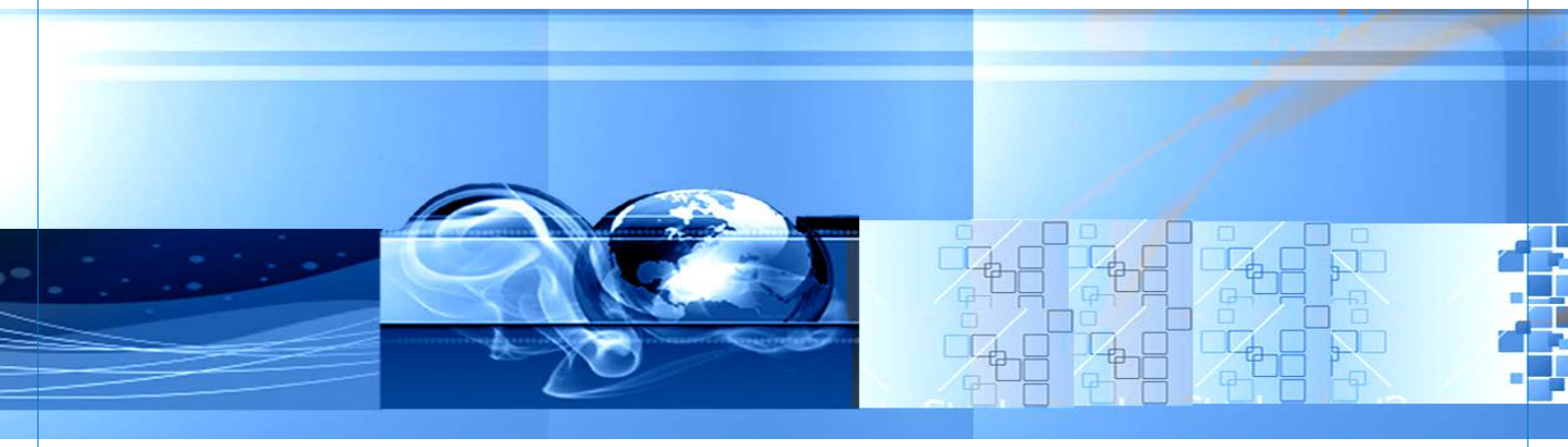
แนวปฏิบัติตามมาตรฐานขั้นต่ำในการควบคุมภายใน และการรักษาความปลอดภัยสำหรับสหกรณ์ ที่ใช้โปรแกรมระบบบัญชีคอมพิวเตอร์ประมวลผลข้อมูล

โดย

วรรณพร ตั้งพรโชติช่วง



กรมตรวจบัญชีสหกรณ์ กระทรวงเกษตรและสหกรณ์

แนวปฏิบัติตามมาตรฐานขั้นต่ำในการควบคุมภายในและการรักษาความปลอดภัย สำหรับสหกรณ์ที่ใช้โปรแกรมระบบบัญชีคอมพิวเตอร์ประมวลผลข้อมูล

โดย

นางสาววรรณพร ตั้งพรโชติช่วง

กรมตรวจบัญชีสหกรณ์ กระทรวงเกษตรและสหกรณ์

บทคัดย่อ

ปัจจุบันสหกรณ์มีการใช้โปรแกรมระบบบัญชีในการประมวลผลข้อมูลทางการเงินและ ใช้ในการให้บริการสมาชิกเพิ่มขึ้นอย่างมาก จากระบบฐานข้อมูลของกรมตรวจบัญชีสหกรณ์พบว่า ในจำนวนสหกรณ์ทั้งสิ้น 6,637 แห่ง ใช้โปรแกรมระบบบัญชีสหกรณ์ในการประมวลผลข้อมูลถึงจำนวน 3,785 แห่ง หรือคิดเป็นร้อยละ 57.03 การนำเทคโนโลยีสารสนเทศมาใช้ในองค์กรนั้นมีทั้งข้อดีที่ช่วยให้การดำเนินงานรวดเร็วและถูกต้องแม่นยำมากขึ้น แต่มีข้อเสียคือการใช้เทคโนโลยีนั้นจะทำให้เกิดความเสี่ยงในการบริหารจัดการตามมาด้วย เพื่อลดความเสี่ยงดังกล่าว นายทะเบียนสหกรณ์จึงได้กำหนดระเบียบว่าด้วย “มาตรฐานขั้นต่ำในการควบคุมภายในและการรักษาความปลอดภัยสำหรับสหกรณ์และกลุ่มเกษตรกรที่ใช้โปรแกรมระบบบัญชีคอมพิวเตอร์ประมวลผลข้อมูล พ.ศ. 2553” ประกอบด้วยมาตรฐาน 9 ข้อ ซึ่งได้ประยุกต์เนื้อหามาจากหลักการของมาตรฐาน COBIT (Control Objective for Information and related Technology) มาตรฐาน ITIL (The Information Technology Infrastructure Library) และมาตรฐานการสอบบัญชีเรื่องการสอบบัญชีในสภาพแวดล้อมของระบบสารสนเทศที่ใช้คอมพิวเตอร์ ซึ่งเป็นหลักปฏิบัติที่ดี (Best Practice) ที่ใช้ในการบริหารจัดการเทคโนโลยีสารสนเทศ

นับจากที่นายทะเบียนสหกรณ์ได้ประกาศใช้และเริ่มให้ถือปฏิบัติมาตรฐานขั้นต่ำในการควบคุมภายในและการรักษาความปลอดภัยตั้งแต่วันที่ 1 มกราคม 2554 เป็นต้นมา สหกรณ์ส่วนใหญ่ยัง ไม่มีการกำหนดระบบการควบคุมภายในด้านเทคโนโลยีสารสนเทศที่เหมาะสม ดังนั้น จึงได้จัดทำ **แนวปฏิบัติตามมาตรฐานขั้นต่ำในการควบคุมภายในและการรักษาความปลอดภัยสำหรับสหกรณ์ที่ใช้โปรแกรมระบบบัญชีคอมพิวเตอร์ประมวลผลข้อมูล** โดยที่โครงสร้างของแนวปฏิบัติประกอบด้วย **ข้อกำหนด** ซึ่งเป็นมาตรฐานที่นายทะเบียนสหกรณ์กำหนด **แนวปฏิบัติ** ซึ่งเป็นกิจกรรมด้านเทคโนโลยีสารสนเทศที่จะต้องดำเนินการเพื่อให้บรรลุวัตถุประสงค์ของมาตรฐานแต่ละข้อ และ **การประเมินระดับ การควบคุมภายในและการรักษาความปลอดภัยของสหกรณ์** เพื่อช่วยให้สหกรณ์สามารถประเมินระดับความเข้มแข็งของการควบคุมของสหกรณ์เองได้ โดยกำหนดเป็นเกณฑ์ไว้ทั้งหมด 6 ระดับ

การที่สหกรณ์จะสามารถนำแนวปฏิบัตินี้ไปใช้ได้อย่างบังเกิดผลนั้น จำเป็นต้องมีการสร้างให้เกิดความตระหนักถึงความเสี่ยงที่เกิดจากการใช้เทคโนโลยีสารสนเทศและเห็นความสำคัญของการจัดให้มีระบบการควบคุมภายในและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ ควบคู่กับการพัฒนารูปแบบและวิธีการถ่ายโอนองค์ความรู้ให้บังเกิดประสิทธิผลอย่างต่อเนื่อง ทั้งการให้ความรู้แก่บุคลากรของสหกรณ์ กรมตรวจบัญชีสหกรณ์และหน่วยงานอื่นที่เกี่ยวข้อง รวมทั้งควรมีการพัฒนามาตรการบังคับใช้โดยผ่านกลไกการสอบบัญชี เช่น การนำมาเป็นประเด็นหัวข้อในการประเมินความเสี่ยงในการสอบบัญชีและการจัดชั้นคุณภาพการควบคุมภายใน เพื่อกระตุ้นให้สหกรณ์ดำเนินการจนบังเกิดผล เป็นต้น

คำนำ

แนวปฏิบัติตามมาตรฐานขั้นต่ำในการควบคุมภายในและการรักษาความปลอดภัยสำหรับสหกรณ์ที่ใช้โปรแกรมระบบบัญชีคอมพิวเตอร์ประมวลผลข้อมูลนี้ จัดทำขึ้นโดยมีวัตถุประสงค์ที่จะให้สหกรณ์มีแนวทางในการกำหนดวิธีการควบคุมภายในที่เหมาะสมกับสภาพแวดล้อมและลักษณะการใช้เทคโนโลยีสารสนเทศของสหกรณ์ รวมทั้งช่วยให้ผู้สอบบัญชีได้ใช้ในการศึกษาและทำความเข้าใจเพื่อใช้เป็นแนวทางในการประเมินความเสี่ยงในการสอบบัญชีและความมีประสิทธิผลของการควบคุมภายในของสหกรณ์ที่ใช้โปรแกรมระบบบัญชีประมวลผลข้อมูล

แนวปฏิบัตินี้ได้ออกแบบวิธีการควบคุมและอธิบายรายละเอียดวิธีการควบคุมสำหรับข้อกำหนดตามระเบียบนายทะเบียนสหกรณ์ว่าด้วย “มาตรฐานขั้นต่ำในการควบคุมภายในและการรักษาความปลอดภัยสำหรับสหกรณ์และกลุ่มเกษตรกรที่ใช้โปรแกรมระบบบัญชีคอมพิวเตอร์ประมวลผลข้อมูล พ.ศ. 2553” ในแต่ละข้อ รวมทั้งให้แนวทางในการประเมินระดับการควบคุมที่สหกรณ์ได้จัดทำขึ้นเพื่อให้สหกรณ์พิจารณาเพิ่มระดับการควบคุมตามความเหมาะสม นอกจากนี้ยังแสดงให้เห็นถึงความเชื่อมโยงระหว่างมาตรฐานขั้นต่ำในการควบคุมภายในที่กำหนดโดยนายทะเบียนสหกรณ์กับมาตรฐานด้านเทคโนโลยีสารสนเทศที่เป็น Best Practice เพื่อให้มั่นใจว่าแนวปฏิบัติที่ได้ออกแบบได้อ้างอิงหลักวิชาการที่มีการปฏิบัติกันอย่างแพร่หลายและเป็นสากล รวมทั้งเป็นสิ่งจำเป็นสำหรับองค์กรที่มีการใช้เทคโนโลยีสารสนเทศ

ผู้จัดทำหวังเป็นอย่างยิ่งว่า แนวปฏิบัตินี้จะช่วยให้ทุกฝ่ายที่เกี่ยวข้องกับขบวนการสหกรณ์ได้เข้าใจและใช้ให้เกิดประโยชน์ ซึ่งจะทำให้สหกรณ์ลดความเสี่ยงและสามารถใช้เทคโนโลยีสารสนเทศได้อย่างบังเกิดผล

วรรณพร ตั้งพรโชติช่วง

ตุลาคม 2555

สารบัญ

บทที่ 1

บทนำ

บทที่ 1
บทนำ

หลักการและเหตุผล

ด้วยปัจจุบันสหกรณ์มีการใช้โปรแกรมระบบบัญชีในการประมวลผลข้อมูลทางการเงินและใช้ในการให้บริการสมาชิกเพิ่มขึ้นอย่างมาก ตามรายงานจากระบบฐานข้อมูลสหกรณ์ที่ใช้เทคโนโลยีทางการบัญชี กรมตรวจบัญชีสหกรณ์ ณ วันที่ 30 กันยายน 2555 ปรากฏว่า ในจำนวนสหกรณ์ทั้งสิ้น 6,637 สหกรณ์ เป็นสหกรณ์ที่ใช้โปรแกรมระบบบัญชีสหกรณ์ในการประมวลผลข้อมูลถึงจำนวน 3,785 สหกรณ์ หรือคิดเป็นร้อยละ 57.03 ซึ่งนับว่าในระบบสหกรณ์มีการนำเทคโนโลยีมาใช้ในการบริหารจัดการข้อมูลเป็นจำนวนมาก แต่อย่างไรก็ตาม การนำเทคโนโลยีมาใช้ในองค์กรนั้นมีทั้งข้อดีที่ช่วยให้การปฏิบัติงานรวดเร็วและถูกต้องแม่นยำมากขึ้น และข้อเสียก็คือการใช้เทคโนโลยีนั้นจะมีความเสี่ยงมากขึ้นด้วยเช่นกัน ดังนั้น เพื่อให้สหกรณ์ที่ใช้เทคโนโลยีทางการบัญชีได้ตระหนักและมีแนวปฏิบัติในการควบคุมภายใน รวมทั้ง มีแนวทางในการรักษาความปลอดภัย นายทะเบียนสหกรณ์จึงได้ออกระเบียบนายทะเบียนสหกรณ์ ว่าด้วย “มาตรฐานขั้นต่ำในการควบคุมภายในและการรักษาความปลอดภัยสำหรับสหกรณ์และกลุ่มเกษตรกรที่ใช้โปรแกรมระบบบัญชีคอมพิวเตอร์ประมวลผลข้อมูล พ.ศ. 2553” โดยระเบียบนี้มีข้อกำหนดทั้งสิ้นรวม 9 ข้อ

เนื่องจากลักษณะการนำเทคโนโลยีสารสนเทศมาใช้ในแต่ละสหกรณ์มีความแตกต่างกัน ประกอบกับมาตรฐานขั้นต่ำในการควบคุมภายในและการรักษาความปลอดภัยที่กล่าวตามระเบียบนายทะเบียนสหกรณ์นั้นเป็นการกำหนดในภาพกว้างที่สหกรณ์จะต้องนำไปกำหนดวิธีปฏิบัติในรายละเอียดให้เหมาะกับสภาพการใช้เทคโนโลยีสารสนเทศของแต่ละสหกรณ์ ซึ่งปรากฏว่า สหกรณ์ส่วนใหญ่ยังไม่สามารถกำหนดวิธีปฏิบัติได้อย่างเหมาะสม ทั้งนี้ เนื่องจากการกำหนดวิธีปฏิบัตินั้นจำเป็นต้องรู้และเข้าใจหลักการควบคุมภายในและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศที่ถือปฏิบัติตามหลักสากล (Best Practice) เพื่อนำมาประยุกต์เข้ากับลักษณะการดำเนินงานและการใช้เทคโนโลยีสารสนเทศของสหกรณ์ ซึ่งเป็นเรื่องใหม่และยากสำหรับสหกรณ์ ดังนั้น กรมตรวจบัญชีสหกรณ์จึงได้จัดทำแนวปฏิบัติสำหรับการปฏิบัติตามมาตรฐานขั้นต่ำในการควบคุมภายในและการรักษาความปลอดภัยสำหรับสหกรณ์ที่ใช้โปรแกรมระบบบัญชีคอมพิวเตอร์ประมวลผลข้อมูลขึ้น เพื่อให้สหกรณ์นำไปใช้ให้เกิดประโยชน์สามารถป้องกันความเสี่ยงอันเกิดจากการใช้เทคโนโลยีสารสนเทศของสหกรณ์

วัตถุประสงค์

เพื่อให้มีแนวปฏิบัติตามมาตรฐานขั้นต่ำในการควบคุมภายในและการรักษาความปลอดภัยสำหรับสหกรณ์ที่ใช้โปรแกรมระบบบัญชีคอมพิวเตอร์ประมวลผลข้อมูล ที่เหมาะสมตามลักษณะการใช้เทคโนโลยีสารสนเทศของสหกรณ์

ความรู้ทางวิชาการหรือแนวคิดที่ใช้ดำเนินการ

(1) ความรู้ด้านแนวปฏิบัติที่เป็นมาตรฐานสากล (Best Practice) สำหรับการจัดการด้านเทคโนโลยีสารสนเทศในองค์กร ได้แก่ Information Technology Infrastructure Library : ITIL และ Control Objectives for Information and Related Technology : COBIT

(2) ความรู้เกี่ยวกับมาตรฐานขั้นต่ำในการควบคุมภายในและการรักษาความปลอดภัยตามที่นายทะเบียนสหกรณ์กำหนด

(3) ความรู้ด้านระบบการควบคุมภายในและการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ

(4) ความรู้เกี่ยวกับลักษณะการใช้ระบบเทคโนโลยีสารสนเทศของสหกรณ์

สาระสำคัญของผลงาน

สาระสำคัญประกอบด้วย แนวปฏิบัติด้านการจัดการเทคโนโลยีสารสนเทศในองค์กรตามหลักปฏิบัติที่เป็นสากล (Best Practice) มาตรฐาน ITIL (Information Technology Infrastructure Library) ที่กำหนดโดย The Office of Government Commerce (OGC) ประเทศอังกฤษ และมาตรฐาน COBIT (Control Objectives for Information Related Technology) ที่กำหนดโดย The Information Systems Audit and Control Association (ISACA) ประเทศสหรัฐอเมริกา หลักปฏิบัติการควบคุมภายในระบบสารสนเทศที่กำหนดโดยสภาวิชาชีพบัญชี ประเทศไทย หลักปฏิบัติตามที่กำหนดในระเบียบนายทะเบียนสหกรณ์ ว่าด้วย มาตรฐานขั้นต่ำในการควบคุมภายในและการรักษาความปลอดภัยสำหรับสหกรณ์และกลุ่มเกษตรกรที่ใช้โปรแกรมระบบบัญชีคอมพิวเตอร์ประมวลผลข้อมูล พ.ศ. 2553 การออกแบบแนวทางปฏิบัติที่เหมาะสมของสหกรณ์ในแต่ละประเด็นตามที่กำหนดในระเบียบนายทะเบียนสหกรณ์ รวมทั้งวิธีการนำแนวปฏิบัติไปใช้ให้บังเกิดผลในแต่ละสหกรณ์

ประโยชน์ที่คาดว่าจะได้รับ

(1) สหกรณ์ที่ใช้โปรแกรมระบบบัญชีคอมพิวเตอร์ประมวลผลข้อมูล มีแนวทางในการกำหนดวิธีปฏิบัติในการควบคุมภายในและการรักษาความปลอดภัยที่เหมาะสมกับสภาพการใช้เทคโนโลยีของสหกรณ์

(2) สหกรณ์มีความรู้เกี่ยวกับวิธีการควบคุมภายในและการรักษาความปลอดภัยในสถานการณ์ของการนำเทคโนโลยีสารสนเทศมาใช้ในองค์กร

(3) ข้าราชการกรมตรวจบัญชีสหกรณ์มีความรู้ด้านการควบคุมภายในและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ ที่จะช่วยให้คำปรึกษาแนะนำแก่สหกรณ์ได้อย่างเหมาะสม

(4) ผู้สอบบัญชีสหกรณ์มีความรู้ด้านการควบคุมภายในและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศซึ่งเป็นประโยชน์ในการสอบบัญชีสหกรณ์ที่ใช้โปรแกรมระบบบัญชีคอมพิวเตอร์ประมวลผลข้อมูล

บทที่ 2

แนวคิดและทฤษฎีที่เกี่ยวข้อง

บทที่ 2
แนวคิดและทฤษฎีที่เกี่ยวข้อง

การควบคุมภายในระบบเทคโนโลยีสารสนเทศ

การควบคุมภายในระบบเทคโนโลยีสารสนเทศสามารถจำแนกตามลักษณะของการควบคุมได้ 2 ลักษณะ ได้แก่ การควบคุมทั่วไปและการควบคุมเฉพาะระบบงาน ซึ่งระเบียบนายทะเบียนสหกรณ์ว่าด้วย มาตรฐานขั้นต่ำในการควบคุมภายในและการรักษาความปลอดภัยสำหรับสหกรณ์และกลุ่มเกษตรกรที่ใช้โปรแกรมระบบบัญชีคอมพิวเตอร์ประมวลผลข้อมูล พ.ศ. 2553 ให้ความสำคัญกับการควบคุมทั่วไปเป็นหลัก เนื่องจากการควบคุมทั่วไปจะเป็นกรอบป้องกันขั้นพื้นฐานที่จะช่วยในการรักษาความปลอดภัยให้แก่องค์กร

การควบคุมทั่วไปในระบบเทคโนโลยีสารสนเทศ

การควบคุมทั่วไปในระบบเทคโนโลยีสารสนเทศ เป็นการควบคุมในส่วนที่เกี่ยวข้องกับสภาพแวดล้อมของการควบคุมภายใน นโยบายและวิธีการในการควบคุมระบบเทคโนโลยีสารสนเทศ การจัดแบ่งส่วนงานและหน้าที่ความรับผิดชอบ รวมทั้งวิธีการปฏิบัติงานของผู้ที่เกี่ยวข้อง การควบคุมความปลอดภัยของระบบ การควบคุมการพัฒนาและปรับปรุงระบบ และการป้องกันความเสียหายหรือลดความเสียหายของระบบ การควบคุมทั่วไปเป็นการควบคุมภายในระดับองค์กรที่ควรจัดให้มีในทุกส่วนที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ เพื่อให้เกิดความมั่นใจว่าระบบคอมพิวเตอร์ขององค์กรมีเสถียรภาพ สามารถให้บริการได้อย่างต่อเนื่อง และมีระบบการบริหารจัดการที่ดี

การควบคุมทั่วไปในระบบเทคโนโลยีสารสนเทศอาจจัดการได้ด้วยกิจกรรมต่าง ๆ ดังนี้ การกำหนดนโยบายการใช้สารสนเทศ การแบ่งแยกหน้าที่ การควบคุมโครงการพัฒนาระบบสารสนเทศ การควบคุมการเปลี่ยนแปลงแก้ไขระบบ การควบคุมการปฏิบัติงานในหน่วยงานที่ใช้ระบบคอมพิวเตอร์ การควบคุมการเข้าถึงอุปกรณ์คอมพิวเตอร์ การควบคุมการเข้าถึงระบบงาน การควบคุมการเข้าถึงข้อมูลและทรัพยากรสารสนเทศ การควบคุมการจัดเก็บข้อมูล การควบคุมการสื่อสารข้อมูล การกำหนดมาตรฐานเอกสารระบบสารสนเทศ การลดความเสียหายที่อาจเกิดขึ้นกับระบบคอมพิวเตอร์ และการวางแผนแก้ไขความเสียหายจากเหตุฉุกเฉิน

การรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ

การรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ หมายถึง มาตรการที่ใช้สำหรับป้องกันผู้ที่ไม่ได้รับอนุญาตเข้าถึง เพิ่ม ลบ แก้ไขข้อมูลหรือขัดขวางไม่ให้ผู้ที่ได้รับอนุญาตเข้าใช้งานได้

โดยที่หลักการของการรักษาความปลอดภัยคือการรักษาคุณสมบัติในเรื่องของความลับ ความถูกต้อง และความพร้อมใช้งานให้คงไว้ ทั้งนี้ การรักษาความปลอดภัยจะเกิดประสิทธิภาพสูงสุดได้ต้องเกิดจากการประสานกันระหว่าง ความร่วมมือของผู้ปฏิบัติ (People) ความชัดเจนของกระบวนการที่กำหนด (Process) และเครื่องมือหรือเทคโนโลยีที่ใช้ (Technology)

องค์ประกอบหลักของความปลอดภัยของข้อมูล

ในระบบเทคโนโลยีสารสนเทศซึ่งประกอบด้วย ฮาร์ดแวร์ ซอฟต์แวร์ เครือข่าย กระบวนการ คน และข้อมูล นั้น ส่วนของข้อมูลนับเป็นองค์ประกอบที่มีค่ามากที่สุดขององค์กร ดังนั้น การรักษาความปลอดภัยของข้อมูลจึงเป็นสิ่งสำคัญจำเป็นที่จะต้องควบคุมดูแลให้เกิดความมั่นคงปลอดภัยสูงสุด โดยองค์กรจะต้องจัดเป็นกระบวนการควบคุมในเชิงรุกเพื่อบริหารความเสี่ยง (Risk Management) ให้อยู่ในระดับที่ยอมรับได้ การจัดการในเชิงรุกนั้นเป็นขั้นตอนที่ต้องทำก่อนที่จะเกิดเหตุการณ์นั้นขึ้น ในทางกลับกันถ้าองค์กรกำหนดการรักษาความปลอดภัยเป็นแบบตั้งรับ ค่าใช้จ่ายของระบบการรักษาความปลอดภัยของข้อมูลนั้นก็จะสูงหรืออาจจะไม่สามารถประเมินได้

ความปลอดภัยของข้อมูลวิเคราะห์จากความครบถ้วนของคุณสมบัติทั้ง 3 ด้านคือ ความลับ ความถูกต้อง และความพร้อมใช้งาน ถ้าขาดคุณสมบัติด้านใดด้านหนึ่งแสดงว่าข้อมูลนั้นไม่มีความปลอดภัย ดังนั้น การรักษาความปลอดภัยข้อมูลจึงเป็นการปกป้องรักษาคุณสมบัติทั้ง 3 ด้าน ดังนี้

1. ความลับ (Confidentiality) การทำให้ข้อมูลสามารถเข้าถึงหรือเปิดเผยได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น
2. ความถูกต้อง (Integrity) การรักษาความคงสภาพจากแหล่งที่มาต้นทางหรือไม่ได้ถูกแก้ไขโดยผู้ที่ไม่ได้รับอนุญาต
3. ความพร้อมใช้งาน (Availability) การทำให้ผู้ที่ได้รับอนุญาตสามารถเข้าถึงข้อมูลได้เมื่อต้องการ

มาตรฐานการรักษาความปลอดภัยของข้อมูล

เพื่อป้องกันการดำเนินธุรกิจให้สามารถดำเนินการได้อย่างต่อเนื่อง และเสริมสร้างความเชื่อมั่นให้แก่ผู้รับบริการ หลาย ๆ องค์กรได้นำมาตรฐานเกี่ยวกับการรักษาความปลอดภัยของข้อมูลมาใช้เพื่อให้การดำเนินการเกิดประสิทธิภาพและเกิดความน่าเชื่อถือในกระบวนการควบคุมข้อมูลว่าเป็นไปอย่างมีระบบ เช่น มาตรฐาน ITIL มาตรฐาน COBIT หรือมาตรฐานทางวิชาชีพบัญชี เป็นต้น

มาตรฐาน ITIL

มาตรฐาน ITIL (The Information Technology Infrastructure Library) เป็นหลักการที่พัฒนาขึ้นด้วยความร่วมมือระหว่างภาครัฐบาลและภาคเอกชน ประเทศอังกฤษ ที่ตระหนักถึงคุณภาพของการให้บริการด้านเทคโนโลยีสารสนเทศ ซึ่งพบว่าปัญหาที่เกิดขึ้นในการให้บริการด้านเทคโนโลยีสารสนเทศไม่ได้เกิดจากระบบงานหรือบุคลากรที่ให้บริการ แต่เกิดจากกระบวนการทำงานที่ไม่เป็นระบบ หรือไม่มีระบบการจัดการที่ดีพอ จึงได้มีการกำหนดหลักการด้านการจัดการเทคโนโลยีสารสนเทศในองค์กรขึ้น เพื่อใช้เป็นแนวทางในการจัดการระบบการให้บริการด้านเทคโนโลยีสารสนเทศ ภายใต้การควบคุมและพัฒนาของ OGC (United Kingdom's Office of Government Commerce)

มาตรฐาน ITIL มีวัตถุประสงค์เพื่อกำหนดแนวปฏิบัติที่ดีที่สุด (Best Practices) สำหรับกระบวนการของการส่งมอบงานและการให้บริการด้านเทคโนโลยีสารสนเทศ สาระสำคัญของ ITIL เน้นที่วงจรการให้บริการด้วยระบบเทคโนโลยีสารสนเทศ (Integrated service lifecycle approach) เพื่อให้เหมาะสมกับงานบริการ โดยที่เทคโนโลยีสารสนเทศต้องทำงานสอดคล้องกับการดำเนินงานทางธุรกิจ และสามารถสร้างคุณค่าจากการใช้เทคโนโลยีสารสนเทศได้ ซึ่งผู้บริหารต้องพิจารณาถึงความคุ้มค่าจากการลงทุนด้านเทคโนโลยีสารสนเทศที่มีค่าใช้จ่ายค่อนข้างสูงมากในปัจจุบัน

มาตรฐาน ITIL ได้แบ่งแนวทางในการปฏิบัติออกเป็น 5 ด้าน ดังนี้

- **ยุทธศาสตร์งานบริการ (Service Strategy)** เป็นจุดเริ่มต้นของกระบวนการ ITIL ประกอบด้วยข้อกำหนดเกี่ยวกับแนวทางในการแบ่งประเภทการให้บริการและการจัดลำดับความสำคัญในการลงทุนการให้บริการ ในส่วนนี้จะเป็นข้อแนะนำสำหรับหน่วยงานในด้านเทคโนโลยีสารสนเทศเพื่อการปรับปรุงพัฒนาในระยะยาว แนวคิดที่สำคัญ เช่น คำจำกัดความของการให้บริการอย่างมีคุณค่า การพัฒนาธุรกิจ ทรัพยากรที่เกี่ยวข้องกับการให้บริการ การวิเคราะห์การตลาด และการแบ่งประเภทของผู้ให้บริการ เป็นต้น กระบวนการที่ครอบคลุมในกลุ่มนี้ คือ การบริหารการบริการที่หลากหลาย การบริหารความต้องการ และการบริหารงบประมาณที่ลงทุนด้านเทคโนโลยีสารสนเทศ

- **การออกแบบงานบริการ (Service Design)** เน้นการออกแบบกิจกรรมที่จะเกิดขึ้นในกระบวนการให้บริการ รวมทั้งการพัฒนากลยุทธ์และวิธีการบริหารจัดการระบบบริการ หลักสำคัญได้แก่ การบริหารความพร้อมที่จะให้บริการ การบริหารขีดความสามารถในการให้บริการอย่างรวดเร็วและมีประสิทธิภาพ รวมทั้งการบริหารความสามารถในการให้บริการอย่างต่อเนื่อง และการบริหารระบบการรักษาความปลอดภัย

- **การส่งมอบงานบริการ (Service Transition)** เน้นการดำเนินการเพื่อให้ได้ผลลัพธ์ของการบริการที่ดีที่สุด รวมทั้งการสรรค์สร้างวิธีการบริการใหม่ ๆ ขึ้น ตลอดจนการปรับปรุงวิธีการบริการที่มีอยู่แล้วโดยมีข้อมูลบางส่วนคาบเกี่ยวกับการส่งมอบงานและการปฏิบัติงาน หลักสำคัญของการส่งมอบงาน ได้แก่ การบริหารการเปลี่ยนแปลง การบริหารการปรับค่าของระบบ การบริหารการส่งมอบใช้งาน และการบริหารความรู้เกี่ยวกับการให้บริการ

- **การปฏิบัติงานบริการ (Service Operation)** ให้ความสำคัญกับกิจกรรมที่จำเป็นต่อการปฏิบัติงานเพื่อให้บรรลุผลสำเร็จในการดูแลรักษาให้การทำงานหรือบริการเป็นไปตามข้อตกลงว่าด้วยพันธะสัญญาบริการ (Service Level Agreement) ที่มีต่อลูกค้า หลักสำคัญของการให้บริการได้แก่ การบริหารเหตุการณ์ การบริหารปัญหา และการเติมเต็มความต้องการ

- **การปรับปรุงงานบริการอย่างต่อเนื่อง (Continual Service Improvement)** เน้นขีดความสามารถที่จะทำให้เกิดการปรับปรุงการให้บริการที่มีคุณภาพอยู่แล้วให้มีความต่อเนื่อง โดยมีหลักอยู่ที่การรายงานการให้บริการ การประเมินการให้บริการ และการบริหารระดับการให้บริการ

มาตรฐาน ITIL เป็นแนวทางในการจัดการระบบเทคโนโลยีสารสนเทศที่สามารถนำไปปรับใช้กับองค์กร ซึ่งจะก่อให้เกิดประโยชน์ต่อองค์กรหลายประการ ไม่ว่าจะเป็นการปรับปรุงการใช้งานทรัพยากรที่มีอยู่ได้คุ้มค่ามากขึ้น การเสริมสร้างความสามารถในการแข่งขันกับคู่แข่งในตลาด การลดเวลาโดยไม่ทำงานซ้ำซ้อนหรือลดงานที่ไม่จำเป็นลง การจัดการให้การดำเนินการโครงการแล้วเสร็จตามแผนที่กำหนดไว้ การเพิ่มขีดความสามารถในการให้บริการด้านเทคโนโลยีสารสนเทศแก่ลูกค้าให้สูงขึ้น การควบคุมต้นทุนของการให้บริการที่มีคุณภาพตามที่กำหนดได้ การดูแลการให้บริการที่มีคุณภาพแก่ลูกค้าได้ตามที่กำหนดในสัญญา และการจัดระบบการรักษาความปลอดภัยในกรณีที่เกิดเหตุฉุกเฉิน

มาตรฐาน COBIT

มาตรฐาน COBIT (Control Objective for Information and related Technology) เป็นแนวทางในการปฏิบัติสำหรับการบริหารองค์กรที่ใช้เทคโนโลยีสารสนเทศ ซึ่งสมาคมผู้ตรวจสอบและควบคุมระบบสารสนเทศ หรือ ISACA (Information Systems Audit and Control Association) เป็นหน่วยงานที่กำหนดและกำกับดูแลมาตรฐาน COBIT มาตรฐาน COBIT นี้องค์กรสามารถนำไปปรับใช้ในกิจกรรมทางด้านเทคโนโลยีสารสนเทศเพื่อให้มีระบบการควบคุมภายในที่รัดกุม โดยการรวบรวมจากวิธีปฏิบัติในอดีตที่ประสบความสำเร็จในการดำเนินการซึ่งถือเป็นแนวปฏิบัติที่ดี (Best Practice) ที่จะก่อให้เกิดประโยชน์สูงสุดต่อองค์กร

มาตรฐาน COBIT จัดแบ่งแนวทางปฏิบัติเป็นกระบวนการ และได้กำหนดวัตถุประสงค์ของการควบคุมหลักของแต่ละกระบวนการด้วย โดยแบ่งเป็น 4 กระบวนการ ดังนี้

1. การวางแผนและการจัดการองค์กร (PO : Planning and Organization)
2. การจัดหาและการติดตั้งใช้งาน (AI : Acquisition and Implementation)
3. การส่งมอบและการบริการ (DS : Delivery and Support)
4. การติดตามและการประเมินผล (ME : Monitor and Evaluate)

การวางแผนและการจัดการองค์กร (PO : Planning and Organization)

การวางแผนและการจัดการองค์กร เป็นส่วนที่กำหนดวิธีที่ทำให้เทคโนโลยีสารสนเทศมีบทบาทสำคัญและสนองตอบความต้องการขององค์กร ประกอบด้วย 10 กระบวนการย่อย ดังนี้

1. การจัดทำแผนยุทธศาสตร์ด้านเทคโนโลยีสารสนเทศ เพื่อให้องค์กรได้รับประโยชน์สูงสุดจากการใช้ IT โดยรวม ทั้งแผนงานระยะสั้นและระยะยาว และมีการติดตามและประเมินผลการดำเนินงานตามแผนงานนั้น

2. การกำหนดโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ เพื่อให้ได้รับประโยชน์สูงสุดจากการจัดรูปแบบระบบเทคโนโลยีสารสนเทศ รวมถึงการจัดประเภทของข้อมูลและระดับการรักษาความปลอดภัยของข้อมูล

3. การกำหนดทิศทางแนวโน้มของเทคโนโลยี เพื่อให้สามารถใช้เทคโนโลยีที่ทันสมัยเป็นกลยุทธ์ในการบริหารองค์กร และสามารถวางแผนการจัดซื้อฮาร์ดแวร์และซอฟต์แวร์ได้

4. การกำหนดกระบวนการ จัดโครงสร้างองค์กร และกำหนดความสัมพันธ์กับหน่วยงานด้านเทคโนโลยีสารสนเทศ เพื่อให้สามารถให้บริการด้านเทคโนโลยีสารสนเทศได้อย่างเหมาะสม

5. การบริหารการลงทุนด้านเทคโนโลยีสารสนเทศ เพื่อให้มั่นใจในเงินทุนที่ต้องใช้ และมีการดูแลการใช้จ่ายเงินอย่างเหมาะสม

6. การประชาสัมพันธ์เป้าหมายและทิศทาง เพื่อให้แน่ใจว่าคนในองค์กรรับรู้ และเข้าใจเป้าหมายและทิศทางที่องค์กรกำลังดำเนินไป

7. การจัดการทรัพยากรบุคคลด้านเทคโนโลยีสารสนเทศ เพื่อให้บุคลากรที่มีความสามารถ และทุ่มเทในการทำงาน

8. การจัดการคุณภาพ เพื่อให้สามารถตอบสนองความต้องการของผู้ใช้งานได้

9. การประเมินและบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อให้เทคโนโลยีสารสนเทศสามารถตอบสนองความต้องการของผู้บริหารในการตัดสินใจเพื่อลดความเสี่ยง โดยให้ข้อมูลที่เป็นรูปธรรมและชี้ให้เห็นประเด็นที่สำคัญ

10. การบริหารโครงการ เพื่อกำหนดระดับความสำคัญ และดำเนินการให้แล้วเสร็จภายในเวลาและงบประมาณที่กำหนด

การจัดหาและการติดตั้งใช้งาน (AI : Acquisition and Implementation)

1. การเลือกใช้ระบบอัตโนมัติ เพื่อให้มั่นใจว่าจะตอบสนองความต้องการข้อมูลของผู้ใช้งานได้อย่างมีประสิทธิผลและประสิทธิภาพ

2. การจัดหาและบำรุงรักษาซอฟต์แวร์ประยุกต์ เพื่อให้บริการประมวลผลที่สนับสนุนการดำเนินงานและการปฏิบัติงานขององค์กรได้อย่างมีประสิทธิภาพ

3. การจัดหาและบำรุงรักษาโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ เพื่อให้องค์กรมีระบบเทคโนโลยีสารสนเทศที่เหมาะสมกับระบบงาน

4. การปฏิบัติการและการใช้งาน เพื่อใช้ประโยชน์สูงสุดจากระบบเทคโนโลยีสารสนเทศที่มีอยู่

5. การจัดหาทรัพยากรด้านเทคโนโลยีสารสนเทศ เพื่อให้มีทรัพยากรที่เพียงพอและจำเป็นสำหรับการดำเนินธุรกิจ

6. การบริหารการเปลี่ยนแปลง เพื่อลดโอกาสการหยุดชะงัก การแก้ไขโดยพลการ และความผิดพลาด

7. การติดตั้งและใช้งานระบบพร้อมปรับปรุงให้เหมาะสม เพื่อให้มีระบบที่สามารถใช้งานได้อย่างถูกต้องมีประสิทธิภาพ

การส่งมอบและการบริการ (DS : Delivery and Support)

1. การกำหนดและการจัดการระดับการให้บริการ เพื่อให้เกิดความเข้าใจที่ถูกต้องของระดับบริการที่เป็นที่ต้องการ

2. การจัดการการใช้บริการจากบุคคลภายนอก เพื่อให้มั่นใจว่ามีการกำหนดหน้าที่และความรับผิดชอบของบุคคลภายนอกไว้อย่างชัดเจน และมีการดำเนินการที่ถูกต้องต่อเนื่อง

3. การจัดการด้านประสิทธิภาพและ เพื่อให้มั่นใจได้ว่าระบบมีศักยภาพที่เหมาะสมสามารถใช้ประโยชน์ได้สูงสุด และให้บริการได้ตามที่กำหนด

4. การทำให้มีความต่อเนื่องในการให้บริการ เพื่อให้มั่นใจว่าบริการด้านเทคโนโลยีสารสนเทศมีให้ใช้ได้ตามที่ต้องการ และหากมีเหตุการณ์สำคัญที่ทำให้ระบบต้องหยุดชะงักจะเกิดปัญหาต่อการดำเนินธุรกิจน้อยที่สุด

5. การรักษาความปลอดภัยระบบ เพื่อปกป้องข้อมูลจากการถูกใช้เปิดเผย แก้ไข ทำลายโดยไม่ได้รับอนุมัติหรือการสูญหาย

6. การกำหนดและจัดสรรต้นทุน เพื่อให้เกิดการรับรู้ต้นทุนการให้บริการด้านเทคโนโลยีสารสนเทศอย่างถูกต้อง

7. การให้ความรู้และฝึกอบรมผู้ใช้งาน เพื่อให้มั่นใจว่าผู้ใช้สามารถใช้บริการได้อย่างมีประสิทธิภาพ และเข้าใจถึงความเสี่ยง ความรับผิดชอบที่เกี่ยวเนื่องจากการใช้นั้นๆ

8. การบริหารการให้บริการและเหตุการณ์ เพื่อให้มั่นใจว่า ปัญหาที่ผู้ใช้ประสบได้รับการแก้ไขอย่างเหมาะสม

9. การจัดการค่าของระบบและอุปกรณ์ เพื่อให้มีการดูแลรักษาจดบันทึกอย่างเหมาะสมในอุปกรณ์ด้านเทคโนโลยีสารสนเทศ ป้องกันการแก้ไขเปลี่ยนแปลงโดยไม่ได้รับอนุญาต มีการตรวจนับและมีระบบการควบคุมการเปลี่ยนแปลง

10. การจัดการปัญหาที่เกิดขึ้น เพื่อให้มั่นใจว่าปัญหาและอุบัติเหตุที่เกิดขึ้น ได้รับการแก้ไข และป้องกันไม่ให้เกิดขึ้นซ้ำอีก

11. การจัดการข้อมูล เพื่อให้มั่นใจว่าข้อมูลมีความสมบูรณ์ ถูกต้องและน่าเชื่อถือ ทั้งในช่วงการนำข้อมูลเข้าระบบ การปรับปรุงแก้ไข และการจัดเก็บในระบบ

12. การจัดการด้านสิ่งอำนวยความสะดวก เพื่อให้มีสภาพแวดล้อมทางกายภาพที่เหมาะสมในการปกป้องอุปกรณ์ด้านเทคโนโลยีสารสนเทศและบุคลากรจากภัยที่อาจเกิดขึ้น

13. การจัดการด้านการปฏิบัติการ เพื่อให้มั่นใจว่าการปฏิบัติการด้านเทคโนโลยีสารสนเทศที่สำคัญ มีการดำเนินงานอย่างสม่ำเสมอและเป็นลำดับอย่างเหมาะสม

การติดตามและการประเมินผล (ME : Monitor and Evaluate)

1. การเฝ้าติดตามและประเมินกระบวนการด้านเทคโนโลยีสารสนเทศ เพื่อให้มั่นใจว่ากิจกรรมด้านเทคโนโลยีสารสนเทศ สามารถบรรลุเป้าหมายการปฏิบัติงานตามที่กำหนด

2. การเฝ้าติดตามและประเมินการควบคุมภายใน เพื่อให้มั่นใจว่าเป้าหมายของการควบคุมภายในของกิจกรรมด้านเทคโนโลยีสารสนเทศ สามารถบรรลุผลตามที่กำหนด

3. การปฏิบัติตามกฎระเบียบ เพื่อหลีกเลี่ยงการกระทำผิดต่อระเบียบ กฎหมาย และศีลธรรมจรรยาบรรณ

4. การให้บริการตามหลักธรรมาภิบาล ซึ่งเป็นหลักการที่นำมาใช้บริหารงานปกครองในปัจจุบัน

มาตรฐาน COBIT เป็นทั้งแนวคิดและแนวปฏิบัติ (Framework) ที่มุ่งเน้นในการยกระดับประสิทธิภาพของระบบเทคโนโลยีสารสนเทศให้เป็นส่วนผลักดันงานขององค์กร โดยกำหนดแนวทางอย่างครอบคลุมครบทุกด้านของการดำเนินงานด้านเทคโนโลยีสารสนเทศ ซึ่งจะทำให้การนำเอาระบบเทคโนโลยีสารสนเทศมาใช้ในองค์กรเกิดประโยชน์ คุ้มค่าต่อการลงทุน และสนับสนุนการดำเนินธุรกิจให้ประสบผลสำเร็จ

มาตรฐานการสอบบัญชี รหัส 401

มาตรฐานการสอบบัญชีที่เกี่ยวกับการตรวจสอบระบบสารสนเทศที่ใช้คอมพิวเตอร์ คือ มาตรฐานการสอบบัญชี รหัส 401 “การสอบบัญชีในสภาพแวดล้อมของระบบสารสนเทศที่ใช้คอมพิวเตอร์” กำหนดเกี่ยวกับการสอบบัญชีกิจการที่ประมวลผลข้อมูลด้วยคอมพิวเตอร์ สภาพแวดล้อมของระบบสารสนเทศที่ใช้คอมพิวเตอร์เกิดขึ้นเมื่อมีการใช้คอมพิวเตอร์ไม่ว่าประเภทใดหรือขนาดใดในการประมวลผลข้อมูลทางการเงินซึ่งมีความสำคัญต่อการสอบบัญชี ทั้งนี้ ไม่ว่าการประมวลผลนั้นจะดำเนินการโดยกิจการหรือมอบหมายให้บุคคลภายนอกดำเนินการ ผู้สอบบัญชีควรมีความรู้เกี่ยวกับระบบสารสนเทศที่ใช้คอมพิวเตอร์อย่างเพียงพอ เพื่อวางแผน สั่งการ ควบคุมดูแล และสอบทานงานที่ได้ปฏิบัติ รวมทั้งต้องพิจารณาว่าจำเป็นต้องใช้ผู้เชี่ยวชาญด้านระบบสารสนเทศช่วยในการตรวจสอบหรือไม่

