



# นโยบายการคุ้มครองข้อมูล

GENERAL DATA PROTECTION POLICY

ฉบับวันที่ 11 พฤศจิกายน 2565

## นโยบายการคุ้มครองข้อมูล (General Data Protection Policy)

เพื่อเป็นการกำหนดทิศทางและสนับสนุนการดำเนินการด้านการคุ้มครองข้อมูลของบริษัทฯ ต่อลูกค้า ผู้ถือหุ้น พนักงาน และผู้เกี่ยวข้อง และเพื่อให้เป็นไปตามหรือสอดคล้องกับข้อกำหนดทางธุรกิจ กฎหมาย และระเบียบปฏิบัติที่เกี่ยวข้อง บริษัทฯ ไซติวิวัฒน์อุตสาหกรรมการผลิต จำกัด (มหาชน) ซึ่งต่อไปนี้จะเรียกว่า (“บริษัทฯ”) จึงได้อนุมัติให้ใช้นโยบายคุ้มครองข้อมูล เพื่อให้บริษัทฯ มีหลักเกณฑ์ มาตรการกำกับดูแล และการบริหารจัดการข้อมูลอย่างถูกต้อง ชัดเจน และเหมาะสม

ทางบริษัทฯ จึงกำหนดนโยบายการคุ้มครองข้อมูล เพื่อนำไปปฏิบัติ ดังนี้

### 1. ขอบเขตการบังคับใช้

นโยบายการคุ้มครองข้อมูลนี้ ใช้บังคับกับ บริษัทฯ ไซติวิวัฒน์อุตสาหกรรมการผลิต จำกัด (มหาชน) ลูกจ้าง พนักงาน ลูกค้า คู่ค้า และหน่วยงานหรือบุคคลอื่นๆ ที่เกี่ยวข้องกับการเก็บ รวบรวม ใช้ และประมวลผลข้อมูลตามคำสั่ง หรือในนามของ บริษัทฯ

### 2. คำนิยาม

คำศัพท์	ความหมาย
บริษัท	บริษัท ไซติวิวัฒน์อุตสาหกรรมการผลิต จำกัด (มหาชน) และบริษัทย่อย
ผู้บริหาร	ผู้บริหารของ บริษัทฯ ไซติวิวัฒน์อุตสาหกรรมการผลิต จำกัด (มหาชน)
คณะกรรมการบริหาร	คณะกรรมการบริหารของ บริษัทฯ ไซติวิวัฒน์อุตสาหกรรมการผลิต จำกัด (มหาชน)
ผู้ถือหุ้น	ผู้ถือหุ้นของ บริษัทฯ ไซติวิวัฒน์อุตสาหกรรมการผลิต จำกัด (มหาชน)
คณะกรรมการควบคุมข้อมูล	คณะกรรมการควบคุมข้อมูลของ บริษัทฯ ไซติวิวัฒน์อุตสาหกรรมการผลิต จำกัด (มหาชน) (CMC) (Data Controller Committee, DCC) (CMC DCC)
ข้อมูล	ข้อมูลใด ๆ ที่เกี่ยวข้องหรืออาจเกี่ยวข้องอันได้แก่ข้อมูลทั่วไปที่มีข้อมูลส่วนบุคคล ทั้งทางตรง และทางอ้อม เช่น ข้อมูลจดทะเบียนบริษัทฯ ข้อมูลการรับรองการตรวจสุขภาพ ข้อมูลของบุคคลธรรมดา ที่อาจจะระบุตัวตนได้ ซึ่งสามารถระบุได้ทั้งทางตรง หรือทางอ้อมโดยเฉพาะอย่างยิ่งโดยการอ้างอิงถึงตัวตน เช่น ชื่อ หมายเลขประจำตัว ข้อมูลตำแหน่งออนไลน์ (GEOLOCATION) หรือปัจจัยหนึ่งหรือหลายปัจจัยที่เฉพาะเจาะจงเกี่ยวกับร่างกายสรีรวิทยา ลักษณะทางพันธุกรรม จิตใจ เศรษฐกิจ วัฒนธรรม หรือสังคมของบุคคลธรรมดานั้น รวมถึงข้อมูลสารสนเทศใด ๆ

