สหกรณ์ออมทรัพย์โรงพยาบาลมหาราชนครราชสีมา จำกัด

ระเบียบว่าด้วย การควบคุมและการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ

พ.ศ.2554

อาศัยอำนาจตามความในข้อบังคับสหกรณ์ ข้อ 65(8) และ ข้อ 93(11) ที่ประชุมคณะกรรมการดำเนินการชุดที่ 12 ครั้งที่ 10/2554 วันที่ 26 กรกฎาคม 2554 ตามที่นายทะเบียนสหกรณ์ ได้กำหนดระเบียบนายทะเบียนสหกรณ์ ว่าด้วย มาตรฐานขั้นต่ำในการควบคุมภายในและการรักษาความปลอดภัยสำหรับสหกรณ์และกลุ่มเกษตรกรที่ใช้โปรแกรมระบบบัญชีคอมพิวเตอร์ประมวลผลข้อมูล พ.ศ.2553 สหกรณ์จึงได้กำหนดระเบียบว่าด้วย การควบคุมและการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ พ.ศ.2554 โดยความเห็นชอบของกรมตรวจบัญชีสหกรณ์ ไว้ดังต่อไปนี้

ข้อ 1. ระเบียบนี้เรียกว่า "ระเบียบสหกรณ์ออมทรัพย์โรงพยาบาลมหาราชนครราชสีมา จำกัด ว่าด้วย การควบคุมและรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ พ.ศ.2554"

ข้อ 2. ระเบียบนี้ใช้บังคับตั้งแต่วัน 1 สิงหาคม 2554 เป็นต้นไป

ข้อ 3. ในระเบียบนี้

"สหกรณ์"	หมายถึง	สหกรณ์ออมทรัพย์โรงพยาบาลมหาราชนครราชสีมา จำกัด
"ผู้บริหารสหกรณ์"	หมายถึง	คณะกรรมการดำเนินการสหกรณ์ออมทรัพย์โรงพยาบาลมหาราชนครราชสีมา จำกัด
"เจ้าหน้าที่"	หมายถึง	เจ้าหน้าที่และลูกจ้างของสหกรณ์
"ผู้ดูแลระบบ"	หมายถึง	เจ้าหน้าที่ที่ได้รับมอบหมายให้ดูแลรับผิดชอบระบบคอมพิวเตอร์ของสหกรณ์
"ผู้ใช้งาน"	หมายถึง	บุคคลใด ๆ ที่สหกรณ์อนุญาตให้เข้าใช้ระบบคอมพิวเตอร์ของสหกรณ์ด้วยเครือข่ายท้องถิ่น (LAN) เครือข่ายไร้สาย (Wireless/Wifi) ไม่ว่าจะได้รับอนุญาตจากสหกรณ์หรือไม่ก็ตาม
"ระบบคอมพิวเตอร์"	หมายถึง	อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยมีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติของสหกรณ์
"อุปกรณ์"	หมายถึง	อุปกรณ์ทุกประเภทที่ต่อเชื่อมกับคอมพิวเตอร์ และระบบคอมพิวเตอร์เพื่อใช้งาน หรือประมวลผลข้อมูล
"ข้อมูลคอมพิวเตอร์"	หมายถึง	ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่

ในระบบคอมพิวเตอร์ ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้ หมายรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

"ทรัพยากรสารสนเทศ" หมายถึง ข้อมูลคอมพิวเตอร์ ซอฟต์แวร์ ได้แก่ ระบบปฏิบัติการ ซอฟต์แวร์ประยุกต์ และอื่น ๆ ที่เกี่ยวข้อง และฮาร์ดแวร์ ได้แก่ เครื่องคอมพิวเตอร์ อุปกรณ์ต่อพ่วง อุปกรณ์สื่อสาร รวมถึง สื่อบันทึกข้อมูลทุกประเภทของสหกรณ์

ข้อ 4 ให้ผู้บริหารสหกรณ์รักษาการให้เป็นไปตามระเบียบนี้ และให้มีอำนาจวินิจฉัยชี้ขาดปัญหาอันเกิดจากการใช้ระเบียบนี้ คำวินิจฉัยของผู้บริหารสหกรณ์ให้เป็นที่สุด

ข้อ 5 วัตถุประสงค์

5.1 เพื่อให้ผู้ใช้งานปฏิบัติตามระเบียบนี้โดยเคร่งครัดเมื่อเข้าใช้งานคอมพิวเตอร์ผ่านระบบเครือข่ายคอมพิวเตอร์ของสหกรณ์

5.2 เพื่อควบคุม ติดตาม ดูแลและปกป้องระบบเทคโนโลยีสารสนเทศของสหกรณ์อันหมายรวมถึงข้อมูลคอมพิวเตอร์ ซอฟต์แวร์และฮาร์ดแวร์ทั้งหมด

