการจัดทำ ทบทวน และทดสอบแผนฉุกเฉิน (Disaster Recovery Plan - DRP และ Business Continuity Plan - BCP) สำหรับระบบสารสนเทศที่สำคัญอย่างน้อยปีละ 1 ครั้ง และนำผลการทดสอบมาปรับปรุงแผนอย่างต่อเนื่อง

ข้อ 21. รณรงค์ให้บุคลากรใช้พลังงานไฟฟ้าอย่างประหยัดและใช้ทรัพยากร IT อย่างมีประสิทธิภาพ รวมถึงการพิจารณามาตรการลดการใช้กระดาษและส่งเสริมการใช้เอกสารอิเล็กทรอนิกส์

ข้อ 22. จัดให้มีการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Assessment) อย่างเป็นระบบและสม่ำเสมอ เพื่อระบุ วิเคราะห์ และประเมินความเสี่ยงด้านไซเบอร์ที่อาจเกิดขึ้นกับระบบและข้อมูลของสหกรณ์

หมวด 5

ผู้จัดการสหกรณ์ / ผู้ดูแลระบบงาน / เจ้าหน้าที่ IT

ข้อ 23. ควบคุมดูแลการใช้ระบบเทคโนโลยีสารสนเทศให้เป็นไปตามวัตถุประสงค์ นโยบายและระเบียบที่เกี่ยวข้องอย่างเคร่งครัด รวมถึงการบังคับใช้นโยบายการใช้งานที่ยอมรับได้ (Acceptable Use Policy) สำหรับอุปกรณ์และระบบของสหกรณ์

ข้อ 24. ดำเนินการให้ระบบเทคโนโลยีสารสนเทศของสหกรณ์ทำงานได้อย่างมีประสิทธิภาพทันสมัย และมั่นคงปลอดภัยตามนโยบายการรักษาความปลอดภัยของสหกรณ์

ข้อ 25. ติดตั้งและกำหนดค่าความปลอดภัยของระบบบัญชีคอมพิวเตอร์และระบบเครือข่ายให้สามารถป้องกันบุคคลที่ไม่ได้รับอนุญาตเข้าสู่ระบบได้อย่างมีประสิทธิภาพ โดยมีมาตรการดังนี้:

(1) กำหนดความยาวและความซับซ้อนของรหัสผ่าน (Password Complexity) อย่างน้อย 8 ตัวอักษร ประกอบด้วยตัวอักษรพิมพ์เล็ก พิมพ์ใหญ่ ตัวเลข และอักขระพิเศษ

(2) กำหนดระยะเวลาการเปลี่ยนแปลงรหัสผ่านอย่างสม่ำเสมอ (เช่น ทุก 90 วัน) และห้ามใช้รหัสผ่านซ้ำเดิมภายในระยะเวลาที่กำหนดอย่างน้อย 3 รหัสที่ผ่านมา

(3) กำหนดระยะเวลาการตั้งเวลาพักหน้าจอ (Screen Lock) ในกรณีผู้ใช้งานไม่อยู่ที่เครื่อง (เช่น 5-10 นาที) และกำหนดให้ต้องใส่รหัสผ่านเพื่อปลดล็อก

(4) พิจารณาและดำเนินการใช้งานการยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication - MFA) สำหรับการเข้าถึงระบบที่สำคัญและข้อมูลอ่อนไหว

(5) ตรวจสอบและแก้ไขช่องโหว่ความปลอดภัยของระบบปฏิบัติการและซอฟต์แวร์ที่ใช้งาน (Patch Management) อย่างสม่ำเสมอและทันท่วงทีที่ตรวจพบช่องโหว่

ข้อ 26. มีหน้าที่รับผิดชอบในการบริหารจัดการผู้ใช้งานเกี่ยวกับการสร้าง/เปลี่ยนแปลง/ลบชื่อผู้ใช้งาน (username) โดยการกำหนดสิทธิการใช้งานจะต้องเป็นไปตามหลักการกำหนดสิทธิ์ตามบทบาท (Role-Based Access Control) และหลักการสิทธิ์ขั้นต่ำที่จำเป็น (Principle of Least Privilege) เพื่อลดโอกาสที่บุคคลภายนอกหรือโปรแกรมเมอร์เข้าถึงระบบงานและข้อมูลโดยไม่ได้รับอนุญาต

