# ประกาศ

## ที่ บพ. 016/2565

## เรื่อง ระเบียบปฏิบัติเกี่ยวกับข้อมูลส่วนบุคคลของบริษัท บางกอกโซลาร์ พาวเวอร์ จำกัด

**********

ด้วย บริษัท บางกอกโซลาร์ พาวเวอร์ จำกัด ตระหนักถึงความสำคัญของข้อมูลส่วนบุคคลและข้อมูลอื่น อีกทั้งเพื่อให้การดำเนินงานของบริษัท บางกอกโซลาร์ พาวเวอร์ จำกัด มีความโปร่งใสและความรับผิดชอบในการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลของท่านตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 รวมถึงกฎหมายอื่นที่เกี่ยวข้อง นโยบายการคุ้มครองข้อมูลส่วนบุคคล จึงออกระเบียบนี้เพื่อเป็นแนวทางในการทำงานต่อไปดังนี้

**ข้อ 1** ระเบียบนี้เรียกว่า ระเบียบปฏิบัติเกี่ยวกับข้อมูลส่วนบุคคลของบริษัท บางกอกโซลาร์ พาวเวอร์ จำกัด

**ข้อ 2** ระเบียบนี้ให้มีผลใช้บังคับตั้งแต่วันที่ 1 มิถุนายน 2565 เป็นต้นไป

**ข้อ3** การรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคลที่ระเบียบนี้ไม่ได้กำหนดเอาไว้ ให้ดำเนินการไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 รวมถึงกฎหมายลำดับรอง และนโยบายการคุ้มครองข้อมูลส่วนบุคคลของบริษัท บางกอกโซลาร์ พาวเวอร์ จำกัด

**ข้อ 4** นิยามศัพท์

"**บริษัท** " หมายถึง บริษัท บางกอกโซลาร์ พาวเวอร์ จำกัด

"**ข้อมูลส่วนบุคคล**" หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรม และข้อมูลของนิติบุคคล

"**เจ้าของข้อมูลส่วนบุคคล**" หมายความว่า บุคคลที่ข้อมูลนั้นระบุตัวตนไปถึงได้ ไม่ว่าจะเป็นข้อมูลทางตรง ข้อมูลทางอ้อม ข้อมูลอ่อนไหว

"**การประมวลผลข้อมูลส่วนบุคคล**" หมายถึง การดำเนินการใด ๆ กับข้อมูลส่วนบุคคลไม่ว่าจะเป็นการเก็บรวบรวม บันทึก สำเนา จัดระเบียบ เก็บรักษา ปรับปรุง เปลี่ยนแปลง ใช้ กู้คืน เปิดเผย ส่งต่อ เผยแพร่ โอน รวม ลบ ทำลาย

"**ผู้ควบคุมข้อมูลส่วนบุคคล**" หมายความว่า บริษัท บางกอกโซลาร์ พาวเวอร์ จำกัดในฐานผู้มีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

"**ผู้ประมวลผลข้อมูลส่วนบุคคล**" หมายถึง บุคคลธรรมดา หรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่ง หรือกระทำในนามของผู้ควบคุมข้อมูลส่วนบุคคล

"**เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล**" หมายความว่า บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของบริษัท บางกอกโซลาร์ พาวเวอร์ จำกัด ในฐานผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

**“ผู้บริหาร”** หมายถึง ผู้บริหารในแผนก หรือฝ่าย หรือสาขาที่มีอำนาจบังคับบัญชาสูงสุดในแผนก หรือฝ่าย หรือสาขานั้น ซึ่งบริษัทกำหนดให้เป็นผู้มีหน้าที่ควบคุมกำกับให้การรวบรวม ใช้ เปิดเผย รวมถึงมาตรการรักษาความมั่นคงปลอดภัย ในแผนหรือฝ่ายหรือสาขานั้นให้เป็นไปตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล และระเบียบนี้ ซึ่งบริษัทจะประกาศรายชื่อเอาไว้ให้ทราบในระเบียบนี้

**“พนักงาน”** หมายถึงพนักงานซึ่งผูกพันกับ บริษัท บางกอกโซลาร์ พาวเวอร์ จำกัด ตามสัญญาจ้างแรงงาน และ/หรือมีนิติสัมพันธ์กันตามกฎหมายคุ้มครองแรงงานในฐานะนายจ้าง ลูกจ้าง

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

## หมวดที่ 1
## หน้าที่และความรับผิดชอบ

**ข้อ 5** ให้คณะกรรมการบริษัทมีอำนาจ หน้าที่ ดังนี้

1) กำหนดนโยบาย และแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล
2) กำกับดูแลให้มีการดำเนินการตามกฎหมาย นโยบาย และระเบียบที่เกี่ยวข้อง

**ข้อ 6** ผู้บริหารซึ่งมีตำแหน่งดังต่อไปนี้ เป็นผู้กำกับการให้เป็นไปตามกฎหมายและระเบียบในแผนกหรือฝ่ายที่ตนเองมีหน้าที่รับผิดชอบ คือ

1) ประธานกรรมการบริหาร
2) รองประธานกรรมการบริหาร
3) ผู้อำนวยการฝ่ายโครงการและงานวิศวกรรม
4) ผู้จัดการฝ่ายปฏิบัติการ
5) ผู้จัดการฝ่ายโครงการและงานวิศวกรรม
6) ผู้จัดการฝ่ายสรรหาและพัฒนาผลิตภัณฑ์
7) ผู้จัดการฝ่ายบริการงานวิศวกรรม
8) ผู้จัดการแผนกพัฒนาธุรกิจ 1
9) ผู้จัดการแผนกพัฒนาธุรกิจ 2
10) ผู้จัดการแผนกควบคุมการผลิตพลังงาน
11) ผู้จัดการแผนกปฏิบัติการและบริการ
12) ผู้จัดการแผนกวิจัยพัฒนาผลิตภัณฑ์และนวัตกรรม

