**นโยบายรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล**

**บริษัท เอทู เทคโนโลยี จำกัด** (“**บริษัท**”) เห็นถึงความสำคัญ ในการประมวลผลข้อมูลส่วนบุคคลให้เหมาะสมและ ถูกต้องตามกฎหมาย โดยเฉพาะการปฏิบัติหน้าที่ของบริษัท ในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล บริษัท จึงอนุมัติรับรองและออกประกาศนโยบายรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคลฉบับนี้ขึ้น เพื่อกำหนดกรอบการรักษาความมั่นคงปลอดภัยของบริษัท ให้สอดคล้องตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (“**พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล**”) และมาตรฐานที่กำหนดไว้โดยหน่วยงานกำกับดูแล และเพื่อเป็นแนวทางเพื่อการปฏิบัติตามโดยพนักงาน และบุคคลที่เกี่ยวข้องซึ่งมีส่วนประมวลผลข้อมูลส่วนบุคคลในนามและเพื่อบริษัท

**ข้อ 1 ประกาศและผลบังคับใช้ของประกาศ**

นโยบายฉบับนี้เรียกว่า “นโยบายรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล” โดยให้มีผลบังคับใช้นับแต่วันที่ประกาศเป็นต้นไป และใช้ครอบคลุมการประมวลผลข้อมูลส่วนบุคคลทั้งหมดของทุกกลุ่มเจ้าของข้อมูลที่ดำเนินการโดยบริษัท ไม่ว่าในรูปแบบเอกสารหรือรูปแบบอิเล็กทรอนิกส์ หรือรูปแบบอื่นใดก็ตาม

**ข้อ 2 กรอบการรักษาความมั่นคงปลอดภัย**

2.1 บริษัท กำหนดกรอบการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล โดยต้องดำเนินการให้ครอบคลุมการเก็บรวบรวม ใช้และเปิดเผยข้อมูลส่วนบุคคล ให้ประกอบด้วยมาตรการเชิงองค์กร (organizational measures) มาตรการเชิงเทคนิค (technical measures) และมาตรการทางกายภาพ (physical measures) ที่จำเป็น โดยคำนึงถึงระดับความเสี่ยง ตามลักษณะและวัตถุประสงค์ของการเก็บ รวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล

2.2 มาตรการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคลทั้งหมดของบริษัท ต้องคำนึงถึงความสามารถในการธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของข้อมูลส่วนบุคคลไว้ได้อย่างเหมาะสมตามระดับความเสี่ยง โดยคำนึงถึงปัจจัยทางเทคโนโลยี บริบทสภาพแวดล้อม มาตรฐานที่เป็นที่ยอมรับสำหรับหน่วยงานหรือกิจการในประเภทลักษณะเดียวกันหรือใกล้เคียงกัน ลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้และเปิดเผยข้อมูลส่วนบุคคล ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการประกอบกัน

**ข้อ 3 โครงสร้างการบริหารการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล**

เพื่อรับประกันการดำเนินมาตรการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล ให้สมบูรณ์ถูกต้องสอดคล้องกับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล บริษัท กำหนดจัดตั้งโครงสร้างดังต่อไปนี้

3.1 คณะกรรมการบริหารบริษัท มีหน้าที่หลักในการกำหนดทิศทางและการกำกับดูแลการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล ในภาพรวมของแต่ละบริษัท และบริหารจัดการความเสี่ยงต่างๆ ที่อาจเกิดจากการประมวลผลข้อมูลส่วนบุคคล โดยมีบทบาทหลักในการตรวจสอบและอนุมัติทุกนโยบาย และแนวทางการปฏิบัติที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล

3.2 เพื่อการกำกับดูแลการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล ให้ถูกต้องตามนโยบายและพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล บริษัท กำหนดมาตรการการรักษาความมั่นคงปลอดภัย ภายใต้รูปแบบโครงสร้าง maker-checker ดังนี้

- Maker: หัวหน้าฝ่าย/หน่วยงานภายใน ซึ่งมีหน้าที่รับผิดชอบ โดยตรงในการกำกับดูแลการประมวลผลข้อมูลส่วนบุคคลภายในหน่วยงานของตน ให้ถูกต้องและสอดคล้องตามหน้าที่และกรอบการประมวลผลที่กำหนดไว้

- Checker: บริษัท แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer) ทำหน้าที่โดยอิสระในการติดตาม และตรวจสอบการปฏิบัติหน้าที่ของ Maker และรายงานผลการตรวจสอบโดยตรงไปยังคณะกรรมการบริหารบริษัท

3.3 กรณีที่ตรวจพบการฝ่าฝืนนโยบายและมาตรการการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะเป็นหน่วยงานรับเรื่องร้องเรียน กำกับดูแลหลัก รวมถึงทำหน้าที่ตรวจสอบจนทราบข้อเท็จจริง หากพบว่าเกิดการฝ่าฝืนหรือละเมิดนั้นจริง เจ้าหน้าที่จะเสนอไปยังคณะกรรมการบริหารบริษัท แล้วแต่ความรุนแรงของการละเมิดและตำแหน่งของผู้ที่กระทำผิดเพื่อพิจารณากำหนดมาตรการลงโทษตามข้อกำหนดที่ระบุไว้ ตามการลงโทษทางวินัยตามระเบียบบริหารงานบุคคลต่อไป

