

แบบประเมินการปฏิบัติตามระเบียบนายทะเบียนสหกรณ์  
ว่าด้วย มาตรฐานขั้นต่ำในการควบคุมภายในและการรักษาความปลอดภัย  
สำหรับสหกรณ์และกลุ่มเกษตรกรที่ใช้โปรแกรมระบบบัญชีคอมพิวเตอร์ประมวลผลข้อมูล  
พ.ศ. 2553

สหกรณ์ .....

ปีบัญชี .....

ลำดับ ที่	รายการ	ระดับการควบคุม			
		N/A	น้อย	ปานกลาง	มาก
	ระเบียบข้อที่ 1 จัดให้มีนโยบายหรือระเบียบปฏิบัติในการควบคุมการปฏิบัติงานเกี่ยวกับการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของสหกรณ์และกลุ่มเกษตรกรที่เป็นลายลักษณ์อักษร				
1.1	มีการกำหนดนโยบายหรือระเบียบปฏิบัติในการควบคุมการปฏิบัติงานเกี่ยวกับการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศที่ชัดเจนและเป็นลายลักษณ์อักษร		ไม่เป็นทางการ	ชัดเจนหรือเป็นลายลักษณ์อักษร	ชัดเจนและเป็นลายลักษณ์อักษร
1.2	มีการสื่อสารเกี่ยวกับการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศภายในสหกรณ์ให้ทราบทั่วกัน		ไม่ทราบ	พนักงานทราบแต่ไม่มีหลักฐานการสื่อสาร	มีติดประกาศหรือผ่าน Intranet
1.3	มีการจัดฝึกอบรมเกี่ยวกับการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศให้พนักงานเกิดความตระหนักและเข้าใจอย่างต่อเนื่อง		ไม่มี	มีฝึกอบรมครั้งแรกครั้งเดียว	มีการฝึกอบรมทุกปี
1.4	มีกระบวนการติดตามการถือปฏิบัติตามนโยบายเกี่ยวกับการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของภายในสหกรณ์อย่างสม่ำเสมอ		ไม่มี	มีการติดตามบ้าง	มีการกำหนดความถี่ในการติดตามอย่างน้อยปีละครั้ง
	ระเบียบข้อที่ 2 จัดให้มีระบบการรักษาความปลอดภัยทางกายภาพที่เพียงพอแก่การป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่ที่เกี่ยวข้องเข้าถึงอุปกรณ์สำคัญ และจัดให้มีระบบป้องกันความเสียหายจากสถานะแวดล้อมหรือภัยพิบัติต่าง ๆ ให้แก่อุปกรณ์คอมพิวเตอร์ที่สำคัญด้วย				
2.1	มีการควบคุมการเข้าถึงอุปกรณ์คอมพิวเตอร์ที่สำคัญจากบุคคลที่ไม่มีอำนาจหน้าที่ที่เกี่ยวข้อง		ไม่มี	อยู่ในสถานที่เป็นสัดส่วนแต่ไม่จำกัด	อยู่ในห้องคอมพิวเตอร์หรือ

ลำดับ ที่	รายการ	ระดับการควบคุม			
		N/A	น้อย	ปานกลาง	มาก
				การเข้าถึง	สถานที่ที่ล็อก ตลอดเวลา
2.2	มีระบบเตือนไฟไหม้ หรืออุปกรณ์ดับเพลิงเพื่อป้องกัน หรือระงับเหตุไฟไหม้ได้ทันเวลา		ไม่มีหรือมีแต่ ไม่สามารถใช้ งานได้	มีระบบเตือนไฟ ไหม้หรืออุปกรณ์ ดับเพลิงที่ใช้งานได้	มีระบบเตือนไฟ ไหม้และอุปกรณ์ ดับเพลิงที่ใช้งานได้
2.3	มีระบบสำรองไฟฟ้าและบำรุงรักษาให้ใช้งานได้อย่าง ต่อเนื่อง		ไม่มีหรือมีแต่ ไม่สามารถใช้ งานได้	มีระบบสำรอง ไฟฟ้าแต่ไม่ เพียงพอสำหรับ เครื่องที่สำคัญ	มีระบบสำรอง ไฟฟ้าและเพียงพอ
2.4	มีระบบปรับอากาศหรือควบคุมอุณหภูมิให้แก่อุปกรณ์ คอมพิวเตอร์อย่างเพียงพอ		ไม่มี	มีระบบปรับอากาศ แต่อุณหภูมิ ไม่ เหมาะสม	มีระบบปรับอากาศ และการควบคุม อุณหภูมิที่ เหมาะสม
	<b>ระเบียบข้อที่ 3 จัดให้มีระบบการรักษาความ ปลอดภัยของข้อมูลในระบบคอมพิวเตอร์และ เครือข่ายเพียงพอแก่การป้องกันมิให้บุคคลที่ไม่มี อำนาจหน้าที่ที่เกี่ยวข้องได้เข้าถึง ล้วงรู้ ใช้ประโยชน์ หรือแก้ไขเปลี่ยนแปลงข้อมูลหรือระบบดังกล่าวได้</b>				
3.1	มีวิธีการปฏิบัติเกี่ยวกับการบริหารจัดการรหัสผู้ใช้งาน User Account ในเรื่อง การสร้างหรือการเปลี่ยนแปลง หรือการลบรหัสผู้ใช้งานของระบบบัญชีคอมพิวเตอร์ อย่างเหมาะสม		ไม่มี	มีแต่ไม่ได้ถือปฏิบัติ อย่างสม่ำเสมอ	มีและถือปฏิบัติ อย่างสม่ำเสมอ
3.2	มีการกำหนดให้ผู้ใช้แต่ละรายมี User Account เป็นของตัวเอง ไม่ใช้ร่วมกับผู้อื่น		ไม่มี User Account/ใช้ User Account ร่วมกัน แต่ไม่ แบ่งแยกแผนก หรือระดับ พนักงาน	มีกำหนด User Account ร่วมกัน ในระดับแผนกหรือ ระดับพนักงาน	ไม่ใช่ User Account ร่วมกับ ผู้อื่น
3.3	มีการกำหนดรหัสผ่านในการเข้าถึงระบบบัญชี คอมพิวเตอร์อย่างน้อย 6 ตัวอักษร		รหัสผ่านน้อย กว่าหรือ เท่ากับ 4 ตัวอักษร	รหัสผ่าน น้อยกว่าหรือ เท่ากับ 6 ตัวอักษร	รหัสผ่านอย่างน้อย 6 ตัวอักษร
3.4	มีการกำหนดระยะเวลาการเปลี่ยนรหัสผ่านของผู้ใช้งาน อย่างน้อยทุก ๆ 6 เดือน		ไม่มีการเปลี่ยน รหัสผ่าน	เปลี่ยนรหัสผ่าน มากกว่า 6 เดือน	เปลี่ยนรหัสผ่านทุก ๆ 6 เดือน