การตรวจสอบระบบสารสนเทศที่ใช้คอมพิวเตอร์ เป็นการตรวจเพื่อแสดงความเห็นต่อระบบการควบคุมสารสนเทศที่องค์กรใช้ว่าเหมาะสมและเป็นไปตามวัตถุประสงค์ของการควบคุมที่กำหนดไว้หรือไม่ ทั้งนี้ ต้องเข้าใจว่าวัตถุประสงค์ของการควบคุมอาจกำหนดโดยผู้บริหารหรือผู้ออกแบบระบบ แต่ผู้ตรวจสอบจะตรวจสอบเพื่อให้ความมั่นใจว่าระบบที่ออกแบบไว้นั้นยังคงเพียงพอ เหมาะสม มีการปฏิบัติตาม และได้ผลตามวัตถุประสงค์ที่กำหนดไว้หรือไม่อย่างไร การตรวจสอบระบบสารสนเทศที่ใช้คอมพิวเตอร์นั้นดำเนินการเพื่อให้ทราบว่า ระบบสารสนเทศที่กิจการใช้ในการประมวลผลข้อมูลที่จำเป็นต่อการจัดทำงบการเงินและการตรวจสอบ มีการทำงานตามที่กำหนดไว้หรือไม่ รวมทั้งรายการทางบัญชีที่บันทึกอยู่ในระบบและข้อมูลที่ออกจากระบบมีความถูกต้อง ครบถ้วน และสะท้อนสถานะทางการเงินที่แท้จริงของกิจการเพียงใด

ระบบสารสนเทศทางการบัญชี

ระบบสารสนเทศทางการบัญชีเป็นส่วนหนึ่งของระบบสารสนเทศขององค์กร ที่เก็บรวบรวมและประมวลผลข้อมูล ทั้งข้อมูลที่เกี่ยวข้องกับเงินตราและข้อมูลที่ไม่เกี่ยวข้องกับเงินตรา จากระบบงานย่อยต่าง ๆ ขององค์กร และสื่อสารข้อมูลหรือสารสนเทศที่รวบรวมได้ไปยังผู้ใช้ทุกคนขององค์กร ระบบสารสนเทศทางการบัญชีมีองค์ประกอบที่สำคัญ คือ บุคลากรที่ปฏิบัติงานในแต่ละส่วน ขั้นตอนการปฏิบัติงาน และเทคโนโลยีสารสนเทศ ทั้งระบบคอมพิวเตอร์ ระบบเครือข่ายและโปรแกรมระบบบัญชีคอมพิวเตอร์ที่เลือกใช้ โดยหน้าที่หลักของระบบสารสนเทศทางการบัญชี ดังนี้

1. เก็บรวบรวม บันทึก และจัดเก็บเหตุการณ์ทางธุรกิจ รายการค้า และสรุปผลในรายงานทางการเงิน

2. ประมวลผลเหตุการณ์ทางธุรกิจและรายการค้า เพื่อนำเสนอสารสนเทศให้ผู้บริหารนำไปใช้ในการตัดสินใจได้อย่างมีประสิทธิภาพ

3. มีระบบการควบคุมที่สามารถปกป้องสินทรัพย์ของกิจการรวมทั้งข้อมูลต่าง ๆ โดยระบบการควบคุมจะต้องสามารถควบคุมความถูกต้อง ความน่าเชื่อถือ และความพร้อมงานของข้อมูล

โปรแกรมระบบบัญชีคอมพิวเตอร์

ในระบบสารสนเทศทางการบัญชีที่ประมวลผลด้วยคอมพิวเตอร์นั้น จำเป็นต้องใช้โปรแกรมระบบบัญชีคอมพิวเตอร์ในการสั่งการให้เครื่องคอมพิวเตอร์บันทึกข้อมูล ประมวลผล จัดทำรายงานทางการเงินและรายงานเพื่อการบริหารเสนอต่อผู้ใช้ที่เกี่ยวข้อง ประโยชน์ที่ได้รับจากการนำโปรแกรมระบบบัญชีคอมพิวเตอร์มาใช้นั้นมีอยู่หลายประการ เช่น ทำให้กิจการทราบฐานะการเงินและผลการดำเนินงานได้อย่างรวดเร็วทันเวลา การปฏิบัติงานด้านบัญชีมีความสะดวก และถูกต้องแม่นยำมากยิ่งขึ้น ผู้บริหารสามารถเรียกดูข้อมูลที่เก็บไว้ในฐานข้อมูลมาใช้ในการบริหารงานได้ตลอดเวลา เป็นต้น สำหรับการจัดหาโปรแกรมระบบบัญชีคอมพิวเตอร์นั้นองค์กรสามารถจัดหาโปรแกรมระบบบัญชีคอมพิวเตอร์ได้โดยการพัฒนาขึ้นมาใช้เองในกิจการ หรือจัดซื้อโปรแกรมระบบบัญชีคอมพิวเตอร์สำเร็จรูปตามคุณสมบัติที่ต้องการ

บทที่ 3

มาตรฐานขั้นต่ำในการควบคุมภายในและการรักษาความปลอดภัย สำหรับสหกรณ์

บทที่ 3

มาตรฐานขั้นต่ำในการควบคุมภายในและการรักษาความปลอดภัยสำหรับสหกรณ์

ลักษณะการดำเนินงานของสหกรณ์

สหกรณ์เป็นนิติบุคคลที่จัดตั้งขึ้นโดยจดทะเบียนตามพระราชบัญญัติสหกรณ์ พ.ศ. 2542 (แก้ไขเพิ่มเติม พ.ศ. 2553) มีลักษณะการดำเนินธุรกิจใน 5 ธุรกิจหลัก ได้แก่ ธุรกิจสินเชื่อ ธุรกิจการรับฝากเงิน ธุรกิจการจัดหาสินค้ามาจำหน่าย ธุรกิจรวบรวมผลิตผล และธุรกิจส่งเสริมการเกษตร ซึ่งในการดำเนินธุรกิจของสหกรณ์นั้นจำเป็นที่จะต้องมีการนำระบบเทคโนโลยีสารสนเทศมาใช้เป็นเครื่องมือในการดำเนินการเพื่อเพิ่มประสิทธิภาพในการให้บริการแก่สมาชิกและใช้ในการประมวลผลข้อมูลทางการเงินเพื่อจัดทำรายงานทางการเงินเสนอต่อคณะกรรมการดำเนินการ รวมทั้งเพื่อเพิ่มประสิทธิภาพในการให้บริการสมาชิก

การใช้เทคโนโลยีสารสนเทศของสหกรณ์

โปรแกรมระบบบัญชีคอมพิวเตอร์ เป็นเทคโนโลยีสารสนเทศทางการบัญชีที่นำมาใช้ในสหกรณ์ ซึ่งสามารถจำแนกการใช้โปรแกรมระบบบัญชีคอมพิวเตอร์ ได้ดังนี้

1. โปรแกรมระบบบัญชีสำหรับสหกรณ์ออมทรัพย์ ใช้สำหรับการบันทึกรายการบัญชีของสหกรณ์ที่ดำเนินธุรกิจทางด้านการเงินเป็นหลักได้แก่ การให้สินเชื่อ การรับฝากเงิน และมีการประมวลผลเพื่อเรียกเก็บค่าหุ้นและเรียกเก็บเงินชำระหนี้เป็นประจำทุกเดือน โดยมีการเชื่อมโยงการทำงานระหว่างระบบงานย่อย รวมทั้งการเชื่อมโยงจากระบบงานย่อยกับระบบการเงินเพื่อรวบรวมผ่านรายการไปบันทึกบัญชีแยกประเภทที่เกี่ยวข้อง ประกอบด้วย 5 ระบบงานย่อย ดังนี้

1.1 ระบบสมาชิกและหุ้น เป็นระบบที่จัดการเกี่ยวกับประวัติสมาชิกและการถือหุ้น จัดได้ว่าเป็นฐานข้อมูลหลักของสหกรณ์ เพราะเป็นระบบที่เก็บประวัติของสมาชิกและประวัติการสะสมหุ้นของสมาชิกที่จะถูกนำไปใช้ในการทำธุรกรรมในระบบงานอื่น ๆ

1.2 ระบบเงินให้กู้ เป็นระบบที่จัดการเกี่ยวกับสัญญาเงินกู้ ตั้งแต่การที่สมาชิกขอกู้ การจ่ายเงินกู้ การค้ำประกัน การคำนวณดอกเบี้ยรับจากเงินให้กู้ จนกระทั่งปิดสัญญาเงินกู้

1.3 ระบบเงินรับฝาก เป็นระบบที่จัดการเกี่ยวกับกระบวนการเกี่ยวกับเงินที่สมาชิกนำมาฝากไว้กับสหกรณ์ ตั้งแต่การขอเปิดบัญชีเงินฝาก การรับฝาก การจ่ายคืน

เงินรับฝาก การคำนวณดอกเบี้ยจ่ายเงินรับฝาก การทบดอกเบี้ยเป็นต้นเงิน จนกระทั่งการปิดบัญชีเงินฝาก

1.4 ระบบการเงิน เป็นระบบที่ทำหน้าที่ประมวลผลเพื่อเรียกเก็บเงินประจำเดือนจากสมาชิกและเป็นศูนย์รวมของข้อมูล เพราะระบบการเงินจะทำหน้าที่ในการติดต่อกับระบบงานย่อยทุกระบบ

1.5 ระบบบัญชีแยกประเภท ทำหน้าที่ในการบันทึกรายการบัญชี ทั้งการบันทึกโดยตรงผ่านหน้าจอรับข้อมูลและการเชื่อมโยงข้อมูลจากการผ่านรายการอัตโนมัติจากระบบอื่น ๆ และทำหน้าที่ประมวลผลเพื่อจัดทำรายงานงบการเงิน

2. โปรแกรมระบบบัญชีสำหรับสหกรณ์ภาคเกษตร/บริการ/เครดิตยูเนี่ยน ใช้สำหรับการบันทึกรายการบัญชีของสหกรณ์ที่มีธุรกิจทั้งการให้สินเชื่อ การรับฝากเงิน การจัดหาสินค้ามาจำหน่าย และการให้บริการ สหกรณ์ที่มีการดำเนินธุรกิจดังกล่าว ได้แก่ สหกรณ์การเกษตร สหกรณ์ประมง สหกรณ์นิคม สหกรณ์ร้านค้า สหกรณ์บริการ และสหกรณ์เครดิตยูเนี่ยน โดยแบ่งออกเป็นระบบงาน ดังนี้

2.1 ระบบสมาชิกและหุ้น ใช้ในการจัดการฐานข้อมูลสมาชิกและหุ้น โดยเริ่มตั้งแต่การที่สมาชิกได้รับอนุมัติให้เป็นสมาชิก การรับค่าหุ้นและค่าธรรมเนียมแรกเข้า การที่สมาชิกซื้อหุ้นเพิ่ม การลาออกและจ่ายคืนค่าหุ้น

2.2 ระบบเงินให้กู้ เป็นโปรแกรมที่ทำหน้าที่ในการจัดการสัญญาเงินกู้โดยเริ่มตั้งแต่สมาชิกได้รับอนุมัติเงินกู้เพื่อดำเนินการจัดทำสัญญาเงินกู้ การจ่ายเงินกู้ การรับชำระเงินกู้ การประมวลผลดอกเบี้ยรับ และการคำนวณค่าปรับ

2.3 ระบบเงินรับฝาก เป็นระบบที่จัดการเกี่ยวกับบัญชีเงินฝากที่สมาชิกมาฝากไว้กับสหกรณ์ ตั้งแต่การขอเปิดบัญชีเงินฝาก การรับฝาก การถอนเงิน การคำนวณดอกเบี้ยจ่ายเงินรับฝาก การทบดอกเบี้ยเป็นต้นเงิน จนกระทั่งการปิดบัญชีเงินฝาก รวมทั้งการจัดการเกี่ยวกับการพิมพ์สมุดคู่ฝาก

2.4 ระบบสินค้า ใช้ในการบริหารจัดการเกี่ยวกับการซื้อ - ขายสินค้า การขายสินค้าผ่านเครื่องรับเงิน การคำนวณต้นทุนสินค้า การคำนวณส่วนลด การจัดทำรายงานสินค้าคงเหลือ และการจัดทำรายงานภาษีซื้อ และภาษีขายในกรณีที่สหกรณ์อยู่ในระบบภาษีมูลค่าเพิ่ม

2.5 ระบบบัญชีแยกประเภท ใช้สำหรับการบันทึกรายการบัญชีและจัดทำงบการเงิน

3. โปรแกรมระบบบัญชีสำหรับสหกรณ์การเกษตรเพื่อการตลาดลูกค้า ธ.ก.ส. (สกต.) เป็นชุดโปรแกรมที่มีลักษณะเฉพาะ ได้แก่ การไม่มีธุรกิจสินเชื่อ การมีสาขาอยู่ทุกอำเภอ การมีปริมาณข้อมูลจำนวนมาก เนื่องจากมีสมาชิกมาก รวมทั้งการที่ต้องเชื่อมโยงข้อมูลกับระบบงานของธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร

3.1 ระบบสมาชิกและหุ้น ใช้ในการจัดการฐานข้อมูลสมาชิกและหุ้น ทั้งการรับสมัครสมาชิกที่สหกรณ์และการรับสมัครสมาชิกผ่าน ธ.ก.ส. โดยเริ่มตั้งแต่การที่สมาชิกได้รับอนุมัติให้เป็นสมาชิก การรับค่าหุ้นและค่าธรรมเนียมแรกเข้า การซื้อหุ้นเพิ่ม การลาออกและจ่ายคืนค่าหุ้น

3.2 ระบบสินค้า ใช้ในการบริหารจัดการเกี่ยวกับการซื้อ - ขายสินค้า การจัดทำทะเบียนคุมสินค้า และการจัดทำรายงานภาษีซื้อ และภาษีขายในกรณีที่สหกรณ์อยู่ในระบบภาษีมูลค่าเพิ่ม

3.3 ระบบบัญชีแยกประเภท ใช้สำหรับการบันทึกรายการบัญชีและจัดทำงบการเงิน

3.4 ระบบเชื่อมโยง ธ.ก.ส. เป็นโปรแกรมที่ทำหน้าที่ในการเชื่อมต่อระหว่างฐานข้อมูลสมาชิกและหุ้นและฐานข้อมูลเงินปันผลและเฉลี่ยคืนของโปรแกรมระบบบัญชี สกต. กับฐานข้อมูลของธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร จำกัด โดยการส่งข้อมูลเงินปันผลและเฉลี่ยคืนออกไปให้ ธ.ก.ส. และรับข้อมูลประวัติสมาชิกเข้าใหม่และการซื้อหุ้นเพื่อมาพิมพ์ใบเสร็จรับเงินและปรับปรุงทะเบียนสมาชิกและหุ้น

4. โปรแกรมระบบบัญชีสำหรับสหกรณ์ร้านค้า

4.1 ระบบสมาชิกและหุ้น ใช้ในการจัดการฐานข้อมูลสมาชิกและหุ้น ทั้งการรับสมัครสมาชิกที่สหกรณ์และการรับสมัครสมาชิกผ่าน ธ.ก.ส. โดยเริ่มตั้งแต่การที่สมาชิกได้รับอนุมัติให้เป็นสมาชิก การรับค่าหุ้นและค่าธรรมเนียมแรกเข้า การซื้อหุ้นเพิ่ม การลาออกและจ่ายคืนค่าหุ้น

4.2 ระบบสินค้า ใช้ในการบริหารจัดการเกี่ยวกับการซื้อ - ขายสินค้า การจัดทำทะเบียนคุมสินค้า และการจัดทำรายงานภาษีซื้อ และภาษีขายในกรณีที่สหกรณ์อยู่ในระบบภาษีมูลค่าเพิ่ม

4.3 ระบบบัญชีแยกประเภท ใช้สำหรับการบันทึกรายการบัญชีและจัดทำงบการเงิน

จากระบบฐานข้อมูลสหกรณ์ที่ใช้เทคโนโลยีทางการบัญชีของกรมตรวจบัญชีสหกรณ์ พบว่า ในจำนวนสหกรณ์ทั้งสิ้นจำนวน 6,637 แห่ง มีการใช้โปรแกรมระบบบัญชีในการประมวลผลข้อมูลจำนวน 3,785 แห่ง คิดเป็นร้อยละ 57.03 จะเห็นได้ว่าในขบวนการสหกรณ์มีการนำเทคโนโลยีมาใช้อย่างแพร่หลาย และมีแนวโน้มที่จะใช้เพิ่มมากขึ้น

การใช้เทคโนโลยีสารสนเทศนั้นมีทั้งข้อดีและมีความเสี่ยง สิ่งที่ดีคือทำให้การดำเนินงานของสหกรณ์มีประสิทธิภาพ ในขณะเดียวกันก็มีความเสี่ยงที่จะเกิดข้อผิดพลาดได้ง่าย ทั้งโดยเจตนาและไม่เจตนา จากผลการตรวจสอบบัญชีสหกรณ์ต่าง ๆ พบว่ามีสหกรณ์ที่ใช้เทคโนโลยีสารสนเทศเกิดการทุจริตเพิ่มขึ้นเรื่อย ๆ ด้วยสาเหตุส่วนใหญ่มาจากมีการใช้เทคโนโลยีสารสนเทศโดยไม่มีระบบการควบคุมภายในที่รัดกุมเพียงพอ หรือบางสหกรณ์ขาดความรู้และเข้าใจในการจัดให้มีระบบการรักษาความปลอดภัยในระบบเทคโนโลยีสารสนเทศ

มาตรฐานขั้นต่ำการควบคุมภายในและการรักษาความปลอดภัย

จากสภาพการใช้เทคโนโลยีสารสนเทศของสหกรณ์ ที่มีสัดส่วนการใช้โปรแกรมระบบบัญชีคอมพิวเตอร์มากถึงร้อยละ 57.03 และมีการใช้ระบบงานคอมพิวเตอร์กับทุกธุรกิจของสหกรณ์ แต่จากผลการตรวจสอบบัญชีประจำปี พบว่าสหกรณ์ส่วนใหญ่ยังไม่มีระบบการควบคุมภายในและมาตรการการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศที่ดีและเหมาะสมกับสหกรณ์ ในขณะที่สหกรณ์มีแนวโน้มที่จะนำเทคโนโลยีมาใช้มากขึ้นและมีลักษณะที่ซับซ้อนมากขึ้น เช่น กรณีที่มีการนำเทคโนโลยีสารสนเทศมาใช้ในการดำเนินงานระหว่างสำนักงานใหญ่กับสาขาสำหรับสหกรณ์ประเภทการเกษตร หรือมีการใช้ระบบ ATM ในการให้บริการสมาชิกของสหกรณ์ประเภทออมทรัพย์ เป็นต้น

กรมตรวจบัญชีสหกรณ์ในฐานะที่เป็นหน่วยงานที่กำกับดูแลด้านการเงินการบัญชีของสหกรณ์เห็นความจำเป็นที่จะต้องกำหนดให้มีมาตรการรักษาความปลอดภัยและระบบการควบคุมภายในสำหรับสหกรณ์ที่มีการนำเทคโนโลยีสารสนเทศมาใช้ในการดำเนินงาน จึงได้กำหนดระเบียบนายทะเบียนสหกรณ์ว่าด้วย มาตรฐานขั้นต่ำในการควบคุมภายในและการรักษาความปลอดภัยสำหรับสหกรณ์และกลุ่มเกษตรกรที่ใช้โปรแกรมระบบบัญชีคอมพิวเตอร์ประมวลผลข้อมูล พ.ศ. 2553 โดยให้มีผลบังคับใช้กับสหกรณ์และกลุ่มเกษตรกรที่มีการใช้โปรแกรมระบบบัญชีคอมพิวเตอร์ทุกแห่ง ตั้งแต่วันที่ 1 มกราคม 2554 เป็นต้นไป โดยได้กำหนดข้อปฏิบัติสำหรับสหกรณ์และกลุ่มเกษตรกรที่ใช้โปรแกรมระบบบัญชีคอมพิวเตอร์ประมวลผลข้อมูลต้องจัดให้มีมาตรฐานขั้นต่ำในการควบคุมภายในและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ จำนวน 9 ข้อ ดังนี้

1. จัดให้มีนโยบายหรือระเบียบปฏิบัติในการควบคุมการปฏิบัติงานเกี่ยวกับการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของสหกรณ์และกลุ่มเกษตรกรที่เป็นลายลักษณ์อักษร

2. จัดให้มีระบบการรักษาความปลอดภัยทางกายภาพที่เพียงพอแก่การป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่ที่เกี่ยวข้องเข้าถึงอุปกรณ์คอมพิวเตอร์ที่สำคัญ และจัดให้มีระบบป้องกันความเสียหายจากสภาวะแวดล้อมหรือภัยพิบัติต่างๆ ให้แก่อุปกรณ์คอมพิวเตอร์ที่สำคัญด้วย

3. จัดให้มีระบบการรักษาความปลอดภัยของข้อมูลในระบบคอมพิวเตอร์และระบบเครือข่ายที่เพียงพอแก่การป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่ที่เกี่ยวข้องได้เข้าถึง ล่วงรู้ ใช้ประโยชน์ หรือแก้ไขเปลี่ยนแปลงข้อมูลหรือระบบดังกล่าวได้

4. จัดให้มีมาตรการควบคุมการพัฒนาหรือแก้ไขเปลี่ยนแปลงที่เพียงพอ เพื่อให้ระบบบัญชีคอมพิวเตอร์ มีการประมวลผลที่ถูกต้องครบถ้วนและเป็นไปตามความต้องการของผู้ใช้งาน รวมทั้งต้องมีการสื่อสารหรือฝึกอบรมเกี่ยวกับระบบบัญชีคอมพิวเตอร์ให้ผู้เกี่ยวข้องได้รับทราบอย่างทั่วถึงเพื่อให้สามารถใช้งานได้อย่างถูกต้อง

5. จัดให้มีและควบคุมดูแลเอกสารสนับสนุนการปฏิบัติงานสำหรับระบบบัญชีคอมพิวเตอร์ โดยมีรายละเอียด ดังนี้

5.1 เอกสารสนับสนุนการปฏิบัติงาน

5.1.1 เอกสารด้านฐานข้อมูลของระบบบัญชีคอมพิวเตอร์ เป็นเอกสารแสดงรายละเอียดการจัดเก็บข้อมูลที่เป็นสาระสำคัญทางบัญชี ทั้งนี้ เพื่อให้สหกรณ์และกลุ่มเกษตรกรสามารถเข้าใจถึงโครงสร้างการจัดเก็บข้อมูลของระบบบัญชีคอมพิวเตอร์ที่ใช้งานอยู่และใช้อ้างอิงเพื่อแก้ไขปัญหาได้ โดยเอกสารด้านฐานข้อมูลของระบบบัญชีคอมพิวเตอร์ที่จำเป็นจะต้องมีคือ โครงสร้างฐานข้อมูล (Data Structure) หรือพจนานุกรมข้อมูล (Data Dictionary) หรือตารางแสดงรายละเอียดของข้อมูลตามแบบที่กรมตรวจบัญชีสหกรณ์กำหนด

5.1.2 คู่มือการใช้ระบบบัญชีคอมพิวเตอร์ เพื่อเป็นเอกสารประกอบการทำงานของผู้ใช้งานในการบันทึกข้อมูล ประมวลผลข้อมูลและออกรายงานได้อย่างถูกต้อง

5.2 การควบคุมดูแลเอกสารสนับสนุนการปฏิบัติงาน โดยจัดให้มีสถานที่เก็บ และปรับปรุงเอกสารให้ถูกต้องและทันสมัยอยู่เสมอ

6. จะต้องสามารถเข้าถึงฐานข้อมูลของระบบบัญชีคอมพิวเตอร์ได้ และสามารถนำข้อมูลออกจากฐานข้อมูลในรูปแบบที่อ่านเข้าใจได้

7. จัดให้มีการสำรองข้อมูลของระบบบัญชีคอมพิวเตอร์เพื่อให้สามารถรองรับการประกอบธุรกิจได้อย่างต่อเนื่อง มีประสิทธิภาพและทันเหตุการณ์ ตลอดจนจัดให้มีการดูแลรักษาข้อมูลชุดสำรองให้มีความปลอดภัย รวมทั้งจัดให้มีการป้องกันมิให้มีการนำข้อมูลชุดสำรองมาใช้อย่างไม่ถูกต้อง

8. ในกรณีที่มีการใช้บริการงานเทคโนโลยีสารสนเทศจากผู้ให้บริการซึ่งเป็นบุคคลภายนอก ต้องจัดให้มีหลักเกณฑ์ในการคัดเลือกและพิจารณาความเหมาะสมของผู้ให้บริการ รวมทั้งต้องควบคุมและตรวจสอบการปฏิบัติงานของผู้ให้บริการอย่างเข้มงวด เพื่อให้มั่นใจว่า ผู้ให้บริการสามารถปฏิบัติตามระเบียบนี้ได้

9. จัดให้มีการตรวจสอบคอมพิวเตอร์โดยหน่วยงานภายในของสหกรณ์และกลุ่มเกษตรกรเองหรือโดยผู้ตรวจสอบที่เป็นบุคคลภายนอก เพื่อทำหน้าที่ตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศทุกประเภทที่อาจเกิดขึ้นได้

ความเชื่อมโยงระหว่างมาตรฐานขั้นต่ำการควบคุมภายในและการรักษาความปลอดภัยของสหกรณ์กับมาตรฐาน COBIT

ข้อปฏิบัติที่กำหนดในระเบียบนายทะเบียนสหกรณ์ดังกล่าวข้างต้นได้มีการพัฒนามาจากหลักการของมาตรฐาน COBIT โดยได้พิจารณานำมาพัฒนาใช้กับสหกรณ์เฉพาะเรื่องที่จำเป็นสำหรับสภาพการใช้เทคโนโลยีสารสนเทศของสหกรณ์ในปัจจุบัน ซึ่งสามารถแสดงความเชื่อมโยงระหว่างมาตรฐานขั้นต่ำการควบคุมภายในและการรักษาความปลอดภัยของสหกรณ์กับมาตรฐาน COBIT ได้ดังรูปที่ 3 - 1 ภาพแสดงความเชื่อมโยงระหว่างมาตรฐานขั้นต่ำการควบคุมภายในของสหกรณ์กับมาตรฐาน COBIT

รูปที่ 3 - 1 ภาพแสดงความเชื่อมโยงระหว่างมาตรฐานขั้นต่ำการควบคุมภายในของสหกรณ์กับมาตรฐาน COBIT

การเชื่อมโยงระหว่างมาตรฐานขั้นต่ำในการควบคุมภายในและการรักษาความปลอดภัยสำหรับสหกรณ์และกลุ่มเกษตรกรที่ใช้โปรแกรมระบบบัญชีคอมพิวเตอร์กับ มาตรฐาน COBIT

มาตรฐานข้อที่ 1 จัดให้มีนโยบายหรือระเบียบปฏิบัติในการควบคุมการปฏิบัติงานเกี่ยวกับการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของสหกรณ์และกลุ่มเกษตรกรที่เป็นลายลักษณ์อักษร

เป็นการพัฒนามาจากหลักการของมาตรฐาน COBIT เรื่องการวางแผนและการจัดองค์กร (PO : Planning and Organization) ในกระบวนการย่อยเรื่อง การประชาสัมพันธ์เป้าหมายและทิศทาง (PO6 : Communicate Management Aims and Direction) โดยที่มาตรฐาน COBIT ข้อนี้มีวัตถุประสงค์เพื่อให้แน่ใจว่าบุคลากรในองค์กรรับรู้และเข้าใจในเป้าหมายและทิศทางขององค์กรที่กำลังดำเนินไป

มาตรฐานข้อที่ 2 จัดให้มีระบบการรักษาความปลอดภัยทางกายภาพที่เพียงพอแก่การป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่ที่เกี่ยวข้องเข้าถึงอุปกรณ์คอมพิวเตอร์ที่สำคัญ และจัดให้มีระบบป้องกันความเสียหายจากสภาวะแวดล้อมหรือภัยพิบัติต่างๆ ให้แก่อุปกรณ์คอมพิวเตอร์ที่สำคัญด้วย

เป็นการพัฒนามาจากหลักการของมาตรฐาน COBIT เรื่องการส่งมอบและการบริการดูแล (DS : Delivery and Support) ในกระบวนการย่อยเรื่อง การจัดการด้านสิ่งอำนวยความสะดวก (DS12 : Manage Physical Environment) โดยที่มาตรฐาน COBIT ข้อนี้มีวัตถุประสงค์เพื่อให้องค์กรมีสภาพแวดล้อมทางกายภาพที่เหมาะสมในการปกป้องอุปกรณ์ด้านเทคโนโลยีสารสนเทศและบุคลากรจากภัยธรรมชาติและบุคคล

มาตรฐานข้อที่ 3 จัดให้มีระบบการรักษาความปลอดภัยของข้อมูลในระบบคอมพิวเตอร์และระบบเครือข่าย ที่เพียงพอแก่การป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่ที่เกี่ยวข้องได้เข้าถึง ล่วงรู้ ใช้ประโยชน์ หรือแก้ไขเปลี่ยนแปลงข้อมูลหรือระบบดังกล่าวได้

เป็นการพัฒนามาจากหลักการของมาตรฐาน COBIT เรื่องการส่งมอบและการบริการดูแล (DS : Delivery and Support) ในกระบวนการย่อยเรื่อง การรักษาความปลอดภัยระบบ (DS5: Ensure System security) โดยที่มาตรฐาน COBIT ข้อนี้มีวัตถุประสงค์เพื่อปกป้องข้อมูลจากการถูกใช้ เปิดเผย แก้ไข ทำลายโดยไม่ได้รับอนุญาตหรือการสูญหาย

มาตรฐานข้อที่ 4 จัดให้มีมาตรการควบคุมการพัฒนาหรือแก้ไขเปลี่ยนแปลงที่เพียงพอ เพื่อให้ระบบบัญชีคอมพิวเตอร์ มีการประมวลผลที่ถูกต้องครบถ้วนและเป็นไปตามความต้องการของผู้ใช้งาน รวมทั้งต้องมีการสื่อสารหรือฝึกอบรมเกี่ยวกับระบบบัญชีคอมพิวเตอร์ให้ผู้เกี่ยวข้องได้รับทราบอย่างทั่วถึงเพื่อให้สามารถใช้งานได้อย่างถูกต้อง

เป็นการพัฒนามาจากหลักการของมาตรฐาน COBIT เรื่องการจัดหาและการติดตั้งใช้งาน (AI: Acquisition and Implementation) ในกระบวนการย่อยเรื่อง การจัดหาและบำรุงรักษาซอฟต์แวร์ประยุกต์ (AI2: Acquire and Maintain Application Software*)* ซึ่งมีวัตถุประสงค์เพื่อให้บริการประมวลผลที่สนับสนุนการดำเนินงาน และการปฏิบัติงานขององค์กรได้อย่างมีประสิทธิภาพ และเรื่องการบริหารการเปลี่ยนแปลง (AI6: Manage Changes) ซึ่งมีวัตถุประสงค์เพื่อลดโอกาสการหยุดชะงัก การแก้ไขโดยพลการ และความผิดพลาด

มาตรฐานข้อที่ 5 จัดให้มีและควบคุมดูแลเอกสารสนับสนุนการปฏิบัติงานสำหรับระบบบัญชีคอมพิวเตอร์

เป็นการพัฒนามาจากหลักการของมาตรฐาน COBIT เรื่องการจัดหาและการติดตั้งใช้งาน (AI : Acquisition and Implementation) ในกระบวนการย่อยเรื่องการปฏิบัติและการใช้งาน (AI4: Enable Operation and Use) ซึ่งมีวัตถุประสงค์เพื่อใช้ประโยชน์สูงสุดจากระบบเทคโนโลยีสารสนเทศที่มีอยู่

มาตรฐานข้อที่ 6 จะต้องสามารถเข้าถึงฐานข้อมูลของระบบบัญชีคอมพิวเตอร์ได้ และสามารถนำข้อมูลออกจากฐานข้อมูลในรูปแบบที่อ่านเข้าใจได้

เป็นการพัฒนามาจากหลักการของมาตรฐาน COBIT เรื่องการวางแผนและการจัดองค์กร (PO : Planning and Organization) ในเรื่อง การกำหนดโครงสร้างด้านสารสนเทศ (PO2 : Define the Information Architecture) ซึ่งมีวัตถุประสงค์เพื่อให้ได้รับประโยชน์สูงสุดจากการจัดรูปแบบระบบสารสนเทศ รวมถึงการจัดประเภทของข้อมูลและระดับการรักษาความปลอดภัยของข้อมูล

มาตรฐานข้อที่ 7 จัดให้มีการสำรองข้อมูลของระบบบัญชีคอมพิวเตอร์เพื่อให้สามารถรองรับการประกอบธุรกิจได้อย่างต่อเนื่อง มีประสิทธิภาพและทันเหตุการณ์ ตลอดจนจัดให้มีการดูแลรักษาข้อมูลชุดสำรองให้มีความปลอดภัย รวมทั้งจัดให้มีการป้องกันมิให้มีการนำข้อมูลชุดสำรองมาใช้อย่างไม่ถูกต้อง

เป็นการพัฒนามาจากหลักการของมาตรฐาน COBIT เรื่อง การส่งมอบและการบริการดูแล (DS : Delivery and Support) ในกระบวนการย่อยเรื่อง การทำให้มีการต่อเนื่องในการให้บริการ (DS4 : Ensure Continuous Service) ซึ่งมีวัตถุประสงค์เพื่อให้มั่นใจว่าบริการด้าน IT มีให้ใช้ได้ตามที่ต้องการและเกิดปัญหาต่อการดำเนินธุรกิจน้อยที่สุดหากมีเหตุการณ์สำคัญทำให้ต้องหยุดชะงัก

มาตรฐานข้อที่ 8 ในกรณีที่มีการใช้บริการงานเทคโนโลยีสารสนเทศจากผู้ให้บริการซึ่งเป็นบุคคลภายนอก ต้องจัดให้มีหลักเกณฑ์ในการคัดเลือกและพิจารณาความเหมาะสมของผู้ให้บริการ รวมทั้งต้องควบคุมและตรวจสอบการปฏิบัติงานของผู้ให้บริการอย่างเข้มงวด เพื่อให้มั่นใจว่า ผู้ให้บริการสามารถปฏิบัติตามระเบียบนี้ได้

เป็นการพัฒนามาจากหลักการของมาตรฐาน COBIT เรื่องการส่งมอบและการบริการดูแล (DS : Delivery and Support) ในกระบวนการย่อยเรื่องการจัดการใช้บริการจากบุคคลภายนอก (DS2 : Manage Third - party Services) เพื่อให้มั่นใจว่าหน้าที่และความรับผิดชอบของบุคคลภายนอกมีกำหนดไว้ชัดเจน และมีการดำเนินการที่ถูกต้องต่อเนื่อง

มาตรฐานข้อที่ 9 จัดให้มีการตรวจสอบคอมพิวเตอร์โดยหน่วยงานภายในของสหกรณ์และกลุ่มเกษตรกรเอง หรือโดยผู้ตรวจสอบที่เป็นบุคคลภายนอก เพื่อทำหน้าที่ตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศทุกประเภทที่อาจเกิดขึ้นได้

เป็นการพัฒนามาจากหลักการของมาตรฐาน COBIT เรื่องการติดตามและการประเมินผล (ME : Monitor and Evaluate) ในกระบวนการย่อยเรื่อง การเฝ้าติดตามและประเมินการควบคุมภายใน (ME2 : Monitor and Evaluate Internal Control) เพื่อให้มั่นใจว่าเป้าหมายของการควบคุมภายในของกิจกรรมด้านเทคโนโลยีสารสนเทศสามารถบรรลุได้ตามที่กำหนด

บทที่ 4

แนวปฏิบัติตามมาตรฐานขั้นต่ำในการควบคุมภายในและการรักษาความปลอดภัยสำหรับสหกรณ์ที่ใช้โปรแกรมระบบบัญชีคอมพิวเตอร์ประมวลผลข้อมูล

บทที่ 4

แนวปฏิบัติตามมาตรฐานขั้นต่ำในการควบคุมภายในและการรักษาความปลอดภัย สำหรับสหกรณ์ที่ใช้โปรแกรมระบบบัญชีคอมพิวเตอร์ประมวลผลข้อมูล

กระบวนการปฏิบัติตามระเบียบนายทะเบียนสหกรณ์

เพื่อให้การดำเนินการตามระเบียบนายทะเบียนสหกรณ์ว่าด้วย มาตรฐานขั้นต่ำในการควบคุมภายในและการรักษาความปลอดภัยสำหรับสหกรณ์และกลุ่มเกษตรกรที่ใช้โปรแกรมระบบบัญชีคอมพิวเตอร์ประมวลผลข้อมูล พ.ศ. 2553 เป็นไปอย่างเหมาะสมและเป็นรูปธรรม กรมตรวจบัญชีสหกรณ์จึงได้กำหนดขั้นตอนการดำเนินการตามระเบียบนายทะเบียนสหกรณ์สำหรับผู้ที่เกี่ยวข้อง ดังนี้

1. ซักซ้อมทำความเข้าใจกับผู้สอบบัญชี

โดยที่เนื้อหาของระเบียบนายทะเบียนสหกรณ์ฉบับดังกล่าวเป็นเรื่องของการควบคุมภายในและการรักษาความปลอดภัย ซึ่งผู้สอบบัญชีมีหน้าที่จะต้องทำการประเมินความเหมาะสมและความมีประสิทธิผลของระบบการควบคุมภายในและการรักษาความปลอดภัยของสหกรณ์ กรมตรวจบัญชีสหกรณ์จึงได้ทำการซักซ้อมผู้สอบบัญชีเพื่อให้มีความรู้และความเข้าใจในเจตนารมณ์ของระเบียบนายทะเบียนสหกรณ์และเข้าใจเนื้อหาของมาตรฐานขั้นต่ำในการควบคุมภายในและการรักษาความปลอดภัยอย่างเพียงพอที่จะสามารถทำการซักซ้อมความเข้าใจแก่สหกรณ์ได้

2. ชี้แจงทำความเข้าใจแก่สหกรณ์

ระเบียบนายทะเบียนสหกรณ์มีวัตถุประสงค์ที่จะให้สหกรณ์นำไปปฏิบัติให้ได้อย่างถูกต้องและบังเกิดผล จึงกำหนดให้ผู้สอบบัญชีทำการซักซ้อมความเข้าใจแก่สหกรณ์ทุกแห่งที่ใช้โปรแกรมระบบบัญชีคอมพิวเตอร์ในการประมวลผลข้อมูล โดยพิจารณาถึงความสะดวกและเหมาะสมในการดำเนินการแต่ละเขตพื้นที่ความรับผิดชอบ

3. ติดตามผลการปฏิบัติตามระเบียบนายทะเบียนสหกรณ์

เพื่อให้สหกรณ์มีการนำเอามาตรฐานขั้นต่ำในการควบคุมภายในและการรักษาความปลอดภัยไปปฏิบัติอย่างบังเกิดผล กรมตรวจบัญชีสหกรณ์จึงกำหนดให้ผู้สอบบัญชีเข้าไปติดตามผลการปฏิบัติตามระเบียบนายทะเบียนสหกรณ์ ณ ที่ทำการหรือสำนักงานของสหกรณ์ จำนวน 1 ครั้ง ภายในหนึ่งรอบปีบัญชีของสหกรณ์ ทั้งนี้ ให้เริ่มตั้งแต่วันที่ 1 มกราคม 2554 เป็นต้นไป โดยให้รายงานผลการติดตามใน “ระบบติดตามผลการปฏิบัติตามระเบียบนายทะเบียนสหกรณ์” บนระบบ Intranet ของกรมตรวจบัญชีสหกรณ์

แนวปฏิบัติตามมาตรฐานขั้นต่ำในการควบคุมภายในและการรักษาความปลอดภัย

แนวปฏิบัติตามมาตรฐานขั้นต่ำในการควบคุมภายในและการรักษาความปลอดภัย ได้ออกแบบเพื่อใช้เป็นแนวทางสำหรับสหกรณ์ในการบริหารจัดการให้การนำเทคโนโลยีสารสนเทศมาใช้ในสหกรณ์มีการควบคุมและการรักษาความปลอดภัยในระดับที่เหมาะสม โดยในมาตรฐานแต่ละข้อจะประกอบด้วยรายละเอียด ดังนี้

1. **ข้อกำหนด**

เป็นมาตรฐานที่นายทะเบียนสหกรณ์กำหนดไว้ในระเบียบ

2. **แนวปฏิบัติ**

เป็นกิจกรรมด้านเทคโนโลยีสารสนเทศที่จะต้องดำเนินการเพื่อให้บรรลุวัตถุประสงค์ของมาตรฐานแต่ละข้อ

3. **การประเมินระดับการควบคุมภายในและการรักษาความปลอดภัยของสหกรณ์**

เพื่อทำให้คณะกรรมการดำเนินการทราบว่าการบริหารจัดการด้านเทคโนโลยีสารสนเทศของสหกรณ์ในปัจจุบันอยู่ในระดับใด ทำให้สามารถกำหนดเป้าหมายที่ต้องการได้ โดยกำหนดเป็นเกณฑ์ไว้ 6 ระดับ ได้แก่

3.1	ระดับ 0 Non - existent	ไม่มีกระบวนการควบคุม
3.2	ระดับ 1 Initial	มีกระบวนการควบคุมกำหนดเฉพาะที่ต้องการ (ad-hoc) ซึ่งไม่เป็นระบบ
3.3	ระดับ 2 Repeatable	มีกระบวนการควบคุมให้ปฏิบัติตามอย่างเป็นระบบ
3.4	ระดับ 3 Defined	มีกระบวนการควบคุมเป็นเอกสารและสื่อสารให้ทราบทั่วกัน
3.5	ระดับ 4 Managed	มีกระบวนการควบคุม ติดตามและวัดผลการปฏิบัติ
3.6	ระดับ 5 Optimized	กำหนดวิธีการปฏิบัติที่ดีให้สามารถปฏิบัติตามและมีเครื่องมือช่วยในดำเนินงานได้อย่างมีประสิทธิภาพสูง

มาตรฐานข้อที่ 1

ก. ข้อกำหนด จัดให้มีนโยบายหรือระเบียบปฏิบัติในการควบคุมการปฏิบัติงานเกี่ยวกับการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของสหกรณ์และกลุ่มเกษตรกรที่เป็นลายลักษณ์อักษร

ข. แนวปฏิบัติ

การจัดให้มีนโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศมีวัตถุประสงค์เพื่อให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องได้ตระหนักถึงความสำคัญของการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ รวมทั้งรับทราบเกี่ยวกับหน้าที่และความรับผิดชอบ และแนวทางปฏิบัติในการควบคุมความเสี่ยงด้านต่าง ๆ

การรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศเป็นการควบคุมที่สำคัญอย่างหนึ่งที่จะต้องมีการกำหนดเป็นนโยบายเพื่อให้ถือปฏิบัติ โดยที่ในการกำหนดนโยบายเกี่ยวกับการรักษาความปลอดภัยของเทคโนโลยีสารสนเทศนั้น ให้เริ่มพิจารณาว่า ใครเป็นผู้ที่ต้องเข้าถึงระบบเทคโนโลยีสารสนเทศบ้างเข้าถึงเมื่อไร มีสิทธิ์ทำงานอะไรได้บ้าง และปฏิบัติการกับข้อมูลในระบบงานใด ซึ่งผลการพิจารณาดังกล่าวจะเป็นปัจจัยให้ทราบถึงภัยคุกคาม (Threat) ความเสี่ยง (Risk) และผลของความเสี่ยงที่จะมีต่อระบบเทคโนโลยีสารสนเทศ ทำให้สามารถเลือกวิธีการรักษาความปลอดภัยที่เหมาะสมที่สุดและคุ้มค่ากับการลงทุน โดยผู้บริหารระดับสูงมีหน้าที่ในการกำหนดนโยบาย กำกับดูแล และควบคุมให้เป็นไปตามนโยบายที่กำหนดไว้ และมีการทบทวนและปรับปรุงอย่างต่อเนื่อง รวมทั้งชี้แจงให้ผู้ปฏิบัติงานที่เกี่ยวข้องทุกคนรับทราบ

ในการจัดทำนโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ มีแนวทางที่สำคัญดังนี้

1. กำหนดนโยบายและสภาพแวดล้อมการควบคุมด้านเทคโนโลยีสารสนเทศให้สอดคล้องกับแนวทางการบริหารงานของสหกรณ์ เช่น แนวทางการบริหารงานต้องการขยายการดำเนินงานเป็นแบบสาขาและต้องการเชื่อมโยงข้อมูลระหว่างสำนักงานใหญ่กับสาขา สหกรณ์ก็ควรมีการกำหนดนโยบายเกี่ยวกับการใช้งานระบบเครือข่ายอินเตอร์เน็ต เป็นต้น

2. กำหนดนโยบายด้านเทคโนโลยีสารสนเทศ ให้สอดคล้องกับแผนกลยุทธ์ด้านเทคโนโลยีสารสนเทศ ซึ่งควรจะรวมบทบาทหน้าที่ความรับผิดชอบ การรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ การรักษาความลับ การควบคุมภายในและทรัพย์สินทางปัญญาที่เกี่ยวข้อง โดยนโยบายดังกล่าวควรได้รับการพิจารณาและอนุมัติจากคณะกรรมการดำเนินการ

ในการกำหนดนโยบายหรือระเบียบปฏิบัติซึ่งจะต้องสอดคล้องกับแผนกลยุทธ์ด้านเทคโนโลยีสารสนเทศนั้น มีความจำเป็นสำหรับสหกรณ์ขนาดใหญ่ที่มีการใช้เทคโนโลยีสารสนเทศที่ซับซ้อนและใช้เทคโนโลยีสารสนเทศเป็นเครื่องมือสำคัญในการขับเคลื่อนธุรกิจ แต่สำหรับสหกรณ์ที่มิได้ใช้เทคโนโลยีสารสนเทศอย่างซับซ้อนอาจไม่มีความจำเป็นต้องจัดทำแผนกลยุทธ์ด้านเทคโนโลยีสารสนเทศ

3. จัดทำนโยบายเป็นลายลักษณ์อักษร โดยคณะกรรมการดำเนินการของสหกรณ์ ฝ่ายจัดการ เจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศ และผู้ใช้งานแต่ละแผนก มีส่วนร่วมในการดำเนินการ

