

มาตรการสร้างความตระหนักในการกำกับติดตามและควบคุมระบบการควบคุมภายใน
ด้านเทคโนโลยีสารสนเทศจากการใช้โปรแกรมระบบบัญชีคอมพิวเตอร์ที่มีความเสี่ยงและไม่ปลอดภัย
สหกรณ์ออมทรัพย์ฐานทัพเรือสัตหีบ จำกัด

เพื่อให้การใช้ระบบเทคโนโลยีสารสนเทศของสหกรณ์ออมทรัพย์ฐานทัพเรือสัตหีบ จำกัด เป็นไปอย่างเหมาะสมมีความปลอดภัย ป้องกันความเสี่ยงและความเสียหายแก่ระบบสารสนเทศของสหกรณ์ สามารถสนับสนุนการดำเนินงานและให้บริการสมาชิกของสหกรณ์ได้อย่างต่อเนื่อง มีการใช้งานระบบในลักษณะที่ถูกต้องและสอดคล้องกับระเบียบสหกรณ์ฯ ว่าด้วย วิธีปฏิบัติในการควบคุมภายใน และการรักษาความปลอดภัยด้านระบบสารสนเทศของสหกรณ์ พ.ศ.๒๕๖๗ รวมถึงเพื่อให้เป็นไปตามมาตรการการควบคุมภายในที่ดีด้านเทคโนโลยีสารสนเทศสำหรับสหกรณ์ของกรมตรวจบัญชีสหกรณ์ จึงกำหนดมาตรการและวิธีการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศเพื่อกำกับดูแลและเป็นแนวทางให้ผู้ใช้งานสามารถใช้งานระบบเทคโนโลยีสารสนเทศให้มีความมั่นคงปลอดภัย ประกอบด้วย ๘ มาตรการ โดยมีรายละเอียดดังต่อไปนี้

๑. มาตรการแบ่งแยกหน้าที่เพื่อความโปร่งใส

สหกรณ์มีการกำหนดหน้าที่ความรับผิดชอบของแต่ละตำแหน่งงานแยกออกจากกัน อาทิ การบันทึกข้อมูล การอนุมัติ และการตรวจสอบ ตลอดจนมีการกำกับ ควบคุม ติดตาม ประเมินผลการปฏิบัติหน้าที่ให้เป็นไปตามที่ได้รับมอบหมายเป็นประจำ

- ผู้ใช้งานที่ทำหน้าที่ป้อนข้อมูลไม่เป็นผู้ที่มีสิทธิ์อนุมัติหรือประมวลผลข้อมูลนั้นได้ และผู้ที่มีสิทธิ์อนุมัติไม่เป็นผู้ที่สามารถเข้าถึงหรือแก้ไขข้อมูลได้โดยตรง
- ผู้ที่ทำหน้าที่ป้อนข้อมูลการทำธุรกรรม (อาทิ การฝาก ถอน โอน) ไม่เป็นผู้ที่มีสิทธิ์อนุมัติการทำธุรกรรมนั้นและผู้ที่มีสิทธิ์อนุมัติไม่เป็นผู้ที่สามารถเข้าถึงข้อมูลบัญชีของสมาชิกได้โดยตรง
- ผู้ที่ทำหน้าที่ป้อนข้อมูลสมาชิก (อาทิ การเพิ่ม แก้ไข ลบ) ไม่เป็นผู้ที่มีสิทธิ์อนุมัติการเปลี่ยนแปลงข้อมูล และผู้ที่มีสิทธิ์อนุมัติไม่เป็นผู้ที่มีสิทธิ์เข้าถึงข้อมูลทางการเงินของสมาชิก
- มีการทบทวนและปรับปรุงระบบการแบ่งแยกหน้าที่อย่างสม่ำเสมอ

๒. มาตรการกำหนดสิทธิ์การเข้าถึงระบบตามบทบาท (Role-Based Access Control)

<u>มาตรการควบคุมการเข้าถึงระบบ</u>

สหกรณ์มีการกำหนดสิทธิ์การเข้าถึงระบบและข้อมูลต่างๆ ให้เหมาะสมกับหน้าที่และขอบเขตความรับผิดชอบของแต่ละบุคคล ชัดเจน เพื่อจำกัดการเข้าถึงข้อมูล และไม่สามารถดำเนินการเกินขอบเขตที่กำหนดได้ อาทิ เจ้าหน้าที่บันทึกบัญชีไม่สามารถเข้าถึงการตั้งค่าหรือข้อมูลสมาชิกได้

- ควบคุมการเข้าถึงระบบงานโดยใช้การระบุตัวตนของผู้ใช้งานด้วย รหัสผ่าน
- กำหนดสิทธิการเข้าถึงของผู้ใช้ระบบในแต่ละคนให้สอดคล้องกับหน้าที่ความรับผิดชอบและหลักการควบคุมภายใน

/ ตรวจสอบและ...

