ที่ กษ ๑๑๑๕/๑๑๔๑

ถึง สำนักงานส่งเสริมสหกรณ์กรุงเทพมหานคร พื้นที่ ๑ - ๒, สำนักงานสหกรณ์จังหวัดทุกจังหวัด

ด้วยกรมตรวจบัญชีสหกรณ์มีหนังสือแจ้งมาตรการสร้างความตระหนักในการกำกับติดตามและควบคุมระบบการควบคุมภายในด้านเทคโนโลยีสารสนเทศจากการใช้โปรแกรมระบบบัญชีคอมพิวเตอร์ที่มีความเสี่ยงและไม่ปลอดภัย เพื่อให้สหกรณ์และกลุ่มเกษตรกรมีมาตราการหลักเกณฑ์ที่ปลอดภัยทางสารสนเทศที่กรมตรวจบัญชีสหกรณ์กำหนดให้เกิดความรัดกุมยิ่งขึ้น และสร้างความโปร่งใสแก่สหกรณ์ต่อไป กรมส่งเสริมสหกรณ์จึงขอส่งหนังสือกรมตรวจบัญชีสหกรณ์ดังกล่าว เพื่อใช้เป็นแนวทางในการปฏิบัติงานต่อไป รายละเอียดตามเอกสารแนบท้ายหนังสือนี้

กรมส่งเสริมสหกรณ์
๑๐ มิถุนายน ๒๕๖๘

เรียน ผู้อำนวยการสำนักงานส่งเสริมสหกรณ์กรุงเทพมหานคร พื้นที่ ๒

- ☐ เพื่อโปรดทราบ
- ☑ เพื่อโปรดพิจารณา เห็นควรแจ้ง กสส.๑ - กสส.๗ และลงเว็บไซต์ สำนักงานฯ กรุงเทพมหานคร ทุกเขต ๑๔.
- ☐ เพื่อโปรดพิจารณาลงนาม

สำนักนายทะเบียนและกฎหมาย
โทร. ๐ ๒๒๘๒ ๕๐๔๒
ไปรษณีย์อิเล็กทรอนิกส์ saraban@cpd.go.th

(นางสาวกมลวรรณ นุชัย)
ผู้อำนวยการสำนักงานส่งเสริมสหกรณ์กรุงเทพมหานคร พื้นที่ ๒

บันทึกข้อความ

ส่วนราชการ กรมตรวจบัญชีสหกรณ์ สำนักมาตรฐานการบัญชีและการสอบบัญชี โทร. ๐ ๒๒๘๒ ๕๘๘๖

ที่ กษ ๐๔๐๔/ ๙๔๒ **วันที่** ๒๘ พฤษภาคม ๒๕๖๘

เรื่อง มาตรการสร้างความตระหนักในการกำกับควบคุมและสอบทานระบบการควบคุมภายในด้านเทคโนโลยีและกฎหมาย สารสนเทศจากการใช้โปรแกรมระบบบัญชีคอมพิวเตอร์ที่มีความเสี่ยงและไม่ปลอดภัย

เรียน อธิบดีกรมส่งเสริมสหกรณ์

ด้วยสถานการณ์ปัจจุบันสหกรณ์และกลุ่มเกษตรกรได้นำเทคโนโลยีมาใช้ในการบริหารจัดการกิจการอย่างแพร่หลาย จากการตรวจสอบบัญชี พบว่า มีสหกรณ์หลายแห่งที่ใช้โปรแกรมระบบบัญชีคอมพิวเตอร์ที่พัฒนาขึ้นเองหรือจัดจ้างผู้ให้บริการภายนอก หรือจัดซื้อโปรแกรมสำเร็จรูปที่พัฒนาโดยบริษัทเอกชน โดยไม่มีระบบควบคุมการเข้าถึงหรือการแก้ไขข้อมูลที่รัดกุม ทำให้เกิดความเสี่ยงด้านความมั่นคงปลอดภัยของข้อมูล และมีบางกรณีเกิดการทุจริตจากการตกแต่งข้อมูลโดยโปรแกรมเมอร์หรือบุคคลที่เกี่ยวข้องกับระบบสารสนเทศของสหกรณ์

