



A S T R A

---

# นโยบายคุ้มครองข้อมูลส่วนบุคคล

## นโยบายคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Policy)

### นิยาม

| คำศัพท์                            | ความหมาย                                                                                                                                                                                                           |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| คณะกรรมการ                         | คณะกรรมการบริษัท หรือคณะกรรมการที่ได้รับมอบหมายเพื่อกำกับดูแลการคุ้มครองข้อมูลส่วนบุคคล                                                                                                                            |
| เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล | บุคคลหรือกลุ่มบุคคลที่ได้รับการแต่งตั้งเป็นเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือได้รับมอบหมายให้รับผิดชอบในการคุ้มครองข้อมูลส่วนบุคคล หรือหน่วยงานกำกับดูแลเพื่อให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล |
| ผู้ควบคุมข้อมูลส่วนบุคคล           | บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล                                                                                                                  |
| ผู้ประมวลผลข้อมูลส่วนบุคคล         | บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับ การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล  |
| เจ้าของข้อมูล                      | บุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลซึ่งข้อมูลดังกล่าวสามารถเชื่อมโยงกับบุคคลและระบุตัวตนไปยังบุคคลดังกล่าวได้                                                                                                       |
| บุคคล                              | บุคคลธรรมดา                                                                                                                                                                                                        |
| ข้อมูลส่วนบุคคล                    | ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ                                                                                          |
| ประมวลผล                           | การจัดเก็บใช้หรือเปิดเผยข้อมูล                                                                                                                                                                                     |

| คำศัพท์              | ความหมาย                                                                                                                                                                                                                                                                                                 |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ข้อมูลอ่อนไหว        | ข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใด ซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด |
| การลบ/ทำลาย          | รวมไปถึงการทำให้เป็นข้อมูลนิรนาม                                                                                                                                                                                                                                                                         |
| การทำให้ข้อมูลนิรนาม | การทำให้ข้อมูลนิรนามกล่าวอีกนัยหนึ่งคือการทำให้ชุดข้อมูลที่เคยสามารถเชื่อมโยงกับบุคคลและระบุตัวตนได้ ไม่สามารถเชื่อมโยงข้อมูลและทำให้ไม่สามารถระบุตัวตนได้อีกต่อไป                                                                                                                                       |

## ภาพรวมของนโยบาย

### บทนำ

บริษัทมุ่งมั่นที่จะปกป้องข้อมูลส่วนบุคคลที่ได้รับจากลูกค้าหรือบุคคลที่สาม โดยเฉพาะข้อมูลที่มีความละเอียดอ่อน และเพื่อรักษาสิทธิความเป็นส่วนตัวเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคลและเพื่อเป็นการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล

โดยที่นโยบายฉบับนี้จะอธิบายถึง หน้าที่ ภาระผูกพัน และขั้นตอนในการรวบรวม ใช้ และจัดเก็บข้อมูลส่วนบุคคลเพื่อให้เป็นไปตามมาตรฐานการคุ้มครองข้อมูลของบริษัท กฎหมายไทย และมาตรฐานสากล

โดยแนวทางปฏิบัติของบริษัทจะยึดถือหลักการดังต่อไปนี้:

- การเก็บรวบรวม การใช้ และการเปิดเผยข้อมูลจะต้องเป็นไปตามวัตถุประสงค์ที่ประกาศ หรือที่ได้รับไว้และถูกต้องตามกฎหมายภายในขอบเขตที่กฎหมายกำหนดไว้
- ข้อมูลส่วนบุคคลจะได้รับการประมวลผลอย่างเป็นธรรมและชอบด้วยกฎหมาย
- วัตถุประสงค์ของการประมวลผลจะต้องถูกกำหนดและประกาศไว้อย่างชัดเจน

- เฉพาะข้อมูลส่วนบุคคลที่จำเป็นและสอดคล้องกับวัตถุประสงค์ที่ประกาศหรือระบุไว้และถูกต้องตามกฎหมายเท่านั้นที่จะถูกเก็บรวบรวม
- ข้อมูลส่วนบุคคลที่รวบรวมจะต้องมีความถูกต้องและเป็นปัจจุบัน
- ข้อมูลส่วนบุคคลจะต้องไม่ถูกเก็บไว้นานเกินความจำเป็น
- การจัดเก็บข้อมูลจะต้องได้รับการปกป้องด้วยวิธีที่เหมาะสม

อีกทั้งบริษัทยังมีความรับผิดชอบที่จะต้องตรวจสอบให้แน่ใจว่าข้อมูลส่วนบุคคลจะได้รับการเก็บรวบรวมและใช้อย่างเป็นธรรม จัดเก็บอย่างปลอดภัยและไม่ถูกเปิดเผยด้วยวิธีการที่ไม่ชอบกฎหมาย

### กฎระเบียบที่เกี่ยวข้อง

บริษัทจะคำนึงถึงภาระผูกพันของตนภายใต้กฎหมายป้องกันการฟอกเงินที่เกี่ยวข้อง กฎหมายว่าด้วยหลักทรัพย์และตลาดหลักทรัพย์ และกฎระเบียบที่บังคับใช้ที่เกี่ยวข้องกับการรวบรวม การใช้ การเปิดเผย และการจัดเก็บข้อมูลส่วนบุคคล ตามความเหมาะสม

### วัตถุประสงค์

วัตถุประสงค์ของนโยบายนี้กำหนดขึ้นเพื่อเป็นแนวทางให้กับบุคลากรทุกคนของบริษัทในการประมวลผลข้อมูลส่วนบุคคลอย่างเหมาะสม เพื่อให้มั่นใจว่าข้อมูลทั้งหมดที่ได้รับจากลูกค้าและบุคคลที่สามได้รับการคุ้มครองและมีมาตรการรักษาความปลอดภัยที่จำเป็นในการรักษาความปลอดภัย นโยบายนี้ถูกนำมาใช้เพื่อให้สอดคล้องกับกฎหมายที่กล่าวมาข้างต้น และพยายามที่จะปลูกฝังให้องค์กรเคารพและปกป้องสิทธิความเป็นส่วนตัวของข้อมูลลูกค้าของบริษัท และตรวจสอบให้แน่ใจว่าข้อมูลส่วนบุคคลทั้งหมดที่รวบรวมได้รับการประมวลผลตามหลักการทั่วไปของความโปร่งใส ถูกต้องตามกฎหมาย มีวัตถุประสงค์ที่ชอบด้วยกฎหมายและได้สัดส่วน

### นโยบายความเป็นส่วนตัวของข้อมูลนี้ทำให้บริษัทมั่นใจว่า:

1. มีการปฏิบัติงานที่เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และแนวทางปฏิบัติที่ดีที่สุด
2. คุ้มครองสิทธิของกรรมการ ผู้บริหาร พนักงาน ลูกค้า และคู่ค้า (ถ้ามี)

3. กำกับวิธีการจัดเก็บและประมวลผลข้อมูลของแต่ละบุคคล
4. ปกป้องตัวเองจากความเสี่ยงของการละเมิดข้อมูลส่วนบุคคล

### ขอบเขตนโยบาย

ความรับผิดชอบในการปฏิบัติตามนโยบายและขั้นตอนการปฏิบัติงานนี้ เป็นของเจ้าหน้าที่ส่วนงาน ทั้งนี้ บริษัทควรพิจารณาแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลขึ้นเพื่อทำหน้าที่ตรวจสอบการปฏิบัติงานตามนโยบายฉบับนี้

โดยที่นโยบายนี้ต้องได้รับการตรวจสอบและอนุมัติโดยคณะกรรมการบริษัทก่อนมีผลบังคับใช้ ซึ่งหมายถึง การเปลี่ยนแปลงที่สำคัญใด ๆ ในเนื้อหาของนโยบายฉบับนี้

นอกจากนั้นนโยบายฉบับนี้ควรมีการทบทวนเนื้อหาอย่างสม่ำเสมอเพื่อให้มั่นใจว่านโยบายของบริษัทนั้นเป็นไปตามกฎหมายและเป็นการลดความเสี่ยงของการไม่ปฏิบัติตามกฎหมาย

