ระเบียบ
สหกรณ์ออมทรัพย์วชิรพยาบาล จำกัด
ว่าด้วยการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ
พ.ศ. 2554

****

อาศัยอำนาจตามความในข้อบังคับของสหกรณ์ ข้อ 58 (9) และข้อ 83 (13) ที่ประชุมคณะกรรมการดำเนินการสหกรณ์ออมทรัพย์วชิรพยาบาล จำกัด ชุดที่ 38 ครั้งที่ 5/2554 เมื่อวันศุกร์ที่ 18 กุมภาพันธ์ 2554 ได้มีมติให้กำหนดระเบียบสหกรณ์ออมทรัพย์วชิรพยาบาล จำกัด ว่าด้วยการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ พ.ศ. 2554 ดังต่อไปนี้

ข้อ 1. ระเบียบนี้เรียกว่า “ระเบียบสหกรณ์ออมทรัพย์วชิรพยาบาล จำกัด ว่าด้วยการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ พ.ศ. 2554”

ข้อ 2. ระเบียบนี้ให้ใช้บังคับตั้งแต่ วันที่ 18 กุมภาพันธ์ 2554 เป็นต้นไป

ข้อ 3. ให้ยกเลิก ระเบียบ ประกาศ คำสั่ง และมติอื่นใดในส่วนที่กำหนดไว้แล้วในระเบียบนี้ หรือซึ่งขัด หรือแย้งกับระเบียบนี้ให้ใช้ระเบียบนี้แทน

ข้อ 4. ในระเบียบนี้

“สหกรณ์”	หมายถึง	สหกรณ์ออมทรัพย์วชิรพยาบาล จำกัด
“ผู้บริหารสหกรณ์”	หมายถึง	คณะกรรมการดำเนินการสหกรณ์ออมทรัพย์วชิรพยาบาล จำกัด
“ประธานกรรมการ”	หมายถึง	ประธานกรรมการดำเนินการสหกรณ์ออมทรัพย์วชิรพยาบาล จำกัด
“ผู้จัดการ”	หมายถึง	ผู้จัดการสหกรณ์ออมทรัพย์วชิรพยาบาล จำกัด
“ผู้ดูแลระบบ”	หมายถึง	ผู้ช่วยผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ
“ผู้ใช้งาน”	หมายถึง	เจ้าหน้าที่สหกรณ์ออมทรัพย์วชิรพยาบาล จำกัด

หมวดที่ 1
ว่าด้วยการพิสูจน์ตัวตน
(ACCOUNTABILITY, IDENTIFICATION AND AUTHENTICATION)

ข้อ 5. ผู้ใช้งานมีหน้าที่ในการป้องกัน ดูแลรักษาข้อมูลบัญชีชื่อผู้ใช้งาน (USERNAME) และรหัสผ่าน (PASSWORD) โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งาน (USERNAME) ของตนเอง ห้ามใช้ร่วมกับผู้อื่นรวมทั้งห้ามทำการเผยแพร่ แจกจ่าย หรือกระทำการใด ๆ ทำให้ผู้อื่นล่วงรู้รหัสผ่าน (PASSWORD)

ข้อ 6. ผู้ใช้งานต้องรับผิดชอบต่อการกระทำใด ๆ ที่เกิดจากบัญชีของผู้ใช้งาน (USERNAME) ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม

ข้อ 7. ผู้ใช้งานต้องตั้งรหัสผ่านให้เกิดความปลอดภัย โดยรหัสผ่านประกอบด้วยตัวอักษรไม่น้อยกว่า 8 ตัวอักษร ซึ่งต้องประกอบด้วยตัวเลข (NUMERICAL CHARACTER) ตัวอักษร (ALPHABET) และตัวอักษรพิเศษ (SPECIAL CHARACTER)

ข้อ 8. ผู้ใช้งานต้องไม่ใช้งานรหัสผ่านซึ่งเคยใช้มาแล้ว อย่างน้อย 5 รหัสผ่าน

ข้อ 9. ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (PASSWORD) ทุก ๆ 60 วันหรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน

ข้อ 10. ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้ทรัพย์สินหรือด้านเทคโนโลยีสารสนเทศของสหกรณ์และหากการพิสูจน์ตัวตนนั้นมีปัญหา ไม่ว่าจะเกิดจากรหัสผ่าน การโดนล็อคก็ดี หรือเกิดจากความผิดพลาดใด ๆ ก็ดี ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันที โดย

10.1 คอมพิวเตอร์โน้ตบุ๊ก (NOTEBOOK) ต้องทำการพิสูจน์ตัวตนในระดับไบออส (BIOS) ก่อนการใช้งาน

10.2 คอมพิวเตอร์ทุกประเภท ก่อนการเข้าถึงระบบปฏิบัติการต้องทำการพิสูจน์ตัวตนทุกครั้ง