กรมตรวจบัญชีสหกรณ์ พิจารณาว่าการทุจริตด้านสารสนเทศทางบัญชี (Accounting Information System : AIS) ผ่านโปรแกรมสารสนเทศด้านการบัญชีของสหกรณ์ กระทำโดยบุคคลผู้ไม่มีสิทธิ์เข้าถึงระบบ และไม่ได้รับอนุญาตจากผู้มีอำนาจ รวมทั้งมีการแก้ไข ลบการบันทึกรายการบัญชีอย่างไร้ร่องรอยอันถือเป็นการละเมิดมาตรฐานการบัญชี และมาตรฐานการควบคุมภายในที่ดีรวมทั้งเป็นทางที่ทำให้สหกรณ์และสมาชิกได้รับความเสียหาย ในฐานะหน่วยงานที่ตรวจสอบบัญชีและกำหนดมาตรฐานด้านการบัญชี จึงเห็นความสำคัญในการให้สหกรณ์และกลุ่มเกษตรกรปฏิบัติตามหลักเกณฑ์มาตรฐานด้านการบัญชี การควบคุมภายในด้านสารสนเทศที่ดีและให้ผู้มีหน้าที่รับผิดชอบให้ความสำคัญด้านความเสี่ยงและการป้องกันข้อมูลการบัญชีของสหกรณ์ให้ถูกต้องโปร่งใส จึงได้กำหนดมาตรการสร้างความตระหนักในการกำกับควบคุมและสอบทานระบบการควบคุมภายในด้านเทคโนโลยีสารสนเทศจากการใช้โปรแกรมระบบบัญชีคอมพิวเตอร์ที่มีความเสี่ยงและไม่ปลอดภัยให้เป็นไปตามแนวทางของระเบียบนายทะเบียนสหกรณ์ ว่าด้วยมาตรฐานขั้นต่ำในการควบคุมภายในและการรักษาความปลอดภัยสำหรับสหกรณ์และกลุ่มเกษตรกรที่ใช้โปรแกรมระบบบัญชีคอมพิวเตอร์ประมวลผลข้อมูล พ.ศ. ๒๕๕๓ และหนังสือ ที่ กษ ๐๔๐๔/ว ๔๑ เรื่อง มาตรการการควบคุมภายในที่ดีด้านเทคโนโลยีสารสนเทศสำหรับสหกรณ์และกลุ่มเกษตรกร โดยมุ่งหวังให้สหกรณ์และกลุ่มเกษตรกรมีมาตรการหลักเกณฑ์ที่ปลอดภัยทางสารสนเทศที่กรมตรวจบัญชีสหกรณ์กำหนดให้เกิดความรัดกุมยิ่งขึ้น และสร้างความโปร่งใสแก่สหกรณ์ต่อไป ตามรายละเอียดที่แนบมาพร้อมนี้ จึงแจ้งเพื่อประโยชน์ในการบูรณาการการกำกับดูแล และสนับสนุนส่งเสริมการดำเนินการของสหกรณ์และกลุ่มเกษตรกรที่โปร่งใสต่อไป

จึงเรียนมาเพื่อโปรดทราบ

(นายวิณะโรจน์ ทรัพย์ส่งสุข)
อธิบดีกรมตรวจบัญชีสหกรณ์

มาตรการสร้างความตระหนักในการกำกับติดตามและควบคุมระบบการควบคุมภายในด้านเทคโนโลยีสารสนเทศจากการใช้โปรแกรมระบบบัญชีคอมพิวเตอร์ที่มีความเสี่ยงและไม่ปลอดภัย