### การละเว้นไม่ปฏิบัติตามนโยบาย

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลมีหน้าที่กำกับดูแลติดตามให้มีการปฏิบัติงานเป็นไปตามนโยบายที่กำหนด และรายงานผลการปฏิบัติงานให้คณะกรรมการบริษัทตามรอบระยะเวลาการประชุมของคณะกรรมการบริษัท หรือรายงานทันทีโดยไม่ชักช้าต่อประธานเจ้าหน้าที่บริหารเพื่อประโยชน์ในการแก้ไขข้อบกพร่องและลดผลกระทบความเสียหายที่อาจเกิดขึ้น

บริษัทห้ามมิให้บุคลากรไม่ปฏิบัติ หรือละเว้นไม่ปฏิบัติตามนโยบายนี้ เว้นแต่มีเหตุจำเป็นที่ต้องละเว้นการปฏิบัติตามนโยบายนี้ ซึ่งจะต้องได้รับการอนุมัติจากคณะกรรมการบริษัทแล้วเท่านั้น

### การระบุข้อมูลส่วนบุคคล

“ข้อมูลส่วนบุคคล” (Personal Data) ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล หมายความว่า ข้อมูลเกี่ยวกับ บุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลผู้ถึงแก่กรรม

โดยเฉพาะ “เจ้าของข้อมูลส่วนบุคคล” (Data Subject) หมายความว่า บุคคลผู้ที่ข้อมูลส่วนบุคคลสามารถระบุไปถึง

ทั้งนี้ เพื่อเป็นการอธิบายคำว่าข้อมูลส่วนบุคคล ทางบริษัทฯ ได้อ้างอิงถึง National Institutional of Standard and Technology (“NIST”) ที่ได้ให้คำนิยามของ Personal Identifiable Information (PII) โดยหมายถึง ข้อมูลที่เกี่ยวกับตัวบุคคลทำให้สามารถระบุตัวบุคคลได้ ไม่ว่าทางตรงหรือทางอ้อม

โดยความสามารถในการระบุตัวบุคคลสามารถแบ่ง ได้เป็น 3 ลักษณะ อันได้แก่

1. **การแยกแยะ (Distinguishability)** คือการที่ข้อมูลมีความสามารถในการระบุแยกแยะตัวบุคคลออกจากกันได้ ตัวอย่างเช่น ในชุดข้อมูล มี ชื่อ หมายเลขหนังสือเดินทาง หมายเลขประกันสังคม หรือ ข้อมูล Biometric ซึ่งข้อมูลดังกล่าวสามารถระบุตัวของเจ้าของข้อมูลได้ ในทางตรงกันข้าม หากชุดข้อมูลระบุเพียงคะแนนเครดิต (Credit score) นั้น ไม่สามารถระบุไปยังตัวบุคคลได้ จำเป็นจะต้องมีข้อมูลเกี่ยวกับตัวบุคคลเพิ่มเติมจึงจะสามารถแยกแยะตัวบุคคลได้
2. **การติดตาม (Traceability)** คือการที่ข้อมูลสามารถถูกใช้ในการติดตาม เพื่อระบุลักษณะเฉพาะของบุคคลนั้นได้ ยกตัวอย่างเช่น พฤติกรรม กิจกรรมที่บุคคลนั้นกระทำ สถานะหรือการบันทึกการกระทำของผู้ใช้งานระบบที่ทำให้สามารถใช้ในการติดตามกิจกรรมของแต่ละบุคคลได้
3. **การเชื่อมโยง (Linkability)** คือการที่ข้อมูลมีคุณสมบัติในการเชื่อมโยงกันและระบุไปยังตัวบุคคลได้ ซึ่งแบ่งออกเป็น 2 ประเภท
  - **ข้อมูลที่ถูกเชื่อมโยงแล้ว (Linked Information)** คือกรณีที่ข้อมูลที่เกี่ยวข้องกับเจ้าของข้อมูลส่วนบุคคลคนละชุด เมื่อใช้ข้อมูลทั้งสองชุดประกอบกันแล้วจะมีความสามารถในการระบุตัวเจ้าของข้อมูลส่วนบุคคลได้ เช่น ข้อมูลสองชุดที่มีองค์ประกอบ PII ต่างกัน เมื่อมีบุคคลที่สามารถเข้าถึงชุดข้อมูลทั้งสองชุดได้ ก็จะสามารถเชื่อมโยงข้อมูลดังกล่าวในการระบุตัวเจ้าของข้อมูลส่วนบุคคลได้ รวมถึงกรณี que การเข้าถึงข้อมูลอื่นที่เกี่ยวข้องกับเจ้าของข้อมูลส่วนบุคคล หากฐานข้อมูลทั้งสองชุดอยู่ในระบบเดียวกันหรือระบบที่เกี่ยวข้องกันอย่างใกล้ชิด และ ไม่มีควบคุมการเข้าถึงอย่างมีประสิทธิภาพ กรณีนี้ถือเป็นข้อมูลที่ถูกเชื่อมโยงแล้วได้
  - **ข้อมูลที่สามารถเชื่อมโยงได้ (Linkable Information)** คือกรณีที่ หากมีชุดข้อมูลที่หากใช้ร่วมกันกับข้อมูลอื่นแล้วก็จะสามารถระบุตัวบุคคลได้ โดยที่ข้อมูลอื่นที่จะนำมาใช้ร่วมกันนั้นมาจากแหล่งข้อมูลอื่น โดยไม่อยู่ในระบบเดียวกันหรือระบบที่ไม่เกี่ยวข้องกัน มีอยู่ในอินเทอร์เน็ตหรือแหล่งอื่น ในกรณีนี้ถือเป็นข้อมูลที่สามารถเชื่อมโยงได้

ตัวอย่างของ PII (Personally Identifiable Information) เช่น ชื่อ ที่อยู่ อีเมล ข้อมูลทางการเงิน ข้อมูลสุขภาพ ประวัติอาชญากรรม เป็นต้น การเข้าถึง ใช้ หรือเปิดเผย PII โดยมิได้รับอนุญาตนั้นอาจก่อให้เกิดผลกระทบทางลบกับทั้งเจ้าของข้อมูลส่วนบุคคล เช่น อาจถูกสวมรอยโดยคนร้ายและเอาข้อมูลไปแอบอ้างเพื่อประโยชน์บางประการ อาจทำให้เกิดความอับอาย มีผลกระทบต่อความเป็นอยู่หรืออาจทำให้เกิดความเสียหายทางการเงิน เป็นต้น และเกิดผลในทางลบกับ ผู้ควบคุมข้อมูลส่วนบุคคลเอง เช่น มีผลกระทบต่อชื่อเสียงขององค์กร ทำให้ความน่าเชื่อถือลดลง หรือต้องรับผิดชอบตามกฎหมาย เป็นต้น

### ตัวอย่างของข้อมูลที่เป็นข้อมูลส่วนบุคคล

รายการต่อไปนี้คือตัวอย่างของข้อมูลที่สามารถถูกพิจารณาเป็นข้อมูลส่วนบุคคล

- ชื่อ นามสกุล ชื่อกลาง
- เลขประจำตัวประชาชน หมายเลขประกันสังคม หมายเลขหนังสือเดินทาง หมายเลขใบขับขี่ หมายเลขประจำตัวผู้เสียภาษีเลขบัญชีธนาคาร เลขบัตร เครดิต
- ข้อมูลที่อยู่อีเมล หมายเลขโทรศัพท์
- ข้อมูลอุปกรณ์ เช่น เลข IP address, MAC address, Cookie ID
- ข้อมูลที่เป็นลักษณะเฉพาะ เช่น รูปภาพใบหน้า
- ข้อมูลทางชีวมิติ (Biometric) ซึ่งเป็นข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหว (Sensitive Personal Data) เช่น ข้อมูลแบบจำลองใบหน้า ข้อมูลแบบจำลอง ลายนิ้วมือ फिल्मเอกซเรย์ข้อมูลสแกนม่านตา ข้อมูลอัตลักษณ์เสียง ข้อมูล พันธุกรรม เป็นต้น
- ข้อมูลระบุทรัพย์สินของบุคคล เช่น หมายเลขกระเป๋าเดินทาง ข้อมูลเกี่ยวกับบุคคลที่เชื่อมโยงหรือถูกเชื่อมโยงกับหนึ่งในข้างต้น เช่น วัน เกิด สถานที่เกิด น้ำหนัก ส่วนสูง ข้อมูลตำแหน่งทางภูมิศาสตร์ (Location)
- เชื้อชาติศาสนา ความเชื่อ ลัทธิ เผ่าพันธุ์ ปรัชญา พฤติกรรมทางเพศ ความเห็นทางการเมือง ประวัติอาชญากรรม