4. มีการทบทวนและปรับปรุงนโยบายให้เป็นปัจจุบันอยู่เสมอ ทั้งนี้เนื่องจากเทคโนโลยีสารสนเทศมีการพัฒนาอย่างรวดเร็ว การกำหนดนโยบายและระเบียบปฏิบัติอาจจะเหมาะสมกับสภาพแวดล้อมในขณะที่กำหนดระเบียบและประกาศถือใช้ แต่เมื่อสภาพแวดล้อมต่างไป นโยบายหรือระเบียบปฏิบัติเดิมอาจไม่เหมาะสมอีกต่อไป

5. มีการกำหนดกรอบในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการควบคุมภายในเพื่อป้องกันทรัพยากรด้านเทคโนโลยีสารสนเทศ และระบบงานที่สำคัญ รวมทั้งลดความเสี่ยงที่อาจจะก่อให้เกิดความเสียหายแก่ทรัพยากรด้านเทคโนโลยีสารสนเทศ โดยทำการประเมินความเสี่ยง ระบุความเสี่ยงที่เกี่ยวข้อง จัดลำดับความสำคัญของข้อมูลและระบบงาน กำหนดระดับความเสี่ยงที่ยอมรับได้ และกำหนดมาตรการหรือวิธีปฏิบัติในการควบคุมความเสี่ยง

6. จัดเก็บนโยบายที่เป็นลายลักษณ์อักษรไว้ในที่ที่ผู้ใช้งานและบุคคลที่เกี่ยวข้องสามารถเข้าถึงได้โดยง่าย

7. ประกาศใช้และสื่อสารนโยบายให้แก่บุคคลที่เกี่ยวข้องอย่างทั่วถึงทุกหัวข้อ เพื่อให้บุคลากรได้รับทราบและปฏิบัติตามได้อย่างถูกต้อง เช่น จัดประชุมชักซ้อม ปิดประกาศนโยบายไว้ที่กระดานข่าวประจำวัน หรือในกรณีที่เป็นเรื่องทางเทคนิคอาจจำเป็นต้องจัดให้มีการฝึกอบรมให้แก่ผู้รับผิดชอบ เป็นต้น

8. ผู้บริหารต้องแสดงเจตนารมณ์ให้บุคลากรทั้งหมดเห็นความสำคัญในการปฏิบัติตามนโยบายโดยเคร่งครัดอย่างสม่ำเสมอ

9. สร้างความตระหนักในนโยบายด้านเทคโนโลยีสารสนเทศให้แก่บุคลากรทั้งสหกรณ์ ผู้บริหารจะต้องสร้างความตระหนักให้เห็นถึงความเสียหายที่อาจเกิดขึ้นแก่สหกรณ์หากไม่ปฏิบัติตามนโยบายอย่างเคร่งครัด

10. มีระบบติดตามการปฏิบัติงานของเจ้าหน้าที่ให้เป็นไปตามนโยบายที่กำหนดอย่างสม่ำเสมอโดยเคร่งครัด นโยบายการรักษาความปลอดภัยจำเป็นต้องมีมาตรการที่จะให้ความมั่นใจว่านโยบายดังกล่าวได้มีการปฏิบัติตามอย่างถูกต้องตลอดเวลา จึงควรมีการกำหนดบุคคลภายในสหกรณ์ให้เป็นผู้รับผิดชอบในการติดตามการปฏิบัติตามนโยบาย อย่างไรก็ตาม เพื่อให้นโยบายด้านเทคโนโลยีสารสนเทศนั้นมีประสิทธิภาพทันกับสถานการณ์มากยิ่งขึ้น สหกรณ์ควรกำหนดให้มีการประเมินและตรวจสอบโดยผู้ประเมินอิสระซึ่งจะช่วยให้การปรับปรุงนโยบายครั้งต่อไปได้ผลสัมฤทธิ์มากขึ้น

11. มีการตรวจสอบรวมทั้งประเมินความเหมาะสมของนโยบายและระบบการควบคุมภายในด้านเทคโนโลยีสารสนเทศ การตรวจสอบการปฏิบัติตามนโยบายเป็นกระบวนการติดตามผลหลังจากที่ได้ประกาศหรือถือใช้ระเบียบปฏิบัติออกไปแล้ว ซึ่งสามารถทำได้โดยการมอบหมายผู้รับผิดชอบในการตรวจสอบการปฏิบัติตามนโยบาย และควรกำหนดให้มีการรายงานผลการตรวจสอบต่อคณะกรรมการดำเนินงานเป็นระยะ การตรวจสอบจะช่วยเพิ่มความตระหนักในมาตรการรักษาความปลอดภัยของผู้ปฏิบัติและช่วยให้ผู้บริหารได้รับทราบปัญหาเพื่อให้สามารถหาแนวทางการแก้ไขปัญหาได้ทันเวลา

12. เมื่อมีเหตุการณ์ที่ส่งผลกระทบต่อการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศที่มีนัยสำคัญ ต้องแจ้งผู้ที่เกี่ยวข้องหรือผู้รับผิดชอบโดยเร็ว

13. กำหนดหน้าที่และความรับผิดชอบของผู้ใช้งาน และบุคคลที่เกี่ยวข้องไว้อย่างชัดเจน เช่น หน้าที่ของผู้ใช้งานในกรณีที่พบว่าเครื่องคอมพิวเตอร์ติดไวรัส หน้าที่ความรับผิดชอบของเจ้าหน้าที่ระบบเครือข่าย เป็นต้น

ค. การประเมินระดับการควบคุมภายในและการรักษาความปลอดภัยของสหกรณ์

ในการจัดให้มีนโยบายหรือระเบียบปฏิบัติในการควบคุมการปฏิบัติงานเกี่ยวกับการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของสหกรณ์และกลุ่มเกษตรกรที่เป็นลายลักษณ์อักษร พิจารณาลักษณะการควบคุมเพื่อจัดระดับได้ดังนี้

ระดับ	ลักษณะการควบคุม	0	1	2	3	4	5
Non-existent	เมื่อผู้บริหารไม่ได้มีการกำหนดสภาพแวดล้อมการควบคุม ไม่ได้ตระหนักในการสร้างนโยบายและระเบียบวิธีปฏิบัติ หรือมาตรฐานในการทำงาน	√					

ระดับ	ลักษณะการควบคุม	0	1	2	3	4	5
Initial	เมื่อผู้บริหารมีการกำหนดสภาพแวดล้อมการควบคุม โดยกำหนดนโยบาย ระเบียบวิธีปฏิบัติ และมาตรฐานในการทำงานและมีการสื่อสารให้พนักงานทราบเมื่อมีการร้องขอ การพัฒนาการสื่อสารและการปฏิบัติยังไม่เป็นทางการและปฏิบัติอย่างสม่ำเสมอ		√				
Repeatable	เมื่อผู้บริหารมีการเข้าใจความต้องการของสหกรณ์และกำหนดสภาพแวดล้อมการควบคุมให้มีประสิทธิภาพ แต่วิธีปฏิบัติยังไม่มีการกำหนดอย่างเป็นทางการ ผู้บริหารมีการสื่อสารนโยบายและระเบียบวิธีปฏิบัติให้ทราบ แต่การพัฒนานโยบายหรือระเบียบวิธีปฏิบัติยังไม่เป็นมาตรฐานมีความแตกต่างกันระหว่างหน่วยงาน ยังไม่มีการจัดการแบบองค์รวม			√			
Defined	เมื่อผู้บริหารพัฒนาและจัดทำนโยบายและระเบียบวิธีปฏิบัติเป็นลายลักษณ์อักษร มีการสื่อสารให้พนักงานทั่วทั้งสหกรณ์ทราบ และมีการสร้างความตระหนักด้านการรักษาความปลอดภัยของเทคโนโลยีสารสนเทศอย่างเป็นทางการ แต่ยังไม่มีการฝึกอบรมพนักงานเป็นประจำสม่ำเสมอ รวมทั้งยังไม่มีการติดตามผลของการปฏิบัติตามนโยบายหรือระเบียบวิธีปฏิบัติอย่างเป็นทางการ				√		

ระดับ	ลักษณะการควบคุม	0	1	2	3	4	5
Managed	เมื่อผู้บริหารมีความรับผิดชอบในการสื่อสารเกี่ยวกับนโยบายเกี่ยวกับการควบคุมภายใน และมีความกระตือรือร้นเพื่อให้มีการปฏิบัติตามนโยบายอย่างมีคุณภาพ รวมทั้งมีการสร้างความตระหนักด้านการรักษาความปลอดภัยของเทคโนโลยีสารสนเทศ มีกระบวนการจัดพัฒนาและปรับปรุง รวมทั้งสื่อสารให้เข้าใจรวมทั้งมีการกำหนดกรอบการประเมินการปฏิบัติตามนโยบายอย่างชัดเจน					√	
Optimized	เมื่อการกำหนดนโยบายหรือสภาพแวดล้อมการควบคุมเป็นไปตามกลยุทธ์การบริหารของสหกรณ์ มีการสอบทานและปรับปรุงอย่างต่อเนื่อง มีการใช้ผู้เชี่ยวชาญทั้งภายในและภายนอกสหกรณ์มากำหนดแนวทางการควบคุมให้สอดคล้องกับธุรกิจของสหกรณ์ และมีการประเมินผลด้วยตนเองเกี่ยวกับการปฏิบัติตามนโยบายและวิธีปฏิบัติขององค์กร การสร้างความตระหนักหรือถ่ายทอดความรู้ใช้การสื่อสารผ่านสื่ออัตโนมัติของสหกรณ์หรือเครื่องมือของระบบการฝึกอบรม						√

มาตรฐานข้อที่ 2

ก. ข้อกำหนด จัดให้มีระบบการรักษาความปลอดภัยทางกายภาพที่เพียงพอแก่การป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่ที่เกี่ยวข้องเข้าถึงอุปกรณ์ที่สำคัญและจัดให้มีระบบป้องกันความเสียหายทางสภาวะแวดล้อมหรือภัยพิบัติต่าง ๆ ให้แก่อุปกรณ์คอมพิวเตอร์ที่สำคัญด้วย

ข. แนวปฏิบัติ

การรักษาความปลอดภัยทางกายภาพ เป็นการควบคุมการเข้าถึงเครื่องคอมพิวเตอร์ อุปกรณ์เครือข่ายและอุปกรณ์คอมพิวเตอร์ โดยการบริหารจัดการสภาพแวดล้อมให้สามารถสร้างความมั่นคงปลอดภัยให้กับอุปกรณ์ด้านเทคโนโลยีสารสนเทศ มีแนวทางพิจารณา ดังนี้

1. มีการกำหนดกลยุทธ์หรือมาตรฐานเกี่ยวกับสิ่งอำนวยความสะดวกทางด้านเทคโนโลยีสารสนเทศ ได้แก่ คัดเลือกสถานที่ใช้เป็นบริเวณที่ปฏิบัติการคอมพิวเตอร์ ผู้รักษาความปลอดภัยหรืออุปกรณ์ทางอิเล็กทรอนิกส์ ระบบดับเพลิง ระบบไฟ ระบบป้องกันน้ำท่วม

อุปกรณ์คอมพิวเตอร์เป็นองค์ประกอบสำคัญประการหนึ่งที่มีผลต่อการทำงานของระบบเทคโนโลยีสารสนเทศ หากอุปกรณ์คอมพิวเตอร์เกิดความเสียหายหรือขัดข้องย่อมทำให้ระบบเทคโนโลยีสารสนเทศหยุดชะงักตามไปด้วย มาตรฐานเกี่ยวกับสิ่งอำนวยความสะดวกทางด้านเทคโนโลยีสารสนเทศ หมายถึง กระบวนการจัดการที่จะช่วยให้อุปกรณ์คอมพิวเตอร์สามารถปฏิบัติงานได้อย่างมีประสิทธิภาพซึ่งตามหลักปฏิบัติสากลมีด้วยกันหลากหลายวิธี สำหรับสหกรณ์ควรจัดการด้วยวิธีการ ดังนี้

1.1 จัดสถานที่ตั้งที่เอื้ออำนวยต่อการทำงานของอุปกรณ์คอมพิวเตอร์ โดยจัดบริเวณเป็นการเฉพาะและต้องกำหนดให้มีผู้ดูแลรักษา มีอุณหภูมิที่เหมาะสม มีระบบดับเพลิงสำหรับระงับเหตุกรณีไฟไหม้ จัดให้มีระบบไฟฟ้าที่มีกำลังรองรับให้ใช้งานได้อย่างต่อเนื่อง รวมถึง จัดให้มีเครื่องสำรองไฟที่มีขนาดเพียงพอที่จะจัดการกับระบบได้ในกรณีไฟฟ้าดับ หรือในกรณีที่เป็นสหกรณ์ขนาดใหญ่มีการใช้ระบบเทคโนโลยีสารสนเทศตลอดเวลา อาจจำเป็นต้องมีระบบไฟฟ้าสำรอง สำหรับสถานที่ตั้งของอุปกรณ์เครื่องแม่ข่ายควรมีเครื่องตรวจจับควันไฟเพื่อจะสามารถแจ้งเหตุได้ทันเวลาหากเกิดไฟไหม้ และในสถานการณ์ปัจจุบัน อาจจำเป็นต้องพิจารณาจัดให้มีระบบป้องกันน้ำท่วมด้วย

1.2 กรณีมีการเข้าเยี่ยมชมสหกรณ์ จำเป็นต้องชี้แจงให้บุคคลที่เข้ามาเยี่ยมชมทราบถึงกฎระเบียบในการเยี่ยมชม เช่น การบันทึกชื่อและเวลาเข้าเยี่ยมชม การติดเครื่องหมายหรือบัตรประจำตัวตลอดเวลาที่เข้ามาเยี่ยมชม หรือห้ามถ่ายรูประหว่างการเยี่ยมชม เป็นต้น

1.3 แนวปฏิบัติในการดูแลอุปกรณ์คอมพิวเตอร์ดังกล่าวข้างต้น จำเป็นที่จะต้องกำหนดไว้เป็นมาตรฐาน ทั้งนี้ เนื่องจากการกำหนดมาตรการดูแลรักษาแต่ละกรณีจะต้องกำหนดให้เหมาะกับสภาพการใช้เทคโนโลยีสารสนเทศของสหกรณ์ซึ่งต้องมีการศึกษาและประเมินก่อนที่จะนำมากำหนดเป็นแนวปฏิบัติ ตัวอย่างการจัดให้มีเครื่องสำรองไฟ จะต้องพิจารณาทั้งจำนวนที่ต้องจัดหาและขนาดของเครื่องสำรองไฟให้สัมพันธ์กับลักษณะการใช้ระบบงานของสหกรณ์ เช่น มีการจัดเก็บข้อมูลรวมไว้ที่เครื่องแม่ข่าย เครื่องคอมพิวเตอร์ที่ให้บริการสมาชิกติดตั้งเป็นระบบเครือข่ายเพื่อเชื่อมโยงข้อมูลระหว่างกัน เป็นต้น จำนวนเครื่องสำรองไฟหากจัดเตรียมไว้น้อยไปอาจไม่สามารถรองรับสถานการณ์ได้ หรือหากมากเกินไปก็ย่อมจะกระทบต่อค่าการลงทุนของสหกรณ์

2. กำหนดมาตรฐานเกี่ยวกับสิ่งอำนวยความสะดวกทางด้านเทคโนโลยีสารสนเทศ ควรจะปรับให้เหมาะสมและเป็นไปตามนโยบายการรักษาความปลอดภัยของสหกรณ์ ความพร้อมใช้งานของระบบเทคโนโลยีสารสนเทศ และสามารถรวมเป็นส่วนหนึ่งของแผนรองรับเหตุการณ์ฉุกเฉินของสหกรณ์และสนับสนุนการบริหารจัดการเหตุสุดวิสัย

เนื่องจากการใช้เทคโนโลยีสารสนเทศของแต่ละสหกรณ์มีความแตกต่างกันจึงมีความจำเป็นต้องการใช้อุปกรณ์คอมพิวเตอร์ที่แตกต่างกันตามไปด้วย ดังนั้น สหกรณ์จึงต้องพิจารณาปรับความเหมาะสมของการจัดการเกี่ยวกับสิ่งอำนวยความสะดวกด้านเทคโนโลยีสารสนเทศกับสภาพการใช้เทคโนโลยีสารสนเทศของสหกรณ์ โดยเฉพาะต้องสอดคล้องกับระบบการควบคุมภายในที่สหกรณ์กำหนดถือใช้ เพื่อให้มาตรการรักษาความปลอดภัยที่มีประสิทธิภาพ ซึ่งรวมถึงการที่สหกรณ์จะต้องมีมาตรการที่จะทำให้อุปกรณ์คอมพิวเตอร์มีความพร้อมในการใช้งานอยู่ตลอดเวลาด้วย ในกรณีที่สหกรณ์มีการจัดทำแผนรองรับเหตุฉุกเฉินจะต้องรวมเรื่องความพร้อมในการใช้งานไว้ในแผนรองรับเหตุฉุกเฉินด้วย

3. มีการติดตามการทำงานของสิ่งอำนวยความสะดวกทางด้านเทคโนโลยีสารสนเทศ โดยตรวจสอบความพร้อมใช้งานของอุปกรณ์ด้านเทคโนโลยีสารสนเทศ กล้องวงจรปิด ระบบตรวจจับควัน ระบบดับเพลิง โดยการสังเกตการณ์และสุ่มตรวจสอบอย่างสม่ำเสมอ

แม้ว่าสหกรณ์จะกำหนดมาตรฐานเกี่ยวกับสิ่งอำนวยความสะดวกทางด้านเทคโนโลยีสารสนเทศได้อย่างเหมาะสม แต่หากว่าไม่มีการปฏิบัติตามหรือมีการปฏิบัติตามแต่ไม่ครบถ้วนถูกต้องย่อมจะสร้างความเสียหายต่อระบบเทคโนโลยีสารสนเทศของสหกรณ์ได้ เช่น ไม่มีการตรวจสอบการทำงานของระบบดับเพลิงและระบบตรวจจับควัน เมื่อเพลิงไหม้ปรากฏว่าระบบไม่ส่งสัญญาณเตือนทำให้ไม่สามารถป้องกันเหตุเพลิงไหม้ไว้ได้ ระบบเทคโนโลยีสารสนเทศเสียหายไม่สามารถใช้งานได้ทั้งระบบ ดังนั้น เพื่อให้มาตรการที่กำหนดบรรลุผลจึงต้องจัดให้มีการตรวจสอบความพร้อมของอุปกรณ์คอมพิวเตอร์อย่างสม่ำเสมอ หากพบข้อบกพร่องจะสามารถแก้ไขได้ทันเวลาก่อนที่จะเกิดความเสียหาย

4. มีการกำหนดตารางการบำรุงรักษาอุปกรณ์ด้าน เทคโนโลยีสารสนเทศ และถือปฏิบัติตามอย่างเคร่งครัด

การกำหนดตารางการบำรุงรักษาอุปกรณ์ด้านเทคโนโลยีสารสนเทศ เป็นการบำรุงดูแลรักษาที่จำเป็นและต้องปฏิบัติอย่างเคร่งครัด เนื่องจากอุปกรณ์คอมพิวเตอร์นั้น ก็เช่นเดียวกับทรัพย์สินอื่น ๆ ที่จะต้องมีกำหนดตารางเวลาในการบำรุงดูแลรักษา นอกจากนั้นอุปกรณ์คอมพิวเตอร์ยังเป็นอุปกรณ์อิเล็กทรอนิกส์ที่มีคุณลักษณะพิเศษกว่าทรัพย์สินอื่น จึงจำเป็นจะต้องได้รับการบำรุงดูแลโดยผู้ที่มีความรู้เฉพาะด้าน

5. มีการรักษาความปลอดภัยทางกายภาพ จะต้องมีการกำหนดพื้นที่จำกัดจากบุคคลภายนอกและต้องได้รับอนุญาตในกรณีที่ต้องการจะเข้าสู่พื้นที่จำกัดนั้น ๆ

การเข้าถึงอุปกรณ์คอมพิวเตอร์มีโอกาสเข้าถึงระบบและข้อมูลสารสนเทศของสหกรณ์ได้ ดังนั้น ในการกำหนดมาตรการรักษาความปลอดภัยทางกายภาพจึงต้องมีการกำหนดจำกัดการเข้าถึงเฉพาะบุคคลที่มีหน้าที่เกี่ยวข้องเท่านั้น โดยวิธีการกำหนดพื้นที่ตั้งของอุปกรณ์คอมพิวเตอร์และผู้ที่เข้าถึงจะต้องได้รับอนุญาตจากผู้มีอำนาจอนุมัติเท่านั้น

การจำกัดการเข้าถึงสามารถทำได้โดย จัดห้องสำหรับเก็บอุปกรณ์คอมพิวเตอร์ไว้โดยเฉพาะและอนุญาตให้ผู้มีหน้าที่รับผิดชอบเข้าไปเฉพาะเมื่อมีความจำเป็น กรณีเช่นนี้ใช้สำหรับการดูแลรักษาอุปกรณ์แม่ข่าย แต่สำหรับอุปกรณ์คอมพิวเตอร์ของเครื่องลูกที่ต้องมีพนักงานใช้ในการนำเข้าและเรียกดูข้อมูลในการให้บริการสมาชิกตลอดเวลา กรณีเช่นนี้สามารถทำได้โดยการกำหนดเป็นพื้นที่สำหรับพนักงานเท่านั้น

ในกรณีที่บุคคลภายนอกมีความจำเป็นต้องเข้าในพื้นที่เก็บอุปกรณ์คอมพิวเตอร์แม่ข่าย เช่นกรณีเข้าไปเพื่อบำรุงดูแลรักษา หรือแก้ไขปัญหาข้อขัดข้องในการทำงานของอุปกรณ์นั้นต้องได้รับอนุญาตจากผู้มีอำนาจอนุมัติทุกครั้ง

6. มีการกำหนดขั้นตอนการปฏิบัติตามกฎหรือระเบียบการรักษาความปลอดภัยให้ชัดเจนและง่ายต่อการปฏิบัติ รวมทั้ง มีการฝึกอบรมให้มีความเข้าใจต่อกฎหรือระเบียบดังกล่าว

การกำหนดนโยบายหรือระเบียบปฏิบัตินั้นกำหนดเป็นคำบรรยายเพื่อการประกาศถือใช้ ซึ่งอาจไม่เอื้อต่อการนำไปปฏิบัติ ดังนั้น เพื่อให้ผู้ปฏิบัติสามารถปฏิบัติได้อย่างถูกต้องจึงควรทำเป็นแผนผังขั้นตอนการปฏิบัติงาน (Flow Chart) ซึ่งง่ายต่อการนำไปปฏิบัติ นอกจากนั้นการปฏิบัติงานในระบบเทคโนโลยีสารสนเทศ ผู้ปฏิบัติงานต้องมีความรู้อย่างถ่องแท้ จึงต้องมีการฝึกอบรมผู้รับผิดชอบแต่ละงานตามความรับผิดชอบให้เกิดความเข้าใจและปฏิบัติได้

ค. การประเมินระดับการควบคุมภายในและการรักษาความปลอดภัยของสหกรณ์

ในการจัดให้มีระบบการรักษาความปลอดภัยทางกายภาพที่เพียงพอแก่การป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่ที่เกี่ยวข้องเข้าถึงอุปกรณ์ที่สำคัญและจัดให้มีระบบป้องกันความเสียหายทางสภาวะแวดล้อมหรือภัยพิบัติต่าง ๆ ให้แก่อุปกรณ์คอมพิวเตอร์ที่สำคัญด้วยนั้น สามารถพิจารณาลักษณะการควบคุมเพื่อจัดระดับได้ ดังนี้

ระดับ	ลักษณะการควบคุม	0	1	2	3	4	5
Non - existent	ไม่มีการกำหนดความต้องการหรือตระหนักในการป้องกันสิ่งอำนวยความสะดวกหรือลงทุนเพื่อให้เกิดการรักษาความปลอดภัยทางกายภาพ ซึ่งได้แก่ ปัจจัยด้านสถานที่ ระบบการป้องกันเพลิง ฝุ่นหรือความร้อนเกินและไม่การควบคุมความชื้น	√					
Initial	องค์กรมีความตระหนักในการป้องกันทรัพยากรหรือบุคลากรให้มีความปลอดภัยจากสิ่งที่กระทำโดยคนหรือภัยธรรมชาติ แต่ยังไม่การกำหนดมาตรฐานหรือระเบียบปฏิบัติเพื่อให้แนวทางในการปฏิบัติงาน ทักษะและความสามารถในการทำงานยังขึ้นอยู่กับตัว		√				

ระดับ	ลักษณะการควบคุม	0	1	2	3	4	5
	บุคคลนั้น การเคลื่อนย้ายหรือจัดเก็บอุปกรณ์เทคโนโลยีสารสนเทศไปยังสถานที่ต่าง ๆ สามารถทำได้โดยไม่ถูกจำกัดหรือตรวจสอบ ผู้บริหารไม่มีกระบวนการติดตาม ควบคุมหรือกระบวนการป้องกันนั้นสัมฤทธิผลหรือไม่						
Repeatable	องค์กรมีความตระหนักและมีการจัดสรรงบประมาณในการติดตั้งระบบการรักษาความปลอดภัยทางกายภาพ รวมทั้งมีการกำหนดบุคลากรในการติดตามผลการปฏิบัติตามหรือละเมิดกฎ แต่โดยส่วนใหญ่การรักษาความปลอดภัยทางกายภาพทำอย่างไม่เป็นทางการหรือไม่มีระเบียบปฏิบัติอย่างเป็นลายลักษณ์อักษรและอนุมัติเห็นชอบโดยผู้บริหารขององค์กร			√			
Defined Process	มีการกำหนดการควบคุมทางกายภาพ จัดสรรงบประมาณและติดตามผลโดยผู้บริหารขององค์กร การเข้าถึงสิ่งอำนวยความสะดวกด้าน เทคโนโลยีสารสนเทศ ถูกจำกัดบุคคลในการเข้าถึงและผู้มาเยี่ยมหรือผู้ให้บริการภายนอกต้องได้รับอนุมัติจากผู้มีอำนาจ มีการจัดเก็บรายการเข้าออกห้องปฏิบัติการคอมพิวเตอร์ ไม่มีการประกันภัยอุปกรณ์หรือสิ่งอำนวยความสะดวกด้าน เทคโนโลยีสารสนเทศ				√		
Managed	มีการกำหนดการควบคุมทางกายภาพ จัดสรรงบประมาณและติดตามผลโดยผู้บริหารของ องค์กรมีความเข้าใจเกี่ยวกับนโยบายหรือระเบียบปฏิบัติใน					√	

ระดับ	ลักษณะการควบคุม	0	1	2	3	4	5
	การควบคุมทางกายภาพอย่างเป็นลายลักษณ์อักษรและสื่อสารในกับพนักงานในองค์กรทราบทั่วกัน กำหนดผู้รับผิดชอบในการควบคุม ติดตามและรายงานความผิดปกติ รวมทั้งมีการประเมินมูลค่าของอุปกรณ์ เทคโนโลยีสารสนเทศ ให้สามารถประกันภัยอุปกรณ์ได้ครอบคลุมความเสียหายที่อาจจะเกิดขึ้น						
Optimized	มีการจัดแผนระยะยาวเพื่อให้สิ่งอำนวยความสะดวกด้าน เทคโนโลยีสารสนเทศ สามารถรองรับกับความต้องการทางเทคโนโลยีสารสนเทศ องค์กร ซึ่งประกอบด้วย ขนาดของห้องปฏิบัติการคอมพิวเตอร์ ระบบรักษาความปลอดภัย ระบบไฟฟ้า ระบบดับเพลิง ระบบป้องกันน้ำท่วม มีการจำกัดสิทธิการเข้าถึงห้องปฏิบัติการคอมพิวเตอร์ตลอดเวลา มีการกำหนดแผนการบำรุงรักษาอุปกรณ์และจัดรายงานผลการบำรุงรักษาอย่างสม่ำเสมอ รวมทั้งความพร้อมใช้งานของอุปกรณ์ เทคโนโลยีสารสนเทศ ควรจะกำหนดให้สอดคล้องกับตามแผนการรองรับเหตุการณ์ฉุกเฉินหรือเหตุสุดวิสัยได้อย่างเหมาะสม						√

มาตรฐานข้อที่ 3

ก. ข้อกำหนด จัดให้มีระบบการรักษาความปลอดภัยของข้อมูลในระบบคอมพิวเตอร์และเครือข่ายเพียงพอแก่การป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่ที่เกี่ยวข้องได้เข้าถึง ล่วงรู้ ใช้ประโยชน์ หรือแก้ไขเปลี่ยนแปลงข้อมูลหรือระบบดังกล่าวได้

ข. แนวปฏิบัติ

ในการรักษาความปลอดภัยของข้อมูลนั้น นอกจากสหกรณ์จะจัดให้มีการรักษาความปลอดภัยทางด้านกายภาพซึ่งเป็นวิธีการที่ดีสำหรับการปกป้องทรัพย์สินที่เป็นวัตถุแล้ว ยังมีความจำเป็นที่จะต้องจัดระบบไม่ให้ผู้ที่ไม่มีสิทธิ์สามารถเข้าถึงระบบงานเพื่อให้เกิดความมั่นคงปลอดภัยของข้อมูลซึ่งเป็นทรัพย์สินอิเล็กทรอนิกส์อีกระดับหนึ่ง

การเข้าถึงระบบงาน หมายถึง ความสามารถในการเข้าถึงโปรแกรมและข้อมูลในระบบงาน การควบคุมความสามารถดังกล่าวก็เพื่อรักษาความปลอดภัยของโปรแกรมและระบบงาน ผู้ใช้ระบบจะได้รับอนุญาตให้เข้าถึงข้อมูลได้เพื่อทำการอ่าน ทำสำเนา เพิ่มและลบเฉพาะส่วนที่ตนมีสิทธิ์ในการใช้งานเท่านั้น และการป้องกันข้อมูลจากบุคคลภายนอกก็มีความสำคัญเช่นเดียวกัน การจำกัดการเข้าถึงระบบงานนั้น โดยคุณสมบัติของระบบงานจะต้องสามารถจำแนกความแตกต่างระหว่างการเข้าใช้งานของผู้ได้รับอนุญาตกับผู้ไม่ได้รับอนุญาตได้

การควบคุมการเข้าถึงระบบงาน ประกอบด้วย

1. การพิสูจน์ตัวตน (Authentication)

1.1 รหัสผ่าน (Password) ใช้ในการระบุตัวตนของผู้ใช้ระบบงานเพื่อแสดงสิทธิ์การใช้ระบบงาน การป้อนรหัสผ่านเพื่อเข้าสู่ระบบงาน ผู้ใช้จะป้อนชื่อตามบัญชีผู้ใช้ระบบ หลังจากมีการป้อนรหัสผ่านแล้ว ชุดของตัวอักขระที่ไม่ซ้ำกันนั้นจะเป็นสิ่งที่ระบุว่าเป็นผู้ใช้ระบบ ซึ่งจะเป็นที่ทราบกันเฉพาะระหว่างผู้ใช้ระบบงานกับตัวระบบงานเท่านั้น ถ้าผู้ใช้ระบบงานป้อนชื่อผู้ใช้ระบบและรหัสผ่านที่ตรงกันกับที่มีอยู่ในระบบงานแล้ว จะถือว่าเป็นการแสดงสิทธิ์ของผู้ใช้ระบบงาน ในทางปฏิบัติความสำคัญของรหัสผ่านได้ลดลงเนื่องจากสามารถคาดเดาได้ง่าย สูญหาย ถูกจดไว้ หรือเปิดเผย จึงเป็นช่องทางให้ผู้ไม่ได้รับอนุญาตสามารถเข้าถึงระบบได้

1.2 การระบุตัวตนด้วยสิ่งที่มีทางกายภาพ (Physical Possession Identification) เช่น บัตรประจำตัว (ID Card) ที่มีการบันทึกข้อมูลบุคคลและสามารถอ่านได้ด้วยเครื่องคอมพิวเตอร์ เป็นต้น ระดับการรักษาความปลอดภัยอาจเพิ่มขึ้นหากมีการใช้ทั้งบัตรประจำตัวและรหัสผ่านร่วมกันใน

การผ่านเข้าสู่ระบบงาน นอกจากนี้ การระบุตัวตนด้วยสิ่งที่มีทางกายภาพอาจใช้อุปกรณ์รักษาความปลอดภัยอื่นร่วมด้วย เช่น กุญแจประตู เป็นต้น

1.3 การระบุตัวตนด้วยค่าทางชีวภาพ (Biometric Identification) อุปกรณ์อ่านค่าทางชีววิทยา เพื่อระบุตัวตนแยกลักษณะบุคคลตามคุณสมบัติของร่างกาย เช่น ลายมือ เสียง เรตินา โครงสร้างและลักษณะใบหน้า ลายเซ็น และลักษณะการใช้แป้นพิมพ์จากรูปแบบการใช้ตัวอักษรต่างๆ เมื่อผู้ใช้ระบบต้องการเข้าระบบงาน ข้อมูลของร่างกายผู้ใช้หรือคุณสมบัติทางชีวภาพที่ใช้ระบุตัวตนต้องตรงกับข้อมูลที่จัดเก็บในระบบงาน

2. การกำหนดสิทธิ์

สามารถทำได้โดยใช้วิธีการทดสอบความเข้ากันได้ (Compatibility Test) เมื่อผู้ใช้ระบบที่ถูกต้องเข้าใช้ระบบงาน การทดสอบการเข้ากันได้จะใช้การพิจารณาว่าผู้ใช้ระบบนั้นมีสิทธิ์ในการทำงานในระบบงานหรือไม่ เช่น พนักงานสินเชื่อมีสิทธิ์ในการบันทึกคำขอกู้และสัญญาเงินกู้เท่านั้น ต้องไม่มีสิทธิ์ในการนำเข้าข้อมูลเกี่ยวกับเงินรับฝาก หรือเจ้าหน้าที่จัดซื้อต้องไม่ได้รับอนุญาตให้นำเข้าข้อมูลการขายสินค้า เป็นต้น วิธีการนี้มีความสำคัญต่อการป้องกันข้อผิดพลาดที่อาจเกิดขึ้นกับระบบงานทั้งโดยเจตนาและไม่เจตนา การทดสอบการเข้ากันได้ ใช้ประโยชน์จากตารางการควบคุมการเข้าถึง (Access control matrix) ที่แสดงรายการเลขประจำตัวและรหัสผ่านของผู้ใช้ระบบงาน ชื่อระบบงาน และสิทธิ์การเข้าถึงของผู้ใช้ระบบแต่ละคน

ผู้ใช้ระบบงาน		ระบบเงินให้กู้		ระบบเงินรับฝาก	
เลขประจำตัว	รหัสผ่าน	จ่ายเงินกู้	รับชำระเงินกู้	รับฝาก	ถอน
1111	aaaaa1	2	1	0	0
2222	bbbbb2	1	2	0	0
3333	cccccc3	3	1	3	1
4444	ddddd4	0	0	2	1
5555	eeeee5	0	0	1	2

ตาราง 2 - 2 การควบคุมการเข้าถึงระบบงาน

รหัสประเภทของการเข้าถึง

0 – ไม่อนุญาตให้เข้าถึง

1 – เรียกดูรายงานเท่านั้น

2 – เรียกดูรายงาน เพิ่มเติม และแก้ไขรายการ

3 – เรียกดูรายงาน เพิ่มเติม แก้ไข และยกเลิกรายการ

3. การบันทึกกิจกรรมต่าง ๆ ในระบบเพื่อใช้ในการตรวจสอบ (Audit Logging)

เป็นการบันทึกกิจกรรมต่าง ๆ ที่ผู้ใช้เข้าใช้งานในระบบรวมทั้งเวลาที่เข้าใช้เพื่อให้สามารถตรวจสอบได้ และช่วยให้เกิดหลักฐานสำหรับติดตามรายการต่าง ๆ ที่เกิดขึ้นในระบบสารสนเทศ

เพื่อให้มั่นใจในการบริหารจัดการความมั่นคงปลอดภัยสำหรับระบบงาน (Ensure System Security) สหกรณ์ควรดำเนินการด้านเทคโนโลยีสารสนเทศ (IT Activities) ดังนี้

1. ประเมินความเสี่ยงในระดับองค์กรสำหรับทรัพย์สินด้านสารสนเทศเป็นระยะๆ โดยจัดทำแผนลดความเสี่ยงและบรรจุไว้เป็นส่วนหนึ่งของแผนความมั่นคงปลอดภัยสารสนเทศขององค์กร

2. จัดให้มีงบประมาณและทรัพยากรที่เพียงพอสำหรับแผนความมั่นคงปลอดภัยสารสนเทศที่จะดำเนินการ

แผนการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศจะสามารถดำเนินการได้อย่างมีประสิทธิภาพนั้น จำเป็นต้องมีงบประมาณและทรัพยากรอย่างเพียงพอ ในกรณีของสหกรณ์ที่ต้องมีการขออนุมัติวงเงินงบประมาณต่อที่ประชุมใหญ่สามัญประจำปีนั้น ก็จำเป็นที่จะต้องมีการจัดทำแผนจัดการความมั่นคงปลอดภัยสารสนเทศเพื่อตั้งงบประมาณไว้ให้เพียงพอที่จะจัดหาทรัพยากรที่ต้องใช้ในการจัดการตามแผนงานให้มีอย่างเพียงพอ

3. มีการจัดทำใบคำขอรหัสผู้ใช้งานก่อนอนุญาตให้เข้าใช้ระบบงานต่าง ๆ ของสหกรณ์ โดยให้ขออนุมัติผ่านทางแบบฟอร์มการขอรหัสผู้ใช้งาน ดังปรากฏตามภาคผนวก ค.

ระบบการรักษาความปลอดภัยที่ดีในส่วนของผู้เข้าใช้ระบบงานคือการจำกัดผู้เข้าใช้ระบบงานไว้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้นและต้องสามารถพิสูจน์ได้ว่ารายการข้อมูลต่าง ๆ ที่มีการนำเข้าหรือปรับปรุงแต่ละรายการนั้นบุคคลใดเป็นผู้ดำเนินการ หากมีข้อผิดพลาดเกิดขึ้นจะสามารถระบุผู้รับผิดชอบได้อย่างชัดเจน สหกรณ์จึงควรมีการกำหนดให้ผู้เข้าใช้ระบบงานต้องจัดทำใบคำขอรหัสผู้ใช้ระบบงานต่างๆ และกำหนดให้มีผู้อนุมัติคำขอ และจัดเก็บเอกสารใบคำขอรหัสผู้ใช้เอาไว้เป็นหลักฐาน

4. ตั้งชื่อบัญชีผู้ใช้งานตามมาตรฐานการตั้งชื่อของสหกรณ์ เช่น “ชื่อของผู้ขอ ตามด้วยอักษรตัวแรกของนามสกุล” เป็นต้น

ในการจัดการบัญชีผู้ใช้งานนั้นควรมีการกำหนดมาตรฐานการตั้งชื่อผู้ใช้ (User Name) ให้ถือปฏิบัติกับผู้ใช้ระบบทุกคน หลักการตั้งชื่อนั้นขึ้นอยู่กับเป้าหมายของสหกรณ์แต่ต้องให้ความหมาย

ของความชัดเจนในการสื่อสาร และควรตั้งชื่อเป็นภาษาอังกฤษ โดยกำหนดให้มีผู้รับผิดชอบในการตั้งชื่อบัญชีผู้ใช้ในระบบงาน

ตัวอย่างเช่น การตั้งชื่อผู้ใช้โดย ชื่อของผู้ขอ ตามด้วยอักษรตัวแรกของนามสกุล

นายนพพล สอนเก่ง

Mr. Nopphon Sonkeng

ชื่อผู้ใช้งาน (User Name) คือ “Nopphons”

5. จัดส่งบัญชีผู้ใช้งานและรหัสผ่านโดยใส่ซองปิดผนึก และประทับตรา “ลับ” และแนบเอกสารนโยบายการรักษาความปลอดภัยไปพร้อมด้วย

การจัดส่งบัญชีผู้ใช้งานและรหัสผ่านเป็นกระบวนการที่ต้องจัดการอย่างระมัดระวัง ทั้งนี้เนื่องจากมีการแจ้ง “รหัสผ่าน” ไปพร้อมกันด้วยจึงต้องมีมาตรการที่จะให้ความมั่นใจว่า ไม่มีผู้อื่นรู้รหัสผ่านของผู้ใช้นั้นนอกจากผู้เป็นเจ้าของ จึงควรดำเนินการโดยใส่ซองปิดผนึกและประทับตรา “ลับ” ส่งถึงเจ้าของบัญชีผู้ใช้โดยตรง และเพื่อให้มาตรการรักษาความปลอดภัยเรื่องรหัสผ่านมีประสิทธิผล จึงควรแนบเอกสารนโยบายเกี่ยวกับการรักษาความปลอดภัยให้ผู้ใช้ได้รู้ เข้าใจและตระหนักไปพร้อมกันด้วย

อย่างไรก็ตาม ในขั้นตอนของการกำหนดบัญชีผู้ใช้ระบบงานนั้นผู้รับผิดชอบจำเป็นต้องกำหนดรหัสผ่านให้ด้วย ทำให้ในขั้นเริ่มแรกผู้รับผิดชอบในการกำหนดบัญชีผู้ใช้งานจึงรู้รหัสผ่านของผู้ใช้แต่ละราย ดังนั้น ในการจัดส่งบัญชีผู้ใช้พร้อมรหัสผ่านนั้น ควรมีคำแนะนำให้ผู้ใช้ระบบงานทำการเปลี่ยนรหัสผ่านทันทีที่เริ่มใช้งาน

6. สร้างบัญชีผู้ใช้งานแยกเป็นรายบุคคล ในกรณีที่มีความจำเป็นต้องใช้งานบัญชีผู้ใช้งานร่วมกัน ให้ขออนุมัติเป็นกรณีๆ ไป

เพื่อให้สหกรณ์สามารถจำแนกความรับผิดชอบของผู้ใช้ระบบงานแต่ละคนได้จึงควรสร้างบัญชีผู้ใช้เป็นรายบุคคล เนื่องจากในระบบเทคโนโลยีสารสนเทศนั้นจะสามารถจำแนกได้ว่าใครเป็นผู้ทำรายการจากการระบุตัวผู้ใช้งาน การใช้บัญชีผู้ใช้งานร่วมกันไม่อาจจำแนกได้ว่าใครเป็นผู้ทำรายการ เพราะแม้ว่าบุคคลจะแยกกันแต่ระบบจะรู้จักเพียงชื่อผู้ใช้รายเดียว ดังนั้น จึงไม่ควรสร้างบัญชีผู้ใช้ร่วมในกรณีมีความจำเป็นควรอนุมัติให้ใช้เป็นครั้ง ๆ ไปและต้องให้ผู้ใช้ร่วมเข้าใจถึงความรับผิดชอบร่วมกันด้วย

7. ในกรณีที่มีการใช้งานบัญชีผู้ใช้งานร่วมกัน หากมีความเสียหายเกิดขึ้น ผู้ที่ใช้งานบัญชีร่วมกันนั้นจะต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้นร่วมกัน

ดังที่กล่าวมาแล้ว ระบบสารสนเทศจะรับรู้ผู้ใช้ระบบตามบัญชีผู้ใช้งาน ดังนั้น ในกรณีที่มีการกำหนดบัญชีผู้ใช้งานร่วมจะต้องทำความเข้าใจกับผู้ใช้ร่วมทุกรายให้ทราบถึงความรับผิดชอบร่วมกันด้วย

8. จัดทำและปรับปรุงระบบสำหรับการพิสูจน์ตัวตนก่อนเข้าใช้ระบบสำคัญต่าง ๆ เพื่อให้มีความมั่นคงปลอดภัยมากขึ้น

การพัฒนาระบบพิสูจน์ตัวตนของแต่ละองค์กรนั้นเป็นไปตามความจำเป็นของแต่ละองค์กร เช่น กรณีที่ธนาคารใช้ระบบพิสูจน์ตัวตนสำหรับผู้ฝากเงินที่ต้องการเข้าสู่ระบบผ่านตู้ ATM ของธนาคารโดยการใช้ทั้งบัตรพลาสติกร่วมกับรหัสผ่าน หากถูกต้องจะสามารถเข้าสู่ระบบและทำรายการฝาก – ถอน หรือสอบถามได้ เป็นต้น

การพิสูจน์ตัวตนของสหกรณ์ที่จำเป็นต้องใช้อาจแบ่งได้ ดังนี้

ผู้ใช้ระบบ เป็นผู้ที่ทำหน้าที่ในการบันทึกข้อมูลนำเข้า การออกรายงานประจำวัน การสอบทานข้อมูล การพิสูจน์ตัวตนควรใช้ บัญชีผู้ใช้ (User Name) และ รหัสผ่าน (Password) ร่วมกัน โดยมีมาตรฐานการกำหนดรหัสผ่านไม่น้อยกว่า 6 ตัวอักษร มีการเปลี่ยนรหัสผ่านทุกๆ 6 เดือน และให้ปฏิบัติเรื่องการรักษาความลับอย่างเคร่งครัด

ผู้รับผิดชอบระบบเครือข่ายและฐานข้อมูล เป็นผู้ทำหน้าที่บริหารเครือข่ายและบริหารฐานข้อมูล ซึ่งถือได้ว่า มีระดับความสำคัญสูงกว่า ผู้ใช้งาน ระบบการพิสูจน์ตัวตนควรเคร่งครัดมากขึ้น เช่น การกำหนดรหัสผ่าน ควรเป็น ตัวอักษรผสมกับอักขระพิเศษ และมีความยาวมากกว่า 6 ตัวอักษร มีระยะการเปลี่ยนรหัสผ่านถี่ขึ้น เป็นต้น

