ระเบียบสหกรณ์ออมทรัพย์ครูสมุทรปราการ จำกัด
ว่าด้วยการปฏิบัติงานเกี่ยวกับข้อมูลส่วนบุคคล พ.ศ. 2565

.....

ด้วยสหกรณ์ออมทรัพย์ครูสมุทรปราการ จำกัด ตระหนักถึงความสำคัญของข้อมูลส่วนบุคคลและข้อมูลอื่น อีกทั้งเพื่อให้การดำเนินงานของสหกรณ์ออมทรัพย์ครูสมุทรปราการ จำกัด มีความโปร่งใสและความรับผิดชอบในการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลของท่านตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 รวมถึงกฎหมายอื่นที่เกี่ยวข้อง นโยบายการคุ้มครองข้อมูลส่วนบุคคล ดังนั้น อาศัยอำนาจตามความในข้อบังคับสหกรณ์ออมทรัพย์ครูสมุทรปราการ จำกัด พ.ศ. 2564 ข้อ 77 (19) และข้อ 117 (12) ประกอบกับมติที่ประชุมคณะกรรมการดำเนินการ ชุดที่ 61 ในการประชุมครั้งที่ 11/2565เมื่อวันที่ 30 พฤษภาคม พ.ศ. 2565 จึงกำหนดระเบียบสหกรณ์ออมทรัพย์ครูสมุทรปราการ จำกัด ว่าด้วยการปฏิบัติเกี่ยวกับการปฏิบัติงานเกี่ยวกับข้อมูลส่วนบุคคลพ.ศ. 2565 ดังต่อไปนี้

ข้อ 1 ระเบียบนี้เรียกว่า “ระเบียบสหกรณ์ออมทรัพย์ครูสมุทรปราการ จำกัด ว่าด้วยการปฏิบัติเกี่ยวกับข้อมูลส่วนบุคคล พ.ศ. 2565”

ข้อ 2 ระเบียบนี้ให้ใช้บังคับตั้งแต่วันที่ 1 มิถุนายน พ.ศ. 2565 เป็นต้นไป

ข้อ 3 การรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคลที่ระเบียบนี้ไม่ได้กำหนดเอาไว้ ให้ดำเนินการไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 รวมถึงกฎหมายลำดับรอง และนโยบายการคุ้มครองข้อมูลส่วนบุคคลของสหกรณ์ออมทรัพย์ครูสมุทรปราการ จำกัด

ข้อ 4 ในระเบียบนี้

สหกรณ์ หมายถึง สหกรณ์ออมทรัพย์ครูสมุทรปราการ จำกัด

คณะกรรมการ หมายถึง คณะกรรมการดำเนินการสหกรณ์ออมทรัพย์ครูสมุทรปราการ จำกัด

ประธานกรรมการ หมายถึง ประธานกรรมการดำเนินการสหกรณ์ออมทรัพย์ครูสมุทรปราการ จำกัด

ผู้จัดการ หมายถึง ผู้จัดการสหกรณ์ออมทรัพย์ครูสมุทรปราการ จำกัด

เจ้าหน้าที่ หมายถึง เจ้าหน้าที่สหกรณ์ออมทรัพย์ครูสมุทรปราการ จำกัด

หัวหน้าฝ่าย หมายถึง หมายถึง หัวหน้าฝ่าย ที่มีอำนาจบังคับบัญชาสูงสุดในฝ่าย ซึ่งสหกรณ์กำหนดให้เป็นผู้มีหน้าที่ควบคุมกำกับให้การรวบรวม ใช้ เปิดเผย รวมถึงมาตรการรักษาความมั่นคงปลอดภัยในแผนหรือฝ่ายนั้นให้เป็นไปตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล และระเบียบนี้ ซึ่งสหกรณ์จะประกาศรายชื่อเอาไว้ให้ทราบในระเบียบนี้

ข้อมูลส่วนบุคคล หมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรม และข้อมูลของนิติบุคคล

เจ้าของข้อมูลส่วนบุคคล หมายถึง บุคคลที่ข้อมูลนั้นระบุตัวตนไปถึงได้ ไม่ว่าจะเป็นข้อมูลทางตรง ข้อมูลทางอ้อม ข้อมูลอ่อนไหว

การประมวลผลข้อมูลส่วนบุคคล หมายถึง การดำเนินการใด ๆ กับข้อมูลส่วนบุคคลไม่ว่าจะเป็นการเก็บรวบรวม บันทึก สำเนา จัดระเบียบ เก็บรักษา ปรับปรุง เปลี่ยนแปลง ใช้ กู้คืน เปิดเผย ส่งต่อเผยแพร่ โอน รวม ลบ ทำลาย

ผู้ควบคุมข้อมูลส่วนบุคคล หมายถึง สหกรณ์ออมทรัพย์ครูสมุทรปราการ จำกัด ในฐานะผู้มีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

ผู้ประมวลผลข้อมูลส่วนบุคคล หมายถึง บุคคลธรรมดา หรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่ง หรือกระทำในนามของผู้ควบคุมข้อมูลส่วนบุคคล

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หมายถึง บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของสหกรณ์ออมทรัพย์ครูสมุทรปราการ จำกัด ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถระบุตัวบุคคลได้ทั้งทางตรงและทางอ้อม นอกเหนือจากข้อมูลอ่อนไหว

ข้อมูลอ่อนไหว หมายถึง ข้อมูลที่อาจนำไปสู่การเลือกปฏิบัติอัน ได้แก่ เชื้อชาติ เผ่าพันธ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนา หรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ ข้อมูลอื่นที่คณะกรรมการอาจประกาศออกมาเพิ่มเติม

หมวดที่ 1
หน้าที่และความรับผิดชอบ

ข้อ 5 ให้คณะกรรมการมีอำนาจ หน้าที่ ดังนี้

(1) กำหนดนโยบาย และแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล

(2) กำกับดูแลให้มีการดำเนินการตามกฎหมาย นโยบาย และระเบียบที่เกี่ยวข้อง

ข้อ 6 เจ้าหน้าที่ซึ่งมีตำแหน่งดังต่อไปนี้ เป็นผู้กำกับการให้เป็นไปตามกฎหมายและระเบียบในแผนกหรือฝ่ายที่ตนเองมีหน้าที่รับผิดชอบ คือ