## ตัวอย่างของข้อมูลที่ไม่เป็นข้อมูลส่วนบุคคล

รายการต่อไปนี้เป็นตัวอย่างของข้อมูลที่ไม่ถูกพิจารณาเป็นข้อมูลส่วนบุคคล

- ข้อมูลจดทะเบียนบริษัท, ข้อมูลติดต่อทางธุรกิจ ที่ไม่ได้ระบุถึงตัวบุคคล เช่น ที่อยู่สำนักงาน, อีเมลบริษัท, หมายเลขโทรศัพท์สำนักงาน, หมายเลขแฟกซ์ สำนักงาน
- ข้อมูลที่ไม่สามารถระบุถึงตัวบุคคลได้ เช่น ข้อมูลนิรนาม (Anonymized Data)
- ข้อมูลผู้ถึงแก่กรรม

## ผลบังคับใช้ของนโยบายฉบับนี้

นโยบายความเป็นส่วนตัวนี้ใช้กับข้อมูลทั้งหมดรวมที่บริษัทจัดเก็บโดยเฉพาะอย่างยิ่งข้อมูลส่วนบุคคลที่สามารถระบุตัวตนได้ ซึ่งบริษัทมีอยู่และสามารถเชื่อมโยงไปยังเจ้าของข้อมูลได้ ซึ่งอาจรวมถึงแต่ไม่จำกัดเพียงข้อมูลดังต่อไปนี้:

1. ข้อมูล KYC รวมถึงชื่อ ที่อยู่ ข้อมูลธุรกรรม ฯลฯ
2. ข้อมูล EDD ได้แก่ ฐานะทางการเงิน เอกสารทางการเงิน ฯลฯ
3. ข้อมูลสัญญา จากข้อตกลงการบริการ ข้อตกลงการจ้างงาน ฯลฯ
4. ข้อมูลส่วนบุคคลที่ได้รับผ่านทางบริการลูกค้า
5. ข้อมูลอื่นใดที่เกี่ยวข้องกับบุคคล

พนักงานทุกคนของบริษัท โดยไม่คำนึงถึงประเภทของการจ้างงานไม่ว่าจะเป็นการจ้างแรงงานหรือการจ้างทำของตามสัญญา จะต้องปฏิบัติตามข้อกำหนดที่กำหนดไว้ในนโยบายฉบับนี้

## ความเสี่ยงที่อาจเกิดขึ้นต่อการไม่ปฏิบัติตาม

นโยบายนี้ช่วยปกป้องบริษัทจากความเสี่ยงด้านความปลอดภัยของข้อมูลที่สำคัญ ซึ่งรวมถึง:

1. การละเมิดการรักษาความลับ กรณีที่มีการให้ข้อมูลออกไปอย่างไม่เหมาะสมหรือฝ่าฝืนข้อตกลงการรักษาความลับ
2. ความเสียหายต่อชื่อเสียง ซึ่งรวมถึงความล้มเหลวในการป้องกันการเข้าถึงข้อมูลส่วนบุคคลและ/หรือข้อมูลที่ละเอียดอ่อนโดยบุคคลที่สามโดยไม่ได้รับอนุญาต

### 3. การละเมิดความปลอดภัย กรณีของการใช้งานโดยไม่ตั้งใจ ผิดกฎหมายหรือไม่ได้รับอนุญาต การแทรกแซงหรือขัดขวางการทำงานหรือความไม่พร้อมใช้ข้อมูลส่วนบุคคล

#### แนวปฏิบัติด้านบุคลากรทั่วไป

1. การเข้าถึงข้อมูลส่วนบุคคลนั้นต้องอยู่ภายใต้พื้นฐานหลักความจำเป็นที่ต้องทราบเพื่อปฏิบัติงานเท่านั้น
2. ไม่ควรเปิดเผยข้อมูลด้วยวิธีที่ไม่เป็นทางการ เช่น การส่งผ่านโซเชียลมีเดีย (รวมถึงแอปส่งข้อความ) หรือการส่งข้อมูลทางกายภาพยกเว้นในกรณีที่มีความจำเป็นและมีมาตรการเพียงพอในการรักษาซึ่งความลับ
3. บริษัทจะจัดให้มีการฝึกอบรมแก่บุคลากรทุกคนเพื่อให้เข้าใจความรับผิดชอบของตนในการจัดประมวลผลข้อมูลและสร้างความเข้าใจพื้นฐานต่อนโยบายฉบับนี้
4. พนักงานควรรักษาข้อมูลทั้งหมดให้ปลอดภัยโดยใช้มาตรการป้องกันที่สมเหตุสมผลและปฏิบัติตามแนวทางที่บริษัทได้กำหนดขึ้น
5. บุคลากรต้องใช้รหัสผ่านที่รัดกุมตามหลักปฏิบัติด้านความปลอดภัยของบริษัทและหลักปฏิบัติสากลที่ดีที่สุด และไม่ควรเปิดเผยรหัสผ่านดังกล่าว
6. ข้อมูลส่วนบุคคลไม่ควรเปิดเผยแก่บุคคลที่ไม่ได้รับอนุญาตทั้งภายในบริษัทหรือภายนอก
7. ข้อมูลควรได้รับการตรวจสอบและปรับปรุงเป็นประจำ หากไม่จำเป็นอีกต่อไป ควรลบและกำจัดทิ้งตามกรอบเวลาที่กฎหมายกำหนดไว้
8. บุคลากรจะต้องขอความช่วยเหลือจากหัวหน้าสายงานและ/หรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หากไม่แน่ใจเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลที่จะรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
9. บุคลากรทุกคนที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลจะต้องดำเนินการและรักษาข้อมูลส่วนบุคคลภายใต้มาตรการการรักษาความลับที่เข้มงวด ในกรณีที่ข้อมูลส่วนบุคคลนั้นไม่ได้มีไว้สำหรับการเปิดเผยต่อสาธารณะ หน้าที่เหล่านี้ยังคงผูกพันแม้บุคลากรดังกล่าวจะออกจากบริษัท โอนไปยังตำแหน่งอื่น หรือเมื่อเลิกจ้าง หรือความสัมพันธ์ตามสัญญาได้สิ้นสุดลง

## การประมวลผลข้อมูลส่วนบุคคล - การรวบรวมข้อมูล

บริษัทเก็บรวบรวมข้อมูลเพื่อให้สามารถดำเนินการตามภาระหน้าที่ที่มีต่อเจ้าของข้อมูลส่วนบุคคลได้ โดยบริษัทมุ่งเน้นให้การจัดเก็บข้อมูลนั้นมีความปลอดภัย มีประสิทธิภาพ และเพื่อให้สอดคล้องกับภาระผูกพันภายใต้กฎหมายและข้อบังคับที่บังคับใช้

บริษัทจะไม่เก็บรวบรวม ใช้ หรือ/และเปิดเผยข้อมูลส่วนบุคคลในทุกกรณี เว้นแต่ เป็นข้อยกเว้นทางกฎหมายที่กำหนดไว้ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ซึ่งประกอบด้วย:

1. **ฐานการวิจัย:** เพื่อวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารทางประวัติศาสตร์หรือเอกสารสำคัญเพื่อประโยชน์สาธารณะ หรือเพื่อวัตถุประสงค์ที่เกี่ยวกับการวิจัยหรือสถิติ โดยมีการกำหนดมาตรการที่เหมาะสมเพื่อปกป้องสิทธิและเสรีภาพของเจ้าของข้อมูล และตามประกาศที่คณะกรรมการกำหนด
2. **ฐานประโยชน์อันสำคัญต่อชีวิต ร่างกาย หรือสุขภาพ:** เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล
3. **ฐานสัญญา:** เพื่อเป็นการปฏิบัติตามสัญญาที่เจ้าของข้อมูลเป็นคู่สัญญา หรือเพื่อดำเนินการตามคำร้องขอของเจ้าของข้อมูลก่อนที่จะทำสัญญา
4. **ฐานประโยชน์อันชอบธรรม:** โดยที่ผลประโยชน์ดังกล่าวถูกแทนที่โดยสิทธิพื้นฐานของเจ้าของข้อมูลในข้อมูลส่วนบุคคลนั้น
5. **ฐานเพื่อประโยชน์สาธารณะ:** เพื่อเป็นการปฏิบัติงานที่ผู้ควบคุมข้อมูลส่วนบุคคล ดำเนินการเพื่อประโยชน์ต่อสาธารณะ
6. **ฐานทางกฎหมาย:** เพื่อเป็นการปฏิบัติตามกฎหมายที่ผู้ควบคุมข้อมูลอยู่ใต้การบังคับใช้
7. **ฐานความยินยอมของเจ้าของข้อมูล**