ลำดับ ที่	รายการ	ระดับการควบคุม			
		N/A	น้อย	ปานกลาง	มาก
3.5	มีการเปลี่ยนรหัสผ่านใหม่ทันทีเมื่อผู้ใช้งานได้รับรหัสผ่านครั้งแรกก่อนเข้าถึงระบบบัญชีคอมพิวเตอร์		ไม่มีการเปลี่ยนรหัสครั้งแรก	ระบบไม่ได้บังคับเปลี่ยนรหัสครั้งแรก	ระบบบังคับให้มีการเปลี่ยนรหัสผ่านครั้งแรกเสมอ
3.6	มีการเก็บรหัสผ่านไว้เป็นความลับของผู้ใช้งานเพียงผู้เดียว		รหัสผ่านรับรู้ร่วมกันเป็นวงกว้างเนื่องจากการใช้ User Account ร่วมกัน	รหัสผ่านรับรู้ร่วมกันเนื่องจากมีกำหนด User Account ร่วมกันในระดับแผนกหรือระดับพนักงาน	รหัสผ่านเก็บไว้เป็นความลับเนื่องจากไม่ใช้งาน User Account ร่วมกัน
3.7	มีการกำหนดสิทธิของผู้ใช้งานในการใช้กิจกรรมต่างๆ ของระบบบัญชีคอมพิวเตอร์เป็นไปตามหน้าที่รับผิดชอบ รวมทั้งคำนึงถึงการแบ่งแยกหน้าที่ที่ดีและเหมาะสม		กำหนดสิทธิของผู้ใช้งานให้สามารถทำได้ทุกเมนู	กำหนดสิทธิการใช้งานตามหน้าที่ความรับผิดชอบ	กำหนดสิทธิการใช้งานตามหน้าที่ความรับผิดชอบและคำนึงการแบ่งแยกหน้าที่ที่ดีและเหมาะสม
3.8	มีการสอบถามสิทธิการใช้งานของผู้ใช้งานในระบบบัญชีคอมพิวเตอร์ ณ ปัจจุบัน ว่าสอดคล้องตามหน้าที่ความรับผิดชอบ อย่างน้อยปีละ 1 ครั้ง		ไม่มีการสอบถามสิทธิการใช้งาน	มีการสอบถามสิทธิการใช้งานว่าเหมาะสมกับหน้าที่น้อยกว่าปีละครั้ง	มีการสอบถามสิทธิการใช้งานว่าเหมาะสมกับหน้าที่ปีละครั้ง
3.9	มีการควบคุมการใช้งานผู้ใช้งานที่มีสิทธิสูงสุดในระบบบัญชีคอมพิวเตอร์ เช่น รหัสผู้ใช้งาน Administrator เป็นต้น โดยการเก็บของ Password ไว้ในตู้เซฟ หรือ จำกัดเฉพาะในกรณีจำเป็นเท่านั้น		ไม่มีการควบคุมการใช้ผู้ใช้งานที่มีสิทธิสูงสุด	มีผู้ใช้งานที่มีสิทธิสูงสุดในระบบ จำนวนมากกว่า 1 ผู้ใช้งานและใช้งานเฉพาะกรณีจำเป็น เช่น การติดตั้งโปรแกรม แก้ปัญหาระบบ เป็นต้น	มีผู้ใช้งานที่มีสิทธิสูงสุดในระบบ จำนวน 1 ผู้ใช้งานและจำกัดการใช้งานเฉพาะกรณีจำเป็นเท่านั้น เช่น การติดตั้งโปรแกรม แก้ปัญหาระบบ เป็นต้น และมีการเก็บรหัสผ่านของผู้ใช้งานที่มีสิทธิสูงสุดไว้ในที่ปลอดภัยรวมทั้งเปลี่ยนรหัสผ่านทุกครั้งเมื่อมีการใช้