- ตรวจสอบและทบทวนสิทธิการเข้าระบบต่างๆ สม่ำเสมอ เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

- บันทึกกิจกรรมต่างๆ ในระบบเพื่อใช้ในการตรวจสอบผู้เข้าใช้งานในระบบ รวมทั้งเวลาที่เข้าใช้เพื่อให้สามารถตรวจสอบได้

- ผู้ที่พัฒนาและปรับปรุงระบบ IT ไม่เป็นผู้ที่มีสิทธิ์ใช้งานระบบในสถานะปกติ เพื่อป้องกันการเปลี่ยนแปลงหรือแก้ไขระบบโดยไม่ได้รับอนุญาต

<u>มาตรการอนุมัติการแก้ไข ยกเลิก เพิ่มเติมข้อมูล</u>

สหกรณ์มีระบบการควบคุมภายในด้าน IT ของสหกรณ์ออมทรัพย์ ที่ชัดเจนและเป็นระบบ เพื่อให้การดำเนินการเป็นไปอย่างโปร่งใสและมีประสิทธิภาพ โดยการแก้ไข ยกเลิก เพิ่มเติมข้อมูลในระบบงานสหกรณ์ออมทรัพย์ ต้องได้รับความเห็นชอบจากผู้มีอำนาจอนุมัติ

การเสนอขออนุมัติ

- ผู้ที่ต้องการแก้ไข เพิ่มเติม หรือยกเลิกข้อมูลในระบบควบคุมภายในด้าน IT ต้องยื่นคำขอเป็นลายลักษณ์อักษรต่อผู้มีอำนาจอนุมัติ

- คำขอต้องระบุรายละเอียดของข้อมูลที่ต้องการแก้ไข เพิ่มเติม หรือยกเลิก รวมถึงเหตุผลและความจำเป็นที่ต้องดำเนินการ อาทิ ใครเป็นผู้แก้ไข แก้ไขเมื่อใด แก้ไขอะไร และสาเหตุใดจึงแก้ไข

การพิจารณาอนุมัติ

- ผู้มีอำนาจอนุมัติ หรือผู้ที่ได้รับมอบหมาย พิจารณาคำขออนุมัติ โดยคำนึงถึงความเหมาะสม ความถูกต้อง ความจำเป็น และผลกระทบที่อาจเกิดขึ้น

- อาจมีการสอบถามข้อมูลเพิ่มเติม หรือขอให้ผู้เสนอคำขอชี้แจงรายละเอียดเพิ่มเติม

- การอนุมัติ/ไม่อนุมัติ ควรมีบันทึกเป็นลายลักษณ์อักษร

การติดตามและประเมินผล

- ผู้บริหารและผู้ดูแลระบบ กำกับติดตามการปฏิบัติให้เป็นไปตามสิทธิที่กำหนด

- หลังจากดำเนินการแล้วต้องมีการติดตามและประเมินผล เพื่อให้แน่ใจว่าการแก้ไข เพิ่มเติม หรือยกเลิกข้อมูลเป็นไปตามที่ต้องการ และไม่มีผลกระทบในทางลบ

- หากพบปัญหาหรือข้อผิดพลาด ต้องมีการแก้ไขอย่างเร่งด่วน

๓. มาตรการรักษาความปลอดภัยข้อมูลสำรอง

สหกรณ์มีการกำหนดให้มีระบบสำรองข้อมูล (Backup) อย่างสม่ำเสมอและปลอดภัย ทั้งในสถานที่ตั้งสหกรณ์และสถานที่สำรองภายนอก ตลอดจนมีแผนฟื้นฟูระบบเมื่อเกิดเหตุการณ์ไม่คาดคิด

- ทำการสำรองข้อมูลระบบทุกวัน และจัดเก็บไว้ในพื้นที่ปลอดภัย

- กำหนดสิทธิเข้าถึงข้อมูลสำรองเฉพาะเจ้าหน้าที่ที่ได้รับอนุญาตเท่านั้นพร้อมใช้เทคโนโลยีการเข้ารหัส

- มีการติดตั้งระบบป้องกันภัยคุกคามทางไซเบอร์ และมี Audit Log การบันทึกประวัติการเข้าถึงและการใช้งานข้อมูล

- การเรียกคืนข้อมูลชุดสำรองต้องได้รับอนุมัติจากผู้มีอำนาจ และมีการบันทึกเหตุผลรายละเอียด

/๔. มาตรการติดตาม...