10.3 การใช้งานระบบคอมพิวเตอร์อื่นในเครือข่ายจะต้องทำการพิสูจน์ตัวตนทุกครั้ง

10.4 การใช้งานอินเทอร์เน็ต (INTERNET) ต้องทำการพิสูจน์ตัวตนและต้องมีการบันทึกข้อมูลซึ่งสามารถบ่งบอกตัวตนบุคคลผู้ใช้งานได้

10.5 เมื่อผู้ใช้งานไม่อยู่ที่เครื่องคอมพิวเตอร์ เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการล็อคหน้าจอทุกครั้ง และต้องทำการพิสูจน์ตัวตนก่อนการใช้งานทุกครั้ง

10.6 เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการตั้งเวลาพักหน้าจอ (SCREEN SAVER) โดยตั้งเวลาอย่างน้อย 15 นาที

หมวดที่ 2
ว่าด้วยการบริหารจัดการทรัพย์สิน
(ASSETS MANAGEMENT)

ข้อ 11. ผู้ใช้งานต้องไม่เข้าไปในห้องคอมพิวเตอร์แม่ข่าย (SERVER) สหกรณ์ที่เป็นเขตหวงห้ามโดยเด็ดขาด เว้นแต่ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ 12. ผู้ใช้งานต้องไม่นำอุปกรณ์หรือชิ้นส่วนใดออกจากห้องคอมพิวเตอร์แม่ข่าย (SERVER) เว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ 13. ผู้ใช้งานต้องไม่นำเครื่องมือ หรืออุปกรณ์อื่นใดเชื่อมเข้าเครือข่ายเพื่อการประกอบธุรกิจส่วนบุคคล

ข้อ 14. ผู้ใช้งานต้องไม่ใช้ หรือลบแฟ้มข้อมูลของผู้อื่นไม่ว่ากรณีใด ๆ

ข้อ 15. ผู้ใช้งานต้องไม่คัดลอกหรือทำสำเนาแฟ้มข้อมูลที่มีลิขสิทธิ์กำกับการใช้งาน ก่อนได้รับอนุญาต

ข้อ 16. ผู้ใช้งานมีหน้าที่ต้องรับผิดชอบต่อทรัพย์สินที่สหกรณ์มอบไว้ให้ใช้งานเสมือนหนึ่งเป็นทรัพย์สินของผู้ใช้งานเอง โดยบรรดารายการทรัพย์สิน (ASSET LISTS) ที่ผู้ใช้งานต้องรับผิดชอบจะอยู่แนบท้ายเอกสารข้อบังคับนี้ การรับหรือคืนทรัพย์สินจะถูกบันทึกและตรวจสอบทุกครั้งโดยเจ้าหน้าที่ที่สหกรณ์มอบหมาย

ข้อ 17. กรณีทำงานนอกสถานที่ผู้ใช้งานต้องดูแลและรับผิดชอบทรัพย์สินของสหกรณ์ที่ได้รับมอบหมาย

ข้อ 18. ผู้ใช้งานมีหน้าที่ต้องชดใช้ค่าเสียหายไม่ว่าทรัพย์สินนั้นจะชำรุด หรือสูญหายตามมูลค่าทรัพย์สิน หากความเสียหายนั้นเกิดจากความประมาทของผู้ใช้งาน

ข้อ 19. ผู้ใช้งานต้องไม่ให้ผู้อื่นยืมคอมพิวเตอร์ หรือโน้ตบุ๊ก ไม่ว่ากรณีใด ๆ เว้นแต่การยืมนั้นได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้มีอำนาจ

ข้อ 20. ทรัพย์สินและด้านเทคโนโลยีสารสนเทศต่าง ๆ ที่สหกรณ์จัดเตรียมไว้ให้ใช้งานมีวัตถุประสงค์เพื่อการใช้งานของสหกรณ์เท่านั้น ห้ามมิให้ผู้ใช้งานนำทรัพย์สินและด้านเทคโนโลยีสารสนเทศต่าง ๆ ไปใช้ในกิจกรรมที่สหกรณ์ไม่ได้กำหนด หรือทำให้เกิดความเสียหายต่อสหกรณ์

ข้อ 21. ความเสียหายใด ๆ ที่เกิดจากการละเมิดตามข้อ 16 ให้ถือเป็นความผิดส่วนบุคคลโดยผู้ใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

หมวดที่ 3
ว่าด้วยการบริหารจัดการข้อมูลองค์กร
(CORPORATE MANAGEMENT)

ข้อ 22. ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูล ไม่ว่าข้อมูลนั้นจะเป็นของสหกรณ์หรือเป็นข้อมูลของบุคคลภายนอก