13) ผู้จัดการแผนกประกันคุณภาพ

14) ผู้จัดการแผนกจัดซื้อและจัดจ้าง

15) ผู้จัดการแผนกออกแบบ

16) ผู้จัดการแผนกประสานงานโครงการ

17) ผู้จัดการแผนกควบคุมบัญชีและการเงิน

18) ผู้จัดการแผนกบริหารและพัฒนาทรัพยากรมนุษย์

อนึ่ง รายชื่อผู้บริหาร บริษัทจะออกประกาศให้ทราบ

มีอำนาจและหน้าที่ดังนี้

1) ดำเนินการให้เป็นไปตามข้อกฎหมายในการรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคลให้เหมาะสมกับลักษณะหรือสภาพของงาน

2) จัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลทั้งทางด้านบริหาร ด้านกายภาพ และด้านเทคนิคสำหรับข้อมูลส่วนบุคคลที่อยู่ในความรับผิดขอบของตน เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ รวมทั้งแจ้งให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลทราบถึงเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น

3) บริหารจัดการให้พนักงานที่อยู่ภายใต้การบังคับบัญชาดำเนินการปฏิบัติตามกฎหมาย โดยห้ามไม่ให้รวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคลโดยไม่ชอบด้วยกฎหมาย

4) พิจารณาโทษทางวินัยแก่พนักงานที่อยู่ภายใต้บังคับบัญชา ที่ฝ่าฝืนไม่ปฏิบัติตามระเบียบนี้ หรือระเบียบอื่น หรือคำสั่งที่เกี่ยวข้อง หรือกฎหมายคุ้มครองข้อมูลส่วนบุคคล

5) การติดต่อบุคคลภายนอกเพื่อทำการประมวลผลจะต้องมีการทำสัญญากำกับไม่ให้ใช้หรือเปิดเผยข้อมูลโดยไม่ชอบด้วยกฎหมาย รวมถึงควรคัดเลือกบุคคลที่มีนโยบายการคุ้มครองข้อมูลส่วนบุคคล และมีระบบการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

6) ดำเนินการและควบคุมการลบหรือทำลายข้อมูลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวม หรือตามที่เจ้าของข้อมูลส่วนบุคคลได้ร้องขอ

7) ตรวจสอบ และควบคุม ปรับปรุงข้อมูลส่วนบุคคลให้มีความถูกต้อง ทันสมัยและเป็นปัจจุบัน

8) เมื่อพบการรั่วไหล หรือการละเมิดข้อมูลส่วนบุคคลต้องแจ้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลในทันที

9) ดำเนินการควบคุมการบันทึกข้อมูลและรายงานที่เกี่ยวข้องกับข้อมูลส่วนบุคคลที่รับผิดชอบ

10) ประเมินความเสี่ยงที่เกี่ยวข้องกับข้อมูลส่วนบุคคลที่ตนรับผิดชอบ บริหารจัดการและดำเนินตามมาตรการที่กำหนดเพื่อลดความเสี่ยง

11) สร้างความตระหนักรู้เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลแก่พนักงานที่อยู่ภายใต้การบังคับบัญชา

12) ควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์การจัดเก็บและการประมวลผลข้อมูลส่วนบุคคล

13) ธำรงไว้ซึ่งความลับของข้อมูลส่วนบุคคล

14) อนุญาต หรือไม่อนุญาตการเข้าถึงข้อมูลส่วนบุคคล

**ข้อ 6** ให้แต่งตั้งคณะบุคคลอย่างน้อยต้องประกอบไปด้วยผู้จัดการแผนกบริหารและพัฒนาทรัพยากรมนุษย์เป็นเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของบริษัท

**ข้อ 7** เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลมีอำนาจหน้าที่ ดังนี้

1) ให้ข้อเสนอแนะแก่บริษัท และพนักงานในการรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคล และการรักษาความมั่นคงปลอดภัยทั้งทางด้านบริหาร ด้านกายภาพ และด้านเทคนิค

2) ทวนสอบ ตรวจสอบการดำเนินงานภายในบริษัทเพื่อให้การรวบรวม ใช้ เปิดเผย ประมวลผล และการรักษาความมั่นคงปลอดภัยทั้งทางด้านบริหาร ด้านกายภาพ และด้านเทคนิคเป็นไปตามกฎหมาย

3) รวมถึงการตรวจสอบการบันทึกรายการกิจกรรมข้อมูลส่วนบุคคล(Ropa) และ Privacy Notice ในทุก ๆ 3 เดือนเพื่อให้ข้อมูลถูกต้อง และเป็นปัจจุบัน

4) ประสานงาน ให้ความร่วมมือกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

5) รับข้อร้องเรียน ตรวจสอบการกระทำที่ได้รับการร้องเรียน ดำเนินการแก้ไขตามข้อร้องเรียน ไกล่เกลี่ยข้อพิพาท พิจารณาความเสียหายและเสนอแนะต่อบริษัท

6) ซักซ้อมกรณีข้อมูลรั่วไหล จัดให้มีการตระหนักรู้แก่พนักงาน รวมถึงจัดทำแผนงานประจำปีด้านการคุ้มครองข้อมูลส่วนบุคคล

