นโยบายด้านความปลอดภัยสารสนเทศ
และการพัฒนาเทคโนโลยีปัญญาประดิษฐ์อย่างรับผิดชอบ
บริษัท ทีฆาก่อสร้าง จำกัด (มหาชน)

บริษัท ทีฆาก่อสร้าง จำกัด (มหาชน) ตระหนักถึงความสำคัญของการบริหารจัดการด้านความปลอดภัยของสารสนเทศและการพัฒนาเทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence - AI)-อย่างปลอดภัยและมีจริยธรรม เพื่อรองรับการเปลี่ยนแปลงในยุคดิจิทัลและสร้างคุณค่าที่ยั่งยืนแก่ธุรกิจและผู้มีส่วนได้เสียทุกกลุ่ม คณะกรรมการบริษัทจึงได้อนุมัติให้มีนโยบายด้านความปลอดภัยสารสนเทศและการพัฒนาเทคโนโลยีปัญญาประดิษฐ์อย่างรับผิดชอบ เพื่อให้ผู้ที่เกี่ยวข้องใช้เป็นแนวทางในการดำเนินการได้อย่างเหมาะสม

1. ขอบเขตนโยบาย

นโยบายด้านความปลอดภัยสารสนเทศและการพัฒนาเทคโนโลยีปัญญาประดิษฐ์อย่างรับผิดชอบนี้มีผลบังคับใช้กับบุคลากรทุกระดับของบริษัท รวมถึงพนักงานประจำ พนักงานชั่วคราว ผู้บริหาร คู่ค้า และผู้ที่เกี่ยวข้องที่ได้รับมอบหมายหรือได้รับสิทธิ์ในการเข้าถึงข้อมูลหรือระบบเทคโนโลยีของบริษัท นโยบายนี้ครอบคลุมการจัดเก็บ การใช้ และการป้องกันข้อมูลทุกประเภทของบริษัท ทั้งข้อมูลทางการเงิน ข้อมูลการดำเนินธุรกิจ ข้อมูลส่วนบุคคลของลูกค้า คู่ค้า พนักงาน และผู้มีส่วนได้เสียทุกกลุ่ม รวมถึงการพัฒนาและการใช้งานเทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence - AI) อย่างมีจริยธรรมและปลอดภัย

2. วัตถุประสงค์

- เพื่อป้องกันการรั่วไหล การเข้าถึงโดยไม่ได้รับอนุญาต และการถูกโจมตีทางไซเบอร์ที่อาจก่อให้เกิดความเสียหายต่อข้อมูลและระบบเทคโนโลยีของบริษัท
- เพื่อให้การพัฒนาและใช้งาน AI ของบริษัทเป็นไปอย่างปลอดภัย โปร่งใส ยุติธรรม และไม่สร้างผลกระทบในเชิงลบต่อผู้มีส่วนได้เสียทุกกลุ่ม
- เพื่อให้การดำเนินงานด้านความปลอดภัยสารสนเทศและ AI เป็นไปตามกฎหมาย ระเบียบข้อบังคับ และมาตรฐานที่เกี่ยวข้อง เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) และหลักธรรมาภิบาลที่กำหนดไว้ในคู่มือจรรยาบรรณและหลักการกำกับดูแลกิจการของบริษัท

- เพื่อสร้างความเชื่อมั่นในความโปร่งใสและความน่าเชื่อถือของบริษัทในการจัดการข้อมูลและการใช้เทคโนโลยีอย่างรับผิดชอบ
- เพื่อให้การบริหารจัดการด้านความปลอดภัยสารสนเทศและ AI สอดคล้องกับเป้าหมายการพัฒนาที่ยั่งยืน (SDGs) และส่งเสริมความสามารถทางการแข่งขันของบริษัทในระยะยาว

3. หน้าที่ความรับผิดชอบ

เพื่อให้การบริหารจัดการด้านความปลอดภัยสารสนเทศและการพัฒนาเทคโนโลยีปัญญาประดิษฐ์เป็นไปอย่างมีประสิทธิภาพ ครอบคลุมทุกระดับขององค์กร และสอดคล้องกับทิศทางธุรกิจของบริษัท จึงกำหนดหน้าที่และความรับผิดชอบของหน่วยงานและบุคคลที่เกี่ยวข้อง ดังนี้

3.1 คณะกรรมการบริษัท

- อนุมัติและกำกับดูแลนโยบายด้านความปลอดภัยสารสนเทศและการพัฒนาเทคโนโลยีปัญญาประดิษฐ์อย่างรับผิดชอบให้สอดคล้องกับเป้าหมายเชิงกลยุทธ์และแนวทางธรรมาภิบาลของบริษัท
- ให้คำแนะนำเชิงกลยุทธ์แก่ผู้บริหารระดับสูงเพื่อส่งเสริมความยั่งยืนในด้านเทคโนโลยีและการป้องกันความเสี่ยง

