บริษัท ทางยกระดับดอนเมือง จำกัด (มหาชน)
Don Muang Tollway Public Company Limited

40/40 ถนนวิภาวดีรังสิต แขวงสนามบิน
เขตดอนเมือง กรุงเทพฯ 10210
โทร : (66) (02) 792-6500
โทรสาร : (66) (02) 552-8065
เลขทะเบียน บมจ. 0107537001129

40/40 ViphavadiRangsit Road,
Sanambin, DonMuang, Bangkok 10210
Tel. : (66) (02) 792-6500
Fax. : (66) (02) 552-8065
Plc Registration No. 0107537001129

แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล
(Personal Data Protection Practice guideline)

บริษัท ทางยกระดับดอนเมือง จำกัด (มหาชน) (**"บริษัทฯ"**) ตระหนักถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection) ซึ่งเป็นสิทธิขั้นพื้นฐานสำคัญในความเป็นส่วนตัวที่ต้องได้รับความคุ้มครองตามรัฐธรรมนูญแห่งราชอาณาจักรไทย โดยบริษัทได้ประกาศใช้นโยบายคุ้มครองข้อมูลส่วนบุคคลเพื่อให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เมื่อวันที่ 30 พฤษภาคม 2563

บริษัทฯ จึงจัดทำแนวปฏิบัติตามนโยบายในการคุ้มครองข้อมูลส่วนบุคคลฉบับนี้ขึ้น เพื่อป้องกันการล่วงละเมิดสิทธิความเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคล และเพื่อให้บริษัทฯ มีการควบคุมภายในด้านการเก็บรวบรวม ใช้ เปิดเผย เก็บรักษา ประมวลผล มาตรการคุ้มครองส่วนบุคคลที่ดี มีความมั่นคงปลอดภัย เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 และกฎหมายอื่นที่เกี่ยวข้อง รวมถึงให้สอดคล้องกับนโนบายและแนวปฏิบัติอื่นๆ ที่บริษัทได้จัดทำขึ้นด้วย ทั้งนี้ผู้บริหารและพนักงานทุกคนรวมถึงผู้เกี่ยวข้อง ดำเนินการจัดการข้อมูลส่วนบุคคลให้เป็นไปในแนวทางเดียวกันและสอดคล้องตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ให้ความร่วมมือในการปฏิบัติตามรายละเอียดดังต่อไปนี้

1. คำนิยาม

เจ้าของข้อมูลส่วนบุคคล (Data Subject)	หมายถึง บุคคลซึ่งสามารถถูกระบุตัวตนได้โดยข้อมูลส่วนบุคคลนั้น ๆ ไม่ว่าโดยทางตรงหรือทางอ้อม
ข้อมูลส่วนบุคคล (Personal Data)	หมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ (มาตรา 6 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562) เช่น ชื่อ นามสกุล อีเมล์ รูป ลายนิ้วมือ รหัสประชาชน ซึ่งสามารถระบุตัวบุคคลได้ในทางตรง หรือการเก็บ Location หรือ Cookie เป็นการเก็บข้อมูลซึ่งทำให้สามารถระบุตัวบุคคลได้ในทางอ้อม นอกจากนี้ ข้อมูลที่โดยพื้นฐานแล้วไม่สามารถนำไประบุตัวบุคคลได้แต่เมื่อนำไปใช้ร่วมกับข้อมูลอื่นแล้วก่อให้เกิดชุดข้อมูลที่สามารถระบุข้อมูลส่วนบุคคลได้ ก็ถือเป็นข้อมูลส่วนบุคคลเช่นกัน เช่น ที่อยู่ เพศ และอายุ ที่เมื่อนำมารวมกันแล้วสามารถระบุตัวบุคคลได้
การประมวลผลข้อมูลส่วนบุคคล (Processing)	หมายถึง การดำเนินการใด ๆ ซึ่งกระทำต่อข้อมูลส่วนบุคคลหรือชุดข้อมูลส่วนบุคคล ไม่ว่าจะโดยวิธีการอัตโนมัติหรือไม่ เช่น การเก็บ บันทึก จัดระบบ จัดโครงสร้างเก็บรักษา เปลี่ยนแปลงหรือปรับเปลี่ยน การรับ พิจารณา ใช้ เปิดเผยด้วยการส่งต่อ เผยแพร่ หรือการกระทำอื่นใดซึ่งทำให้เกิดความพร้อม ใช้งาน การจัดวางหรือผสมเข้าด้วยกัน การจำกัด การลบ หรือการทำลาย

ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)	หมายถึง บุคคลหรือนิติบุคคลซึ่งเป็นผู้ที่มีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคล
ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)	หมายถึง ผู้ซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล
ข้อมูลบริษัท	หมายถึง ข้อมูลในรูปแบบใดก็ตามทั้งในแบบอิเล็กทรอนิกส์และไม่ใช่อิเล็กทรอนิกส์ เช่น ข้อมูลในสิ่งพิมพ์ซึ่งอยู่ในระบบภายในหรือระบบภายนอกที่นอกเหนือการควบคุมของบริษัทฯ และปรากฏเงื่อนไขดังต่อไปนี้ - ข้อมูลที่พนักงานของบริษัทฯ หรือบุคคลที่ได้รับมอบหมายได้มา ประมวลผล จัดการ และ/หรือ ดูแล (เช่น ผู้รับเหมา หน่วยงานภายนอก ที่ปรึกษา) เพื่อปฏิบัติหน้าที่ - ข้อมูลที่เกี่ยวเนื่องกับการจัดการ การปฏิบัติงาน วางแผน รายงาน หรือการตรวจสอบการดำเนินงานของบริษัทฯ - ข้อมูลที่ใช้อ้างอิงหรือจำเป็นต่อการทำงานของหน่วยงานอย่างน้อยหนึ่งหน่วย
การเข้าถึงข้อมูล (Access)	หมายถึง สิทธิในการอ่าน/ดู บันทึก คัดลอก เก็บสำรอง จัดเก็บ สืบค้น ดาวน์โหลด หรือแก้ไข (อัพเดท แทรก/เพิ่ม ลบ) ข้อมูล รวมถึงการจัดการสิทธิการเข้าถึงนั้น ๆ
ผู้ใช้ หรือ ผู้ใช้ข้อมูล (Data Users)	หมายถึง บุคคลดังต่อไปนี้ - พนักงานบริษัท ทางยกระดับดอนเมือง จำกัด (มหาชน) - บุคลากรที่บริษัทฯ กำหนดให้เข้าถึงข้อมูล เพื่อปฏิบัติงานตามที่ได้รับมอบหมาย เช่น ผู้รับเหมา หน่วยงานภายนอก ที่ปรึกษาฯ - บุคลากรของพันธมิตรของบริษัทฯ ซึ่งได้รับความยินยอม/อนุญาตจากบริษัทฯ ให้เข้าถึงข้อมูลอย่างเฉพาะเจาะจงและจำกัด เพื่อปฏิบัติงานตามที่ได้รับมอบหมาย ซึ่งเป็นไปเพื่อสนับสนุนการดำเนินงานของบริษัทฯ
หน่วยธุรกิจ	หมายถึง สายงาน ฝ่ายงาน หรือหน่วยปฏิบัติงานภายใต้ความรับผิดชอบของบริษัทฯ เพื่อกิจกรรมเฉพาะขององค์กร
การบันทึก (Record)	หมายถึง ข้อมูลหรือสารสนเทศในรูปแบบเฉพาะ ซึ่งถูกสร้างขึ้นหรือได้มาจากกิจกรรมบุคคลหรือกิจกรรมองค์กร และได้สำรอง (เก็บรักษา) ไว้เป็นหลักฐานของกิจกรรมนั้น ๆ เพื่อใช้อ้างอิงในอนาคต
บริษัทฯ	หมายถึง บริษัท ทางยกระดับดอนเมือง จำกัด (มหาชน)
แนวปฏิบัติ	หมายถึง ข้อปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลที่บริษัทฯ กำหนดขึ้นและประกาศใช้
กฎหมายคุ้มครองข้อมูลส่วนบุคคล	หมายถึง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และที่จะมีการแก้ไขเพิ่มเติม รวมถึงกฎระเบียบ และคำสั่งที่เกี่ยวข้อง

