นโยบายการคุ้มครองข้อมูลส่วนบุคคล

(Data Protection Policy)

1. คำนิยาม

เจ้าของข้อมูลส่วนบุคคล (Data Subject)	หมายถึง บุคคลซึ่งสามารถถูกระบุตัวตนได้โดยข้อมูลส่วนบุคคลนั้นๆ ไม่ว่าโดยทางตรงหรือทางอ้อม
ข้อมูลส่วนบุคคล (Personal Data)	หมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรง หรือทางอ้อม 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 การดำเนินการใดๆ ซึ่งกระทำต่อข้อมูลส่วนบุคคลหรือชุดข้อมูลส่วนบุคคล ไม่ว่าจะโดยวิธีการอัตโนมัติหรือไม่ เช่น การเก็บ บันทึก จัดระบบ จัดโครงสร้างเก็บรักษา เปลี่ยนแปลง หรือปรับเปลี่ยน การรับ พิจารณา ใช้ เปิดเผยด้วยการส่งต่อ เผยแพร่ หรือการกระทำอื่นใดซึ่งทำให้เกิดความพร้อม ใช้งาน การจัดวาง หรือผสมเข้าด้วยกัน การจำกัด การลบ หรือการทำลาย
ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)	หมายถึง ผู้ที่มีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)	หมายถึง ผู้ซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่ง หรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล
ข้อมูลบริษัทฯ	หมายถึง ข้อมูลในรูปแบบใดก็ตามทั้งในแบบอิเล็กทรอนิกส์ และไม่ใช่อิเล็กทรอนิกส์ เช่น ข้อมูลในสิ่งพิมพ์ซึ่งอยู่ในระบบภายใน หรือระบบภายนอกที่นอกเหนือการควบคุมของบริษัทฯ และปรากฏเงื่อนไขดังต่อไปนี้ - ข้อมูลที่พนักงานของบริษัทฯ หรือบุคคลที่ได้รับมอบหมายได้มา ประมวลผล จัดการ และ/หรือดูแล (เช่น ผู้รับเหมา หน่วยงานภายนอก ที่ปรึกษา) เพื่อปฏิบัติหน้าที่ - ข้อมูลที่เกี่ยวเนื่องกับการจัดการ การปฏิบัติงาน วางแผน รายงาน หรือการตรวจสอบการดำเนินงานของบริษัทฯ - ข้อมูลที่ใช้อ้างอิง หรือจำเป็นต่อการทำงานของหน่วยงานอย่างน้อยหนึ่งหน่วย
การเข้าถึงข้อมูล (Access)	หมายถึง สิทธิในการอ่าน/ดู บันทึก คัดลอก เก็บสำรอง จัดเก็บ สืบค้น ดาวน์โหลด หรือแก้ไข (อัพเดท แทรก/เพิ่ม ลบ) ข้อมูล รวมถึงการจัดการสิทธิการเข้าถึงนั้นๆ
ผู้ใช้ หรือ ผู้ใช้ข้อมูล (Data Users)	หมายถึง บุคคลดังต่อไปนี้ - พนักงานบริษัท มิวซิกมูฟ จำกัด และบริษัทในเครือ - บุคลากรที่บริษัทฯ กำหนดให้เข้าถึงข้อมูล เพื่อปฏิบัติงานตามที่ได้รับมอบหมาย เช่น ผู้รับเหมา หน่วยงานภายนอก ที่ปรึกษา - บุคลากรของพันธมิตรของบริษัทฯ ซึ่งได้รับความยินยอม/อนุญาตจากบริษัทฯ ให้เข้าถึงข้อมูลอย่างเฉพาะเจาะจง และจำกัด เพื่อปฏิบัติงานตามที่ได้รับมอบหมายซึ่งเป็นไปเพื่อสนับสนุนการดำเนินงานของบริษัทฯ