**ข้อ 4 การประเมินและบริหารจัดการความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยการประมวลผลข้อมูลส่วนบุคคล**

บริษัท ต้องประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยในการประมวลผลข้อมูลส่วนบุคคลอย่างน้อยปีละ 1 ครั้ง หรือทุกครั้งที่มีการเปลี่ยนแปลงที่เพิ่มเติมรูปแบบการประมวลผลข้อมูลส่วนบุคคลจากที่ได้ประเมินไว้ โดยต้องเริ่มดำเนินการตั้งแต่การระบุความเสี่ยงที่สำคัญที่อาจจะเกิดขึ้นกับทรัพย์สินสารสนเทศที่สำคัญ การป้องกันความเสี่ยงที่สำคัญที่อาจจะเกิดขึ้น การตรวจสอบและเฝ้าระวังภัยคุกคามและเหตุการละเมิดข้อมูลส่วนบุคคล การเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามและเหตุการละเมิดข้อมูลส่วนบุคคล และการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคาม หรือเหตุการละเมิดข้อมูลส่วนบุคคลเท่าที่จำเป็น โดยคำนึงถึงความจำเป็นในการเข้าถึง และใช้งาน ตามลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล การรักษาความมั่นคงปลอดภัยตามระดับความเสี่ยง ทรัพยกรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการประกอบกัน

**ข้อ 5 การสื่อสารประชาสัมพันธ์นโยบาย**

บริษัท ให้ความสำคัญต่อการสื่อสารนโยบาย และแนวทางการปฏิบัติงานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยประมวลผลข้อมูลส่วนบุคคล ให้แก่พนักงานทั้งหมดของบริษัท โดยกำหนดเป็นนโยบายการสื่อสารผ่านทุกช่องทางการติดต่อกับพนักงาน อย่างเป็นปกติ โดยเฉพาะเมื่อมีการเปลี่ยนแปลงที่มีสาระสำคัญและกระทบต่อการประมวลผลข้อมูลส่วนบุคคลรวมของบริษัท โดยเฉพาะการสร้างเสริมความตระหนักรู้ ด้านความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัย (privacy and security awareness) และการแจ้งนโยบาย แนวปฏิบัติ และมาตรการด้านการคุ้มครองข้อมูล ส่วนบุคคลและการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคลอย่างเหมาะสม

**ข้อ 6 มาตรการรักษาความมั่นคงปลอดภัย**

บริษัท กำหนดมาตรฐานการรักษาความมั่นคงปลอดภัย ในส่วนที่เกี่ยวกับการเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข ลบหรือเปิดเผยข้อมูลส่วนบุคคล อย่างน้อยต้องประกอบด้วยการดำเนินการดังต่อไปนี้อย่างเหมาะสมตามระดับความเสี่ยง ดังนี้

6.1 การควบคุมการเข้าถึงข้อมูลส่วนบุคคล และส่วนประกอบของระบบสารสนเทศที่สำคัญ (access control ) ที่มีการพิสูจน์และยืนยันตัวตน (identity proofing and authentication ) และการอนุญาตหรือการกำหนดสิทธิในการเข้าถึงและใช้งาน (authorization ) ที่เหมาะสม โดยคำนึงถึง หลักการให้สิทธิเท่าที่จำเป็น (need -to -know basis ) ตามหลักการให้สิทธิที่น้อยที่สุดเท่าที่จำเป็น (principle of least privilege )

6.2 การบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) ที่เหมาะสม ซึ่งอาจรวมถึงการลงทะเบียนและการถอนสิทธิผู้ใช้งาน (user registration and de -registration) การจัดการสิทธิการเข้าถึงของผู้ใช้งาน (user access provisioning ) การบริหารจัดการสิทธิการเข้าถึงตามสิทธิ (management of privileged access rights) การบริหารจัดการข้อมูลความลับสำหรับ การพิสูจน์ตัวตนของผู้ใช้งาน (management of secret authentication information

of users) การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (review of user access rights) และการถอดถอนหรือ ปรับปรุงสิทธิการเข้าถึง (removal or adjustment of access rights)

6.3 การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกัน การเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข ลบ หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ซึ่งรวมถึงกรณีที่เป็นการกระทำนอกเหนือบทบาทหน้าที่ที่ได้รับมอบหมาย ตลอดจนการลักลอบ ทำสำเนาข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และการลักขโมยอุปกรณ์จัดเก็บ หรือประมวลผลข้อมูลส่วนบุคคล

6.4 การจัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง แก้ไข หรือลบข้อมูลส่วนบุคคล (audit trails) ที่เหมาะสมกับวิธีการและสื่อที่ใช้ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

**ข้อ 7. การทบทวนหรือปรับปรุงนโยบาย**

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลต้องทบทวน หรือปรับปรุงนโยบายฉบับนี้ ด้วยการพิจารณาจากรายงานการปฏิบัติตามนโยบายการบริหารจัดการคุ้มครองการประมวลผลข้อมูลอย่างน้อยปีละ 1 ครั้งหรือกรณีที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญในส่วนของกระบวนการประมวลผลข้อมูลส่วนบุคคลที่บริษัท ดำเนินการ เพื่อให้นโยบายเป็นปัจจุบันอยู่เสมอ โดยจะมีการเสนอให้คณะกรรมการบริหารบริษัท แต่ละบริษัท พิจารณารับรองทุกครั้ง ที่มีการทบทวนและแก้ไขเปลี่ยนแปลง

ประกาศนับแต่วันที่ 9 พฤศจิกายน 2566

**บริษัท เอทู เทคโนโลยี จำกัด**