เพื่อลดความซับซ้อนในการปฏิบัติงานบริษัทควรใช้ความพยายามอย่างสุดความสามารถในการหลีกเลี่ยงการใช้ฐานความยินยอมเนื่องจากเป็นฐานที่ก่อให้เกิดภาระต่อบริษัทมากที่สุด

นอกจากนี้ บริษัทจะต้องจัดทำนโยบายความเป็นส่วนตัวก่อนหรือในขณะที่เก็บรวบรวมข้อมูล โดยจะต้องมีเนื้อหาดังต่อไปนี้:

1. วัตถุประสงค์ของการเก็บรวบรวมเพื่อใช้หรือเปิดเผยข้อมูลส่วนบุคคล

2. แจ้งฐานทางกฎหมายต่อเจ้าของข้อมูลส่วนบุคคล ในกรณีที่เจ้าของข้อมูลส่วนบุคคลต้องให้ข้อมูลส่วนบุคคลของตนเพื่อปฏิบัติตามฐานทางกฎหมายนั้น รวมทั้งการแจ้งผลกระทบที่อาจเกิดขึ้นได้ หากเจ้าของข้อมูลไม่ได้ให้ข้อมูลส่วนบุคคลดังกล่าว
3. ข้อมูลส่วนบุคคลที่จะรวบรวมและระยะเวลาที่จะเก็บรักษาข้อมูลส่วนบุคคลหากไม่สามารถระบุระยะเวลาการเก็บรักษาได้ให้ระบุระยะเวลาการเก็บรักษาข้อมูลที่คาดหวังตามมาตรฐานการเก็บรักษาข้อมูล
4. ประเภทของบุคคลหรือหน่วยงานที่อาจเปิดเผยข้อมูลส่วนบุคคลที่รวบรวมให้
5. ข้อมูล ที่อยู่ และรายละเอียดช่องทางการติดต่อของผู้ควบคุมข้อมูล .
6. สิทธิของเจ้าของข้อมูลตามที่กำหนดไว้ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

### ข้อมูลอ่อนไหว

รายการต่อไปนี้เป็นข้อมูลที่ละเอียดอ่อน:

- เชื้อชาติ ชาติพันธุ์ สถานภาพสมรส อายุ สีผิว และศาสนา ศาสนา ปรัชญา หรือความเกี่ยวข้องทางการเมือง
- สุขภาพ ความพิการ การศึกษา พันธุกรรม ข้อมูลไบโอเมตริกซ์ ข้อมูลเพศวิถีของบุคคล ประวัติอาชญากรรม
- หมายเลขประกันสังคม ข้อมูลสุขภาพ ใบอนุญาต การคืนภาษี ข้อมูลสหภาพแรงงาน
- หรือข้อมูลใดที่อาจกระทบต่อเจ้าของข้อมูลในลักษณะเดียวกันตามที่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนด

บริษัทจะรวบรวมข้อมูลที่ละเอียดอ่อนของเจ้าของข้อมูล โดยได้รับความยินยอมจากเจ้าของข้อมูลเท่านั้น เว้นแต่เข้าข้อยกเว้นทางกฎหมาย

พนักงานของบริษัทควรเข้าถึงและ/หรือประมวลผลข้อมูลอ่อนไหวเฉพาะเมื่อ:

- มีการบันทึกวัตถุประสงค์อันชอบธรรมในการดำเนินการดังกล่าวไว้อย่างชัดเจน
- ได้รับความยินยอมจากเจ้าของข้อมูลแต่ละราย และ
- มีการใช้มาตรการป้องกันเพื่อให้สามารถเข้าถึงข้อมูลส่วนบุคคลเฉพาะบุคคลที่ได้รับอนุญาตเท่านั้น

## บุคคลไร้ความสามารถ

ในกรณีที่บริษัทมีการประมวลผลข้อมูลของบุคคลไร้ความสามารถ บริษัทจำเป็นต้องได้รับความยินยอมจากผู้แทนโดยชอบธรรมก่อนดำเนินการประมวลผลข้อมูล

## การเก็บรวบรวมข้อมูล

บริษัทอาจเก็บรวบรวม ใช้ ประมวลผล และตรวจสอบข้อมูลส่วนบุคคลของลูกค้า พนักงาน คู่ค้า หุ้นส่วน และ/หรือผู้สมัคร เมื่อ:

- เป็นการให้บริการของบริษัทและเพื่อการสนับสนุนลูกค้าอย่างทันทั่วทั้งที่และมีประสิทธิภาพ
- ประมวลผลธุรกรรมและส่งประกาศเกี่ยวกับธุรกรรมของลูกค้า
- แก้ไขข้อผิดพลาด เก็บค่าธรรมเนียม และแก้ไขปัญหา
- ป้องกันกิจกรรมที่อาจต้องห้ามหรือผิดกฎหมาย
- ปรับแต่ง วัตถุประสงค์ และปรับปรุงบริการของบริษัท ตลอดจนเนื้อหาและเค้าโครงของเว็บไซต์และแอปพลิเคชันของบริษัท
- จัดส่งการตลาดทางตรง การแจ้งเตือนการปรับปรุงบริการ และข้อเสนอส่งเสริมการขาย
- เปรียบเทียบข้อมูลเพื่อความต้องการและตรวจสอบกับบุคคลที่สาม
- ตรวจสอบคุณภาพและความปลอดภัยของเครือข่ายและฝึกอบรมพนักงานของเรา
- บริการอื่นที่เกี่ยวข้องที่บริษัทจัดให้มี

ประเภทของข้อมูลส่วนบุคคลที่บริษัทเก็บรวบรวมขึ้นอยู่กับลักษณะของความสัมพันธ์และ/หรือธุรกรรมที่พิจารณารวมถึงแต่ไม่จำกัดเพียง:

1. ชื่อนามสกุล เพศ สถานที่ และวันเดือนปีเกิด
2. ที่อยู่อาศัยชั่วคราว/ถาวร;
3. สำเนาบัตรประจำตัวประชาชน หนังสือเดินทาง หมายเลขประกันสังคม
4. ข้อมูลการจ้างงานหรือธุรกิจ
5. รายละเอียดการชำระเงิน รวมถึงข้อมูลบัตรเครดิตและข้อมูลธนาคาร
6. รายละเอียดการติดต่อ รวมถึงหมายเลขโทรศัพท์และที่อยู่อีเมล
7. เอกสารรายได้ล่าสุด

---

8. หลักฐานการเรียกเก็บเงินที่อยู่ล่าสุด (ถ้ามี)

9. ข้อมูลอื่นๆ ที่จำเป็น

บริษัทอาจเก็บรวบรวมข้อมูลเกี่ยวกับเจ้าของข้อมูล รวมถึงแต่ไม่จำกัดเพียง ชุกรกรม ประวัติบัญชีและข้อมูล การสอบถามเกี่ยวกับผลิตภัณฑ์และบริการ ข้อมูลส่วนบุคคลที่บริษัทรวบรวมตามที่ได้รับอนุญาตหรือกำหนดโดยกฎหมาย

บริษัทอาจเก็บรวบรวมข้อมูลเกี่ยวกับเจ้าของข้อมูลเมื่อจำเป็นหรือได้รับอนุญาตตามกฎหมาย ตัวอย่างเช่น บริษัทอาจต้องการข้อมูลส่วนบุคคลเพื่อตรวจสอบตัวตนของเจ้าของข้อมูลภายใต้ นโยบายต่อต้านการฟอกเงินที่เกี่ยวข้องและกฎหมายที่บังคับใช้