ข้อ 27. มีหน้าที่สอบทานสิทธิ์การใช้งานของเจ้าหน้าที่ในระบบบัญชีคอมพิวเตอร์และระบบเครือข่ายให้สอดคล้องกับหน้าที่ความรับผิดชอบในแต่ละตำแหน่งเป็นประจำอย่างน้อยปีละ 1 ครั้ง และทำการเพิกถอนสิทธิ์การเข้าถึงทั้งหมดของบุคลากรที่พ้นจากตำแหน่งหรือลาออกโดยทันที

ข้อ 28. บริหารจัดการระบบเครือข่ายและระบบคอมพิวเตอร์ให้มีความมั่นคงปลอดภัยมีประสิทธิภาพ ครอบคลุมพื้นที่การทำงานทั้งหมด ได้แก่

(1) กำหนดสิทธิ์การเข้าถึงระบบเครือข่ายและทรัพยากรบนเครือข่ายให้กับผู้ที่ได้รับอนุญาตเท่านั้น

(2) จัดทำการปรับปรุงแผนผังเครือข่ายและอุปกรณ์ที่เกี่ยวข้องให้เป็นปัจจุบันอยู่เสมอ

(3) มีการตรวจสอบหรือเฝ้าระวังเกี่ยวกับการรักษาความปลอดภัยระบบคอมพิวเตอร์และระบบเครือข่ายอย่างสม่ำเสมอ (เช่น การตรวจสอบ Log, การเฝ้าระวังการบุกรุกโดยระบบ SIEM)

(4) ติดตั้งและปรับปรุงระบบป้องกันไวรัส (Antivirus), ระบบป้องกันมัลแวร์ (Antimalware), ระบบ Firewall, และระบบ Intrusion Detection/Prevention System (IDS/IPS) บนเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องลูกข่ายให้เป็นปัจจุบันสม่ำเสมอ

(5) พิจารณาการเข้ารหัสข้อมูล (Data Encryption) ทั้งในขณะจัดเก็บ (Data at Rest) และในขณะส่งผ่าน (Data in Transit) สำหรับข้อมูลที่มีความสำคัญสูง โดยเฉพาะข้อมูลส่วนบุคคล

(6) ดำเนินการสแกนช่องโหว่ (Vulnerability Scanning) และอาจจ้างผู้เชี่ยวชาญภายนอกมาทำการทดสอบเจาะระบบ (Penetration Testing) อย่างน้อยปีละ 1 ครั้ง

ข้อ 29. จัดทำตารางแผนการสำรองข้อมูล (Backup Plan) และวิธีการกู้คืนข้อมูล (Recovery Procedure) ที่ชัดเจน และให้มีการสำรองข้อมูลและการทดสอบการกู้คืนข้อมูลเป็นไปตามแผนที่กำหนด ได้แก่

(1) กำหนดตารางแผนการสำรองข้อมูลให้เหมาะสมกับการปฏิบัติงานของสหกรณ์ โดยคำนึงถึงความถี่และความสำคัญของข้อมูล (เช่น ข้อมูลที่มีความสำคัญสูงอาจสำรองแบบต่อเนื่อง)

(2) กำหนดให้สำรองข้อมูลจากระบบบัญชีคอมพิวเตอร์ที่สหกรณ์ใช้ในเครื่องคอมพิวเตอร์ที่แยกต่างหากจากเครื่องแม่ข่ายหลักของสหกรณ์อย่างน้อย 1 ชุดเป็นประจำทุกวันทำการ และสำรองข้อมูลไว้ในสื่อบันทึกข้อมูลภายนอก (Offsite Backup) อย่างน้อย 1 ชุด เป็นประจำทุกเดือน โดยจัดเก็บในสถานที่ที่ปลอดภัยและมีระบบควบคุมการเข้าถึง

(3) กำหนดให้สำรองโปรแกรม ระบบปฏิบัติการ ระบบฐานข้อมูล และระบบบัญชีคอมพิวเตอร์ (Software/System Backup) ไว้ในสื่อบันทึกข้อมูลอย่างน้อย 1 ชุด เป็นประจำทุก 3 เดือน

(4) ให้เจ้าหน้าที่ผู้รับผิดชอบระบบงานสำรองข้อมูลในสื่อบันทึกข้อมูลและติดฉลากที่มีรายละเอียดโปรแกรมระบบงาน วันเดือนปี จำนวนหน่วยข้อมูล และข้อมูลที่เกี่ยวข้อง