2. วัตถุประสงค์

บริษัทฯ ตระหนักถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคล เนื่องจากการคุ้มครองข้อมูลส่วนบุคคลเป็นส่วนหนึ่งของการรับผิดชอบต่อสังคมและเป็นรากฐานในการสร้างความสัมพันธ์ทางธุรกิจที่น่าเชื่อถือกับลูกค้า บริษัทฯ จึงยึดมั่นในการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล และกฎเกณฑ์ทางการอื่น ๆ ที่เกี่ยวข้อง

เอกสารฉบับนี้ได้รับการจัดทำขึ้นโดยมีวัตถุประสงค์ ดังต่อไปนี้

- เพื่อชี้แจงความรับผิดชอบเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลเพื่อกำหนดแนวปฏิบัติให้ผู้บริหาร พนักงาน ลูกค้า บริษัทร่วมค้า และบุคคลภายนอกที่ปฏิบัติงานให้กับบริษัทฯ ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย ในการรวบรวม ใช้ เปิดเผย หรือเก็บรักษาข้อมูลตามที่กฎหมายกำหนด รับรู้สิทธิและหน้าที่ในการเข้าถึงหรือขอใช้ข้อมูลส่วนบุคคลนั้น เพื่อป้องกันไม่ให้ทุกคนในบริษัทฯและบุคคลที่เกี่ยวข้องกระทำความผิดตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562
- เพื่อกำหนดมาตรฐานและแนวทางบริหารข้อมูลส่วนบุคคล โดยครอบคลุมถึงการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล

3. ขอบเขต

แนวปฏิบัติฉบับนี้ใช้บังคับการจัดเก็บข้อมูลส่วนบุคคลซึ่งมีการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลโดยครอบคลุมถึงบุคลากรทั้งหมด ได้แก่ พนักงานประจำ พนักงานชั่วคราว พนักงานสัญญาจ้าง รวมถึงสายงานหน่วยธุรกิจ และบริษัทภายใต้การควบคุมของบริษัทฯ รวมถึงพันธมิตรของบริษัทฯ ซึ่งมีส่วนร่วมในการเข้าถึงหรือประมวลผลข้อมูลของบริษัทฯ นอกจากนี้ยังครอบคลุมถึงการส่งต่อข้อมูลสู่องค์กรภายนอก หน่วยงานราชการ หรือบุคคลที่ได้รับอนุญาตตามกฎหมาย ข้อบังคับ หรือข้อบังคับกฎหมายอื่น ๆ และใช้บังคับกับข้อมูลทุกรูปแบบทั้งข้อมูลอิเล็กทรอนิกส์และไม่ใช่อิเล็กทรอนิกส์

4. คำแถลงแนวปฏิบัติ

4.1 แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล

- แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลนี้ บริษัทฯ ต้องจัดให้มีการประกาศและสื่อสารไปยังพนักงานและหน่วยงานที่เกี่ยวข้องและกำหนดให้มีการทบทวนและปรับปรุงแนวปฏิบัติฉบับนี้ให้เป็นปัจจุบันอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง
- การประมวลผลข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลจะต้องเป็นไปตามกฎหมาย มีความเป็นธรรม และมีความโปร่งใส
- การเก็บรวบรวมข้อมูลส่วนบุคคล จะต้องพอเหมาะเป็นไปตามวัตถุประสงค์ที่กำหนด เป็นไปตามฐานในการประมวลผลข้อมูลส่วนบุคคล
- การประมวลผลข้อมูลส่วนบุคคลจะต้องมีการประมวลผลข้อมูลส่วนบุคคลอย่างจำกัดและสอดคล้องตามวัตถุประสงค์ที่กำหนด
- การประมวลผลข้อมูลส่วนบุคคลจะต้องมีการปรับปรุงอยู่เสมอ รวมทั้งจะต้องมีการกำหนดขั้นตอนในการตรวจสอบ เพื่อให้ข้อมูลส่วนบุคคลมีความถูกต้องเป็นไปตามกฎหมายหรือหน่วยงานกำกับดูแลที่เกี่ยวข้องกำหนด