คำศัพท์	ความหมาย
	ก็ตามที่สัมพันธ์กับบุคคลธรรมดาที่สามารถระบุตัวลักษณะได้ (ข้อมูลส่วนบุคคล และข้อมูลทั่วไป) ข้อมูลที่ไม่นับรวม ได้แก่ ข้อมูลที่ไม่มีข้อมูลส่วนบุคคลแฝง ยกตัวอย่างเช่น อุณหภูมิตู้แช่แข็ง จำนวนเข็มฉีดยาในห้องพยาบาล เป็นต้น ซึ่งไม่เกี่ยวข้องกับข้อมูลส่วนบุคคลใดๆ เลย
เจ้าของข้อมูล	บุคคลที่สามารถระบุตัวลักษณะได้ คือบุคคลที่สามารถระบุตัวลักษณะได้ไม่ว่าจะโดยตรงหรือโดยอ้อมโดยเฉพาะอย่างยิ่งด้วยการอ้างอิงจากสิ่งระบุตัวลักษณะเป็นการเฉพาะ เช่น ชื่อ หมายเลขประจำตัว ข้อมูลสถานที่ สิ่งระบุตัวลักษณะออนไลน์ หรือปัจจัยอย่างหนึ่งหรือมากกว่าที่เจาะจงไปยังตัวลักษณะทางกายภาพ กายวิถยา พันธุกรรม จิตใจ เศรษฐกิจ วัฒนธรรม หรือสังคมของบุคคล
ผู้ควบคุมข้อมูล	บริษัท โซติวิวัฒน์อุตสาหกรรมการผลิต จำกัด (มหาชน) มีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บ รวบรวม ใช้ และประมวลผลข้อมูล
ผู้ประมวลผลข้อมูล	บุคคลธรรมดาหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บ รวบรวม ใช้ และประมวลผลข้อมูลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูล
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO)	เจ้าหน้าที่คุ้มครองข้อมูลของบริษัท โซติวิวัฒน์อุตสาหกรรมการผลิต จำกัด (มหาชน) (CMC DPO) เป็นผู้ทำหน้าที่ปกป้องข้อมูลของบริษัทฯ ให้ไม่ถูกมีการใช้หรือละเมิดตามกฎหมาย พรบ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
การประมวลผล	ปฏิบัติการใด ๆ หรือชุดของปฏิบัติการใด ๆ ที่ดำเนินการกับข้อมูลส่วนบุคคลหรือชุดของข้อมูลส่วนบุคคล ไม่ว่าจะด้วยวิธีการอัตโนมัติหรือไม่ก็ตาม เช่น การเก็บ รวบรวม การบันทึก การจัดระบบ การวางโครงสร้าง การเก็บรักษา การปรับใช้หรือการแปรสภาพ การค้นคืน การสืบค้นข้อมูลเพิ่มเติม การใช้ประโยชน์ การเปิดเผย โดยการส่งต่อ เผยแพร่ หรือวิธีอื่นใดอันทำให้เข้าถึงได้ การจัดเรียงหรือรวมเข้าด้วยกัน การจำกัดการเข้าถึง การลบหรือทำลาย
การจำกัดการประมวลผล	การทำเครื่องหมายระบุข้อมูลส่วนบุคคลด้วยเป้าหมายในการจำกัดขอบเขตของการประมวลผลข้อมูลเหล่านั้นในอนาคต
การทำโพรไฟล์	รูปแบบใด ๆ ก็ตามของการประมวลผลข้อมูลส่วนบุคคลที่ประกอบด้วยการใช้ประโยชน์จากข้อมูลส่วนบุคคลในการประเมินบางแง่มุมส่วนบุคคลที่สัมพันธ์กับ