กรมตรวจบัญชีสหกรณ์ ได้กำหนดมาตรการควบคุมภายในด้านเทคโนโลยีสารสนเทศสำหรับสหกรณ์ ได้แก่ (๑) ระเบียบนายทะเบียนสหกรณ์ ว่าด้วยมาตรฐานขั้นต่ำในการควบคุมภายในและการรักษาความปลอดภัยสำหรับสหกรณ์และกลุ่มเกษตรกรที่ใช้โปรแกรมระบบบัญชีคอมพิวเตอร์ประมวลผล พ.ศ. ๒๕๕๓ ลงวันที่ ๑๗ ธันวาคม ๒๕๕๓ เพื่อให้สหกรณ์และกลุ่มเกษตรกรมีการนำระบบโปรแกรมบัญชีคอมพิวเตอร์มาใช้ในการประมวลผลข้อมูลทางการบัญชีและจัดทำงบการเงิน เพื่อป้องกันความเสี่ยงและความเสียหายแก่ระบบสารสนเทศของสหกรณ์และกลุ่มเกษตรกร โดยระบุวิธีปฏิบัติเกี่ยวกับการกำหนดนโยบาย ระเบียบปฏิบัติ การรักษาความปลอดภัยทางกายภาพ การรักษาความปลอดภัยของข้อมูล การพัฒนาและการแก้ไขเปลี่ยนแปลง และการสื่อสารที่ถูกต้องครบถ้วนเพื่อให้ผู้สอบบัญชี และสหกรณ์ถือปฏิบัติ และ (๒) มาตรการควบคุมภายในที่ดีด้านเทคโนโลยีสารสนเทศ สำหรับสหกรณ์และกลุ่มเกษตรกร ตามหนังสือ ที่ กษ ๐๔๐๔/ว ๔๑ ลงวันที่ ๒๘ มิถุนายน ๒๕๖๖ เพื่อให้สอดคล้องกับสถานการณ์ปัจจุบันที่เปลี่ยนแปลงไป โดยระบุถึงมาตรการด้านการควบคุมด้านกายภาพ การควบคุมการเข้าถึงระบบงาน การควบคุมข้อมูลและฐานข้อมูล การควบคุม กำกับ และติดตาม การผลักดันสมาชิกให้ความสำคัญกับการตรวจสอบข้อมูลการทำธุรกรรมของตนเองกับสหกรณ์เป็นสำคัญ

ด้วยสถานการณ์การทุจริตด้านสารสนเทศทางบัญชี (Accounting Information System : AIS) เกิดจากการแก้ไข ลบ ปกปิด รายการบัญชีเพื่อยักยอกรายการเงินฝาก เบิกถอนเงินฝาก หรือเพิ่มจำนวนเงินกู้ของสมาชิกเกินกว่าความเป็นจริง โดยผู้ไม่มีสิทธิ์เข้าถึงระบบ และไม่ได้รับอนุญาตจากผู้มีอำนาจ จากการใช้สิทธิ์ของผู้มีอำนาจโดยมิชอบ หรือการทำธุรกรรมเงินสดโดยไม่ได้รับอนุญาต โดยปลอมแปลงเพื่อโอนเงินเข้าบัญชีบุคคลอื่นหรือตนเองหรือรับฝากเงินสมาชิกโดยไม่บันทึกบัญชี หรือบันทึกแล้วลบรายการออกจากบัญชีโดยไม่มีอำนาจกระทำ รวมทั้งการเข้าระบบโปรแกรมเพื่อแก้ไข ลบการบันทึกรายการบัญชีอย่างไร้ร่องรอย กรมตรวจบัญชีสหกรณ์ ในฐานะหน่วยงานที่ตรวจสอบบัญชีและให้คำแนะนำด้านการบัญชีที่ดีแก่สหกรณ์และกลุ่มเกษตรกร จึงเห็นความสำคัญในการให้สหกรณ์ปฏิบัติตามหลักเกณฑ์มาตรฐานด้านการบัญชีสารสนเทศที่ดีและให้ผู้มีหน้าที่รับผิดชอบเห็นถึงความเสี่ยงและการป้องกันข้อมูลการบัญชีของสหกรณ์ให้ถูกต้องโปร่งใส รวมถึงการป้องกันปัญหาที่ยังคงเกิดขึ้น ได้แก่ การฝ่าฝืนมาตรฐานการควบคุมภายในที่ดีด้านสารสนเทศทางการบัญชี อันเป็นการละเมิดการเข้าถึงการแก้ไขปรับเปลี่ยนข้อมูล การกระทำผิดโดยเจ้าหน้าที่ของสหกรณ์และหรือบุคคลภายนอกที่เกี่ยวข้องกับโปรแกรมของสหกรณ์โดยไม่ได้รับความเห็นชอบหรือกระทำไปโดยฝ่าฝืนเงื่อนไข ข้อบังคับ ระเบียบสหกรณ์ รวมถึงหลักเกณฑ์ที่นายทะเบียนสหกรณ์และกรมตรวจบัญชีสหกรณ์กำหนดข้างต้น จึงได้จัดทำมาตรการกำกับติดตามและควบคุมระบบการควบคุมภายในด้านเทคโนโลยีสารสนเทศจากการใช้โปรแกรมระบบบัญชีคอมพิวเตอร์ที่มีความเสี่ยงและไม่ปลอดภัยโดยให้สหกรณ์พิจารณาสาระสำคัญเพื่อเสริมสร้างระบบการควบคุมภายในด้านเทคโนโลยีสารสนเทศ เพื่อป้องกันความเสี่ยงและเกิดความปลอดภัยจากการใช้โปรแกรมระบบบัญชีคอมพิวเตอร์ที่พัฒนาขึ้นเองหรือจัดจ้างผู้ให้บริการภายนอก โดยให้สหกรณ์และกลุ่มเกษตรกรกำกับ กวดขัน ตรวจสอบ ควบคุมการปฏิบัติให้เป็นไปตามข้อบังคับ ระเบียบสหกรณ์และกลุ่มเกษตรกร และมาตรการหลักเกณฑ์ที่ปลอดภัยทางสารสนเทศที่กรมตรวจบัญชีสหกรณ์กำหนดให้เกิดความรัดกุมยิ่งขึ้น ซึ่งมีสาระสำคัญภายใต้กรอบ “มาตรการ ๘ ประการ” ดังต่อไปนี้