7) ปฏิบัติการอื่นใดตามที่กฎหมายคุ้มครองข้อมูลส่วนบุคคล และกฎหมายอื่นกำหนด

8) รักษาความลับที่เกี่ยวกับข้อมูลส่วนบุคคลอันเนื่องมาจากการที่ตนได้ล่วงรู้อันเนื่องมาจากการปฏิบัติหน้าที่

## หมวดที่ 2
## การรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคล

**ข้อ 8** การรวบรวมข้อมูลส่วนบุคคล ให้พนักงานดำเนินการดังนี้

1) ห้ามมิให้รวบรวม โดยไม่ได้รับความยินยอม หรือมีฐานรองรับเพื่อให้เกิดความชอบด้วยกฎหมาย

2) การรวบรวมข้อมูลส่วนบุคคลต้องทำโดยชัดแจ้ง เป็นหนังสือ หรือสื่ออิเล็กทรอนิกส์ โดยต้องแยกความยินยอมนั้นออกจากข้อความอื่นอย่างชัดแจ้ง มีแบบ หรือข้อความที่เข้าถึงได้ง่ายและเข้าใจได้ ใช้ภาษาที่เข้าใจง่าย ไม่หลอกลวงหรือทำให้เข้าใจผิดในวัตถุประสงค์

3) ในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ต้องดำเนินการโดยให้เจ้าของข้อมูลเป็นอิสระ

4) ให้ดำเนินการตรวจสอบสิทธิ อำนาจและฐานอื่น ๆ เพื่อร้องขอการรวบรวมข้อมูลส่วนบุคคล

5) ต้องมีการแจ้งวัตถุประสงค์ในขณะที่ขอความยินยอมเพื่อรวมรวมข้อมูลส่วนบุคคลก่อนหรือขณะรวบรวมข้อมูลส่วนบุคคล

6) ต้องมีการดำเนินการอย่างโปร่งใสโดยการแจ้งรายละเอียดความเป็นส่วนตัวหรือ Privacy Notice ทุกครั้ง

7) ห้ามมิให้หลอกลวง เงื่อนไขด้านราคา เงื่อนไขด้านส่วนลด หรือเอาผลเชิงลบอื่น มาเป็นเงื่อนไขในการรวบรวมข้อมูลส่วนบุคคล

8) การเก็บรวมรวมข้อมูลส่วนบุคคลต้องดำเนินการโดยน้อยที่สุด เฉพาะที่จำเป็นเท่านั้น โดยต้องดำเนินการสอบถามวัตถุประสงค์ในการนำข้อมูลไปใช้งานเพื่อให้สามารถประเมินว่าควรสำเนาข้อมูลให้ในระดับรายละเอียดเท่าใด เช่น กรณีส่งสินค้าจำเป็นต้องทราบที่อยู่ และ GPS แต่ไม่จำเป็นต้องทราบ วัน เดือน ปีเกิด หรือหมู่โลหิต หรือรหัสไปรษณีย์ เป็นต้น

9) ห้ามมิให้รวบรวมข้อมูลอ่อนไหวโดยไม่จำเป็น

**ข้อ 9** ห้ามมิให้พนักงานรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่เจ้าของข้อมูลโดยตรง เว้นแต่ในกรณีดังต่อไปนี้

1) ได้แจ้งถึงการเก็บรวมรวมข้อมูลส่วนบุคคลจากแหล่งอื่นให้เจ้าของข้อมูลส่วนบุคคลทราบภายใน 15 วันนับแต่วันที่รวบรวมข้อมูลส่วนบุคคล และได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

2) เป็นการรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ได้รับความยินยอม แต่มีฐานอื่นที่ไม่ต้องขอความยินยอมรองรับ ได้แก่

(ก) ฐานที่ไม่ต้องได้รับความยินยอมกรณีข้อมูลทั่วไป

- ฐานจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัยหรือสถิติซึ่งได้จัดให้มีมาตรการปกป้องที่เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล

- ฐานป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล

- ฐานจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น

- ฐานจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล

- ฐานจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลหรือของบุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล เว้นแต่ประโยชน์ดังกล่าวมีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล

- ฐานปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล

(ข) ฐานที่ไม่ต้องได้รับความยินยอมกรณีข้อมูลอ่อนไหว

- ฐานป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคลซึ่งเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมได้ ไม่ว่าด้วยเหตุใดก็ตาม

- ฐานดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมของมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรที่มีวัตถุประสงค์เกี่ยวกับการเมือง ศาสนา ปรัชญา หรือสหภาพแรงงานให้แก่สมาชิก ผู้ซึ่งเคยเป็นสมาชิก หรือผู้ซึ่งมีการติดต่ออย่างสม่ำเสมอกับมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรตามวัตถุประสงค์ดังกล่าวโดยไม่ได้เปิดเผยข้อมูลส่วนบุคคลนั้นออกไปภายนอกมูลนิธิสมาคม หรือองค์กรที่ไม่แสวงหากำไรนั้น

- ฐานข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคล

- ฐานจำเป็นเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย

- ฐานเป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับ

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

(ข) ประโยชน์สาธารณะด้านการสาธารณสุข เช่น การป้องกันด้านสุขภาพจากโรคติดต่ออันตรายหรือโรคระบาดที่อาจติดต่อหรือแพร่เข้ามาในราชอาณาจักร หรือการควบคุมมาตรฐานหรือคุณภาพของยาเวชภัณฑ์ หรือเครื่องมือแพทย์ ซึ่งได้จัดให้มีมาตรการที่เหมาะสมและเจาะจงเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลโดยเฉพาะการรักษาความลับของข้อมูลส่วนบุคคลตามหน้าที่หรือตามจริยธรรมแห่งวิชาชีพ