คำศัพท์	ความหมาย
	บุคคลธรรมดาหนึ่ง ๆ โดยเฉพาะอย่างยิ่งเพื่อวิเคราะห์หรือคาดการณ์ในแง่ที่เกี่ยวข้องกับประสิทธิภาพในการทำงาน สถานภาพทางเศรษฐกิจ สุขภาพ ความชอบส่วนบุคคล ความสนใจ ความเชื่อถือได้ อุปนิสัย สถานที่หรือการเคลื่อนไหวของบุคคลธรรมดานั้น ๆ
การปกปิดอัตลักษณ์ (pseudonymization)	การประมวลผลข้อมูลส่วนบุคคลในลักษณะที่ข้อมูลส่วนบุคคลไม่สามารถระบุเจาะจงไปยังผู้ถูกประมวลผลคนใดคนหนึ่งหากไม่มีการใช้ข้อมูลเพิ่มเติม ด้วยเงื่อนไขว่าข้อมูลเพิ่มเติมดังกล่าวจะถูกเก็บแยกจากกันและอยู่ภายใต้การควบคุมโดยมาตรการทางเทคนิคและการจัดการองค์กรที่จะรับประกันว่าข้อมูลเพิ่มเติมดังกล่าวจะไม่ถูกใช้บ่งชี้ไปถึงบุคคลธรรมดาที่ถูกระบุอัตลักษณ์หรือสามารถถูกระบุอัตลักษณ์ได้
ความยินยอมของผู้ถูกประมวลผลข้อมูล	การชี้ชัดถึงความต้องการของผู้ถูกประมวลผลข้อมูลที่ได้มาโดยอิสระ เฉพาะเจาะจง มีการแจ้งข้อมูล และไม่กำกวม โดยการประกาศหรือการแสดงอย่างชัดเจนว่ายินยอมการตกลงถึงการประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวข้องกับตน
ข้อมูลเกี่ยวข้องกับสุขภาพ	ข้อมูลส่วนบุคคลที่สัมพันธ์กับสุขภาพกายหรือสุขภาพจิตของบุคคลธรรมดา รวมถึงการจัดหาบริการสาธารณสุขที่เปิดเผยข้อมูลเกี่ยวกับสถานะทางสุขภาพของบุคคลนั้น
ข้อมูลพันธุกรรม	ข้อมูลส่วนบุคคลที่สัมพันธ์กับคุณลักษณะทางพันธุกรรมที่สืบทอดกันมาหรือเกิดขึ้นภายหลัง ซึ่งให้ข้อมูลลักษณะพิเศษเฉพาะเกี่ยวกับกายวิทยาหรือสุขภาพของบุคคลธรรมดานั้น และโดยเฉพาะอย่างยิ่งเป็นผลจากการวิเคราะห์ตัวอย่างทางชีววิทยาของบุคคลธรรมดาที่ถูกกล่าวถึง
ข้อมูลชีวมาตร	ข้อมูลส่วนบุคคลอันเป็นผลจากกระบวนการประมวลผลทางเทคนิคเฉพาะที่สัมพันธ์กับคุณลักษณะทางกายภาพ กายวิทยาหรืออุปนิสัยของบุคคลธรรมดาที่ทำให้สามารถระบุหรือยืนยันอัตลักษณ์ของบุคคลธรรมดาโดยเฉพาะได้เช่น ข้อมูลภาพ

### 3. ด้านการกำกับดูแล (Personal and General Data Protection Governance)

3.1 บริษัทฯ จัดให้มีโครงสร้างและกลไกที่เหมาะสมในการกำกับดูแลการคุ้มครองข้อมูลส่วนบุคคล และข้อมูลทั่วไปตามกฎหมาย ดังนี้

3.1.1 กำหนดให้มีโครงสร้างองค์กร รวมทั้งกำหนดบทบาท ภารกิจ ความรับผิดชอบของหน่วยงาน และผู้ปฏิบัติงานที่เกี่ยวข้องให้ชัดเจน เพื่อสร้างมาตรการการกำกับดูแล การควบคุม ความรับผิดชอบ การปฏิบัติงาน การบังคับใช้ และการติดตามมาตรการคุ้มครองข้อมูลให้สอดคล้องกับกฎหมาย และนโยบายการคุ้มครองข้อมูลของบริษัทฯ