บริษัทอาจรวบรวมข้อมูลจากแหล่งอื่นและเมื่อมีฐานทางกฎหมายรองรับผ่าน:

- การติดต่อและการสื่อสารกับฝ่ายที่ต้องติดต่อลูกค้าของเรา เพื่อตอบคำถามของเจ้าของข้อมูล บริษัท และตัวแทนอาจขอชื่อ หมายเลขติดต่อ และที่อยู่อีเมล
- แบ่งปันข้อมูลส่วนบุคคลของเจ้าของข้อมูลกับผู้ให้บริการ หรือบุคคลที่สาม ตามที่ลูกค้าได้ให้ความยินยอมไว้

### การประมวลผลข้อมูลส่วนบุคคล - การใช้ข้อมูล

บริษัทยังคงอยู่ภายใต้การปฏิบัติตามการใช้ข้อมูลส่วนบุคคลให้เป็นไปตามหลักเกณฑ์ทางกฎหมาย และฐานทางกฎหมายที่กล่าวไว้ข้างต้นในนโยบายนี้ ทั้งนี้วัตถุประสงค์ของการใช้ข้อมูลนั้นอาจประกอบไปด้วยแต่ไม่จำกัดเพียง

- เพื่อให้เป็นไปตามกฎหมายและข้อบังคับ (สำหรับ KYC หรือการระบุตัวตนลูกค้า)
- เพื่อปฏิบัติตามภาระผูกพันของเราที่เกิดจากสัญญาที่สร้างขึ้นระหว่างบริษัทกับลูกค้า
- เพื่อดำเนินวัตถุประสงค์ทางธุรกิจในแต่ละวันของเรา (เพื่อประมวลผลธุรกรรม แอปพลิเคชัน และคำขอของเจ้าของข้อมูล ฯลฯ)

## การใช้ข้อมูลส่วนบุคคลตามวัตถุประสงค์เดิม

บริษัทมีสิทธิในการเก็บ รวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลที่บริษัทได้รับมาจากเจ้าของข้อมูลส่วนบุคคลก่อนวันที่ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลในส่วนที่เกี่ยวข้องมีผลบังคับใช้ โดยสามารถดำเนินการต่อไปตามวัตถุประสงค์เดิม ซึ่งหากเจ้าของข้อมูลส่วนบุคคลไม่ประสงค์ที่จะให้บริษัทเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่ได้รับมาดังกล่าวต่อไป เจ้าของข้อมูลสามารถแจ้งกับทางบริษัทเพื่อขอถอนความยินยอมได้ตามช่องทางที่บริษัทกำหนดเมื่อใดก็ได้ เว้นแต่ เป็นการเก็บ รวบรวม ใช้ หรือเปิดเผยตามที่กฎหมายกำหนด

## การใช้เพื่อการตลาด

ในกรณีที่บริษัทมีการนำเสนอผลิตภัณฑ์และบริการภายใต้ความยินยอมของเจ้าของข้อมูลในการประมวลผลข้อมูลส่วนบุคคลของเจ้าของข้อมูล บริษัทอาจประมวลผลข้อมูลเพื่อวัตถุประสงค์ทางการตลาดรวมไปถึง บริษัทยังสามารถใช้ข้อมูลของเจ้าของข้อมูลเพื่อ:

- ดำเนินจัดกลุ่มการใช้บริการเพื่อนำเสนอสิทธิพิเศษ;
- ดำเนินการวิจัยตลาด;
- เสนอบริการทางการตลาดและสื่อส่งเสริมการขาย

กิจกรรมทางการตลาดดังกล่าวอาจเป็นทางไปรษณีย์ โทรศัพท์ SMS อีเมล หรือวิธีการทางอิเล็กทรอนิกส์อื่นใด เจ้าของข้อมูลสามารถแจ้งให้บริษัททราบได้ตลอดเวลาหากไม่ต้องการรับข้อเสนอการตลาดทางตรงอีกต่อไป (เลือกไม่รับ) ซึ่งระบุไว้ในส่วนของสิทธิของเจ้าของข้อมูลที่อยู่ในหัวข้อถัดไปของนโยบายฉบับนี้

## การประมวลผลข้อมูล - การเปิดเผยข้อมูลและแบ่งปัน

บริษัทจะไม่แบ่งปันข้อมูลส่วนบุคคลของเจ้าของข้อมูลกับบุคคลที่สามเพื่อวัตถุประสงค์ทางการตลาดทางตรง เว้นแต่เจ้าของข้อมูลจะให้ความยินยอมเป็นการเฉพาะ

บริษัทอาจแบ่งปันข้อมูลส่วนบุคคลของเจ้าของข้อมูลกับบุคคลที่สามเพื่อวัตถุประสงค์อื่น เฉพาะในสถานการณ์ต่อไปนี้:

1. เพื่อประมวลผลการชำระเงิน/บริการ บริษัทอาจแบ่งปันข้อมูลส่วนบุคคลอย่างปลอดภัยกับบุคคลหรือบริษัทที่เป็นคู่สัญญาในการทำธุรกรรมนี้ ซึ่งอาจรวมถึงข้อมูลติดต่อของเจ้าของข้อมูล วันที่ลงทะเบียน จำนวนการชำระเงินที่ได้รับ ข้อมูลนี้จะถูกแบ่งปันเพื่อวัตถุประสงค์ในการทำธุรกรรมเท่านั้น
2. ผู้ให้บริการภายใต้สัญญาที่ช่วยเหลือในส่วนของการดำเนินธุรกิจของบริษัท เช่น การป้องกันการฉ้อโกง การเก็บบิล การตลาด บริการ KYC (Idp, AS, RP) และบริการด้านเทคโนโลยี
3. สถาบันการเงินที่บริษัทเป็นพันธมิตรและ/หรือร่วมงานด้วย
4. บริษัทที่จะรวบรวมกิจการหรือถูกซื้อกิจการ โดยบริษัท (หากการรวมกันดังกล่าวเกิดขึ้น บริษัทจะต้องกำหนดให้นิติบุคคลที่รวมกันใหม่ปฏิบัติตามนโยบายความเป็นส่วนตัวในส่วนนี้ในส่วนที่เกี่ยวข้องกับข้อมูลส่วนบุคคลของเจ้าของข้อมูล เจ้าของข้อมูลทั้งหมดจะได้รับการแจ้งเตือนล่วงหน้าหากมีการเปลี่ยนแปลงในนโยบายที่เกี่ยวข้อง)
5. การบังคับใช้กฎหมายจากเจ้าหน้าที่ของรัฐหรือบุคคลที่สาม เมื่อ:
  - บริษัทถูกบังคับให้ทำเช่นนั้นโดยหมายศาล คำสั่งศาล หรือกระบวนการทางกฎหมายที่คล้ายคลึงกัน หรือ
  - บริษัทเชื่อโดยสุจริตว่าการเปิดเผยข้อมูลส่วนบุคคลมีความจำเป็นเพื่อป้องกันอันตรายทางร่างกายหรือการสูญเสียทางการเงิน
  - บริษัทรายงานกิจกรรมที่น่าสงสัยที่ผิดกฎหมายหรือเพื่อตรวจสอบการละเมิดข้อตกลงในสัญญาหรือการให้บริการ
  - บุคคลที่สามที่ได้รับความยินยอมจากเจ้าของข้อมูลหรือคำสั่งให้ทำเช่นนั้น
6. กรณีอื่นใดที่มีฐานทางกฎหมายรองรับ

บริษัทจะไม่ขายหรือให้เช่าข้อมูลส่วนบุคคลของเจ้าของข้อมูลให้กับบุคคลที่สามเพื่อวัตถุประสงค์ทางการตลาด และจะแบ่งปันข้อมูลส่วนบุคคลกับบุคคลที่สามตามที่อธิบายไว้ในนโยบายนี้เท่านั้น เพื่อบรรเทาความเสี่ยงในการเปิดเผยข้อมูลส่วนบุคคลโดยไม่ชอบ บริษัทมีแนวทางปฏิบัติสำหรับขั้นตอนการร้องขอให้เปิดเผยข้อมูลส่วนบุคคล