(ค) การคุ้มครองแรงงาน การประกันสังคม หลักประกันสุขภาพแห่งชาติ สวัสดิการเกี่ยวกับการรักษาพยาบาลของผู้มีสิทธิตามกฎหมาย การคุ้มครองผู้ประสบภัยจากรถ หรือการคุ้มครองทางสังคม ซึ่งการเก็บรวบรวมข้อมูลส่วนบุคคลเป็นสิ่งจำเป็นในการปฏิบัติตามสิทธิหรือหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลหรือเจ้าของข้อมูลส่วนบุคคล โดยได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

(ง) การศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ หรือประโยชน์สาธารณะอื่น ทั้งนี้ ต้องกระทำเพื่อให้บรรลุวัตถุประสงค์ดังกล่าวเพียงเท่าที่จำเป็นเท่านั้น และได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล ตามที่คณะกรรมการประกาศกำหนด

(จ) ประโยชน์สาธารณะที่สำคัญ โดยได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

**ข้อ 10** ห้ามมิให้พนักงานรวบรวมข้อมูลส่วนบุคคลที่ยังไม่บรรลุนิติภาวะ ซึ่งมีอายุครบ 20 ปีบริบูรณ์ เว้นแต่

1) บุคคลที่มีอายุครบ 17 ปีบริบูรณ์ และได้ทำการสมรสตามกฎหมายสามารถรวบรวมข้อมูลส่วนบุคคลโดยได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลนั้นได้

2) ผู้เยาว์ที่มีฐานะดั่งเช่นบุคคลที่บรรลุนิติภาวะแล้ว ซึ่งผู้แทนโดยชอบธรรมได้ให้ความยินยอมในการทำธุรกิจ การค้า ทำสัญญาจ้างแรงงานไว้แล้ว

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

4) ผู้เยาว์ที่มีอายุต่ำกว่า 10 ปี การขอความยินยอมในการรวบรวมข้อมูลส่วนบุคคลจะต้องขอกับผู้ใช้อำนาจปกครอง

**ข้อ 11** การใช้ข้อมูลส่วนบุคคล ให้พนักงานดำเนินการดังนี้

1) ห้ามมิให้ใช้ข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมหรือมีฐานรับเพื่อให้เกิดความชอบด้วยกฎหมาย

2) ห้ามมิให้ใช้ข้อมูลส่วนบุคคลโดยไม่มีความจำเป็น

3) ห้ามมิให้ใช้ข้อมูลส่วนบุคคลโดยมิได้แจ้งรายละเอียดเอาไว้ในการแจ้งรายละเอียดความเป็นส่วนตัว หรือ Privacy Notice

4) ห้ามมิให้ใช้ข้อมูลส่วนบุคคลนอกจากวัตถุประสงค์ที่ได้ขอความยินยอมไว้จากเจ้าของข้อมูลส่วนบุคคล

5) ห้ามมิให้ใช้ข้อมูลส่วนบุคคลเพื่อการอื่นนอกจากกิจการของบริษัท

6) ห้ามมิให้ทำลาย คัดลอกทำสำเนา เปิดเผย ขโมยหรือเอาไปเสียซึ่งอุปกรณ์การจัดเก็บหรือประมวลผลข้อมูลส่วนบุคคล

7) เมื่อพ้นกำหนดระยะเวลาการเก็บข้อมูลส่วนบุคคล ห้ามมิให้ใช้ข้อมูลส่วนบุคคลต่อไป เว้นแต่จะมีกฎหมายกำหนด และให้รายงานผู้บริหาร

8) ห้ามมิให้เข้าถึงข้อมูลส่วนบุคคลที่ถูกควบคุมการเข้าถึง เว้นแต่จะได้รับอนุญาตจากผู้บริหาร

**ข้อ 12** การใช้หรือเปิดเผยข้อมูลส่วนบุคคล ให้พนักงานดำเนินการดังนี้

1) ห้ามมิให้ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่อยู่ในความควบคุมของบริษัทโดยไม่ได้รับความยินยอม หรือมีฐานทางกฎหมายรองรับเพื่อความชอบธรรมในการเปิดเผยข้อมูลส่วนบุคคล

2) ห้ามมิให้ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อการอื่นนอกเหนือจากวัตถุประสงค์ที่ได้แจ้งเอาไว้ในขณะรวบรวมข้อมูลส่วนบุคคล และดังที่ได้แจ้งเอาไว้ในการแจ้งรายละเอียดความเป็นส่วนตัว หรือ Privacy Notice

3) การใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ไม่ได้รับความยินยอม แต่สามารถอ้างฐานอื่นเพื่อความชอบธรรม ได้ให้ผู้บริหารดำเนินการให้มีการบันทึกการใช้ หรือเปิดเผยเอาไว้ในบันทึกรายการกิจกรรมข้อมูลส่วนบุคคล หรือ Ropa

4) ห้ามมิให้โอนข้อมูลส่วนบุคคล หรือส่งข้อมูลไปต่างประเทศ เว้นแต่จะได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล หรือมีฐานรองรับเพื่อให้เกิดความชอบธรรม หรือนโยบายการคุ้มครองข้อมูลส่วนบุคคลของบริษัทจะได้รับการตรวจสอบและรับรองจากสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

5) การดำเนินการจะต้องได้รับการอนุญาตจากผู้บริหาร และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

6) ห้ามมิให้เปิดเผยข้อมูลส่วนบุคคลโดยมิได้แจ้งประเภทของบุคคลหรือหน่วยงานเอาไว้ในการแจ้งรายละเอียดความเป็นส่วนตัว หรือ Privacy Notice