- บริษัทฯ อนุญาตให้จัดเก็บข้อมูลส่วนบุคคลภายในระยะเวลาที่บริษัทฯกำหนดเท่านั้น ข้อมูลส่วนบุคคลที่มีการจัดเก็บเกินระยะเวลาที่กำหนด ผู้รับผิดชอบจะต้องมีการลบ ทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้
- การประมวลผลข้อมูลส่วนบุคคลจะต้องคำนึงถึงความมั่นคงปลอดภัยสารสนเทศ ซึ่งรวมถึงการป้องกันการประมวลผลข้อมูลส่วนบุคคลโดยผู้ที่ไม่มีสิทธิ การลบหรือทำลายข้อมูลทั้งโดยความตั้งใจและไม่ตั้งใจ และรวมถึงการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศให้อยู่ในระดับที่บริษัทฯยอมรับได้

4.2 การปฏิบัติตามสิทธิของเจ้าของข้อมูลส่วนบุคคล (Rights of Data Subject)

- สายงานที่เกี่ยวข้องจะต้องพิจารณาถึงสิทธิของเจ้าของข้อมูลส่วนบุคคลดังต่อไปนี้
  - สิทธิในการเพิกถอนความยินยอม
  - สิทธิในการขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคล
  - สิทธิในการขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลที่เจ้าของข้อมูลส่วนบุคคลไม่ได้ให้ความยินยอม
  - สิทธิในการขอให้โอนย้ายข้อมูลส่วนบุคคลไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่น
  - สิทธิในการคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
  - สิทธิในการขอให้ลบ ทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้
  - สิทธิในการขอให้ระงับการใช้ข้อมูลส่วนบุคคล
  - สิทธิในการขอให้แก้ไขข้อมูลให้ถูกต้อง เป็นปัจจุบัน สมบูรณ์
- สายงานที่เกี่ยวข้องและ DPO จะต้องร่วมจัดทำบันทึกรายการการประมวลผลข้อมูลส่วนบุคคล โดยรายละเอียดของบันทึกรายการการประมวลผลข้อมูลส่วนบุคคลจะต้องมีความสอดคล้องกับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และหลักเกณฑ์ที่เกี่ยวข้อง
- จัดให้มีการระบุช่องทางในการใช้สิทธิให้กับเจ้าของข้อมูลส่วนบุคคลทราบ
- สายงานที่เกี่ยวข้องและ DPO จะต้องบันทึกรายละเอียดเกี่ยวกับการขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล โดยต้องประกอบด้วยข้อมูลดังต่อไปนี้
  - รายละเอียดของเจ้าของข้อมูลส่วนบุคคล
  - รายละเอียดการขอตามสิทธิของเจ้าของข้อมูลส่วนบุคคล
  - รายละเอียดของการดำเนินการ ซึ่งรวมถึงเหตุผลในกรณีที่มีการปฏิเสธการขอตามสิทธิของเจ้าของข้อมูลส่วนบุคคล
- เมื่อมีการขอใช้สิทธิจากเจ้าของข้อมูลส่วนบุคคล หน่วยธุรกิจจะต้องปฏิบัติตามกระบวนการการขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลของบริษัทฯ โดยเคร่งครัด

4.3 การประมวลผลข้อมูลส่วนบุคคลให้สอดคล้องตามกฎหมาย (Lawfulness of Processing)

- สายงานที่เกี่ยวข้องและ DPO จะต้องร่วมกันทบทวนให้การประมวลผลข้อมูลส่วนบุคคลมีความสอดคล้องกับกฎหมาย โดยจะต้องระบุฐานในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

โดยการในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลจะต้องเป็นไปตามวัตถุประสงค์อันชอบด้วยกฎหมาย และมีความสอดคล้องกับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล โดยในการระบุฐานในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลสามารถพิจารณาได้ดังนี้