3.1.2 แต่งตั้งคณะทำงานควบคุมข้อมูลของบริษัทฯ (Data Controller committee: DCC) และเจ้าหน้าที่คุ้มครองข้อมูลของบริษัทฯ (Data Protection Officer : DPO) โดยมีบทบาท และหน้าที่ตามที่กำหนดในนโยบายการคุ้มครองข้อมูลของบริษัทฯ

3.2 บริษัทฯ จัดทำนโยบาย (Policy) มาตรฐานการปฏิบัติงาน (Standards) แนวปฏิบัติ (Guidelines) ขั้นตอนปฏิบัติ (Procedures) และเอกสารอื่นที่เกี่ยวข้องกับการคุ้มครองข้อมูลให้สอดคล้องกับกฎหมาย และนโยบายคุ้มครองข้อมูล

3.3 บริษัทฯ จัดให้มีกระบวนการบริหารการปฏิบัติตามนโยบาย เพื่อควบคุมดูแลให้มีการปฏิบัติตามนโยบายการคุ้มครองข้อมูลของบริษัทฯ อย่างต่อเนื่อง

3.4 บริษัทฯ จัดให้มีการฝึกอบรมลูกจ้าง/พนักงานของบริษัทฯ อย่างสม่ำเสมอ เพื่อให้ลูกจ้าง/พนักงานของบริษัทฯ ตระหนักถึงความสำคัญของการคุ้มครองข้อมูล และทำให้มั่นใจได้ว่าลูกจ้าง/พนักงานของบริษัทฯ มีความรู้ความเข้าใจในการคุ้มครองข้อมูล และสามารถปฏิบัติตามนโยบายการคุ้มครองข้อมูลของบริษัทฯ

### 4. ด้านการเก็บ รวบรวม ใช้ ประมวลผลข้อมูล (Personal and General Data Keeping, Collecting, Using and Processing)

4.1 บริษัทฯ จะเก็บ รวบรวม ใช้ ประมวลผลข้อมูลทั้งในฐานะผู้ควบคุม และผู้ประมวลผลให้ถูกต้องตามกฎหมาย อย่างเป็นธรรม โปร่งใส คำนึงถึงความถูกต้อง และสิทธิของเจ้าของข้อมูล ทั้งนี้ บริษัทฯ จะกำหนดขอบเขต วัตถุประสงค์ ของการเก็บ รวบรวม ใช้ ประมวลผลข้อมูล และระยะเวลาในการดำเนินการกับข้อมูล ให้ทำได้เท่าที่จำเป็น หรือตามที่บริษัทฯ กำหนด หรือตามที่มาตรฐาน หรือกฎหมายอื่นกำหนด และภายใต้วัตถุประสงค์อันชอบด้วยกฎหมาย และแนวทางในการดำเนินกิจการของบริษัทฯ สำหรับข้อมูลที่บริษัทฯ เก็บ รวบรวม ใช้ ประมวลผล ด้วยการรักษาความลับ ความถูกต้องสมบูรณ์ และความปลอดภัยของข้อมูลอย่างเพียงพอ และเหมาะสม

4.2 บริษัทฯ จัดให้มีกระบวนการ การควบคุม รวมถึงการบริหารจัดการกับข้อมูลในทุกกระบวนการให้มีความสอดคล้องกับกฎหมาย และนโยบายการคุ้มครองข้อมูลของบริษัทฯ

4.3 บริษัทฯ รักษา และบันทึกการเก็บ รวบรวม ใช้ ประมวลผลข้อมูล ที่เกี่ยวข้องให้มีความสอดคล้องกับกฎหมาย รวมทั้งจะปรับปรุงบันทึกการเก็บ รวบรวม ใช้ ประมวลผลข้อมูลเมื่อมีการเปลี่ยนแปลงรายการหรือกิจกรรมที่เกี่ยวข้อง

4.4 บริษัทฯ จัดให้มีกระบวนการที่ชัดเจนเพื่อให้มั่นใจได้ว่าการแจ้งวัตถุประสงค์ของการเก็บ รวบรวม ใช้ ประมวลผลข้อมูล และการขอความยินยอมจากเจ้าของข้อมูล ให้มีความสอดคล้องกับกฎหมาย รวมทั้งจัดให้มีมาตรการดูแล เก็บรักษา และตรวจสอบ ขั้นตอนการดำเนินการดังกล่าว