7) กรณีส่งข้อมูลให้กับบุคคลภายนอกซึ่งอยู่ในราชอาณาจักรเพื่อทำการประมวลผลข้อมูลผู้บริหารและพนักงานจะต้องดำเนินเพื่อป้องกันมิให้ผู้นั้นใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือมิชอบ ดังนี้

(ก) จัดทำสัญญาการประมวลผลข้อมูลส่วนบุคคล

(ข) ตรวจสอบนโยบายการคุ้มครองข้อมูลส่วนบุคคลของบุคคลภายนอกซึ่งเป็นผู้ประมวลผล

(ค) ผู้ประมวลผลต้องมีการดำเนินการตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลโดยครบถ้วน

**ข้อ 13** ให้ผู้บริหาร ดำเนินการบันทึกกิจกรรมการใช้ข้อมูลส่วนบุคคล (Ropa) ให้ถูกต้อง เป็นปัจจุบัน และแจ้งการดำเนินการ หรือปรับปรุงการดำเนินงานให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลทราบ และให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลปรับปรุงข้อมูลในการแจ้งรายละเอียดการใช้ข้อมูลส่วนบุคคลให้ถูกต้องเป็นปัจจุบัน

**ข้อ 14** ให้ผู้บริหาร พนักงาน และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลด้วยเหตุดังนี้

1) เมื่อพ้นกำหนดระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล

2) เมื่อไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น

3) ตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ หรือที่เจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอม เว้นแต่

เก็บรักษาไว้เพื่อวัตถุประสงค์ในการใช้เสรีภาพในการแสดงความคิดเห็นการเก็บรักษาไว้เพื่อวัตถุประสงค์ตามที่มีฐานอื่น อันได้แก่

(ก) ข้อมูลทั่วไป ฐานการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือการศึกษาวิจัย หรือฐานป้องกันหรือระงับอันตรายต่อชีวิต ร่างกายหรือสุขภาพ หรือฐานจำเป็นเพื่อปฏิบัติตามสัญญา หรือฐานประโยชน์สาธารณะ หรือฐานประโยชน์อันชอบธรรมของผู้ควบคุมข้อมูลส่วนบุคคล หรือฐานปฏิบัติตามกฎหมาย

(ข) ข้อมูลอ่อนไหว เป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับ

- เวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ การประเมินความสามารถในการทำงานของลูกจ้าง การวินิจฉัยโรคทางการแพทย์ การให้บริการด้านสุขภาพหรือด้านสังคม การรักษาทางการแพทย์ การจัดการด้านสุขภาพ หรือระบบและการให้บริการด้านสังคมสงเคราะห์ ทั้งนี้ ในกรณีที่ไม่ใช่การปฏิบัติตามกฎหมายและข้อมูลส่วนบุคคลนั้นอยู่ในความรับผิดชอบของผู้ประกอบอาชีพหรือวิชาชีพหรือผู้มีหน้าที่รักษาข้อมูลส่วนบุคคลนั้นไว้เป็นความลับตามกฎหมาย ต้องเป็นการปฏิบัติตามสัญญาระหว่างเจ้าของข้อมูลส่วนบุคคลกับผู้ประกอบวิชาชีพทางการแพทย์

- ประโยชน์สาธารณะด้านการสาธารณสุข เช่น การป้องกันด้านสุขภาพจากโรคติดต่ออันตรายหรือโรคระบาดที่อาจติดต่อหรือแพร่เข้ามาในราชอาณาจักร หรือการควบคุมมาตรฐานหรือคุณภาพของยาเวชภัณฑ์ หรือเครื่องมือแพทย์ ซึ่งได้จัดให้มีมาตรการที่เหมาะสมและเจาะจงเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลโดยเฉพาะการรักษาความลับของข้อมูลส่วนบุคคลตามหน้าที่หรือตามจริยธรรมแห่งวิชาชีพ

## หมวดที่ 3
## การรักษาความมั่นคงปลอดภัย

**ข้อ 15** การรักษาความมั่นคงปลอดภัย เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ ผู้บริหาร และพนักงาน หรือบุคคลากรไม่ว่าจะอยู่ในตำแหน่งหรือสถานะใดต้องดำเนินการให้ครอบคลุมใน 3 หัวข้อ ดังนี้

1) การธำรงไว้ซึ่งความลับ
2) ความถูกต้อง ครบถ้วน
3) สภาพพร้อมใช้งาน

**ข้อ 16** ให้ผู้บริหาร และพนักงาน หรือบุคคลากรไม่ว่าจะอยู่ในตำแหน่งหรือสถานะใดการดำเนินการรักษาความมั่นคงปลอดภัยต้องดำเนินการใน 3 ด้าน ดังนี้

1) ด้านบริหาร

2) ด้านเทคนิค

3) ด้านกายภาพ

การดำเนินการ อย่างน้อยต้องเป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนด

**ข้อ 17** การดำเนินการรักษาความมั่นคงปลอดภัยด้านบริหาร ให้ผู้บริหาร และพนักงาน หรือบุคคลากรไม่ว่าจะอยู่ในตำแหน่งหรือสถานะใดดำเนินการดังนี้

1) ผู้บริหาร พนักงานจะต้องดำเนินการตามระเบียบที่เกี่ยวกับการรวบรวม ใช้ และเปิดเผย ในข้อ 8 ถึงข้อ 14 โดยเคร่งครัด