## การจัดเก็บข้อมูลและมาตรการรักษาความปลอดภัย

1. รูปแบบการจัดเก็บข้อมูล บริษัทอาจรวบรวมและเก็บรักษาข้อมูลส่วนบุคคลทั้งในรูปแบบดิจิทัล/อิเล็กทรอนิกส์ และในรูปแบบกระดาษ/ทางกายภาพ
2. บริษัทจะดูแลรักษาระบบจัดเก็บข้อมูลอิเล็กทรอนิกส์ที่ปลอดภัยตามแนวทางปฏิบัติที่ดีที่สุดในด้านไอที เพื่อดำรงไว้ซึ่งความปลอดภัย ความเป็นส่วนตัวของข้อมูล และดำเนินการเข้ารหัสข้อมูล ในกรณีที่จัดเก็บเป็นเอกสารทางกายภาพควรจัดเก็บโดยมีมาตรการจำกัดการเข้าถึง
3. บริษัทจะพยายามอย่างดีที่สุดเพื่อรักษาความปลอดภัยที่ทันสมัยสำหรับการจัดเก็บข้อมูล เพื่อให้มั่นใจว่าการเก็บรักษานั้นจะอยู่ในกรอบเวลาตามที่กฎหมายกำหนดไว้เท่านั้น
4. ระบบความปลอดภัยให้เป็นไปตามมาตรฐานที่ดีที่สุดที่ได้กำหนดไว้ในนโยบายที่เกี่ยวข้อง

## การเข้าถึงข้อมูล

### มาตรการรักษาความปลอดภัย:

บริษัทจะใช้มาตรการรักษาความปลอดภัยที่เหมาะสมเพื่อปกป้องข้อมูลส่วนบุคคลของเจ้าของข้อมูลจากการเข้าถึงโดยไม่ได้รับอนุญาตหรือการเปลี่ยนแปลง การเปิดเผย หรือการทำลายโดยไม่ได้รับอนุญาต มาตรการเหล่านี้รวมถึงการตรวจสอบภายในเกี่ยวกับแนวทางปฏิบัติในการรวบรวม การจัดเก็บ และการประมวลผลข้อมูล ตลอดจนมาตรการรักษาความปลอดภัยทางกายภาพเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

### กรอบการทำงานขององค์กร

บริษัทจะใช้มาตรการที่เหมาะสมและมีประสิทธิภาพในเวลาที่เหมาะสมเพื่อป้องกันการเปิดเผย ลบ หรือดัดแปลงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตซึ่งบริษัทได้มีไว้ในครอบครอง บริษัทจะใช้มาตรการทางกายภาพ เทคนิค เพื่อปกป้องข้อมูลส่วนบุคคล การดำเนินการเหล่านี้มีจุดมุ่งหมายเพื่อรักษาความพร้อมใช้งาน ความสมบูรณ์ และความลับของข้อมูลส่วนบุคคลและปกป้องข้อมูลจากภัยพิบัติทางธรรมชาติที่อาจเกิดขึ้นได้ การสูญหายหรือการทำลายโดยอุบัติเหตุ หรือความอันตรายจากการกระทำของมนุษย์ เช่น การเข้าถึงโดยผิดกฎหมาย การใช้ในทางที่ผิด การฉ้อโกง การทำลายโดยผิดกฎหมาย การลักลอบเปลี่ยนแปลงข้อมูล และอื่นๆ

## บุคคลากรที่รับผิดชอบ

บริษัทกำหนดบทบาทหน้าที่ และความรับผิดชอบที่เกี่ยวข้องกับการปฏิบัติตามนโยบายและพ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล ดังนี้

- คณะกรรมการบริษัท** มีหน้าที่ในการกำกับดูแลให้บริษัทต้องดำเนินการ ให้เป็นไปตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้องผ่านหน่วยงานกำกับดูแลของบริษัท รวมทั้ง มีหน้าที่ในการอนุมัตินโยบายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล และกำกับดูแลให้มีระเบียบ วิธีปฏิบัติ คู่มือการปฏิบัติงานอย่างเพียงพอ เพื่อให้บุคลากรสามารถดำเนินการให้สอดคล้องกับการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลนี้
- หน่วยงานกำกับดูแล** มีหน้าที่กำกับดูแลให้บุคลากรของบริษัททุกคน ต้องปฏิบัติตามนโยบายฉบับนี้อย่างเคร่งครัด และตรวจสอบให้แต่ละหน่วยงานที่เกี่ยวข้องกับข้อมูลส่วนบุคคลต้องจัดให้มีแนวทางในการปฏิบัติงานเพื่อให้สอดคล้องกับการปฏิบัติตามนโยบายฉบับนี้ รวมทั้ง ให้คำปรึกษาในด้านกฎเกณฑ์และแนวทางปฏิบัติงานที่สอดคล้องกับกฎหมายและนโยบาย การอบรมให้ความรู้แก่บุคลากรของบริษัท และร่วมจัดทำข้อมูลการบันทึกกิจกรรมการประมวลผลข้อมูล ประกาศนโยบายความเป็นส่วนตัว การประเมินความเสี่ยง และกิจกรรมอื่นใด เพื่อให้สอดคล้องตามกฎหมายและนโยบายฉบับนี้ พร้อมทั้ง จัดเก็บไว้เป็นหลักฐานเพื่อให้หน่วยงานกำกับดูแลที่เกี่ยวข้องทั้งภายในและภายนอกสามารถตรวจสอบได้
- หน่วยงานที่เกี่ยวข้องกับข้อมูลส่วนบุคคล** มีหน้าที่ให้ความสำคัญและปฏิบัติตามกฎหมายและนโยบายฉบับนี้อย่างเคร่งครัด โดยต้องจัดทำระเบียบและวิธีปฏิบัติงานเพื่อให้สามารถปฏิบัติงานได้สอดคล้องตามกฎหมายและนโยบายฉบับนี้ รวมทั้ง จัดให้มีระบบเทคโนโลยีสารสนเทศ หรือการจัดทำสัญญากับบุคคลภายนอกเพื่อให้เป็นไปตามกฎหมายและนโยบายฉบับนี้กำหนด
- เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล** กรณีที่บริษัทมีการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลโดยคณะกรรมการบริษัทเห็นสมควร เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลโดยความร่วมมือกับเจ้าหน้าที่ฝ่ายกำกับและตรวจสอบ จะดูแลการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลและนโยบายที่เกี่ยวข้องขององค์กร ดังนี้
  - ให้คำแนะนำแก่บริษัท รวมถึงพนักงาน หรือผู้ให้บริการของบริษัทเกี่ยวกับการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

- ตรวจสอบการดำเนินงานของบริษัท รวมถึงพนักงาน หรือผู้ให้บริการของบริษัท เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล เพื่อให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล
- ประสานงานและให้ความร่วมมือกับคณะกรรมการในกรณีที่เกิดปัญหาในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของบริษัท รวมทั้งพนักงานหรือผู้ให้บริการของบริษัทในส่วนที่เกี่ยวข้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล
- การรายงานความคืบหน้าผู้บริหารระดับสูงรับทราบเกี่ยวกับความรับผิดชอบ ความเสี่ยง และประเด็นในการปกป้องข้อมูล
- ดำเนินการประเมินผลกระทบความเป็นส่วนตัวและดำเนินการตามขั้นตอนที่จำเป็นเพื่อบรรเทาและจัดการกับความเสี่ยง
- ทบทวนขั้นตอนการปกป้องข้อมูลและนโยบายที่เกี่ยวข้องทั้งหมดตามกำหนดเวลา
- จัดให้มีการฝึกอบรมและคำแนะนำด้านการปกป้องข้อมูลสำหรับบุคคลที่อยู่ภายใต้การบังคับใช้นโยบายนี้
- ตอบสนองต่อคำร้องขอจากบุคคลเพื่อดูข้อมูลที่บริษัทเก็บไว้
- ตอบคำถามและจัดการขั้นตอนการใช้สิทธิของเจ้าของข้อมูล
- ตรวจสอบและอนุมัติข้อตกลงทางการค้าหรือข้อตกลงการแบ่งปันข้อมูลกับบุคคลที่สาม
- ใช้มาตรการรักษาความปลอดภัย เหตุการณ์ด้านความปลอดภัย และโปรโตคอลการละเมิดข้อมูลอย่างมีประสิทธิภาพ และจัดการกระบวนการแจ้งเตือนและรายงานไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
- ความรับผิดชอบอื่นที่ระบุไว้ในนโยบายที่เกี่ยวข้อง