ลำดับ ที่	รายการ	ระดับการควบคุม			
		N/A	น้อย	ปานกลาง	มาก
3.10	มีการเปลี่ยนรหัสผ่านของรหัสผู้ใช้งานที่มีสิทธิสูงสุดอย่างน้อยปีละครั้ง		ไม่มีการเปลี่ยนรหัสผ่านของผู้ใช้งานที่มีสิทธิสูงสุด	มีการเปลี่ยนรหัสผ่านของผู้ใช้งานที่มีสิทธิสูงสุดมากกว่าปีละครั้ง	มีการเปลี่ยนรหัสผ่านของผู้ใช้งานที่มีสิทธิสูงสุดปีละครั้ง
3.11	มีการตรวจสอบหรือเฝ้าระวังเกี่ยวกับการรักษาความปลอดภัยระบบคอมพิวเตอร์แม้ช่วยอย่างสม่ำเสมอ	ไม่มีการบุคคลากรในการตรวจสอบหรือเฝ้าระวังเกี่ยวกับการรักษาความปลอดภัย	ไม่มีการตรวจสอบหรือเฝ้าระวัง	มีการตรวจสอบหรือเฝ้าระวังเฉพาะเมื่อมีเหตุการณ์ผิดปกติเท่านั้น	มีการตรวจสอบหรือเฝ้าระวังจากการสอบทาน Log อย่างสม่ำเสมอ
3.12	ในกรณีที่มีการเชื่อมต่อกับระบบภายนอกสหกรณ์ มีการติดตั้งอุปกรณ์ Firewall เพื่อป้องกันการบุกรุกเข้าสู่ระบบบัญชีคอมพิวเตอร์ภายในของสหกรณ์	ไม่มีการเชื่อมต่อกับระบบภายนอกสหกรณ์	มีการเชื่อมต่อแต่ไม่มีการติดตั้งอุปกรณ์ Firewall	มีการเชื่อมต่อและติดตั้งอุปกรณ์ Firewall แต่ยังไม่พิจารณาถึง Firewall Policy ให้สอดคล้องกับสภาพแวดล้อมของสหกรณ์	มีการเชื่อมต่อและติดตั้งอุปกรณ์ Firewall และมีการกำหนด Firewall Policy ไว้อย่างเหมาะสม
3.13	มีการติดตั้งระบบป้องกันไวรัสให้กับเครื่องคอมพิวเตอร์ที่สำคัญทุกเครื่องและปรับปรุงระบบป้องกันไวรัสให้เป็นปัจจุบันอย่างสม่ำเสมอ		ไม่มีการติดตั้งระบบป้องกันไวรัส	มีการติดตั้งระบบป้องกันไวรัสแต่ไม่ได้ปรับปรุงให้เป็นปัจจุบัน	มีการติดตั้งระบบป้องกันไวรัสและปรับปรุงให้เป็นปัจจุบันอยู่เสมอ
	ระเบียบข้อที่ 4 จัดให้มีมาตรการควบคุมการพัฒนาหรือเปลี่ยนแปลงแก้ไขที่เพียงพอ เพื่อให้ระบบบัญชีคอมพิวเตอร์ มีการประมวลผลที่ถูกต้องครบถ้วนและเป็นไปตามความต้องการของผู้ใช้งาน รวมทั้งต้องมีการสื่อสารหรือฝึกอบรมเกี่ยวกับระบบบัญชีคอมพิวเตอร์ให้ผู้เกี่ยวข้องได้รับทราบอย่างทั่วถึง เพื่อให้สามารถใช้งานได้ถูกต้อง				
4.1	มีการกำหนดวิธีปฏิบัติในการพัฒนาระบบงานใหม่อย่าง	ไม่มีการพัฒนา	ไม่มีการ	มีการกำหนดวิธี	มีการกำหนดวิธี

ลำดับ ที่	รายการ	ระดับการควบคุม			
		N/A	น้อย	ปานกลาง	มาก
	เป็นลายลักษณ์อักษร โดยครอบคลุมถึงขั้นตอนที่สำคัญ ได้แก่ การกำหนดแผนการทำงาน การกำหนดความต้องการของระบบ การออกแบบระบบ การทดสอบ และนำระบบออกใช้งานจริง	หรือ เปลี่ยนแปลง ระบบงานใหม่ หรือใช้ โปรแกรมที่ พัฒนาโดยกรม ตรวจบัญชี สหกรณ์	กำหนดวิธี ปฏิบัติ	ปฏิบัติเป็นลาย ลักษณ์อักษร แต่ไม่ ถือปฏิบัติในทุก ขั้นตอน	ปฏิบัติเป็นลาย ลักษณ์อักษรและ ถือปฏิบัติในทุก ขั้นตอน
4.2	ในการพัฒนาระบบบัญชีคอมพิวเตอร์ใหม่ มีกำหนดแผนการทำงานและขั้นตอนการทำงานที่ชัดเจน	ไม่มีการพัฒนา หรือ เปลี่ยนแปลง ระบบงานใหม่ หรือใช้ โปรแกรมที่ พัฒนาโดยกรม ตรวจบัญชี สหกรณ์	ไม่มีกำหนด แผนการ ทำงาน	มีกำหนดแผนการ ทำงานและขั้นตอน การทำงานในชั้น แรกของการพัฒนา ระบบ แต่ไม่ได้ ปรับปรุงแผนหรือ ติดตาม ความก้าวหน้าของ แผนงานหรือ ขั้นตอนการทำงาน อย่างสม่ำเสมอ	มีกำหนดแผนการ ทำงานและขั้นตอน การทำงานของการ พัฒนาระบบ และมี การปรับปรุงแผน หรือติดตาม ความก้าวหน้าของ แผนงานหรือ ขั้นตอนการทำงาน อย่างสม่ำเสมอ
4.3	ในการพัฒนาระบบบัญชีคอมพิวเตอร์ใหม่ มีการกำหนดหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องอย่างชัดเจน	ไม่มีการพัฒนา หรือ เปลี่ยนแปลง ระบบงานใหม่ หรือใช้ โปรแกรมที่ พัฒนาโดยกรม ตรวจบัญชี สหกรณ์	ไม่มีการ กำหนดหน้าที่ ความ รับผิดชอบใน การพัฒนา ระบบงานใหม่ ที่ชัดเจน	มีการกำหนดหน้าที่ ความรับผิดชอบ ของผู้ที่เกี่ยวข้องใน การพัฒนา ระบบงานใหม่ อย่างไม่เป็น ทางการ	มีการกำหนดหน้าที่ ความรับผิดชอบ ของผู้ที่เกี่ยวข้องใน การพัฒนา ระบบงานใหม่ที่ ชัดเจน
4.4	มีการกำหนดความต้องการของผู้ใช้งานของระบบงานใหม่ (User Requirements) อย่างชัดเจน เพื่อใช้ในการควบคุมการพัฒนาระบบงานว่าเป็นไปตามความต้องการของผู้ใช้งานอย่างเหมาะสม	ไม่มีการพัฒนา หรือ เปลี่ยนแปลง ระบบงานใหม่ หรือใช้ โปรแกรมที่ พัฒนาโดยกรม ตรวจบัญชี	ความต้องการ ของผู้ใช้งานไม่ ชัดเจน	มีการกำหนดความ ต้องการของ ผู้ใช้งานยังไม่มี รายละเอียด เพียงพอ	มีการกำหนดความ ต้องการของ ผู้ใช้งานอย่าง ชัดเจนและละเอียด เพียงพอ