มาตรการ ๘ ประการ

๑. มาตรการแบ่งแยกหน้าที่เพื่อความโปร่งใส

สหกรณ์ต้องกำหนดกระบวนการที่เกี่ยวข้องกับการบันทึกข้อมูล การอนุมัติ และการตรวจสอบ ให้ดำเนินการโดยบุคคลหรือหน่วยงานที่แยกออกจากกันอย่างชัดเจนให้สอดคล้องกับหน้าที่ความรับผิดชอบของแต่ละตำแหน่งงาน เพื่อป้องกันมิให้บุคคลใดบุคคลหนึ่งหรือกลุ่มใดกลุ่มหนึ่งมีอำนาจควบคุมกระบวนการทั้งหมดแต่เพียงฝ่ายเดียว ซึ่งอาจนำไปสู่ความเสี่ยงในการกระทำทุจริต ทั้งนี้ ต้องมีการกำกับ ควบคุม ติดตาม และประเมินผลการปฏิบัติหน้าที่ให้เป็นไปตามที่ได้รับมอบหมายเป็นประจำอย่างเคร่งครัด

๒. มาตรการกำหนดสิทธิ์การเข้าถึงระบบตามบทบาท (Role-Based Access Control)

มาตรการควบคุมการเข้าถึงระบบ สหกรณ์ต้องจัดให้มีการกำหนดสิทธิ์การเข้าถึงระบบงานและข้อมูลเฉพาะผู้มีหน้าที่เกี่ยวข้อง โดยใช้หลักการควบคุมตามบทบาทหน้าที่ ลดโอกาสที่บุคคลภายนอกหรือโปรแกรมเมอร์เข้าถึงระบบงานและข้อมูลโดยไม่ได้รับอนุญาต รวมทั้งสหกรณ์ต้องมีการกำกับติดตามการปฏิบัติให้เป็นไปตามสิทธิ์ที่กำหนด