๔. มาตรการติดตามและประเมินผล

สหกรณ์มีการแต่งตั้งเจ้าหน้าที่รับผิดชอบการควบคุมติดตาม ตรวจสอบ และประเมินผลการดำเนินงานด้านเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ เพื่อให้มั่นใจว่ามีการปฏิบัติตามกฎหมาย ระเบียบและมาตรฐานที่เกี่ยวข้อง

- จัดให้มีการติดตาม ตรวจสอบ และประเมินผลการดำเนินงานด้าน IT อย่างสม่ำเสมอ
- ประเมินความสอดคล้องกับ กฎหมาย ระเบียบ มาตรฐาน และหลักธรรมาภิบาล
- ครอบคลุมถึงการควบคุมทั่วไปของระบบ, การควบคุมระบบงาน, การประเมินความเสี่ยง IT
- ผลการประเมินนำไปใช้ปรับปรุงนโยบายและแนวทางการบริหาร IT ให้สอดคล้องกับความเสี่ยงที่เปลี่ยนแปลง

๕. มาตรการเสริมสร้างความรู้ สร้างเสริมวินัยด้านดิจิทัล และบทลงโทษ

ส่งเสริมให้ผู้ปฏิบัติได้รับความรู้ คำแนะนำเกี่ยวกับความเสี่ยงด้านเทคโนโลยีสารสนเทศ อาทิ การใช้ระบบอย่างปลอดภัย การรักษาความลับของข้อมูลสมาชิก และบทลงโทษทางวินัยและกฎหมาย

- สนับสนุนให้กรรมการและเจ้าหน้าที่อบรมและพัฒนาความรู้ด้าน IT Security การใช้งานระบบและการรักษาความลับของข้อมูล
- ให้ความรู้ในการตั้งรหัสผ่านที่ปลอดภัย การอับเดตซอฟต์แวร์ และการใช้ระบบคลาวด์อย่างถูกต้อง
- ส่งเสริมวัฒนธรรมองค์กรที่ตระหนักรู้ภัยไซเบอร์ และเคารพกฎระเบียบในการใช้งานเทคโนโลยีสารสนเทศภายในองค์กร
- สื่อสารหลักจรรยาบรรณดิจิทัล และระเบียบวินัยการใช้งานเทคโนโลยีสารสนเทศภายในองค์กร
- หากเจ้าหน้าที่สหกรณ์ผู้ใดกระทำผิดหรือกระทำการใดๆ อันเป็นการฝ่าฝืนมาตรการ และวิธีการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศนี้ ให้ถือว่าผู้นั้นกระทำความผิดวินัย และจะถูกดำเนินการลงโทษทางวินัยตามหลักเกณฑ์ที่กำหนดไว้ในระเบียบสหกรณ์ฯ ว่าด้วย ข้อบังคับเกี่ยวกับการทำงาน พ.ศ.๒๕๖๕ หมวด ๖ ข้อ ๑๘. โทษทางวินัย มีดังนี้
  - ตักเตือนด้วยวาจา
  - ตักเตือนด้วยหนังสือ
  - พักงาน
  - งดเลื่อนเงินเดือนประจำปี
  - เลิกจ้าง

สหกรณ์สงวนสิทธิ์ที่จะลงโทษเจ้าหน้าที่ตามความร้ายแรงของการกระทำความผิด โดยไม่จำเป็นต้องเป็นไปตามลำดับ และหากการกระทำดังกล่าวเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ที่บังคับใช้ในปัจจุบัน ให้สหกรณ์ฯ ดำเนินการกับผู้กระทำความผิดตามกฎหมาย

๖. มาตรการปฏิบัติกับผู้ให้บริการโปรแกรมสารสนเทศทางบัญชี

สหกรณ์มีการตรวจสอบว่าผู้ให้บริการโปรแกรมระบบงานมีคุณสมบัติเหมาะสม โปรแกรมที่ใช้ได้รับใบอนุญาตถูกต้องตามกฎหมาย มีการพัฒนาระบบอย่างปลอดภัย มีการรักษาความลับข้อมูล และให้บริการตามหลัก PDPA

- จัดทำข้อตกลง (MOU/สัญญา) กับผู้ให้บริการให้มีการรักษาความลับของข้อมูลสมาชิก
- โปรแกรมมีการรองรับ PDPA และระบบจัดการสิทธิ์ผู้ใช้งาน (Access Control)