6.1 หัวหน้าฝ่ายการเงินและและบัญชี

6.2 หัวหน้าฝ่ายสินเชื่อ

6.3 หัวหน้าทะเบียนสมาชิก

6.4 หัวหน้าฝ่ายอำนวยการ

6.5 หัวหน้าฝ่ายเร่งรัดหนี้สินและงานกฎหมาย

6.6 หัวหน้าศูนย์บริการ

อนึ่ง รายชื่อคณะกรรมการ สหกรณ์จะออกประกาศให้ทราบ

ข้อ 7 มีอำนาจและหน้าที่ดังนี้

7.1 ดำเนินการให้เป็นไปตามข้อกฎหมายในการรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคลให้เหมาะสมกับลักษณะหรือสภาพของงาน

7.2 จัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลทั้งทางด้านบริหาร ด้านกายภาพ และด้านเทคนิคสำหรับข้อมูลส่วนบุคคลที่อยู่ในความรับผิดขอบของตน เพื่อป้องกันการสูญ หาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ รวมทั้งแจ้งให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลทราบถึงเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น

7.3 บริหารจัดการให้เจ้าหน้าที่ที่อยู่ภายใต้การบังคับบัญชาดำเนินการปฏิบัติตามกฎหมาย โดยห้ามไม่ให้รวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคลโดยไม่ชอบด้วยกฎหมาย

7.4 พิจารณาโทษทางวินัยแก่เจ้าหน้าที่ที่อยู่ภายใต้บังคับบัญชา ที่ฝ่าฝืนไม่ปฏิบัติตามระเบียบนี้ หรือระเบียบอื่น หรือคำสั่งที่เกี่ยวข้อง หรือกฎหมายคุ้มครองข้อมูลส่วนบุคคล

7.5 การติดต่อบุคคลภายนอกเพื่อทำการประมวลผลจะต้องมีการทำสัญญากำกับไม่ให้ใช้หรือเปิดเผยข้อมูลโดยไม่ชอบด้วยกฎหมาย รวมถึงควรคัดเลือกบุคคลที่มีนโยบายการคุ้มครองข้อมูลส่วนบุคคลและมีระบบการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

7.6 ดำเนินการและควบคุมการลบหรือทำลายข้อมูลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวม หรือตามที่เจ้าของข้อมูลส่วนบุคคลได้ร้องขอ

7.7 ตรวจสอบ และควบคุม ปรับปรุงข้อมูลส่วนบุคคลให้มีความถูกต้อง ทันสมัยและเป็นปัจจุบัน

7.8 เมื่อพบการรั่วไหล หรือการละเมิดข้อมูลส่วนบุคคลต้องแจ้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลในทันที

7.9 ดำเนินการควบคุมการบันทึกข้อมูลและรายงานที่เกี่ยวข้องกับข้อมูลส่วนบุคคลที่รับผิดชอบ

7.10 ประเมินความเสี่ยงที่เกี่ยวข้องกับข้อมูลส่วนบุคคลที่ตนรับผิดชอบ บริหารจัดการและดำเนินตาม มาตรการที่กำหนดเพื่อลดความเสี่ยง

7.11 สร้างความตระหนักรู้เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลแก่เจ้าหน้าที่ที่อยู่ภายใต้การบังคับบัญชา

7.12 ควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์การจัดเก็บและการประมวลผลข้อมูลส่วนบุคคล

7.13 ธำรงไว้ซึ่งความลับของข้อมูลส่วนบุคคล

7.14 อนุญาต หรือไม่อนุญาตการเข้าถึงข้อมูลส่วนบุคคล

ข้อ 8 ให้แต่งตั้งคณะบุคคลอย่างน้อยต้องประกอบไปด้วยรองผู้จัดการ ฝ่ายงานบุคคล ฝ่ายบริหารระบบคอมพิวเตอร์ ฝ่ายงานกฎหมาย เป็นเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของสหกรณ์

ข้อ 9 เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลมีอำนาจหน้าที่ ดังนี้

9.1 ให้ข้อเสนอแนะแก่สหกรณ์ และเจ้าหน้าที่ในการรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัยทั้งทางด้านบริหาร ด้านกายภาพ และด้านเทคนิค

9.2 ทวนสอบ ตรวจสอบการดำเนินงานภายในสหกรณ์เพื่อให้การรวบรวม ใช้ เปิดเผย ประมวลผล และการรักษาความมั่นคงปลอดภัยทั้งทางด้านบริหาร ด้านกายภาพ และด้านเทคนิคเป็นไปตามกฎหมายรวมถึงการตรวจสอบการบันทึกรายการกิจกรรมข้อมูลส่วนบุคคล (Ropa) และ Privacy Notice ในทุก ๆ 3 เดือนเพื่อให้ข้อมูลถูกต้อง และเป็นปัจจุบัน

9.3 ประสานงาน ให้ความร่วมมือกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

9.4 รับข้อร้องเรียน ตรวจสอบการกระทำที่ได้รับการร้องเรียน ดำเนินการแก้ไขตามข้อร้องเรียน ไกล่เกลี่ยข้อพิพาท พิจารณาความเสียหายและเสนอแนะต่อสหกรณ์

9.5 ซักซ้อมกรณีข้อมูลรั่วไหล จัดให้มีการตระหนักรู้แก่เจ้าหน้าที่ รวมถึงจัดทำแผนงานประจำปีด้านการคุ้มครองข้อมูลส่วนบุคคล

9.6 ปฏิบัติการอื่นใดตามที่กฎหมายคุ้มครองข้อมูลส่วนบุคคล และกฎหมายอื่นกำหนด

9.7 รักษาความลับที่เกี่ยวกับข้อมูลส่วนบุคคลอันเนื่องมาจากการที่ตนได้ล่วงรู้อันเนื่องมาจากการปฏิบัติหน้าที่

หมวดที่ 2
การรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคล

ข้อ 10 การรวบรวมข้อมูลส่วนบุคคล ให้เจ้าหน้าที่ดำเนินการดังนี้

10.1 ห้ามมิให้รวบรวม โดยไม่ได้รับความยินยอม หรือมีฐานรองรับเพื่อให้เกิดความชอบด้วยกฎหมาย