(5) จัดเก็บสื่อบันทึกข้อมูลสำรองไว้ในที่ปลอดภัย ทั้งในสำนักงานสหกรณ์และสถานที่สำรองภายนอกสำนักงาน (Offsite) และให้สามารถนำมาใช้งานได้ทันทีในกรณีที่มีเหตุฉุกเฉิน

(6) ผู้จัดการหรือผู้ที่ได้รับมอบหมายต้องทดสอบการกู้คืนข้อมูลจากชุดสำรองอย่างน้อยทุก 6 เดือน และเก็บรักษาชุดสำรองข้อมูลไว้อย่างน้อย 10 ปี หรือตามที่กฎหมายกำหนด

(7) จัดทำทะเบียนคุมข้อมูลชุดสำรองและควบคุมการนำข้อมูลชุดสำรองออกมาใช้งานโดยมีการบันทึกเหตุผล รายละเอียด และผลกระทบของการเรียกคืนข้อมูลทุกครั้ง

(8) เมื่อสหกรณ์มีการแก้ไขหรือปรับปรุงข้อมูลในระบบ ต้องได้รับความเห็นชอบจากผู้มีอำนาจและต้องบันทึกรายละเอียดการแก้ไขข้อมูลไว้ เช่น ใครเป็นผู้แก้ไข แก้ไขเมื่อใด แก้ไขอะไร และเหตุผลในการแก้ไข เพื่อให้สามารถตรวจสอบย้อนหลังได้

ข้อ 30. จัดทำแผนฉุกเฉินรองรับเมื่อเกิดปัญหากับระบบเทคโนโลยีสารสนเทศในกรณีระบบคอมพิวเตอร์ได้รับความเสียหาย หรือหยุดชะงัก และกำหนดผู้รับผิดชอบที่ชัดเจน โดยครอบคลุมถึง:

(1) ขั้นตอนการตอบสนองต่อเหตุการณ์ (Incident Response) ตั้งแต่การตรวจจับการวิเคราะห์การกักกัน การกำจัด การฟื้นฟู และการเรียนรู้จากเหตุการณ์

(2) บทบาทและหน้าที่ของทีมตอบสนองเหตุการณ์ (Incident Response Team)

(3) แนวทางการสื่อสารภายในและภายนอก (เช่น การแจ้งสมาชิกหรือหน่วยงานกำกับดูแลหากข้อมูลส่วนบุคคลรั่วไหล)

ข้อ 31. ดำเนินการทดสอบแผนฉุกเฉินร่วมกับบุคลากรที่เกี่ยวข้องอย่างน้อยปีละ 1 ครั้ง และจัดทำผลการทดสอบพร้อมข้อเสนอแนะเพื่อปรับปรุง

ข้อ 32. จัดการกับเหตุการณ์ผิดปกติที่เกี่ยวข้องกับความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ (เช่น การบุกรุก, ข้อมูลรั่วไหล, มัลแวร์เรียกค่าไถ่) โดยทันทีที่ได้รับรายงานจากบุคลากร หรือตรวจพบจากระบบ และมีการจัดทำรายงานเหตุการณ์และแนวทางแก้ไข เพื่อป้องกันไม่ให้เกิดเหตุการณ์ซ้ำ

ข้อ 33. จัดทำทะเบียนทรัพย์สินสารสนเทศ (Information Asset Inventory) ที่ครอบคลุมทั้งฮาร์ดแวร์ ซอฟต์แวร์ และข้อมูลสำคัญ โดยระบุเจ้าของ (Owner) ความสำคัญ (Criticality) และระดับการจำแนกข้อมูล (Classification) เพื่อให้สามารถบริหารจัดการและป้องกันได้อย่างเหมาะสม

ข้อ 34. กำหนดกระบวนการบริหารจัดการการเปลี่ยนแปลง (Change Management) สำหรับการเปลี่ยนแปลงใดๆ ที่มีผลต่อระบบสารสนเทศ เพื่อให้มั่นใจว่าการเปลี่ยนแปลงเหล่านั้นจะไม่ส่งผลกระทบต่อความมั่นคงปลอดภัยหรือประสิทธิภาพของระบบโดยไม่ได้ตั้งใจ