9. กำหนด ปรับปรุง หรือทบทวนสิทธิการเข้าใช้งานระบบต่างๆ ให้แก่ผู้ใช้งานตามหน้าที่และความรับผิดชอบของผู้ใช้งานนั้น หรือตามความจำเป็นในการเข้าถึง (ทั้งพนักงาน และบุคคลภายนอกที่สหกรณ์อนุญาตให้ใช้งาน)

ในการปฏิบัติงานของพนักงานแต่ละคนนั้น สหกรณ์ได้มีการกำหนดหน้าที่ความรับผิดชอบของแต่ละตำแหน่งไว้ในระเบียบปฏิบัติงานของพนักงาน ในการปฏิบัติงานเพื่อเข้าใช้ระบบของพนักงานแต่ละคน จะต้องมีการกำหนดสิทธิ์การใช้งานของผู้ใช้งานแต่ละราย ซึ่งควรจะต้องสอดคล้องกับหน้าที่ความรับผิดชอบที่สหกรณ์ได้กำหนดไว้ในระเบียบปฏิบัติงานของพนักงานแต่ละคน

หากพิจารณาในรายละเอียดจะพบว่าการกำหนดหน้าที่ความรับผิดชอบในระเบียบปฏิบัติงานนั้นสหกรณ์มักจะกำหนดไว้ในลักษณะทั่วๆ ไปของแต่ละหน้าที่ไม่ได้ระบุเป็นรายบุคคล ในขณะที่การกำหนดสิทธิ์การใช้งานจะต้องกำหนดเป็นรายบุคคลโดยละเอียด จึงมักพบเสมอว่าผู้กำหนด

สิทธิ์การใช้งานจะต้องพิจารณาโดยใช้ดุลยพินิจประกอบด้วย ซึ่งอาจเกิดความคลาดเคลื่อน กรณีเช่นนี้ สหกรณ์ควรมีการปรับปรุงระเบียบปฏิบัติในส่วนที่เกี่ยวกับการกำหนดหน้าที่ความรับผิดชอบของพนักงานให้ชัดเจนยิ่งขึ้น นอกจากนี้ในกรณีที่มีการเปลี่ยนแปลงหน้าที่ความรับผิดชอบ ก็จะต้องมีการปรับเปลี่ยนสิทธิ์การใช้งานตามไปด้วยทุกครั้ง

การกำหนดสิทธิ์การใช้งานนอกจากจะต้องให้สอดคล้องกับหน้าที่ความรับผิดชอบตามที่กำหนดไว้ในระเบียบของสหกรณ์แล้ว อีกประการหนึ่งที่ต้องพิจารณาคือ จะต้องกำหนดสิทธิ์การใช้งานให้สอดคล้องกับหลักการควบคุมภายในด้านเทคโนโลยีสารสนเทศด้วย

10. ตรวจสอบและทบทวนสิทธิ์การเข้าถึงระบบต่างๆ อย่างสม่ำเสมอเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

เมื่อมีการกำหนดสิทธิ์การใช้งานไปแล้วระบบจะรับรู้ผู้ใช้งานตามที่กำหนดไว้ หากมีการเปลี่ยนแปลงหน้าที่ความรับผิดชอบหรือพนักงานลาออกจากสหกรณ์แต่ไม่มีการเปลี่ยนแปลงสิทธิ์การใช้งานในระบบ อาจเกิดเหตุการณ์ที่ผู้ไม่มีอำนาจหน้าที่แต่สามารถเข้าสู่ระบบได้ ดังนั้น เพื่อป้องกันเหตุการณ์ดังกล่าว สหกรณ์ควรกำหนดให้มีการทบทวนสิทธิ์การใช้งานในระบบงานเป็นระยะๆ หากพบว่ามีการเปลี่ยนแปลงพนักงานแต่ไม่มีการเปลี่ยนแปลงสิทธิ์การใช้งานให้รีบดำเนินการแก้ไขโดยเร็ว

11. จัดให้มีการอนุมัติสิทธิ์การเข้าถึงระบบงานโดยผู้เป็นเจ้าของระบบ

ในการกำหนดผู้รับผิดชอบระบบงานของสหกรณ์นั้นควรกำหนดให้มีผู้รับผิดชอบเป็นรายระบบ เช่น กำหนดให้หัวหน้าฝ่ายสินเชื่อเป็นผู้รับผิดชอบระบบงานเงินให้กู้ ซึ่งมีเจ้าหน้าที่สินเชื่อเป็นผู้รับผิดชอบในการเข้าสู่ระบบเพื่อนำเข้าและปรับปรุงข้อมูลเกี่ยวกับการขอกู้เงินของสมาชิก ในกรณีเช่นนี้ หัวหน้าฝ่ายสินเชื่อ เป็นเจ้าของระบบ หรือ หัวหน้าฝ่ายการเงินเป็นผู้รับผิดชอบระบบการเงิน มีเจ้าหน้าที่การเงินเป็นผู้ใช้ระบบที่ทำหน้าที่ในการออกใบเสร็จรับเงินต่างๆ ในการกำหนดสิทธิ์ผู้ใช้งานแต่ละระบบควรให้หัวหน้าฝ่ายนั้นๆ เป็นผู้พิจารณาและอนุมัติ

12. แจ้งให้ผู้ดูแลระบบได้รับทราบเมื่อมีการย้ายแผนก หรือลาออก เพื่อให้ดำเนินการปรับปรุง หรือลบสิทธิ์ แล้วแต่กรณี รวมทั้งให้ทำการตรวจสอบคอมพิวเตอร์ หรืออุปกรณ์ที่มีการใช้งานโดยพนักงานที่ลาออกนั้นว่ายังอยู่ในสภาพที่พร้อมใช้งานอยู่หรือไม่

ในการพัฒนาระบบการพิสูจน์ตัวตน นั้นควรรวมกระบวนการของการปรับปรุงข้อมูลเกี่ยวกับความเปลี่ยนแปลงตัวบุคคลที่อาจมีการสับเปลี่ยน โยกย้าย หรือลาออก ดังที่กล่าวมาแล้วข้างต้นว่า ระบบจะรับรู้ผู้ใช้ระบบตามที่กำหนดไว้ครั้งแรก เมื่อมีการเปลี่ยนแปลงตัวบุคคล ควรกำหนดให้มีการแจ้งผู้รับผิดชอบในการปรับปรุงข้อมูลเพื่อจะได้ปรับปรุงข้อมูลผู้ใช้ระบบงานให้สอดคล้องกับหน้าที่ความ

รับผิดชอบใหม่ และป้องกันไม่ให้ผู้ไม่มีสิทธิ์การใช้งานได้เข้าไปใช้ระบบงานซึ่งอาจเป็นต้นเหตุของความเสียหาย ในกรณีที่พนักงานลาออก ควรกำหนดให้มีการลบสิทธิ์ผู้นั้นไม่ให้สามารถใช้ระบบงานได้อีกต่อไป

13. จัดให้มีการรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยตามที่ได้กำหนดไว้โดยผู้ประสบหรือพบเห็นเหตุการณ์

ในสถานการณ์ของการใช้ระบบเทคโนโลยีสารสนเทศประจำวันของสหกรณ์นั้นจะต้องเผชิญกับภัยคุกคามต่างๆ เช่น ปัญหาที่เกิดจาก Virus คอมพิวเตอร์ ที่อาจทำให้การทำงานของระบบผิดปกติไป หรือมีการทำลายแฟ้มข้อมูล หรือปัญหาที่เกิดจากระบบแม่ข่ายไม่ทำงานทำให้ไม่สามารถให้บริการสมาชิกได้ ปัญหาที่เกิดขึ้นประจำวันจะต้องมีการรายงานโดยผู้รับผิดชอบหรือผู้ที่พบปัญหา ทั้งปัญหาที่เกิดขึ้นและวิธีการแก้ไขปัญหา เพื่อให้ผู้บริหารได้ทราบ เพื่อที่จะ นำมาปรับปรุงระบบ นโยบายที่เกี่ยวข้อง

ค. การประเมินระดับการควบคุมภายในและการรักษาความปลอดภัยของสหกรณ์

การจัดให้มีระบบการรักษาความปลอดภัยของข้อมูลในระบบคอมพิวเตอร์และเครือข่ายเพียงพอแก่การป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่ที่เกี่ยวข้องได้เข้าถึง ล่วงรู้ ใช้ประโยชน์ หรือแก้ไขเปลี่ยนแปลงข้อมูลหรือระบบดังกล่าวได้ สามารถพิจารณาลักษณะการควบคุมเพื่อจัดระดับได้ดังนี้

ระดับ	ลักษณะการควบคุม	0	1	2	3	4	5
Non-existent	องค์กรไม่มีความต้องการหรือตระหนักทางด้านการรักษาความปลอดภัยทางด้าน เทคโนโลยีสารสนเทศ ไม่มีการกำหนดผู้ดูแลหรือรับผิดชอบในเรื่องการรักษาความปลอดภัยทางด้านเทคโนโลยีสารสนเทศ	√					
Initial/Ad Hoc	องค์กรมีความต้องการเรื่องการรักษาความปลอดภัย แต่มีความตระหนักด้านการรักษาความปลอดภัยโดยขึ้นอยู่กับตัวบุคคล ยังไม่มีการกำหนดผู้รับผิดชอบด้านการรักษาความปลอดภัยอย่างชัดเจน ไม่สามารถคาดเดาว่าเหตุการณ์ที่จะมีผลต่อการรักษาความปลอดภัยด้าน เทคโนโลยีสารสนเทศ		√				
Repeatable	มีการกำหนดความรับผิดชอบด้านการรักษาความปลอดภัยให้กับหน่วยงานเทคโนโลยีสารสนเทศ แต่ยังไม่ถึงระดับผู้บริหารขององค์กร การสร้างความตระหนักด้านการรักษาความปลอดภัยยังอยู่ในวงจำกัด ข้อมูลเกี่ยวกับการรักษาความปลอดภัยยังไม่มีการวิเคราะห์และวางแผนในการรับรองกับเหตุการณ์ที่อาจจะมีผลต่อระดับการรักษาความปลอดภัยในองค์กร มีการกำหนดนโยบายการรักษาความปลอดภัยแต่อาจจะยังไม่มีเครื่องมือหรือทักษะในการใช้อย่างเหมาะสม			√			

ระดับ	ลักษณะการควบคุม	0	1	2	3	4	5
Defined	มีการสร้างความตระหนักด้านการรักษาความปลอดภัยให้เป็นมาตรฐานและทำอย่างเป็นทางการ โดยได้รับการสนับสนุนจากผู้บริหารขององค์กร มีการกำหนดระเบียบการปฏิบัติงานด้านการรักษาความปลอดภัยและจัดทำเป็นลายลักษณ์ นำออกใช้งาน แต่ยังไม่มีการกำหนดโครงสร้างของบุคลากรที่เกี่ยวข้องไว้อย่างชัดเจน แผนการรักษาความปลอดภัยขององค์กรเน้นการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ มากกว่าสนับสนุนทางด้านธุรกิจขององค์กร มีการทดสอบการบุกรุกของระบบเทคโนโลยีสารสนเทศ เป็นบางครั้ง				√		
Managed	มีการกำหนดความรับผิดชอบด้านการรักษาความปลอดภัยด้าน เทคโนโลยีสารสนเทศ อย่างชัดเจนและถือปฏิบัติ ความเสี่ยงด้านเทคโนโลยีสารสนเทศมีการนำมาวิเคราะห์และปรับให้เหมาะสมกับองค์กร นโยบายการรักษาความปลอดภัยมีการกำหนดและถือปฏิบัติอย่างสมบูรณ์ตามกรอบการกำหนดค่าด้านรักษาความปลอดภัยพื้นฐาน (Security Baseline) การเผยแพร่และสร้างความตระหนักด้านการรักษาความปลอดภัยต้องมีการปฏิบัติอย่างสม่ำเสมอ การกำหนดรหัสผู้ใช้งาน พิสูจน์ตัวตนและสิทธิการใช้งานให้เป็นมาตรฐานเดียวกัน กำหนดมาตรฐานในการทดสอบการบุกรุกและมีกระบวนการทดสอบอย่างชัดเจน และนำผลการทดสอบมาปรับปรุงระบบให้มีความปลอดภัยมากขึ้น มีการเปรียบเทียบต้นทุนและผลประโยชน์ที่จะได้รับมาสนับสนุนการติดตั้งระบบ					√	

ระดับ	ลักษณะการควบคุม	0	1	2	3	4	5
	รักษาความปลอดภัยที่ให้ประโยชน์สูงสุดแก่องค์กร การรายงานเกี่ยวกับการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ มีการเชื่อมโยงกับวัตถุประสงค์ทางธุรกิจขององค์กร						
Optimized	การรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศเป็นความรับผิดชอบร่วมกันระหว่างหน่วยงานธุรกิจกับผู้บริหารด้าน เทคโนโลยีสารสนเทศ โดยกำหนดวัตถุประสงค์ด้านการรักษาความปลอดภัยขององค์กรร่วมกัน ความต้องการด้านการรักษาความปลอดภัยของเทคโนโลยีสารสนเทศ มีการกำหนดไว้อย่างชัดเจน ได้ประโยชน์สูงสุดและสอดคล้องกันต่อแผนด้านรักษาความปลอดภัยขององค์กร ผู้ใช้งานมีส่วนรับผิดชอบและร่วมกันบริหารจัดการด้านรักษาความปลอดภัย มีการรายงานเหตุการณ์การรักษาความปลอดภัย ระบบเตือนภัยด้านการรักษาความปลอดภัยโดยใช้เครื่องมืออัตโนมัติ และกำหนดระดับการเตือนจุดวิกฤติเพื่อจะจัดการกับเหตุการณ์ที่อาจเกิดขึ้นได้ มีการปรับปรุงข้อมูลหรือเหตุการณ์ใหม่ ๆ ด้านการรักษาความปลอดภัยเทคโนโลยีสารสนเทศ อย่างสม่ำเสมอเพื่อให้มั่นใจสามารถรับสถานการณ์ที่อาจเกิดขึ้นได้ การทดสอบการบุกรุกระบบมีการวิเคราะห์หาสาเหตุและกำหนดแนวทางการรับมือไว้อย่างเหมาะสมหรือลดความเสี่ยงที่อาจจะเกิดขึ้นได้						√

มาตรฐานข้อที่ 4

ก. ข้อกำหนด จัดให้มีมาตรการควบคุมการพัฒนาหรือเปลี่ยนแปลงแก้ไขที่เพียงพอ เพื่อให้ระบบบัญชีคอมพิวเตอร์ มีการประมวลผลที่ถูกต้องครบถ้วนและเป็นไปตามความต้องการของผู้ใช้งาน รวมทั้งต้องมีการสื่อสารหรือฝึกอบรมเกี่ยวกับระบบบัญชีคอมพิวเตอร์ให้ผู้ที่เกี่ยวข้องได้รับทราบอย่างทั่วถึงเพื่อให้สามารถใช้งานได้ถูกต้อง

ข. แนวปฏิบัติ

ข.1 แนวปฏิบัติ - มาตรการควบคุมการพัฒนาระบบ

มาตรฐานข้อที่ 4 นี้ได้กล่าวถึงมาตรการควบคุม 2 เรื่อง คือ มาตรการควบคุมการพัฒนาระบบและมาตรการควบคุมการเปลี่ยนแปลงแก้ไข สำหรับมาตรการควบคุมการพัฒนาระบบนั้น หากขาดการควบคุมการบริหารจัดการที่ดี จะก่อให้เกิดความเสี่ยงในการที่ระบบจะไม่สามารถตอบสนองความต้องการทางธุรกิจ หรือระบบงานที่พัฒนาขึ้นอาจไม่มีการควบคุมภายในที่เพียงพอ ทำให้ทำงานผิดพลาด นอกจากนั้นยังอาจเป็นผลให้สหกรณ์สูญเสียเงินลงทุนจำนวนมากในโครงการพัฒนาระบบสารสนเทศ องค์ประกอบสำคัญในการควบคุมการพัฒนาระบบสารสนเทศ ประกอบด้วย

1. แผนแม่บทระยะยาว (Long – range master plan) เป็นแผนงานที่แสดงให้เห็นทิศทางของเทคโนโลยีและโครงร่างของโครงการต่างๆ ที่จะตอบสนองความต้องการเป้าหมายขององค์กรในระยะยาวซึ่งส่วนใหญ่จะเป็นแผนในระยะ 3 – 5 ปี

2. แผนงานพัฒนาระบบ (Project Development Plan) เป็นแผนงานที่แสดงให้เห็นว่าจะดำเนินโครงการอย่างไร ประกอบด้วย รายละเอียดขั้นตอนของงาน ผู้ปฏิบัติงานในแต่ละขั้นตอน ช่วงเวลาในการปฏิบัติงาน และค่าใช้จ่ายโครงการในแต่ละขั้นตอน โดยในแผนงานนั้นควรระบุการวัดความก้าวหน้าของโครงการ (Project Milestone) หรือจุดสำคัญที่จะใช้ในการสอบทานความก้าวหน้าของโครงการ และใช้ในการเปรียบเทียบระยะเวลาที่ใช้จริงกับประมาณการ

3. กำหนดการประมวลผลข้อมูล (Data Processing Schedule) เพื่อให้มีการใช้ทรัพยากรสารสนเทศในองค์กรให้เกิดประโยชน์สูงสุด ควรกำหนดให้งานประมวลผลข้อมูลทุกงานมีการดำเนินการตามตารางเวลาที่กำหนดไว้

4. การมอบหมายหน้าที่และความรับผิดชอบ โครงการพัฒนาระบบแต่ละโครงการจะต้องมีการกำหนดผู้จัดการโครงการและทีมงาน รวมถึงหน้าที่และความรับผิดชอบของแต่ละคน โดยผู้จัดการโครงการและทีมงานจะมีหน้าที่รับผิดชอบโดยตรงต่อความสำเร็จหรือความล้มเหลวของโครงการ

5. การประเมินผลระหว่างการดำเนินโครงการ ควรมีการแบ่งแยกระบบออกเป็นแต่ละส่วน (Module หรือ Task) ซึ่งจะแยกย่อยมาจากประเภทงานต่างๆ ตามแผนงาน เพื่อประเมินผลการดำเนินงานของบุคคลที่รับผิดชอบในแต่ละส่วน

6. การสอบทานภายหลังการติดตั้งระบบและนำระบบมาใช้งาน หลังจากโครงการพัฒนาระบบได้เสร็จสิ้นลงควรมีการสอบทานเพื่อพิจารณาว่าผลประโยชน์ที่ได้รับเป็นไปตามที่คาดหวังไว้หรือไม่ การสอบทานดังกล่าวจะช่วยในการควบคุมกิจกรรมการพัฒนาระบบ และส่งเสริมให้มีการประมาณการต้นทุนและผลประโยชน์อย่างถูกต้อง แม่นยำ

7. การวัดผลการดำเนินงานของระบบ เพื่อให้มีการประเมินระบบงานที่พัฒนาขึ้นอย่างเหมาะสม การวัดผลโดยทั่วไปอาจรวมถึงการวัดปริมาณงาน การวัดอรรถประโยชน์ และการวัดระยะเวลาตอบสนอง

ในการพัฒนาระบบ รวมทั้งการบำรุงรักษาระบบงาน (Acquire and Maintain Application Software) และการบริหารการเปลี่ยนแปลงระบบสารสนเทศ (Manage Changes) มีกิจกรรมด้านเทคโนโลยีสารสนเทศ (IT Activities) ดังนี้

1. จัดทำและปรับปรุงเอกสารการวิเคราะห์และออกแบบระบบโดยละเอียดและเอกสารความต้องการทางเทคนิคให้มีความทันสมัย

ตามหลักการพัฒนาระบบสารสนเทศนั้น ได้กำหนดให้มีการจัดทำเอกสารประกอบการพัฒนาเพื่อที่จะสามารถใช้เป็นเอกสารอ้างอิงให้ผู้พัฒนาระบบใช้สำหรับการพัฒนา เอกสารดังกล่าวได้แก่

1.1 เอกสารการวิเคราะห์ระบบ เป็นเอกสารที่ผู้วิเคราะห์ใช้บันทึกผลการวิเคราะห์ระบบงานเดิม ซึ่งจะแสดงให้เห็นสภาพข้อเท็จจริงที่เป็นอยู่ในปัจจุบันของระบบ ทั้งนี้ จะรวมถึงความต้องการระบบใหม่ด้วย เอกสารนี้เป็นประโยชน์ต่อผู้ออกแบบที่จะนำไปใช้ในการออกแบบระบบใหม่ให้สนองความต้องการและแก้ปัญหาของระบบเดิมได้ตรงประเด็น

1.2 เอกสารการออกแบบระบบใหม่ เป็นเอกสารที่ผู้ออกแบบได้จัดทำขึ้นเพื่อเป็นการสื่อสารและหลักฐานของการออกแบบ เมื่อได้มีการพัฒนาระบบขึ้นใหม่จะใช้เป็นหลักฐานเพื่อประกอบการตรวจสอบการทำงานของระบบใหม่ ดังนั้น สหกรณ์ควรให้ความสำคัญกับเอกสารประกอบการออกแบบโดยกำหนดให้มีการส่งมอบเอกสารประกอบระบบให้ครบถ้วนตามกำหนด

1.3 เอกสารความต้องการทางเทคนิค เป็นเอกสารที่ผู้ออกแบบระบบได้จัดทำขึ้นเพื่อแสดงให้เห็นว่าระบบใหม่ที่ออกแบบนั้นจะสามารถทำงานได้อย่างมีประสิทธิภาพตามที่ควรนั้นต้องได้รับการสนับสนุนด้านเทคนิคตามเอกสารความต้องการทางเทคนิค

2. จัดให้มีการอนุมัติการออกแบบระบบโดยภาพรวมจากผู้เป็นเจ้าของโครงการ เพื่อให้พิจารณาว่าตรงกับความต้องการการใช้งานหรือไม่

ในการพัฒนาระบบสารสนเทศนั้น การบริหารจัดการโครงการพัฒนาระบบสารสนเทศเป็นปัจจัยสำคัญต่อความสำเร็จของการพัฒนาระบบสารสนเทศของสหกรณ์ ในการบริหารจัดการโครงการนี้ต้องกำหนดให้มีผู้บริหารโครงการ โดยใช้แผนงานเป็นเครื่องมือในการบริหาร

แผนงานของการดำเนินการโครงการพัฒนาระบบสารสนเทศต้องจัดให้มีการพิจารณาอนุมัติการดำเนินการในขั้นตอนที่สำคัญคือ ขั้นตอนของการออกแบบระบบ การทดสอบระบบ และการนำระบบใหม่ออกใช้งาน

การอนุมัติขั้นตอนการออกแบบระบบ เป็นขั้นตอนที่สำคัญมากเพราะขั้นตอนนี้คือการที่ผู้ออกแบบระบบได้ทำการออกแบบระบบใหม่พร้อมทำเอกสารความต้องการด้านเทคนิคเป็นที่เรียบร้อยแล้วพร้อมที่จะส่งมอบให้ผู้พัฒนาโปรแกรมนำไปพัฒนาโปรแกรมต่อไป ขั้นตอนนี้เป็นจุดเสี่ยงของความสำเร็จของโครงการ หากปล่อยไปถึงขั้นพัฒนาโปรแกรมแล้วมีการแก้ไขจะทำให้การดำเนินการมีต้นทุนสูงขึ้นมาก และในบางโครงการอาจดำเนินการต่อไม่ได้ ดังนั้น เพื่อให้ได้ระบบตามความต้องการและการดำเนินการของโครงการบรรลุเป้าหมาย จึงต้องกำหนดให้มีการพิจารณาอนุมัติการออกแบบระบบโดยผู้บริหารโครงการ

3. ตรวจสอบว่าการออกแบบในรายละเอียดสอดคล้องกับการออกแบบระบบโดยภาพรวมหรือไม่

ในการพิจารณาอนุมัติการออกแบบก่อนที่จะดำเนินการพัฒนาโปรแกรมนั้นจะต้องดำเนินการตรวจสอบการออกแบบระบบใหม่ทั้งหมดโดยพิจารณาเอกสารการออกแบบโดยละเอียดเพื่อทราบวิธีการทำงานของระบบใหม่ ในขณะเดียวกันจ้องพิจารณาการออกแบบระบบโดยรวมเพื่อให้เห็นเป้าหมายของระบบใหม่ซึ่งจะช่วยพิจารณาว่าระบบตอบสนองนโยบายและความต้องการโดยรวมของสหกรณ์หรือไม่ ในขณะเดียวกันต้องพิจารณาความสัมพันธ์ระหว่างการออกแบบโดยรวมและการออกแบบโดยละเอียดด้วย

4. กำหนดให้มีการควบคุมเฉพาะระบบงาน (Application control)

ในการพัฒนาระบบใหม่สิ่งที่สหกรณ์ควรให้ความสำคัญคือ การออกแบบการควบคุมภายในเฉพาะระบบงาน ซึ่งประกอบด้วย

- ออกแบบการควบคุมเพื่อให้มีการจัดเตรียมเอกสารต้นฉบับให้มีความถูกต้อง
- ออกแบบการควบคุมเพื่อให้สามารถตรวจสอบความถูกต้องของข้อมูลนำเข้า
- ออกแบบการควบคุมเพื่อให้สามารถตรวจสอบความถูกต้องของการประมวลผลข้อมูลที่เกิดขึ้น
- ออกแบบการควบคุมเพื่อตรวจสอบความถูกต้องของรายงาน ในระหว่างที่ทำการพัฒนาและหากพบข้อผิดพลาดให้ตรวจสอบหาสาเหตุ และดำเนินการแก้ไข

5. ตรวจสอบเป็นระยะๆ ว่าขีดความสามารถของระบบงานที่พัฒนานั้นสอดคล้องกับเอกสารการวิเคราะห์และออกแบบระบบหรือไม่

6. ตรวจสอบเป็นระยะๆ ว่าระบบงานที่พัฒนานั้นสอดคล้องกับมาตรฐานการพัฒนาระบบงาน ซึ่งรวมถึงมาตรฐานทางด้านความมั่นคงปลอดภัยในการพัฒนาระบบงาน

7. จัดทำและปรับปรุงแผนการทดสอบระบบงานตามมาตรฐานการทดสอบ ดังนี้

- แผนการทดสอบ Unit Test
- แผนการทดสอบ Integration Test
- แผนการทดสอบ User Acceptance Test

การทดสอบการทำงานของโปรแกรมเป็นขั้นตอนที่เกิดขึ้นหลังจากผู้พัฒนาโปรแกรมได้ทำการพัฒนาแล้ว ก่อนที่จะนำระบบออกใช้งานจะต้องดำเนินการทดสอบการทำงานของระบบก่อนเพื่อให้มั่นใจว่าระบบสามารถทำงานได้อย่างถูกต้อง โดยต้องจัดทีมงานที่ทำหน้าที่ทดสอบ (System Tester) เป็นการเฉพาะ และจะต้องจัดทำเป็นแผนการทดสอบการทำงานของระบบงาน ซึ่งควรมีผู้รับผิดชอบทดสอบ ช่วงเวลา และวิธีการ สำหรับวิธีการการทดสอบระบบงานตามมาตรฐาน มีลำดับการทดสอบ ดังนี้

7.1 การทดสอบหน่วยย่อย (Unit Test)

หน่วยย่อย หมายถึง โมดูลต่าง ๆ ที่โปรแกรมสร้างขึ้นหรืออาจเป็นโปรแกรมย่อยในระบบ การทดสอบหน่วยย่อยเป็นการทดสอบที่เน้นประสิทธิภาพของหน่วยย่อย ๆ ที่จะนำมารวมกันเป็นระบบทั้งหมด

7.2 การทดสอบการรวมกันของแต่ละหน่วยย่อย (Integration Test)

เมื่อมีการนำหน่วยย่อยมาประกอบรวมกันเป็นระบบแล้ว จะดำเนินการทดสอบว่าแต่ละส่วนย่อยสามารถทำงานร่วมกันได้โดยไม่มีข้อผิดพลาด เพื่อให้การทดสอบมีความครบถ้วนเป็นไปตามขั้นตอนตามลำดับ อาจเลือกรูปแบบการทดสอบได้ ดังนี้

7.2.1 การรวมแบบล่างขึ้นบน (Bottom – up Integration)

การทดสอบการรวมจะเริ่มโดยประกอบจากโมดูลล่างสุดตามผังโครงสร้างโปรแกรม เพื่อทดสอบการทำงานร่วมกัน จากนั้นก็จะประกอบโมดูลในระดับสูงขึ้นพร้อมทดสอบการทำงานร่วมกันของโมดูลที่เชื่อมต่อกัน

7.2.2 การรวมแบบบนลงล่าง (Top – down Integration)

การทดสอบการรวมจะเริ่มโดยประกอบจากโมดูลบนสุดตามผังโครงสร้างโปรแกรม เพื่อทดสอบการทำงานร่วมกัน จากนั้นก็จะประกอบโมดูลในระดับรองลงมาพร้อมทดสอบการทำงานร่วมกันของโมดูลที่เชื่อมต่อกัน

7.3 การทดสอบการยอมรับระบบ (User Acceptance Test)

แม้จะมีการทดสอบการทำงานครบทั้งระบบแล้ว เพื่อให้เกิดการยอมรับระบบใหม่อย่างสมบูรณ์จากผู้ใช้งานระบบ ผู้ใช้งานระบบต้องมีส่วนในการทดสอบการทำงานของระบบใหม่ด้วย และพิจารณาว่าตรงกับความต้องการหรือไม่ การทดสอบการยอมรับระบบแบ่งเป็น 2 ขั้นตอน ดังนี้

7.3.1 การทดสอบบนสภาพแวดล้อมจำลอง (Alpha Test)

การทดสอบในขั้นตอนนี้จะทดสอบด้วยการสมมติผู้ใช้งานและข้อมูลที่ใช้นำเข้าในระบบ โดยทดสอบทั้งระบบและทดสอบให้ครบทุกกรณีที่คาดว่าจะเกิดขึ้นในระบบ

7.3.2 การทดสอบบนสภาพแวดล้อมจริง (Beta Test)

การทดสอบจะให้ผู้ใช้งานจริงใช้ข้อมูลจริงในการทดสอบการทำงานของระบบ แต่ระบบจริงจะอยู่ในสภาพแวดล้อมจำลองแทน โดยติดตั้งระบบแยกออกมาต่างหากแล้วให้ผู้ใช้ลองทำงานกับระบบที่ติดตั้งขึ้นนี้เสมือนว่าทำงานจริง การทดสอบแบบ Unit Test

8. ทดสอบตามแผนการทดสอบดังกล่าว และบันทึกผลการทดสอบไว้ด้วย

การปฏิบัติการทดสอบการทำงานของระบบเป็นขั้นตอนงานที่ต้องมีการจัดการที่ดี กล่าวคือต้องปฏิบัติตามแผนงานที่กำหนด รวมทั้งต้องมีการบันทึกผลการทดสอบเพื่อใช้ประกอบการอนุมัติการนำระบบออกใช้งาน และหากผลการทดสอบพบว่าระบบการทำงานมีข้อผิดพลาดหรือมีการ

ทำงานถูกต้องแต่ไม่เป็นไปตามการออกแบบระบบที่ได้รับการอนุมัติในขั้นตอนการอนุมัติการออกแบบ กรณีนี้จะต้องใช้การบันทึกผลการทดสอบเป็นหลักฐานเพื่อให้ผู้พัฒนาโปรแกรมนำไปปรับปรุงแก้ไขให้ถูกต้องต่อไป ในขั้นตอนปฏิบัติการทดสอบระบบตามแผนการทดสอบนั้นมีความสำคัญและต้องใช้เทคนิคการสื่อสารที่ดี เพราะอาจมีข้อขัดแย้งระหว่างทีมงานพัฒนาโปรแกรมกับทีมงานทดสอบโปรแกรมขึ้นได้ อย่างไรก็ดี การบริหารจัดการที่ดีจะสามารถช่วยให้ขั้นตอนนี้สำเร็จได้

9. จัดทำและปรับปรุงแผนการบำรุงรักษาระบบงานอย่างสม่ำเสมอ

การบำรุงรักษาระบบไม่ใช่เพียงแค่การรักษาสภาพเดิมให้ใช้งานได้ แต่หมายความรวมถึงการแก้ไขข้อบกพร่องและการปรับปรุงความสามารถของระบบตามความต้องการที่เพิ่มขึ้น ในกรณีที่เป็นการพัฒนาระบบโดยว่าจ้างบุคคลภายนอก ขอบเขตการบำรุงรักษาจะขึ้นอยู่กับข้อตกลงระหว่างผู้ว่าจ้างและผู้รับจ้าง

แม้ว่าระบบใหม่จะถูกพัฒนาครบถ้วนตามข้อกำหนดความต้องการและสามารถใช้งานได้จริงแล้ว การบำรุงรักษาก็เป็นสิ่งจำเป็นที่ต้องจัดให้มี เพราะระหว่างการใช้งานอาจจะพบข้อบกพร่องตามระยะเวลาการใช้งาน หรือเกิดความต้องการเพิ่มเติมขึ้น การบำรุงรักษาสามารถแบ่งได้เป็น 4 ลักษณะดังนี้

9.1 **การแก้ไขข้อบกพร่อง** (Corrective Maintenance) เป็นการแก้ไขโปรแกรมที่ไม่ตรงกับข้อกำหนดความต้องการที่ระบุไว้หรือไม่ครบถ้วน หรือมีประสิทธิภาพการทำงานต่ำ ซึ่งอาจเกิดจากการใช้เทคนิคการเขียนโปรแกรมที่ไม่เหมาะสม

9.2 **การดัดแปลง** (Adaptive Maintenance) เป็นการปรับปรุงโปรแกรมให้ตรงกับความต้องการที่เพิ่มขึ้นภายหลังจากการส่งมอบงานหรือการปรับปรุงให้รองรับกับสภาพแวดล้อมใหม่ ๆ เช่น เพิ่มเติมเมนูการสอบถามข้อมูลเพื่อให้สมาชิกสอบถามข้อมูลทาง online ได้ หรือแก้ไขโปรแกรมเพื่อให้สามารถทำงานร่วมกับเครื่องเก็บเงินรุ่นใหม่ เป็นต้น

9.3 **การทำให้สมบูรณ์** (Perfective Maintenance) เป็นการปรับปรุงเพื่อเพิ่มประสิทธิภาพ แต่ไม่ใช่ความต้องการของระบบโดยตรง เช่น การปรับลำดับการทำงานในแต่ละหน้าจอ การปรับวิธีการนำข้อมูลเข้า หรือการปรับหน้าจอให้ทำงานง่ายขึ้น เป็นต้น

9.4 **การป้องกันปัญหา** (Preventive Maintenance) เป็นการปรับปรุงเพื่อลดโอกาสในการเกิดข้อผิดพลาดหรือปัญหาที่อาจเกิดขึ้น เช่น การแก้ไขระบบเพื่อรองรับ

การใช้งานกับเทคโนโลยีใหม่ในอนาคต หรือการเปลี่ยนแปลงระบบฐานข้อมูลที่รองรับปริมาณข้อมูลที่มากขึ้น เป็นต้น

10. จัดให้มีการฝึกอบรมให้ผู้ใช้งานและผู้ดูแลระบบได้รู้ถึงวิธีการใช้งานและวิธีดูแลรักษาระบบอย่างมีประสิทธิภาพ การฝึกอบรมจะทำให้ผู้ใช้เข้าใจขั้นตอนการใช้งาน ซึ่งจะช่วยลดข้อผิดพลาดจากการใช้งานได้

ข.2 แนวปฏิบัติ - มาตรการควบคุมการเปลี่ยนแปลงแก้ไข

สำหรับมาตรการควบคุมการเปลี่ยนแปลงแก้ไข ให้ความสำคัญกับการแก้ไขเปลี่ยนแปลงระบบโดยไม่ได้รับอนุญาต ซึ่งอาจมีผลก่อให้เกิดความผิดพลาดในโปรแกรม การทุจริต หรือมีข้อมูลที่ไม่ถูกต้องในงบการเงินและรายงานต่าง ๆ และอาจทำให้ระบบล้มเหลวหรือหยุดชะงักการทำงานได้ การเปลี่ยนแปลงแก้ไขระบบหรือโปรแกรมที่ใช้อยู่จึงควรกำหนดเป็นขั้นตอน โดยมีการอนุมัติและจัดทำเอกสารประกอบการควบคุมการเปลี่ยนแปลงแก้ไขระบบ ในการบริหารการเปลี่ยนแปลงแก้ไขระบบสารสนเทศ (Manage Changes) นั้น จำเป็นต้องกำหนดให้มีมาตรการควบคุม ดังนี้

1. กำหนดระเบียบวิธีปฏิบัติในการเปลี่ยนแปลงแก้ไขระบบที่เป็นลายลักษณ์อักษร

2. กำหนดขอบเขตของการควบคุมการเปลี่ยนแปลงตามความจำเป็น โดยพิจารณาว่าการเปลี่ยนแปลงทางด้านเทคโนโลยีใดบ้างที่องค์กรต้องการควบคุม

3. จัดทำและปรับปรุงกระบวนการเพื่อขออนุมัติจากคณะกรรมการดำเนินการของสหกรณ์ก่อนดำเนินการเปลี่ยนแปลง

4. กรอกแบบฟอร์มเพื่อขออนุมัติการเปลี่ยนแปลงและดำเนินการตามขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลง ที่ได้กำหนดไว้

การเปลี่ยนแปลงระบบสารสนเทศจะมีการร้องขอมาจากเจ้าของระบบ สหกรณ์ควรมีระบบจัดการโดยการกำหนดแบบฟอร์มในการขอเปลี่ยนแปลงระบบ โดยควรระบุขอบเขตที่ต้องการพร้อมเหตุผลความจำเป็นที่ต้องการเปลี่ยนแปลงระบบ

5. ประเมินผลกระทบของการอนุมัติการเปลี่ยนแปลงนั้น

การเปลี่ยนแปลงระบบสารสนเทศย่อมเกิดผลกระทบต่อสหกรณ์หลายด้าน ทั้งวิธีการปฏิบัติและต้นทุนในการเปลี่ยนแปลง จึงต้องทำการประเมินผลกระทบก่อนที่จะอนุมัติให้ดำเนินการเปลี่ยนแปลง โดยศึกษาทั้งผลกระทบด้านเทคนิค ผลกระทบต่อระบบงานอื่น และความเสี่ยงจากการเปลี่ยนแปลง

6. จัดลำดับความสำคัญของการอนุมัติการเปลี่ยนแปลงที่มีการขออนุมัติเข้ามาพร้อมๆ กัน เพื่อให้สามารถดำเนินการเรียงตามลำดับก่อนหลังตามความเหมาะสม

ตามที่กล่าวมาแล้วข้างต้นว่า เจ้าของระบบจะเป็นผู้ร้องขอโดยการจัดทำคำขอเปลี่ยนแปลงระบบสารสนเทศ มายังผู้บริหารเพื่อขออนุมัติ จึงอาจเกิดปรากการณ์มีคำขออนุมัติการเปลี่ยนแปลงระบบสารสนเทศเข้ามาพร้อมๆกันจากหลายระบบ หรือเจ้าของระบบเดียวอาจร้องขอเปลี่ยนแปลงหลายเรื่อง และเนื่องจากการดำเนินการนี้เป็นการเปลี่ยนแปลงไม่ใช่การพัฒนาใหม่ จึงต้องดำเนินการในระยะเวลาสั้นและได้ผลเร็ว อาจไม่สารถดำเนินการได้ทั้งหมดในครั้งเดียวแต่อาจต้องดำเนินการเป็นระยะ จึงต้องจัดลำดับของการดำเนินการ โดยพิจารณาความจำเป็นเร่งด่วนของเรื่องและผลกระทบเป็นปัจจัยในการพิจารณา

7. จัดให้มีการอนุมัติเพื่อดำเนินการเปลี่ยนแปลงนั้น

เนื่องจากการเปลี่ยนแปลงมีผลกระทบทั้งระบบงานเดิมและการใช้ทรัพยากรของสหกรณ์ จึงจำเป็นที่ผู้บริหารจะต้องพิจารณาก่อนที่จะดำเนินการ ดังนั้น ขั้นตอนของการอนุมัติจึงถูกกำหนดขึ้นเพื่อให้มีการกลั่นกรองความเหมาะสม และพิจารณาทรัพยากรเพื่อสนับสนุนให้สามารถดำเนินการได้สำเร็จ

8. ตรวจสอบ ติดตามและรายงานสถานการณ์ดำเนินการเปลี่ยนแปลงในทุกระยะ

การดำเนินการเปลี่ยนแปลงระบบสารสนเทศเช่นเดียวกับการพัฒนาระบบใหม่ที่ต้องมีการจัดทำแผนปฏิบัติการเปลี่ยนแปลงและมีการติดตามผลความสำเร็จในการดำเนินการเป็นระยะ

9. มีการทดสอบระบบที่แก้ไขเปลี่ยนแปลงแล้วก่อนนำมาใช้งาน

10. สรุปผลการดำเนินการเปลี่ยนแปลงและบันทึกไว้เป็นลายลักษณ์อักษร

เมื่อมีการดำเนินการเปลี่ยนแปลงต้องมีการสรุปผลและบันทึกไว้เป็นลายลักษณ์อักษร ผลการดำเนินการนี้จะต้องเปรียบเทียบกับคำขอเปลี่ยนแปลงในขั้นตอนเริ่มแรก เป็นหลักฐานที่แสดงให้เห็นจุดสิ้นสุดของการดำเนินการเปลี่ยนแปลง

11. ในกรณีที่การเปลี่ยนแปลงนั้นมีความเกี่ยวข้องกับคู่มือ ขั้นตอนปฏิบัติ หรือเอกสารอื่นๆ ที่เป็นเอกสารควบคุมภายใต้นโยบายทางด้านสารสนเทศ ให้ปรับปรุงเอกสารเหล่านั้นตามความจำเป็น

การเปลี่ยนแปลงระบบสารสนเทศโดยส่วนใหญ่มักมีผลกระทบกับเอกสารในส่วนที่เป็นคู่มือการใช้งาน ในบางกรณีมีผลกระทบกับขั้นตอนการปฏิบัติงาน หรือในบางสถานการณ์อาจ

กระทบกับโครงสร้างฐานข้อมูล ดังนั้น หากการเปลี่ยนแปลงระบบมีผลกระทบกับเอกสารใดจะต้องกำหนดให้มีการปรับปรุงให้ถูกต้องเป็นปัจจุบันด้วยและควรระบุไว้ในสรุปผลการดำเนินการด้วย

12. ในกรณีที่เป็นการเปลี่ยนแปลงตามปกติ (Normal change) ซึ่งไม่ใช่กรณีเร่งด่วน ให้ผู้ขออนุมัติเขียนแบบฟอร์มขออนุมัติและเข้าสู่ขั้นตอนการอนุมัติตามปกติ

13. ในกรณีที่เป็นการเปลี่ยนแปลงเร่งด่วน (Emergency change) หากไม่รีบดำเนินการอาจเกิดผลเสียหายต่อสหกรณ์ ให้คณะกรรมการดำเนินการเป็นผู้มอบหมายผู้ที่จะเข้าไปทำการแก้ไขหลังจากนั้นจึงทำเอกสารขออนุมัติทำการเปลี่ยนแปลงในภายหลัง

ค. การประเมินระดับการควบคุมภายในและการรักษาความปลอดภัยของสหกรณ์

ค.1 การประเมิน - มาตรการควบคุมการพัฒนาระบบ

การจัดให้มีมาตรการควบคุมการพัฒนา เพื่อให้ระบบบัญชีคอมพิวเตอร์มีการประมวลผลที่ถูกต้องครบถ้วนและเป็นไปตามความต้องการของผู้ใช้งาน รวมทั้งต้องมีการสื่อสารหรือฝึกอบรมเกี่ยวกับระบบบัญชีคอมพิวเตอร์ให้ผู้ที่เกี่ยวข้องได้รับทราบอย่างทั่วถึงเพื่อให้สามารถใช้งานได้ถูกต้อง สามารถพิจารณาลักษณะการควบคุมเพื่อจัดระดับได้ ดังนี้

ระดับ	ลักษณะการควบคุม	0	1	2	3	4	5
Non-existent	ไม่มีการกำหนดกระบวนการพัฒนาและออกระบบงานอย่างชัดเจน รวมทั้งไม่มีการพิจารณาถึงความต้องการการใช้งานที่แท้จริง	√					
Initial/Ad Hoc	มีความตระหนักว่าควรจะมีกระบวนการจัดหาและบำรุงรักษาระบบงานขึ้น แต่อย่างไรก็ตามแต่ละโครงการหรือแต่ละงานมีวิธีปฏิบัติงานที่แตกต่างกันขึ้นอยู่กับตัวบุคคลอาจจะทำให้เกิดขึ้นจัดหาระบบงานที่ล้าสมัยแล้ว การบำรุงรักษาระบบงานไม่มีประสิทธิภาพ		√				