10.2 การรวบรวมข้อมูลส่วนบุคคลต้องทำโดยชัดแจ้ง เป็นหนังสือ หรือสื่ออิเล็กทรอนิกส์ โดยต้องแยกความยินยอมนั้นออกจากข้อความอื่นอย่างชัดแจ้ง มีแบบ หรือข้อความที่เข้าถึงได้ง่ายและเข้าใจได้ ใช้ภาษาที่เข้าใจง่าย ไม่หลอกลวงหรือทำให้เข้าใจผิดในวัตถุประสงค์

10.3 ในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ต้องดำเนินการโดยให้เจ้าของข้อมูลเป็นอิสระ

10.4 ให้ดำเนินการตรวจสอบสิทธิ อำนาจและฐานอื่น ๆ เพื่อร้องขอการรวบรวมข้อมูลส่วนบุคคล

10.5 ต้องมีการแจ้งวัตถุประสงค์ในขณะที่ขอความยินยอมเพื่อรวมรวมข้อมูลส่วนบุคคลก่อนหรือขณะรวบรวมข้อมูลส่วนบุคคล

10.6 ต้องมีการดำเนินการอย่างโปร่งใสโดยการแจ้งรายละเอียดความเป็นส่วนตัว หรือ Privacy Notice ทุกครั้ง

10.7 ห้ามมิให้หลอกลวง เงื่อนไขด้านราคา เงื่อนไขด้านส่วนลด หรือเอาผลเชิงลบอื่น มาเป็นเงื่อนไขในการรวบรวมข้อมูลส่วนบุคคล

10.8 การเก็บรวมรวมข้อมูลส่วนบุคคลต้องดำเนินการโดยน้อยที่สุด เฉพาะที่จำเป็นเท่านั้น โดยต้องดำเนินการสอบถามวัตถุประสงค์ในการนำข้อมูลไปใช้งานเพื่อให้สามารถประเมินว่าควรสำเนาข้อมูลให้ในระดับรายละเอียดเท่าใด เช่น กรณีส่งจดหมายหรือสารสัมพันธ์จำเป็นต้องทราบที่อยู่ แต่ไม่จำเป็นต้องทราบ วัน เดือน ปีเกิด หรือหมู่โลหิต เป็นต้น

10.9 ห้ามมิให้รวบรวมข้อมูลอ่อนไหวโดยไม่จำเป็น

ข้อ 11 ห้ามมิให้เจ้าหน้าที่รวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่เจ้าของข้อมูลโดยตรง เว้นแต่ในกรณีดังต่อไปนี้

11.1 ได้แจ้งถึงการเก็บรวมรวมข้อมูลส่วนบุคคลจากแหล่งอื่นให้เจ้าของข้อมูลส่วนบุคคลทราบภายใน 15 วันนับแต่วันที่รวบรวมข้อมูลส่วนบุคคล และได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

11.2 เป็นการรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ได้รับความยินยอม แต่มีฐานอื่นที่ไม่ต้องขอความยินยอมรองรับ ได้แก่

(ก) ฐานที่ไม่ต้องได้รับความยินยอมกรณีข้อมูลทั่วไป

1. ฐานจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัยหรือสถิติซึ่งได้จัดให้มีมาตรการปกป้องที่เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล

2. ฐานป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล

3. ฐานจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น

4. ฐานจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล

5. ฐานจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลหรือของบุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล เว้นแต่ประโยชน์ดังกล่าวมีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล

6. ฐานปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล

(ข) ฐานที่ไม่ต้องได้รับความยินยอมกรณีข้อมูลอ่อนไหว

1. ฐานป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคลซึ่งเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมได้ ไม่ว่าด้วยเหตุใดก็ตาม

2. ฐานดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมของมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรที่มีวัตถุประสงค์เกี่ยวกับการเมือง ศาสนา ปรัชญา หรือสหภาพแรงงานให้แก่สมาชิก ผู้ซึ่งเคยเป็นสมาชิก หรือผู้ซึ่งมีการติดต่ออย่างสม่ำเสมอกับมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรตามวัตถุประสงค์ดังกล่าวโดยไม่ได้เปิดเผยข้อมูลส่วนบุคคลนั้นออกไปภายนอกมูลนิธิสมาคม หรือองค์กรที่ไม่แสวงหากำไรนั้น

3. ฐานข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคล

4. ฐานจำเป็นเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย

5. ฐานเป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับ

5.1 เวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ การประเมินความสามารถในการทำงานของลูกจ้าง การวินิจฉัยโรคทางการแพทย์ การให้บริการด้านสุขภาพหรือด้านสังคม การรักษาทางการแพทย์ การจัดการด้านสุขภาพ หรือระบบและการให้บริการด้านสังคมสงเคราะห์ ทั้งนี้ ในกรณีที่ไม่ใช่การปฏิบัติตามกฎหมายและข้อมูลส่วนบุคคลนั้นอยู่ในความรับผิดชอบของผู้ประกอบอาชีพหรือวิชาชีพหรือผู้มีหน้าที่รักษาข้อมูลส่วนบุคคลนั้นไว้เป็นความลับตามกฎหมาย ต้องเป็นการปฏิบัติตามสัญญาระหว่างเจ้าของข้อมูลส่วนบุคคลกับผู้ประกอบวิชาชีพทางการแพทย์

5.2 ประโยชน์สาธารณะด้านการสาธารณสุข เช่น การป้องกันด้านสุขภาพจากโรคติดต่ออันตรายหรือโรคระบาดที่อาจติดต่อหรือแพร่เข้ามาในราชอาณาจักร หรือการควบคุมมาตรฐานหรือคุณภาพของยา เวชภัณฑ์ หรือเครื่องมือแพทย์ ซึ่งได้จัดให้มีมาตรการที่เหมาะสมและเจาะจงเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลโดยเฉพาะการรักษาความลับของข้อมูลส่วนบุคคลตามหน้าที่หรือตามจริยธรรมแห่งวิชาชีพ