ลำดับ ที่	รายการ	ระดับการควบคุม			
		N/A	น้อย	ปานกลาง	มาก
		สหกรณ์			
4.5	ในกรณีที่มีการแปลงข้อมูลจากระบบเดิมไประบบงานใหม่ มีกระบวนการตรวจสอบหรือกระตบยอตระหว่างระบบงานเดิมและระบบงานใหม่อย่างเหมาะสม	ไม่มีการพัฒนาหรือเปลี่ยนแปลงระบบงานใหม่หรือไม่มีการแปลงข้อมูลจากระบบงานเดิม	ไม่มีการตรวจสอบหรือกระตบยอตข้อมูลระหว่างระบบงานเดิมกับระบบงานใหม่	มีการตรวจสอบบางส่วนหรือกระตบยอตเฉพาะยอตรวมของระบบงานเดิมกับระบบงานใหม่	มีการตรวจสอบรายละเอียดทั้งหมดรวมทั้งกระตบยอตในรายตัวและยอตรวมอย่างครบถ้วน
4.6	มีการทดสอบระบบงานที่พัฒนาใหม่เพื่อให้มั่นใจว่าระบบสามารถทำงานได้มีประสิทธิภาพ ประมวลผลถูกต้องและเป็นไปตามความต้องการก่อนจะนำระบบงานออกใช้งานจริง	ไม่มีการพัฒนาหรือเปลี่ยนแปลงระบบงานใหม่หรือใช้โปรแกรมที่พัฒนาโดยกรมตรวจบัญชีสหกรณ์	ไม่มีการทดสอบระบบงาน	มีการทดสอบระบบงานใหม่บางส่วนและไม่ครอบคลุมทั้งระบบใหม่	มีการทดสอบระบบงานใหม่อย่างครบถ้วน
4.7	มีการอนุมัติตามขั้นตอนของกระบวนการพัฒนาระบบงานใหม่ในทุกขั้นตอนจากผู้บริหารของสหกรณ์	ไม่มีการพัฒนาหรือเปลี่ยนแปลงระบบงานใหม่หรือใช้โปรแกรมที่พัฒนาโดยกรมตรวจบัญชีสหกรณ์	ไม่มีการอนุมัติจากผู้บริหาร	มีการอนุมัติตามขั้นตอนของกระบวนการพัฒนาระบบงานใหม่ แต่ไม่ครบถ้วนทุกขั้นตอน	มีการอนุมัติตามขั้นตอนของกระบวนการพัฒนาระบบงานใหม่ทุกขั้นตอน
4.8	มีการจัดฝึกอบรมเกี่ยวกับระบบบัญชีคอมพิวเตอร์ให้กับผู้ใช้งาน เพื่อให้สามารถประมวลผลข้อมูลได้ถูกต้องและครบถ้วน	ไม่มีการพัฒนาหรือเปลี่ยนแปลงระบบงานใหม่หรือใช้	ไม่มีการฝึกอบรม	มีการฝึกอบรมเฉพาะผู้ใช้งานที่สำคัญเท่านั้น	มีการฝึกอบรมให้กับผู้ใช้งานทุกคน

ลำดับ ที่	รายการ	ระดับการควบคุม			
		N/A	น้อย	ปานกลาง	มาก
		โปรแกรมที่ พัฒนาโดยกรม ตรวจบัญชี สหกรณ์			
4.9	มีการกำหนดวิธีปฏิบัติงานเกี่ยวกับการขอเปลี่ยนแปลงแก้ไขระบบงานโดยครอบคลุมกระบวนการขอเปลี่ยนแปลงแก้ไข ขั้นตอนในการทดสอบ และขั้นตอนในการนำระบบงานออกใช้งานจริงอย่างเป็นลายลักษณ์อักษร	ชื่อโปรแกรมสำเร็จรูปที่ไม่สามารถเปลี่ยนแปลงแก้ไขระบบงานหรือใช้โปรแกรมที่พัฒนาโดยกรมตรวจบัญชีสหกรณ์	ไม่มีการกำหนดวิธีปฏิบัติงาน	มีการกำหนดวิธีปฏิบัติงานแต่ไม่ได้ถือปฏิบัติอย่างเคร่งครัด หรือกำหนดวิธีปฏิบัติงานอย่างไม่เป็นทางการ	มีการกำหนดวิธีปฏิบัติงานอย่างเป็นลายลักษณ์อักษรและถือปฏิบัติอย่างเคร่งครัด
4.10	มีการอนุมัติการขอเปลี่ยนแปลงแก้ไขโปรแกรม/ระบบงานจากผู้บริหารสหกรณ์อย่างเป็นลายลักษณ์อักษร	ชื่อโปรแกรมสำเร็จรูปที่ไม่สามารถเปลี่ยนแปลงแก้ไขระบบงานหรือใช้โปรแกรมที่พัฒนาโดยกรมตรวจบัญชีสหกรณ์	ไม่มีการอนุมัติการขอเปลี่ยนแปลงแก้ไข	มีการอนุมัติการขอเปลี่ยนแปลงแก้ไขแต่ไม่ครบถ้วนทุกกรณี	มีการอนุมัติการขอเปลี่ยนแปลงแก้ไขทุกกรณี
4.11	มีการทดสอบโปรแกรม/ระบบงานที่เปลี่ยนแปลงแก้ไขจากผู้ที่เกี่ยวข้องรวมทั้งผู้ใช้งานอื่นเพื่อให้มั่นใจว่าระบบสามารถทำงานได้มีประสิทธิภาพ ประมวลผลถูกต้องและเป็นไปตามความต้องการก่อนจะที่โอนย้ายไปยังระบบงานที่ใช้จริง	ชื่อโปรแกรมสำเร็จรูปที่ไม่สามารถเปลี่ยนแปลงแก้ไขระบบงานหรือใช้โปรแกรมที่พัฒนาโดยกรมตรวจบัญชีสหกรณ์	ไม่มีการทดสอบโปรแกรม/ระบบงาน	มีการทดสอบโปรแกรม/ระบบงานแต่ไม่ถือปฏิบัติอย่างเคร่งครัด	มีการทดสอบโปรแกรม/ระบบงานและถือปฏิบัติอย่างเคร่งครัด
4.12	มีการแบ่งแยกหน้าที่ระหว่างผู้พัฒนาหรือผู้เปลี่ยนแปลงแก้ไขระบบงานออกจากผู้โอนย้าย	ชื่อโปรแกรมสำเร็จรูปที่ไม่	ไม่มีการแบ่งแยกหน้าที่	มีการแบ่งแยกหน้าที่ระหว่าง	มีการแบ่งแยกหน้าที่ระหว่าง