ข้อ 23. ข้อมูลทั้งหลายที่อยู่ภายในทรัพย์สินของสหกรณ์ ถือเป็นทรัพย์สินของสหกรณ์ ห้ามไม่ให้ทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย โดยไม่ได้รับอนุญาตจากผู้บริหารสหกรณ์

ข้อ 24. ผู้ใช้งานมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลของสหกรณ์ หรือข้อมูลของผู้รับบริการ หากเกิดการสูญหาย โดยนำไปใช้ในทางที่ผิด การเผยแพร่โดยไม่รับอนุญาต ผู้ใช้งานต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้นด้วย

ข้อ 25. ผู้ใช้งานต้องป้องกัน ดูแล รักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูล

ข้อ 26. ผู้ใช้งานมีสิทธิโดยชอบธรรมที่จะเก็บ รักษา ใช้งานและป้องกันข้อมูลส่วนบุคคลตามเห็นสมควร สหกรณ์จะให้การสนับสนุนและเคารพต่อสิทธิ์ส่วนบุคคล และไม่อนุญาตให้บุคคลหนึ่งบุคคลใดทำการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้น ยกเว้นในกรณีที่สหกรณ์ต้องการตรวจสอบข้อมูลหรือ คาดว่าข้อมูลนั้นเกี่ยวข้องกับสหกรณ์ ซึ่งสหกรณ์อาจแต่งตั้งให้ผู้ทำหน้าที่ตรวจสอบ ทำการตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลา โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

หมวดที่ 4
ว่าด้วยการบริหารจัดการด้านเทคโนโลยีสารสนเทศ
(IT INFRASTRUCTURE MANAGEMENT)

ข้อ 27. ผู้ใช้งานมีสิทธิที่จะพัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ แต่ต้องไม่ดำเนินการ ดังนี้

27.1 พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ที่จะทำลายกลไกรักษาความปลอดภัยระบบรวมทั้งการกระทำในลักษณะเป็นการแอบใช้รหัสผ่าน การลักลอบทำสำเนาข้อมูลบุคคลอื่นหรือแกะรหัสผ่านของบุคคลอื่น

27.2 พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ซึ่งทำให้ผู้ใช้มีสิทธิและลำดับความสำคัญในการครอบครองทรัพยากรระบบมากกว่าผู้ใช้อื่น

27.3 พัฒนาโปรแกรมใดที่จะทำซ้ำตัวโปรแกรมหรือแฝงตัวโปรแกรมไปกับโปรแกรมอื่นในลักษณะเช่นเดียวกับหนอน หรือไวรัสคอมพิวเตอร์

27.4 พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ที่จะทำลายระบบจำกัดสิทธิ์การใช้ (LICENSE) ซอฟต์แวร์

27.5 นำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์แสดงข้อความรูปภาพไม่เหมาะสม หรือขัดต่อศีลธรรมประเพณีอันดีงามของประเทศไทย กรณีที่ผู้ใช้สร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์

ข้อ 28. ห้ามติดตั้งอุปกรณ์หรือกระทำการใดเพื่อให้สามารถเข้าถึงด้านเทคโนโลยีสารสนเทศของสหกรณ์โดยไม่ได้รับอนุญาตจากผู้มีอำนาจ

หมวดที่ 5
ว่าด้วยซอฟต์แวร์และลิขสิทธิ์
(SOFTWARE LICENSING AND INTELLECTUAL PROPERTY)

ข้อ 29. สหกรณ์ ได้ให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญา ดังนั้นซอฟต์แวร์ที่สหกรณ์อนุญาตให้ใช้งานหรือที่สหกรณ์ มีลิขสิทธิ์ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และสหกรณ์ห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากมีการตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ์ สหกรณ์ถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงผู้เดียว

ข้อ 30. ซอฟต์แวร์ (SOFTWARE) ที่สหกรณ์ได้จัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็นต่อการทำงาน ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น

หมวดที่ 6
การป้องกันโปรแกรมไม่ประสงค์ดี
(PREVENTING MALWARE)

ข้อ 31. คอมพิวเตอร์ของผู้ใช้งานติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (ANTIVIRUS) ตามที่สหกรณ์ได้ประกาศให้ใช้ เว้นแต่คอมพิวเตอร์นั้นเป็นเครื่องเพื่อการศึกษา พัฒนา ระบบป้องกัน โดยต้องได้รับอนุญาตจากผู้บริหารสหกรณ์

ข้อ 32. บรรดาข้อมูล ไฟล์ ซอฟต์แวร์ หรือสิ่งอื่นใด ที่ได้รับจากผู้ใช้งานอื่นต้องได้รับการตรวจสอบไวรัสคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดีก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง

ข้อ 33. ผู้ใช้งานต้องทำการปรับปรุงข้อมูล สำหรับตรวจสอบและปรับปรุงระบบปฏิบัติการ (UPDATE PATCH) ให้ใหม่เสมอ เพื่อเป็นการป้องกันความเสียหายที่อาจเกิดขึ้น