5.3 การคุ้มครองแรงงาน การประกันสังคม หลักประกันสุขภาพแห่งชาติ สวัสดิการเกี่ยวกับการรักษาพยาบาลของผู้มีสิทธิตามกฎหมาย การคุ้มครองผู้ประสบภัยจากรถ หรือการคุ้มครองทางสังคม ซึ่งการเก็บรวบรวมข้อมูลส่วนบุคคลเป็นสิ่งจำเป็นในการปฏิบัติตามสิทธิหรือหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลหรือเจ้าของข้อมูลส่วนบุคคล โดยได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

5.4 การศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ หรือประโยชน์สาธารณะอื่น ทั้งนี้ ต้องกระทำเพื่อให้บรรลุวัตถุประสงค์ดังกล่าวเพียงเท่าที่จำเป็นเท่านั้น และได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล ตามที่คณะกรรมการประกาศกำหนด

5.5 ประโยชน์สาธารณะที่สำคัญ โดยได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

ข้อ 12 ห้ามมิให้เจ้าหน้าที่รวบรวมข้อมูลส่วนบุคคลที่ยังไม่บรรลุนิติภาวะ ซึ่งมีอายุครบ 20 ปีบริบูรณ์ เว้นแต่

12.1 บุคคลที่มีอายุครบ 17 ปีบริบูรณ์ และได้ทำการสมรสตามกฎหมายสามารถรวบรวมข้อมูลส่วนบุคคลโดยได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลนั้นได้

12.2 ผู้เยาว์ที่มีฐานะดั่งเช่นบุคคลที่บรรลุนิติภาวะแล้ว ซึ่งผู้แทนโดยชอบธรรมได้ให้ความยินยอมในการทำธุรกิจ การค้า ทำสัญญาจ้างแรงงานไว้แล้ว

12.3 ผู้เยาว์ซึ่งมีอายุ 10 ปี แต่ไม่ครบ 20 ปี โดยได้รับความยินยอมจากผู้แทนโดยชอบธรรม หรือกิจการอื่นที่ต้องทำเองเฉพาะตัว อันได้แก่ การได้ไปซึ่งสิทธิ หรือหลุดพ้นจากหน้าที่ หรือการที่ต้องทำเองเฉพาะตัว หรือการนั้นสมควรแก่ฐานานุรูป

12.4 ผู้เยาว์ที่มีอายุต่ำกว่า 10 ปี การขอความยินยอมในการรวบรวมข้อมูลส่วนบุคคลจะต้องขอกับผู้ใช้อำนาจปกครอง

ข้อ 13 การใช้ข้อมูลส่วนบุคคล ให้เจ้าหน้าที่ดำเนินการดังนี้

13.1 ห้ามมิให้ใช้ข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมหรือมีฐานรับเพื่อให้เกิดความชอบด้วยกฎหมาย

13.2 ห้ามมิให้ใช้ข้อมูลส่วนบุคคลโดยไม่มีความจำเป็น

13.3 ห้ามมิให้ใช้ข้อมูลส่วนบุคคลโดยมิได้แจ้งรายละเอียดเอาไว้ในการแจ้งรายละเอียดความเป็นส่วนตัว หรือ Privacy Notice

13.4 ห้ามมิให้ใช้ข้อมูลส่วนบุคคลนอกจากวัตถุประสงค์ที่ได้ขอความยินยอมไว้จากเจ้าของข้อมูลส่วนบุคคล

13.5 ห้ามมิให้ใช้ข้อมูลส่วนบุคคลเพื่อการอื่นนอกจากกิจการของสหกรณ์

13.6 ห้ามมิให้ทำลาย คัดลอกทำสำเนา เปิดเผย ขโมยหรือเอาไปเสียซึ่งอุปกรณ์การจัดเก็บหรือประมวลผลข้อมูลส่วนบุคคล

13.7 เมื่อพ้นกำหนดระยะเวลาการเก็บข้อมูลส่วนบุคคล ห้ามมิให้ใช้ข้อมูลส่วนบุคคลต่อไป เว้นแต่จะมีกฎหมายกำหนด และให้รายงานหัวหน้าฝ่าย

13.8 ห้ามมิให้เข้าถึงข้อมูลส่วนบุคคลที่ถูกควบคุมการเข้าถึง เว้นแต่จะได้รับอนุญาตจากหัวหน้าฝ่าย

ข้อ 14 การใช้หรือเปิดเผยข้อมูลส่วนบุคคล ให้เจ้าหน้าที่ดำเนินการดังนี้

14.1 ห้ามมิให้ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่อยู่ในความควบคุมขอสหกรณ์โดยไม่ได้รับความยินยอม หรือมีฐานทางกฎหมายรองรับเพื่อความชอบธรรมในการเปิดเผยข้อมูลส่วนบุคคล

14.2 ห้ามมิให้ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อการอื่นนอกเหนือจากวัตถุประสงค์ที่ได้แจ้งเอาไว้ในขณะรวบรวมข้อมูลส่วนบุคคล และดังที่ได้แจ้งเอาไว้ในการแจ้งรายละเอียดความเป็นส่วนตัว หรือ Privacy Notice

14.3 การใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ไม่ได้รับความยินยอม แต่สามารถอ้างฐานอื่นเพื่อความชอบธรรมได้ ให้หัวหน้าฝ่ายดำเนินการให้มีการบันทึกการใช้ หรือเปิดเผยเอาไว้ในบันทึกรายการกิจกรรมข้อมูลส่วนบุคคล หรือ Ropa

14.4 ห้ามมิให้โอนข้อมูลส่วนบุคคล หรือส่งข้อมูลไปต่างประเทศ เว้นแต่จะได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล หรือมีฐานรองรับเพื่อให้เกิดความชอบธรรม หรือนโยบายการคุ้มครองข้อมูลส่วนบุคคลของสหกรณ์จะได้รับการตรวจสอบและรับรองจากสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

14.5 การดำเนินการจะต้องได้รับการอนุญาตจากหัวหน้าฝ่าย และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

14.6 ห้ามมิให้เปิดเผยข้อมูลส่วนบุคคลโดยมิได้แจ้งประเภทของบุคคลหรือหน่วยงานเอาไว้ในการแจ้งรายละเอียดความเป็นส่วนตัว หรือ Privacy Notice