ระดับ	ลักษณะการควบคุม	0	1	2	3	4	5
Repeat but Intuitive	มีกระบวนการจัดหาและการบำรุงรักษาระบบงานที่มีความคล้ายคลึงกัน แต่จะขึ้นอยู่ระดับความเชี่ยวชาญด้าน IT ของแต่ละหน่วยงาน แต่อาจจะไม่มีกำหนดกระบวนการนี้อย่างเป็นทางการ การคัดเลือกหรือจัดหาระบบงานมีกำหนดวิธีการให้คะแนนแต่ยังขึ้นอยู่ทักษะและประสบการณ์ของบุคลากร การบำรุงรักษาระบบงานมีปัญหาและขาดแคลนบุคลากร			√			
Defined Process	มีการกำหนดกระบวนการจัดหาและบำรุงรักษาระบบงานเป็นลายลักษณ์อักษร แต่การจัดหาระบบงานเพื่อสนับสนุนความต้องการของแต่ละหน่วยงานอาจจะยังไม่สามารถทำเป็นมาตรฐานได้เนื่องจากข้อจำกัดทางเทคโนโลยี ส่วนการบำรุงรักษาระบบงานยังไม่สามารถทำได้อย่างมีประสิทธิภาพ				√		
Managed and Measurable	มีการกำหนดกระบวนการจัดหาและนำมาใช้งานโดยกำหนดนโยบายการจัดหา หลักเกณฑ์ในการจัดหา ระเบียบวิธีปฏิบัติ และการกำหนดความต้องการของระบบงาน กำหนดรายละเอียดคุณลักษณะของระบบงาน รวมถึงกระบวนการทดสอบระบบงานอย่างเป็นทางการ มีการอนุมัติขั้นตอนต่าง ๆ จากผู้บริหาร และมีการติดตามสถานะการณ์ทำงานรวมทั้งปัญหาที่เกิดขึ้นอย่างสม่ำเสมอ					√	
Optimized	มีการกำหนดกระบวนการจัดหาและนำมาใช้งานโดยกำหนดนโยบายการจัดหา หลักเกณฑ์ในการจัดหา ระเบียบวิธีปฏิบัติ และการกำหนดความต้องการของระบบงานสอดคล้องกับความต้องการทางธุรกิจ เป็นระเบียบปฏิบัติที่ถือใช้ของสหกรณ์ กระบวนการจัดหาและบำรุงรักษาระบบงานสามารถดำเนินงานได้						√

ระดับ	ลักษณะการควบคุม	0	1	2	3	4	5
	อย่างรวดเร็วและตอบรับกับความต้องการได้อย่างมีประสิทธิภาพ มีการปรับปรุงระบบอย่างต่อเนื่องและมีฐานข้อมูลความรู้เพื่อจัดเก็บเอกสารที่จำเป็นหรือเป็นแนวทางตามมาตรฐานสากล ซึ่งเป็นฐานข้อมูลความรู้ทั้งภายในและภายนอกสหกรณ์						

ค.2 การประเมิน – การควบคุมการเปลี่ยนแปลง

การจัดให้มีมาตรการควบคุมการเปลี่ยนแปลงแก้ไขที่เพียงพอ เพื่อให้ระบบบัญชีคอมพิวเตอร์ มีการประมวลผลที่ถูกต้องครบถ้วนและเป็นไปตามความต้องการของผู้ใช้งาน รวมทั้งต้องมีการสื่อสารหรือฝึกอบรมเกี่ยวกับระบบบัญชีคอมพิวเตอร์ให้ผู้ที่เกี่ยวข้องได้รับทราบอย่างทั่วถึงเพื่อให้สามารถใช้งานได้ถูกต้อง สามารถพิจารณาลักษณะการควบคุมเพื่อจัดระดับได้ ดังนี้

ระดับ	ลักษณะการควบคุม	0	1	2	3	4	5
Non-existent	ไม่มีระเบียบการเปลี่ยนแปลงแก้ไขระบบงานและไม่มีการควบคุมการเปลี่ยนแปลงที่เหมาะสม	√					
Initial/Ad Hoc	มีความตระหนักว่าการเปลี่ยนแปลงแก้ไขระบบงานจะต้องมีการกำหนดระเบียบปฏิบัติและควบคุมให้เหมาะสม แต่ยังมีการปฏิบัติที่แตกต่างกัน มีการเปลี่ยนแปลงแก้ไขระบบงานโดยไม่ได้รับอนุมัติอย่างเหมาะสม ไม่มีเอกสารประกอบเกี่ยวกับการเปลี่ยนแก้ไขระบบงาน มีข้อผิดพลาดของระบบงานเกิดขึ้นทำให้ระบบงานเกิดการหยุดชะงักเนื่องจากจขาดการควบคุมการเปลี่ยนแปลงแก้ไขที่เหมาะสม		√				
Repeat but Intuitive	มีกระบวนการเปลี่ยนแปลงแก้ไขระบบงานแต่ยังไม่เป็นลายลักษณ์อักษร มีเอกสารเกี่ยวกับระบบงานแต่อาจจะไม่ถูกปรับปรุงให้ถูกต้องและทันสมัย			√			

ระดับ	ลักษณะการควบคุม	0	1	2	3	4	5
Defined Process	กระบวนการเปลี่ยนแปลงแก้ไขระบบงานอย่างเป็นลายลักษณ์อักษร รวมถึงมีการจัดประเภทการเปลี่ยนแปลงแก้ไข จัดลำดับความสำคัญ และกำหนดกระบวนการเปลี่ยนแปลงแก้ไขโปรแกรมในกรณีฉุกเฉิน การอนุมัติการแก้ไขระบบงานและการออกใช้งานจริง อาจจะมีการไม่ปฏิบัติตามกระบวนการดังกล่าวบ้างซึ่งก่อให้ข้อผิดลาดและมีการเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุมัติอย่างเหมาะสม มีการประเมินผลกระทบจากการเปลี่ยนแปลงระบบ IT ต่อกระบวนการธุรกิจในกรณีที่มีการนำเทคโนโลยีใหม่เข้ามาใช้ในองค์กร				√		
Managed and Measurable	มีการกำหนดกระบวนการเปลี่ยนแปลงแก้ไขระบบงานอย่างเป็นลายลักษณ์อักษรและถือปฏิบัติทั่วทั้งองค์กร มีการประเมินผลกระทบต่อการเปลี่ยนแปลงแก้ไขระบบงานเพื่อลดโอกาสที่จะเกิดข้อผิดพลาดขึ้นเมื่อมีการใช้งานจริง มีการอนุมัติการเปลี่ยนแปลงแก้ไขระบบงานทุกครั้ง มีการฝึกอบรมเพิ่มในกรณีที่มีการเปลี่ยนแปลงที่จะมีผลต่อการปฏิบัติงานที่ใช้อยู่ในปัจจุบัน					√	
Optimized	มีการกำหนดกระบวนการเปลี่ยนแปลงแก้ไขระบบงานอย่างเป็นลายลักษณ์อักษรและมีการสอบทานและปรับปรุงให้สอดคล้องตามมาตรฐานสากลอย่างสม่ำเสมอ มีการควบคุมเวอร์ชันของโปรแกรมโดยใช้เครื่องมือหรือโปรแกรมช่วย มีการควบคุมการนำเข้าส่งออกโปรแกรมเพื่อไปเปลี่ยนแปลงแก้ไขโปรแกรมด้วยเครื่องมือหรือโปรแกรม มีการติดตามสถานะการเปลี่ยนแปลงแก้ไขโปรแกรม การ						√

ระดับ	ลักษณะการควบคุม	0	1	2	3	4	5
	เปลี่ยนแปลงแก้ไขระบบงานจะต้องสอดคล้องกัน การเปลี่ยนแปลงทางธุรกิจอย่างเหมาะสม						

มาตรฐานข้อที่ 5

ก. ข้อกำหนด จัดให้มีและควบคุมดูแลเอกสารสนับสนุนการปฏิบัติงานสำหรับระบบบัญชีคอมพิวเตอร์

ข. แนวปฏิบัติ

มาตรฐานการควบคุมภายในที่สำคัญประการหนึ่งคือ วิธีการและมาตรฐานในการจัดทำเอกสารระบบสารสนเทศเพื่อให้มั่นใจว่ามีความชัดเจนและรัดกุม การจัดทำเอกสารที่มีคุณภาพทำให้การใช้งานมีความถูกต้อง การติดต่อสื่อสารระหว่างกันมีความเข้าใจตรงกัน และใช้เป็นเอกสารอ้างอิงและเป็นเครื่องมือฝึกอบรมพนักงาน รวมทั้งช่วยในการบำรุงรักษาและแก้ไขปรับปรุงโปรแกรม การจัดทำเอกสารดังกล่าว ประกอบด้วย

1. เอกสารประกอบระบบงาน (System Document) สำหรับผู้ดูแลระบบ อธิบายระบบงานแต่ละระบบ แผนผังการทำงาน รายการโปรแกรม (Program Listing) รายละเอียดการทำงานของแต่ละโปรแกรม โครงสร้างข้อมูล และเอกสารการกำหนดค่าของระบบ

2. เอกสารทางการบริหาร (Administrative Document) สำหรับผู้บริหารหรือผู้ควบคุมงาน อธิบายวิธีการใช้งานที่เกี่ยวข้องกับการกำหนดข้อมูลที่สำคัญ ได้แก่ ข้อมูลหลัก การกำหนดรอบปีบัญชี การกำหนดผู้ใช้งาน การกำหนดสิทธิ์การใช้งาน การสำรองข้อมูล และการเชื่อมโยงข้อมูล

3. เอกสารประกอบการใช้งาน (Operating Document) สำหรับผู้ปฏิบัติงานในแผนกต่างๆ สำหรับใช้งานประจำวัน อธิบายเมนูการใช้งาน ขั้นตอนการใช้งาน การประมวลผลประจำปีและการเรียกดูรายงาน

ในการพัฒนาและปรับปรุงเอกสาร (Develop and Maintain Procedure) เพื่อใช้สนับสนุนการปฏิบัติงานและการฝึกอบรม มีแนวทางในการจัดระบบการควบคุม ดังนี้

1. มีการกำหนดมาตรฐานของเอกสารของระบบงาน

สหกรณ์ควรกำหนดมาตรฐานเอกสารประกอบระบบงานเพื่อใช้เป็นข้อกำหนดในการพัฒนาระบบงาน ในกรณีที่สหกรณ์มีการจ้างบุคคลภายนอกพัฒนาระบบใหม่ควรมีการกำหนดให้มีการจัดทำเอกสารตามมาตรฐานที่กำหนดและส่งมอบพร้อมกับระบบงานที่พัฒนาแล้วเสร็จ

2. จัดทำแผนการอบรมและเอกสารฝึกอบรมเพื่อถ่ายโอนความรู้ และทักษะการใช้งานไปสู่**เจ้าของระบบ** สำหรับระบบงานใหม่ หรือระบบงานที่มีการเปลี่ยนแปลงจำนวนมาก

ก่อนที่จะมีการใช้งานจริงจะต้องมีการจัดอบรมให้เจ้าของระบบได้ทราบและเข้าใจการทำงานของระบบงานให้เพื่อที่จะสามารถบริหารจัดการระบบงานใหม่ได้อย่างถูกต้อง

3. จัดทำแผนการอบรมและเอกสารฝึกอบรมเพื่อถ่ายโอนความรู้ และทักษะการใช้งานไปสู่**ผู้ใช้งาน** สำหรับระบบงานใหม่ หรือระบบงานที่มีการเปลี่ยนแปลงจำนวนมาก

ผู้ใช้งานถือได้ว่าเป็นผู้ที่มีความสำคัญมากสำหรับการนำระบบออกใช้งานจึงต้องมีการฝึกอบรมให้เข้าใจและสามารถปฏิบัติงานได้อย่างถูกต้องในแต่ละขั้นตอน ดังนั้น แผนการอบรมพนักงานผู้ใช้ระบบจะต้องมีเนื้อหารายละเอียดมากกว่าเจ้าของระบบ และต้องมีการฝึกปฏิบัติโดยควรมีกรณีศึกษาโดยใช้สถานการณ์ที่จะเกิดขึ้นบ่อยๆให้พนักงานได้ฝึกอบรมด้วย เอกสารที่ใช้ประกอบการอบรมบุคคลกลุ่มนี้คือ คู่มือการปฏิบัติงาน (User Manual)

4. จัดทำแผนการอบรมและเอกสารฝึกอบรมเพื่อถ่ายโอนความรู้ และทักษะการใช้งานไปสู่ผู้ดูแลระบบ และ Helpdesk สำหรับระบบงานใหม่ หรือระบบงานที่มีการเปลี่ยนแปลงจำนวนมาก

บุคคลที่เกี่ยวข้องกับระบบสารสนเทศอีกกลุ่มหนึ่ง คือ ผู้ดูแลรักษาระบบงานและผู้ให้บริการHelpdesk บุคคลกลุ่มนี้จะต้องได้รับการฝึกอบรมเพื่อถ่ายโอนความรู้ด้านเทคนิคเพื่อที่จะสามารถช่วยแก้ปัญหาการใช้งานหลังจากที่ระบบจริงเริ่มใช้แล้ว เอกสารที่ใช้สำหรับการอบรมบุคคลกลุ่มนี้ส่วนใหญ่เป็นเอกสารประกอบการปฏิบัติงาน (Operating Document)

5. มีการพัฒนาฐานข้อมูลบริหารความรู้ เอกสารระบบงาน ผังการไหลของงาน เพื่อใช้ในการเปลี่ยนแปลงแก้ไขระบบงานหรือมอบให้กับผู้ใช้งาน

เมื่อระบบงานใหม่ออกใช้งานแล้ว ในระหว่างการใช้งานอาจเกิดปัญหาข้อขัดข้องซึ่งได้มีการแก้ไขปัญหาเพื่อให้ระบบสารสนเทศสามารถดำเนินไปได้อย่างต่อเนื่อง วิธีการแก้ไขปัญหาเหล่านั้นถือเป็นฐานข้อมูลที่มีประโยชน์สำหรับการใช้งานระบบสารสนเทศของสหกรณ์ สามารถใช้สำหรับการฝึกสอนผู้ปฏิบัติงานใหม่ หรือใช้เป็นแหล่งข้อมูลเมื่อสหกรณ์มีความจำเป็นที่จะต้องปรับปรุงและเปลี่ยนแปลงระบบ จึงควรให้มีการจัดระบบข้อมูลเหล่านี้เพื่อใช้เป็นฐานข้อมูลองค์ความรู้ด้านระบบสารสนเทศของสหกรณ์ที่พร้อมให้บริการสืบค้นได้ตลอดเวลา

ค. การประเมินระดับการควบคุมภายในและการรักษาความปลอดภัยของสหกรณ์

การจัดให้มีและควบคุมดูแลเอกสารสนับสนุนการปฏิบัติงานสำหรับระบบบัญชีคอมพิวเตอร์ สามารถพิจารณาลักษณะการควบคุมเพื่อจัดระดับได้ ดังนี้

ระดับ	ระดับการควบคุม	0	1	2	3	4	5
Non-existent	ไม่มีกระบวนการเกี่ยวกับการจัดทำคู่มือการใช้งาน การปฏิบัติงาน และเอกสารสำหรับฝึกอบรม	√					
Initial	สหกรณ์มีความตระหนักว่าเอกสารระบบงานควรจะมีการจัดทำขึ้น มีการจัดทำเอกสารระบบงานบ้างแต่รูปแบบของแต่ละหน่วยงานไม่เหมือนกัน เอกสารส่วนใหญ่ไม่ถูกปรับปรุงให้เป็นปัจจุบัน ไม่มีการเชื่อมโยงข้อมูลกันระหว่างหน่วยงาน มีการฝึกอบรมเพียงครั้งแรกเมื่อตอนเริ่มใช้ระบบงานใหม่		√				
Repeatable	มีการจัดทำเอกสารเกี่ยวกับขั้นตอนการปฏิบัติงานหรือเอกสารระบบงาน แต่ยังไม่มีการวางโครงสร้างของเอกสารหรือรูปแบบที่ชัดเจน ขึ้นอยู่กับความสามารถของแต่ละบุคคล มีเอกสารประกอบการฝึกอบรมแต่ยังไม่มีการเชื่อมโยงข้อมูลระหว่างระบบงาน			√			
Defined	มีการกำหนดรูปแบบที่ชัดเจนและทำความเข้าใจในการกำหนดกรอบการจัดทำเอกสารคู่มือการใช้งาน คู่มือการปฏิบัติงานและเอกสารการฝึกอบรม มีการจัดเก็บเอกสารให้สามารถค้นหาหรือจำกัดสิทธิการใช้งานได้ตามต้องการ มีการปรับปรุงเอกสารให้เป็นปัจจุบัน แต่ยังไม่มีการตรวจสอบหรือควบคุมให้มีการจัดทำเอกสารตามรูปแบบที่กำหนดไว้อย่างเคร่งครัด				√		

ระดับ	ระดับการควบคุม	0	1	2	3	4	5
Managed	กำหนดวิธีการปรับปรุงวิธีการปฏิบัติงานและเอกสารประกอบการฝึกอบรมโดยสามารถเชื่อมโยงทุกระบบทุกหน่วยงานหรือให้การเชื่อมโยงข้อมูลหรือการเชื่อมต่อระหว่างระบบงาน มีการเก็บรวบรวมข้อคิดเห็นของผู้ใช้งานและการให้คะแนนเพื่อนำไปปรับปรุงกระบวนการให้ดีขึ้น มีการนำเครื่องมือมาใช้ในการบริหารจัดการเกี่ยวกับการจัดเก็บและเผยแพร่เอกสารสามารถแสดงข้อมูลได้ตามต้องการ					√	
Optimized	มีการนำเครื่องมือหรือระบบมาช่วยบริหารจัดการเกี่ยวกับกระบวนการทำงานของผู้ใช้งานและการเข้าถึงคู่มือการใช้งานต่าง ๆ เป็นระบบอิเล็กทรอนิกส์ การปรับปรุงและการเผยแพร่เอกสารสามารถเข้าถึงได้โดยง่าย และสะท้อนถึงกระบวนการทำงานของสหกรณ์โดยแสดงภาพการเชื่อมโยงการทำงานระหว่างระบบงาน						√

มาตรฐานข้อที่ 6

ก. ข้อกำหนด จะต้องสามารถเข้าถึงฐานข้อมูลระบบบัญชีคอมพิวเตอร์ได้ และสามารถนำข้อมูลออกจากฐานข้อมูลในรูปแบบที่อ่านเข้าใจได้

ข. แนวปฏิบัติ

ในระบบฐานข้อมูลซึ่งเน้นความสำคัญของความปลอดภัยในข้อมูลเพื่อให้ข้อมูลมีความถูกต้อง เที่ยงตรง ครบถ้วน และพร้อมใช้งาน แต่ลักษณะการใช้งานข้อมูลในปัจจุบันมีความจำเป็นในเรื่องของการใช้ข้อมูลร่วมกัน ทำให้มีความเสี่ยงในการควบคุมการเข้าถึงข้อมูลและทรัพยากรสารสนเทศเพิ่มมากขึ้น ตัวอย่างเช่น ความเสี่ยงจากการทุจริต การขโมยข้อมูล การนำข้อมูลไปใช้ในทางที่ผิด การทำลายข้อมูล เป็นต้น ความเสี่ยงเหล่านี้อาจเกิดขึ้นจากการที่ผู้ที่ไม่ได้รับอนุญาตเข้าถึงข้อมูล หรือการที่ผู้ใช้ที่ได้รับอนุญาตมีการเข้าถึงข้อมูลที่เกินกว่าขอบเขตที่ได้รับ การควบคุมการเข้าถึงข้อมูลในฐานข้อมูลมีหลายลักษณะดังต่อไปนี้

1. การออกแบบขอบเขตการเข้าถึงฐานข้อมูลของผู้ใช้แต่ละราย ผู้บริหารฐานข้อมูล มีหน้าที่รับผิดชอบโดยตรงต่อการออกแบบขอบเขตการใช้ฐานข้อมูลของผู้ใช้ โดยดำเนินการอย่างใกล้ชิดร่วมกับผู้ใช้และผู้ออกแบบระบบ ซึ่งการออกแบบขอบเขตการใช้ฐานข้อมูลนี้ต้องสอดคล้องกับความต้องการของผู้ใช้

2. การอนุญาตให้เข้าถึงฐานข้อมูล เป็นการกำหนดกฎเกณฑ์และการกระทำที่ผู้ใช้สามารถทำได้ตามสิทธิ์การใช้งาน ได้แก่ การอ่าน การเพิ่มข้อมูล การแก้ไขข้อมูล และการลบข้อมูล โดยมีชื่อผู้ใช้และรหัสผ่านเป็นตัวกำหนด ดังรายละเอียดตามตารางที่ 4 - 2 การอนุญาตให้เข้าถึงฐานข้อมูล

ข้อมูลบัญชีเงินฝาก					
แผนก	**เปิดบัญชี**	**ฝากเงิน**		**ถอนเงิน**	
ชื่อผู้ใช้	A	B	C	D	E
รหัสผ่าน	mond12	tues34	wedn23	thur34	frid12
สิทธิการใช้งาน :					
อ่าน	Y	Y	Y	Y	Y
เพิ่มข้อมูล	Y	Y	Y	Y	Y
แก้ไขข้อมูล	Y	Y	N	Y	N
ลบข้อมูล	N	N	N	N	N

ตาราง 4 - 2 การอนุญาตให้เข้าถึงฐานข้อมูล

3. การเข้ารหัสข้อมูล (Data Encryption) ระบบฐานข้อมูลอาจใช้การเข้ารหัสสำหรับป้องกันข้อมูลที่เป็นความลับ เช่น สูตรการผลิต อัตราเงินเดือนของพนักงาน แฟ้มข้อมูลรหัสผ่าน เป็นต้น การเข้ารหัสข้อมูลเป็นการใช้ขั้นตอนวิธีแปลงข้อมูลในรูปแบบที่คละกัน เพื่อให้ข้อมูลอยู่ในรูปแบบที่ไม่สามารถอ่านออกได้ นอกจากนี้ การเข้ารหัสข้อมูลยังสามารถใช้ในการรักษาความปลอดภัยของข้อมูลที่มีการรับส่งผ่านระบบเครือข่ายได้

4. การควบคุมการใช้ฐานข้อมูล ในระบบฐานข้อมูลจะมีผู้บริหารฐานข้อมูลรับผิดชอบในการจัดการและดูแลฐานข้อมูล โดยจัดทำพจนานุกรมข้อมูล (Data Dictionary) สำหรับใช้เป็นเอกสารกำกับและควบคุมการปรับปรุงข้อมูลที่ใช้ในระบบงาน พจนานุกรมข้อมูลจะเป็นเครื่องมือที่สร้างความมั่นใจว่ารายการข้อมูลมีการกำหนดและใช้อย่างถูกต้อง ในกระบวนการรักษาความปลอดภัยของข้อมูล ผู้บริหารฐานข้อมูลจะเป็นผู้สร้างและควบคุมให้การเข้าถึงและปรับปรุงฐานข้อมูลเป็นไปตามวิธีการที่กำหนด

ฐานข้อมูลระบบบัญชีคอมพิวเตอร์ของสหกรณ์จะต้องมีการควบคุมให้มีความปลอดภัยให้เข้าถึงฐานข้อมูลได้เฉพาะผู้ที่ได้รับอนุญาต นอกจากนี้ หากต้องการนำข้อมูลออกจากฐานข้อมูลต้องสามารถนำออกในรูปแบบที่อ่านเข้าใจได้ เพื่อให้ระบบการจัดการที่ดีสหกรณ์ควรกำหนดให้มีการกำหนดกระบวนการในการจัดทำผังโครงสร้างข้อมูลด้านสารสนเทศให้สอดคล้องตามต้องการทางธุรกิจ

เพื่อให้เกิดความเชื่อถือในระบบงานและข้อมูลในแต่ละระบบงานของสหกรณ์สามารถเชื่อมโยงข้อมูลระหว่างกันได้อย่างมีประสิทธิภาพ ควรมีกระบวนการตามแนวทาง ดังนี้

1. มีการกำหนดแบบโครงสร้างข้อมูลด้านสารสนเทศที่ตรงกับความต้องการ โดยมีการระบุว่าข้อมูลนั้นเป็นประเภทใด ใครที่สามารถใช้ได้ และนำไปใช้ได้ทันตามความต้องการ

2. มีการปรับปรุงโครงสร้างของข้อมูลอย่างสม่ำเสมอ

3. โครงสร้างของข้อมูลควรมีการเก็บให้สอดคล้องกันกับแผนระยะยาวของระบบเทคโนโลยีสารสนเทศ

4. มีการสร้างและมีการปรับปรุง Data Dictionary อย่างต่อเนื่องโดยต้องเป็นไปตามกฎเกณฑ์ของสหกรณ์ที่กำหนดไว้

5. มีการกำหนดกฎเกณฑ์เพื่อแยกประเภทของข้อมูลแต่ละประเภทออกจากกัน รวมไปถึงกำหนดการเป็นเจ้าของข้อมูลเหล่านั้น

6. มีการกำหนดกฎเกณฑ์ในการเข้าถึงข้อมูลแต่ละประเภทไว้อย่างเหมาะสม

7. ฝ่ายจัดการมีการระบุให้มีการพัฒนาและดูแลระดับความปลอดภัยของข้อมูลในแต่ละประเภท โดยกำหนดความปลอดภัยและการควบคุมให้รัดกุม

8. ระบุถึงเกณฑ์ที่จะเข้าไปถึงข้อมูลแต่ละประเภทไว้อย่างเหมาะสมพร้อมทั้งทำการประเมินเป็นระยะและปรับปรุงให้มีความสัมพันธ์กัน

9. มีการกำหนดบรรทัดฐานของความปลอดภัยที่อยู่ในระดับที่แตกต่างกัน เพื่อรองรับการขยายตัวทางด้าน e-commerce และ mobile computer ซึ่งมีแนวโน้มที่จะเข้ามามีบทบาทในธุรกรรมสหกรณ์

ค. การประเมินระดับการควบคุมภายในและการรักษาความปลอดภัยของสหกรณ์

การควบคุมให้สามารถเข้าถึงฐานข้อมูลระบบบัญชีคอมพิวเตอร์ได้ และสามารถนำข้อมูลออกจากฐานข้อมูลในรูปแบบที่อ่านเข้าใจได้ สามารถพิจารณาลักษณะการควบคุมเพื่อจัดระดับได้ ดังนี้

ระดับ	ลักษณะการควบคุม	0	1	2	3	4	5
Non-existent	ไม่มีความตระหนักถึงความสำคัญของผังโครงสร้างข้อมูลภายในองค์กร	√					
Initial	ผู้บริหารมีความตระหนักว่าองค์กรควรมีการกำหนดผังโครงสร้างข้อมูลด้านสารสนเทศ แต่การกำหนดโครงสร้างข้อมูลด้านสารสนเทศจะขึ้นอยู่กับผู้พัฒนาระบบหรือผู้ขายซอฟท์แวร์		√				
Repeatable	มีการกำหนดผังโครงสร้างข้อมูลด้านสารสนเทศโดยขึ้นอยู่กับความสามารถของบุคลากรภายในองค์กร แต่ยังไม่เป็นรูปแบบเดียวกัน			√			

ระดับ	ลักษณะการควบคุม	0	1	2	3	4	5
Defined	ให้ความสำคัญกับผังโครงสร้างข้อมูลด้านสารสนเทศ อบรมหรือสื่อสารให้มีความเข้าใจของบุคลการในองค์กรที่สอดคล้องตรงกัน กำหนดเครื่องมือที่ใช้และออกแบบโครงสร้างข้อมูลด้านสารสนเทศมาตรฐาน แต่ยังไม่บังคับใช้อย่างเป็นทางการภายในองค์กร				√		
Managed	มีกระบวนการกำหนดผังโครงสร้างข้อมูลด้านสารสนเทศเป็นทางการและบังคับให้ใช้ กำหนดบทบาทหน้าที่ของผู้ดูแลระบบข้อมูลด้านสารสนเทศขององค์กรและมีส่วนร่วมในการให้ข้อมูลเมื่อมีการพัฒนาหรือเปลี่ยนแปลงแก้ไขระบบงาน มีการนำเครื่องมืออัตโนมัติในการสร้างหรือเก็บรวบรวมผังโครงสร้างข้อมูลขององค์กร					√	
Optimized	มีกระบวนการที่ชัดเจนและบังคับใช้ทุกระดับภายในองค์กร มีการพัฒนาและอบรมบุคลากรอย่างต่อเนื่องและมีการทบทวนหรือปรับปรุงให้สามารถนำมาปรับปรุงกระบวนการทำงานให้มีประสิทธิภาพมากขึ้น รวมทั้งมีการกำหนดกลยุทธ์ในการทำ Data mining หรือ Data Warehouse เพื่อให้สามารถนำข้อมูลมาบริหารจัดการได้ตามความต้องการทางธุรกิจ						√

มาตรฐานข้อที่ 7

ก. ข้อกำหนด จัดให้มีสำรองข้อมูลของระบบบัญชีคอมพิวเตอร์เพื่อให้สามารถรองรับการประกอบธุรกิจได้อย่างต่อเนื่อง มีประสิทธิภาพและทันเหตุการณ์ ตลอดจนจัดให้มีการดูแลรักษาข้อมูลชุดสำรองให้มีความปลอดภัย รวมทั้งจัดให้มีการป้องกันมิให้มีการนำข้อมูลสำรองมาใช้อย่างไม่ถูกต้อง

ข. แนวปฏิบัติ

สหกรณ์ที่ใช้เทคโนโลยีสารสนเทศเป็นเครื่องมือในการดำเนินธุรกิจและให้บริการสมาชิก มีความจำเป็นอย่างยิ่งที่จะต้องให้ความสำคัญกับการวางแผนจัดการให้สหกรณ์สามารถดำเนินธุรกิจได้อย่างต่อเนื่องไม่หยุดชะงักแม้จะเกิดเหตุการณ์ผิดปกติเกิดขึ้น มาตรการอย่างหนึ่งที่จะสร้างความมั่นใจให้กับสหกรณ์ในกรณีที่ระบบงานไม่สามารถให้บริการแก่สมาชิกได้ นั่นคือ การจัดให้มีการสำรองข้อมูล

การสำรองข้อมูล เป็นวิธีการที่จะช่วยป้องกันข้อมูลจากการสูญหายเนื่องจากเหตุการณ์ต่างๆ ที่ทำให้ข้อมูลถูกทำลาย ลักษณะของการสำรองข้อมูลขึ้นอยู่กับวิธีการประมวลผลและเทคโนโลยีที่ใช้ในระบบสารสนเทศทางการบัญชี การควบคุมภายในที่เกี่ยวกับการสำรองข้อมูล มีดังนี้

1. ผู้บริหารควรกำหนดนโยบายเกี่ยวกับการสำรองข้อมูลและการกู้คืนข้อมูล ในกรณีที่ข้อมูลถูกทำลาย

2. มีการสำรองข้อมูลเป็นประจำ โดยจัดทำตารางเวลาการทำงานเกี่ยวกับการสำรองข้อมูลของแต่ละระบบงานไว้เป็นส่วนหนึ่งของตารางการประมวลผล โดยจัดทำตารางเวลาสำหรับการสำรองโปรแกรมและข้อมูลแยกจากกัน

3. จัดเก็บข้อมูลสำรองไว้นอกสถานที่แยกต่างหากจากข้อมูลจริง โดยมีการกำหนดระเบียบวิธีในการนำไปจัดเก็บ

4. ทดสอบข้อมูลสำรองเป็นระยะๆ โดยการทดลองนำข้อมูลสำรองที่จัดทำไว้มาทำการกู้คืนข้อมูล และทดสอบแฟ้มข้อมูลที่กู้คืนอย่างสม่ำเสมอ

5. กำหนดเงื่อนไขในการนำสื่อที่ใช้เก็บข้อมูลสำรองมาใช้ใหม่ในการจัดเก็บข้อมูลสำรองชุดใหม่ และเนื่องจากสื่อที่ใช้เก็บข้อมูลสำรองมีอายุงานจำกัด จึงควรมีการหมุนเวียนนำสื่อการจัดเก็บข้อมูลสำรองมาเปลี่ยนแทนอย่างสม่ำเสมอ นอกจากนั้นข้อมูลชุดสำรองอาจต้องมีการจัดเก็บไว้อย่างถาวร เพื่อให้มีข้อมูลสำรองทั้งหมดสำหรับแต่ละเดือนหรือปี

6. จัดระบบสำหรับสื่อที่ใช้เก็บข้อมูลชุดสำรอง

7. ในการกู้คืนข้อมูลจะเริ่มต้นระบบงานใหม่ ควรมีการกำหนดขั้นตอนการทำงานที่เป็นลายลักษณ์อักษร และบันทึกการทำงานที่เกี่ยวข้องเพื่อใช้ในการสอบทาน

นอกจากการจัดให้มีการสำรองข้อมูลแล้ว อีกกระบวนการหนึ่งที่จะต้องพิจารณาร่วมกันเสมอสำหรับสหกรณ์ที่ใช้ระบบเทคโนโลยีสารสนเทศคือ การจัดทำแผนแก้ไขความเสียหายจากเหตุฉุกเฉินต่าง ๆ เพื่อให้การนำข้อมูลสำรองกลับมาใช้เป็นไปอย่างเรียบร้อยและรวดเร็วที่สุดเมื่อเกิดเหตุการณ์ที่ก่อความเสียหาย โดยแผนแก้ไขความเสียหาย มีวัตถุประสงค์ ดังนี้

1. ลดขนาดของความเสียหายหรือความสูญเสีย
2. สร้างระบบการประมวลผลสารสนเทศชั่วคราวเพื่อเป็นทางเลือก
3. เริ่มปฏิบัติงานปกติให้ได้เร็วที่สุด
4. ฝึกอบรมและสร้างบุคลากรให้คุ้นเคยกับเหตุการณ์ฉุกเฉิน

แผนแก้ไขความเสียหายควรประกอบด้วยกิจกรรมต่าง ๆ ดังต่อไปนี้

1. **จัดลำดับความสำคัญของการกู้คืนระบบ** โดยเริ่มจากโปรแกรมที่จำเป็นที่จะทำให้สหกรณ์เริ่มงานได้ อุปกรณ์คอมพิวเตอร์ที่จะต้องใช้เพื่อให้โปรแกรมทำงานได้ และลำดับขั้นตอนรวมทั้งเวลาที่ใช้ในการกู้คืนระบบทั้งหมดกลับมาใช้ได้อีกครั้งหนึ่ง

2. **การสำรองข้อมูลและโปรแกรม** เนื่องจากในการกู้คืนระบบจะต้องมีการกู้แฟ้มข้อมูลที่สูญหายหรือถูกทำลาย โปรแกรมและข้อมูลทุกอย่างต้องมีการสำรองให้ครบถ้วนอย่างสม่ำเสมอ และจัดเก็บไว้ในที่ปลอดภัยและห่างจากระบบคอมพิวเตอร์หลัก นอกจากนี้ วิธีการในการสำรองข้อมูลต้องมีการจัดทำเป็นเอกสาร และต้องมีการฝึกการนำข้อมูลที่สำรองกลับมาใช้ ซึ่งจะช่วยให้พนักงานมีความชำนาญ เมื่อเกิดเหตุการณ์ฉุกเฉินก็สามารถกู้ระบบได้อย่างรวดเร็ว

3. **การมอบหมายหน้าที่เป็นการเฉพาะ** ในการแก้ไขความเสียหาย จะต้องมีการกำหนดหน้าที่ให้แต่ละบุคคลและทีมงานรับผิดชอบเป็นการเฉพาะ โดยกิจกรรมเหล่านี้ต้องรวมถึงการจัดเตรียมสถานที่ตั้งใหม่ การปฏิบัติการคอมพิวเตอร์ การติดตั้งโปรแกรม การสร้างระบบการสื่อสารข้อมูล การกู้คืนข้อมูลรายการที่สำคัญ และการจัดเตรียมแบบฟอร์มและวัสดุต่างๆ

4. **การจัดทำเอกสารประกอบที่สมบูรณ์** แผนการแก้ไขความเสียหายจากเหตุฉุกเฉินจะต้องมีการจัดทำเป็นเอกสารประกอบ มีการจัดทำสำเนาและจัดเก็บไว้ในที่ปลอดภัย เพื่อให้สามารถนำมาใช้งานได้เมื่อมีเหตุการณ์ฉุกเฉิน

5. **เครื่องคอมพิวเตอร์และระบบเครือข่ายสำรอง** ในการจัดเตรียมเครื่องคอมพิวเตอร์และระบบเครือข่ายสำรอง นอกจากการจัดหาเองแล้วยังมีวิธีการอื่นๆ อีก เช่น ทำข้อตกลงกับองค์กรที่มี

ความคล้ายคลึงกันในเรื่องการให้ใช้อุปกรณ์และระบบงานของกันและกันได้ชั่วคราว ในกรณีมีเหตุฉุกเฉิน หรือทำสัญญาขอใช้บริการจากผู้ให้บริการด้านการแก้ไขความเสียหาย เป็นต้น

ในการจัดทำแผนการแก้ไขความเสียหายจากเหตุฉุกเฉิน มีข้อควรพิจารณาที่สำคัญ ดังนี้

1. แผนการแก้ไขความเสียหายจากเหตุฉุกเฉินต้องมีการทดสอบ โดยการจำลองสถานการณ์ทุกรูปแบบโดยมีทีมงานเฉพาะเพื่อกำหนดกิจกรรมต่างๆและควรทดสอบการดำเนินการตามแผนอย่างน้อยปีละครั้ง

2. ต้องมีการสอบทานแผนและปรับปรุงแผนอย่างต่อเนื่อง เพื่อสร้างความมั่นใจว่าแผนงานรองรับสถานการณ์ปัจจุบัน ทั้งในเรื่องระบบงาน การกำหนดค่าอุปกรณ์ต่างๆ และการมอบหมายหน้าที่ให้แต่ละบุคคล

3. ในแผนจะต้องพิจารณาถึงความคุ้มครองที่จะได้จากการประกันภัยว่าครอบคลุมถึงมูลค่าต้นทุนเครื่องจักรและอุปกรณ์ที่ต้องจัดหาทดแทน กิจกรรมต่างๆ ในการกู้ระบบ และการหยุดชะงักของธุรกิจด้วย

การบริหารจัดการการสำรองข้อมูลเพื่อสร้างความต่อเนื่องให้กับธุรกิจ (Ensure Continuous Service) ควรจัดให้มีกิจกรรมดำเนินการ ดังนี้

1. กำหนดและปรับปรุงวิธีการสำหรับการบริหารจัดการเพื่อให้ธุรกิจสามารถดำเนินไปได้อย่างต่อเนื่อง

ความเสี่ยงของการใช้ระบบเทคโนโลยีสารสนเทศประการสำคัญคือ การมีเหตุฉุกเฉินที่ทำให้สหกรณ์ไม่สามารถดำเนินการไปได้อย่างต่อเนื่อง ทำให้ไม่สามารถให้บริการสมาชิกได้ตามปกติ หรืออาจเกิดความเสียหายกับข้อมูลในระบบสารสนเทศ การที่จะสามารถรับสถานการณ์ดังกล่าวนี้ได้โดยการจัดให้มีแผนการแก้ไขความเสียหายจากเหตุฉุกเฉินที่เหมาะสมกับสภาพการใช้งานของสหกรณ์ อย่างไรก็ตาม การสำรองข้อมูลและโปรแกรมระบบงานเป็นมาตรฐานขั้นต่ำที่ทุกสหกรณ์ต้องจัดให้มีในแผนการแก้ไขความเสียหายจากเหตุฉุกเฉิน

2. จัดทำและปรับปรุงแผนสร้างความต่อเนื่องอย่างสม่ำเสมอ

การแก้ไขความเสียหายจากเหตุฉุกเฉิน เป็นสถานการณ์ที่จะต้องดำเนินการด้วยความรวดเร็วและแม่นยำ จึงต้องจัดทำเป็นแผนปฏิบัติการ อย่างไรก็ตาม หากไม่มีเหตุฉุกเฉินจะไม่มีการปฏิบัติการตามแผน ซึ่งโดยปกติเหตุฉุกเฉินจะไม่เกิดขึ้นบ่อย จึงมักปรากฏว่ามีการจัดทำแผนแต่ไม่ทันสมัยหรือไม่เหมาะกับสถานการณ์ของระบบสารสนเทศที่มีการเปลี่ยนแปลงเป็นประจำ ดังนั้น ในการบริหารจัดการสร้างความต่อเนื่องของสหกรณ์จึงควรต้องมีการปรับปรุงแผนทุกๆ ปี

3. กำหนดและปรับปรุงบัญชีรายชื่อระบบงานสำคัญที่มีความจำเป็นต้องกู้คืน

ในแผนการแก้ไขความเสียหายจากเหตุฉุกเฉินควรต้องมีการจัดทำบัญชีรายชื่อระบบงานที่สำคัญที่มีความจำเป็นในการกู้คืนโดยมีการจัดลำดับการเรียกคืนด้วย

ระบบงานของสหกรณ์ที่ใช้และเรียงตามลำดับความสำคัญได้ ดังนี้ ระบบสมาชิกและหุ้น ระบบเงินให้กู้ ระบบเงินรับฝาก ระบบสินค้า ระบบการจัดการระบบ และระบบบัญชีแยกประเภท อย่างไรก็ตาม หากสหกรณ์มีการพัฒนาระบบเพิ่มเติมจากที่กล่าวมาแล้ว ก็ต้องนำมาจัดเรียงลำดับความสำคัญเพิ่มเติม

4. ประเมินความเสี่ยงสำหรับระบบงานสำคัญเหล่านั้น กำหนดมาตรการเพื่อลดความเสี่ยงที่พบ จัดทำรายงานการประเมินความเสี่ยง และแผนดำเนินการลดความเสี่ยง รวมทั้งให้ปรับปรุงรายงานและแผนดำเนินการลดความเสี่ยงอย่างน้อยปีละ 1 ครั้ง ทั้งนี้เนื่องจากระบบงาน และเทคโนโลยีสารสนเทศอาจมีการเปลี่ยนแปลง ซึ่งอาจก่อให้เกิดความเสี่ยงใหม่ๆ เพิ่มเติมได้

5. จัดประชุม แจกจ่าย และแจ้งผู้ที่เกี่ยวข้องทั้งหมดให้ได้รับทราบหลังจากที่มีการปรับปรุงแผนใหม่ โดยระมัดระวังให้ส่งมอบเฉพาะผู้ที่เกี่ยวข้องเท่านั้น

6. ทดสอบแผนสร้างความต่อเนื่องตามรอบระยะเวลาที่กำหนดไว้

เพื่อให้ได้ข้อมูลสำหรับการปรับปรุงแผนและสร้างความคุ้นเคยและความแม่นยำในการปฏิบัติตามแผนเมื่อเกิดเหตุฉุกเฉิน จึงควรมีการทดสอบการปฏิบัติตามแผน อย่างไรก็ตาม ในทางปฏิบัติการทดสอบให้แก่ผู้ปฏิบัติการทดสอบแผนการแก้ไขความเสียหายจากเหตุฉุกเฉินต้องสมมติสถานการณ์ให้เสมือนจริง โดยปกติจะกำหนดดำเนินการทดสอบแผนปีละครั้ง

7. จัดทำรายงานผลการทดสอบและนำเสนอต่อคณะกรรมการดำเนินการ

ดังที่กล่าวมาแล้วว่าข้อมูลที่ได้จากการทดสอบแผนนั้นจะช่วยให้ทราบว่าควรจะต้องปรับปรุงแผนอย่างไร จึงต้องมีการจัดทำรายงานและเสนอต่อคณะกรรมการดำเนินการให้รับทราบ

8. จัดสถานการณ์การทดสอบให้หลากหลายในแต่ละครั้งที่มีการทดสอบ เพื่อให้ครอบคลุมในกรณีต่างๆ ที่อาจเกิดขึ้นได้

การปฏิบัติการแก้ไขความเสียหายจากเหตุฉุกเฉินของผู้ปฏิบัติจะถูกต้องรวดเร็วหรือไม่อย่างไรก็ขึ้นอยู่กับการทดสอบการปฏิบัติตามแผน อย่างไรก็ตาม เหตุฉุกเฉินที่จะเกิดขึ้นเป็นการคาดการณ์ซึ่งอาจเป็นเรื่องของไฟไหม้ การถูกบุกรุก ไฟฟ้าดับ หรือฐานข้อมูลถูกทำลาย ซึ่งไม่อาจจะทราบได้ว่าเหตุฉุกเฉินที่จะเกิดขึ้นเป็นเรื่องใด ในการทดสอบแผนจะต้องสมมติสถานการณ์ให้ครอบคลุมเพื่อที่ผู้ปฏิบัติจะได้เกิดความแม่นยำในการแก้ไขความเสียหายแต่ละกรณี

9. จัดอบรมหรือสร้างความตระหนักให้กับผู้ที่เกี่ยวข้องทั้งหมดเพื่อให้เรียนรู้ถึงหน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติต่างๆ ที่ต้องรับผิดชอบ

การปฏิบัติการแก้ไขความเสียหายจากเหตุฉุกเฉินนั้นมีผู้ที่เกี่ยวข้องหลายฝ่ายที่ต้องทำงานประสานและสอดคล้องกันภายใต้สถานการณ์ฉุกเฉิน การที่จะให้แต่ละบุคคลสามารถปฏิบัติได้อย่างถูกต้องทันเวลานั้นจำเป็นจะต้องมีการอบรมให้มีความรู้ ความเข้าใจอย่างเพียงพอ และสามารถปฏิบัติได้ พร้อมๆ ไปกับการสร้างความตระหนักในหน้าที่และความรับผิดชอบของทุกคนที่เกี่ยวข้อง เพื่อป้องกันไม่ให้เมื่อเกิดเหตุฉุกเฉินขึ้นจะมีการกระทำที่ผิดขั้นตอนซึ่งจะทำให้การปฏิบัติการแก้ไขความเสียหายไม่บังเกิดผล

10. จัดเก็บแผนไว้นอกสถานที่และแจ้งให้ผู้ที่เกี่ยวข้องได้รับทราบเพื่อให้สามารถเข้าถึงได้เมื่อมีความจำเป็น และเมื่อมีการปรับปรุงแผนใหม่ให้นำแผนฉบับใหม่ไปจัดเก็บไว้ด้วย

แผนแก้ไขความเสียหายจากเหตุฉุกเฉิน เป็นเอกสารสำคัญที่จำเป็นอย่างมากที่ต้องใช้เมื่อเกิดเหตุ จึงต้องเก็บเอาไว้ในสถานที่ปลอดภัย มีผู้รับผิดชอบในการดูแลรักษาและการนำออกใช้งาน รวมถึงหากมีการปรับปรุงใหม่ต้องมีการจัดเก็บแผนฉบับล่าสุดไว้ด้วยกันเพื่อให้พร้อมที่จะนำมาใช้งาน