ข้อ 34. ผู้ใช้งานต้องพึงระวังไวรัสและโปรแกรมไม่พึงประสงค์ดีตลอดเวลา รวมทั้งเมื่อพบสิ่งผิดปกติผู้ใช้งานต้องแจ้งเหตุแก่ผู้ดูแลระบบ

ข้อ 35. เมื่อผู้ใช้งานพบว่าเครื่องคอมพิวเตอร์ติดไวรัส ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่เครือข่าย และต้องแจ้งแก่ผู้ดูแลระบบ

ข้อ 36. ห้ามลักลอบทำสำเนา เปลี่ยนแปลง ลบทิ้ง ซึ่งข้อมูล ข้อความ เอกสาร หรือสิ่งใด ๆ ที่เป็นทรัพย์สินของสหกรณ์ หรือของผู้อื่น โดยไม่ได้รับอนุญาตจากผู้มีอำนาจ

ข้อ 37. ห้ามทำการเผยแพร่ไวรัสคอมพิวเตอร์ มัลแวร์ หรือโปรแกรมอันตรายใด ๆ ที่อาจก่อให้เกิดความเสียหายมาสู่ทรัพย์สินของสหกรณ์

หมวดที่ 7
การรักษาความปลอดภัยของเครือข่ายไร้สาย
(WIRELESS POLICY)

ข้อ 38. ผู้ดูแลระบบ (SYSTEM ADMINISTRATOR) ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (ACCESS POINT) ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายน้อยที่สุด

ข้อ 39. ผู้ดูแลระบบ (SYSTEM ADMINISTRATOR) ควรทำการเปลี่ยนค่า SSID (SERVICE SET IDENTIFIER) ที่ถูกกำหนดเป็นค่าโดยปริยาย (DEFAULT) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ (ACCESS POINT) มาใช้งาน

ข้อ 40. ผู้ดูแลระบบ (SYSTEM ADMINISTRATOR) ต้องกำหนดค่า WEP (WIRED EQUIVALENT PRIVACY) หรือ WPA (WI-FI PROTECTED ACCESS) ในการเข้ารหัสข้อมูลระหว่าง WIRELESS LAN CLIENT และอุปกรณ์กระจายสัญญาณ (ACCESS POINT) และควรกำหนดค่าให้ไม่แสดงชื่อระบบเครือข่ายไร้สาย

ข้อ 41. ผู้ดูแลระบบ (SYSTEM ADMINISTRATOR) ควรเลือกใช้วิธีการควบคุม MAC ADDRESS (MEDIA ACCESS CONTROL ADDRESS) และชื่อผู้ใช้ (USERNAME) รหัสผ่าน (PASSWORD) ของผู้ใช้บริการที่มีสิทธิ์ในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC ADDRESS (MEDIA ACCESS CONTROL ADDRESS) และชื่อผู้ใช้ (USERNAME) รหัสผ่าน (PASSWORD) ตามที่กำหนดไว้เท่านั้นให้เข้าใช้ระบบเครือข่ายไร้สายได้อย่างถูกต้อง

ข้อ 42. ผู้ดูแลระบบ (SYSTEM ADMINISTRATOR) ควรมีการติดตั้งไฟร์วอลล์ (FIREWALL) ระหว่างระบบเครือข่ายไร้สายกับระบบเครือข่ายภายในหน่วยงาน

ข้อ 43. ผู้ดูแลระบบ (SYSTEM ADMINISTRATOR) ควรกำหนดให้ผู้ใช้บริการในระบบเครือข่ายไร้สายติดต่อสื่อสารได้เฉพาะกับ VPN (VIRTUAL PRIVATE NETWORK) เพื่อช่วยป้องกันการบุกรุกในระบบเครือข่ายไร้สาย

ข้อ 44. ผู้ดูแลระบบ (SYSTEM ADMINISTRATOR) ควรใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบการรักษาความปลอดภัยของระบบเครือข่ายไร้สายเพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย และจัดส่งรายงานผลการตรวจสอบทุก 3 เดือน และในกรณีที่ตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติ ให้ผู้ดูแลระบบ (SYSTEM ADMINISTRATOR) รายงานต่อผู้จัดการสหกรณ์ทราบทันที

ข้อ 45. ผู้ดูแลระบบ (SYSTEM ADMINISTRATOR) ต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาตใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต (INTRANET) และฐานข้อมูลภายในต่าง ๆ ของหน่วยงาน

หมวดที่ 8
การรักษาความปลอดภัยของไฟร์วอลล์
(FIREWALL POLICY)

ข้อ 46. สหกรณ์มีหน้าที่ในการบริหารจัดการ การติดตั้งและกำหนดค่าของไฟร์วอลล์ทั้งหมด