14.7 กรณีส่งข้อมูลให้กับบุคคลภายนอกซึ่งอยู่ในราชอาณาจักรเพื่อทำการประมวลผลข้อมูล หัวหน้าฝ่าย และเจ้าหน้าที่จะต้องดำเนินเพื่อป้องกันมิให้ผู้นั้นใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือมิชอบ ดังนี้

14.7.1 จัดทำสัญญาการประมวลผลข้อมูลส่วนบุคคล

14.7.2 ตรวจสอบนโยบายการคุ้มครองข้อมูลส่วนบุคคลของบุคคลภายนอกซึ่งเป็นผู้ประมวลผล

14.7.3 ผู้ประมวลผลต้องมีการดำเนินการตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลโดยครบถ้วน

ข้อ 15 ให้หัวหน้าฝ่ายดำเนินการบันทึกกิจกรรมการใช้ข้อมูลส่วนบุคคล (Ropa) ให้ถูกต้อง เป็นปัจจุบัน และแจ้งการดำเนินการ หรือปรับปรุงการดำเนินงานให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลทราบ และให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลปรับปรุงข้อมูลในการแจ้งรายละเอียดการใช้ข้อมูลส่วนบุคคลให้ถูกต้องเป็นปัจจุบัน

ข้อ 16 ให้หัวหน้าฝ่าย เจ้าหน้าที่ และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลด้วยเหตุดังนี้

16.1 เมื่อพ้นกำหนดระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล

16.2 เมื่อไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น

16.3 ตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ หรือที่เจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอม เว้นแต่เก็บรักษาไว้เพื่อวัตถุประสงค์ในการใช้เสรีภาพในการแสดงความคิดเห็นการเก็บรักษาไว้เพื่อวัตถุประสงค์ตามที่มีฐานอื่นอันได้แก่

16.4 ข้อมูลทั่วไป ฐานการจัดทำเอกสารประวัตศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือการศึกษาวิจัย หรือฐานป้องกันหรือระงับอันตรายต่อชีวิต ร่างกายหรือสุขภาพ หรือฐานจำเป็นเพื่อปฏิบัติตามสัญญา หรือฐานประโยชน์สาธารณะ หรือฐานประโยชน์อันชอบธรรมของผู้ควบคุมข้อมูลส่วนบุคคล หรือฐานปฏิบัติตามกฎหมาย

16.5 ข้อมูลอ่อนไหว เป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับ

(ก) เวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ การประเมินความสามารถในการทำงานของลูกจ้าง การวินิจฉัยโรคทางการแพทย์ การให้บริการด้านสุขภาพหรือด้านสังคม การรักษาทางการแพทย์ การจัดการด้านสุขภาพ หรือระบบและการให้บริการด้านสังคมสงเคราะห์ ทั้งนี้ ในกรณีที่ไม่ใช่การปฏิบัติตามกฎหมายและข้อมูลส่วนบุคคลนั้นอยู่ในความรับผิดชอบของผู้ประกอบอาชีพหรือวิชาชีพหรือผู้มีหน้าที่รักษาข้อมูลส่วนบุคคลนั้นไว้เป็นความลับตามกฎหมาย ต้องเป็นการปฏิบัติตามสัญญาระหว่างเจ้าของข้อมูลส่วนบุคคลกับผู้ประกอบวิชาชีพทางการแพทย์

(ข) ประโยชน์สาธารณะด้านการสาธารณสุข เช่น การป้องกันด้านสุขภาพจากโรคติดต่ออันตรายหรือโรคระบาดที่อาจติดต่อหรือแพร่เข้ามาในราชอาณาจักร หรือการควบคุมมาตรฐานหรือคุณภาพของยา เวชภัณฑ์ หรือเครื่องมือแพทย์ ซึ่งได้จัดให้มีมาตรการที่เหมาะสมและเจาะจงเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลโดยเฉพาะการรักษาความลับของข้อมูลส่วนบุคคลตามหน้าที่หรือตามจริยธรรมแห่งวิชาชีพ

หมวดที่ 3
การรักษาความมั่นคงปลอดภัย

ข้อ 17 การรักษาความมั่นคงปลอดภัย เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ หัวหน้าฝ่ายและเจ้าหน้าที่ หรือบุคคลากรไม่ว่าจะอยู่ในตำแหน่งหรือสถานะใดต้องดำเนินการให้ครอบคลุมใน 3 หัวข้อ ดังนี้

17.1 การธำรงไว้ซึ่งความลับ

17.2 ความถูกต้อง ครบถ้วน

17.3 สภาพพร้อมใช้งาน

ข้อ 18 ให้หัวหน้าฝ่าย และเจ้าหน้าที่ หรือบุคคลากรไม่ว่าจะอยู่ในตำแหน่งหรือสถานะใดการดำเนินการรักษาความมั่นคงปลอดภัยต้องดำเนินการใน 3 ด้าน ดังนี้

18.1 ด้านบริหาร

18.2 ด้านเทคนิค

18.3 ด้านกายภาพ

การดำเนินการ อย่างน้อยต้องเป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนด

ข้อ 19 การดำเนินการรักษาความมั่นคงปลอดภัยด้านบริหาร ให้หัวหน้าฝ่าย และเจ้าหน้าที่ หรือบุคคลากรไม่ว่าจะอยู่ในตำแหน่งหรือสถานะใดดำเนินการดังนี้

19.1 หัวหน้าฝ่าย เจ้าหน้าที่จะต้องดำเนินการตามระเบียบที่เกี่ยวกับการรวบรวม ใช้ และเปิดเผย ในข้อ 10 ถึงข้อ 16 โดยเคร่งครัด

19.2 การใช้งาน การเข้าถึงข้อมูลส่วนบุคคล การเข้าพื้นที่ซึ่งมีการเก็บข้อมูลส่วนบุคคลที่ถูกจัดไว้เป็นความลับเจ้าหน้าที่จะต้องมีการขออนุญาตจากหัวหน้าฝ่ายที่ได้รับมอบหมายให้เป็นผู้อนุญาต

19.3 ให้หัวหน้าฝ่ายมีการกำหนดรายชื่อเจ้าหน้าที่ผู้มีสิทธิเข้าถึงข้อมูลส่วนบุคคล โดยออกเป็นประกาศภายในส่วนงาน