ลำดับ ที่	รายการ	ระดับการควบคุม			
		N/A	น้อย	ปานกลาง	มาก
	โปรแกรมหรือระบบงานเข้าสู่ระบบงานที่ใช้จริง	สามารถเปลี่ยนแปลงแก้ไขระบบงานหรือใช้โปรแกรมที่พัฒนาโดยกรมตรวจบัญชีสหกรณ์		ผู้พัฒนาหรือผู้เปลี่ยนแปลงแก้ไขออกจากผู้โอนย้ายโปรแกรมอย่างไม่เป็นทางการ	ผู้พัฒนาหรือผู้เปลี่ยนแปลงแก้ไขออกจากผู้โอนย้ายโปรแกรมอย่างเด็ดขาด
4.13	มีการแบ่งแยกส่วนคอมพิวเตอร์ที่มีไว้สำหรับการพัฒนาระบบงานหรือระบบงานสำหรับทดสอบออกจากระบบงานที่ใช้งานจริง	ซื้อโปรแกรมสำเร็จรูปที่ไม่สามารถเปลี่ยนแปลงแก้ไขระบบงานหรือใช้โปรแกรมที่พัฒนาโดยกรมตรวจบัญชีสหกรณ์	ไม่มีการแบ่งแยกส่วนคอมพิวเตอร์ระหว่างระบบพัฒนาหรือระบบทดสอบออกจากระบบงานจริง	มีการแบ่งแยกระบบงานพัฒนาหรือระบบงานทดสอบออกจากระบบงานที่ใช้จริง	มีการแบ่งแยกระบบงานพัฒนาออกจากระบบงานที่ทดสอบและระบบงานที่ใช้งานจริง
4.14	มีการสื่อสารการเปลี่ยนแปลงให้ผู้ใช้งานที่เกี่ยวข้องได้รับทราบอย่างทั่วถึง เพื่อให้สามารถใช้งานได้อย่างถูกต้อง	ซื้อโปรแกรมสำเร็จรูปที่ไม่สามารถเปลี่ยนแปลงแก้ไขระบบงานหรือใช้โปรแกรมที่พัฒนาโดยกรมตรวจบัญชีสหกรณ์	ไม่มีการสื่อสารการเปลี่ยนแปลงให้ผู้ใช้งานทราบ	มีการสื่อสารการเปลี่ยนแปลงให้ผู้ใช้งานอย่างไม่เป็นทางการ	มีการสื่อสารการเปลี่ยนแปลงให้ผู้ใช้งานทุกครั้งที่มีการเปลี่ยนแปลงที่สำคัญ
	<b>ระเบียบข้อที่ 5 จัดให้มีและควบคุมดูแลเอกสารสนับสนุนการปฏิบัติงานสำหรับระบบบัญชีคอมพิวเตอร์</b>				
5.1	มีการจัดทำเอกสารด้านฐานข้อมูลที่เป็นต้องมี ได้แก่ โครงสร้างฐานข้อมูล (Data Structure) หรือ พจนานุกรมข้อมูล (Data Dictionary)		ไม่มีการจัดทำเอกสารด้านฐานข้อมูล	มีการจัดทำเอกสารด้านฐานข้อมูลแต่ไม่ครอบคลุมทุกระบบ	มีการจัดทำเอกสารด้านฐานข้อมูลและครอบคลุมทุกระบบของสหกรณ์
5.2	มีการจัดทำเอกสารเกี่ยวกับคู่มือการใช้ระบบงาน		ไม่มีการจัดทำ	มีการจัดทำเอกสาร	มีการจัดทำเอกสาร



ลำดับ ที่	รายการ	ระดับการควบคุม			
		N/A	น้อย	ปานกลาง	มาก
	สำหรับผู้ใช้งาน		คู่มือระบบงาน	เกี่ยวกับคู่มือระบบงานแต่ไม่ครอบคลุมทุกระบบ	เกี่ยวกับคู่มือระบบงานและครอบคลุมทุกระบบของสหกรณ์
5.3	มีการจัดเก็บเอกสารสนับสนุนการปฏิบัติงานสำหรับระบบบัญชีคอมพิวเตอร์อยู่ในรูปแบบของ Hard Copy หรืออยู่ในรูปแบบอิเล็กทรอนิกส์		ไม่มีการจัดเก็บเอกสาร	มีการจัดเก็บเอกสารสนับสนุนการปฏิบัติงานจำนวน 1 ชุด	มีการจัดเก็บเอกสารสนับสนุนการปฏิบัติงานมากกว่า 1 ชุดและจัดเก็บไว้ในสถานที่เพื่อไว้ใช้ในกรณีฉุกเฉิน
5.4	มีการปรับปรุงเอกสารสนับสนุนการปฏิบัติงานสำหรับระบบบัญชีคอมพิวเตอร์ให้เป็นปัจจุบันอย่างสม่ำเสมอ		ไม่มีการปรับปรุงเอกสารอย่างสม่ำเสมอ	มีการปรับปรุงเอกสารแต่ไม่ครอบคลุมทุกระบบที่มีการเปลี่ยนแปลง	มีการปรับปรุงเอกสารและครอบคลุมทุกระบบที่มีการเปลี่ยนแปลง
5.5	มีการจัดเก็บเอกสารสนับสนุนการปฏิบัติงานสำหรับระบบบัญชีให้อยู่ในสถานที่ที่ปลอดภัยและสามารถเรียกใช้งานได้		ไม่มีการจัดเก็บเอกสาร	มีการจัดเก็บเอกสารกระจาย	มีการจัดเก็บเอกสารไว้ในที่ปลอดภัยและสามารถเรียกใช้งานได้
	<b>ระเบียบข้อที่ 6 จะต้องสามารถเข้าถึงฐานข้อมูลระบบบัญชีคอมพิวเตอร์ได้ และสามารถนำข้อมูลออกจากฐานข้อมูลในรูปแบบที่อ่านเข้าใจได้</b>				
6.1	ฐานข้อมูลของระบบบัญชีคอมพิวเตอร์ไม่มีการเข้ารหัส (Encryption) และสามารถใช้ซอฟต์แวร์ในการดึงข้อมูลอยู่ในรูปแบบที่สามารถอ่านเข้าใจได้		มีการเข้ารหัสในฐานข้อมูลหรือไม่สามารถส่งออกข้อมูลออกมาได้	ฐานข้อมูลไม่มีการเข้ารหัสและสามารถใช้ซอฟต์แวร์ในการดึงข้อมูลเฉพาะรูปแบบที่จำกัด	ฐานข้อมูลไม่มีการเข้ารหัสและสามารถใช้ซอฟต์แวร์ในการดึงข้อมูลและส่งออกข้อมูลได้หลากหลายตามต้องการ
	ให้ตอบแยกตามระบบดังต่อไปนี้				
	6.1.1 ระบบสมาชิกและหุ้น				
	6.1.2 ระบบเงินให้กู้				
	6.1.3 ระบบเงินรับฝาก				