ข้อ 47. การกำหนดค่าเริ่มต้นพื้นฐานของทุกเครือข่ายจะต้องเป็นการปฏิเสธทั้งหมด

ข้อ 48. ทุกเส้นทางเชื่อมต่ออินเทอร์เน็ตและบริการอินเทอร์เน็ตที่ไม่อนุญาตตามนโยบาย จะต้องถูกบล็อก (BLOCK) โดยไฟร์วอลล์

ข้อ 49. ผู้ใช้งานอินเทอร์เน็ตจะต้องมีการ LOGIN ACCOUNT ก่อนการใช้งานทุกครั้ง

ข้อ 50. ค่าการเปลี่ยนแปลงทั้งหมดในไฟร์วอลล์ เช่น ค่าพารามิเตอร์ การกำหนดค่าใช้บริการ และการเชื่อมต่อที่อนุญาต จะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง

ข้อ 51. การเข้าถึงตัวอุปกรณ์ไฟร์วอลล์ จะต้องสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น

ข้อ 52. ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ไฟร์วอลล์ จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า 90 วัน

ข้อ 53. การกำหนดนโยบายในการให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่ายจะเปิดพอร์ตการเชื่อมต่อพื้นฐานของโปรแกรมทั่วไป ที่ทางสหกรณ์อนุญาตให้ใช้งาน ซึ่งหากมีความจำเป็นที่จะใช้งานพอร์ตการเชื่อมต่อนอกเหนือที่กำหนด จะต้องได้รับความยินยอมจากสหกรณ์ก่อน

ข้อ 54. การกำหนดค่าการให้บริการเครื่องคอมพิวเตอร์แม่ข่ายในส่วนของเครือข่าย จะต้องกำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น โดยข้อนโยบายจะต้องถูกระบุให้กับเครื่องคอมพิวเตอร์แม่ข่ายเป็นรายเครื่องที่ให้บริการจริง

ข้อ 55. จะต้องมีการสำรองข้อมูลการกำหนดค่าต่าง ๆ ของอุปกรณ์ไฟร์วอลล์เป็นประจำทุกสัปดาห์ หรือทุกครั้งที่มีการเปลี่ยนแปลงค่า

ข้อ 56. เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่าง ๆ จะต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็น โดยจะต้องกำหนดเป็นกรณีไป

ข้อ 57. สหกรณ์ มีสิทธิที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้งานที่ผิดนโยบาย หรือเกิดจากการทำงานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัย จนกว่าจะได้รับการแก้ไข

ข้อ 58. การเชื่อมต่อในลักษณะของการ REMOTE LOGIN จากภายนอกมายังเครื่องแม่ข่าย หรืออุปกรณ์เครือข่ายภายใน จะต้องบันทึกรายการของการดำเนินการตามแบบการขออนุญาตดำเนินการเกี่ยวกับเครื่องคอมพิวเตอร์และอุปกรณ์เครือข่าย และจะต้องได้รับความเห็นชอบจากสหกรณ์ก่อน

ข้อ 59. ผู้ละเมิดนโยบายด้านความปลอดภัยของไฟร์วอลล์ จะถูกระงับการใช้งานอินเทอร์เน็ตทันที

หมวดที่ 9
การรักษาความปลอดภัยของอีเมล์
(E-MAIL POLICY)

ข้อ 60. ในการลงทะเบียนบัญชีผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ (E-MAIL) ต้องทำการกรอกข้อมูลคำขอเข้าใช้บริการจดหมายอิเล็กทรอนิกส์ (E-MAIL) ของหน่วยงานโดยยื่นคำขอกับเจ้าหน้าที่สหกรณ์

ข้อ 61. เมื่อได้รับรหัสผ่าน (PASSWORD) ครั้งแรกในการเข้าระบบจดหมายอิเล็กทรอนิกส์ (E-MAIL) และเมื่อมีการเข้าสู่ระบบในครั้งแรกนั้น ควรเปลี่ยนรหัสผ่าน (PASSWORD) โดยทันที

ข้อ 62. ไม่ควรบันทึกหรือเก็บรหัสผ่าน (PASSWORD) ไว้ในระบบคอมพิวเตอร์

ข้อ 63. ควรเปลี่ยนรหัสผ่าน (PASSWORD) ทุก 3 – 6 เดือน

ข้อ 64. ไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-MAIL ADDRESS) ของผู้อื่นเพื่ออ่านหรือรับหรือส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้บริการและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์ (E-MAIL) เป็นผู้รับผิดชอบต่อการใช้งานในจดหมายอิเล็กทรอนิกส์ (E-MAIL) ของตน

ข้อ 65. หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (E-MAIL) เสร็จสิ้นควรลงบันทึกออก (LOGOUT) ทุกครั้ง

ข้อ 66. การส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์ (E-MAIL)