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะต้องรักษาความลับของข้อมูลส่วนบุคคลที่ทราบหรือได้มาในระหว่างการปฏิบัติหน้าที่ตามนโยบายนี้

### หน้าที่ในการรักษาความลับ

พนักงานทุกคนจะถูกขอให้ลงนามในข้อตกลงไม่เปิดเผยข้อมูล (NDA) ซึ่งเป็นส่วนหนึ่งของสัญญาจ้าง พร้อมกับข้อตกลงความรับผิดชอบของพนักงานเกี่ยวกับการละเมิดนโยบายคุ้มครองข้อมูลเพื่อให้แน่ใจว่าบริษัทสามารถเรียกร้องให้พนักงานรับผิดชอบได้ตามกฎหมาย ในกรณีที่บริษัทต้องรับผิดชอบต่อการกระทำของลูกจ้าง

พนักงานทุกคนที่เข้าถึงข้อมูลส่วนบุคคลจะต้องดำเนินการและเก็บข้อมูลส่วนบุคคลไว้ภายใต้การรักษาความลับที่เข้มงวด ทั้งนี้ หากข้อมูลดังกล่าวไม่ได้มีไว้สำหรับการเปิดเผยต่อสาธารณะ หน้าที่ของการรักษาความลับนี้จะมีผลอยู่ต่อการถ่ายโอนไปยังแผนกอื่น ทีม ตำแหน่ง หรือแม้แต่ภายหลังการยุติความสัมพันธ์ในการจ้างงาน

### **การทดสอบ การประเมิน และการประเมินประสิทธิผลของมาตรการรักษาความปลอดภัย**

บริษัทจะทบทวนนโยบายความปลอดภัย ดำเนินการแสวงหาจุดอ่อน และทำการทดสอบการเจาะระบบภายในบริษัทเป็นประจำตามนโยบายด้านไอทีและความปลอดภัยของบริษัท บุคคลที่สามอาจได้รับการว่าจ้างให้ทำการประเมินการทดสอบดังกล่าวให้เสร็จสิ้น ข้อบกพร่องและคำแนะนำจะต้องได้รับการสื่อสารกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลและได้รับการแก้ไขอย่างทันทั่วถึง

### **การบันทึกข้อมูลและการตรวจสอบภายใน**

บริษัทจะต้องเก็บรักษาบันทึกดังต่อไปนี้อย่างน้อยเพื่อให้เจ้าของข้อมูลและสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลสามารถตรวจสอบได้ ซึ่งอาจจัดทำเป็นลายลักษณ์อักษรหรืออยู่ในรูปแบบอิเล็กทรอนิกส์ได้

1. ข้อมูลส่วนบุคคลที่รวบรวม;
2. วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลในแต่ละประเภท;
3. รายละเอียดของผู้ควบคุมข้อมูล;
4. ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล;
5. สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมถึงเงื่อนไขเกี่ยวกับบุคคลที่มีสิทธิเข้าถึงข้อมูลส่วนบุคคล และเงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคลดังกล่าว;
6. การใช้หรือเปิดเผยข้อมูลส่วนบุคคลในกรณีที่บริษัทใช้หรือเปิดเผยข้อมูลส่วนบุคคลตามกฎหมายโดยไม่ต้องขอความยินยอม;
7. การปฏิเสธคำขอหรือการคัดค้านที่กล่าวถึงในส่วนสิทธิของเจ้าของข้อมูล;

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะต้องดำเนินการตรวจสอบภายในอย่างต่อเนื่องตามนโยบายนี้ของบริษัท แล้วรายงานผลการตรวจสอบต่อคณะกรรมการ โดยตรง

## ขั้นตอนการเก็บรักษาและการกำจัดข้อมูล

บริษัทจะเก็บรักษาข้อมูลส่วนบุคคลของลูกค้าตราบนานเท่าที่บัญชีของลูกค้ายังคงใช้งานอยู่ ข้อมูลการระบุตัวตนลูกค้าทั้งหมดจะต้องได้รับการเก็บรักษาไว้อย่างปลอดภัยตราบนานเท่าที่ยังมีบัญชีอยู่จนกว่าจะสิ้นสุดความสัมพันธ์ทางธุรกิจระหว่างบริษัทแล้ว ซึ่งบริษัทจะไม่สามารถเรียกร้องฐานสัญญาในการใช้ รวบรวม หรือเปิดเผยข้อมูลลูกค้าที่บัญชีถูกปิดใช้งานได้อีกต่อไป

อย่างไรก็ตาม ตามพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 บริษัทอยู่ภายใต้ความจำเป็นในการปฏิบัติตามกฎหมายในการเก็บรักษาข้อมูลลูกค้าดังต่อไปนี้ภายหลังการสิ้นสุดความสัมพันธ์ทางธุรกิจ

- บันทึกการทำธุรกรรมและเอกสารทั้งหมดของลูกค้าของบริษัทจะต้องได้รับการเก็บรักษาและเก็บไว้อย่างปลอดภัยเป็นเวลาห้า (5) ปีนับจากวันที่เกิดการทำธุรกรรม เว้นแต่จะมีเรื่องที่ทำเป็นและสมเหตุสมผลแจ้งเป็นลายลักษณ์อักษรจากเลขาธิการ
- เมื่อบัญชีของลูกค้าถูกปิด บริษัทจะจัดเก็บบันทึกการระบุตัวตนลูกค้าและเอกสารธุรกรรมทั้งหมดที่เกี่ยวข้องกับกระบวนการ CDD และ EDD ไว้อย่างปลอดภัยเป็นเวลาอย่างน้อยสิบ (10) ปีนับจากวันที่ปิดนั้น เว้นแต่ในกรณีที่มีความจำเป็นและสมเหตุสมผล เรื่องที่เลขาธิการแจ้งเป็นหนังสือเมื่อสิ้นสุดระยะเวลาข้างต้น สำเนาทางกายภาพและอิเล็กทรอนิกส์ของข้อมูลส่วนบุคคลทั้งหมดจะถูกทำลายและกำจัดโดยใช้เทคโนโลยีที่ปลอดภัย

## เหตุการณ์การละเมิดความมั่นคงปลอดภัยของข้อมูล

บริษัทจะดำเนินการตามขั้นตอนเพื่อแก้ไขและจัดการการละเมิดข้อมูลเพื่อให้สอดคล้องกับนโยบายความปลอดภัยของบริษัท

## คณะทำงานเพื่อตอบสนองการละเมิดข้อมูล

คณะทำงานเพื่อตอบสนองการละเมิดข้อมูลจะต้องรับหน้าที่รับผิดชอบต่อการดำเนินการใดเพื่อตอบสนองต่อเหตุการณ์โดยเร็ว ในกรณีที่เกิดเหตุการณ์การละเมิดข้อมูลส่วนบุคคล คณะทำงานจะต้องดำเนินการประเมินเบื้องต้นของเหตุการณ์หรือการละเมิดเพื่อยืนยันลักษณะและขอบเขตของเหตุการณ์ดังกล่าว นอกจากนี้ ยังต้องจัดให้มีมาตรการในการบรรเทาและควบคุมผลกระทบจากเหตุการณ์ดังกล่าว

คณะทำงานเพื่อตอบสนองการละเมิดข้อมูลจะประกอบด้วยพนักงาน/เจ้าหน้าที่ดังต่อไปนี้:

- เจ้าหน้าที่รักษาความมั่นคงปลอดภัยด้านไอที
- เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

คณะทำงานยังมีหน้าที่แจ้งผู้บริหารระดับสูงเกี่ยวกับการละเมิดความปลอดภัยและเหตุการณ์ด้านความปลอดภัยที่เกี่ยวข้อง และแจ้งเตือนเจ้าของข้อมูลที่ได้รับผลกระทบจากเหตุการณ์ดังกล่าว รวมถึงแจ้งให้สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบภายในระยะเวลา 72 ชั่วโมงตามที่กฎหมายกำหนด คณะทำงานจะต้องจัดเตรียมเอกสาร โดยละเอียดของเหตุการณ์ที่พบ รวมถึงรายงานประจำปีเพื่อส่งให้ผู้บริหารรับทราบ