4.5 บริษัทฯ จัดให้มีกลไกการตรวจสอบความถูกต้องของข้อมูล รวมทั้งจัดให้มีกลไกการแก้ไขข้อมูลให้มีความถูกต้องอย่างสม่ำเสมอ

4.6 บริษัทฯ จะจัดทำข้อตกลง/สัญญากับผู้รับโอนในการเก็บ รวบรวม ใช้ ประมวลผลข้อมูล เพื่อกำหนดสิทธิหน้าที่ และความรับผิดชอบในกรณีที่จะต้องมีการส่ง หรือโอนข้อมูล ให้มีความสอดคล้องกับกฎหมาย และนโยบายการคุ้มครองข้อมูลของบริษัทฯ

4.7 หากมีความจำเป็นในการส่ง โอนข้อมูลไปยังบุคคลอื่นที่อยู่ต่างประเทศ บริษัทฯ จะดำเนินการให้สอดคล้องกับกฎหมาย และมาตรการที่เกี่ยวข้องกับข้อมูลของประเทศนั้น ๆ บริษัทฯ จะทำลายข้อมูล หรือจัดทำกระบวนการปกปิดอัตลักษณ์ (pseudonymization) เมื่อครบกำหนดระยะเวลาในการจัดเก็บข้อมูล โดยปฏิบัติให้มีความสอดคล้องกับกฎหมาย และแนวทางการดำเนินกิจการของบริษัทฯ

## 5. ด้านการรับรองการใช้สิทธิของเจ้าของข้อมูล (Data Subject Right)

### 5.1 สิทธิได้รับการแจ้งให้ทราบ (Right to be informed)

เจ้าของข้อมูลต้องได้รับการแจ้งให้ทราบ ก่อน หรือขณะเก็บรวบรวมข้อมูล ในเรื่องของวัตถุประสงค์ และฐานทางกฎหมาย, เงื่อนไขในการใช้บริการ, ประเภทของข้อมูลและระยะเวลาการเก็บ, การโอนข้อมูลส่วนบุคคล, ข้อมูลการติดต่อผู้ควบคุมข้อมูล, สิทธิของเจ้าของข้อมูลส่วนบุคคล

### 5.2 สิทธิในการเข้าถึงข้อมูลส่วนบุคคล (right to access)

โดยเจ้าของข้อมูลมีสิทธิร้องขอในการเข้าถึงข้อมูล การรับสำเนาข้อมูล การขอแก้ไขหรือปรับปรุงข้อมูลส่วนบุคคลที่เกี่ยวข้องกับตนเอง

### 5.3 ขอเปิดเผยถึงการได้มาข้อมูลซึ่งเจ้าของข้อมูลไม่ได้ให้ความยินยอม

โดยเจ้าของข้อมูลมีสิทธิรับทราบถึงแหล่งที่มาของข้อมูลเมื่อเกิดความสงสัยถึงข้อมูลที่ได้รับการติดต่อ

### 5.4 สิทธิในการเพิกถอนความยินยอม (right to withdraw consent)

เจ้าของข้อมูลมีสิทธิถอนความยินยอมผ่านทางผู้ควบคุมข้อมูลเมื่อใดก็ได้ แต่จะไม่มีผลกระทบต่อกรที่ให้ความยินยอมไปแล้ว และผู้ควบคุมข้อมูลมีหน้าที่แจ้งให้เจ้าของข้อมูลทราบถึงผลกระทบของการถอนความยินยอมดังกล่าว

การเพิกถอนความยินยอมในบางกรณีอาจกระทำมิได้หากเป็นกรณีการดำเนินการประมวลผลที่ไม่จำเป็นต้องขอความยินยอมจากเจ้าของข้อมูล เช่นการประมวลผลอันเนื่องมาจากการปฏิบัติตามสัญญา หรือเพื่อการปฏิบัติหน้าที่ตามกฎหมาย เป็นต้น