2) การใช้งาน การเข้าถึงข้อมูลส่วนบุคคล การเข้าพื้นที่ซึ่งมีการเก็บข้อมูลส่วนบุคคลที่ถูกจัดไว้เป็นความลับพนักงานจะต้องมีการขออนุญาตจากผู้บริหารที่ได้รับมอบหมายให้เป็นผู้อนุญาต

3) ให้ผู้บริหารมีการกำหนดรายชื่อพนักงานผู้มีสิทธิเข้าถึงข้อมูลส่วนบุคคล โดยออกเป็นประกาศภายในส่วนงานในการเข้าถึงข้อมูลส่วนบุคคลของผู้ใช้งาน (user responsibilities) ผู้บริหารอาจแบ่งเป็น รูปแบบต่าง ๆ เช่น สิทธิในการเข้าอ่านอย่างเดียว หรือสิทธิในการแก้ไขเพิ่มเติม สิทธิในการเปิดเผยและเผยแพร่ สิทธิในการตรวจสอบคุณภาพข้อมูล สิทธิในการลบทำลาย ทั้งนี้บริษัทจะประกาศให้ทราบต่อไป

4) บุคคลตามข้อ 3) หากจะเข้าถึงข้อมูลเพื่ออ่าน หรือเพื่อแก้ไขเพิ่มเติม หรือเพื่อเปิดเผยและเผยแพร่ หรือตรวจสอบคุณภาพข้อมูล หรือลบทำลายข้อมูล จะกระทำได้ต่อเมื่อได้ขออนุญาตจากผู้บริหาร โดยให้ผู้บริหารตรวจสอบสิทธิตามประกาศ ตรวจสอบว่าการขอใช้สิทธิดังกล่าวมีเหตุอันสมควรและชอบด้วยกฎหมายหรือไม่ หรือการเข้าออกพื้นที่ หรือสถานที่ หรืออุปกรณ์เก็บข้อมูลส่วนบุคคล และให้ลงบันทึกการเข้าใช้งานเอาไว้ ซึ่งการบันทึกอาจทำในรูปกระดาษ หรืออิเล็กทรอนิกส์ก็ได้

5) เมื่อมีการเข้าถึงข้อมูลส่วนบุคคลตามข้อ 4) แล้ว ผู้บริหารจะต้องมีการตรวจสอบถูกแก้ไข ถูกคัดลอก หรือ ถูกทำลาย หรือมีการกระทำที่ผิดกฎหมายหรือระเบียบนี้หรือไม่

6) ให้พนักงานและบุคลากรทุกคนปฏิบัติตามระเบียบการใช้เทคโนโลยีสารสนเทศอย่างเคร่งครัด

**ข้อ 18** การดำเนินการรักษาความมั่นคงปลอดภัยด้านเทคนิค ให้ผู้บริหาร และพนักงาน หรือบุคคลากรไม่ว่าจะอยู่ในตำแหน่งหรือสถานะใดดำเนินการดังนี้

1) ให้ฝ่ายเทคโนโลยีสารสนเทศจัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง ลบ หรือถ่ายโอนข้อมูลส่วนบุคคล ให้สอดคล้องเหมาะสมกับวิธีการและสื่อที่ใช้ในการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคล

2) ให้ฝ่ายเทคโนโลยีสารสนเทศการบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) เพื่อควบคุมการเข้าถึงข้อมูลส่วนบุคคลเฉพาะผู้ที่ได้รับอนุญาต ตามระดับสิทธิการใช้งาน ได้แก่ การนำเข้า เปลี่ยนแปลง แก้ไข เปิดเผย ตลอดจนการลบทำลาย

3) ให้ฝ่ายเทคโนโลยีสารสนเทศจัดให้มีระบบสำรองและกู้คืนข้อมูล เพื่อให้ระบบ และ/หรือ บริการต่าง ๆ ยังสามารถดำเนินการได้อย่างต่อเนื่อง โดยดำเนินการสำรองข้อมูลทุกวัน

4) ให้ฝ่ายเทคโนโลยีสารสนเทศจัดให้มีระบบการป้องกันการกระทำที่มิชอบด้วยกฎหมายซึ่งข้อมูลส่วนบุคคลโดยใช้เทคโนโลยีที่เหมาะสม เช่น การติดตั้งไฟล์วอลแบบมาตรฐาน หรือระบบปัญญาประดิษฐ์ หรือ AI

5) การใช้คอมพิวเตอร์ในพื้นที่ซึ่งมีบุคคลภายนอกสามารถมองเห็นหน้าจอได้ พนักงานจะต้องปรับมุมคอมพิวเตอร์เพื่อป้องกันการมองเห็น รวมถึงการใช้ Screen saver หรือต้องมีการพักหน้าจอเอาไว้

6) เมื่อใช้งานคอมพิวเตอร์ทำงานที่เกี่ยวกับข้อมูลส่วนบุคคลเสร็จสิ้น ห้ามมิให้พนักงานเก็บข้อมูลเอาไว้ตรงส่วน Desktop จะต้องจัดเก็บข้อมูลเอาไว้ในเครื่องมือ หรืออุปกรณ์ หรือตู้ หรือพื้นที่ซึ่งมีระบบป้องกันการเข้าถึง หรือการตั้งรหัสผ่านทุกครั้ง

7) การใช้ข้อมูลทางด้านสารสนเทศพนักงานต้องมีการตั้งรหัสผ่าน และเก็บรหัสผ่านเอาไว้ในสถานที่ปลอดภัย และธำรงไว้ซึ่งความลับ

8) ห้ามมิให้พนักงานคัดลอกข้อมูลส่วนบุคคล (Copy) หรือการทำซ้ำข้อมูลไม่ว่าจะผ่านอุปกรณ์เครื่องมือ โดยไม่ได้รับอนุญาตจากผู้บริหาร