11. จัดให้มีการสำรองข้อมูลของระบบงานสำคัญไว้ทั้งในและนอกสถานที่

การสำรองข้อมูลเป็นเรื่องที่สำคัญอย่างยิ่งสำหรับการแก้ไขความเสียหายจากเหตุฉุกเฉิน เป็นมาตรฐานการควบคุมภายในที่ทุกสหกรณ์ต้องจัดทำ หากสหกรณ์ใดไม่มีการสำรองข้อมูลถือได้ว่าระบบการควบคุมภายในมีจุดอ่อนที่เป็นสาระสำคัญ โดยให้ปฏิบัติตามแนวทางดังนี้

11.1 กำหนดชนิดของข้อมูลที่จะทำการสำรอง

การจัดทำสำรองข้อมูลนั้นต้องเริ่มจากการกำหนดว่าจะสำรองข้อมูลอะไรบ้าง สำหรับสหกรณ์ต้อง**สำรองข้อมูล**ที่เป็นข้อมูลในระบบงานหลักที่ใช้ในการดำเนินธุรกิจและให้บริการสมาชิก ได้แก่ ข้อมูลสมาชิกและหุ้น ข้อมูลเงินให้กู้ ข้อมูลเงินรับฝาก ข้อมูลสินค้า และข้อมูลบัญชีแยกประเภท นอกจากนั้นยังจำเป็นที่จะต้องสำรองข้อมูลที่เกี่ยวกับการกำหนดสิทธิ์การใช้งานและข้อมูลหลักต่างๆ

นอกจากสำรองในส่วนของข้อมูลแล้วยังต้องกำหนดด้วยว่าจะต้องทำ**สำรองโปรแกรม**ด้วย ซึ่งได้แก่ โปรแกรมระบบงานหรือโปรแกรมระบบบัญชี โปรแกรมระบบปฏิบัติการและโปรแกรมระบบจัดการฐานข้อมูล

11.2 ความถี่ในการสำรองข้อมูล

ข้อมูลในระบบสมาชิกและหุ้น ระบบเงินให้กู้ ระบบเงินรับฝาก และระบบสินค้า เป็นข้อมูลที่เกิดทุกวัน ควรสำรองทุกวัน

ข้อมูลในระบบบัญชีแยกประเภท ควรสำรองอย่างน้อยอาทิตย์ละ 3 ครั้ง สำหรับข้อมูลหลัก และข้อมูลในระบบการจัดการควรสำรองเมื่อมีการเปลี่ยนแปลงข้อมูล

11.3 วิธีการสำรอง

วิธีการสำรองข้อมูลซึ่งมีทั้งแบบการสำรองข้อมูลครบทั้งหมด (Full Backup) หรือแบบการสำรองข้อมูลเฉพาะส่วนเพิ่ม (Incremental Backup) ซึ่งจะต้องระบุให้ชัดเจนเพื่อให้เมื่อเกิดความจำเป็นต้องนำข้อมูลสำรองออกใช้งาน จะไม่เกิดความเข้าใจที่คลาดเคลื่อนและปฏิบัติไม่ถูกต้อง

11.4 ทำการสำรองตามความถี่และวิธีการสำรองที่ได้กำหนดไว้

11.5 ประเมินสถานที่เก็บข้อมูลสำรอง (ทั้งภายในและภายนอกสถานที่ทำการ) ปีละครั้งเพื่อให้มั่นใจได้ว่ามีการป้องกันข้อมูลและการเข้าถึงทางกายภาพอย่างเพียงพอ

ข้อมูลชุดสำรองจะต้องจัดเก็บลงสื่ออื่นจัดเก็บนอกระบบงาน แล้วเก็บรักษาไว้ภายนอกสหกรณ์ด้วย โดยมีระบบการดูแลรักษาที่มั่นใจในความปลอดภัยได้ ในกรณีสหกรณ์ที่พิจารณาจัดเก็บไว้ในสหกรณ์ต้องมีระบบการจัดเก็บในที่ปลอดภัย เช่น เก็บในตู้นิรภัยและกำหนดให้มีผู้ดูแลรักษา เป็นต้น

12. ทดสอบกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ เพื่อดูว่าข้อมูลเหล่านั้นยังสามารถใช้งานได้หรือไม่ ถ้าพบว่ามีปัญหาเกิดขึ้นในระหว่างทดสอบกู้คืน ให้หาสาเหตุ ดำเนินการแก้ไข และบันทึกข้อมูลปัญหาพร้อมทั้งวิธีการแก้ไขไว้

เพื่อเป็นการสร้างความมั่นใจว่าเมื่อถึงคราวที่จะต้องปฏิบัติการแก้ไขความเสียหายจากเหตุฉุกเฉินที่ต้องทำการเรียกคืนข้อมูลนั้น จะสามารถดำเนินการได้อย่างเรียบร้อยและได้ข้อมูลกลับมาอย่างครบถ้วนสมบูรณ์ จะต้องมีการทดสอบการเรียกคืนข้อมูลและทดสอบด้วยว่าข้อมูลที่เรียกคืนจากชุดข้อมูลสำรองนั้นสามารถทำงานได้อย่างปกติเทียบเท่าข้อมูลจริง ในบางสถานการณ์อาจพบว่าเมื่อทำการทดสอบการเรียกคืนข้อมูลแล้ว ปรากฏว่าข้อมูลชุดสำรองนั้นเสียหายตั้งแต่กระบวนการสำรองข้อมูล หรือบางแห่งอาจพบปัญหาจากกระบวนการเรียกคืนข้อมูล ซึ่งปัญหาเหล่านี้จะต้องหาสาเหตุและนำไปปรับปรุงแก้ไขต่อไป

13. ให้ตรวจสอบอย่างสม่ำเสมอว่ายังสามารถเข้าถึงข้อมูลที่สำรองไว้ในเครื่องคอมพิวเตอร์และสื่อที่บันทึกข้อมูลนั้นได้หรือไม่

14. ให้ระมัดระวังเรื่องความล้าหลังของเทคโนโลยีที่ใช้ในการบันทึกข้อมูลสำรอง และตรวจสอบเป็นระยะๆ ว่ายังคงจะสามารถถ่ายโอนข้อมูลที่สำรองไว้นั้นไปยังระบบหรือเทคโนโลยีที่ใหม่กว่าได้หรือไม่

เนื่องจากเทคโนโลยีมีการเปลี่ยนแปลงอย่างรวดเร็ว สหกรณ์ควรตระหนักและตรวจสอบว่าสื่อที่ใช้เก็บข้อมูลนั้นยังใช้ได้อยู่หรือไม่ สื่อสำหรับข้อมูลที่ใช้ในปัจจุบัน เช่น External Hard disk, CD ROM หรือ Handy drive เป็นต้น สื่อที่ไม่อาจจะใช้ได้หรือใช้ยากในปัจจุบัน เช่น เทป หรือ Floppy Disk เป็นต้น

15. เมื่อเกิดเหตุฉุกเฉินที่ทำให้เกิดการหยุดชะงักต่อธุรกิจของสหกรณ์ และต้องนำแผนสร้างความต่อเนื่องมาใช้งานหลังเกิดเหตุ ให้ประเมินความเหมาะสมของการปฏิบัติตามแผนว่าสามารถดำเนินการได้สำเร็จหรือไม่ และปรับปรุงแผนตามความจำเป็น

ค. การประเมินระดับการควบคุมภายในและการรักษาความปลอดภัยของสหกรณ์

การจัดให้มีสำรองข้อมูลของระบบบัญชีคอมพิวเตอร์เพื่อให้สามารถรองรับการประกอบธุรกิจได้อย่างต่อเนื่อง มีประสิทธิภาพและทันเหตุการณ์ ตลอดจนจัดให้มีการดูแลรักษาข้อมูลชุดสำรองให้มีความปลอดภัย รวมทั้งจัดให้มีการป้องกันมิให้มีการนำข้อมูลสำรองมาใช้อย่างไม่ถูกต้อง สามารถพิจารณาลักษณะการควบคุมเพื่อจัดระดับได้ ดังนี้

ระดับ	ลักษณะการควบคุม	0	1	2	3	4	5
Non-existent	ไม่มีการประเมินความเสี่ยง หรือภัยคุกคามทางการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ ที่อาจจะมีผลกระทบต่อการให้บริการด้านเทคโนโลยีสารสนเทศต่อสหกรณ์	√					
Initial	มีการกำหนดผู้รับผิดชอบในการให้บริการ เทคโนโลยีสารสนเทศ อย่างต่อเนื่อง ผู้บริหารมีความตระหนักถึงความเสี่ยงที่อาจจะเกิดขึ้นในกรณีที่ไม่สามารถให้บริการเทคโนโลยีสารสนเทศ ซึ่งจะเน้นความต้องการด้านเทคโนโลยีสารสนเทศ มากกว่าความ		√				

ระดับ	ลักษณะการควบคุม	0	1	2	3	4	5
	ต้องการทางด้านธุรกิจ						
Repeatable	มีการกำหนดผู้รับผิดชอบในการให้บริการเทคโนโลยีสารสนเทศอย่างต่อเนื่อง แต่กระบวนการในการจัดการยังไม่เป็นแผนในภาพรวมกรณีที่มีหน่วยงานที่เกี่ยวข้อง มีการรายงานถึงความมีอยู่หรือการพร้อมใช้งานของระบบงานแต่ยังไม่สมบูรณ์ ไม่มีเอกสารเกี่ยวกับแผนการดำเนินระบบให้มีความต่อเนื่องอย่างเป็นลายลักษณ์อักษรถึงแม้ว่าจะให้ความสำคัญต่อความมีอยู่หรือการพร้อมใช้งานของระบบ มีการกำหนดระบบงานที่สำคัญและอุปกรณ์ เทคโนโลยีสารสนเทศ ที่จะมีสถานะพร้อมใช้งาน			√			
Defined	มีการกำหนดผู้รับผิดชอบในการให้บริการเทคโนโลยีสารสนเทศอย่างต่อเนื่องชัดเจน มีการจัดทำแผนการให้บริการเทคโนโลยีสารสนเทศอย่างต่อเนื่องและทดสอบว่าสามารถปฏิบัติได้ตามแผน การกำหนดแผนไปตามระบบงานที่มีความสำคัญและผลกระทบต่อการดำเนินธุรกิจ มีการรายงานผลการทดสอบการให้บริการเทคโนโลยีสารสนเทศอย่างต่อเนื่องเป็นระยะ มีการริเริ่มนำมาตรฐานหรือการฝึกอบรมให้บุคลากรสามารถปฏิบัติได้ตามแผนที่วางไว้ ผู้บริหารมีการสื่อสารให้เข้าใจถึงความต้องการเกี่ยวกับการให้บริการเทคโนโลยีสารสนเทศอย่างต่อเนื่อง แต่การพร้อมใช้งานหรือความมีอยู่ของระบบงานอย่างต่อเนื่องอาจจะมีการกำหนดซ้ำซ้อนและไม่มีประสิทธิภาพ				√		

ระดับ	ลักษณะการควบคุม	0	1	2	3	4	5
Managed	ความรับผิดชอบและมาตรฐานการให้บริการเทคโนโลยีสารสนเทศ ต่อเนื่องกำหนดให้มีการถือปฏิบัติ มีการปรับปรุงแผนการให้บริการ เทคโนโลยีสารสนเทศต่อเนื่องจากสม่ำเสมอ กระบวนการบำรุงรักษาอุปกรณ์เทคโนโลยีสารสนเทศ ทำให้สามารถป้องกันการหยุดชะงักของบริการให้เทคโนโลยีสารสนเทศ และมีทดสอบแผนอย่างสม่ำเสมอ มีการเก็บรวมรวมข้อมูล วิเคราะห์และรายงานเกี่ยวกับการให้บริการเทคโนโลยีสารสนเทศอย่างต่อเนื่อง มีระบบสำรองหรือศูนย์สำรองที่สามารถรองรับเหตุการณ์ฉุกเฉินได้อย่างทันท่วงที					√	
Optimized	การให้บริการ เทคโนโลยีสารสนเทศอย่างต่อเนื่องอย่างเป็นระบบ มีระบบอัตโนมัติมาช่วยให้การบริการเทคโนโลยีสารสนเทศต่อเนื่องและสามารถดำเนินได้ตามแผนที่วางไว้ สามารถนำระดับการให้บริการเทคโนโลยีสารสนเทศ อย่างต่อเนื่องไปเทียบเคียงกับองค์กรอื่น นำผลการทดสอบแผนดำรงอยู่กิจการอย่างต่อเนื่องมาปรับปรุงกระบวนการบำรุงรักษาให้สอดคล้องกับความต้องการหรือสถานการณ์ที่อาจจะมีผลกระทบต่อการดำเนินธุรกิจ						√

มาตรฐานข้อที่ 8

ก. ข้อกำหนด ในกรณีที่มีการใช้บริการงานเทคโนโลยีสารสนเทศของผู้ให้บริการ ซึ่งเป็นบุคคลภายนอกต้องจัดให้มีหลักเกณฑ์ในการคัดเลือกและพิจารณาความเหมาะสมของผู้ให้บริการ รวมทั้งควบคุมและตรวจสอบการปฏิบัติงานของผู้ให้บริการอย่างเข้มงวด เพื่อให้มั่นใจว่าผู้ให้บริการสามารถปฏิบัติตามระเบียบนี้ได้

ข. แนวปฏิบัติ

การใช้บริการงานเทคโนโลยีสารสนเทศของผู้ให้บริการ ซึ่งเป็นบุคคลภายนอกต้องจัดให้มีหลักเกณฑ์ในการคัดเลือกและพิจารณาความเหมาะสมของผู้ให้บริการ โดยควรพิจารณาการบริหารจัดการการให้บริการโดยหน่วยงานภายนอก (Manage Third-party Services) ดังนี้

1. กำหนดและปรับปรุงชนิดของบริการต่างๆ ที่ให้โดยหน่วยงานภายนอก และจัดหมวดหมู่บริการเหล่านั้นตามชนิดของบริการ และระดับความสำคัญ

2. จัดทำและปรับปรุงเอกสารข้อตกลงการให้บริการตามความจำเป็นหรือตามกรอบระยะเวลาที่กำหนดไว้ ดังตัวอย่างสัญญาให้บริการบำรุงรักษาระบบงานคอมพิวเตอร์

3. กำหนดผู้ดูแลรับผิดชอบสำหรับการให้บริการของหน่วยงานภายนอก เพื่อให้สามารถควบคุมดูแลการให้บริการเป็นไปตามเอกสารข้อตกลง

4. กรณีที่มีการเปลี่ยนผู้ดูแลรับผิดชอบ ให้ปรับปรุงสัญญาเพื่อเปลี่ยนชื่อผู้ดูแลรับผิดชอบนั้น และแจ้งให้ผู้ที่เกี่ยวข้องได้รับทราบ

5. จัดทำและปรับปรุงสัญญาการให้บริการตามความจำเป็นโดยต้อง

   5.1 ประเมินความเสี่ยงสำหรับการให้บริการนั้น และกำหนดมาตรการเพื่อลดความเสี่ยง เพื่อให้การให้บริการเป็นไปอย่างได้ผล และบรรจุมาตรการลดความเสี่ยงไว้เป็นส่วนหนึ่งของสัญญา

   5.2 อ้างอิงตามมาตรฐานของสัญญาการพัฒนาระบบงาน สัญญาบำรุงรักษาห้องเครื่อง สัญญาดูแลรักษาฮาร์ดแวร์ สัญญาให้บริการเครือข่าย และ/หรือสัญญาให้บริการ Helpdesk

   5.3 จัดทำสัญญาการไม่เปิดเผยความลับ (Non Disclosure Agreement) เนื่องจากข้อมูลของสหกรณ์เป็นข้อมูลทางการเงินของสมาชิกและของสหกรณ์เป็นส่วนใหญ่ ดังนั้น เพื่อป้องกันไม่ให้มีการเปิดเผยข้อมูลส่วนบุคคลจึงควรมีการตกลงการไม่เปิดเผยความลับไว้ในสัญญาด้วย

6. ติดตามและรายงานการให้บริการโดยหน่วยงานภายนอกอย่างสม่ำเสมอ เพื่อให้เป็นไปตามระดับการให้บริการและตรงตามความต้องการทางธุรกิจของสหกรณ์

7. ตรวจสอบเป็นระยะๆ ว่าความสามารถในการให้บริการของผู้ให้บริการจะต้องเทียบเคียงได้กับผู้ให้บริการรายอื่น ๆ

ตัวอย่างสัญญาให้บริการบำรุงรักษาระบบงานคอมพิวเตอร์

สัญญานี้ทำที่.....

เมื่อวันที่.....เดือน.....พ.ศ.....ระหว่าง

ก. นาย/นาง/นางสาว..... อายุ.....ปี

ห้างหุ้นส่วนจำกัด..... โดยผู้มีอำนาจลงนามท้ายสัญญา/

บริษัท.....จำกัด โดยผู้มีอำนาจลงนามท้ายสัญญา

อยู่บ้านเลขที่/สำนักงานเลขที่.....หมู่ที่.....ตรอก/ซอย.....

ถนน.....แขวง/ตำบล.....เขต/อำเภอ.....

จังหวัด..... บัตรประจำตัวประชาชนเลขที่.....

ออกให้โดย.....ซึ่งต่อไปจะเรียกว่า “ผู้ให้บริการ” ฝ่ายหนึ่ง กับ

ข. นาย/นาง/นางสาว.....อายุ.....ปี

ห้างหุ้นส่วนจำกัด.....โดยผู้มีอำนาจลงนามท้ายสัญญา/

บริษัท.....จำกัด โดยผู้มีอำนาจลงนามท้ายสัญญา

อยู่บ้านเลขที่/สำนักงานเลขที่.....หมู่ที่.....ตรอก/ซอย.....

ถนน.....แขวง/ตำบล.....เขต/อำเภอ.....

จังหวัด.....บัตรประจำตัวประชาชนเลขที่.....

ออกให้โดย.....ซึ่งต่อไปจะเรียกว่า “ผู้รับบริการ” อีกฝ่ายหนึ่ง

โดยที่ผู้รับบริการเป็นผู้ประกอบธุรกิจเกี่ยวกับ.....

มีความประสงค์จะใช้บริการแก้ไข และบำรุงรักษาระบบงานคอมพิวเตอร์ของผู้รับบริการ และ

โดยที่ผู้ให้บริการเป็นผู้ประกอบธุรกิจเกี่ยวกับ.....

เป็นผู้มีความรู้ ความสามารถ ความชำนาญ และประสบการณ์ในด้านดังกล่าว และประสงค์จะให้บริการ

แก้ไข และบำรุงรักษาระบบงานคอมพิวเตอร์ของผู้รับบริการ ภายใต้หลักเกณฑ์และเงื่อนไขที่กำหนดไว้ในสัญญานี้

ดังนั้น ทั้งสองฝ่ายจึงตกลงทำสัญญากัน โดยมีข้อความดังต่อไปนี้

ข้อ 1. วัตถุที่ประสงค์แห่งสัญญา

1.1 ผู้ให้บริการตกลงให้บริการ และผู้รับบริการตกลงรับบริการแก้ไขและบำรุงรักษาระบบงานคอมพิวเตอร์ของผู้รับบริการ ดังนี้

1.1.1 .....

1.1.2 .....

1.1.3 .....

ระบบงานคอมพิวเตอร์ตามข้อ 1.1.1 ถึง 1.1.3 ต่อไปจะเรียกรวมเรียกว่า “ระบบงานคอมพิวเตอร์”

การให้บริการตามสัญญานี้ จะต้องเป็นไปตามกำหนดเวลาที่ได้ระบุไว้ ในสัญญา หรือเมื่อผู้รับบริการร้องขอ โดยรายละเอียดของการให้บริการปรากฏตามเอกสารแนบท้ายสัญญา และให้ถือเป็นส่วนหนึ่งของสัญญานี้ ซึ่งต่อไปจะเรียกว่า “งานบริการ”

1.2 ทั้งสองฝ่ายทราบและเข้าใจดีว่างานบริการไม่รวมถึงการให้บริการดังต่อไปนี้

ก) การแก้ไข ปรับปรุงหรือเปลี่ยนแปลงระบบงานคอมพิวเตอร์ โดยผู้รับบริการหรือบุคคลภายนอก โดยไม่ได้รับความยินยอมจากผู้ให้บริการ

ข) การละเลย หรือใช้ระบบงานคอมพิวเตอร์ไม่ถูกวิธี หรือไม่ปฏิบัติตามคำแนะนำที่ได้ระบุไว้ในเอกสารประกอบ

ค) การแก้ไข บำรุงรักษาระบบงานคอมพิวเตอร์ที่ไม่ได้กำหนดในสัญญานี้

ง) ความเสียหายอันเกิดจากเหตุสุดวิสัย

จ) การที่ผู้รับบริการใช้หรือเชื่อมต่อระบบงานคอมพิวเตอร์กับฮาร์ดแวร์หรือระบบงานคอมพิวเตอร์อื่น ๆ ที่ผู้ให้บริการไม่ได้ระบุว่าสามารถใช้ได้กับระบบงานคอมพิวเตอร์ของผู้รับบริการ

ฉ) ระบบงานคอมพิวเตอร์ของบุคคลภายนอก

ข้อ 2. กำหนดระยะเวลาของสัญญา

ทั้งสองฝ่ายตกลงให้สัญญานี้มีกำหนดระยะเวลา.....ปี นับแต่วันที่.....เดือน.....พ.ศ.....ถึงวันที่.....เดือน.....พ.ศ.....

ข้อ 3. ราคาและการชำระราคา

ในวันทำสัญญาฉบับนี้ ผู้รับบริการตกลงชำระค่าบริการตามสัญญานี้ให้ผู้ให้บริการล่วงหน้าเป็นระยะเวลา.....เดือน/ปี เป็นจำนวนเงิน..... บาท (.....) โดยรวมภาษีมูลค่าเพิ่มตามอัตราที่กฎหมายกำหนด (ถ้ามี) ชำระเป็นเงินสด/เช็คธนาคาร..... สาขา..... เลขที่..... ลงวันที่.....เดือน.....พ.ศ. ..... ผู้ให้บริการได้รับเงินสด/เช็คดังกล่าวไว้เรียบร้อยแล้วในวันทำสัญญาฉบับนี้

ข้อ 4. สิทธิและหน้าที่ของผู้รับบริการ

ผู้รับบริการสัญญาทราบดีว่า

4.1 ผู้รับบริการจะต้องให้ความร่วมมือแก่ผู้ให้บริการในการจัดหาข้อมูลรวมทั้งเอกสารต่าง ๆ ที่จำเป็นเพื่อให้ผู้ให้บริการสามารถปฏิบัติงานบริการได้อย่างสำเร็จลุล่วง

4.2 ผู้รับบริการจะต้องจัดสภาพการทำงานซึ่งปลอดภัย และอำนวยความสะดวกให้แก่ช่างผู้ชำนาญงาน และหรือตัวแทนของผู้ให้บริการ ในการที่จะเข้าไปทำงานบริการ

ข้อ 5. สิทธิและหน้าที่ของผู้ให้บริการ

ผู้ให้บริการสัญญาทราบดีว่า

5.1 ผู้ให้บริการจะใช้ความรู้ความสามารถ และความอุตสาหะในการทำงานบริการให้แก่ผู้รับบริการตามสัญญานี้เพื่อให้งานบริการสำเร็จลุล่วง

5.2 ในกรณีที่ผู้ให้บริการจะต้องมาทำงานบริการ ณ สถานที่ทำการของผู้รับบริการ ผู้ให้บริการจะต้องปฏิบัติตามระเบียบการใช้สถานที่ของผู้รับบริการที่มีอยู่ ณ วันทำสัญญานี้ และที่จะมีขึ้นในอนาคต ให้ถือเป็นส่วนหนึ่งของสัญญานี้ด้วย

5.3 ผู้ให้บริการจะทำงานบริการเฉพาะระบบงานคอมพิวเตอร์ที่ผู้รับบริการได้รับอนุญาตให้ใช้จากผู้ให้บริการเท่านั้น

5.4 ผู้ให้บริการไม่มีสิทธินำงานบริการตามสัญญานี้ออกให้บุคคลภายนอกให้บริการช่วง เว้นแต่จะได้รับความยินยอมจากผู้รับบริการก่อน

5.5 กรณีที่เกิดเหตุขัดข้องกับระบบงานคอมพิวเตอร์ทำให้ระบบงานคอมพิวเตอร์ไม่สามารถใช้การได้ตามปกติ ผู้ให้บริการจะส่งช่างผู้ชำนาญงานมาดำเนินการแก้ไข ระบบงานคอมพิวเตอร์ ภายในเวลา..... ชั่วโมง นับจากเวลาที่ได้รับแจ้งถึงเหตุขัดข้องนั้น จากผู้รับบริการ

โดยผู้ให้บริการจะดำเนินการแก้ไขระบบงานคอมพิวเตอร์ ให้อยู่ในสภาพใช้งาน ได้ดีตามปกติภายใน .....ชั่วโมงนับแต่วันที่ได้รับแจ้งโดยไม่คิดค่าบริการและค่าใช้จ่ายใดๆเพิ่มเติมจากผู้รับบริการอีก

5.6 จะไม่ใช้ เปิดเผย และหรือเอาไป ซึ่งข้อมูลการค้าอันเป็นความลับทางการค้าของผู้รับบริการ และหรืออนุญาตให้บุคคลอื่นกระทำการดังกล่าว โดยไม่ได้รับความยินยอมจากผู้รับบริการเป็นลายลักษณ์อักษร

ข้อ 6. นิติสัมพันธ์ระหว่างคู่สัญญา

ผู้ให้บริการตกลงและทราบดีว่า การให้บริการตามสัญญานี้ ผู้รับบริการและผู้ให้บริการไม่มีนิติสัมพันธ์กันในลักษณะจ้างแรงงานแต่อย่างใด

ข้อ 7. การผิดนัดผิดสัญญา

หากคู่สัญญาฝ่ายใดผิดสัญญาข้อหนึ่งข้อใด ให้คู่สัญญาอีกฝ่ายบอกกล่าวเป็นหนังสือให้คู่สัญญาที่ผิดสัญญาแก้ไขเยียวยาภายใน.....วันทำการ หากคู่สัญญาฝ่ายที่ผิดสัญญาเพิกเฉย หรือไม่แก้ไขเยียวยาให้แล้วเสร็จภายในระยะเวลาที่กำหนด คู่สัญญาอีกฝ่ายมีสิทธิบอกเลิกสัญญา และเรียกค่าเสียหายได้

ข้อ 8. ข้อตกลงอื่นๆ

8.1 กรณีที่คู่สัญญามีสิทธิคิดดอกเบี้ยต่อกัน ทั้งสองฝ่ายตกลงให้ใช้อัตราดอกเบี้ยร้อยละ.....ต่อปี นับแต่วันผิดนัด

8.2 การผ่อนผัน ผ่อนเวลา หรือการละเว้นการใช้สิทธิใด ๆ ที่คู่สัญญาฝ่ายหนึ่งมีอยู่กับคู่สัญญาอีกฝ่ายหนึ่งตามสัญญานี้ ไม่ถือว่า คู่สัญญาฝ่ายนั้นได้สละสิทธิประโยชน์นั้นต่อคู่สัญญาอีกฝ่ายหนึ่งแต่อย่างใด

8.3 การบอกกล่าว ทวงถาม หรือส่งเอกสารใดๆอันพึงมีแก่คู่สัญญาอีกฝ่ายหนึ่งตามภูมิลำเนาที่ปรากฏในสัญญานี้ ให้ถือว่าส่งโดยชอบและคู่สัญญาอีกฝ่ายได้ทราบแล้วนับแต่วันที่คำบอกกล่าวหรือเอกสารนั้นพึงไปถึงตามปกติ

สัญญานี้ทำขึ้นเป็นสองฉบับ มีข้อความถูกต้องตรงกันทั้งสองฝ่ายได้ทราบและเข้าใจข้อความโดยตลอดดีแล้ว เห็นว่าถูกต้องตรงตามเจตนาของตน จึงได้ลงลายมือชื่อพร้อมประทับตรา (ถ้ามี) ไว้เป็นสำคัญต่อหน้าพยาน และต่างยึดถือไว้ฝ่ายละฉบับ

ลงชื่อ .....ผู้ให้บริการ
( )

ลงชื่อ ..... ผู้รับบริการ
( )

ลงชื่อ .....พยาน
( )

ลงชื่อ .....พยาน
( )

ค. การประเมินระดับการควบคุมภายในและการรักษาความปลอดภัยของสหกรณ์

การใช้บริการงานเทคโนโลยีสารสนเทศของผู้ให้บริการ ซึ่งเป็นบุคคลภายนอกต้องจัดให้มีหลักเกณฑ์ในการคัดเลือกและพิจารณาความเหมาะสมของผู้ให้บริการ รวมทั้งควบคุมและตรวจสอบการปฏิบัติงานของผู้ให้บริการอย่างเข้มงวด เพื่อให้มั่นใจว่าผู้ให้บริการสามารถปฏิบัติตามระเบียบนี้ สามารถพิจารณาลักษณะการควบคุมเพื่อจัดระดับได้ ดังนี้

ระดับ	ลักษณะการควบคุม	0	1	2	3	4	5
Non-existent	ไม่มีการกำหนดนโยบายหรือวิธีปฏิบัติเกี่ยวกับสัญญาการใช้บริการงานเทคโนโลยีสารสนเทศของผู้ให้บริการ	√					
Initial	ผู้บริหารให้ความสำคัญและมีการลงนามในสัญญาการให้บริการงานเทคโนโลยีสารสนเทศ แต่ยังไม่มีการกำหนดข้อกำหนดมาตรฐานการให้บริการอย่างเหมาะสม		√				

ระดับ	ลักษณะการควบคุม	0	1	2	3	4	5
Repeatable	มีกระบวนการควบคุมดูแลผู้ให้บริการงานเทคโนโลยีสารสนเทศให้มีการบริการงานอย่างเหมาะสม สัญญาการให้บริการมีการใช้ข้อกำหนดมาตรฐานการให้บริการของผู้ให้บริการมากกว่าที่จะกำหนดตามความต้องการของสหกรณ์เป็นหลัก			√			
Defined	มีกระบวนการปฏิบัติงานที่ครอบคลุมการจัดจ้างผู้ให้บริการงานเทคโนโลยีสารสนเทศ ลักษณะการให้บริการจะมีรายละเอียดเกี่ยวกับขอบเขตการทำงาน ข้อกฎหมายและความต้องการด้านการควบคุมภายในของสหกรณ์ที่ผู้ให้บริการจะต้องปฏิบัติตาม มีการควบคุมดูแลการให้บริการและมีกรอบมาตรฐานการให้บริการที่ถือเป็นส่วนหนึ่งของสัญญา				√		
Managed	ขอบเขตการให้บริการ ลักษณะการให้บริการ ผลงานที่ส่งมอบ ข้อสมมติฐาน ระยะเวลาการทำงาน และข้อกำหนดทางธุรกิจมีการกำหนดไว้อย่างเป็นลายลักษณ์อักษรและเป็นมาตรฐาน มีการติดตามผลการให้บริการเปรียบเทียบกับข้อกำหนดในสัญญาเพื่อให้สามารถประเมินความสามารถในการให้บริการทั้งในปัจจุบันและต่อไปในอนาคต					√	
Optimized	มีการประเมินคุณภาพการให้บริการ และมีการติดตามการปฏิบัติตามขอบเขตการทำงาน ข้อกฎหมายและความต้องการด้านการควบคุมภายในของสหกรณ์อย่างสม่ำเสมอ ผู้ให้บริการประเมินตนเองและรับฟังความคิดเห็นจากสหกรณ์เพื่อปรับปรุงให้มีประสิทธิภาพและสอดคล้องกับความต้องการทางธุรกิจของสหกรณ์ การวัดผลการทำงานของผู้						√

ระดับ	ลักษณะการควบคุม	0	1	2	3	4	5
	ให้บริการเพื่อให้สามารถทราบปัญหาการทำงานได้ล่วงหน้า						

มาตรฐานข้อที่ 9

ก. ข้อกำหนด จัดให้มีการตรวจสอบคอมพิวเตอร์โดยหน่วยงานภายในของสหกรณ์และกลุ่มเกษตรกรเองหรือโดยผู้ตรวจสอบที่เป็นบุคคลภายนอก เพื่อทำหน้าที่ตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศทุกประเภทที่อาจเกิดขึ้นได้

ข. แนวปฏิบัติ

การสอบบัญชีในสภาพแวดล้อมของระบบสารสนเทศที่ใช้คอมพิวเตอร์ซึ่งเกิดขึ้นเมื่อมีการใช้คอมพิวเตอร์ไม่ว่าระบบคอมพิวเตอร์ที่สหกรณ์ใช้จะเป็นระบบคอมพิวเตอร์ประเภทใดหรือมีขนาดเท่าใดโดยได้มีการประมวลผลข้อมูลทางการเงินซึ่งมีความสำคัญต่อการสอบบัญชี ทั้งนี้ ไม่ว่าการประมวลผลนั้นจะดำเนินการโดยสหกรณ์หรือมอบหมายให้บุคคลภายนอกดำเนินการก็ตาม ผู้สอบบัญชีจึงควรมีความรู้เกี่ยวกับระบบสารสนเทศที่ใช้คอมพิวเตอร์อย่างเพียงพอ เพื่อวางแผน สั่งการ ควบคุมดูแล และสอบทานงานที่ได้ปฏิบัติ รวมทั้ง ต้องพิจารณาว่าจำเป็นต้องใช้ผู้เชี่ยวชาญด้านระบบสารสนเทศช่วยในการตรวจสอบหรือไม่

การตรวจสอบระบบสารสนเทศที่ใช้คอมพิวเตอร์ เป็นการตรวจสอบเพื่อแสดงความเห็นต่อระบบการควบคุมสารสนเทศที่องค์กรใช้ว่าเหมาะสมและเป็นไปตามวัตถุประสงค์ของการควบคุมที่กำหนดไว้หรือไม่เพียงใด โดยที่วัตถุประสงค์ของการควบคุมนั้นถูกกำหนดขึ้นโดยผู้บริหารหรือผู้ออกแบบระบบ แต่ผู้ตรวจสอบจะเป็นผู้ที่ทำการตรวจสอบเพื่อให้เกิดความมั่นใจว่าระบบการควบคุมที่กำหนดขึ้นหรือที่ได้ออกแบบไว้นั้นเพียงพอ เหมาะสม มีการปฏิบัติตาม และบรรลุผลตามวัตถุประสงค์ที่กำหนดไว้หรือไม่เพียงใด ทั้งนี้ วัตถุประสงค์ในการตรวจสอบระบบสารสนเทศที่ใช้คอมพิวเตอร์โดยผู้สอบบัญชีนั้น เพื่อพิจารณาว่า ระบบสารสนเทศที่สหกรณ์ใช้ในการประมวลผลข้อมูลที่จำเป็นต่อการจัดทำงบการเงินและการตรวจสอบมีการทำงานตามที่กำหนดไว้หรือไม่ และรายการทางบัญชีที่บันทึกอยู่ในระบบและข้อมูลที่ออกจากระบบมีความถูกต้อง ครบถ้วน และสะท้อนสถานะทางการเงินที่แท้จริงของสหกรณ์หรือไม่

การตรวจสอบคอมพิวเตอร์โดยหน่วยงานภายในของสหกรณ์หรือโดยบุคคลภายนอก เพื่อทำการตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศที่อาจเกิดขึ้น มีแนวทางในการจัดระบบการควบคุม ดังนี้

1. มีการกำหนดนโยบายและติดตามประเมินผลการควบคุมภายในด้านเทคโนโลยีสารสนเทศ

2. มีการกำหนดรายละเอียดของรายงานการควบคุมภายในให้เพียงพอที่คณะกรรมการดำเนินการจะสามารถนำไปใช้ประกอบการตัดสินใจได้

3. มีการทบทวนการควบคุมภายในด้านเทคโนโลยีสารสนเทศโดยคณะกรรมการดำเนินการ

4. มีการจัดเก็บข้อมูลที่เกี่ยวข้องกับข้อผิดลาด การทำงานที่ผิดปกติ และการละเว้นไม่ปฏิบัติอย่างเป็นระบบ และรายงานให้คณะกรรมการดำเนินการทราบ

5. มีการสอบทานการควบคุมภายในโดยคณะกรรมการดำเนินการ เพื่อกำหนดแนวทางการปฏิบัติและการแก้ไข

6. คณะกรรมการดำเนินการให้ความสำคัญในเรื่องของการรายงานด้านการรักษาความปลอดภัย และการสอบทานการควบคุมภายใน

7. จัดให้มีการปรับปรุงการควบคุมภายในให้เข้ากับการปฏิบัติงานอย่างสม่ำเสมอ เพื่อให้ทันสมัยและทันต่อเหตุการณ์ปัจจุบัน

8. ระยะเวลาในการรายงานควรมีความรวดเร็ว เพื่อที่จะดำเนินการแก้ไขปัญหาและข้อผิดพลาดได้ทันเวลา

9. มีการกำหนดนโยบายเกี่ยวกับความปลอดภัยในการปฏิบัติงานและการควบคุมภายในให้ชัดเจน

10. มีการประเมินระบบการรักษาความปลอดภัยและการควบคุมภายในว่ายังเชื่อถือได้โดยประเมินตัวเองหรือให้ผู้ประเมินอิสระ

11. มีการสอบทานอย่างสม่ำเสมอเพื่อปรับปรุงให้น่าเชื่อถือโดยผู้ตรวจสอบภายในหรือภายนอก

ค. การประเมินระดับการควบคุมภายในและการรักษาความปลอดภัยของสหกรณ์

การจัดให้มีการตรวจสอบคอมพิวเตอร์โดยหน่วยงานภายในของสหกรณ์และกลุ่มเกษตรกรเองหรือโดยผู้ตรวจสอบที่เป็นบุคคลภายนอก เพื่อทำหน้าที่ตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศทุกประเภทที่อาจเกิดขึ้นได้ สามารถพิจารณาลักษณะการควบคุมเพื่อจัดระดับได้ ดังนี้

ระดับ	ระดับการควบคุม	0	1	2	3	4	5
Non-existent	ไม่มีการประเมินการควบคุมภายในด้านเทคโนโลยีสารสนเทศขององค์กร	√					
Initial	มีการประเมินการควบคุมภายในด้านเทคโนโลยีสารสนเทศเมื่อผู้บริหารมีความต้องการและร้องขอให้มีการประเมิน ยังไม่มีกระบวนการประเมินการควบคุมภายในด้านเทคโนโลยีสารสนเทศอย่างเป็นทางการ		√				
Repeatable	องค์กรมีการประเมินการควบคุมภายในด้านเทคโนโลยีสารสนเทศ โดยมีการจัดทำรายงานผลการตรวจสอบเพื่อปรับปรุงการควบคุมภายในและมีการติดตามผล แต่ยังไม่มีการกำหนดแผนการประเมินการควบคุมภายในอย่างเป็นทางการ และปัจจัยเสี่ยงด้านเทคโนโลยีสารสนเทศจะกำหนดตามความสามารถของตัวบุคคล			√			
Defined	คณะกรรมการดำเนินการให้การสนับสนุนในการประเมินผลการควบคุมภายใน มีการกำหนดนโยบายและกระบวนการประเมินและการรายงานผลของการประเมินการควบคุม มีโปรแกรมการฝึกอบรมให้สามารถประเมินการควบคุมภายในด้วยตนเองหรือผู้ประเมินการควบคุมภายในภายนอกองค์กร มีการใช้เครื่องมือในการประเมินแต่ยังไม่มีการเชื่อมโยงความเสี่ยงด้านเทคโนโลยีสารสนเทศกันภายในกระบวนการหรือภายในสหกรณ์				√		

ระดับ	ระดับการควบคุม	0	1	2	3	4	5
Managed	คณะกรรมการดำเนินการกำหนดกรอบการประเมินการควบคุมภายในด้านเทคโนโลยีสารสนเทศ มีการกำหนดหรือนำมาตรฐานสากลมาใช้ในการประเมิน กำหนดบทบาทหน้าที่ของผู้ประเมินการควบคุมภายในด้านเทคโนโลยีสารสนเทศอย่างเป็นทางการ มีการจัดทำฐานข้อมูลองค์ความรู้และผู้ประเมินมีทักษะหรือใบประกาศนียบัตรในการประเมินการควบคุมภายในด้านเทคโนโลยีสารสนเทศ					√	
Optimized	คณะกรรมการดำเนินการมีการกำหนดกระบวนการปรับปรุงการควบคุมภายในอย่างต่อเนื่องโดยนำผลจากการประเมินและเปรียบเทียบกับมาตรฐานสากลในธุรกิจระดับเดียวกัน มีการใช้เครื่องมือในการตรวจสอบหรือติดตามประเมินผลการควบคุมภายในอย่างต่อเนื่อง						√

บทที่ 5

บทสรุปและข้อเสนอแนะ

บทที่ 5
บทสรุปและข้อเสนอแนะ

บทสรุป

ความเป็นมาของมาตรฐานขั้นต่ำการควบคุมภายในสำหรับสหกรณ์ที่ใช้โปรแกรมระบบบัญชี

ปัจจุบันสหกรณ์มีการใช้โปรแกรมระบบบัญชีในการประมวลผลข้อมูลทางการเงินและใช้ในการให้บริการสมาชิกเพิ่มขึ้นอย่างมาก ตัวเลขจากระบบฐานข้อมูลสหกรณ์ที่ใช้เทคโนโลยีทางการบัญชี กรมตรวจบัญชีสหกรณ์ ณ วันที่ 30 กันยายน 2555 พบว่า ในจำนวนสหกรณ์ทั้งสิ้น 6,637 แห่ง เป็นสหกรณ์ที่ใช้โปรแกรมระบบบัญชีสหกรณ์ในการประมวลผลข้อมูลถึงจำนวน 3,785 แห่ง หรือคิดเป็นร้อยละ 57.03 ซึ่งนับว่าในระบบสหกรณ์มีการนำเทคโนโลยีมาใช้ในการบริหารจัดการข้อมูลเป็นจำนวนมาก แต่อย่างไรก็ตาม การนำเทคโนโลยีมาใช้ในองค์กรนั้นมีทั้งข้อดีที่ช่วยให้การดำเนินการรวดเร็วและถูกต้องแม่นยำมากขึ้น และข้อเสียก็คือการใช้เทคโนโลยีนั้นจะมีความเสี่ยงในการบริหารจัดการมากขึ้น ดังนั้น เพื่อให้สหกรณ์ที่ใช้เทคโนโลยีทางการบัญชีได้ตระหนักและมีแนวปฏิบัติในการควบคุมภายใน รวมทั้งมีแนวทางในการรักษาความปลอดภัย นายทะเบียนสหกรณ์จึงได้ออกระเบียบนายทะเบียนสหกรณ์ ว่าด้วย “มาตรฐานขั้นต่ำในการควบคุมภายในและการรักษาความปลอดภัยสำหรับสหกรณ์และกลุ่มเกษตรกรที่ใช้โปรแกรมระบบบัญชีคอมพิวเตอร์ประมวลผลข้อมูล พ.ศ. 2553” โดยระเบียบนี้มีการกำหนดมาตรฐานขั้นต่ำในการควบคุมภายในและการรักษาความปลอดภัยสำหรับสหกรณ์ที่ใช้โปรแกรมระบบบัญชีคอมพิวเตอร์ประมวลผลข้อมูลจำนวน 9 ข้อ

มาตรฐานการรักษาความปลอดภัยข้อมูล

เพื่อปกป้องการดำเนินธุรกิจสหกรณ์ จึงได้นำหลักการของมาตรฐานการรักษาความปลอดภัยของข้อมูลที่อยู่ในสภาพแวดล้อมที่ใช้คอมพิวเตอร์ มาเป็นแนวทางในการพัฒนามาตรฐานขั้นต่ำการควบคุมภายในและการรักษาความปลอดภัยตามที่กำหนดในระเบียบนายทะเบียนสหกรณ์ มาตรฐานดังกล่าวคือ มาตรฐาน COBIT (Control Objective for Information and Related Technology) และมาตรฐาน ITIL (The Information Technology Infrastructure) รวมทั้งมาตรฐานการสอบบัญชีที่เกี่ยวข้องกับการตรวจสอบระบบสารสนเทศในสภาพแวดล้อมที่ใช้คอมพิวเตอร์

มาตรฐาน COBIT เป็นแนวทางในการปฏิบัติสำหรับการบริหารองค์กรที่ใช้เทคโนโลยีสารสนเทศ ซึ่งสมาคมผู้ตรวจสอบและควบคุมระบบสารสนเทศ หรือ ISACA (Information Systems Audit and Control Association) เป็นหน่วยงานที่กำหนดและกำกับดูแลมาตรฐาน COBIT ซึ่งองค์กร

สามารถนำไปปรับใช้ในกิจกรรมทางด้านเทคโนโลยีสารสนเทศเพื่อให้มีระบบการควบคุมภายในที่รัดกุม โดยรวบรวมจากวิธีปฏิบัติที่ผ่านกระบวนการคิดพิจารณาเพื่อให้เป็นแนวปฏิบัติที่ดี (Best Practice) ที่จะก่อให้เกิดประโยชน์สูงสุดต่อองค์กร มาตรฐาน COBIT จัดแบ่งแนวทางปฏิบัติเป็นกระบวนการ รวมทั้งได้กำหนดวัตถุประสงค์ของการควบคุมหลักของแต่ละกระบวนการด้วย โดยแบ่งออกเป็น 4 กระบวนการ ดังนี้

1. การวางแผนและการจัดการองค์กร (PO : Planning and Organization)
2. การจัดหาและการติดตั้งใช้งาน (AI : Acquisition and Implementation)
3. การส่งมอบและการบริการ (DS : Delivery and Support)
4. การติดตามและการประเมินผล (ME : Monitor and Evaluate)