หมวดที่ 10
การรักษาความปลอดภัยของอินเทอร์เน็ต
(INTERNET SECURITY POLICY)

ข้อ 67. ไม่ใช้ระบบอินเทอร์เน็ต (INTERNET) ของหน่วยงาน เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อการรักษาความมั่นคงและความปลอดภัยต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับหน่วยงาน

ข้อ 68. ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงานที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต (INTERNET)

ข้อ 69. ระมัดระวังการดาวน์โหลด โปรแกรมใช้งานจากระบบอินเทอร์เน็ต (INTERNET) การดาวน์โหลด การอัพเดท (UPDATE) โปรแกรมต่าง ๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์

ข้อ 70. ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของหน่วยงาน

ข้อ 71. ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน การทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่น ๆ

ข้อ 72. หลังจากใช้งานระบบอินเทอร์เน็ต (INTERNET) เสร็จแล้วให้ปิดเว็บเบราเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ

หมวดที่ 11
การรักษาความปลอดภัยของการควบคุมการเข้าถึงระบบ
(ACCESS CONTROL POLICY)

การควบคุมการเข้าถึงด้านเทคโนโลยีสารสนเทศ

ข้อ 73. สหกรณ์ กำหนดมาตรการควบคุมการเข้าใช้งาน ด้านเทคโนโลยีสารสนเทศของหน่วยงานเพื่อดูแลรักษาความปลอดภัย โดยที่บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานด้านเทคโนโลยีสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษรต่อผู้จัดการสำนักงานสหกรณ์

ข้อ 74. ผู้ดูแลระบบ (SYSTEM ADMINISTRATOR) ต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งานระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ด้านเทคโนโลยีสารสนเทศ รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ

ข้อ 75. ผู้ดูแลระบบ (SYSTEM ADMINISTRATOR) ควรจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานด้านเทคโนโลยีสารสนเทศของหน่วยงานและตรวจตราการละเมิดความปลอดภัย ที่มีต่อระบบข้อมูล

ข้อ 76. ผู้ดูแลระบบ (SYSTEM ADMINISTRATOR) ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิ์ต่างๆ และการผ่านเข้า-ออกสถานที่ตั้งของระบบ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาตเพื่อเป็นหลักฐานในการตรวจสอบ

การบริหารจัดการการเข้าถึงด้านเทคโนโลยีสารสนเทศ

ข้อ 77. ผู้ดูแลระบบ (SYSTEM ADMINISTRATOR) ต้องกำหนดการลงทะเบียนบุคลากรใหม่ของสหกรณ์ ควรกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการเพื่อให้มีสิทธิ์ต่าง ๆ ในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เช่น การลาออก หรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น

ข้อ 78. ผู้ดูแลระบบ (SYSTEM ADMINISTRATOR) ต้องกำหนดการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (APPLICATION) จดหมายอิเล็กทรอนิกส์ (E-MAIL) ระบบเครือข่ายไร้สาย (WIRELESS LAN) ระบบอินเทอร์เน็ต (INTERNET) เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บริหารสหกรณ์เป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

ข้อ 79. ผู้ดูแลระบบ (SYSTEM ADMINISTRATOR) ต้องบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่านของบุคลากร ดังต่อไปนี้

79.1 กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (PASSWORD) เมื่อผู้ใช้งานระบบลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

79.2 ส่งมอบรหัสผ่าน (PASSWORD) ชั่วคราวให้กับผู้ใช้บริการด้วยวิธีการที่ปลอดภัย ควรหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (E-MAIL) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน (PASSWORD)

79.3 ควรกำหนดให้ผู้ใช้บริการตอบยืนยันการได้รับรหัสผ่าน (PASSWORD)

79.4 ควรกำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (PASSWORD) ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

79.5 กำหนดชื่อผู้ใช้หรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

79.6 ในกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บริหารสหกรณ์ โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิ์พิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานปกติ

ข้อ 80. ผู้ดูแลระบบ (SYSTEM ADMINISTRATOR) ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ ในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

80.1 ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

80.2 ต้องกำหนดรายชื่อผู้ใช้ (USERNAME) และรหัสผ่าน (PASSWORD) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

80.3 ควรกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

80.4 การรับ-ส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (ENCRYPTION) ที่เป็นมาตรฐานสากล เช่น SSL VPN หรือ XML ENCRYPTION เป็นต้น

80.5 ควรกำหนดการเปลี่ยนรหัสผ่าน (PASSWORD) ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

80.6 ควรกำหนดมาตรการรักษาความปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

หมวดที่ 12
การรักษาความปลอดภัยของการตรวจจับการบุกรุก
(INTRUSION DETECTION SYSTEM / INTRUSION PREVENTION SYSTEM POLICY : IDS/IPS POLICY)