มาตรการอนุมัติการแก้ไข ยกเลิก เพิ่มเติมข้อมูล ทุกครั้งที่สหกรณ์มีการแก้ไขหรือปรับปรุงข้อมูลในระบบ ต้องได้รับความเห็นชอบจากผู้มีอำนาจ ซึ่งต้องเป็นผู้ที่ได้รับมอบหมายเป็นลายลักษณ์อักษร และต้องบันทึกรายละเอียดการแก้ไขข้อมูลไว้ เช่น ใครเป็นผู้แก้ไข แก้ไขเมื่อใด แก้ไขอะไร และเหตุใดจึงแก้ไข เพื่อให้สามารถตรวจสอบย้อนหลังได้หากเกิดปัญหา และป้องกันไม่ให้มีการแก้ไขข้อมูลโดยพลการ

๓. มาตรการรักษาความปลอดภัยข้อมูลชุดสำรอง สหกรณ์ต้องจัดให้มีระบบการเก็บรักษาข้อมูลชุดสำรอง (Backup Data) อย่างปลอดภัย ทั้งในสถานที่ตั้งของสหกรณ์และสถานที่สำรองภายนอก โดยต้องมีมาตรการควบคุมที่เข้มงวดเพื่อป้องกันมิให้ข้อมูลดังกล่าวถูกเข้าถึง แก้ไข หรือเรียกคืนมาใช้งานโดยมิชอบ เช่น การกำหนดสิทธิ์การเข้าถึงข้อมูลชุดสำรองเฉพาะเจ้าหน้าที่ที่ได้รับอนุญาตเท่านั้น การเข้ารหัสข้อมูลชุดสำรองเพื่อป้องกันการเข้าถึงจากบุคคลภายนอก รวมทั้งการจัดเก็บในระบบที่มีการป้องกันความเสี่ยงจากภัยคุกคามทางไซเบอร์ กำหนดให้มีระบบบันทึกประวัติการเข้าใช้งานและการดำเนินการในระบบสารสนเทศ (Audit Log) และกำหนดขั้นตอนและเงื่อนไขการเรียกคืนข้อมูลชุดสำรองที่ชัดเจน เช่น ต้องได้รับอนุมัติจากผู้มีอำนาจ และต้องมีการบันทึกเหตุผล รายละเอียด และผลกระทบของการเรียกคืนข้อมูลทุกครั้ง ทั้งนี้ เพื่อให้การจัดเก็บและการเรียกใช้ข้อมูลชุดสำรองเป็นไปอย่างโปร่งใส ตรวจสอบได้ และไม่ถูกนำมาใช้เพื่อการแก้ไขข้อมูลโดยมิชอบ หรือเพื่อปกปิดและอำพรางการกระทำผิด

๔. มาตรการติดตามและประเมินผล สหกรณ์ต้องจัดให้มีกระบวนการติดตาม ตรวจสอบ และประเมินผลการดำเนินงานด้านเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ เพื่อให้มั่นใจว่ามีการปฏิบัติตามกฎหมาย ระเบียบและมาตรฐานที่เกี่ยวข้องอย่างต่อเนื่องและสามารถปรับปรุงนโยบายหรือแนวทางการควบคุมภายในให้สอดคล้องกับความเสี่ยงที่เปลี่ยนแปลงไปการประเมินผลควรครอบคลุมประเด็นสำคัญ ได้แก่ การควบคุมทั่วไปของระบบสารสนเทศ (IT General Controls) การควบคุมเฉพาะระบบงาน (Application Controls) การประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ และการปฏิบัติตามระเบียบ ข้อบังคับ และหลักธรรมาภิบาล โดยผลการประเมินต้องถูกนำไปใช้ในการปรับปรุงระบบ นโยบาย และแนวทางการบริหารจัดการด้านเทคโนโลยีสารสนเทศให้เหมาะสมและทันสมัยอยู่เสมอ

๕. มาตรการเสริมความรู้ สร้างเสริมวินัยด้านดิจิทัล และบทลงโทษ สหกรณ์ต้องส่งเสริมและสนับสนุนให้กรรมการและเจ้าหน้าที่ได้รับความรู้หรือได้รับการฝึกอบรมเกี่ยวกับการป้องกันความเสี่ยงด้านเทคโนโลยีสารสนเทศ การใช้งานระบบอย่างปลอดภัย และการรักษาความลับของข้อมูลสมาชิก สร้างวัฒนธรรมองค์กรที่ตระหนักรู้และป้องกันภัยคุกคามจากเทคโนโลยีสารสนเทศ การปฏิบัติตามข้อบังคับ ระเบียบสหกรณ์ และหลักเกณฑ์ที่กรมตรวจบัญชีสหกรณ์กำหนด รวมทั้งต้องตระหนักรู้ถึงบทลงโทษ และความผิดตามวินัยเจ้าหน้าที่และกฎหมายความรับผิดที่เกี่ยวข้อง