มาตรฐาน ITIL เป็นหลักการที่พัฒนาขึ้นด้วยความร่วมมือระหว่างภาครัฐบาลและภาคเอกชน ประเทศอังกฤษ ที่ตระหนักถึงคุณภาพของการให้บริการด้านเทคโนโลยีสารสนเทศ ซึ่งพบว่าปัญหาที่เกิดขึ้นในการให้บริการด้านเทคโนโลยีสารสนเทศไม่ได้เกิดจากระบบงานหรือบุคลากรที่ให้บริการ แต่เกิดจากกระบวนการทำงานที่ไม่เป็นระบบ หรือไม่มีระบบการจัดการที่ดีพอ จึงได้มีการกำหนดหลักการด้านการจัดการเทคโนโลยีสารสนเทศในองค์กรขึ้น เพื่อใช้เป็นแนวทางในการจัดการระบบการให้บริการด้านเทคโนโลยีสารสนเทศ ภายใต้การควบคุมและพัฒนาโดย OGC (United Kingdom’s Office of Government Commerce) มีวัตถุประสงค์เพื่อกำหนดแนวปฏิบัติที่ดีที่สุด (Best Practices) สำหรับกระบวนการของการส่งมอบงานและการให้บริการด้านเทคโนโลยีสารสนเทศ เพื่อให้เหมาะสมกับงานบริการ โดยที่เทคโนโลยีสารสนเทศต้องทำงานสอดคล้องกับการดำเนินงานทางธุรกิจ และสามารถสร้างคุณค่าจากการใช้เทคโนโลยีสารสนเทศได้ ซึ่งผู้บริหารต้องพิจารณาถึงความคุ้มค่าจากการลงทุนด้านเทคโนโลยีสารสนเทศที่มีค่าใช้จ่ายค่อนข้างสูงมากในปัจจุบัน โดยแบ่งแนวทางในการปฏิบัติออกเป็น 5 กลุ่ม คือ ยุทธศาสตร์งานบริการ (Service Strategy) การออกแบบงานบริการ (Service Design) การส่งมอบงานบริการ (Service Transition) การปฏิบัติงานบริการ (Service Operation) การปรับปรุงงานบริการอย่างต่อเนื่อง (Continual Service Improvement)

ITIL เป็นแนวทางในการจัดการระบบเทคโนโลยีสารสนเทศและที่สามารถนำไปปรับใช้กับองค์กร ซึ่งจะก่อให้เกิดประโยชน์ต่อองค์กรหลายอย่าง เช่น เป็นการปรับปรุงการใช้งานทรัพยากรที่มีอยู่ได้คุ้มค่ามากขึ้น สร้างเสริมความสามารถในการแข่งขันกับคู่แข่งในตลาด ลดการทำงานซ้ำซ้อนหรืองานที่ไม่จำเป็นลงได้ ช่วยทำให้งานแต่ละโครงการดำเนินไปได้ตามที่วางแผนไว้ ปรับปรุงความสามารถใน

การให้บริการด้านเทคโนโลยีสารสนเทศแก่ลูกค้าให้ดีขึ้น มีการพัฒนาในส่วนของเวลาในการทำงาน สามารถหาต้นทุนของการให้บริการที่มีคุณภาพตามที่กำหนดได้ สามารถให้บริการที่มีคุณภาพแก่ลูกค้าได้ตามที่สัญญาไว้ การปรับปรุงในส่วนการใช้ประโยชน์ ความน่าเชื่อถือ และการรักษาความปลอดภัยในกรณีที่เกิดเหตุวิกฤติในส่วนของแผนเทคโนโลยีสารสนเทศ

มาตรฐานการสอบบัญชีในสภาพแวดล้อมของระบบสารสนเทศที่ใช้คอมพิวเตอร์

สภาพแวดล้อมของระบบสารสนเทศที่ใช้คอมพิวเตอร์เกิดขึ้นเมื่อมีการใช้คอมพิวเตอร์ไม่ว่าประเภทใดหรือขนาดใดในการประมวลผลข้อมูลทางการเงินซึ่งมีความสำคัญต่อการสอบบัญชี ทั้งนี้ไม่ว่าการประมวลผลนั้นจะดำเนินการโดยกิจการหรือมอบหมายให้บุคคลภายนอกดำเนินการ

การตรวจสอบระบบสารสนเทศที่ใช้คอมพิวเตอร์ หมายถึง การตรวจเพื่อแสดงความเห็นต่อระบบการควบคุมสารสนเทศที่องค์กรใช้ว่าเหมาะสมและเป็นไปตามวัตถุประสงค์ของการควบคุมที่กำหนดไว้หรือไม่

มาตรฐานขั้นต่ำในการควบคุมภายในและการรักษาความปลอดภัยสำหรับสหกรณ์

มาตรฐานที่กำหนดในระเบียบนายทะเบียนสหกรณ์ ว่าด้วย “มาตรฐานขั้นต่ำในการควบคุมภายในและการรักษาความปลอดภัยสำหรับสหกรณ์และกลุ่มเกษตรกรที่ใช้โปรแกรมระบบบัญชีคอมพิวเตอร์ประมวลผลข้อมูล พ.ศ. 2553” เป็นการพัฒนามาจากหลักการของมาตรฐาน COBIT มาตรฐาน ITIL และมาตรฐานการสอบบัญชี โดยได้พิจารณานำมาพัฒนาใช้กับสหกรณ์เฉพาะเรื่องที่จำเป็นสำหรับสภาพการใช้เทคโนโลยีสารสนเทศของสหกรณ์ในปัจจุบัน

แนวปฏิบัติตามมาตรฐานขั้นต่ำในการควบคุมภายในและการรักษาความปลอดภัย

แนวปฏิบัติตามมาตรฐานขั้นต่ำในการควบคุมภายในและการรักษาความปลอดภัย ได้ออกแบบเพื่อใช้เป็นแนวทางสำหรับสหกรณ์ในการบริหารจัดการให้การนำเทคโนโลยีสารสนเทศมาใช้ในสหกรณ์มีการควบคุมและการรักษาความปลอดภัยในระดับที่เหมาะสม โดยในแต่ละข้อได้กำหนดโครงสร้างของมาตรฐานไว้ ดังนี้

1. ข้อกำหนดตามมาตรฐานที่นายทะเบียนสหกรณ์กำหนดไว้ในระเบียบ
2. แนวปฏิบัติ ซึ่งเป็นกิจกรรมด้านเทคโนโลยีสารสนเทศที่จะต้องดำเนินการเพื่อให้บรรลุวัตถุประสงค์ของมาตรฐานแต่ละข้อ

3. การประเมินระดับการควบคุมภายในและการรักษาความปลอดภัยของสหกรณ์ต้นแบบ (Maturity Model) เพื่อทำให้คณะกรรมการดำเนินการทราบว่าการบริหารจัดการด้านเทคโนโลยีสารสนเทศของสหกรณ์ในปัจจุบันอยู่ในระดับใด เพื่อจะได้กำหนดเป้าหมายที่ต้องการได้ โดยกำหนดไว้ 6 ระดับ ได้แก่

3.1 ระดับ 0 Non - existent	ไม่มีกระบวนการควบคุม
3.2 ระดับ 1 Initial	มีกระบวนการควบคุมกำหนดเฉพาะที่ต้องการ (ad-hoc) ซึ่งไม่เป็นระบบ
3.3 ระดับ 2 Repeatable	มีกระบวนการควบคุมให้ปฏิบัติตามอย่างเป็นระบบ
3.4 ระดับ 3 Defined	มีกระบวนการควบคุมเป็นเอกสารและสื่อสารในทราบทั่วกัน
3.5 ระดับ 4 Managed	มีกระบวนการควบคุม ติดตามและวัดผลการปฏิบัติ
3.6 ระดับ 5 Optimized	กำหนดวิธีการปฏิบัติที่ดีให้สามารถปฏิบัติตามและมีเครื่องมือช่วยในดำเนินงานได้อย่างมีประสิทธิภาพสูง

ปัญหาที่พบจากการปฏิบัติตามมาตรฐานขั้นต่ำในการควบคุมภายในและการรักษาความปลอดภัย

นับจากที่นายทะเบียนสหกรณ์ได้ประกาศใช้และเริ่มให้ถือปฏิบัติมาตรฐานขั้นต่ำในการควบคุมภายในและการรักษาความปลอดภัยตั้งแต่วันที่ 1 มกราคม 2554 เป็นต้นมา มีประเด็นปัญหาที่ควรนำมาพิจารณา ดังนี้

1. ความรู้และความเข้าใจ

1.1 การขาดความตระหนัก

แม้ว่าแต่ละองค์กรที่เกี่ยวข้องจะพยายามเผยแพร่และนำมาตรการรักษาความปลอดภัยและระบบการควบคุมภายในด้านเทคโนโลยีมาบังคับใช้ เช่นกรณีที่สำนักงานคณะกรรมการพัฒนาระบบราชการ (กพร.) ได้มีการกำหนดประเมินคุณภาพการบริหารจัดการด้านเทคโนโลยีสารสนเทศของหน่วยงานราชการโดยได้นำมาตรการการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศมาใช้เป็นตัวชี้วัดก็ตาม แต่ในภาพรวมของสังคมไทยยังขาดความตระหนักในเรื่องความเสี่ยงและการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ จึงพบว่าการลดความเสี่ยงด้านเทคโนโลยีสารสนเทศโดยการนำมาตรการรักษาความปลอดภัยและระบบการควบคุมภายในด้านเทคโนโลยีสารสนเทศมาใช้ในองค์กร ไม่ได้อยู่ในจิตสำนึกของผู้บริหารและผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศอย่างแท้จริง ไม่มีการปฏิบัติโดยเคร่งครัดอย่างสม่ำเสมอ จึงมีการปฏิบัติเฉพาะเมื่อมีการประเมินตัวชี้วัดเท่านั้น

ในการใช้เทคโนโลยีสารสนเทศในขบวนการสหกรณ์ในปัจจุบัน อยู่ในช่วงของความรุ่งเรือง กล่าวคือทุกสหกรณ์เห็นความสำคัญและมีความต้องการนำมาใช้ในการเพิ่มประสิทธิภาพในการให้บริการแก่สมาชิกโดยใช้เทคโนโลยีสารสนเทศเป็นเครื่องมือ จึงยังอยู่ในช่วงที่เห็นเทคโนโลยีสารสนเทศในมุมมองที่ดี คือมีความรวดเร็ว ทันสมัย ลดเวลาและค่าใช้จ่าย ในมุมกลับกันแม้ว่าจะมีบางสหกรณ์ที่ประสบปัญหาที่เกิดจากการทุจริตในระบบเทคโนโลยีสารสนเทศบ้างแล้ว แต่ยังมิได้เข้าใจอย่างแท้จริงว่าที่มาของปัญหาคือการขาดมาตรการรักษาความปลอดภัยและระบบการควบคุมภายในที่ดี จึงปรากฏว่าในขบวนการสหกรณ์ยังไม่ตระหนักถึงความเสี่ยงจากการใช้ระบบเทคโนโลยีสารสนเทศ และไม่เห็นความจำเป็นในการจัดให้มีมาตรการรักษาความปลอดภัยและระบบการควบคุมภายในด้านเทคโนโลยีสารสนเทศ

1.2 ความยากในการทำความเข้าใจ

โดยที่เนื้อหาของมาตรการรักษาความปลอดภัยและระบบการควบคุมภายในสำหรับองค์กรเป็นเรื่องที่ต้องใช้เวลาและความพยายามในการทำความเข้าใจ จึงมีเฉพาะผู้ที่ศึกษาด้านนี้โดยเฉพาะเท่านั้นที่มีความเข้าใจ และในกรณีของมาตรการรักษาความปลอดภัยและระบบการควบคุมภายในด้านเทคโนโลยีสารสนเทศ ที่จะต้องมีความรู้พื้นฐานด้านระบบเทคโนโลยีสารสนเทศประกอบด้วยจึงจะสามารถเข้าใจเรื่องมาตรการรักษาความปลอดภัยและระบบการควบคุมภายในด้านเทคโนโลยีสารสนเทศได้ ดังนั้น ในการศึกษาและทำความเข้าใจในเรื่องนี้จึงเป็นเรื่องที่ยากยิ่งขึ้นไป

1.3 กลไกในการถ่ายโอนองค์ความรู้

ดังที่กล่าวมาแล้วในเบื้องต้น องค์ความรู้ด้านมาตรการรักษาความปลอดภัยและระบบการควบคุมภายในด้านเทคโนโลยีสารสนเทศเป็นองค์ความรู้เฉพาะด้าน การที่จะนำไปปฏิบัติให้ บังเกิดผลได้นั้น จำเป็นต้องมีวิธีการในการถ่ายโอนองค์ความรู้ที่มีประสิทธิภาพ กรมตรวจบัญชีสหกรณ์มีการจัดซักซ้อมผู้สอบบัญชี คณะกรรมการและพนักงานของสหกรณ์ ในปี 2554 มีการฝึกอบรมผู้สอบบัญชีและผู้ช่วยผู้สอบบัญชีเพื่อให้รู้และเข้าใจเนื้อหาของมาตรฐานขั้นต่ำในการควบคุมภายในอย่างเพียงพอที่จะสามารถให้คำแนะนำแก่สหกรณ์และประเมินการควบคุมภายในด้านเทคโนโลยีสารสนเทศได้ อย่างไรก็ตาม การอบรมเป็นวิธีการถ่ายโอนองค์ความรู้ได้ในระดับรู้และเข้าใจ แต่ไม่อาจมั่นใจได้ว่าจะสามารถปฏิบัติได้ นอกจากนี้ยังไม่มีแผนกลยุทธ์ใดที่ดำเนินการนอกจากการฝึกอบรมประกอบกับจัดฝึกอบรมในเรื่องนี้มิได้ดำเนินการอย่างต่อเนื่องจึงทำให้ยังคงมีปัญหาในเรื่องความรู้และเข้าใจอยู่

2. ต้นทุนในการปฏิบัติตามมาตรฐาน

การจัดให้มีระบบการรักษาความปลอดภัยและระบบการควบคุมภายในด้านเทคโนโลยีสารสนเทศนั้นจะต้องมีต้นทุนเกิดขึ้น โดยเฉพาะในสหกรณ์ที่ไม่เคยจัดให้มีระบบการควบคุมมาก่อนก็จะพบว่าสหกรณ์ต้องมีค่าใช้จ่ายในการจัดการ เช่น ในการจัดให้มีระบบการรักษาความปลอดภัยทางกายภาพ จะต้องมีการจัดหาเครื่องสำรองไฟ เครื่องดับเพลิง จัดสถานที่สำหรับเครื่องคอมพิวเตอร์ที่สำคัญ เป็นต้น และในมาตรฐานการควบคุมภายในบางข้อมีข้อกำหนดที่สหกรณ์ปฏิบัติได้ยาก เช่น กรณีมาตรฐานข้อ 5 การกำหนดให้มีเอกสารประกอบระบบสารสนเทศ เช่น การที่ต้องมีเอกสารแสดงโครงสร้างของข้อมูล ซึ่งสหกรณ์ที่จ้างพัฒนาระบบไม่ได้มีการทำสัญญาไว้ในเมื่อจ้างพัฒนา การที่จะให้ผู้พัฒนาระบบจัดทำให้นั้น สหกรณ์จะต้องจ่ายค่าเอกสารในราคาสูงซึ่งสหกรณ์พิจารณาว่าเกินกว่าผลประโยชน์ที่จะได้รับ จึงทำให้สหกรณ์ยอมรับความเสี่ยงโดยไม่มีการจัดให้มีตามมาตรฐานกำหนด

3. มาตรการบังคับใช้เพื่อให้มีการปฏิบัติตามมาตรฐาน

มาตรฐานขั้นต่ำในการควบคุมภายในและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศกำหนดถือใช้ในรูปแบบของระเบียบนายทะเบียนสหกรณ์ ซึ่งไม่มีบทลงโทษสำหรับสหกรณ์ที่ไม่ปฏิบัติตาม ในขณะที่การกำหนดระบบการกำกับดูแลโดยกรมตรวจบัญชีสหกรณ์ได้กำหนดให้ผู้สอบบัญชีต้องเข้าตรวจประเมินการจัดระบบการควบคุมภายในตามที่กำหนดไว้ในระเบียบปีละ 1 ครั้ง โดยไม่มีมาตรการอื่นรองรับ สำหรับกรณีที่สหกรณ์ไม่มีการจัดให้มีระบบการควบคุมภายในที่รัดกุมเพียงพอ รวมทั้งมิได้กำหนดหน่วยงานที่รับผิดชอบในการขับเคลื่อนเพื่อให้เกิดการปฏิบัติอย่างจริงจัง จึงไม่อาจจะมั่นใจได้ว่าระเบียบนายทะเบียนสหกรณ์นี้จะสามารถช่วยลดความเสี่ยงอันเกิดจากการใช้เทคโนโลยีสารสนเทศของขบวนการสหกรณ์ตามเจตนารมณ์ของการกำหนดให้มีระเบียบนี้ขึ้นมากน้อยเพียงใด

ข้อเสนอแนะ

เพื่อให้มาตรฐานในการควบคุมภายในและการรักษาความปลอดภัยที่นายทะเบียนสหกรณ์กำหนดขึ้นได้มีการนำมาปฏิบัติให้บังเกิดผลตามเจตนารมณ์ นั่นคือ การที่สหกรณ์จะสามารถบริหารจัดการจนสามารถควบคุมความเสี่ยง ที่เกิดจากการใช้เทคโนโลยีสารสนเทศของสหกรณ์ไม่ให้เกิดความผิดพลาดจนนำความเสียหายมาสู่สหกรณ์ได้ กรมตรวจบัญชีสหกรณ์และสหกรณ์ ควรดำเนินการดังต่อไปนี้

1. สร้างความตระหนักในเรื่องการรักษาความปลอดภัยและการควบคุมภายในด้านเทคโนโลยีสารสนเทศแก่สหกรณ์และผู้ที่เกี่ยวข้อง

กลไกในการขับเคลื่อนการปฏิบัติตามมาตรฐานการควบคุมภายในที่สำคัญคือ การสร้างความตระหนักให้เกิดขึ้นกับสหกรณ์ที่มีการใช้ระบบเทคโนโลยีสารสนเทศและผู้ที่เกี่ยวข้อง กรมตรวจบัญชีสหกรณ์ในฐานะหน่วยงานผู้รับผิดชอบในการออกระเบียบควรดำเนินการสร้างความตระหนักให้เกิดขึ้นในทุกระดับ ตั้งแต่บุคลากรของกรมตรวจบัญชีสหกรณ์โดยเฉพาะผู้สอบบัญชี ผู้ช่วยผู้สอบบัญชี บุคลากรของสหกรณ์ ตั้งแต่คณะกรรมการดำเนินการ ฝ่ายจัดการ และพนักงานของสหกรณ์ เนื่องจากความตระหนักเป็นรากฐานของความรู้และความเข้าใจ หากได้สร้างความตระหนักให้เกิดขึ้นแก่บุคคลที่เกี่ยวข้องแล้วและเกิดความตระหนักในความจำเป็นของระบบการควบคุมภายในแล้ว การที่กรมตรวจบัญชีสหกรณ์จะช่วยสนับสนุนและผลักดันให้เกิดการปฏิบัติได้เป็นอย่างดี การสร้างความตระหนักควรเกิดขึ้นในกลุ่มบุคคลที่เป็นผู้สอบบัญชีและผู้ช่วยผู้สอบบัญชีเป็นประการแรก เนื่องจากบุคคลเหล่านี้มีบทบาทในการตรวจประเมินระบบการควบคุมภายใน รวมทั้งบทบาทในการให้คำแนะนำแก่สหกรณ์ การสร้างความตระหนักจะสามารถแก้ปัญหาเรื่องการที่สหกรณ์เห็นว่าการจัดให้มีระบบการควบคุมภายในทำให้เกิดต้นทุนเพิ่มขึ้นแต่สหกรณ์จะสามารถประเมินผลประโยชน์ที่จะได้รับกับต้นทุนที่ต้องจ่ายได้อย่างเหมาะสม

2. ดำเนินการถ่ายโอนองค์ความรู้อย่างเป็นระบบและต่อเนื่อง

การที่สหกรณ์จะสามารถนำมาตรฐานการควบคุมภายในไปปฏิบัติได้นั้น จะต้องมีความรู้ความเข้าใจอย่างถ่องแท้ในหลักการรักษาความปลอดภัยและระบบการควบคุมภายในด้านเทคโนโลยีสารสนเทศอย่างเพียงพอ กรมตรวจบัญชีสหกรณ์ควรจัดให้มีกระบวนการถ่ายโอนความรู้อย่างครบทุกมิติทั้งการอบรมเพื่อทำความเข้าใจมาตรฐานการควบคุมแต่ละข้อ การฝึกปฏิบัติการพัฒนาวิธีการควบคุมภายในของแต่ละสหกรณ์ให้สอดคล้องกับสภาพแวดล้อมของสหกรณ์ กระบวนการถ่ายโอนความรู้นี้จะต้องมีการกำหนดเป้าหมายเป็นรายสหกรณ์ภายในระยะเวลาที่กำหนด โดยมีการกำหนดตัวชี้วัดที่ชัดเจน

3. ส่งเสริมและมีระบบในการนำแนวปฏิบัติตามมาตรฐานขั้นต่ำในการควบคุมภายในและการรักษาความปลอดภัยออกใช้

แนวปฏิบัติตามมาตรฐานขั้นต่ำในการควบคุมภายในและการรักษาความปลอดภัยที่พัฒนาขึ้นนี้ มีเจตนารมณ์ที่ทำให้มาตรฐานที่กำหนดไว้ในระเบียบเป็นสิ่งที่สามารถทำความเข้าใจได้ง่ายขึ้น รวมถึงเป็นต้นแบบให้สหกรณ์นำไปปรับใช้กับสภาพแวดล้อมของแต่ละสหกรณ์ได้ง่ายขึ้น

จึงเป็นเครื่องมือสำคัญในการช่วยให้สหกรณ์สามารถกำหนดวิธีการควบคุมภายในได้อย่างเหมาะสม อย่างไรก็ตาม การที่จะบังเกิดผลนั้นจำเป็นต้องมีระบบในการขับเคลื่อนแนวปฏิบัติให้ถึงสหกรณ์จนกลายเป็นวิธีการควบคุมภายในที่สหกรณ์ประกาศใช้ กรมตรวจบัญชีสหกรณ์ควรนำแนวปฏิบัตินี้ไปขยายผลโดยส่งเสริมให้ผู้สอบบัญชีได้นำแนวปฏิบัตินี้ไปแนะนำให้สหกรณ์ถือใช้ให้บังเกิดผล

4. กำหนดมาตรการบังคับใช้

แม้ว่าระเบียบนายทะเบียนสหกรณ์จะไม่มีโทษจากการไม่ปฏิบัติตาม แต่กรมตรวจบัญชีสหกรณ์ก็สามารถที่นำมาเป็นผลบังคับใช้ได้โดยผ่านกระบวนการสอบบัญชีโดยการนำประเด็นการควบคุมภายในด้านเทคโนโลยีสารสนเทศมาเป็นประเด็นประเมินความเสี่ยงในการสอบบัญชี รวมถึงการนำมาเป็นประเด็นในการจัดชั้นคุณภาพการควบคุมภายในของสหกรณ์ เนื่องจากในปัจจุบันมีหลายหน่วยงานนำผลการจัดชั้นคุณภาพการควบคุมภายในโดยผู้สอบบัญชีไปใช้ในการพิจารณา ทั้งการให้สินเชื่อหรือการจัดระดับของสหกรณ์ หากเป็นเช่นนี้ก็จะเป็นผลบังคับให้สหกรณ์ต้องมีการจัดระบบการควบคุมภายในที่ดีและเหมาะสมมากขึ้น

5. สหกรณ์ควรมีแผนดำเนินการพัฒนาระบบการควบคุมภายใน

ผู้บริหารขององค์กรมีหน้าที่จัดให้มีระบบการควบคุมภายในที่เหมาะสมกับกิจการ สหกรณ์เป็นองค์กรที่ได้รับการสนับสนุนจากรัฐ แม้แต่เรื่องของการจัดระบบการควบคุมภายในที่รัฐพิจารณาแล้วว่ามีความจำเป็นที่จะต้องจัดให้มีแต่สหกรณ์อาจจะไม่สามารถพัฒนาวิธีการขึ้นได้เองจึงได้กำหนดเป็นมาตรฐานและจัดทำแนวปฏิบัติ ทั้งนี้ ก็เพื่อที่จะอำนวยความสะดวกให้สหกรณ์กำหนดวิธีการควบคุมภายในได้ง่ายขึ้น ดังนั้น สหกรณ์ควรที่จะมีแผนดำเนินการในการจัดให้มีระบบการควบคุมที่เหมาะสมโดยการกำหนดเป้าหมายและเวลาที่จะจัดให้มีระบบการควบคุมภายในตามมาตรฐานแต่ละข้อ ซึ่งอาจจะไม่จำเป็นต้องจัดทำให้ได้พร้อมกันครบทุกข้อ แต่อาจจะเรียงลำดับความสำคัญแล้วดำเนินการนำแนวปฏิบัติมาปรับปรุงให้เหมาะสมกับสหกรณ์ ในการดำเนินการควรแต่งตั้งคณะทำงานขึ้นเป็นผู้ดำเนินการเนื่องจากการควบคุมภายในนั้นเกี่ยวข้องกับบุคคลหลายฝ่าย โดยคณะทำงานมีหน้าที่ในการศึกษามาตรฐาน และต้องทำการศึกษาลักษณะการใช้เทคโนโลยีสารสนเทศของสหกรณ์ไปพร้อม ๆ กันด้วย เพื่อกำหนดแนวปฏิบัติให้ชัดเจน เมื่อพัฒนาวิธีการควบคุมภายในได้แล้วควรทดลองใช้งานก่อนที่จะนำเสนอต่อคณะกรรมการดำเนินงานเพื่อถือใช้ต่อไป

บรรณานุกรม

บรรณานุกรม

กิตติ ภักดีวัฒนะกุล, *เทคโนโลยีสารสนเทศ*, เคทีพี แอนด์ คอนซัลท์, พิมพ์ครั้งที่ 3, 2553.

ณัฏฐพันธ์ เขจรนันทน์, ผศ.ดร., *การวิเคราะห์และออกแบบระบบสารสนเทศ*, วี. พริ้นท์ (1991), 2551.

จตุพร แพงจันทร์, *Master in Security 2nd Edition,* ไอดีซี พรีเมียร์, 2553.

ธีรวัฒน์ ประกอบผล, รศ., เอกพันธุ์ คำปัญโญ, *การวิเคราะห์และออกแบบระบบ System Analysis and Design,* ซัคเซส มีเดีย, พิมพ์ครั้งที่ 1, 2552.

นิตยา วงศ์ภินันท์วัฒนา, *ระบบสารสนเทศด้านการเงินและการบัญชีเพื่อการวางแผนทรัพยากรองค์กร,* สำนักพิมพ์ฟิสิกส์เซ็นเตอร์, พิมพ์ครั้งที่ 2, 2555.

พลพธู ปิยวรรณ, รศ., สุภาพร เชิงเอี่ยม, รศ.ดร., *ระบบสารสนเทศทางการบัญชี*, วิทยพัฒน์, พิมพ์ครั้งที่ 2, 2551.

วัชนีพร เศรษฐสักโก, รศ.ดร., *ระบบสารสนเทศทางการบัญชี*, เคทีพี แอนด์ คอนซัลท์, พิมพ์ครั้งที่ 7, 2551.

โอภาส เอี่ยมสิริวงศ์, *การวิเคราะห์และออกแบบระบบ (ฉบับปรับปรุงเพิ่มเติม)*, ซีเอ็ดยูเคชั่น, 2555.

อำไพ พรประเสริฐสกุล, ดร., *การวิเคราะห์และออกแบบระบบ*, ออฟเซท เพรส, พิมพ์ครั้งที่ 5, 2544.

ภาคผนวก ก.

ระเบียบนายทะเบียนสหกรณ์

ว่าด้วย มาตรฐานขั้นต่ำในการควบคุมภายในและ

การรักษาความปลอดภัย สำหรับสหกรณ์และกลุ่มเกษตร

ที่ใช้โปรแกรมระบบบัญชีคอมพิวเตอร์ประมวลผลข้อมูล

พ.ศ. 2553

ระเบียบนายทะเบียนสหกรณ์
ว่าด้วย มาตรฐานขั้นต่ำในการควบคุมภายในและการรักษาความปลอดภัย
สำหรับสหกรณ์และกลุ่มเกษตรกรที่ใช้โปรแกรมระบบบัญชีคอมพิวเตอร์ประมวลผลข้อมูล
พ.ศ. ๒๕๕๓

สืบเนื่องจากปัจจุบันสหกรณ์และกลุ่มเกษตรกรได้มีการนำระบบบัญชีคอมพิวเตอร์มาใช้ในการประมวลผลข้อมูลทางการบัญชีและจัดทำงบการเงิน ซึ่งอาจจะก่อให้เกิดความเสี่ยงและความเสียหายต่อข้อมูลที่สำคัญของสหกรณ์และกลุ่มเกษตรกรได้ หากมิได้มีการตระเตรียมมาตรการในการป้องกันความเสี่ยงระบบสารสนเทศไว้ล่วงหน้าอย่างมีประสิทธิภาพเพียงพอ สหกรณ์และกลุ่มเกษตรกรจึงควรมีการบริหารจัดการและการควบคุมงานด้านคอมพิวเตอร์อย่างมีระบบและประสิทธิภาพ รวมทั้งให้เหมาะสมตามสภาพแวดล้อมที่ได้เปลี่ยนแปลงไปในการประมวลผลข้อมูลด้วยคอมพิวเตอร์

ดังนั้น เพื่อให้สหกรณ์และกลุ่มเกษตรกรมีการปฏิบัติในการจัดทำบัญชีตามแบบและรายการที่นายทะเบียนสหกรณ์กำหนด และเพื่อประโยชน์ของสหกรณ์ในการเก็บรักษาบัญชีและเอกสารประกอบการลงบัญชี อาศัยอำนาจตามความในมาตรา ๑๖(๒) (๘) และ มาตรา ๖๕ แห่งพระราชบัญญัติสหกรณ์ พ.ศ. ๒๕๔๒ ประกอบกับคำสั่ง นายทะเบียนสหกรณ์ ที่ ๕๙๘/๒๕๕๒ ลงวันที่ ๒๑ กรกฎาคม ๒๕๕๒ เรื่อง มอบอำนาจหน้าที่ให้พนักงานเจ้าหน้าที่ปฏิบัติการแทนนายทะเบียนสหกรณ์ อธิบดีกรมตรวจบัญชีสหกรณ์ในฐานะพนักงานเจ้าหน้าที่ซึ่งได้รับมอบหมายการปฏิบัติการแทนนายทะเบียนสหกรณ์ จึงกำหนดระเบียบ ว่าด้วยมาตรฐานขั้นต่ำในการควบคุมภายในและการรักษาความปลอดภัยสำหรับสหกรณ์และกลุ่มเกษตรกรที่ใช้โปรแกรมระบบบัญชีคอมพิวเตอร์ประมวลผลข้อมูล พ.ศ. ๒๕๕๓ ไว้ดังนี้

ข้อ ๑. ระเบียบนี้ เรียกว่า “ ระเบียบนายทะเบียนสหกรณ์ ว่าด้วยมาตรฐานขั้นต่ำในการควบคุมภายในและการรักษาความปลอดภัยสำหรับสหกรณ์และกลุ่มเกษตรกรที่ใช้โปรแกรมระบบบัญชีคอมพิวเตอร์ประมวลผลข้อมูล พ.ศ. ๒๕๕๓ ”

ข้อ ๒. ระเบียบนี้ให้มีผลบังคับใช้ตั้งแต่วันถัดจากวันประกาศ เป็นต้นไป

ข้อ ๓. ให้ยกเลิกบรรดาระเบียบ คำสั่ง และคำแนะนำต่าง ๆ ในส่วนที่ได้กำหนดไว้แล้วในระเบียบนี้หรือซึ่งขัดหรือแย้งกับระเบียบนี้ ให้ใช้ระเบียบนี้แทน

ข้อ ๔. ให้อธิบดีกรมตรวจบัญชีสหกรณ์รักษาการตามระเบียบนี้ รวมทั้งวินิจฉัย ให้คำแนะนำหรือกำหนดวิธีปฏิบัติได้ตามความจำเป็น

ข้อ ๕. วิธีปฏิบัติสำหรับสหกรณ์และกลุ่มเกษตรกรที่ใช้โปรแกรมระบบบัญชีคอมพิวเตอร์ประมวลผลข้อมูลต้องจัดให้มีมาตรฐานขั้นต่ำในการควบคุมภายในและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ ดังนี้

๑. จัดให้มีนโยบายหรือระเบียบปฏิบัติในการควบคุมการปฏิบัติงานเกี่ยวกับการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของสหกรณ์และกลุ่มเกษตรกรที่เป็นลายลักษณ์อักษร

๒. จัดให้มีระบบการรักษาความปลอดภัยทางกายภาพที่เพียงพอแก่การป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่ที่เกี่ยวข้องเข้าถึงอุปกรณ์คอมพิวเตอร์ที่สำคัญ และจัดให้มีระบบป้องกันความเสียหายจากสภาวะแวดล้อมหรือภัยพิบัติต่างๆ ให้แก่อุปกรณ์คอมพิวเตอร์ที่สำคัญด้วย

๓. จัดให้มีระบบการรักษาความปลอดภัยของข้อมูลในระบบคอมพิวเตอร์และระบบเครือข่ายที่เพียงพอแก่การป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่ที่เกี่ยวข้องได้เข้าถึง ล่วงรู้ ใช้ประโยชน์ หรือแก้ไขเปลี่ยนแปลงข้อมูลหรือระบบดังกล่าวได้

๔. จัดให้มีมาตรการควบคุมการพัฒนาหรือแก้ไขเปลี่ยนแปลงที่เพียงพอ เพื่อให้ระบบบัญชีคอมพิวเตอร์ มีการประมวลผลที่ถูกต้องครบถ้วนและเป็นไปตามความต้องการของผู้ใช้งาน รวมทั้งต้องมีการสื่อสารหรือฝึกอบรมเกี่ยวกับระบบบัญชีคอมพิวเตอร์ให้ผู้เกี่ยวข้องได้รับทราบอย่างทั่วถึงเพื่อให้สามารถใช้งานได้อย่างถูกต้อง

๕. จัดให้มีและควบคุมดูแลเอกสารสนับสนุนการปฏิบัติงานสำหรับระบบบัญชีคอมพิวเตอร์ โดยมีรายละเอียด ดังนี้

๕.๑ เอกสารสนับสนุนการปฏิบัติงาน

๕.๑.๑ เอกสารด้านฐานข้อมูลของระบบบัญชีคอมพิวเตอร์ เป็นเอกสารแสดงรายละเอียดการจัดเก็บข้อมูลที่เป็นสาระสำคัญทางบัญชี ทั้งนี้ เพื่อให้สหกรณ์และกลุ่มเกษตรกรสามารถเข้าใจถึงโครงสร้างการจัดเก็บข้อมูลของระบบบัญชีคอมพิวเตอร์ที่ใช้งานอยู่และใช้อ้างอิงเพื่อแก้ไขปัญหาได้ โดยเอกสารด้านฐานข้อมูลของระบบบัญชีคอมพิวเตอร์ที่จำเป็นจะต้องมีคือ โครงสร้างฐานข้อมูล (Data Structure) หรือพจนานุกรมข้อมูล (Data Dictionary) หรือตารางแสดงรายละเอียดของข้อมูลตามแบบที่กรมตรวจบัญชีสหกรณ์กำหนด **(เอกสารแนบท้าย)**

๕.๑.๒ คู่มือการใช้ระบบบัญชีคอมพิวเตอร์ เพื่อเป็นเอกสารประกอบการทำงานของผู้ใช้งานในการบันทึกข้อมูล ประมวลผลข้อมูลและออกรายงานได้อย่างถูกต้อง

๕.๒ การควบคุมดูแลเอกสารสนับสนุนการปฏิบัติงาน โดยจัดให้มีสถานที่เก็บ และปรับปรุงเอกสารให้ถูกต้องและทันสมัยอยู่เสมอ

๖. จะต้องสามารถเข้าถึงฐานข้อมูลของระบบบัญชีคอมพิวเตอร์ได้ และสามารถนำข้อมูลออกจากฐานข้อมูลในรูปแบบที่อ่านเข้าใจได้

๗. จัดให้มีการสำรองข้อมูลของระบบบัญชีคอมพิวเตอร์เพื่อให้สามารถรองรับการประกอบธุรกิจได้อย่างต่อเนื่อง มีประสิทธิภาพและทันเหตุการณ์ ตลอดจนจัดให้มีการดูแลรักษาข้อมูลชุดสำรองให้มีความปลอดภัย รวมทั้งจัดให้มีการป้องกันมิให้มีการนำข้อมูลชุดสำรองมาใช้อย่างไม่ถูกต้อง

๘. ในกรณีที่มีการใช้บริการงานเทคโนโลยีสารสนเทศจากผู้ให้บริการซึ่งเป็นบุคคลภายนอก ต้องจัดให้มีหลักเกณฑ์ในการคัดเลือกและพิจารณาความเหมาะสมของผู้ให้บริการ รวมทั้งต้องควบคุมและตรวจสอบการปฏิบัติงานของผู้ให้บริการอย่างเข้มงวด เพื่อให้มั่นใจว่า ผู้ให้บริการสามารถปฏิบัติตามระเบียบนี้ได้

๙. จัดให้มีการตรวจสอบคอมพิวเตอร์โดยหน่วยงานภายในของสหกรณ์และกลุ่มเกษตรกรเอง หรือโดยผู้ตรวจสอบที่เป็นบุคคลภายนอก เพื่อทำหน้าที่ตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศทุกประเภทที่อาจเกิดขึ้นได้

ประกาศ ณ วันที่ ๑๗ ธันวาคม พ.ศ. ๒๕๕๓

สิงห์ทอง ชินวรรังสี
(นายสิงห์ทอง ชินวรรังสี)
อธิบดีกรมตรวจบัญชีสหกรณ์
พนักงานเจ้าหน้าที่ ปฏิบัติการแทน
นายทะเบียนสหกรณ์

เอกสารแนบท้าย

ตารางแสดงรายละเอียดของข้อมูลตามแบบที่กรมตรวจบัญชีสหกรณ์กำหนด

๑. รายละเอียดของข้อมูลสมาชิก

ลำดับที่	รายการข้อมูล	Field ที่เก็บข้อมูล	Table ที่เก็บข้อมูล	หมายเหตุ
๑.	รหัสสมาชิก			
๒.	คำนำหน้า			
๓.	ชื่อสมาชิก			
๔.	นามสกุล			
๕.	เพศ			
๖.	ประเภทสมาชิก			
๗.	ที่อยู่			
๘.	อำเภอ			
๙.	จังหวัด			
๑๐.	รหัสไปรษณีย์			
๑๑.	เบอร์โทรศัพท์			
๑๒.	เบอร์โทรสาร			
๑๓.	เลขที่บัตรประชาชนหรือ เลขที่จดทะเบียนนิติบุคคล			
๑๔.	วันที่อนุมัติให้เป็นสมาชิก			
๑๕.	อนุมัติรายการโดย			
๑๖.	ผู้บันทึกรายการ			
๑๗.	วันที่บันทึกรายการ			
๑๘.	สถานะของสมาชิก			
๑๙.	จำนวนส่งค่าหุ้นต่อเดือน			
๒๐.	มูลค่าหุ้นคงเหลือล่าสุด			

๒. รายละเอียดของทะเบียนหุ้น

ลำดับที่	รายการข้อมูล	Field ที่เก็บข้อมูล	Table ที่เก็บข้อมูล	หมายเหตุ
๑.	รหัสสมาชิก			
๒.	ชื่อ สกุลสมาชิก			
๓.	ประเภทหุ้น			
๔.	ประเภทรายการเคลื่อนไหว			
๕.	จำนวนเงินที่ทำรายการ			
๖.	วันที่ทำรายการ			
๗.	เลขที่อ้างอิงเอกสารการทำรายการ			
๘.	มูลค่าหุ้นคงเหลือ			
๙.	วันที่ปรับปรุงข้อมูลล่าสุด			
๑๐.	สถานะของรายการ			
๑๑.	ผู้บันทึกรายการ			

๓. รายละเอียดของข้อมูลบัญชีเงินฝาก

ลำดับที่	รายการข้อมูล	Field ที่เก็บข้อมูล	Table ที่เก็บข้อมูล	หมายเหตุ
๑.	เลขที่บัญชี			
๒.	ประเภทบัญชีเงินฝาก			
๓.	ชื่อบัญชีเงินฝาก			
๔.	ที่อยู่ในการจัดส่งเอกสาร			
๕.	วันที่เปิดบัญชี			
๖.	จำนวนเงินที่เปิดบัญชี			
๗.	วันที่ยกยอดล่าสุด			
๘.	ยอดเงินต้นยกมา			
๙.	ยอดดอกเบี้ยค้างจ่ายยกมา			
๑๐.	ยอดเงินฝากคงเหลือล่าสุด			
๑๑.	วันที่ปรับปรุงรายการล่าสุด			
๑๒.	ยอดดอกเบี้ยค้างจ่าย			
๑๓.	ยอดดอกเบี้ยจ่าย			
๑๔.	จำนวนเงินที่ติดการค้ำประกัน			
๑๕.	ยอดดอกเบี้ยจ่ายสะสม			
๑๖.	สถานะบัญชี			
๑๗.	วันที่บันทึกรายการ			
๑๘.	ผู้บันทึกรายการ			

๔. รายละเอียดของข้อมูลรายการเคลื่อนไหวบัญชีเงินฝาก

ลำดับที่	รายการข้อมูล	Field ที่เก็บข้อมูล	Table ที่เก็บข้อมูล	หมายเหตุ
๑.	ลำดับที่รายการฝากถอน			
๒.	เลขที่บัญชี			
๓.	ประเภทบัญชีเงินฝาก			
๔.	รหัสการทำรายการ			
๕.	วันที่ทำรายการ			
๖.	ประเภทรับเงิน			
๗.	เลขที่เช็ค			
๘.	วันที่ลงในเช็ค			
๙.	ชื่อธนาคารผู้จ่ายเงิน			
๑๐.	สาขาของธนาคาร			
๑๑.	จำนวนเงินที่ทำรายการ			
๑๒.	เวลาที่ทำรายการ			
๑๓.	ยอดเงินต้น			
๑๔.	ยอดดอกเบี้ย			
๑๕.	ยอดค่าธรรมเนียม			
๑๖.	รหัสพนักงานทำรายการ			
๑๗.	รหัสพนักงานอนุมัติรายการ			

๕. รายละเอียดของข้อมูลสัญญาเงินกู้

ลำดับที่	รายการข้อมูล	Field ที่เก็บข้อมูล	Table ที่เก็บข้อมูล	หมายเหตุ
๑.	เลขที่สัญญาเงินกู้			
๒.	ประเภทบัญชีเงินกู้			
๓.	รหัสสมาชิก			
๔.	ชื่อผู้กู้			
๕.	ที่อยู่ในการจัดส่งเอกสาร			
๖.	ระยะเวลากู้เงิน			
๗.	วันที่อนุมัติเงินกู้			
๘.	วงเงินที่อนุมัติ			
๙.	วัตถุประสงค์ในการกู้			
๑๐.	ประเภทการค้ำประกัน			
๑๑.	มูลค่าหลักประกัน			
๑๒.	เงินต้นคงเหลือล่าสุด			
๑๓.	ดอกเบี้ยคงเหลือล่าสุด			
๑๔.	ค่าธรรมเนียมคงเหลือล่าสุด			
๑๕.	วันที่ทำรายการ			
๑๖.	ผู้บันทึกรายการ			

๖. รายละเอียดข้อมูลรายการเคลื่อนไหวเงินกู้

ลำดับที่	รายการข้อมูล	Field ที่เก็บข้อมูล	Table ที่เก็บข้อมูล	หมายเหตุ
๑.	เลขที่สัญญาเงินกู้			
๒.	ประเภทบัญชีเงินกู้			
๓.	วันที่ทำรายการ			
๔.	รหัสการทำรายการ			
๕.	เลขที่อ้างอิงรายการ			
๖.	จำนวนเงินที่ทำรายการ			
๗.	วันที่สิ้นสุดคำนวณดอกเบี้ย			
๘.	สถานะการปรับปรุง			
๙.	วันที่ทำรายการ			
๑๐.	ผู้บันทึกรายการ			

๗. รายละเอียดข้อมูลดอกเบี้ย

ลำดับที่	รายการข้อมูล	Field ที่เก็บข้อมูล	Table ที่เก็บข้อมูล	หมายเหตุ
๑.	ประเภทรายการดอกเบี้ย (เงินกู้หรือเงินฝาก)			
๒.	ชื่อดอกเบี้ย			
๓.	รหัสบัญชี			
๔.	อัตราดอกเบี้ย			
๕.	อัตราดอกเบี้ยสูงสุด			
๖.	จำนวนเดือนที่ทบต้น			
๗.	ยอดคงเหลือขั้นต่ำ			
๘.	สถานะบัญชี			
๙.	วันทีมีผลบังคับใช้			
๑๐.	วันที่ปรับปรุงรายการล่าสุด			
๑๑.	สถานะการใช้งาน			
๑๒.	ผู้บันทึกรายการ			
๑๓.	วันที่บันทึกรายการ			