ข้อ 6 ขอบเขตและความรับผิดชอบ

ระเบียบฉบับนี้มีผลบังคับใช้ครอบคลุมทรัพยากรสารสนเทศ ผู้ใช้งานต้องรับผิดชอบดูแลรหัสผู้ใช้งานประจำตัว (Username) และรหัสผ่าน (Password) ของตนเองตลอดจนกิจกรรมต่าง ๆ ที่เกิดขึ้นจากการเข้าสู่ระบบคอมพิวเตอร์ภายใต้รหัสผู้ใช้งานประจำตัว และรหัสผ่านที่ตนเองรับผิดชอบ

ระเบียบว่าด้วย การควบคุมและการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศของสหกรณ์ ประกอบด้วย 7 หมวดโดยมีรายละเอียดดังต่อไปนี้

หมวด 1
ว่าด้วยการพิสูจน์ตัวตน
(Accountability,Identification and Authentication)

ข้อ 7 ผู้ใช้งานมีหน้าที่ในการป้องกันดูแลรักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งาน(Username) ของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่ แจกจ่ายทำให้ผู้อื่นล่วงรู้รหัสผ่าน (Password)

ข้อ 8 ผู้ใช้งานต้องรับผิดชอบต่อการกระทำใด ๆ ที่เกิดจากบัญชีของผู้ใช้งาน (Username) ไม่ว่าการกระทำนั้น จะเกิดจากผู้ใช้งานหรือไม่ก็ตาม

ข้อ 9 ผู้ใช้งานต้องตั้งรหัสผ่านให้เกิดความปลอดภัย โดยรหัสผ่านต้องประกอบด้วยตัวอักษร (Character) หรือตัวเลข (Numerical character) ไม่น้อยกว่า 6 ตัวอักษร

ข้อ 10 ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) อย่างน้อยทุก ๆ 6 เดือน หรือทุกครั้งเมื่อมีการแจ้งเตือน

ข้อ 11 ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้ง ก่อนที่จะใช้ทรัพย์สินหรือด้านเทคโนโลยีสารสนเทศของสหกรณ์และหากการพิสูจน์ตัวตนนั้นมีปัญหาไม่ว่าจะเกิดจากรหัสผ่าน การถูกล็อค หรือเกิดจากความผิดพลาดใด ๆ ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบ (System Administrator) ทราบทันที โดย

(1) คอมพิวเตอร์โน๊ตบุ๊ค (Notebook) ต้องทำการพิสูจน์ตัวตนระบบในไบออส (BIOS) ก่อนใช้งาน

(2) คอมพิวเตอร์ทุกประเภท ก่อนการเข้าถึงระบบปฏิบัติการต้องทำการพิสูจน์ตัวตนทุกครั้ง

(3) การใช้งานอินเทอร์เน็ต (Internet) ต้องมีการทึกข้อมูลซึ่งสามารถบ่งบอกตัวตนบุคคลผู้ใช้งานได้

(4) เมื่อผู้ใช้งานไม่อยู่ที่เครื่องคอมพิวเตอร์ เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการล็อคหน้าจอทุกครั้ง และต้องทำการพิสูจน์ตัวตนก่อนการใช้งานทุกครั้ง

(5) เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการตั้งเวลาพักหน้าจอ (screen saver) โดยตั้งเวลาอย่างน้อย 5 นาที

หมวด 2
ว่าด้วยการบริหารจัดการทรัพย์สิน
(Assets Management)

ข้อ 12 ผู้ใช้งานต้องไม่เข้าถึงเครื่องแม่ข่าย(Server)โดยเด็ดขาด เว้นแต่ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ 13 ผู้ใช้งานต้องไม่นำเครื่องมือ หรืออุปกรณ์อื่นใด เชื่อมเข้าเครือข่ายโดยเด็ดขาด

ข้อ 14 ผู้ใช้งานต้องไม่ใช้ หรือลบแฟ้มข้อมูลของผู้อื่น ไม่ว่ากรณีใด ๆ

ข้อ 15 ผู้ใช้งานต้องรับผิดชอบต่อทรัพย์สินที่สหกรณ์มอบไว้ให้ใช้งาน หรือหากมีการใช้งานนอกสถานที่ต้องดูแล การรับหรือคืนทรัพย์สินจะถูกบันทึก และตรวจสอบทุกครั้งโดยเจ้าหน้าที่สหกรณ์มอบหมาย

ข้อ 16 ผู้ใช้งานต้องรับผิดชอบต่อทรัพย์สินที่สหกรณ์มอบไว้ให้ใช้งานเสมือนหนึ่งเป็นทรัพย์สินของผู้ใช้งานเอง โดยชดใช้ค่าเสียหายไม่ว่าทรัพย์สินนั้นจะชำรุดหรือสูญหายตามมูลค่าทรัพย์สิน หากความเสียหายนั้นเกิดจากความประมาทของผู้ใช้งาน