หน่วยธุรกิจ	หมายถึง สายงาน ฝ่ายงาน หรือหน่วยปฏิบัติงานภายใต้ความรับผิดชอบของบริษัทฯ เพื่อกิจกรรมเฉพาะขององค์กร
การบันทึก (Record)	หมายถึง ข้อมูล หรือสารสนเทศในรูปแบบเฉพาะ ซึ่งถูกสร้างขึ้น หรือได้มาจากกิจกรรมบุคคล หรือกิจกรรมองค์กร และได้สำรอง (เก็บรักษา) ไว้เป็นหลักฐานของกิจกรรมนั้นๆ เพื่อใช้อ้างอิงในอนาคต
บริษัทฯ	หมายถึง บริษัท มิวซิกมูฟ จำกัด
กฎหมายคุ้มครองข้อมูลส่วนบุคคล	หมายถึง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 และที่จะมีการแก้ไขเพิ่มเติม รวมถึงกฎ ระเบียบ และคำสั่งที่เกี่ยวข้อง

2. วัตถุประสงค์

บริษัท มิวซิกมูฟ จำกัด (“บริษัทฯ”) ตระหนักถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคล เนื่องจากการคุ้มครองข้อมูลส่วนบุคคลเป็นส่วนหนึ่งของการรับผิดชอบต่อสังคม และเป็นรากฐานในการสร้างความสัมพันธ์ทางธุรกิจที่น่าเชื่อถือระหว่างบริษัทฯ กับบุคคลภายนอก บริษัทฯ จึงยึดมั่นในการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล และกฎเกณฑ์ทางการอื่นๆ ที่เกี่ยวข้อง

เอกสารฉบับนี้ได้รับการจัดทำขึ้นโดยมีวัตถุประสงค์ ดังต่อไปนี้

2.1 เพื่อชี้แจงความรับผิดชอบเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

2.2 เพื่อกำหนดมาตรฐาน และแนวทางบริหารข้อมูลส่วนบุคคล โดยครอบคลุมถึงการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล

3. ขอบเขต

นโยบายฉบับนี้ใช้บังคับกับการจัดเก็บข้อมูลส่วนบุคคลซึ่งมีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล โดยครอบคลุมถึงบุคลากรทั้งหมด ได้แก่ พนักงานประจำ พนักงานชั่วคราว พนักงานสัญญาจ้าง รวมถึงสายงาน หน่วยธุรกิจ และบริษัทภายใต้การควบคุมของบริษัทฯ รวมถึงพันธมิตรของบริษัทฯ ซึ่งมีส่วนร่วมในการเข้าถึง หรือประมวลผลข้อมูลของบริษัทฯ นอกจากนี้ยังครอบคลุมถึงการส่งต่อข้อมูลสู่องค์กรภายนอก หน่วยงานราชการ หรือบุคคลที่ได้รับอนุญาตตามกฎหมาย ข้อบังคับ หรือข้อบังคับกฎหมายอื่นๆ และใช้บังคับกับข้อมูลทุกรูปแบบทั้งข้อมูลอิเล็กทรอนิกส์ และไม่ใช่อิเล็กทรอนิกส์

4. คำแถลงนโยบาย

4.1 นโยบายการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Policy)

4.1.1 นโยบายการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Policy) ดูแลโดยเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล และหน่วยงานที่เกี่ยวข้อง และต้องจัดให้มีการประกาศ และสื่อสารไปยังพนักงาน และหน่วยงานที่เกี่ยวข้อง และกำหนดให้มีการทบทวน และปรับปรุงนโยบายฉบับนี้ให้เป็นปัจจุบันอย่างสม่ำเสมอ

4.1.2 การประมวลผลข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลจะต้องเป็นไปตามกฎหมาย มีความเป็นธรรม และมีความโปร่งใส

4.1.3 การเก็บรวบรวมข้อมูลส่วนบุคคลจะต้องพอเหมาะเป็นไปตามวัตถุประสงค์ที่กำหนด และเป็นไปตามฐานในการประมวลผลข้อมูลส่วนบุคคล

4.1.4 การประมวลผลข้อมูลส่วนบุคคลจะต้องมีการประมวลผลข้อมูลส่วนบุคคลอย่างจำกัด และสอดคล้องตามวัตถุประสงค์ที่กำหนด

4.1.5 การประมวลผลข้อมูลส่วนบุคคลจะต้องมีการปรับปรุงอยู่เสมอ รวมทั้งจะต้องมีการกำหนดขั้นตอนในการตรวจสอบ เพื่อให้ข้อมูลส่วนบุคคลมีความถูกต้องเป็นไปตามกฎหมาย หรือหน่วยงานกำกับดูแลที่เกี่ยวข้องกำหนด