3.2 ผู้บริหารระดับสูง

- จัดสรรทรัพยากร เช่น บุคลากร งบประมาณ และเทคโนโลยีให้เพียงพอและเหมาะสมต่อการดำเนินงานด้านความปลอดภัยสารสนเทศและ AI
- ติดตามความคืบหน้าของการดำเนินงานและการจัดการภัยคุกคาม รวมถึงการตรวจสอบระบบและการประเมินความปลอดภัยอย่างสม่ำเสมอ
- สนับสนุนการพัฒนากระบวนการจัดการ AI อย่างมีจริยธรรม และตรวจสอบให้แน่ใจว่าการพัฒนา AI สอดคล้องกับแนวทางของบริษัท
- ส่งเสริมการสร้างความรู้ ความเข้าใจ และความตระหนักแก่พนักงานและคู่ค้า โดยเน้นถึงความสำคัญของความปลอดภัยสารสนเทศและการใช้งาน AI อย่างมีจริยธรรม
- รายงานการดำเนินงานและความท้าทายที่สำคัญด้านความปลอดภัยสารสนเทศให้คณะกรรมการบริษัทหรือคณะกรรมการชุดย่อยที่เกี่ยวข้องทราบเป็นระยะ

3.3 **หน่วยงานที่เกี่ยวข้อง**

- พัฒนาระบบจัดเก็บและจัดการข้อมูลสารสนเทศและข้อมูลที่เกี่ยวข้องกับ AI ให้มีความปลอดภัยและเป็นไปตามข้อกำหนด
- ดำเนินการตรวจสอบและติดตามภัยคุกคามทางไซเบอร์ รวมถึงการพัฒนาแผนรับมือที่เหมาะสม
- ประสานงานกับผู้บริหารและหน่วยงานภายนอกที่เกี่ยวข้องในการจัดการความเสี่ยงและข้อพิพาทที่เกิดขึ้น
- ติดตามแนวโน้มเทคโนโลยีและภัยคุกคามที่เกี่ยวข้องกับความปลอดภัยสารสนเทศและ AI เพื่อเสนอแนะแนวทางการพัฒนาที่ทันสมัย
- อบรมบุคลากรที่เกี่ยวข้องให้มีความเข้าใจในระบบและเครื่องมือที่เกี่ยวข้องกับการจัดการความปลอดภัย

3.4 **พนักงาน**

- ปฏิบัติตามนโยบาย แนวปฏิบัติ และมาตรการด้านความปลอดภัยสารสนเทศและ AI ที่บริษัทกำหนด
- ใช้ข้อมูลและเทคโนโลยีของบริษัทอย่างเหมาะสม โดยหลีกเลี่ยงการกระทำที่อาจนำไปสู่ความเสียหายหรือการละเมิดสิทธิ์
- แจ้งผู้บังคับบัญชาในกรณีที่พบเห็นภัยคุกคามทางไซเบอร์ การละเมิดข้อมูล หรือการใช้งาน AI ที่ไม่เหมาะสม
- เข้าร่วมการอบรมหรือกิจกรรมที่เกี่ยวข้องกับความปลอดภัยสารสนเทศและ AI เพื่อเพิ่มความรู้และความตระหนักในบทบาทที่สำคัญ

4. นโยบายและมาตรการ

- บุคลากรทุกคนต้องปฏิบัติตามนโยบายและมาตรการด้านความปลอดภัยสารสนเทศที่กำหนดไว้ โดยต้องปกป้องข้อมูลที่เป็นความลับของบริษัท ลูกค้า คู่ค้า และพนักงาน ไม่ให้เกิดการรั่วไหลหรือการนำไปใช้โดยไม่ได้รับอนุญาต
- ห้ามนำข้อมูลภายในของบริษัทไปใช้หรือเปิดเผยเพื่อผลประโยชน์ส่วนตัวหรือบุคคลที่สาม โดยไม่ได้รับการอนุมัติ