### 5.5 สิทธิในการให้โอนย้ายข้อมูลส่วนบุคคล (right to data portability)

สิทธิขอรับข้อมูลส่วนบุคคลที่เกี่ยวข้องกับตน ในกรณีที่ได้ทำอยู่ในรูปแบบที่สามารถอ่านหรือใช้งานโดยทั่วไปได้ด้วยเครื่องมือหรืออุปกรณ์ที่ทำงานได้โดยอัตโนมัติและสามารถใช้หรือเปิดเผยข้อมูลส่วนบุคคลได้ด้วยวิธีการอัตโนมัติ รวมทั้งมีสิทธิ ดังต่อไปนี้

5.5.1 ส่งหรือโอนข้อมูลส่วนบุคคลในรูปแบบดังกล่าวไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่นเมื่อสามารถทำได้ด้วยวิธีการอัตโนมัติ

5.5.2 ขอรับข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลส่งหรือโอนข้อมูลส่วนบุคคลในรูปแบบดังกล่าวไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่นโดยตรง เว้นแต่โดยสภาพทางเทคนิคไม่สามารถทำได้

5.5.3 การส่งหรือโอนข้อมูลไปยังต่างประเทศ ต้องมีมาตรฐานการคุ้มครองข้อมูลที่เหมาะสมและเพียงพอ

### 5.6 สิทธิในการลบ ทำลายหรือลบข้อมูลส่วนบุคคล (right to erasure)

เจ้าของข้อมูลมีสิทธิที่จะร้องขอผู้ควบคุมข้อมูลเพื่อลบข้อมูลส่วนบุคคลของตนออกจากฐานข้อมูลของผู้ควบคุมข้อมูลส่วนบุคคล หรือทำให้ข้อมูลส่วนบุคคลไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ (เป็นข้อมูลนิรนาม)

### 5.7 สิทธิในการคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

เจ้าของข้อมูลมีสิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวข้องกับตนเมื่อใดก็ได้

### 5.8 สิทธิในการห้ามมิให้ประมวลผลข้อมูลส่วนบุคคล (right to restriction of processing)

เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลระงับการใช้ข้อมูลส่วนบุคคลได้ ภายใต้หลักเกณฑ์ที่กำหนดไว้ในกฎหมาย

ในกรณีที่เจ้าของข้อมูลส่วนบุคคลร้องขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการตามสิทธิของเจ้าของข้อมูล หากผู้ควบคุมข้อมูลส่วนบุคคลไม่ดำเนินการตามคำร้องขอ ผู้ควบคุมข้อมูลส่วนบุคคลต้องบันทึกคำร้องขอของเจ้าของข้อมูลส่วนบุคคลพร้อมด้วยเหตุผลไว้ในรายการประมวลผลข้อมูลส่วนบุคคล (RoPA) นอกจากนี้ เจ้าของข้อมูลมีสิทธิในการร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญเพื่อสั่งให้ดำเนินการตามสิทธิได้

## 5.9 สิทธิในการร้องเรียน

เจ้าของข้อมูลส่วนบุคคล มีสิทธิร้องเรียนในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ผิดเพี้ยนหรือไม่ปฏิบัติตามบทบัญญัติของกฎหมาย

6. เจ้าของข้อมูลส่วนบุคคลสามารถแจ้งความประสงค์ เพื่อการใช้สิทธิต่างๆ ตามที่บัญญัติไว้ในกฎหมายได้ โดยแจ้งผ่านทางอีเมลส่งมาที่ [dpo@chotiwat.com](mailto:dpo@chotiwat.com) จากนั้น DPO จะทำการแจ้งต่อไปยังผู้ควบคุมข้อมูลเพื่อขอคำอนุมัติ หรือปฏิเสธการร้องขอต่อไป

## 7. ด้านการรักษาความปลอดภัยของข้อมูลส่วนบุคคล (Personal Data Security)

7.1 บริษัทฯ จัดให้มีมาตรการในการรักษาความปลอดภัยของข้อมูลอย่างเหมาะสม และเพียงพอ รวมถึงจัดให้มีการป้องกันไม่ให้เกิดการรั่วไหลของข้อมูล และการละเมิดที่เกิดจากการนำข้อมูลไปใช้โดยไม่ได้รับอนุญาต