/ ห้ามเจ้าหน้าที่

- ห้ามเจ้าหน้าที่ของสหกรณ์ดำเนินการแก้ไขดัดแปลงกับผู้ให้บริการโดยไม่มีการอนุมัติจากผู้มีอำนาจ

- กรณีเจ้าหน้าที่สหกรณ์หรือบุคคลภายนอกกระทำผิดหรือกระทำการใดๆ อันเป็นการฝ่าฝืนมาตรการ และวิธีการรักษาความมั่งคงปลอดภัยระบบเทคโนโลยีสารสนเทศนี้ และการกระทำดังกล่าวเป็นความผิดตามพระราชบัญญัติ ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ที่บังคับใช้ในปัจจุบัน ให้สหกรณ์ฯ ดำเนินการกับผู้กระทำความผิดตามกฎหมาย

๗. มาตรการประเมินความเสี่ยง และสร้างความปลอดภัยด้านเทคโนโลยีสารสนเทศ

สหกรณ์มีการกำหนดผู้รับผิดชอบในการตรวจสอบประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ การจัดทำแผนการจัดการความเสี่ยงเพื่อลดความเสี่ยงที่อาจเกิดขึ้น จากการใช้งานโปรแกรมบัญชี การเข้าถึงข้อมูล และการประมวลผล

- จัดทำแผนฟื้นฟูระบบกรณีระบบขัดข้อง

- ดำเนินการประเมินความเสี่ยงของระบบอย่างน้อย ๑ ครั้งต่อไตรมาส โดยพิจารณาจากข้อบกพร่องที่อาจเกิดขึ้นจากการใช้งานโปรแกรมระบบบัญชี อาทิ การประมวลผล และการเข้าถึงข้อมูล

- กำหนดสิทธิการเข้าถึงระบบบัญชีตามบทบาทหน้าที่ของผู้ใช้งาน และมีการตรวจสอบการเข้าระบบย้อนหลังได้

- ตรวจสอบความสมบูรณ์ของข้อมูลสำรองเป็นประจำเพื่อให้แน่ใจว่าระบบสำรองทำงานได้อย่างถูกต้องและสามารถกู้คืนข้อมูลได้เมื่อเกิดเหตุฉุกเฉิน

๘. มาตรการการกำหนดช่องทางการร้องเรียนการทุจริตภายในสหกรณ์

สหกรณ์เปิดโอกาสให้สมาชิกหรือเจ้าหน้าที่สามารถแจ้งเรื่องร้องเรียนข้อสงสัยเกี่ยวกับการทุจริต หรือประพฤติมิชอบภายในสหกรณ์ได้อย่างปลอดภัย โปร่งใส และเป็นธรรม ได้โดยตรงถึงประธานกรรมการสหกรณ์ ผ่านช่องทางดังนี้

- เอกสารบรรยายเหตุการณ์พร้อมหลักฐาน ส่งถึง “ประธานกรรมการสหกรณ์” โดยตรง

- กล่องรับข้อร้องเรียน (วางในพื้นที่สำนักงานสหกรณ์ที่เข้าถึงได้ง่าย และมีการเปิดตรวจเป็นประจำ)

-ช่องทาง E-Mail : Snbcoop๑๙๘๙@gmail.com , Appication Line : @rve๖๑๑๓W , Tel : ๐๓๘ ๑๑๐ ๗๙๙๕ Mobile : ๐๙๘ ๖๒๗ ๕๐๐๐ และสำเนาถึงสำนักงานตรวจบัญชีสหกรณ์จังหวัดชลบุรี สำนักงานส่งเสริมสหกรณ์จังหวัดชลบุรี

- สหกรณ์ป้องกันความลับของผู้ร้องเรียน ห้ามมิให้มีการเปิดเผยชื่อผู้แจ้งหรือข้อมูลที่สามารถระบุตัวตนได้

- จัดตั้งคณะทำงานเฉพาะกิจเพื่อตรวจสอบข้อร้องเรียน และรายงานผลการพิจารณาต่อคณะกรรมการดำเนินการมีการบันทึกติดตามผลของการดำเนินการสอบสวน เพื่อให้เกิดความโปร่งใสและสามารถตรวจสอบย้อนหลังได้

ทั้งนี้ตั้งแต่บัดนี้เป็นต้นไป

สั่ง ณ วันที่ ๑ ตุลาคม พ.ศ.๒๕๖๘

พลเรือเอก

(วัชระ พัฒนรัฐ)

ประธานกรรมการดำเนินการ

สหกรณ์ออมทรัพย์ฐานทัพเรือสัตหีบ จำกัด