ในกรณีที่เกิดละเมิดข้อมูลส่วนบุคคลเกิดจากผู้ให้บริการภายนอกของบริษัท บริษัทกำหนดให้ผู้ให้บริการภายนอกต้องแจ้งบริษัทเป็นลายลักษณ์อักษรหรือผ่านช่องทางอีเมลของบริษัท ภายใน 24 ชั่วโมง นับตั้งแต่ผู้ให้บริการภายนอกทราบถึงการละเมิดข้อมูลส่วนบุคคล เพื่อให้บริษัทสามารถประเมินและแจ้งหน่วยงานที่เกี่ยวข้องได้ตามที่กฎหมายกำหนด

### **มาตรการป้องกันการเกิดเหตุการณ์ด้านความปลอดภัย**

บริษัทจะต้องดำเนินการประเมินความเสี่ยงตามรอบระยะเวลา เพื่อระบุความเสี่ยงที่อาจเกิดขึ้นในระบบการประมวลผลข้อมูลและเปิดเผยช่องโหว่ต่อการละเมิดความปลอดภัยข้อมูล นอกจากนี้ฝ่ายงานความปลอดภัยยังต้องตรวจสอบการปฏิบัติตามนโยบายด้านความปลอดภัยของพนักงานเป็นระยะเพื่อลดความเสี่ยงให้น้อยที่สุด

### **ขั้นตอนการกู้คืนและกู้คืนข้อมูลส่วนบุคคล**

องค์กรจะเก็บรักษาไฟล์สำรองสำหรับข้อมูลส่วนบุคคลทั้งหมดภายใต้การดูแลของตนเสมอ ในกรณีที่เกิดเหตุการณ์ด้านความปลอดภัยหรือการละเมิดข้อมูล องค์กรจะเปรียบเทียบการสำรองข้อมูลกับไฟล์ที่ได้รับผลกระทบเสมอเพื่อตรวจสอบความคลาดเคลื่อนหรือการเปลี่ยนแปลงอันเป็นผลมาจากเหตุการณ์นั้น

### **ความถูกต้องของข้อมูล**

บริษัทจะต้องดำเนินการตามขั้นตอนที่เหมาะสมทั้งหมดเพื่อให้แน่ใจว่าข้อมูลส่วนบุคคลจะถูกเก็บไว้อย่างถูกต้องและเป็นปัจจุบัน บริษัทจะต้องตรวจสอบให้แน่ใจว่าเจ้าของข้อมูลมีโอกาสดูแก้ไขข้อมูลส่วน

บุคคลของคุณ บริษัทต้องจัดทำบันทึกรายละเอียดของการเปลี่ยนแปลงดังกล่าวและเก็บไว้เพื่อวัตถุประสงค์ในการตรวจสอบ

บริษัทจะตรวจสอบให้แน่ใจว่าข้อมูลส่วนบุคคลเป็นข้อมูลล่าสุด ไม่เปลี่ยนแปลง เว้นแต่จะได้รับความยินยอมจากลูกค้า:

1. ข้อมูลจะถูกเก็บและทำสำเนาไว้ที่ปลอดภัยที่สุดและทำสำเนาเพียงเท่าที่จำเป็น บุคลากรไม่ควรสร้างสำเนาชุดข้อมูลเพิ่มเติมที่ไม่จำเป็น
2. บุคลากรควรใช้ทุกโอกาสเพื่อให้แน่ใจว่าข้อมูลได้รับการปรับปรุงล่าสุด เช่น การยืนยันรายละเอียดของลูกค้าเมื่อโทรมา
3. บริษัทจะอำนวยความสะดวกแก่เจ้าของข้อมูลในการปรับปรุงข้อมูลที่บริษัทเก็บไว้ เช่น ผ่านทางเว็บไซต์ของบริษัท หรือ ระบบบริการลูกค้า
4. ข้อมูลควรได้รับการปรับปรุงเมื่อพบความไม่ถูกต้อง เช่น หากไม่สามารถติดต่อลูกค้าด้วยหมายเลขโทรศัพท์ที่เก็บไว้ได้ก็ควรหาทางลบออกจากฐานข้อมูลเมื่อไม่จำเป็นต้องใช้แล้ว

### สิทธิของเจ้าของข้อมูล การสอบถาม และการร้องเรียน

เจ้าของข้อมูลทุกคนมีสิทธิย่อมมีสิทธิในข้อมูลของตนเองตามที่กฎหมายกำหนด และบริษัทจะรับประกันสิทธิเหล่านั้นเพื่อให้เจ้าของข้อมูลสามารถใช้ได้ ซึ่งเจ้าของข้อมูลมีสิทธิดังต่อไปนี้

- การเข้าถึงข้อมูล: เจ้าของข้อมูลมีสิทธิเข้าถึงข้อมูลส่วนบุคคลที่อยู่ภายใต้ความรับผิดชอบของบริษัท โดยการขอให้บริษัทจัดทำสำเนาข้อมูลดังกล่าวให้กับเจ้าของข้อมูล และขอให้บริษัทเปิดเผยข้อมูลที่เกี่ยวข้องกับเจ้าของข้อมูลได้
- การแก้ไขข้อมูล: สิทธิในการแก้ไขข้อมูลส่วนบุคคลของเจ้าของข้อมูลให้เป็นปัจจุบัน ครบถ้วน และไม่ทำให้เข้าใจผิด
- การเคลื่อนย้ายข้อมูล: สิทธิสำหรับเจ้าของข้อมูลในการ โอนย้ายข้อมูลส่วนบุคคลของตน หากบริษัทจัดระเบียบข้อมูลส่วนบุคคลดังกล่าวในรูปแบบที่เครื่องอ่านหรือใช้งานได้อัตโนมัติ และสามารถประมวลผลหรือเปิดเผยได้ด้วยวิธีการอัตโนมัติ
- ขัดแย้ง: สิทธิสำหรับเจ้าของข้อมูลในการคัดค้านการรวบรวม การใช้ และ/หรือการเปิดเผยข้อมูลส่วนบุคคลของเจ้าของข้อมูลได้ตลอดเวลา หากการกระทำดังกล่าวเป็นการกระทำเพื่อประโยชน์โดยชอบด้วยกฎหมาย

- การลบหรือทำลายข้อมูล: สิทธิสำหรับเจ้าของข้อมูลในการขอลบ ทำลาย หรือทำให้ข้อมูลส่วนบุคคลของเจ้าของข้อมูลเป็นนิรนามตามข้อกำหนดทางกฎหมาย
- การระงับการประมวลผล: สิทธิสำหรับเจ้าของข้อมูลในการขอระงับการประมวลผลข้อมูลส่วนบุคคลของเจ้าของข้อมูลตามข้อกำหนดทางกฎหมาย
- การเพิกถอนความยินยอม: สิทธิสำหรับเจ้าของข้อมูลในการเพิกถอนความยินยอมดังกล่าวเมื่อใดก็ได้ภายใต้ข้อกำหนดทางกฎหมาย

บริษัทจัดให้มีการยกระดับการใช้สิทธิของเจ้าของข้อมูลดังกล่าวโดยมีช่องทางให้เจ้าของข้อมูลสามารถส่งคำร้องขอการใช้สิทธิของตนไปยังเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลเพื่อตอบสนองการใช้สิทธิดังกล่าว เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะตรวจสอบตัวตนของผู้ใช้สิทธิที่ส่งคำขอเข้ามาก่อนจะให้ใช้สิทธิใด บริษัทอาจจัดทำแบบฟอร์มคำขอมาตรฐานในการให้เจ้าของข้อมูลส่วนบุคคลทำคำร้องขอ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะต้องดำเนินการตามคำร้องขอภายใน 7 ถึง 30 วันทำการ ทั้งนี้ขึ้นอยู่กับความยากง่ายในการให้ใช้สิทธิดังกล่าว

ทั้งนี้ ให้มีผลบังคับใช้ตั้งแต่วันที่ 26 กุมภาพันธ์ 2569 เป็นต้นไป

นายชัชวาลย์ เกียรณนัท  
ประธานกรรมการ  
บริษัท แอสตรา เอ็นเตอร์ไพรส์ จำกัด (มหาชน)

## ภาคผนวก ก.

### ขั้นตอนการปฏิบัติงานเมื่อพบข้อมูลส่วนบุคคลรั่วไหล