๘. รายละเอียดข้อมูลการขายสินค้า

ลำดับที่	รายการข้อมูล	Field ที่เก็บข้อมูล	Table ที่เก็บข้อมูล	หมายเหตุ
๑.	เลขที่ใบสั่งขาย			
๒.	ประเภทสินค้า			
๓.	ชื่อสินค้า			
๔.	กลุ่มสินค้า(รหัสธุรกิจ/โครงการ)			
๕.	รหัสสินค้า			
๖.	ประเภทการขาย			
๗.	อ้างอิงเลขที่ใบเสร็จรับเงินหรือใบกำกับสินค้า			
๘.	วันที่ทำรายการ			
๙.	รหัสลูกค้าหรือรหัสสมาชิก			
๑๐.	ราคาขายมาตรฐาน			
๑๑.	ส่วนลดเงินสด			
๑๒.	ปริมาณสินค้า			
๑๓.	สถานะการขาย			
๑๔.	ภาษีมูลค่าเพิ่ม			

๙. รายละเอียดข้อมูลลูกหนี้

ลำดับที่	รายการข้อมูล	Field ที่เก็บข้อมูล	Table ที่เก็บข้อมูล	หมายเหตุ
๑.	คำนำหน้า			
๒.	รหัสลูกหนี้			
๓.	ชื่อลูกหนี้			
๔.	นามสกุล			
๕.	เพศ			
๖.	ที่อยู่			
๗.	อำเภอ			
๘.	จังหวัด			
๙.	รหัสไปรษณีย์			
๑๐.	เบอร์โทรศัพท์			
๑๑.	เบอร์โทรสาร			
๑๒.	เลขที่บัตรประชาชนหรือเลขที่จดทะเบียนนิติบุคคล			
๑๓.	ประเภทลูกหนี้			
๑๔.	ผู้บันทึกรายการ			

ลำดับที่	รายการข้อมูล	Field ที่เก็บข้อมูล	Table ที่เก็บข้อมูล	หมายเหตุ
๑๕.	วันที่บันทึกรายการ			
๑๖.	สถานะของลูกหนี้			
๑๗.	วงเงินขายเชื่อ			
๑๘.	วันที่อนุมัติวงเงิน			
๑๙.	วันที่ปรับปรุงล่าสุด			
๒๐.	ระยะเวลาการชำระเงิน (Payment Term)			
๒๑.	ยอดลูกหนี้คงเหลือล่าสุด			

๑๐. รายละเอียดข้อมูลการรับชำระเงิน

ลำดับที่	รายการข้อมูล	Field ที่เก็บข้อมูล	Table ที่เก็บข้อมูล	หมายเหตุ
๑.	เลขที่รายการรับชำระเงิน (ใบเสร็จ)			
๒.	อ้างอิงเลขที่ใบกำกับสินค้า			
๓.	วันที่เกิดรายการ			
๔.	รหัสลูกค้าหรือรหัสสมาชิก			
๕.	จำนวนเงินที่ทำรายการ			
๖.	จำนวนเงินค่าปรับ			
๗.	หนี้คงเหลือ			
๘.	จำนวนเงินส่วนลดจ่าย			
๙.	ประเภทลูกค้า			
๑๐.	สถานะลูกหนี้			
๑๑.	เหตุผลการยกเลิก			
๑๒.	สถานะของการรับชำระเงิน			
๑๓.	วันที่ยกเลิก			
๑๔.	วันที่ทำรายการ			
๑๕.	ผู้บันทึกรายการ			

๑๑. รายละเอียดข้อมูลการซื้อสินค้า

ลำดับที่	รายการข้อมูล	Field ที่เก็บข้อมูล	Table ที่เก็บข้อมูล	หมายเหตุ
๑.	ชื่อสินค้า			
๒.	เลขที่ใบสั่งซื้อ			
๓.	วันที่ทำรายการ			
๔.	ประเภทซื้อ			
๕.	รหัสเจ้าหนี้			
๖.	รหัสสินค้า			
๗.	ราคาซื้อต่อหน่วย			
๘.	ปริมาณสินค้า			
๙.	มูลค่าซื้อรวม			
๑๐.	อัตราภาษีมูลค่าเพิ่ม			
๑๑.	ภาษีมูลค่าเพิ่ม			
๑๒.	ส่วนลด			
๑๓.	มูลค่าซื้อสุทธิ			
๑๔.	อ้างอิงเลขที่ใบรับสินค้า			
๑๕.	ค่าใช้จ่ายในการซื้อ			
๑๖.	สถานะยกเลิกรายการซื้อสินค้า			
๑๗.	เหตุผลการยกเลิก			
๑๘.	วันที่ยกเลิก			
๑๙.	ผู้บันทึกรายการ			

๑๒. รายละเอียดข้อมูลเจ้าหนี้

ลำดับที่	รายการข้อมูล	Field ที่เก็บข้อมูล	Table ที่เก็บข้อมูล	หมายเหตุ
๑.	คำนำหน้า			
๒.	รหัสเจ้าหนี้			
๓.	ชื่อเจ้าหนี้			
๔.	นามสกุล			
๕.	ที่อยู่			
๖.	อำเภอ			
๗.	จังหวัด			
๘.	รหัสไปรษณีย์			
๙.	เบอร์โทรศัพท์			
๑๐.	เบอร์โทรสาร			
๑๑.	เลขที่บัตรประชาชนหรือเลขที่จดทะเบียนนิติบุคคล			

ลำดับที่	รายการข้อมูล	Field ที่เก็บข้อมูล	Table ที่เก็บข้อมูล	หมายเหตุ
๑๒.	เลขประจำตัวผู้เสียภาษี			
๑๓.	เลขทะเบียนภาษีมูลค่าเพิ่ม			
๑๔.	อัตราภาษีมูลค่าเพิ่ม			
๑๕.	ประเภทเจ้าหนี้			
๑๖.	ผู้บันทึกรายการ			
๑๗.	วันที่บันทึกรายการ			
๑๘.	สถานะของเจ้าหนี้			
๑๙.	วันที่ปรับปรุงล่าสุด			
๒๐.	ระยะเวลาการชำระเงิน (Payment Term)			
๒๑.	ยอดเจ้าหนี้คงเหลือล่าสุด			

๑๓. รายละเอียดการจ่ายชำระหนี้

ลำดับที่	รายการข้อมูล	Field ที่เก็บข้อมูล	Table ที่เก็บข้อมูล	หมายเหตุ
๑.	เลขที่รายการจ่ายชำระหนี้			
๒.	อ้างอิงเลขที่ใบกำกับสินค้า			
๓.	วันที่ทำรายการ			
๔.	รหัสผู้ขายหรือรหัสสมาชิก			
๕.	จำนวนเงินที่ทำรายการ			
๖.	สถานะของการจ่ายชำระหนี้			
๗.	หนี้คงเหลือ			
๘.	ส่วนลดรับ			
๙.	สถานะเจ้าหนี้			
๑๐.	ยกเลิกรายการจ่ายชำระหนี้เจ้าหนี้การค้า			
๑๑.	สาเหตุการยกเลิกชำระหนี้			
๑๒.	วันที่ยกเลิก			
๑๓.	ผู้บันทึกรายการ			

๑๔. รายละเอียดข้อมูลสินค้า

ลำดับที่	รายการข้อมูล	Field ที่เก็บข้อมูล	Table ที่เก็บข้อมูล	หมายเหตุ
๑.	รหัสสินค้า			
๒.	ชื่อสินค้า			
๓.	ประเภทสินค้า			
๔.	กลุ่มสินค้า(รหัสธุรกิจ/โครงการ)			
๕.	คลังสินค้า			
๖.	หน่วยวัด			
๗.	วิธีการคำนวณต้นทุนสินค้า			
๘.	เป็นสินค้าที่อยู่ในระบบภาษีมูลค่าเพิ่มหรือไม่			
๙.	วันที่บันทึกรายการ			
๑๐.	ผู้บันทึกรายการ			
๑๑.	สถานะของสินค้า			
๑๒.	ราคาซื้อต่อหน่วย			
๑๓.	วันที่ซื้อล่าสุด			
๑๔.	ราคาต้นทุนถัวเฉลี่ยล่าสุด			
๑๕.	ราคาขายต่อหน่วย			
๑๖.	วันที่ขายล่าสุด			
๑๗.	ราคาขายมาตรฐาน			
๑๘.	ปริมาณสินค้าคงเหลือในมือ			

๑๕. รายละเอียดรายการเคลื่อนไหวสินค้า

ลำดับที่	รายการข้อมูล	Field ที่เก็บข้อมูล	Table ที่เก็บข้อมูล	หมายเหตุ
๑.	เลขที่ใบสินค้า			
๒.	รหัสการเคลื่อนไหวสินค้า			
๓.	วันทีเกิดรายการ			
๔.	รหัสสินค้า			
๕.	ชื่อสินค้า			
๖.	คลังสินค้า			
๗.	หน่วยวัด			
๘.	ปริมาณเคลื่อนไหว			
๙.	ราคาต้นทุนเฉลี่ยต่อหน่วย			
๑๐.	อ้างอิงเลขที่เอกสาร (ใบขายหรือใบรับของ)			
๑๑.	วันที่ทำรายการ			
๑๒.	ผู้บันทึกรายการ			

๑๖. รายละเอียดข้อมูลผังบัญชี

ลำดับที่	รายการข้อมูล	Field ที่เก็บข้อมูล	Table ที่เก็บข้อมูล	หมายเหตุ
๑.	รหัสผังบัญชี			
๒.	รหัสบัญชี			
๓.	ชื่อบัญชี			
๔.	ประเภทบัญชี			
๕.	ปรากฏในงบการเงิน			
๖.	รหัสบัญชีคุม			
๗.	รหัสโครงการ			
๘.	รหัสศูนย์ต้นทุน			
๙.	ดุลบัญชี			
๑๐.	วันที่ตั้งยอดยกมา			
๑๑.	ยอดยกมาด้านเดบิต			
๑๒.	ยอดยกมาด้านเครดิต			
๑๓.	สถานะการใช้งาน			
๑๔.	สถานะการลบผังบัญชี			
๑๕.	วันที่บันทึกรายการ			
๑๖.	ผู้บันทึกรายการ			

๑๗. รายละเอียดของรายการผ่านบัญชี

ลำดับที่	รายการข้อมูล	Field ที่เก็บข้อมูล	Table ที่เก็บข้อมูล	หมายเหตุ
๑.	ปีบัญชี			
๒.	เลขที่ใบผ่านบัญชี			
๓.	วันที่ผ่านรายการบัญชี			
๔.	วันที่ในเอกสาร			
๕.	ประเภทรายการผ่านบัญชี			
๖.	รหัสบัญชี			
๗.	เดบิต/เครดิต			
๘.	จำนวนเงินที่ทำรายการ			
๙.	คำอธิบายรายการ			
๑๐.	สถานะรายการ			
๑๑.	วันที่บันทึกรายการ			
๑๒.	ผู้บันทึกรายการ			

๑๘. รายละเอียดข้อมูลอัตราเงินปันผล

ลำดับที่	รายการข้อมูล	Field ที่เก็บข้อมูล	Table ที่เก็บข้อมูล	หมายเหตุ
๑.	งวดปีจ่ายเงินปันผล			
๒.	รหัสรายการของอัตราเงินปันผล			
๓.	อัตราเงินปันผล			
๔.	มูลค่าหุ้นคงเหลือขั้นต่ำ			
๕.	วันที่เริ่มคำนวณเงินปันผล			
๖.	วันที่สิ้นสุดคำนวณเงินปันผล			
๗.	สถานะการใช้งาน			
๘.	วันที่บันทึกรายการ			
๙.	ผู้บันทึกรายการ			

๑๙. รายละเอียดข้อมูลการจ่ายเงินปันผล

ลำดับที่	รายการข้อมูล	Field ที่เก็บข้อมูล	Table ที่เก็บข้อมูล	หมายเหตุ
๑.	รหัสสมาชิก			
๒.	ชื่อสมาชิก			
๓.	รหัสกลุ่ม			
๔.	รหัสตัวแทน			
๕.	มูลค่าหุ้นคงเหลือ			
๖.	อัตราเงินปันผล			
๗.	ระยะเวลาคิดเงินปันผล			
๘.	จำนวนเงินปันผล			
๙.	วันบันทึกรายการ			
๑๐.	ผู้บันทึกรายการ			
๑๑.	ยอดการจ่ายเงินปันผล			
๑๒.	วันที่จ่ายเงินปันผล			

๒๐. รายละเอียดข้อมูลอัตราเงินเฉลี่ยคืน

ลำดับที่	รายการข้อมูล	Field ที่เก็บข้อมูล	Table ที่เก็บข้อมูล	หมายเหตุ
๑.	ประเภทเงินกู้			
๒.	รหัสรายการเฉลี่ยคืน			
๓.	วันที่เริ่มต้นคำนวณเงินเฉลี่ยคืน			
๔.	วันที่สิ้นสุดคำนวณเงินเฉลี่ยคืน			
๕.	อัตราเงินเฉลี่ยคืน			
๖.	สถานะการใช้งาน			
๗.	วันที่ทำรายการ			
๘.	ผู้บันทึกรายการ			

๒๑. รายละเอียดข้อมูลการจ่ายเงินเฉลี่ยคืน

ลำดับที่	รายการข้อมูล	Field ที่เก็บข้อมูล	Table ที่เก็บข้อมูล	หมายเหตุ
๑.	เลขที่สัญญาเงินกู้			
๒.	ประเภทบัญชีเงินกู้			
๓.	ลำดับที่รายการเฉลี่ยคืน			
๔.	จำนวนเงินเฉลี่ยคืน			
๕.	วันที่จ่ายเงินเฉลี่ยคืน			
๖.	ยอดเงินเฉลี่ยคืนที่จ่ายจริง			
๗.	ยอดเงินเฉลี่ยคืนที่ปรับปรุง			
๘.	วันที่ปรับปรุงรายการล่าสุด			
๙.	วันที่ประมวลผลยอดเงินเฉลี่ยคืน			

ภาคผนวก ข.

นโยบาย

[ร่าง]

ระเบียบ สหกรณ์..... จำกัด
ว่าด้วย วิธีปฏิบัติในการควบคุมภายในและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของสหกรณ์
พ.ศ. .....

อาศัยอำนาจตามความในข้อบังคับของสหกรณ์ข้อ..... และข้อ..... และมติที่ประชุมคณะกรรมการดำเนินการ ครั้งที่ ..... วันที่ ..... คณะกรรมการดำเนินการจึงได้กำหนดระเบียบว่าด้วย วิธีปฏิบัติในการควบคุมภายในและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของสหกรณ์ ดังต่อไปนี้

หมวด ๑ บททั่วไป

ข้อ ๑ ระเบียบนี้เรียกว่า “ระเบียบ สหกรณ์.....จำกัด ว่าด้วย วิธีปฏิบัติในการควบคุมภายในและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของสหกรณ์ พ.ศ. ..... ”

ข้อ ๒ ระเบียบนี้ให้ใช้บังคับตั้งแต่วันที่ ..... พ.ศ. ..... เป็นต้นไป

ข้อ ๓ บรรดาระเบียบ ประกาศ คำสั่ง มติ หรือข้อตกลงอื่นใด ซึ่งขัดหรือแย้งกับระเบียบนี้ ให้ใช้ระเบียบนี้แทน

ข้อ ๔ ในระเบียบนี้

“สหกรณ์” หมายถึง สหกรณ์..... จำกัด

“คณะกรรมการ” หมายถึง คณะกรรมการดำเนินการ สหกรณ์..... จำกัด

“ประธานกรรมการ” หมายถึง ประธานคณะกรรมการดำเนินการ สหกรณ์.....จำกัด

“ผู้จัดการ” หมายถึง ผู้จัดการ สหกรณ์.....จำกัด

“เจ้าหน้าที่” หมายถึง เจ้าหน้าที่ สหกรณ์.....จำกัด

“บุคลากร” หมายถึง ผู้ใช้ประโยชน์จากทรัพย์สินด้านเทคโนโลยีสารสนเทศของสหกรณ์ ซึ่งครอบคลุมถึงเจ้าหน้าที่ สมาชิกทุกคน ตลอดจนบุคคลภายนอกที่ได้รับอนุญาตให้ทำงานในสหกรณ์หรือที่เข้ามาดำเนินการด้านเทคโนโลยีสารสนเทศให้กับสหกรณ์ตามข้อตกลงที่ทำไว้กับสหกรณ์ หรือที่เข้ามาอบรมตามโครงการที่ผ่านความเห็นชอบจากที่ประชุมคณะกรรมการ และเจ้าหน้าที่ของรัฐผู้ดูแลการใช้โปรแกรมระบบบัญชีคอมพิวเตอร์ในการประมวลผลข้อมูล

“เครื่องคอมพิวเตอร์” หมายถึง เครื่องคอมพิวเตอร์ทั้งหลาย เครื่องเซิร์ฟเวอร์ หรืออุปกรณ์อื่นใด ที่ทำหน้าที่ได้เสมือนเครื่องคอมพิวเตอร์ ทั้งที่ใช้งานอยู่ภายในสหกรณ์ หรือภายนอกแล้วเชื่อมต่อเข้ากับระบบเครือข่าย

“ระบบเครือข่าย” หมายถึง ระบบเครือข่ายคอมพิวเตอร์ที่สหกรณ์สร้างขึ้นทั้งแบบมีสาย และไร้สาย

“ข้อมูล” หมายถึง สิ่งที่สื่อความหมายให้รู้เรื่องราว ข้อเท็จจริง ข้อมูล หรือสิ่งใด ๆ ไม่ว่าจะได้จัดทำไว้ในรูปแบบของเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้

“ระบบสารสนเทศ” หมายถึง ข้อมูล และสาระต่าง ๆ ที่เกิดจากการประมวลผลมาจากข้อมูล ที่จัดไว้อย่างเป็นระบบ

ข้อ ๕ วิธีการเผยแพร่ระเบียบ

(๑) แจ้งให้ทราบการถือใช้ระเบียบในที่ประชุมคณะกรรมการดำเนินการ

(๒) ทำหนังสือเวียนให้เจ้าหน้าที่รับทราบ

(๒) ติดประกาศไว้ ณ ที่ทำการสหกรณ์ เป็นระยะเวลาอย่างน้อย ๖๐ วัน นับแต่วันที่ประกาศถือใช้ระเบียบนี้

ข้อ ๖ ในกรณีที่มีปัญหาเกี่ยวกับการปฏิบัติตามระเบียบนี้ ให้คณะกรรมการดำเนินการเป็นผู้มีอำนาจวินิจฉัย

ข้อ ๗ ให้ประธานกรรมการเป็นผู้รักษาการให้เป็นไปตามระเบียบนี้

หมวด ๒ วัตถุประสงค์

ข้อ ๘ วัตถุประสงค์ของการออกระเบียบนี้

(๑) เพื่อให้บุคลากรระมัดระวังในการใช้เครื่องคอมพิวเตอร์ โดยจะไม่ทำให้ประสิทธิภาพของระบบบัญชีคอมพิวเตอร์และระบบเครือข่ายด้อยประสิทธิภาพลงอย่างผิดปกติโดยเจตนาหรือไม่เจตนาก็ตาม

(๒) เพื่อให้บุคลากรใช้เทคโนโลยีสารสนเทศอย่างถูกต้องตามบทบาทและหน้าที่ที่ได้รับมอบหมาย

(๓) เพื่อให้การใช้เทคโนโลยีสารสนเทศของสหกรณ์มีความมั่นคง ปลอดภัย และสามารถใช้งานได้อย่างมีประสิทธิภาพ

(๔) เพื่อให้บุคลากรระมัดระวังและตระหนักถึงความเสี่ยงที่อาจเกิดขึ้นจากการใช้เทคโนโลยีสารสนเทศ

(๕) เพื่อให้สหกรณ์ได้มีการควบคุมภายในและรักษาความปลอดภัยระบบสารสนเทศที่ใช้คอมพิวเตอร์เป็นไปตามนโยบาย ระเบียบสหกรณ์และระเบียบนายทะเบียนสหกรณ์

หมวด ๓ การรักษาความปลอดภัยทางกายภาพ

ข้อ ๙ สหกรณ์จะต้องจัดตั้งเครื่องคอมพิวเตอร์ไว้ในที่ที่เหมาะสม และห้ามผู้ไม่มีหน้าที่รับผิดชอบเข้ามาใช้เครื่องคอมพิวเตอร์ของสหกรณ์โดยไม่ได้รับอนุญาต

ข้อ ๑๐ จัดให้มีการติดตั้งอุปกรณ์ดับเพลิงไว้ในที่ที่เหมาะสมและสะดวกต่อการใช้งานเมื่อมีเหตุฉุกเฉิน และจัดทำแผนผังการขนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ รวมทั้งเอกสารที่เกี่ยวข้อง

ข้อ ๑๑ จัดให้มีระบบการควบคุมอุณหภูมิ ให้แก่อุปกรณ์เครื่องคอมพิวเตอร์อย่างเพียงพอและเหมาะสมกับสถานที่รวมทั้งจัดตั้งเครื่องคอมพิวเตอร์ให้อยู่ในสถานที่ที่มีอากาศถ่ายเทได้สะดวก

ข้อ ๑๒ จัดให้มีระบบสำรองไฟเครื่องแม่ข่ายและอุปกรณ์ที่เกี่ยวข้องอย่างเพียง เพื่อลดการหยุดชะงักการทำงานของเครื่องแม่ข่ายในกรณีที่มีไฟฟ้าดับหรือไฟตก

หมวด ๔ คณะกรรมการดำเนินการ

ข้อ ๑๓ ต้องพิจารณาจัดให้มีทรัพย์สินด้านเทคโนโลยีสารสนเทศตามสมควรและเหมาะสมกับสหกรณ์

ข้อ ๑๔ มอบหมายให้มีผู้รับผิดชอบในการติดตามการปฏิบัติตามนโยบายหรือระเบียบปฏิบัติในการควบคุมภายใน และการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของสหกรณ์

ข้อ ๑๕ สื่อสารให้บุคลากรเข้าใจนโยบายหรือระเบียบปฏิบัติในการควบคุมภายในและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของสหกรณ์

ข้อ ๑๖ ส่งเสริมให้มีการฝึกอบรมหรือให้ความรู้เกี่ยวกับระบบงานและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศแก่คณะกรรมการดำเนินการ ผู้จัดการ และเจ้าหน้าที่สหกรณ์ อย่างน้อยปีละ ๑ ครั้ง หรือสนับสนุนให้เข้ารับการฝึกอบรมกับหน่วยงานและองค์กรต่าง ๆ ที่มีการจัดอบรมในเรื่องดังกล่าว

ข้อ ๑๗ ต้องกำหนดให้ผู้บริการโปรแกรมระบบบัญชีจัดทำคู่มือการใช้โปรแกรมและเอกสารด้านฐานข้อมูล ได้แก่ โครงสร้างข้อมูล (Data Structure) หรือพจนานุกรมข้อมูล (Data Dictionary) ให้กับสหกรณ์เพื่อ ประกอบการใช้งานโปรแกรมระบบบัญชี

ข้อ ๑๘ มอบหมายให้มีผู้รับผิดชอบในการเก็บรักษาคู่มือและเอกสารสนับสนุนการปฏิบัติงานให้อยู่ในที่ปลอดภัย และให้เรียกใช้งานได้ทันที

ข้อ ๑๙ พิจารณาคัดเลือกและจัดทำสัญญากับผู้ให้บริการโปรแกรมหรือระบบเทคโนโลยีสารสนเทศ และพิจารณาเกี่ยวกับการรักษาความลับของข้อมูล เงื่อนไขต่างๆ และขอบเขตงานของผู้ให้บริการ กรณีที่ใช้บริการโปรแกรมของเอกชน

ข้อ ๒๐ แต่งตั้งเจ้าหน้าที่เพื่อรับผิดชอบด้านเทคโนโลยีสารสนเทศของสหกรณ์

ข้อ ๒๑ จัดให้มีการทำหรือทบทวนแผนฉุกเฉิน และการประเมินผลของการทดสอบแผนฉุกเฉินอย่างน้อยปีละ ๑ ครั้ง

ข้อ ๒๒ รณรงค์ให้ทุกคนใช้พลังงานไฟฟ้าอย่างประหยัด โดยจัดระดับการทำงานของเครื่องคอมพิวเตอร์และปิดอุปกรณ์ต่อพ่วงทุกครั้งที่ไม่มีการใช้งาน ให้เหมาะสมและมีประสิทธิภาพ รวมทั้งการใช้มาตรการลดการใช้กระดาษให้น้อยลงด้วย

หมวด ๕ ผู้จัดการสหกรณ์/ผู้ดูแลระบบงาน

ข้อ ๒๓ ควบคุมดูแลการใช้ระบบเทคโนโลยีสารสนเทศให้เป็นไปตามวัตถุประสงค์

ข้อ ๒๔ ดำเนินการให้ระบบเทคโนโลยีสารสนเทศของสหกรณ์ทำงานได้อย่างมีประสิทธิภาพ ทันสมัย และมั่นคงปลอดภัยตามนโยบายการรักษาความปลอดภัยของสหกรณ์

ข้อ ๒๕ ติดตั้งค่าการรักษาความปลอดภัยของระบบบัญชีคอมพิวเตอร์และระบบเครือข่ายให้สามารถป้องกันบุคคลที่ไม่ได้รับอนุญาตเข้าสู่ระบบได้ง่าย ได้แก่ ความยาวของรหัสผ่าน ระยะเวลาการเปลี่ยนแปลงรหัสผ่าน ระยะเวลาการตั้งเวลาพักหน้าจอในกรณีผู้ใช้งานไม่อยู่ที่เครื่อง เป็นต้น

ข้อ ๒๖ มีหน้าที่รับผิดชอบในการบริหารจัดการผู้ใช้งาน เกี่ยวกับการสร้าง/เปลี่ยนแปลง/ลบชื่อผู้ใช้งาน (username) โดยการกำหนดสิทธิการใช้งาน จะต้องเป็นไปตามหน้าที่ความรับผิดชอบของผู้ใช้งาน

ข้อ ๒๗ มีหน้าที่สอบทานสิทธิการใช้งานของเจ้าหน้าที่ในระบบบัญชีคอมพิวเตอร์และระบบเครือข่ายให้สอดคล้องกับหน้าที่ความรับผิดชอบในแต่ละตำแหน่งเป็นประจำทุกปี

ข้อ ๒๘ บริหารจัดการระบบเครือข่ายให้มีความมั่นคงปลอดภัย มีประสิทธิภาพ ครอบคลุมพื้นที่การทำงานทั้งหมด ได้แก่

(๑) กำหนดสิทธิการเข้าถึงระบบเครือข่ายให้กับผู้ที่ได้รับอนุญาตเท่านั้น

(๒) จัดทำการปรับปรุงแผนผังเครือข่ายและอุปกรณ์ที่เกี่ยวข้องให้เป็นปัจจุบัน

(๓) มีการตรวจสอบหรือเฝ้าระวังเกี่ยวกับการรักษาความปลอดภัยระบบคอมพิวเตอร์แม่ข่ายอย่างสม่ำเสมอ

(๔) ติดตั้งระบบป้องกันไวรัสกับเครื่องคอมพิวเตอร์แม่ข่าย และปรับปรุงระบบป้องกันไวรัสให้เป็นปัจจุบันสม่ำเสมอ

ข้อ ๒๙ จัดทำตารางแผนการสำรองข้อมูลและวิธีการกู้คืนข้อมูล และให้มีการสำรองข้อมูลและการทดสอบการกู้คืนข้อมูลเป็นไปตามแผนที่กำหนด ได้แก่

(๑) กำหนดตารางแผนการสำรองข้อมูลให้เหมาะสมกับการปฏิบัติงานของสหกรณ์

(๒) กำหนดให้สำรองข้อมูลจากระบบบัญชีคอมพิวเตอร์ที่สหกรณ์ใช้ในเครื่องคอมพิวเตอร์ที่แยกต่างหากจากเครื่องแม่ข่ายหลักของสหกรณ์ จำนวน ๑ ชุดเป็นประจำทุกวันทำการของสหกรณ์และสำรองข้อมูลไว้ในสื่อบันทึกข้อมูล จำนวน ๑ ชุดเป็นประจำทุกเดือน

(๓) กำหนดให้สำรองโปรแกรม ฐานข้อมูลที่เกี่ยวกับระบบปฏิบัติการ ระบบฐานข้อมูลและระบบบัญชีคอมพิวเตอร์ไว้ในสื่อบันทึกข้อมูลจำนวน ๑ ชุด เป็นประจำทุก ๓ เดือน

(๔) ให้เจ้าหน้าที่ผู้รับผิดชอบระบบงานสำรองข้อมูลในสื่อบันทึกข้อมูลและติดฉลากที่มีรายละเอียด โปรแกรมระบบงาน วัน เดือน ปี จำนวนหน่วยข้อมูล

(๕) จัดเก็บสื่อบันทึกข้อมูลไว้ในที่ปลอดภัยทั้งในและนอกสำนักงานสหกรณ์ และให้สามารถนำมาใช้งานได้ทันทีในกรณีที่มีเหตุฉุกเฉิน

(๖) ผู้จัดการหรือผู้ที่ได้รับมอบหมายต้องทดสอบข้อมูลที่สำรองทุก ๖ เดือน และเก็บรักษาชุดสำรองข้อมูลไว้อย่างน้อย ๑๐ ปีตามกฎหมาย

(๗) จัดทำทะเบียนคุมข้อมูลชุดสำรอง และควบคุมการนำข้อมูลชุดสำรองออกมาใช้งาน

ข้อ ๓๐ จัดทำแผนฉุกเฉินรองรับเมื่อเกิดปัญหากับระบบเทคโนโลยีสารสนเทศ ในกรณีเครื่องคอมพิวเตอร์ได้รับความเสียหายหรือหยุดชะงัก และกำหนดผู้รับผิดชอบที่ชัดเจน

ข้อ ๓๑ ดำเนินการทดสอบแผนฉุกเฉินร่วมกับบุคลากรอย่างน้อยปีละ ๑ ครั้งและจัดทำผลการทดสอบแผนฉุกเฉิน

ข้อ ๓๒ จัดการกับเหตุการณ์ผิดปกติที่เกี่ยวข้องกับความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศโดยทันทีเมื่อได้รับรายงานจากบุคลากร

หมวด ๖ บุคลากร

ข้อ ๓๓ ต้องใช้เครื่องคอมพิวเตอร์เพื่อประโยชน์สูงสุดต่อการดำเนินงานของสหกรณ์ และเป็นไปตามวัตถุประสงค์

ข้อ ๓๔ ให้คำนึงถึงการใช้งานอย่างประหยัด และหมั่นตรวจสอบเครื่องคอมพิวเตอร์ให้สามารถใช้งานได้อย่าง สมบูรณ์ และมีประสิทธิภาพ

ข้อ ๓๕ บุคลากรแต่ละคนมีหน้าที่ป้องกันดูแลรักษาข้อมูลชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) ทั้งนี้ต้องห้ามเผยแพร่ให้ผู้อื่นล่วงรู้รหัสผ่าน (password) ของตนเอง

ข้อ ๓๖ การกำหนดรหัสผ่านในการเข้าถึงระบบเทคโนเลยีสารสนเทศอย่างน้อย ๔ ตัวอักษร โดยกำหนดให้มี ความยากต่อการคาดเดาและให้มีการเปลี่ยนแปลงรหัสผ่านของผู้ใช้งานทุก ๆ ๔ เดือน

ข้อ ๓๗ บุคลากรแต่ละคนห้ามใช้ชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) ของบุคคลอื่นมาใช้งานไม่ว่าจะได้รับอนุญาตจากผู้ใช้งานนั้นหรือไม่ก็ตาม

ข้อ ๓๘ การใช้งานเครื่องคอมพิวเตอร์ ผู้ใช้งานต้องรับผิดชอบในฐานะเป็นผู้ถือครองเครื่องนั้น ๆ และต้อง รับผิดชอบต่อความเสียหายที่เกิดขึ้นอันเนื่องมาจากการใช้งานที่ผิดปกติ โดยชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) ของผู้ถือครองเครื่องนั้น ๆ

ข้อ ๓๙ เมื่อพบเหตุการณ์ผิดปกติที่เกี่ยวกับความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ให้รีบแจ้งให้ผู้จัดการ/ผู้ดูแลระบบงานของสหกรณ์โดยทันที

ประกาศใช้เมื่อวันที่ ..... พ.ศ. .....

(.....)

ประธานกรรมการ

สหกรณ์..... จำกัด

ภาคผนวก ค.

แบบฟอร์มการขอรหัสผู้ใช้งาน

แบบฟอร์มการขอรหัสผู้ใช้งาน (User ID/User Name)

สำหรับการใช้ยืนยันตัวตน (Authentication) เพื่อเข้าใช้ระบบงาน

วันที่.....

เรื่อง ขอ UserID สำหรับเข้าใช้ระบบ Authentication

เรียน ผู้จัดการ .....

ด้วยข้าพเจ้า.....ตำแหน่ง .....

ชื่อ – นามสกุลภาษาอังกฤษ .....

สังกัด ..... E-mail address .....

เบอร์ติดต่อกลับ โทรศัพท์ภายใน.....โทรศัพท์มือถือ.....

มีความประสงค์จะขอ UserID/UserName เพื่อใช้ Authentication เข้าใช้

☐ ระบบงาน .....

☐ ระบบงาน .....

☐ ระบบงาน .....

ข้าพเจ้ายินดีจะรับผิดชอบต่อ User ID/User Name ที่ได้รับ และจะปฏิบัติตามนโยบายของสหกรณ์ เกี่ยวกับการใช้ระบบเทคโนโลยีสารสนเทศอย่างเคร่งครัดทุกประการ

จึงเรียนมาเพื่อโปรดพิจารณาดำเนินการ

(ลงชื่อ).....ผู้ขอใช้ระบบ

(.....)

การอนุมัติให้ดำเนินการ

ลงชื่อ.....ผู้อนุมัติ

(.....)

...../...../.....

การดำเนินการ

ลงชื่อ.....ผู้ดำเนินการ

(.....)

...../...../.....

ภาคผนวก ง.

ตัวอย่างสัญญาการให้บริการบำรุงรักษาโปรแกรม

สัญญาให้บริการบำรุงรักษาระบบงานคอมพิวเตอร์

สัญญานี้ทำที่.....

เมื่อวันที่.....เดือน.....พ.ศ.....ระหว่าง

ก. นาย/นาง/นางสาว..... อายุ.....ปี/ห้างหุ้นส่วนจำกัด..... โดยผู้มีอำนาจลงนามท้ายสัญญา/บริษัท.....จำกัด โดยผู้มีอำนาจลงนามท้ายสัญญา อยู่บ้านเลขที่/สำนักงานเลขที่.....หมู่ที่.....ตรอก/ซอย..... ถนน.....แขวง/ตำบล.....เขต/อำเภอ..... จังหวัด..... บัตรประจำตัวประชาชนเลขที่..... ออกให้โดย.....ซึ่งต่อไปจะเรียกว่า “ผู้ให้บริการ” ฝ่ายหนึ่ง กับ

ข. นาย/นาง/นางสาว.....อายุ.....ปี/ห้างหุ้นส่วนจำกัด.....โดยผู้มีอำนาจลงนามท้ายสัญญา/บริษัท.....จำกัด โดยผู้มีอำนาจลงนามท้ายสัญญา อยู่บ้านเลขที่/สำนักงานเลขที่.....หมู่ที่.....ตรอก/ซอย..... ถนน.....แขวง/ตำบล.....เขต/อำเภอ..... จังหวัด.....บัตรประจำตัวประชาชนเลขที่..... ออกให้โดย.....ซึ่งต่อไปจะเรียกว่า “ผู้รับบริการ” อีกฝ่ายหนึ่ง

โดยที่ผู้รับบริการเป็นผู้ประกอบธุรกิจเกี่ยวกับ..... มีความประสงค์จะใช้บริการแก้ไข และบำรุงรักษาระบบงานคอมพิวเตอร์ของผู้รับบริการ และ

โดยที่ผู้ให้บริการเป็นผู้ประกอบธุรกิจเกี่ยวกับ..... เป็นผู้มีความรู้ ความสามารถ ความชำนาญ และประสบการณ์ในด้านดังกล่าว และประสงค์จะให้บริการแก้ไข และบำรุงรักษาระบบงานคอมพิวเตอร์ของผู้รับบริการ ภายใต้หลักเกณฑ์และเงื่อนไขที่กำหนดไว้ในสัญญานี้

ดังนั้น ทั้งสองฝ่ายจึงตกลงทำสัญญากัน โดยมีข้อความดังต่อไปนี้

ข้อ 1. วัตถุที่ประสงค์แห่งสัญญา

1.1 ผู้ให้บริการตกลงให้บริการ และผู้รับบริการตกลงรับบริการแก้ไขและบำรุงรักษาระบบงานคอมพิวเตอร์ของผู้รับบริการ ดังนี้

1.1.1 .....

1.1.2 .....

1.1.3 .....

1.1.4 .....

ระบบงานคอมพิวเตอร์ตามข้อ 1.1.1 ถึง 1.1.4 ต่อไปจะเรียกรวมเรียกว่า “ระบบงานคอมพิวเตอร์”

การให้บริการตามสัญญานี้ จะต้องเป็นไปตามกำหนดเวลาที่ได้ระบุไว้ ในสัญญา หรือเมื่อผู้รับบริการร้องขอ โดยรายละเอียดของการให้บริการปรากฏตามเอกสารแนบท้ายสัญญา และให้ถือเป็นส่วนหนึ่งของสัญญานี้ ซึ่งต่อไปจะเรียกว่า “งานบริการ”

1.2 ทั้งสองฝ่ายทราบและเข้าใจดีว่างานบริการไม่รวมถึงการให้บริการดังต่อไปนี้

ก) การแก้ไข ปรับปรุงหรือเปลี่ยนแปลงระบบงานคอมพิวเตอร์ โดยผู้รับบริการหรือบุคคลภายนอก โดยไม่ได้รับความยินยอมจากผู้ให้บริการ

ข) การละเลย หรือใช้ระบบงานคอมพิวเตอร์ไม่ถูกวิธี หรือไม่ปฏิบัติตามคำแนะนำที่ได้ระบุไว้ในเอกสารประกอบ

ค) การแก้ไข บำรุงรักษาระบบงานคอมพิวเตอร์ที่ไม่ได้กำหนดในสัญญานี้

ง) ความเสียหายอันเกิดจากเหตุสุดวิสัย

จ) การที่ผู้รับบริการใช้หรือเชื่อมต่อระบบงานคอมพิวเตอร์กับฮาร์ดแวร์หรือระบบงานคอมพิวเตอร์อื่น ๆ ที่ผู้ให้บริการไม่ได้ระบุว่าสามารถใช้ได้กับระบบงานคอมพิวเตอร์ของผู้รับบริการ

ฉ) ระบบงานคอมพิวเตอร์ของบุคคลภายนอก

ข้อ 2. กำหนดระยะเวลาของสัญญา

ทั้งสองฝ่ายตกลงให้สัญญานี้มีกำหนดระยะเวลา.....ปี นับแต่วันที่..... เดือน.....พ.ศ.....ถึงวันที่.....เดือน.....พ.ศ.....

ข้อ 3. ราคาและการชำระราคา

ในวันทำสัญญาฉบับนี้ ผู้รับบริการตกลงชำระค่าบริการตามสัญญานี้ให้ผู้ให้บริการล่วงหน้าเป็นระยะเวลา.....เดือน/ปี เป็นจำนวนเงิน..... บาท (.....) โดยรวมภาษีมูลค่าเพิ่มตามอัตราที่กฎหมายกำหนด (ถ้ามี) ชำระเป็น

เงินสด/เช็คธนาคาร..... สาขา.....
เลขที่..... ลงวันที่.....เดือน.....พ.ศ. ..... ผู้ให้บริการได้รับเงินสด/เช็คดังกล่าวไว้เรียบร้อยแล้วในวันทำสัญญาฉบับนี้

ข้อ 4. สิทธิและหน้าที่ของผู้รับบริการ

ผู้รับบริการสัญญาและทราบดีว่า

4.1 ผู้รับบริการจะต้องให้ความร่วมมือแก่ผู้ให้บริการในการจัดหาข้อมูลรวมทั้งเอกสารต่าง ๆ ที่จำเป็นเพื่อให้ผู้ให้บริการสามารถปฏิบัติงานบริการได้อย่างสำเร็จลุล่วง

4.2 ผู้รับบริการจะต้องจัดสภาพการทำงานซึ่งปลอดภัย และอำนวยความสะดวกให้แก่ช่างผู้ชำนาญงาน และหรือตัวแทนของผู้ให้บริการ ในการที่จะเข้าไปทำงานบริการ

ข้อ 5. สิทธิและหน้าที่ของผู้ให้บริการ

ผู้ให้บริการสัญญาและทราบดีว่า

5.1 ผู้ให้บริการจะใช้ความรู้ความสามารถ และความอุตสาหะในการทำงานบริการให้แก่ผู้รับบริการตามสัญญานี้เพื่อให้งานบริการสำเร็จลุล่วง

5.2 ในกรณีที่ผู้ให้บริการจะต้องมาทำงานบริการ ณ สถานที่ทำการของผู้รับบริการ ผู้ให้บริการจะต้องปฏิบัติตามระเบียบการใช้สถานที่ของผู้รับบริการที่มีอยู่ ณ วันทำสัญญานี้และที่จะมีขึ้นในอนาคต ให้ถือเป็นส่วนหนึ่งของสัญญานี้ด้วย

5.3 ผู้ให้บริการจะทำงานบริการเฉพาะระบบงานคอมพิวเตอร์ที่ผู้รับบริการได้รับอนุญาตให้ใช้จากผู้ให้บริการเท่านั้น

5.4 ผู้ให้บริการไม่มีสิทธินำงานบริการตามสัญญานี้ออกให้บุคคลภายนอกให้บริการช่วง เว้นแต่จะได้รับความยินยอมจากผู้รับบริการก่อน

5.5 กรณีที่เกิดเหตุขัดข้องกับระบบงานคอมพิวเตอร์ทำให้ระบบงานคอมพิวเตอร์ไม่สามารถใช้การได้ตามปกติ ผู้ให้บริการจะส่งช่างผู้ชำนาญงานมาดำเนินการแก้ไข ระบบงานคอมพิวเตอร์ ภายในเวลา..... ชั่วโมงนับจากเวลาที่ได้รับแจ้งถึงเหตุขัดข้องนั้น จากผู้รับบริการ

โดยผู้ให้บริการจะดำเนินการแก้ไขระบบงานคอมพิวเตอร์ ให้อยู่ในสภาพใช้งาน ได้ดีตามปกติภายใน .....ชั่วโมงนับแต่วันที่ได้รับแจ้งโดยไม่คิดค่าบริการและค่าใช้จ่ายใดๆเพิ่มเติมจากผู้รับบริการอีก

5.6 จะไม่ใช้ เปิดเผย และหรือเอาไป ซึ่งข้อมูลการค้าอันเป็นความลับทางการค้าของผู้รับบริการ และหรืออนุญาตให้บุคคลอื่นกระทำการดังกล่าว โดยไม่ได้รับความยินยอมจากผู้รับบริการเป็นลายลักษณ์อักษร

ข้อ 6. นิติสัมพันธ์ระหว่างคู่สัญญา

ผู้ให้บริการตกลงและทราบดีว่า การให้บริการตามสัญญานี้ ผู้รับบริการและผู้ให้บริการไม่มีนิติสัมพันธ์กันในลักษณะจ้างแรงงานแต่อย่างใด

ข้อ 7. การผิดนัดผิดสัญญา

หากคู่สัญญาฝ่ายใดผิดสัญญาข้อหนึ่งข้อใด ให้คู่สัญญาอีกฝ่ายบอกกล่าวเป็นหนังสือให้คู่สัญญาที่ผิดสัญญาแก้ไขเยียวยาภายใน.....วันทำการ หากคู่สัญญาฝ่ายที่ผิดสัญญาเพิกเฉย หรือไม่แก้ไขเยียวยาให้แล้วเสร็จภายในระยะเวลาที่กำหนด คู่สัญญาอีกฝ่ายมีสิทธิบอกเลิกสัญญา และเรียกค่าเสียหายได้

ข้อ 8. ข้อตกลงอื่นๆ

8.1 กรณีที่คู่สัญญามีสิทธิคิดดอกเบี้ยต่อกัน ทั้งสองฝ่ายตกลงให้ใช้อัตราดอกเบี้ยร้อยละ.....ต่อปี นับแต่วันผิดนัด

8.2 การผ่อนผัน ผ่อนเวลา หรือการละเว้นการใช้สิทธิใด ๆ ที่คู่สัญญาฝ่ายหนึ่งมีอยู่กับคู่สัญญาอีกฝ่ายหนึ่งตามสัญญานี้ ไม่ถือว่า คู่สัญญาฝ่ายนั้นได้สละสิทธิประโยชน์นั้นต่อคู่สัญญาอีกฝ่ายหนึ่งแต่อย่างใด

8.3 การบอกกล่าว ทวงถาม หรือส่งเอกสารใดๆอันพึงมีแก่คู่สัญญาอีกฝ่ายหนึ่งตามภูมิลำเนาที่ปรากฏในสัญญานี้ ให้ถือว่าส่งโดยชอบและคู่สัญญาอีกฝ่ายได้ทราบแล้วนับแต่วันที่คำบอกกล่าวหรือเอกสารนั้นพึงไปถึงตามปกติ

สัญญานี้ทำขึ้นเป็นสองฉบับ มีข้อความถูกต้องตรงกันทั้งสองฝ่ายได้ทราบและเข้าใจข้อความโดยตลอดดีแล้ว เห็นว่าถูกต้องตรงตามเจตนาของตน จึงได้ลงลายมือชื่อพร้อมประทับตรา (ถ้ามี) ไว้เป็นสำคัญต่อหน้าพยาน และต่างยึดถือไว้ฝ่ายละฉบับ

ลงชื่อ .....ผู้ให้บริการ
( )

ลงชื่อ ..... ผู้รับบริการ
( )

ลงชื่อ .....พยาน
( )

ลงชื่อ .....พยาน
( )