7.2 บริษัทฯ จัดให้มีการบริหารจัดการเหตุการณ์ผิดปกติต่าง ๆ ที่เกี่ยวข้องกับข้อมูล (Personal Data Incident Management) และแนวทางการตอบสนองต่อเหตุการณ์ผิดปกติ เพื่อให้สามารถระบุและจัดการกับเหตุการณ์ผิดปกติที่เกี่ยวข้องตามที่กฎหมายกำหนด

7.3 บริษัทฯ จัดให้มีกระบวนการแจ้งเจ้าของข้อมูล รวมถึงพนักงานของรัฐ ผู้ควบคุมข้อมูล (กรณีของบริษัทฯ ทำหน้าที่เป็นผู้ประมวลผล) และบุคคลอื่นที่เกี่ยวข้อง เพื่อให้สอดคล้องตามที่กฎหมายกำหนด

## 8. ด้านการกำกับให้มีการปฏิบัติตามมาตรการคุ้มครองข้อมูล (General Data Protection Compliance)

8.1 บริษัทฯ จัดให้มีกระบวนการกำกับดูแลในกรณีที่กฎหมายมีการเปลี่ยนแปลง หรือมีการประกาศใช้กฎหมายอื่นที่เกี่ยวข้อง และปรับปรุงมาตรการการคุ้มครองข้อมูลให้มีความเป็นปัจจุบันและสอดคล้องกับกฎหมายอย่างสม่ำเสมอ



8.2 บริษัทฯ จัดให้มีการทบทวนและปรับปรุงนโยบาย มาตรฐานการปฏิบัติงาน แนวทางในการปฏิบัติ ขั้นตอน การปฏิบัติ และเอกสารอื่นที่เกี่ยวข้องกับการคุ้มครองข้อมูลเป็นประจำ เพื่อให้มีความทันสมัย สอดคล้องกับกฎหมาย และสถานการณ์ต่าง ๆ ที่เปลี่ยนแปลงไป

## 9. บทบาท หน้าที่ และความรับผิดชอบ

### 9.1 ผู้บริหาร มีบทบาท หน้าที่ และความรับผิดชอบดังต่อไปนี้

9.1.1 กำกับให้มีโครงสร้างการกำกับดูแลข้อมูล และกำหนดมาตรการควบคุมภายในบริษัทฯ เพื่อปฏิบัติตามกฎหมาย และนโยบายการคุ้มครองข้อมูลของบริษัทฯ

9.1.2 กำกับดูแล และสนับสนุนให้หน่วยงานตามนโยบายคุ้มครองข้อมูลของบริษัทฯ ดำเนินการคุ้มครองข้อมูลให้มีประสิทธิภาพและให้มีความสอดคล้องตามกฎหมายและส่งเสริมการสร้างวัฒนธรรมที่เกื้อหนุนกับลูกจ้าง/พนักงานของบริษัทฯ

### 9.2 คณะทำงานควบคุมข้อมูลของบริษัทฯ (CMC DCC)

คณะทำงานควบคุมข้อมูลของบริษัทฯ ให้มีหน้าที่จัดการบริหารความเสี่ยงด้านข้อมูล (Data Risk Management) โดยมีบทบาท หน้าที่ และความรับผิดชอบ ดังต่อไปนี้

9.2.1 จัดให้มีโครงสร้างการกำกับดูแลข้อมูล และการควบคุมภายในที่เกี่ยวข้อง รวมถึง การบริหารจัดการเหตุการณ์ผิดปกติที่เกี่ยวข้องกับข้อมูล และแนวทางการตอบสนองต่อเหตุการณ์ผิดปกติ เพื่อให้สามารถระบุ ประเมิน และจัดการกับเหตุการณ์ผิดปกติที่เกี่ยวข้องกับข้อมูลได้ตามระยะเวลาที่กฎหมายกำหนด