- มีการจัดการและควบคุมการเข้าถึงข้อมูลอย่างเหมาะสม โดยใช้ระบบรักษาความปลอดภัยที่ทันสมัยและสอดคล้องกับมาตรฐานที่เกี่ยวข้อง
- บุคลากรทุกคนต้องใช้ระบบและอุปกรณ์เทคโนโลยีของบริษัทเพื่อวัตถุประสงค์ในการทำงานเท่านั้น ห้ามนำไปใช้ในทางที่อาจก่อให้เกิดความเสียหายหรือความเสี่ยงต่อความปลอดภัย
- ห้ามติดตั้งซอฟต์แวร์หรือโปรแกรมใด ๆ บนอุปกรณ์ของบริษัทโดยไม่ได้รับอนุญาต เพื่อป้องกันความเสี่ยงจากมัลแวร์หรือไวรัสคอมพิวเตอร์
- การพัฒนาและใช้งาน AI ต้องดำเนินการอย่างมีความรับผิดชอบ โดยคำนึงถึงความโปร่งใส ความเป็นธรรม และไม่สร้างผลกระทบเชิงลบต่อผู้มีส่วนได้เสีย
- บุคลากรต้องหลีกเลี่ยงการใช้ AI ในลักษณะที่ก่อให้เกิดความลำเอียงหรือการเลือกปฏิบัติ และต้องประเมินผลกระทบของ AI ต่อความเป็นส่วนตัวของข้อมูล
- การใช้งาน AI ต้องได้รับการตรวจสอบและประเมินผลอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าเป็นไปตามหลักจริยธรรมและกฎหมายที่เกี่ยวข้อง
- บริษัทมีมาตรการป้องกันภัยคุกคามทางไซเบอร์อย่างเข้มงวด เช่น การตรวจสอบระบบอย่างสม่ำเสมอ การเข้ารหัสข้อมูล และการพัฒนาแผนรับมือในกรณีที่เกิดเหตุไม่คาดฝัน
- บุคลากรมีหน้าที่รายงานเหตุการณ์ที่เกี่ยวข้องกับภัยคุกคามหรือการละเมิดความปลอดภัยของระบบทันทีที่พบ
- บุคลากรทุกคนมีหน้าที่ปฏิบัติตามมาตรการและแนวทางที่กำหนด รวมถึงเข้าร่วมการฝึกอบรมที่เกี่ยวข้องเพื่อพัฒนาความรู้ความเข้าใจในด้านความปลอดภัยของข้อมูลและ AI
- ส่งเสริมให้บุคลากรมีจิตสำนึกและความระมัดระวังในการใช้ข้อมูลและเทคโนโลยีของบริษัท
- การจัดการข้อมูลส่วนบุคคลต้องเป็นไปตามกฎหมายที่เกี่ยวข้อง โดยมีมาตรการคุ้มครองความเป็นส่วนตัว (Privacy) ของข้อมูลในทุกกระบวนการ
- บริษัทมุ่งมั่นที่จะปฏิบัติตามมาตรฐานระดับสากลในการบริหารจัดการข้อมูลและเทคโนโลยี
- การฝึกอบรม การประชุมเชิงปฏิบัติการ และเวิร์กช็อป โดยเนื้อหาจะครอบคลุมถึงหลักการรักษาความปลอดภัยข้อมูล การใช้งาน AI อย่างมีจริยธรรม การป้องกันภัยคุกคามทางไซเบอร์ และการจัดการข้อมูลส่วนบุคคลให้ปลอดภัย เนื้อหาการฝึกอบรมจะถูกออกแบบให้สอดคล้องกับลักษณะงานและความต้องการขององค์กร เพื่อให้บุคลากรสามารถนำไปปรับใช้ในกระบวนการทำงานได้อย่างเหมาะสม

- ผู้มีส่วนได้เสียสามารถแจ้งเบาะแสการละเมิดนโยบายด้านความปลอดภัยสารสนเทศและการพัฒนาเทคโนโลยีปัญญาประดิษฐ์ได้ที่ช่องทางการแจ้งเบาะแสการกระทำผิด (Whistle Blowing) โดยบริษัทมีการเก็บรักษาข้อมูลผู้แจ้งเบาะแสไว้เป็นความลับตามนโยบายการแจ้งเบาะแส
  1. ผู้บังคับบัญชาที่รับผิดชอบโดยตรง หรือ
  2. ส่งจดหมายอิเล็กทรอนิกส์ถึงผู้บังคับบัญชา หรือสำนักตรวจสอบภายใน หรือแผนกบุคคล หรือ
  3. ส่งทางไปรษณีย์ถึงประธานกรรมการตรวจสอบ หรือกรรมการของบริษัทฯ
  4. แจ้งทาง https://investor.tekacon.com/th/corporate-governance/whistleblowing
- หากพบว่ามีการกระทำผิดหรือฝ่าฝืนนโยบาย บริษัทจะดำเนินการลงโทษตามระเบียบวินัยของบริษัทอย่างเหมาะสม เพื่อสร้างมาตรฐานการปฏิบัติงานที่โปร่งใส สนับสนุนการพัฒนาเทคโนโลยีที่ปลอดภัยและมีจริยธรรม ตลอดจนรักษาความเชื่อมั่นจากผู้มีส่วนได้เสีย
- บริษัทกำหนดให้มีการตรวจสอบและปรับปรุงนโยบายด้านความปลอดภัยสารสนเทศและการพัฒนาเทคโนโลยีปัญญาประดิษฐ์อย่างรับผิดชอบอย่างต่อเนื่อง อย่างน้อยปีละหนึ่งครั้ง หรือเมื่อมีการเปลี่ยนแปลงด้านกฎหมาย กฎระเบียบ หรือแนวปฏิบัติที่เกี่ยวข้อง เพื่อให้มั่นใจว่านโยบายดังกล่าวยังคงเหมาะสมและมีประสิทธิภาพในการตอบสนองต่อการเปลี่ยนแปลงทางธุรกิจและเทคโนโลยี

อนุมัติโดยมติที่ประชุมคณะกรรมการบริษัท ครั้งที่ 4/2569 เมื่อวันที่ 4 พฤศจิกายน 2569
ทั้งนี้ ให้มีผลบังคับใช้ตั้งแต่วันที่ 5 พฤศจิกายน 2569 เป็นต้นไป

ลงชื่อ .....

(นายพูลสวัสดิ์ เผ่าประพัธน์)

รักษาการประธานกรรมการ