ในการเข้าถึงข้อมูลส่วนบุคคลของผู้ใช้งาน (user responsibilities) หัวหน้าฝ่ายอาจแบ่งเป็น รูปแบบต่าง ๆ เช่น สิทธิในการเข้าอ่านอย่างเดียว หรือสิทธิในการแก้ไขเพิ่มเติม สิทธิในการเปิดเผยและเผยแพร่ สิทธิในการตรวจสอบคุณภาพข้อมูล สิทธิในการลบทำลาย ทั้งนี้สหกรณ์จะประกาศให้ทราบต่อไป

19.4 บุคคลตาม 19.3 หากจะเข้าถึงข้อมูลเพื่ออ่าน หรือเพื่อแก้ไขเพิ่มเติม หรือเพื่อเปิดเผยและเผยแพร่ หรือตรวจสอบคุณภาพข้อมูล หรือลบทำลายข้อมูลจะกระทำได้ต่อเมื่อได้ขออนุญาตจากหัวหน้าฝ่าย โดยให้หัวหน้าฝ่ายตรวจสอบสิทธิตามประกาศ ตรวจสอบว่าการขอใช้สิทธิดังกล่าวมีเหตุอันสมควรและชอบด้วยกฎหมายหรือไม่ หรือการเข้าออกพื้นที่ หรือสถานที่ หรืออุปกรณ์เก็บข้อมูลส่วนบุคคล และให้ลงบันทึกการเข้าใช้งานเอาไว้ ซึ่งการบันทึกอาจทำในรูปกระดาษ หรืออิเล็กทรอนิกส์ก็ได้

19.5 เมื่อมีการเข้าถึงข้อมูลส่วนบุคคลตามข้อ (19.4) แล้ว หัวหน้าฝ่ายจะต้องมีการตรวจสอบถูกแก้ไข ถูกคัดลอก หรือ ถูกทำลาย หรือมีการกระทำที่ผิดกฎหมายหรือระเบียบนี้หรือไม่

19.6 ให้เจ้าหน้าที่และบุคลากรทุกคนปฏิบัติตามระเบียบการใช้เทคโนโลยีสารสนเทศอย่างเคร่งครัด

ข้อ 20 การดำเนินการรักษาความมั่นคงปลอดภัยด้านเทคนิค ให้หัวหน้าฝ่าย และเจ้าหน้าที่ หรือบุคคลากรไม่ว่าจะอยู่ในตำแหน่งหรือสถานะใดดำเนินการดังนี้

20.1 ให้ฝ่ายบริหารระบบคอมพิวเตอร์จัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง ลบ หรือถ่ายโอนข้อมูลส่วนบุคคล ให้สอดคล้องเหมาะสมกับวิธีการและสื่อที่ใช้ในการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคล

20.2 ให้ฝ่ายบริหารระบบคอมพิวเตอร์การบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) เพื่อควบคุมการเข้าถึงข้อมูลส่วนบุคคลเฉพาะผู้ที่ได้รับอนุญาต ตามระดับสิทธิการใช้งาน ได้แก่ การนำเข้า เปลี่ยนแปลง แก้ไข เปิดเผย ตลอดจนการลบทำลาย

20.3 ให้ฝ่ายบริหารระบบคอมพิวเตอร์จัดให้มีระบบสำรองและกู้คืนข้อมูล เพื่อให้ระบบและ/หรือ บริการต่าง ๆ ยังสามารถดำเนินการได้อย่างต่อเนื่อง โดยดำเนินการทุกวันทำการ

20.4 ให้ฝ่ายบริหารระบบคอมพิวเตอร์จัดให้มีระบบการป้องกันการกระทำที่มิชอบด้วยกฎหมายซึ่งข้อมูลส่วนบุคคลโดยใช้เทคโนโลยีที่เหมาะสม เช่น การติดตั้งไฟล์วอลแบบมาตรฐาน หรือระบบปัญญาประดิษฐ์ หรือ AI หรือ ระบบการป้องกันอื่นที่มีความจำเป็น (ถ้ามี)

20.5 การใช้คอมพิวเตอร์ในพื้นที่ซึ่งมีบุคคลภายนอกสามารถมองเห็นหน้าจอได้ เจ้าหน้าที่จะต้องปรับมุมคอมพิวเตอร์เพื่อป้องกันการมองเห็น รวมถึงการใช้ Screen saver หรือต้องมีการพักหน้าจอเอาไว้

20.6 เมื่อใช้งานคอมพิวเตอร์ทำงานที่เกี่ยวกับข้อมูลส่วนบุคคลเสร็จสิ้น ห้ามมิให้เจ้าหน้าที่เก็บข้อมูลเอาไว้ตรงส่วน Desktop จะต้องจัดเก็บข้อมูลเอาไว้ในเครื่องมือ หรืออุปกรณ์ หรือตู้ หรือพื้นที่ซึ่งมีระบบป้องกันการเข้าถึง หรือการตั้งรหัสผ่านทุกครั้ง

20.7 การใช้ข้อมูลทางด้านสารสนเทศเจ้าหน้าที่ต้องมีการตั้งรหัสผ่าน และเก็บรหัสผ่านเอาไว้ในสถานที่ปลอดภัย และธำรงไว้ซึ่งความลับ

20.8 ห้ามมิให้เจ้าหน้าที่คัดลอกข้อมูลส่วนบุคคล (Copy) หรือการทำซ้ำข้อมูลไม่ว่าจะผ่านอุปกรณ์ เครื่องมือ โดยไม่ได้รับอนุญาตจากหัวหน้าฝ่าย

20.9 ห้ามมิให้เจ้าหน้าที่เคลื่อนย้ายข้อมูลผ่านระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตจากหัวหน้าฝ่าย และการส่งต่อนั้นจะต้องมีการตั้งรหัสผ่านเพื่อป้องกันการเข้าถึง

20.10 ห้ามมิให้เจ้าหน้าที่จัดเก็บข้อมูลส่วนบุคคลเอาไว้ในคอมพิวเตอร์ Note Book เว้นแต่คอมพิวเตอร์เครื่องที่ได้รับอนุญาตจากสหกรณ์ ภายใต้เงื่อนไขที่ต้องดูแลคอมพิวเตอร์นั้นเป็นอย่างดี