ข้อ 81. IDS/IPS POLICY เป็นนโยบายการติดตั้งระบบตรวจสอบการบุกรุก และตรวจสอบความปลอดภัยของเครือข่าย เพื่อป้องกันทรัพยากร ด้านเทคโนโลยีสารสนเทศ และข้อมูลบนเครือข่ายภายในสหกรณ์ ให้มีการรักษาความปลอดภัย เป็นแนวทางการปฏิบัติเกี่ยวกับการตรวจสอบการบุกรุกเครือข่าย พร้อมกับบทบาทและความรับผิดชอบที่เกี่ยวข้อง

ข้อ 82. IDS/IPS POLICY ครอบคลุมทุกโฮสต์ (HOST) ในเครือข่ายของสหกรณ์และเครือข่ายข้อมูลทั้งหมด รวมถึงเส้นทางที่ข้อมูลอาจเดินทาง ซึ่งไม่อยู่ในเครือข่ายอินเทอร์เน็ตทุกเส้นทาง

ข้อ 83. ระบบทั้งหมดที่สามารถเข้าถึงได้จากอินเตอร์เน็ตหรือที่สาธารณะจะต้องผ่านการตรวจสอบจากระบบ IDS/IPS

ข้อ 84. ระบบทั้งหมดใน DMZ จะต้องได้รับการตรวจสอบรูปแบบการให้บริการก่อนการติดตั้งและเปิดให้บริการ

ข้อ 85. โฮสต์และเครือข่ายทั้งหมดที่มีการส่งผ่านข้อมูลผ่าน IDS/IPS จะต้องมีการบันทึกผลการตรวจสอบ

ข้อ 86. มีการตรวจสอบและ UPDATE PATCH/SIGNATURE ของ IDS/IPS เป็นประจำทุก 3 เดือน

ข้อ 87. มีการตรวจสอบเหตุการณ์ ข้อมูลจราจร พฤติกรรมการใช้งาน กิจกรรม และบันทึกปริมาณข้อมูลเข้าใช้งานเครือข่ายเป็นประจำทุกวันโดยผู้ดูแลระบบ

ข้อ 88. IDS/IPS จะทำงานภายใต้กฎควบคุมพื้นฐานของไฟร์วอลล์ ที่ใช้ในการเข้าถึงเครือข่ายของด้านเทคโนโลยีสารสนเทศตามปกติ

ข้อ 89. เครื่องแม่ข่ายที่มีการติดตั้ง HOST-BASED IDS จะต้องมีการตรวจสอบข้อมูลประจำวัน

ข้อ 90. พฤติกรรมการใช้งาน กิจกรรม หรือเหตุการณ์ทั้งหมด ที่มีความเสี่ยงต่อการบุกรุก การโจมตีระบบ พฤติกรรมที่น่าสงสัย หรือการพยายามเข้าระบบ ทั้งที่ประสบความสำเร็จและไม่ประสบความสำเร็จจะต้องมีการรายงานให้ผู้บริหารสหกรณ์ทราบทันทีที่ตรวจพบ

ข้อ 91. การตรวจสอบการบุกรุกทั้งหมดจะต้องเก็บบันทึกข้อมูลไว้ไม่น้อยกว่า 90 วัน

หมวดที่ 13
การรักษาความปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย
(NETWORK AND SERVER POLICY)

ข้อ 92. สหกรณ์กำหนดมาตรการควบคุมการเข้า-ออกห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (SERVER)

ข้อ 93. ผู้ใช้บริการจะนำเครื่องคอมพิวเตอร์และอุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงาน ต้องได้รับอนุญาตจากผู้จัดการสหกรณ์ และต้องปฏิบัติตามนโยบายนี้โดยเคร่งครัด

ข้อ 94. การขออนุญาตใช้งานพื้นที่ WEB SERVER และชื่อโดเมนย่อย (SUB DOMAIN NAME) ที่หน่วยงานรับผิดชอบอยู่ จะต้องทำหนังสือขออนุญาตต่อผู้จัดการสหกรณ์ และจะต้องไม่ติดตั้งโปรแกรมใด ๆ ที่ส่งผลกระทบต่อการกระทำของระบบและผู้ใช้บริการอื่นๆ

ข้อ 95. ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใด ๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (ROUTER) อุปกรณ์กระจายสัญญาณข้อมูล (SWITCH) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลัก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ (SYSTEM ADMINISTRATOR)

ข้อ 96. ผู้ดูแลระบบ (SYSTEM ADMINISTRATOR) ต้องควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ ดังต่อไปนี้

96.1 ต้องมีวิธีการจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้บริการให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น

96.2 ต้องมีวิธีการจำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน

96.3 ต้องกำหนดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่าย เพื่อไม่ให้ผู้ใช้บริการสามารถใช้เส้นทางอื่น ๆ ได้