ลำดับ ที่	รายการ	ระดับการควบคุม			
		N/A	น้อย	ปานกลาง	มาก
	6.1.4 ระบบสินค้า				
	6.1.5 ระบบบัญชีแยกประเภท				
	6.1.6				
	6.1.7				
	6.1.8				
	6.1.9				
6.2	มีการกำหนดรหัสผู้ใช้และรหัสผ่านในการเข้าถึงฐานข้อมูลอย่างรัดกุม เพื่อป้องกันการเปลี่ยนแปลงแก้ไขข้อมูลที่ฐานข้อมูลโดยตรง		ไม่มีการกำหนดรหัสผู้ใช้และรหัสผ่าน	มีการกำหนดรหัสผู้ใช้และรหัสผ่านแต่ไม่ได้จำกัดจำนวนผู้ใช้งานในการเข้าถึงฐานข้อมูล	มีการกำหนดรหัสผู้ใช้และรหัสผ่านรวมทั้งจำกัดจำนวนผู้ใช้งานเพียง 1 รหัสเท่านั้น
6.3	มีการอนุมัติการเข้าถึงฐานข้อมูลเพื่อเปลี่ยนแปลงแก้ไขข้อมูลโดยตรงจากผู้บริหารของสหกรณ์อย่างเหมาะสม		ไม่มีการอนุมัติการเข้าถึงฐานข้อมูลเพื่อเปลี่ยนแปลงแก้ไขข้อมูล	มีการอนุมัติการเข้าถึงฐานข้อมูลแต่ไม่ถือปฏิบัติอย่างเคร่งครัด	มีการอนุมัติการเข้าถึงฐานข้อมูลและถือปฏิบัติอย่างเคร่งครัด
6.4	มีการเปิดการบันทึกเหตุการณ์หรือ Log สำหรับการเข้าถึงฐานข้อมูลของระบบบัญชีคอมพิวเตอร์	ไม่มีบุคลากรในการวิเคราะห์หรือสอบถามเหตุการณ์หรือ Log ของฐานข้อมูล	ไม่มีการเปิดการบันทึกเหตุการณ์หรือ Log สำหรับการเข้าถึงฐานข้อมูล	มีการเปิดการบันทึกเหตุการณ์หรือ Log สำหรับการเข้าถึงฐานข้อมูลแต่ไม่มีการสอบถามอย่างสม่ำเสมอ	มีการเปิดการบันทึกเหตุการณ์หรือ Log สำหรับการเข้าถึงฐานข้อมูลและมีการสอบถามอย่างสม่ำเสมอ
	ระเบียบข้อที่ 7 จัดให้มีสำรองข้อมูลของระบบบัญชีคอมพิวเตอร์เพื่อให้สามารถรองรับการประกอบธุรกิจได้อย่างต่อเนื่อง มีประสิทธิภาพและทันเหตุการณ์ ตลอดจนจัดให้มีการดูแลรักษาข้อมูลชุดสำรองให้มีความปลอดภัย รวมทั้งจัดให้มีการป้องกันมิให้มีการนำข้อมูลสำรองมาใช้โดยไม่ถูกต้อง				
7.1	มีการกำหนดขั้นตอนหรือวิธีปฏิบัติในการสำรองข้อมูลโดยครอบคลุมรายละเอียดอย่างน้อยดังนี้ <ul style="list-style-type: none"> <li>● ข้อมูลที่ต้องสำรองและความถี่ในการสำรอง</li> <li>● ประเภทสื่อบันทึก</li> <li>● จำนวนที่ต้องสำรอง</li> </ul>		ไม่มีการกำหนดขั้นตอนในการสำรองข้อมูล	มีการกำหนดขั้นตอนการสำรองข้อมูลแต่ยังไม่ครอบคลุมรายละเอียดที่	มีการกำหนดขั้นตอนการสำรองข้อมูลและครอบคลุมรายละเอียดที่