4.1.6 บริษัทฯ อนุญาตให้จัดเก็บข้อมูลส่วนบุคคลภายในระยะเวลาที่บริษัทฯ กำหนดเท่านั้น ข้อมูลส่วนบุคคลที่มีการจัดเก็บเกินระยะเวลาที่กำหนด ผู้รับผิดชอบจะต้องมีการลบ ทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้

4.1.7 การประมวลผลข้อมูลส่วนบุคคลจะต้องคำนึงถึงความมั่นคงปลอดภัยสารสนเทศ ซึ่งรวมถึงการป้องกันการประมวลผลข้อมูลส่วนบุคคลโดยผู้ที่ไม่มีสิทธิ การลบ หรือทำลายข้อมูลทั้งโดยความตั้งใจ และไม่ตั้งใจ และรวมถึงการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศให้อยู่ในระดับที่องค์กรยอมรับได้

4.2 **การปฏิบัติตามสิทธิของเจ้าของข้อมูลส่วนบุคคล** (Rights of Data Subject)

4.2.1 สายงานที่เกี่ยวข้องจะต้องพิจารณาถึงสิทธิของเจ้าของข้อมูลส่วนบุคคลดังต่อไปนี้

4.2.1.1 สิทธิในการเพิกถอนความยินยอม

4.2.1.2 สิทธิในการขอเข้าถึง และขอรับสำเนาข้อมูลส่วนบุคคล

4.2.1.3 สิทธิในการขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลที่เจ้าของข้อมูลส่วนบุคคลไม่ได้ให้ความยินยอม

4.2.1.4 สิทธิในการขอให้โอนย้ายข้อมูลส่วนบุคคลไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่น

4.2.1.5 สิทธิในการคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

4.2.1.6 สิทธิในการขอให้ลบ ทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้

4.2.1.7 สิทธิในการขอให้ระงับการใช้ข้อมูลส่วนบุคคล

4.2.1.8 สิทธิในการขอให้แก้ไขข้อมูลให้ถูกต้อง เป็นปัจจุบัน และสมบูรณ์

4.2.2 สายงานที่เกี่ยวข้อง และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะต้องร่วมจัดทำบันทึกรายการการประมวลผลข้อมูลส่วนบุคคล โดยรายละเอียดของบันทึกรายการการประมวลผลข้อมูลส่วนบุคคลจะต้องมีความสอดคล้องกับ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 และหลักเกณฑ์ที่เกี่ยวข้อง

4.2.3 จัดให้มีการระบุช่องทางในการใช้สิทธิให้กับเจ้าของข้อมูลส่วนบุคคลทราบ

4.2.4 สายงานที่เกี่ยวข้อง และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะต้องบันทึกรายละเอียดเกี่ยวกับการขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล โดยต้องประกอบด้วยข้อมูลดังต่อไปนี้

4.2.4.1 รายละเอียดของเจ้าของข้อมูลส่วนบุคคล

4.2.4.2 รายละเอียดการขอใช้สิทธิตามสิทธิของเจ้าของข้อมูลส่วนบุคคล

4.2.4.3 รายละเอียดของการดำเนินการ ซึ่งรวมถึงเหตุผลในกรณีที่มีการปฏิเสธการขอใช้สิทธิตามสิทธิของเจ้าของข้อมูลส่วนบุคคล

4.2.5 เมื่อมีการขอใช้สิทธิจากเจ้าของข้อมูลส่วนบุคคล หน่วยธุรกิจ และสายงานที่เกี่ยวข้องจะต้องปฏิบัติตามกระบวนการการขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลของบริษัทฯ โดยเคร่งครัด

4.3 การประมวลผลข้อมูลส่วนบุคคลให้สอดคล้องตามกฎหมาย (Lawfulness of Processing)

4.3.1 สายงานที่เกี่ยวข้อง และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะต้องร่วมกันทบทวนให้การประมวลผลข้อมูลส่วนบุคคลมีความสอดคล้องกับกฎหมาย โดยจะต้องระบุฐานในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล โดยการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลจะต้องเป็นไปตามวัตถุประสงค์อันชอบด้วยกฎหมาย และมีความสอดคล้องกับ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 โดยการระบุฐานในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล สามารถพิจารณาได้ดังนี้