9) ห้ามมิให้พนักงานเคลื่อนย้ายข้อมูลผ่านระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตจากผู้บริหาร และการส่งต่อนั้นจะต้องมีการตั้งรหัสผ่านเพื่อป้องกันการเข้าถึง

10) ห้ามมิให้พนักงานจัดเก็บข้อมูลส่วนบุคคลเอาไว้ในคอมพิวเตอร์ Note Book เว้นแต่คอมพิวเตอร์เครื่องที่ได้รับอนุญาตจากบริษัท ภายใต้เงื่อนไขที่ต้องดูแลคอมพิวเตอร์นั้นเป็นอย่างดี

11) การใช้คอมพิวเตอร์ส่วนบุคคล Notebook ที่มีข้อมูลสำคัญ พนักงานจะต้องมีการรักษาความมั่นคงปลอดภัยที่มากกว่าคอมพิวเตอร์ทั่วไป เช่น ต้องมีการเข้ารหัส (Encrypted) โดยการกำหนดรหัสแทนชื่อบุคคล รวมถึงมีมาตรการอื่นเสริม เช่น มีการกำหนดรหัสผ่าน (Password)

12) พนักงานจะต้องจัดเก็บข้อมูลส่วนบุคคลเอาไว้ในพื้นที่ซึ่งบริษัทจัดหาให้ และแจ้งให้พนักงานทราบ

13) ห้ามมิให้พนักงานจัดเก็บข้อมูลส่วนบุคคลในอุปกรณ์บันทึกข้อมูลแบบพกพา เช่น Hard Disk แบบ External หรือ Flash Drive

14) กรณีพนักงานทำงานจากระยะไกล ซึ่งไม่ใช่ที่บริษัทหากจะมีการเข้าระบบคอมพิวเตอร์ จะต้องมีมาตรการป้องกันการถูกโจมตีที่เหมาะสม และต้องได้รับอนุญาตจากผู้บริหาร

15) ห้ามมิให้พนักงานนำอุปกรณ์ต่าง ๆ จากภายนอกมาต่อพ่วงเข้ากับระบบคอมพิวเตอร์ของบริษัท เว้นแต่จะได้รับอนุญาตจากผู้บริหาร

16) เมื่อมีการพิมพ์งานซึ่งมีข้อมูลส่วนบุคคล พนักงานจะต้องมีการรักษาความปลอดภัย

17) ห้ามมิให้พนักงานทำการเปลี่ยนแปลงเครือข่าย เช่น IP Address หรืออุปกรณ์อื่นโดยไม่ได้รับอนุญาตจากผู้บริหารของฝ่ายเทคโนโลยีสารสนเทศ

18) ให้ฝ่ายเทคโนโลยีสารสนเทศทบทวนมาตรการที่เหมาะสมเพื่อป้องกันการสูญหาย การเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลให้สอดคล้องกับการเปลี่ยนแปลงของเทคโนโลยีเพื่อให้เกิดประสิทธิภาพในการรักษาความมั่นคงปลอดภัยทางเทคนิคที่เหมาะสม

19) พนักงานจะต้องปฏิบัติตามระเบียบการใช้เทคโนโลยีสารสนเทศของบริษัทอย่างเคร่งครัด

**ข้อ 19** การดำเนินการรักษาความมั่นคงปลอดภัยด้านกายภาพ ให้ผู้บริหาร และพนักงาน หรือบุคคลากรไม่ว่าจะอยู่ในตำแหน่งหรือสถานะใดดำเนินการดังนี้

1) ให้ฝ่ายผู้บริหารแต่ละฝ่าย หรือพนักงานแต่ละแผนกจัดให้มีการควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์ในการจัดเก็บ และประมวลผลข้อมูลส่วนบุคคลโดยคำนึงถึงการใช้งาน และความมั่นคงปลอดภัย โดยมีตู้ ซึ่งมีการล็อกกุญแจจัดเก็บข้อมูลส่วนบุคคล หรือมีห้องเก็บเอกสาร หรือมีการติดตั้งกล้อง CCTV หรืออาจมีการกำหนดให้ล้อมรั้ว หรือกำหนดให้ต้องมีบัตรผ่านเข้าออก

2) การดำเนินการตามข้อ 1 หากมีการรวบรวมข้อมูลส่วนบุคคลให้ถือว่าเป็นการดำเนินการโดยอ้างฐานประโยชน์อันชอบธรรมของบริษัท จึงไม่ต้องขอความยินยอม แต่ให้ดำเนินการตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลให้ถูกต้อง

3) การขออนุญาตเข้าถึงข้อมูลส่วนบุคคล ผู้บริหารจะต้องบันทึกการเปิดตู้ หรือการเข้าพื้นที่จัดเก็บข้อมูลเอาไว้

4) ในการปฏิบัติงาน กรณีที่มีการทำงานอย่างต่อเนื่อง ซึ่งงานนั้นมีข้อมูลส่วนบุคคล หากปฏิบัติงานนั้นเสร็จแล้ว พนักงานจะต้องมีการจัดเก็บเอกสารหรือข้อมูลนั้นเป็นความลับในทันที ห้ามมิให้วางเอกสารไว้ในที่ใด ๆ ซึ่งไม่มีมาตรการป้องกัน โดยพนักงานจะต้องดำเนินการจัดเก็บเอาไว้ในสถานที่ซึ่งมีการป้องกันการเข้าถึงเชิงกายภาพเอาไว้ เช่น มีตู้ มีกุญแจ มีห้องเก็บเอกสาร มีกล้อง CCTV มีเจ้าหน้าที่ช่วยกันสอดส่องดูแล