20.11 การใช้คอมพิวเตอร์ส่วนบุคคล Notebook ที่มีข้อมูลสำคัญ เจ้าหน้าที่จะต้องมีการรักษาความมั่นคงปลอดภัยที่มากกว่าคอมพิวเตอร์ทั่วไป เช่น ต้องมีการเข้ารหัส (Encrypted) โดยการกำหนดรหัสแทนชื่อบุคคล รวมถึงมีมาตรการอื่นเสริม เช่น มีการกำหนดรหัสผ่าน (Password)

20.12 เจ้าหน้าที่จะต้องจัดเก็บข้อมูลส่วนบุคคลเอาไว้ในพื้นที่ซึ่งสหกรณ์จัดหาให้ และแจ้งให้เจ้าหน้าที่ทราบ

20.13 ห้ามมิให้เจ้าหน้าที่จัดเก็บข้อมูลส่วนบุคคลในอุปกรณ์บันทึกข้อมูลแบบพกพา เช่น Hard Disk แบบ External หรือ Flash Drive

20.14 กรณีเจ้าหน้าที่ทำงานจากระยะไกล ซึ่งไม่ใช่ที่สหกรณ์หากจะมีการเข้าระบบคอมพิวเตอร์ จะต้องมีมาตรการป้องกันการถูกโจมตีที่เหมาะสม และต้องได้รับอนุญาตจากหัวหน้าฝ่าย

20.15 ห้ามมิให้เจ้าหน้าที่นำอุปกรณ์ต่าง ๆ จากภายนอกมาต่อพ่วงเข้ากับระบบคอมพิวเตอร์ของสหกรณ์ เว้นแต่จะได้รับอนุญาตจากหัวหน้าฝ่าย

20.16 เมื่อมีการพิมพ์งานซึ่งมีข้อมูลส่วนบุคคล เจ้าหน้าที่จะต้องมีการรักษาความปลอดภัย

20.17 ห้ามมิให้เจ้าหน้าที่ทำการเปลี่ยนแปลงเครือข่าย เช่น IP Address หรืออุปกรณ์อื่นโดยไม่ได้รับอนุญาตจากหัวหน้าฝ่ายของฝ่ายบริหารระบบคอมพิวเตอร์

20.18 ให้ฝ่ายเทคโนโลยีสารสนเทศทบทวนมาตรการที่เหมาะสมเพื่อป้องกันการสูญหาย การเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลให้สอดคล้องกับการเปลี่ยนแปลงของเทคโนโลยีเพื่อให้เกิดประสิทธิภาพในการรักษาความมั่นคงปลอดภัยทางเทคนิคที่เหมาะสม

20.19 เจ้าหน้าที่จะต้องปฏิบัติตามระเบียบการใช้เทคโนโลยีสารสนเทศของสหกรณ์อย่างเคร่งครัด

ข้อ 21 การดำเนินการรักษาความมั่นคงปลอดภัยด้านกายภาพ ให้หัวหน้าฝ่าย และเจ้าหน้าที่ หรือบุคคลากรไม่ว่าจะอยู่ในตำแหน่งหรือสถานะใดดำเนินการดังนี้

21.1 ให้หัวหน้าฝ่ายแต่ละฝ่าย หรือเจ้าหน้าที่แต่ละแผนกจัดให้มีการควบคุมการเข้าถึงข้อมูลส่วนบุคคล และอุปกรณ์ในการจัดเก็บ และประมวลผลข้อมูลส่วนบุคคลโดยคำนึงถึงการใช้งาน และความมั่นคงปลอดภัย โดยมีตู้ ซึ่งมีการล็อกกุญแจจัดเก็บข้อมูลส่วนบุคคล หรือมีห้องเก็บเอกสาร หรือมีการติดตั้งกล้อง CCTV หรืออาจมีการกำหนดให้ล้อมรั้ว หรือกำหนดให้ต้องมีบัตรผ่านเข้าออก

21.2 การดำเนินการตามข้อ (21.1) หากมีการรวบรวมข้อมูลส่วนบุคคลให้ถือว่าเป็นการดำเนินการโดยอ้างฐานประโยชน์อันชอบธรรมของสหกรณ์ จึงไม่ต้องขอความยินยอม แต่ให้ดำเนินการตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลให้ถูกต้อง

21.3 การขออนุญาตเข้าถึงข้อมูลส่วนบุคคล หัวหน้าฝ่ายจะต้องบันทึกการเปิดตู้ หรือการเข้าพื้นที่จัดเก็บข้อมูลเอาไว้

21.4 ในการปฏิบัติงาน กรณีที่มีการทำงานอย่างต่อเนื่อง ซึ่งงานนั้นมีข้อมูลส่วนบุคคล หากปฏิบัติงานนั้นเสร็จแล้ว เจ้าหน้าที่จะต้องมีการจัดเก็บเอกสารหรือข้อมูลนั้นเป็นความลับในทันที ห้ามมิให้วางเอกสารไว้ในที่ใด ๆ ซึ่งไม่มีมาตรการป้องกัน โดยเจ้าหน้าที่จะต้องดำเนินการจัดเก็บเอาไว้ในสถานที่ซึ่งมีการป้องกันการเข้าถึงเชิงกายภาพเอาไว้ เช่น มีตู้ มีกุญแจ มีห้องเก็บเอกสาร มีกล้อง CCTV มีเจ้าหน้าที่ช่วยกันสอดส่องดูแล

หมวดที่ 4
แจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

ข้อ 22 ให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลเป็นผู้รับผิดชอบกิจกรรมและวิธีการแจ้งเหตุละเมิดให้แก่ผู้จัดการหรือผู้ได้รับมอบหมาย พร้อมทั้งแจ้งตัวแทนของสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลได้ทราบโดย การส่งอีเมลล์ แต่ถ้าเป็นจะต้องแจ้งโดยทางโทรศัพท์

ข้อ 23 กรณีความเสี่ยงต่ำ ซึ่งมีมีผลกระทบต่อสิทธิและเสรีภาพของบุคคลไม่ร้ายแรง เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลไม่จำเป็นต้องแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