4.3.1.1 ข้อมูลส่วนบุคคล

ก) การขอความยินยอม

ข) ความจำเป็นเพื่อการปฏิบัติตามสัญญา

ค) ความจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล

ง) ความจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมาย

จ) ความจำเป็นเพื่อปฏิบัติตามกฎหมาย

ฉ) เพื่อการวิจัย และสถิติ

ช) เพื่อป้องกัน หรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล

4.3.1.2 ข้อมูลส่วนบุคคลที่มีลักษณะอ่อนไหว

ก) การขอความยินยอมโดยชัดแจ้ง

ข) เพื่อป้องกัน หรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล

ค) เป็นการดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมของมูลนิธิ สมาคม หรือองค์กรไม่แสวงหากำไรที่มีวัตถุประสงค์เกี่ยวกับการเมือง ศาสนา ปรัชญา หรือสหภาพแรงงานให้แก่สมาชิก ผู้ซึ่งเคยเป็นสมาชิก หรือผู้ซึ่งมีการติดต่ออย่างสม่ำเสมอกับมูลนิธิ สมาคม หรือองค์กรไม่แสวงหากำไรตามวัตถุประสงค์ดังกล่าวโดยไม่ได้เปิดเผยข้อมูลส่วนบุคคลนั้นออกไปภายนอกมูลนิธิ สมาคม หรือองค์กรไม่แสวงหากำไรนั้น

ง) เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคล

จ) ความจำเป็นเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตาม หรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย

ฉ) ความจำเป็นเพื่อปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์ตามที่ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ระบุไว้

4.3.2 หากหน่วยธุรกิจเลือกใช้วิธีการขอความยินยอม จะต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลเท่านั้น และจะต้องขอความยินยอมก่อนที่จะมีการประมวลผลเกิดขึ้น

4.3.3 หากมีการเปลี่ยนแปลงวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไปจากเดิม จะต้องขอความยินยอมใหม่ทุกครั้ง

4.3.4 หน่วยธุรกิจจะต้องมีการคำนึงถึงการเก็บหลักฐานของการขอความยินยอมไว้อย่างเหมาะสม

4.3.5 การเปิดเผยข้อมูลจะต้องเป็นไปตามแนวทาง และกระบวนการเปิดเผยข้อมูลที่บริษัทฯ กำหนดไว้

4.4 **การโอนข้อมูลส่วนบุคคล** (Personal Data Transfer)

4.4.1 การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศจะต้องคำนึงถึงมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ และเป็นไปตามหลักเกณฑ์ของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

4.4.2 ห้ามโอนข้อมูลส่วนบุคคลให้กับผู้นำเข้าข้อมูลที่อยู่นอกประเทศ เว้นแต่

4.4.2.1 บริษัทฯ และผู้นำเข้าข้อมูลได้ตกลงกันเป็นลายลักษณ์อักษรเพื่อให้สัญญาเกี่ยวกับเจ้าของข้อมูลส่วนบุคคลมีความสมบูรณ์

4.4.2.2 เป็นการกระทำตามสัญญาเพื่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

4.4.2.3 เพื่อป้องกัน หรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของเจ้าของข้อมูลส่วนบุคคล

4.4.2.4 บริษัทฯ ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล โดยได้แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพอของประเทศปลายทางแล้ว

4.4.3 การโอน และการประมวลผลข้อมูลต้องดำเนินการด้วยวิธีที่ปลอดภัย และเป็นไปตามมาตรฐานความปลอดภัยขั้นต่ำของบริษัทฯ พร้อมทั้งสอดคล้องกับนโยบาย และกระบวนการความมั่นคงปลอดภัยด้านสารสนเทศ

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

4.5.1 สายงานที่เกี่ยวข้องจะต้องมีการระบุรายละเอียดเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในสัญญาระหว่างบริษัทฯ และหน่วยงานภายนอก โดยจะต้องครอบคลุมเนื้อหาดังต่อไปนี้

4.5.1.1 ข้อตกลงการไม่เปิดเผยความลับของข้อมูล

4.5.1.2 รายละเอียดเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล

4.5.1.3 สิทธิของบริษัทฯ ในการตรวจสอบการประมวลผลข้อมูลส่วนบุคคลของหน่วยงานภายนอก

4.5.1.4 มาตรการการลบ ทำลาย หรือส่งคืนข้อมูลเมื่อสิ้นสุดระยะเวลาการประมวลผลข้อมูล

4.5.1.5 การแจ้งต่อบริษัทฯ เมื่อเกิดเหตุการละเมิดข้อมูลส่วนบุคคล

4.6 **เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล** (Data Protection Officer : DPO)