- ข้อมูลส่วนบุคคล
  - การขอความยินยอม
  - ความจำเป็นเพื่อการปฏิบัติตามสัญญา
  - ความจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล
  - ความจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมาย
  - ความจำเป็นเพื่อปฏิบัติตามกฎหมาย
  - เพื่อการวิจัยและสถิติ
  - เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล
- ข้อมูลส่วนบุคคลที่มีลักษณะอ่อนไหว กรณีเป็นข้อมูลส่วนบุคคลอ่อนไหว ได้แก่ ข้อมูลพันธุกรรม ข้อมูลชีวภาพ (ลายนิ้วมือ/แบบจำลองใบหน้า) ข้อมูลสุขภาพ ความพิการ หรือข้อมูลสุภาพจิต เชื้อชาติ เผ่าพันธุ์ ศาสนา ความเชื่อในลัทธิหรือปรัชญา ความคิดเห็นทางการเมือง พฤติกรรมทางเพศ (sexual behavior) ประวัติอาชญากรรม (officer record จากกรมตำรวจ) ข้อมูลสหภาพแรงงาน เป็นต้น
  - การขอความยินยอมโดยชัดแจ้ง
  - เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล
  - เป็นการดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมของมูลนิธิ สมาคม หรือองค์กรไม่แสวงหากำไรที่มีวัตถุประสงค์เกี่ยวกับการเมือง ศาสนา ปรัชญา หรือสหภาพแรงงานให้แก่สมาชิก ผู้ซึ่งเคยเป็นสมาชิก หรือผู้ซึ่งมีการติดต่ออย่างสม่ำเสมอกับมูลนิธิ สมาคม หรือองค์กรไม่แสวงหากำไรตามวัตถุประสงค์ดังกล่าวโดยไม่ได้เปิดเผยข้อมูลส่วนบุคคลนั้นออกไปภายนอกมูลนิธิ สมาคม หรือองค์กรไม่แสวงหากำไรนั้น
  - เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคล
  - ความจำเป็นเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย
  - ความจำเป็นเพื่อปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์ตามที่ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลระบุไว้

- หากหน่วยธุรกิจเลือกใช้วิธีการขอความยินยอม จะต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลเท่านั้น และจะต้องขอความยินยอมก่อนที่จะมีการประมวลผลเกิดขึ้น
- หากมีการเปลี่ยนแปลงวัตถุประสงค์ที่ใช้ฐานการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล จะต้องขอความยินยอมใหม่ทุกครั้ง
- หน่วยธุรกิจจะต้องมีการคำนึงถึงการเก็บหลักฐานของการขอความยินยอมไว้อย่างเหมาะสม

- การเปิดเผยข้อมูลจะต้องเป็นไปตามแนวทางและกระบวนการเปิดเผยข้อมูลที่บริษัทฯ กำหนดไว้

4.4 การโอนข้อมูลส่วนบุคคล (Personal Data Transfer)

- การถ่ายโอนข้อมูลส่วนบุคคลไปยังต่างประเทศจะต้องคำนึงถึงมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ และเป็นไปตามหลักเกณฑ์ของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
- ห้ามโอนถ่ายข้อมูลส่วนบุคคลให้กับผู้นำเข้าข้อมูลที่อยู่นอกประเทศ เว้นแต่
  - บริษัทฯ และผู้นำเข้าข้อมูลได้ตกลงกันเป็นลายลักษณ์อักษรเพื่อให้สัญญาเกี่ยวกับเจ้าของข้อมูลสมบูรณ์
  - เป็นการกระทำตามสัญญาเพื่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคล
  - เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของเจ้าของข้อมูลส่วนบุคคล
  - เมื่อได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลทราบในกรณีที่มาตรการคุ้มครองข้อมูลส่วนบุคคลของประเทศปลายทางไม่เพียงพอ
- การโอนถ่ายและการประมวลผลข้อมูลต้องดำเนินการด้วยวิธีที่ปลอดภัย และเป็นไปตามมาตรฐานความปลอดภัยขั้นต่ำของบริษัทฯ พร้อมทั้งสอดคล้องกับนโยบายและกระบวนการความมั่นคงปลอดภัยด้านสารสนเทศ

4.5 การควบคุมหน่วยงานภายนอกที่มีการประมวลผลข้อมูลส่วนบุคคล (Controlling Other Parties Involving the Processing of Personal Data)