ข้อ 17 ผู้ใช้งานต้องไม่ให้ผู้อื่นยืมคอมพิวเตอร์หรือโน๊ตบุ๊ค (Notebook) ไม่ว่ากรณีใด ๆ เว้นแต่ การยืมนั้นได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้มีอำนาจ

ข้อ 18 ทรัพย์สินและด้านเทคโนโลยีสารสนเทศต่าง ๆ ที่สหกรณ์จัดเตรียมไว้ให้ใช้งานมีวัตถุประสงค์เพื่อการใช้งานของสหกรณ์เท่านั้น ห้ามมิให้ผู้ใช้งานนำทรัพย์สินและด้านเทคโนโลยีสารสนเทศต่าง ๆ ไปใช้ในกิจกรรมที่สหกรณ์ไม่ได้กำหนด หรือทำให้เกิดความเสียหายต่อสหกรณ์

ข้อ 19 ความเสียหายใด ๆ ที่เกิดจากการละเมิดข้อ 12 ให้ถือเป็นความผิดส่วนบุคคลโดยผู้ใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

หมวด 3

ว่าด้วยการบริหารจัดการข้อมูลองค์กร

(Corporate Management)

ข้อ 20 ผู้ใช้งานต้องป้องกัน ดูแล รักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูล รวมถึงระมัดระวังต่อการใช้งานของข้อมูล ทั้งข้อมูลของสหกรณ์หรือข้อมูลส่วนบุคคล หากเกิดความสูญหาย โดยนำไปใช้ในทางที่ผิด การเผยแพร่โดยไม่ได้รับอนุญาต ผู้ใช้งานต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้น

ข้อ 21 ข้อมูลทั้งหมดที่อยู่ภายในทรัพย์สินของสหกรณ์ ถือเป็นทรัพย์สินของสหกรณ์ห้ามเผยแพร่ แก้ไขเปลี่ยนแปลง หรือทำลาย โดยไม่ได้รับอนุญาตจากผู้บริหารของสหกรณ์

ข้อ 22 ผู้ใช้งานมีส่วนร่วมและมีสิทธิโดยชอบธรรม ที่จะเก็บ ดูแลรักษา ใช้งานและป้องกันข้อมูลของสหกรณ์ หรือข้อมูลส่วนบุคคลตามเห็นสมควร และไม่อนุญาตให้บุคคลหนึ่งบุคคลใดละเมิดต่อข้อมูลส่วนบุคคล โดยไม่ได้รับอนุญาตจากผู้ใช้งาน เว้นแต่ กรณีสหกรณ์ต้องการตรวจสอบ โดยแต่งตั้งผู้ทำหน้าที่ทำการตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลา โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

หมวด 4

ว่าด้วยการบริหารจัดการด้านเทคโนโลยีสารสนเทศ

(IT Infrastructure Management)

ข้อ 23 ผู้ใช้งานมีสิทธิที่จะพัฒนาหรือแก้ไขเปลี่ยนแปลงโปรแกรมให้เหมาะสมและเพียงพอเพื่อให้ระบบบัญชีคอมพิวเตอร์ ประมวลผลได้ถูกต้องและครบถ้วนเป็นไปตามความต้องการของผู้ใช้งาน โดยต้องแจ้งให้ผู้เกี่ยวข้อรับทราบเพื่อให้ใช้งานได้ถูกต้อง แต่ต้องไม่ดำเนินการ ที่จะก่อให้เกิดผลกระทบ ดังนี้

(1) ทำลายกลไกการควบคุมและรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศของสหกรณ์

(2) กระทำซ้ำโปรแกรมหรือแฝงตัวโปรแกรมไปกับโปรแกรมอื่น ในลักษณะเช่นเดียวกับหนอนหรือไวรัสคอมพิวเตอร์

(3) ทำลายระบบจำกัดสิทธิ์การใช้ (License) ซอฟต์แวร์ (Software) หรือก่อเกิดสิทธ์หรือมีความสำคัญในการเข้าถึงข้อมูลหรือครอบครองทรัพยากรระบบมากกว่าผู้ใช้อื่น

(4) สร้างเว็บเพจ บนเครือข่าย เสนอข้อมูลผิดกฎหมาย ละเมิดลิขสิทธิ์ แสดงข้อความรูปภาพที่ไม่เหมาะสม หรือขัดต่อศีลธรรมประเพณีอันดีงามของประเทศ