4.6.1 บริษัทฯ จะต้องมีการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลอย่างเป็นทางการ โดยเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลมีหน้าที่ดังต่อไปนี้

4.6.1.1 ให้คำแนะนำแก่ผู้ที่เกี่ยวข้องทั้งภายในบริษัทฯ และภายนอกบริษัทฯ ในการประมวลผลข้อมูลส่วนบุคคล

4.6.1.2 ตรวจสอบการประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวข้องทั้งภายในบริษัทฯ และภายนอกบริษัทฯ

4.6.1.3 ประสานงาน และให้ความร่วมมือกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

4.6.1.4 ให้คำแนะนำในการวิเคราะห์ผลกระทบของข้อมูลส่วนบุคคล

4.6.1.5 รายงานผลการปฏิบัติงานเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลให้กับผู้บริหารสูงสุดของบริษัทฯ

4.6.2 แจ้งรายชื่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลให้กับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบ หรือเมื่อมีการเปลี่ยนแปลง

4.7 **การออกแบบโดยคำนึงถึงการคุ้มครองข้อมูลส่วนบุคคล** (Privacy by Design)

4.7.1 บริษัทฯ จะต้องคำนึงถึงการคุ้มครองข้อมูลส่วนบุคคลตั้งแต่ขั้นตอนของการออกแบบผลิตภัณฑ์ หรือบริการ โดยคำนึงถึงหลักการดังต่อไปนี้

4.7.1.1 การจัดเก็บข้อมูลอย่างจำกัด

4.7.1.2 การประมวลผลข้อมูลอย่างจำกัด

4.7.1.3 ความถูกต้อง และคุณภาพของข้อมูลส่วนบุคคล

4.7.1.4 การระบุวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลขั้นต่ำ

4.7.1.5 การลบ ทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้

4.7.1.6 การจัดการทำข้อมูลที่ถูกจัดเก็บไว้ชั่วคราวในระหว่างการประมวลผล

4.7.1.7 ระยะเวลาการจัดเก็บข้อมูล

4.7.1.8 มาตรการในการแลกเปลี่ยนข้อมูล

4.8 **การวิเคราะห์ผลกระทบของข้อมูลส่วนบุคคล** (Data Protection Impact Assessment)

4.8.1 สายงานที่เกี่ยวข้องจะต้องเป็นผู้จัดทำขั้นตอนปฏิบัติในการวิเคราะห์ผลกระทบของข้อมูลส่วนบุคคล (Data Protection Impact Assessment Procedure) และมีการทบทวนขั้นตอนปฏิบัติอย่างสม่ำเสมอ

4.8.2 สายงานที่เกี่ยวข้องจะต้องเป็นผู้จัดทำ และทบทวนการประเมินผลกระทบของข้อมูลส่วนบุคคล (Data Protection Impact Assessment) ร่วมกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ก่อนริเริ่มดำเนินกิจกรรมทางธุรกิจ โครงการ หรือการกระทำอื่นๆ ที่อาจก่อให้เกิดผลกระทบต่อการคุ้มครองข้อมูลส่วนบุคคลของบริษัทฯ

4.9 **ความปลอดภัยของข้อมูล** (Data Security)

4.9.1 ควรเก็บข้อมูลเป็นความลับ และเปิดเผยต่อบุคลากรที่ได้รับอนุญาตตามข้อกำหนดทางกฎหมาย และกฎเกณฑ์ที่บังคับใช้เท่านั้น

4.9.2 มีการกำหนดหลักเกณฑ์ดูแล และเก็บรักษาข้อมูล ทั้งที่อยู่ในรูปแบบเอกสารกระดาษ ข้อมูลในรูปแบบอิเล็กทรอนิกส์ และสื่อบันทึกข้อมูลไว้อย่างปลอดภัย ป้องกันการสูญหาย และพร้อมใช้งาน

4.9.3 มีการจัดชั้นความลับของข้อมูล เก็บรักษา และทำลายข้อมูลให้เหมาะสมกับชั้นความลับ และมีการบริหารจัดการการเข้ารหัสข้อมูลที่เชื่อถือได้ และเป็นมาตรฐานสากล