๖. มาตรการปฏิบัติงานกับผู้ให้บริการโปรแกรมสารสนเทศทางบัญชี ในกรณีที่มีการใช้บริการงานเทคโนโลยีสารสนเทศจากผู้ให้บริการภายนอก สหกรณ์ต้องคัดเลือกผู้ให้บริการตามความสามารถและความเชี่ยวชาญ มีความรับผิดชอบอย่างเหมาะสม มีการจัดทำสัญญาว่าจ้างที่ต้องระบุเกี่ยวกับสิทธิ์ในการเข้าถึงข้อมูลของสหกรณ์ การรักษาความลับข้อมูล ขอบเขตงาน และเงื่อนไขในการให้บริการตามกฎหมายความปลอดภัยทางเทคโนโลยีกำหนดอย่างชัดเจน เช่น PDPA ควรมีบทลงโทษหรือแนวทางดำเนินคดีหากผู้ให้บริการหรือบุคคลในสังกัดของผู้ให้บริการไม่ปฏิบัติตามสัญญาและหลักเกณฑ์เกี่ยวกับความปลอดภัยทางเทคโนโลยีที่เกี่ยวข้องทำให้สหกรณ์ได้รับความเสียหาย รวมทั้งสหกรณ์ต้องกำกับ ควบคุมมิให้เจ้าหน้าที่ของสหกรณ์ประสานงานกับผู้ให้บริการเพื่อแก้ไขดัดแปลงนอกเหนือสัญญาโดยไม่ได้รับความเห็นชอบจากผู้มีอำนาจ

๗. มาตรการประเมินความเสี่ยง และสร้างความปลอดภัยด้านเทคโนโลยีสารสนเทศ สหกรณ์ต้องเสริมสร้างความมั่นคงและความพร้อมใช้งานของระบบบัญชีคอมพิวเตอร์อย่างต่อเนื่อง โดยกำหนดให้มีการตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ รวมถึงการตรวจสอบความถูกต้องของข้อมูล การประมวลผล และระบบรักษาความปลอดภัยของข้อมูล ทั้งนี้ สหกรณ์ต้องกำหนดผู้รับผิดชอบในการตรวจสอบประเมินความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศอย่างชัดเจน ซึ่งอาจมอบหมายให้บุคลากรภายในที่มีความรู้ความเชี่ยวชาญเป็นผู้ดำเนินการ หรือจัดจ้างผู้ตรวจสอบอิสระจากภายนอก โดยการตรวจสอบต้องดำเนินการเป็นประจำเพื่อให้สามารถประเมินประสิทธิภาพของระบบ ค้นหาความบกพร่องหรือช่องโหว่ และดำเนินการแก้ไขปรับปรุงได้อย่างทันท่วงที เพื่อให้ระบบสามารถรองรับการดำเนินงานได้อย่างต่อเนื่อง ปลอดภัย และเชื่อถือได้

๘. มาตรการกำหนดช่องทางการร้องเรียนการทุจริตภายในสหกรณ์ โดยแจ้งถึงประธานกรรมการสหกรณ์โดยตรง เช่น หมายเลขโทรศัพท์ , Appication Line , E – Mail และสำเนาถึงสำนักงานตรวจบัญชีสหกรณ์ในพื้นที่ตั้งของสหกรณ์ สำนักงานส่งเสริมสหกรณ์ในพื้นที่ตั้งของสหกรณ์ โดยมิให้บุคคลภายในสหกรณ์ผู้ใดรับรู้และให้ถือกำหนดเป็นความลับ เพื่อป้องกันและคุ้มครองบุคคลมิให้ต้องได้รับภยันอันตรายจากการแจ้งเหตุนั้น

.....