หมวด 6
บุคลากร

ข้อ 35. ต้องใช้ระบบคอมพิวเตอร์และระบบสารสนเทศเพื่อประโยชน์สูงสุดต่อการดำเนินงานของสหกรณ์และเป็นไปตามวัตถุประสงค์ที่กำหนดเท่านั้น ห้ามนำไปใช้ในทางที่มิชอบ ก่อให้เกิดความเสียหาย หรือใช้เพื่อประโยชน์ส่วนตนโดยไม่ได้รับอนุญาต

ข้อ 36. ให้คำนึงถึงการใช้งานอย่างประหยัดและหมั่นตรวจสอบระบบคอมพิวเตอร์และอุปกรณ์ของตนเองให้อยู่ในสภาพสมบูรณ์และพร้อมใช้งาน หากพบความผิดปกติให้แจ้งผู้ดูแลระบบงานทันที

ข้อ 37. บุคลากรแต่ละคนมีหน้าที่ป้องกันดูแลรักษาข้อมูลชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) รวมถึงรหัสผ่านอื่นๆ ที่เกี่ยวข้องกับการเข้าถึงระบบและข้อมูล โดยห้ามเผยแพร่ให้ผู้อื่นล่วงรู้รหัสผ่านของตนเองเป็นอันขาด และห้ามบันทึกรหัสผ่านไว้ในที่ที่ผู้อื่นสามารถเข้าถึงได้ง่าย

ข้อ 38. การกำหนดรหัสผ่านในการเข้าถึงระบบเทคโนโลยีสารสนเทศต้องเป็นไปตามข้อกำหนดในข้อ 25 (1) และให้มีการเปลี่ยนแปลงรหัสผ่านของผู้ใช้งานทุกๆ 90 วัน (ตามข้อ 25 (2)

ข้อ 39. บุคลากรแต่ละคนห้ามใช้ชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) ของบุคคลอื่นมาใช้งานไม่ว่าจะได้รับอนุญาตจากผู้ใช้งานนั้นหรือไม่ก็ตาม

ข้อ 40. ห้ามติดตั้งซอฟต์แวร์ใดๆ ที่ไม่ได้รับอนุญาตจากผู้ดูแลระบบ หรือนำอุปกรณ์ส่วนตัว (เช่น USB Drive, External Hard Drive) มาเชื่อมต่อกับระบบคอมพิวเตอร์ของสหกรณ์โดยไม่ได้รับการตรวจสอบด้านความปลอดภัยจากเจ้าหน้าที่ IT

ข้อ 41. บุคลากรทุกคนต้องปฏิบัติตามนโยบายการรักษาความปลอดภัยข้อมูลส่วนบุคคลอย่างเคร่งครัด รวมถึงการจัดการข้อมูลสมาชิกและบุคลากรให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

ข้อ 42. การใช้งานเครื่องคอมพิวเตอร์หรืออุปกรณ์ใดๆ ของสหกรณ์ ผู้ใช้งานต้องรับผิดชอบในฐานะเป็นผู้ถือครองเครื่องนั้นๆ และต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้นอันเนื่องมาจากการใช้งานที่ผิดปกติหรือการไม่ปฏิบัติตามระเบียบนี้

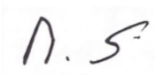
ข้อ 43. เมื่อพบเหตุการณ์ผิดปกติที่เกี่ยวกับความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ เช่น การบุกรุก, ไวรัส, ข้อมูลสูญหาย, มัลแวร์เรียกค่าไถ่ ให้รีบแจ้งให้ผู้จัดการ / ผู้ดูแลระบบงาน / เจ้าหน้าที่ IT ของสหกรณ์โดยทันที

บทลงโทษ

ข้อ 44. บุคลากรผู้ใดฝ่าฝืนหรือไม่ปฏิบัติตามระเบียบนี้ ให้ได้รับโทษทางวินัยตามที่สหกรณ์กำหนด และ/หรือ ถูกดำเนินคดีตามกฎหมายที่เกี่ยวข้อง (เช่น พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์, พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล)

ให้คณะกรรมการดำเนินการเป็นผู้รักษาการตามระเบียบนี้

ประกาศ ณ วันที่ 1 สิงหาคม พ.ศ. 2568

พลตำรวจตรี 

(กิตติ สุขสมภักดิ์)

ประธานกรรมการ

สหกรณ์ออมทรัพย์ตำรวจเพชรบุรีจำกัด