ลำดับ ที่	รายการ	ระดับการควบคุม			
		N/A	น้อย	ปานกลาง	มาก
	<ul style="list-style-type: none"> <li>ขั้นตอนและวิธีการสำรองข้อมูลโดยละเอียด</li> <li>สถานที่และวิธีการเก็บรักษาสื่อบันทึก</li> </ul>			จำเป็น	ครบถ้วน
7.2	มีการสำรองข้อมูลหรือรายการบัญชีของระบบบัญชีคอมพิวเตอร์อย่างน้อยวันละครั้งและเป็นประจำสม่ำเสมอ		ไม่มีการสำรองข้อมูล	มีการสำรองข้อมูลแต่ไม่ได้ทำเป็นประจำสม่ำเสมอ	มีการสำรองข้อมูลวันละครั้งและเป็นประจำสม่ำเสมอ
7.3	มีการสำรองโปรแกรมระบบปฏิบัติการ (Operating System) โปรแกรมระบบบัญชีคอมพิวเตอร์ และชุดคำสั่งที่ใช้ในการทำงานของโปรแกรม อย่างน้อยเดือนละครั้งหรือเมื่อมีการเปลี่ยนแปลงแก้ไขโปรแกรมให้สามารถพร้อมใช้งานได้		ไม่มีการสำรองโปรแกรม	มีการสำรองโปรแกรมแต่ไม่ครอบคลุมทุกโปรแกรมที่สำคัญ	มีการสำรองโปรแกรมเดือนละครั้งและครอบคลุมทุกโปรแกรมที่สำคัญ
7.4	มีการเก็บรักษาสื่อสำรองข้อมูลไว้ที่ปลอดภัยทั้งในและนอกสถานที่ของสหกรณ์ เพื่อความปลอดภัยในกรณีที่สถานที่ปฏิบัติงานได้รับความเสียหาย		ไม่มีการเก็บรักษาสื่อสำรองข้อมูลหรือจัดเก็บกระจาย	มีการเก็บสื่อสำรองข้อมูลไว้ในที่ปลอดภัยเฉพาะในสถานที่สหกรณ์	มีการเก็บสื่อสำรองข้อมูลไว้ในที่ปลอดภัยทั้งในและนอกสถานที่สหกรณ์
7.5	มีการทดสอบข้อมูลที่สำรองอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่าได้ข้อมูลรวมทั้งโปรแกรมระบบต่าง ๆ ที่ได้สำรองไว้ มีความถูกต้องครบถ้วนและใช้งานได้		ไม่มีการทดสอบข้อมูลที่สำรอง	มีการทดสอบข้อมูลที่สำรองน้อยกว่าปีละครั้ง	มีการทดสอบข้อมูลที่สำรองปีละครั้ง
7.6	มีการกำหนดระยะเวลาการสำรองข้อมูลสำหรับการอ้างอิงในอนาคต เช่น การตรวจสอบทางภาษี หรือการค้นหารายการบัญชีย้อนหลังให้เหมาะสม และสื่อที่ใช้ในการสำรองว่ามีความคงทนและสามารถเรียกข้อมูลกลับมาใช้ได้ในอนาคต		ไม่มีการคำนึงถึงระยะเวลาการสำรองข้อมูลสำหรับการอ้างอิงในอนาคต	มีการกำหนดระยะเวลาการสำรองข้อมูลสำหรับการอ้างอิงในอนาคตแต่ยังไม่ถือปฏิบัติ	มีการกำหนดระยะเวลาการสำรองข้อมูลสำหรับการอ้างอิงในอนาคตและถือปฏิบัติ
7.7	มีการติดฉลากที่มีรายละเอียดที่ชัดเจนไว้บนสื่อสำรองข้อมูล เพื่อให้สามารถค้นหาได้เร็วและเพื่อป้องกันการใช้งานสื่อบันทึกผิดพลาด		ไม่มีการติดฉลากไว้บนสื่อสำรองข้อมูล	มีการติดฉลากแต่รายละเอียดไม่ชัดเจนไว้บนสื่อสำรองข้อมูล	มีการติดฉลากที่มีรายละเอียดที่ชัดเจนไว้บนสื่อสำรองข้อมูล
7.8	มีการจัดทำแผนสำรองฉุกเฉินอย่างเป็นลายลักษณ์อักษร โดยครอบคลุมรายละเอียดอย่างน้อยดังนี้ <ul style="list-style-type: none"> <li>จัดลำดับความสำคัญของระบบงานที่อยู่ในแผนสำรองฉุกเฉิน</li> <li>กำหนดสถานการณ์หรือลำดับความรุนแรงของปัญหาที่อาจเกิดขึ้น</li> </ul>	สำหรับสหกรณ์ที่มีสาขาหรือระบบ on-line กับหน่วยงานภายนอก	ไม่มีการจัดทำแผนสำรองฉุกเฉิน	มีการจัดทำแผนสำรองฉุกเฉินแต่รายละเอียดไม่เพียงพอ	มีการจัดทำแผนสำรองฉุกเฉินครอบคลุมรายละเอียดที่เพียงพอและประกาศใช้อย่าง

ลำดับ ที่	รายการ	ระดับการควบคุม			
		N/A	น้อย	ปานกลาง	มาก
	<ul style="list-style-type: none"> <li>กำหนดขั้นตอนการแก้ไขปัญหาโดยละเอียดในแต่ละสถานการณ์</li> <li>กำหนดเจ้าหน้าที่ที่รับผิดชอบ</li> <li>กำหนดรายละเอียดของอุปกรณ์คอมพิวเตอร์ที่ต้องใช้ในกรณีฉุกเฉิน</li> </ul>	สหกรณ์			เป็นทางการ
7.9	มีการทดสอบแผนสำรองฉุกเฉินอย่างน้อยปีละ 1 ครั้ง	สำหรับสหกรณ์ที่มีสาขาหรือระบบ on-line กับหน่วยงานภายนอกสหกรณ์	ไม่มีการทดสอบแผนสำรองฉุกเฉิน	มีการทดสอบแผนสำรองฉุกเฉินน้อยกว่าปีละครั้ง	มีการทดสอบแผนสำรองฉุกเฉินปีละครั้ง
7.10	มีการปรับปรุงแผนสำรองฉุกเฉินให้เป็นปัจจุบันอยู่เสมอ	สำหรับสหกรณ์ที่มีสาขาหรือระบบ on-line กับหน่วยงานภายนอกสหกรณ์	ไม่มีการปรับปรุงแผนสำรองฉุกเฉิน	มีการปรับปรุงแผนสำรองฉุกเฉินบางครั้ง	มีการปรับปรุงแผนสำรองฉุกเฉินทุกครั้งที่มีการเปลี่ยนแปลงระบบหรือพัฒนาระบบงานใหม่ที่สำคัญ
	ระเบียบข้อที่ 8 ในกรณีที่มีการใช้บริการงานเทคโนโลยีสารสนเทศของผู้ให้บริการซึ่งเป็นบุคคลภายนอก ต้องจัดให้มีหลักเกณฑ์ในการคัดเลือกและพิจารณาความเหมาะสมของผู้ให้บริการ รวมทั้งควบคุมและตรวจสอบการปฏิบัติงานของผู้ให้บริการอย่างเข้มงวด เพื่อให้มั่นใจว่า ผู้ให้บริการสามารถปฏิบัติตามระเบียบนี้ได้				
8.1	มีการกำหนดกฎเกณฑ์ในการคัดเลือกผู้ให้บริการและคัดเลือกผู้ให้บริการที่มีขั้นตอนการปฏิบัติงานที่รอบคอบรัดกุม	ไม่มีการใช้บริการจากบุคคลภายนอก	ไม่มีการกำหนดกฎเกณฑ์ในการคัดเลือกผู้ให้บริการ	มีการกำหนดกฎเกณฑ์ในการคัดเลือกผู้ให้บริการแต่ไม่ถือปฏิบัติอย่างเคร่งครัด	มีการกำหนดกฎเกณฑ์ในการคัดเลือกผู้ให้บริการและถือปฏิบัติอย่างเคร่งครัด
8.2	มีข้อสัญญาระหว่างสหกรณ์กับผู้ให้บริการซึ่งเป็นบุคคลภายนอกที่ระบุเกี่ยวกับการรักษาความลับของข้อมูลและขอบเขตงานและเงื่อนไขในการให้บริการอย่างชัดเจน	ไม่มีการใช้บริการจากบุคคลภายนอก	ไม่มีการจัดทำข้อสัญญาระหว่างสหกรณ์กับบุคคลภายนอก	มีการจัดทำข้อสัญญาระหว่างสหกรณ์กับบุคคลภายนอกแต่ไม่รวมถึงเรื่องการ	มีการจัดทำข้อสัญญาระหว่างสหกรณ์กับบุคคลภายนอกโดยระบุเกี่ยวกับการ