96.4 ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกหน่วยงานควรเชื่อมต่ออุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมีความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย (MALWARE) ด้วย

96.5 ระบบเครือข่ายต้องติดตั้งระบบตรวจจับการบุกรุก (INTRUSION PREVENTION SYSTEM/INTRUSION DETECTION SYSTEM) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของหน่วยงานในลักษณะที่ผิดปกติ

96.6 การเข้าสู่ระบบเครือข่ายภายในหน่วยงาน โดยผ่านทางระบบอินเทอร์เน็ตจำเป็นต้องมีการลงบันทึกเข้า (LOGIN) และต้องมีการพิสูจน์ยืนยันตัวตน (AUTHENTICATION) เพื่อตรวจสอบความถูกต้องของผู้ใช้บริการ

96.7 เลขที่อยู่ไอพี (IP ADDRESS) ภายในของระบบเครือข่ายภายในของหน่วยงานจำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้

96.8 ต้องจัดทำแผนผังระบบเครือข่าย (NETWORK DIAGRAM) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

96.9 การใช้เครื่องมือต่าง ๆ เพื่อการตรวจสอบระบบเครือข่าย ควรได้รับการอนุมัติจากผู้ดูแลระบบ (SYSTEM ADMINISTRATOR) และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

ข้อ 97. ผู้ดูแลระบบ (SYSTEM ADMINISTRATOR) ต้องบริหารควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (SERVER) และรับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (SERVER) ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่างๆ ของซอฟต์แวร์ (SYSTEM SOFTWARE)

ข้อ 98. สหกรณ์ กำหนดมาตรการควบคุมการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (LOG) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์ (LOG) มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ตามแนวทาง ดังต่อไปนี้

98.1 ควรจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (LOG) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้อง แท้จริง และระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้และข้อมูลที่ใช้ในการจัดเก็บ ต้องกำหนดชั้นความลับในการเข้าถึงข้อมูลและผู้ดูแลระบบไม่ได้รับอนุญาตในการแก้ไขข้อมูลที่เก็บรักษาไว้ ยกเว้นผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศของหน่วยงาน (IT AUDITOR) หรือบุคคลที่หน่วยงานมอบหมาย

98.2 ควรกำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (APPLICATION LOGS) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้า-ออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน COMMAND LINE และ FIREWALL LOG เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย 90 วัน นับตั้งแต่การใช้บริการสิ้นสุดลง

98.3 ควรตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานระบบอย่างสม่ำเสมอ

98.4 ต้องมีวิธีการป้องกันแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิ์การเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

ข้อ 99. สหกรณ์ กำหนดมาตรการควบคุมการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (SERVER) เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอกตามแนวทาง ดังต่อไปนี้

99.1 บุคคลจากหน่วยงานภายนอกที่ต้องการทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุญาตจากผู้จัดการสหกรณ์

99.2 มีการควบคุมช่องทาง (PORT) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

99.3 วิธีการใดๆ ที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้จากระยะไกลต้องได้รับการอนุญาตจากผู้จัดการสหกรณ์

99.4 การเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐาน ระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับหน่วยงานอย่างเพียงพอ

99.5 การเข้าใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจากระบบของหน่วยงาน

หมวดที่ 14

นโยบายการรักษาความปลอดภัยของการสำรองข้อมูล

(BACKUP POLICY)

ข้อ 100. จัดทำสำเนาข้อมูลและซอฟต์แวร์เก็บไว้ โดยจัดเรียงตามลำดับความจำเป็นของการสำรองข้อมูลด้านเทคโนโลยีสารสนเทศของหน่วยงานจากจำเป็นมากไปหาน้อย

ข้อ 101. มีขั้นตอนการปฏิบัติการจัดทำสำรองข้อมูลและการกู้คืนข้อมูลอย่างถูกต้อง ทั้งระบบซอฟต์แวร์ และข้อมูลในด้านเทคโนโลยีสารสนเทศ โดยขั้นตอนปฏิบัติแยกตามด้านเทคโนโลยีสารสนเทศแต่ละระบบ

ข้อ 102. จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูลและผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน ข้อมูลที่สำรองควรจัดเก็บไว้ในสถานที่เก็บข้อมูลสำรองซึ่งติดตั้งอยู่ที่สถานที่อื่น และต้องมีการทดสอบสื่อเก็บข้อมูลสำรองอย่างสม่ำเสมอ

ข้อ 103. ต้องมีการจัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาที่เหมาะสม

ข้อ 104. ให้ประธานกรรมการรักษาการให้เป็นไปตามระเบียบนี้

ประกาศ ณ วันที่ 22 กุมภาพันธ์ 2554

(นายแพทย์สมเกียรติ ธาตรีธร)

ประธานกรรมการ

สหกรณ์ออมทรัพย์วชิรพยาบาล จำกัด