4.9.4 มีการกำหนดหลักเกณฑ์เพื่อควบคุมการเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข และเปิดเผยข้อมูล โดยผู้ที่มีอำนาจ และได้รับมอบหมาย รวมทั้งสายงานที่เกี่ยวข้องต้องร่วมดำเนินการให้มีการควบคุมการเข้าถึงข้อมูลอย่างเหมาะสม เพื่อให้มั่นใจว่าบุคคลที่เกี่ยวข้องมีสิทธิในการเข้าถึงข้อมูลส่วนบุคคลเท่าที่จำเป็น

4.9.5 การขอสิทธิเพื่อเข้าถึงข้อมูลนอกเหนือจากที่กำหนดไว้ จะต้องผ่านการพิจารณาจากผู้มีอำนาจของบริษัทฯ

4.9.6 การดำเนินการทางเทคนิคในการให้สิทธิเข้าถึงข้อมูลต้องเป็นไปตามนโยบายด้านความมั่นคงปลอดภัยสารสนเทศ และกระบวนการความมั่นคงปลอดภัยด้านสารสนเทศ

4.9.7 กำหนดหลักเกณฑ์ให้มีการทบทวนสิทธิแก่พนักงานที่มีหน้าที่เกี่ยวข้องเพื่อเข้าถึงข้อมูลเท่าที่จำเป็น และควบคุมการเข้าถึงระบบงาน และบริหารจัดการสิทธิของพนักงานให้เป็นปัจจุบัน โดยเฉพาะเมื่อมีการเปลี่ยนแปลงตำแหน่ง หรือการจ้างงาน

4.9.8 หากมีการจ้างผู้ให้บริการภายนอก หรือพันธมิตรทางธุรกิจซึ่งต้องมีการจัดเก็บ และรวบรวมข้อมูลส่วนบุคคล จะต้องมีการกำหนดหลักเกณฑ์เพื่อควบคุม และบริหารจัดการ การเข้าถึง การใช้ และการดูแลรักษาข้อมูล รวมถึงกระบวนการทำลาย หรือลบข้อมูลตามมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศ

4.9.9 มีการออกแบบ พัฒนา และทดสอบระบบงานให้มีความมั่นคงปลอดภัย มีความยืดหยุ่น และมีการบำรุงรักษาสม่ำเสมอ

4.10 **การละเมิดข้อมูลส่วนบุคคล** (Personal Data Breaches)

4.10.1 บริษัทฯ จะต้องกำหนดแนวทางปฏิบัติเกี่ยวกับการจัดการกับเหตุการละเมิดข้อมูลส่วนบุคคล หลักเกณฑ์ในการแยกประเภทเหตุการณ์ ระดับความเสี่ยงและผลกระทบ ตลอดจนการดำเนินการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลให้เป็นไปตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

4.10.2 หากบุคคลใดทราบถึงการละเมิดข้อมูลส่วนบุคคลของบริษัทฯ บุคคลนั้นจะต้องรายงานเหตุการณ์ที่เกิดขึ้นแก่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของบริษัทฯ โดยทันที ทั้งนี้ การรายงานดังกล่าวจะถูกเก็บเป็นความลับ เมื่อมีการแจ้งการละเมิดความปลอดภัยแล้ว ทีมตอบสนองต่อเหตุการณ์ และสายงานที่เกี่ยวข้องจะดำเนินการตรวจสอบข้อเท็จจริงที่เกี่ยวข้องกับเหตุการณ์ร่วมกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล พร้อมเสนอแนวทางแก้ไขที่เหมาะสมแก่คณะบริหารของบริษัทฯ

4.11 บทลงโทษ

ผู้ฝ่าฝืนนโยบายฉบับนี้อาจมีความผิด และถูกลงโทษทางวินัยตามข้อบังคับการทำงานของบริษัทฯ รวมทั้งอาจได้รับโทษตามที่กฎหมายกำหนด

นโยบายการคุ้มครองข้อมูลส่วนบุคคลฉบับนี้ มีผลบังคับใช้ตั้งแต่วันประกาศเป็นต้นไป

ประกาศ ณ วันที่ 19 เดือน พฤษภาคม พ.ศ. 2565