- ให้สัญญาเกี่ยวกับการใช้หรือประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement: DPA)
- กรณีที่หน่วยงานภายนอกใช้ข้อตกลงเช็น NDA (Non-disclosure Agreement) ให้สายงานที่เกี่ยวข้องจะต้องมีการระบุรายละเอียดเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในสัญญาระหว่างบริษัทฯ และหน่วยงานภายนอก โดยจะต้องครอบคลุมเนื้อหาดังต่อไปนี้
  - ข้อตกลงการไม่เปิดเผยความลับและทุกข้อมูลส่วนุคคลที่การประมวลผล ต้องได้รับการรักษาความมั่นคง โดยห้ามนำข้อมูลไปใช้นอกเหนือจากที่กำหนดให้ดำเนินการ
  - รายละเอียดเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล
  - สิทธิของบริษัทฯ ในการตรวจสอบการประมวลผลข้อมูลส่วนบุคคลของหน่วยงานภายนอก
  - มาตรการการลบ ทำลาย หรือส่งคืนข้อมูลเมื่อสิ้นสุดระยะเวลาการประมวลผลข้อมูล
  - การแจ้งต่อบริษัทฯ เมื่อเกิดเหตุการละเมิดข้อมูลส่วนบุคคล

4.6 เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer : DPO)

- บริษัทฯ จะต้องมีการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลอย่างเป็นทางการ โดยเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลมีหน้าที่
  - ให้คำแนะนำแก่ผู้ที่เกี่ยวข้องทั้งภายในบริษัทฯ และภายนอกบริษัทฯ ในการประมวลผลข้อมูลส่วนบุคคล
  - ตรวจสอบการประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวข้องทั้งภายในบริษัทฯ และภายนอกบริษัทฯ
  - ประสานงานและให้ความร่วมมือกับสำนักงานคุ้มครองข้อมูลส่วนบุคคล
  - ให้คำแนะนำในการวิเคราะห์ผลกระทบการคุ้มครองข้อมูลส่วนบุคคล
  - รายงานผลการปฏิบัติงานเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลให้กับผู้บริหารสูงสุดของบริษัทฯ

- แจ้งรายชื่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลให้กับสำนักงานคุ้มครองข้อมูลส่วนบุคคลทราบ หรือเมื่อมีการเปลี่ยนแปลง

4.7 การออกแบบโดยคำนึงถึงการคุ้มครองข้อมูลส่วนบุคคล (Privacy by Design)

- บริษัทฯ จะต้องคำนึงถึงการคุ้มครองข้อมูลส่วนบุคคลตั้งแต่ขั้นตอนของการออกแบบผลิตภัณฑ์หรือบริการ โดยคำนึงถึงหลักการดังต่อไปนี้
  - การจัดเก็บข้อมูลอย่างจำกัด
  - การประมวลผลข้อมูลอย่างจำกัด
  - ความถูกต้อง และคุณภาพของข้อมูลส่วนบุคคล
  - การระบุวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลขั้นต่ำ
  - การลบ ทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้
  - การจัดการป้องกันข้อมูลที่ถูกจัดเก็บไว้ชั่วคราวในระหว่างการประมวลผล
  - ระยะเวลาการจัดเก็บข้อมูล
  - มาตรการในการแลกเปลี่ยนข้อมูล

4.8 การวิเคราะห์ผลกระทบการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment)

- บริษัทฯ ดำเนินการจัดทำขั้นตอนปฏิบัติในการวิเคราะห์ผลกระทบการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment Procedure) และมีการทบทวนขั้นตอนปฏิบัติอย่างสม่ำเสมอ
- สายงานที่เกี่ยวข้องจะต้องเป็นผู้จัดทำและทบทวนการประเมินผลกระทบของข้อมูลส่วนบุคคล (Data Protection Impact Assessment) ร่วมกับ DPO ก่อนริเริ่มดำเนินกิจกรรมทางธุรกิจ โครงการ หรือการกระทำอื่น ๆ ที่อาจก่อให้เกิดผลกระทบต่อการคุ้มครองข้อมูลส่วนบุคคลของบริษัทฯ

4.9 ความปลอดภัยของข้อมูล (Data Security)