ข้อ 24 ห้ามติดตั้งอุปกรณ์อื่นหรือกระทำการใด ๆ เพื่อให้เข้าถึงระบบเทคโนโลยีสารสนเทศของสหกรณ์โดยไม่ได้รับอนุญาตจากผู้มีอำนาจ

ข้อ 25 ห้ามต่อพ่วงเครื่องแม่ข่ายร่วมกับเครื่องที่ใช้ต่อ INTERNET โดยเด็ดขาด

หมวด 5

ว่าด้วยซอฟต์แวร์และลิขสิทธิ์

(Software Licensing and intellectual Property)

ข้อ 26 สหกรณ์ให้ความสำคัญ เรื่องสินทรัพย์ทางปัญญา ทั้งนี้ ซอฟต์แวร์ (Software) ที่สหกรณ์ใช้อนุญาตให้ใช้งานหรือที่สหกรณ์ มีลิขสิทธิ์ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งาน (Software) อื่นที่ไม่มีลิขสิทธิ์ หากตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ์ให้ถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานต้องรับผิดชอบผู้เดียว

ข้อ 27 ซอฟต์แวร์ (Software) ที่สหกรณ์จัดเตรียมไว้ให้ผู้ใช้งาน ถือว่าเป็นสิ่งจำเป็นในการปฏิบัติงาน ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไขหรือทำสำเนาเพื่อนำไปใช้งานที่อื่น

หมวด 6

ว่าด้วยการป้องกันโปรแกรมที่ไม่ประสงค์ดี

(Preventing Malware)

ข้อ 28 ติดตั้งระบบตรวจจับการบุกรุก (Intrusion Detection System) เพื่อตรวจสอบการใช้งาน ที่มีลักษณะที่ผิดปกติ

ข้อ 29 คอมพิวเตอร์ของผู้ใช้งาน ต้องติดตั้งโปรแกรมป้องกันไวรัส (Antivirus) ตามที่สหกรณ์ได้ประกาศให้ใช้

ข้อ 30 บรรดาข้อมูล ไฟล์ ซอฟต์แวร์ (Software) อื่นใด ที่ได้รับจากผู้ใช้งานอื่นต้องทำการตรวจสอบไวรัส และโปรแกรมที่ไม่ประสงค์ดี โดยโปรแกรมป้องกันไวรัส (Antivirus) ก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง

ข้อ 31 ผู้ใช้งานต้องพึงระวังไวรัส (Antivirus) และโปรแกรมที่ไม่ประสงค์ดี อยู่ตลอดเวลา หากพบสิ่งที่ผิดปกติ ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่เครือข่ายและต้องแจ้งให้ผู้ดูแลระบบทราบทันที

ข้อ 32 ผู้ใช้งานต้องปรับปรุงข้อมูล สำหรับตรวจสอบและปรับปรุงระบบปฏิบัติการ (Update patch) ให้ใหม่อยู่เสมอ เพื่อป้องกันความเสียหายที่อาจเกิดขึ้น

หมวด 7

ว่าด้วยการรักษาความปลอดภัยของข้อมูลคอมพิวเตอร์

(Data Security)

ข้อ 33 กระทำการสำรองข้อมูลคอมพิวเตอร์ของแต่ละระบบงานเป็นประจำในเวลา 16.00 น. ทุกวันทำการ

ข้อ 34 ทำการจัดเก็บข้อมูลชุดสำรองไว้ในสื่อภายนอก ได้แก่ CD, DVD หรือ External Harddisk

อย่างน้อยสัปดาห์ละ 3 วัน

ข้อ 35 ติดฉลากบอกรายละเอียดบนสื่อเก็บข้อมูลโดยระบุวัน เวลาที่สำรองข้อมูลให้ชัดเจน

ข้อ 36 มีการทดสอบสื่อเก็บข้อมูลที่สำรองโดยการเรียกคืนข้อมูล อย่างน้อยปีละ 1 ครั้ง

ข้อ 37 มอบหมายผู้เก็บรักษาความปลอดภัยชุดสำรองข้อมูล เพื่อป้องกันเหตุฉุกเฉินและเพื่อให้สามารถกู้ระบบกลับคืนได้ภายในระยะเวลาที่เหมาะสม ไว้ดังนี้

(1) ผู้จัดการสหกรณ์ จำนวน 1 ชุด (แผ่น CD)

(2) เหรัญญิก จำนวน 1 ชุด (แผ่น CD)

(3) ผู้สำรองข้อมูล จำนวน 1 ชุด (แผ่น CD)

กำหนดไว้ ณ วันที่ 26 กรกฎาคม พ.ศ. 2554

(นางนารินทร์ เมธานุวัฒน์)

รองประธานกรรมการ

สหกรณ์ออมทรัพย์โรงพยาบาลมหาราชนครราชสีมา จำกัด