## หมวดที่ 4
## แจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

**ข้อ 20** ให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลเป็นผู้รับผิดชอบกิจกรรมและวิธีการแจ้งเหตุละเมิดให้แก่ผู้บริหารสูงสุด หรือผู้ได้รับมอบหมาย พร้อมทั้งแจ้งตัวแทนของสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลได้ทราบโดยการส่งอีเมลล์ แต่ถ้าจำเป็นจะต้องแจ้งโดยทางโทรศัพท์

**ข้อ 21** กรณีความเสี่ยงต่ำ ซึ่งมีมีผลกระทบต่อสิทธิและเสรีภาพของบุคคลไม่ร้ายแรง เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลไม่จำเป็นต้องแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

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

อนึ่ง การกระทำดังกล่าวในวรรคแรก หากมีการโจรกรรมข้อมูลส่วนบุคคลให้ถือเป็นความเสี่ยงสูง

นอกจากนี้ความเสี่ยงต่ำอาจพิจารณาจากจำนวนผู้เสียหาย จำนวนข้อมูลส่วนบุคคล ความยากง่ายในการเข้าถึงข้อมูลส่วนบุคคลซึ่งมีการกำหนดหรือตั้งค่าการเข้าถึง

กรณีความเสี่ยงต่ำให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลดำเนินการเพียงบันทึกเหตุการณ์ไว้เป็นการภายในก็เพียงพอ โดยไม่จำเป็นต้องแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบ และไม่จำเป็นต้องแจ้งเจ้าของข้อมูลส่วนบุคคลทราบ

**ข้อ 22** กรณีมีความเสี่ยงสูง ซึ่งอาจกระทบต่อสิทธิและเสรีภาพของบุคคล ผู้โจมตีทำการฝังมัลแวร์ หรือไวรัสเพื่อเข้าถึงข้อมูลส่วนบุคคล หรือปริมาณข้อมูลส่วนบุคคลจำนวนมาก ถือว่ามีความเสี่ยงสูงที่เหตุการณ์ดังกล่าวจะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล เช่นนี้ ให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลดำเนินการบันทึกไว้เป็นการภายในถึงการเข้าโจมตี และการโจรกรรมข้อมูล และแจ้งเหตุดังกล่าวโดยไม่ชักช้าภายใน 72 ชั่วโมงนับตั้งแต่ทราบเหตุเท่าที่สามารถทำได้ ไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบ และ ยังต้องแจ้งเจ้าของข้อมูลส่วนบุคคลทราบด้วย

กรณีที่บริษัททำหน้าที่เป็นผู้ประมวลผล ให้แจ้งแก่ผู้ควบคุมข้อมูลส่วนบุคคลถึงเหตุที่มีการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น

**ข้อ 23** ให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล แจ้งการละเมิดต่อเจ้าของข้อมูลส่วนบุคคลให้ทราบ และแจ้งแนวทางการเยียวยาความเสียหายแก่เจ้าของข้อมูลส่วนบุคคลโดยไม่ชักช้า ทั้งนี้ ตามความเสียหายที่แท้จริง โดยรายงานไปยังผู้บริหารสูงสุดหรือที่ได้รับมอบหมายเพื่อดำเนินการต่อไป

**ข้อ 24** ให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลสอบสวนหาสาเหตุการละเมิดข้อมูลส่วนบุคคลในทันทีว่าลักษณะการละเมิดข้อมูลส่วนบุคคลเป็นอย่างไร ประเภทและจำนวนข้อมูลส่วนบุคคลอะไร แหล่งที่เกิดการละเมิดข้อมูลส่วนบุคคลเกิด ณ จุดใด ผลกระทบที่เกิดขึ้นมีอะไรบ้าง และหามาตรการป้องกันที่เหมาะสมในทันที

## หมวดที่ 5
## วินัยและโทษทางวินัยของการไม่ปฏิบัติตามระเบียบ

**ข้อ 25** พนักงานซึ่งไม่ปฏิบัติตามระเบียบนี้ หรือระเบียบอื่น หรือประกาศนโยบายคุ้มครองข้อมูลส่วนบุคคล หรือพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และกฎหมายลำดับรองที่เกี่ยวข้องจนเป็นเหตุให้ข้อมูลรั่วไหล หรือนำข้อมูลส่วนบุคคลไปใช้ หรือเปิดเผยต่อบุคคลภายนอกโดยไม่มีหน้าที่ หรือไม่ได้รับอนุญาตให้เข้าถึงข้อมูลส่วนบุคคล อาจได้รับโทษทางวินัยในระดับการออกหนังสือตักเตือน

อนึ่ง หากการดำเนินการฝ่าฝืนระเบียบตามวรรคแรกเป็นเหตุให้เกิดการรั่วไหลของข้อมูลส่วนบุคคลจนเกิดความเสี่ยงสูง พนักงานจะได้รับโทษถึงขั้นเลิกจ้างโดยไม่จ่ายค่าชดเชย รวมถึงอาจต้องรับผิดในทางแพ่ง อาญา และทางปกครอง

บริษัทฯขอสงวนสิทธิ์ในการแก้ไขเปลี่ยนแปลงหรือยกเลิกประกาศนี้ได้ตามความเหมาะสม

ทั้งนี้ให้มีผลตั้งแต่วันที่ 1 มิถุนายน พ.ศ. 2565

ประกาศ ณ วันที่ 23 พฤษภาคม พ.ศ. 2565

.....

(ดร.ทิศพล นครศรี)

ประธานกรรมการบริหาร