9.2.2 ประเมินประสิทธิภาพการปฏิบัติตามนโยบายการคุ้มครองข้อมูลของบริษัทฯ และรายงานผลการดำเนินการดังกล่าวให้ผู้บริหารทราบอย่างสม่ำเสมอรวมถึงควบคุมดูแลว่าความเสี่ยงต่าง ๆ ที่เกี่ยวข้องกับข้อมูลจะได้รับการจัดการและมีแนวทางการบริหารความเสี่ยงที่เหมาะสม

9.2.3 กำหนดและทบทวนมาตรฐานการปฏิบัติงาน และแนวทางปฏิบัติ เพื่อให้การดำเนินงานของบริษัทฯ มีความสอดคล้องกับกฎหมาย และนโยบายการคุ้มครองข้อมูลของบริษัทฯ

### 9.2.4 แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลของบริษัทฯ (CMC DPO)

9.3 เจ้าหน้าที่คุ้มครองข้อมูลของบริษัทฯ (CMC DPO) มีบทบาท หน้าที่ และความรับผิดชอบตามที่กฎหมายกำหนด ซึ่งรวมถึงหน้าที่ดังต่อไปนี้

9.3.1 รายงานสถานการณ์คุ้มครองข้อมูลให้คณะทำงานควบคุมข้อมูลทราบอย่างสม่ำเสมอ และจัดทำข้อเสนอแนะเพื่อปรับปรุงการคุ้มครองข้อมูลของบริษัทฯ ให้ทันสมัย และสอดคล้องกับกฎหมาย

9.3.2 ให้คำแนะนำต่อลูกจ้าง/พนักงานของบริษัทฯ เกี่ยวกับการปฏิบัติตามกฎหมาย และนโยบายการคุ้มครองข้อมูลของบริษัทฯ

9.3.3 ตรวจสอบการดำเนินงานของหน่วยงานในบริษัทฯ ให้เป็นไปตามกฎหมาย และนโยบายการคุ้มครองข้อมูลของบริษัทฯ

9.3.4 ร่วมพิจารณาประเมินความเสี่ยงด้านข้อมูลกับคณะกรรมการคุ้มครองข้อมูลของบริษัทฯ

9.3.5 เป็นศูนย์กลางในการติดต่อประสานงานกับหน่วยงานภาครัฐ ตัวอย่างเช่น สำนักงานคณะกรรมการคุ้มครองข้อมูล สำนักงานคณะกรรมการตรวจสอบข้อมูล สำนักงานคณะกรรมการคุ้มครองส่วนบุคคลภาครัฐ เป็นต้น ในส่วนที่เกี่ยวข้องกับข้อมูล

9.3.6 ติดต่อประสานงานกับหน่วยงาน องค์กร สถาบันภายนอกในส่วนที่เกี่ยวข้องกับการคุ้มครองข้อมูล

9.4 ลูกจ้าง/พนักงานของบริษัทฯ มีบทบาท หน้าที่ และความรับผิดชอบดังต่อไปนี้

9.4.1 ปฏิบัติตนเองให้สอดคล้องกับนโยบายการคุ้มครองข้อมูลของบริษัทฯ มาตรฐานการปฏิบัติงาน แนวทางปฏิบัติ ขั้นตอนปฏิบัติ และเอกสารอื่นที่เกี่ยวข้องกับการคุ้มครองข้อมูล

9.4.2 รายงานเหตุการณ์ผิดปกติที่เกี่ยวข้องกับการคุ้มครองข้อมูล และการไม่ปฏิบัติตามกฎหมาย และนโยบายการคุ้มครองข้อมูลของบริษัทฯ ให้ผู้บังคับบัญชาทราบ

10. โทษของการไม่ปฏิบัติตามนโยบายการคุ้มครองข้อมูลของบริษัทฯ

การไม่ปฏิบัติตามนโยบายการคุ้มครองข้อมูลของบริษัทฯ อาจมีความผิด และถูกลงโทษทางวินัยของบริษัทฯ รวมทั้งอาจได้รับโทษตามที่กฎหมายกำหนด

จึงประกาศมาให้ทราบ และถือปฏิบัติโดยทั่วกัน

ประกาศ ณ วันที่ 11 พฤศจิกายน 2565