ลำดับ ที่	รายการ	ระดับการควบคุม			
		N/A	น้อย	ปานกลาง	มาก
				รักษาความลับของข้อมูล	รักษาความลับและขอบเขตงานที่ชัดเจน
8.3	มีการควบคุมผู้ให้บริการอย่างเข้มงวดในการปฏิบัติตามระเบียบและวิธีการปฏิบัติงานเกี่ยวกับการรักษาความปลอดภัยของระบบงาน การพัฒนาหรือการเปลี่ยนแปลงแก้ไขระบบงาน การสำรองข้อมูลที่สหกรณ์และกลุ่มเกษตรกรได้กำหนดขึ้น	ไม่มีการใช้บริการจากบุคคลภายนอก	ไม่มีกระบวนการควบคุมการให้บริการของบุคคลภายนอก	มีกระบวนการควบคุมผู้ให้บริการเฉพาะการปฏิบัติงานให้เป็นไปตามขอบเขตงานซึ่งยังไม่ครอบคลุมถึงวิธีการปฏิบัติงานของสหกรณ์ที่ผู้ให้บริการต้องปฏิบัติตาม	มีกระบวนการควบคุมผู้ให้บริการให้ปฏิบัติตามวิธีปฏิบัติงานของสหกรณ์อย่างเคร่งครัด
8.4	มีการดำเนินการให้ผู้ให้บริการจัดทำคู่มือการปฏิบัติงานและเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้เป็นทันสมัยอยู่เสมอ	ไม่มีการใช้บริการจากบุคคลภายนอก	ไม่มีการประสานงานให้ผู้ให้บริการดำเนินการจัดทำคู่มือการปฏิบัติงานหรือเอกสารที่เกี่ยวข้อง	มีการประสานงานให้ผู้ให้บริการดำเนินการจัดทำคู่มือการปฏิบัติงานหรือเอกสารที่เกี่ยวข้องแต่ยังไม่ปรับปรุงให้เป็นทันสมัย	มีการประสานงานให้ผู้ให้บริการดำเนินการจัดทำคู่มือการปฏิบัติงานหรือเอกสารที่เกี่ยวข้องและปรับปรุงให้เป็นทันสมัยอยู่เสมอ
8.5	มีการกำหนดให้ผู้ให้บริการมีการจัดทำรายงานผลการปฏิบัติงาน ปัญหาต่าง ๆ และแนวทางแก้ไขให้แก่สหกรณ์และกลุ่มเกษตรกรอย่างน้อยเดือนละครั้ง	ไม่มีการใช้บริการจากบุคคลภายนอก	ไม่มีการจัดทำรายงานผลการปฏิบัติงานของผู้ให้บริการ	มีการจัดทำรายงานผลการปฏิบัติงานของผู้ให้บริการ แต่ไม่มีการกำหนดความถี่ในการรายงานผลอย่างชัดเจน	มีการจัดทำรายงานผลการปฏิบัติงานของผู้ให้บริการเดือนละครั้ง รวมทั้งมีการจัดประชุมเพื่อติดตามความก้าวหน้าและปัญหาต่าง ๆ
8.6	มีการกำหนดขั้นตอนในการตรวจรับงานผู้ให้บริการอย่างชัดเจนและสอดคล้องกับระเบียบปฏิบัติของสหกรณ์และกลุ่มเกษตรกร	ไม่มีการใช้บริการจากบุคคลภายนอก	ไม่มีการกำหนดขั้นตอนในการตรวจรับงานผู้ให้บริการ	มีการกำหนดขั้นตอนในการตรวจรับงานผู้ให้บริการแต่ไม่ถือปฏิบัติอย่างเคร่งครัด	มีการกำหนดขั้นตอนในการตรวจรับงานผู้ให้บริการและถือปฏิบัติอย่างเคร่งครัด

ลำดับ ที่	รายการ	ระดับการควบคุม			
		N/A	น้อย	ปานกลาง	มาก
	ระเบียบข้อที่ 9 จัดให้มีการตรวจสอบคอมพิวเตอร์โดยหน่วยงานภายในของสหกรณ์และกลุ่มเกษตรกรเองหรือโดยผู้ตรวจสอบที่เป็นบุคคลภายนอก เพื่อทำหน้าที่ตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศทุกประเภทที่อาจเกิดขึ้นได้				
9.1	มีการตรวจสอบการควบคุมทั่วไปด้านเทคโนโลยีสารสนเทศ เช่น ตรวจสอบด้านการรักษาความปลอดภัยระบบข้อมูล การรักษาความปลอดภัยทางกายภาพ เป็นต้น โดยหน่วยงานภายในหรือบุคคลภายนอก				
9.2	มีการใช้คอมพิวเตอร์ช่วยในการตรวจสอบความถูกต้องและครบถ้วนของรายการที่มีการบันทึกประมวลผลและออกรายงานในแต่ละระบบงานของระบบบัญชีคอมพิวเตอร์ โดยหน่วยงานภายในหรือบุคคลภายนอก				

#### หมายเหตุ

#### ระดับการควบคุม

N/A หมายถึง การควบคุมดังกล่าวไม่สอดคล้องกับสภาพแวดล้อมการดำเนินงานของสหกรณ์

น้อย หมายถึง ไม่มีระเบียบขั้นตอนและการควบคุมอย่างเป็นทางการ

ปานกลาง หมายถึง มีระเบียบ ขั้นตอน และการควบคุม แต่ยังมีได้ถือปฏิบัติอย่างต่อเนื่อง หรือมีการควบคุมที่ควรปรับปรุง

มาก หมายถึง มีระเบียบ ขั้นตอน และการควบคุมอย่างเหมาะสมและมีการปฏิบัติตามอย่างสม่ำเสมอ