- ควรเก็บข้อมูลเป็นความลับและเปิดเผยต่อบุคลากรที่ได้รับอนุญาตตามข้อกำหนดทางกฎหมายและกฎเกณฑ์ที่บังคับใช้เท่านั้น
- มีการจัดการดูแลและเก็บรักษาข้อมูล ทั้งที่อยู่ในรูปแบบเอกสารกระดาษ ข้อมูลในรูปแบบอิเล็กทรอนิกส์ และสื่อบันทึกข้อมูลไว้อย่างปลอดภัย ป้องกันการสูญหาย และพร้อมใช้งาน
- มีการจัดชั้นความลับของข้อมูล เก็บรักษาและทำลายข้อมูลให้เหมาะสมกับชั้นความลับ และมีการบริหารจัดการการเข้ารหัสข้อมูลที่เหมาะสม เพียงพอ
- มีการกำหนดหลักเกณฑ์เพื่อควบคุมการเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข และเปิดเผยข้อมูล โดยผู้ที่มีอำนาจและได้รับมอบหมาย รวมทั้งสายงานที่เกี่ยวข้องต้องร่วมดำเนินการให้มีการควบคุมการเข้าถึงข้อมูลอย่างเหมาะสม เพื่อให้มั่นใจว่าบุคคลที่เกี่ยวข้องมีสิทธิในการเข้าถึงข้อมูลส่วนบุคคลเท่าที่จำเป็น
- การขอสิทธิเพื่อเข้าถึงข้อมูลนอกเหนือจากที่กำหนดไว้จะต้องผ่านการพิจารณาจากเจ้าของข้อมูล
- การดำเนินการทางเทคนิคในการให้สิทธิเข้าถึงข้อมูลต้องเป็นไปตามนโยบายที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศและกระบวนการความมั่นคงปลอดภัยด้านสารสนเทศ
- มีการทบทวนสิทธิของพนักงานที่มีหน้าที่เกี่ยวข้องเข้าถึงข้อมูลเท่าที่จำเป็นและควบคุมการเข้าถึงระบบงาน และบริหารจัดการสิทธิของพนักงานให้เป็นปัจจุบัน โดยเฉพาะเมื่อมีการเปลี่ยนแปลงตำแหน่งหรือการจ้างงาน

- หากมีการจ้างผู้ให้บริการภายนอกหรือพันธมิตรทางธุรกิจซึ่งต้องมีการจัดเก็บและรวบรวมข้อมูลส่วนบุคคล จะต้องมีการควบคุมและบริหารจัดการ การเข้าถึง การใช้ และการดูแลรักษาข้อมูล รวมถึงกระบวนการทำลาย หรือลบข้อมูล ตามมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศ
- มีการออกแบบ พัฒนา และทดสอบระบบงานให้มีความมั่นคงปลอดภัย ที่เหมาะสม และมีการบำรุงรักษาอย่างสม่ำเสมอ

4.10 การละเมิดข้อมูลส่วนบุคคล (Personal Data Breaches)

- บริษัทฯ จะดำเนินการจัดการกับเหตุการณ์ละเมิดข้อมูลส่วนบุคคล เพื่อทำการแยกประเภทเหตุการณ์ระดับความเสี่ยงและผลกระทบ ตลอดจนการดำเนินการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลให้เป็นไปตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล
- หากบุคคลใดทราบถึงการละเมิดข้อมูลส่วนบุคคลของบริษัทฯ บุคคลนั้นจะต้องรายงานเหตุการณ์ที่เกิดขึ้นแก่ DPOโดยทันที ทั้งนี้ การรายงานดังกล่าวจะถูกเก็บเป็นความลับ เมื่อมีการแจ้งการละเมิดความปลอดภัย ทีมตอบสนองต่อเหตุการณ์และสายงานที่เกี่ยวข้องจะดำเนินการตรวจสอบข้อเท็จจริงที่เกี่ยวข้องกับเหตุการณ์ร่วมกับ DPO พร้อมเสนอแนวทางแก้ไขที่เหมาะสมแก่คณะผู้บริหารของบริษัทฯ

4.11 วันที่มีผลบังคับใช้ (Effective Date)

แนวปฏิบัติฉบับนี้มีผลบังคับใช้ในวันที่ 15 กุมภาพันธ์ 2565 เป็นต้นไป

ประกาศ ณ วันที่ 9 กุมภาพันธ์ 2565

(นายธานินทร์ พานิชชีวะ)
กรรมการผู้จัดการ