กรณีความเสี่ยงต่ำตามวรรคแรก เช่น กรณีมีการรั่วไหลของข้อมูล แต่ปรากฏว่าข้อมูลส่วนบุคคลนั้นถูกเข้ารหัสผ่านเอาไว้ ซึ่งไม่สามารถเปิดอ่าน หรือเข้าถึงได้หากไม่ทราบรหัสผ่าน หรือถูกซอฟต์แวร์เรียกค่าไถ่ (Ransomware) และมีการเปลี่ยนรหัสผ่านทำให้ไม่สามารถใช้งานได้เพื่อเรียกเงินแลกกับการปลดการเข้ารหัสเพื่อให้ใช้ข้อมูลได้ แต่หากไม่ได้ถูกโจรกรรมข้อมูลส่วนบุคคล

อนึ่ง การกระทำดังกล่าวในวรรคแรก หากมีการโจรกรรมข้อมูลส่วนบุคคลให้ถือเป็นความเสี่ยงสูง

นอกจากนี้ความเสี่ยงต่ำอาจพิจารณาจากจำนวนผู้เสียหาย จำนวนข้อมูลส่วนบุคคล ความยากง่ายในการเข้าถึงข้อมูลส่วนบุคคลซึ่งมีการกำหนดหรือตั้งค่าการเข้าถึง

กรณีความเสี่ยงต่ำให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลดำเนินการเพียงบันทึกเหตุการณ์ไว้เป็นการภายในก็เพียงพอ โดยไม่จำเป็นต้องแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบ และไม่จำเป็นต้องแจ้งเจ้าของข้อมูลส่วนบุคคลทราบ

ข้อ 24 กรณีมีความเสี่ยงสูง ซึ่งอาจกระทบต่อสิทธิและเสรีภาพของบุคคล ผู้โจมตีทำการฝังมัลแวร์หรือไวรัส เพื่อเข้าถึงข้อมูลส่วนบุคคล หรือปริมาณข้อมูลส่วนบุคคลจำนวนมาก ถือว่ามีความเสี่ยงสูงที่เหตุการณ์ดังกล่าวจะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล เช่นนี้ ให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลดำเนินการบันทึกไว้เป็นการภายในถึงการเข้าโจมตี และการโจรกรรมข้อมูล และแจ้งเหตุดังกล่าวโดยไม่ชักช้าภายใน 72 ชั่วโมงนับตั้งแต่ทราบเหตุเท่าที่สามารถทำได้ ไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบ และ ยังต้องแจ้งเจ้าของข้อมูลส่วนบุคคลทราบด้วย

กรณีที่สหกรณ์ทำหน้าที่เป็นผู้ประมวลผล ให้แจ้งแก่ผู้ควบคุมข้อมูลส่วนบุคคลถึงเหตุที่มีการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น

ข้อ 25 ให้เจ้าหน้าที่คุ้มครองข้อมูลส่วน แจ้งการละเมิดต่อเจ้าของข้อมูลส่วนบุคคลให้ทราบ และแจ้งแนวทางการเยียวยาความเสียหายแก่เจ้าของข้อมูลส่วนบุคคลโดยไม่ชักช้า ทั้งนี้ ตามความเสียหายที่แท้จริง โดยรายงานไปยังผู้จัดการหรือที่ได้รับมอบหมายเพื่อดำเนินการต่อไป

ข้อ 26 ให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลสอบสวนหาสาเหตุการละเมิดข้อมูลส่วนบุคคลในทันทีว่าลักษณะการละเมิดข้อมูลส่วนบุคคลเป็นอย่างไร ประเภทและจำนวนข้อมูลส่วนบุคคลอะไร แหล่งที่เกิดการละเมิดข้อมูลส่วนบุคคลเกิด ณ จุดใด ผลกระทบที่เกิดขึ้นมีอะไรบ้าง และหามาตรการป้องกันที่เหมาะสมในทันที

หมวดที่ 5
วินัยและโทษทางวินัยของการไม่ปฏิบัติตามระเบียบ

ข้อ 27 เจ้าหน้าที่ซึ่งไม่ปฏิบัติตามระเบียบนี้ หรือระเบียบอื่น หรือประกาศนโยบายคุ้มครองข้อมูลส่วนบุคคล หรือพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และกฎหมายลำดับรองที่เกี่ยวข้องอาจได้รับโทษทางวินัยโดยออกเป็นหนังสือตักเตือน

ข้อ 28 เจ้าหน้าที่ซึ่งไม่ปฏิบัติตามระเบียบนี้ หรือระเบียบอื่น หรือประกาศนโยบายคุ้มครองข้อมูลส่วนบุคคล หรือพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และกฎหมายลำดับรองที่เกี่ยวข้องจนเป็นเหตุให้ข้อมูลรั่วไหล หรือนำข้อมูลส่วนบุคคลไปใช้ หรือเปิดเผยต่อบุคคลภายนอกโดยไม่มีหน้าที่ หรือไม่ได้รับอนุญาตให้เข้าถึงข้อมูลส่วนบุคคล อาจได้รับโทษทางวินัยในระดับการออกหนังสือตักเตือน

อนึ่ง หากการดำเนินการฝ่าฝืนระเบียบตามวรรคแรกเป็นเหตุให้เกิดการรั่วไหลของข้อมูลส่วนบุคคลจนเกิดความเสี่ยงสูง เจ้าหน้าที่อาจได้รับโทษถึงขั้นเลิกจ้างโดยไม่จ่ายค่าชดเชย รวมถึงอาจต้องรับผิดในทางแพ่ง อาญา และทางปกครอง

ข้อ 29 ในกรณีที่มีปัญหาเกี่ยวกับการปฏิบัติตามระเบียบนี้ให้คณะกรรมการดำเนินการเป็นผู้มีอำนาจวินิจฉัยชี้ขาดและให้ถือเป็นที่สุด

ข้อ 30 ให้ประธานกรรมการดำเนินการเป็นผู้รักษาการตามระเบียบนี้

ประกาศ ณ วันที่ 1 มิถุนายน พ.ศ. 2565

(ลงชื่อ) วรพจน์ สิงหราช
(นายวรพจน์ สิงหราช)
ประธานกรรมการ
สหกรณ์ออมทรัพย์ครูสมุทรปราการ จำกัด