

บริษัท ทีซีเอ็ม คอร์ปอเรชั่น จำกัด (มหาชน) นโยบายความปลอดภัยในการใช้ AI

1. วัตถุประสงค์

นโยบายความปลอดภัยในการใช้ AI นี้จัดทำขึ้นเพื่อกำหนดแนวทางและหลักการในการใช้เทคโนโลยีปัญญาประดิษฐ์ (“AI”) และแอปพลิเคชัน (เรียกรวมกันว่า “ระบบ AI”) ภายในบริษัท ทีซีเอ็ม คอร์ปอเรชั่น จำกัด (มหาชน) (“บริษัท”) โดยมีจุดมุ่งหมายเพื่อให้แน่ใจว่าการใช้งานระบบ AI จะต้องคำนึงถึงหลักจริยธรรม การรักษาความเป็นส่วนตัว ความปลอดภัย กฎหมายและข้อกำหนดที่เกี่ยวข้อง และสอดคล้องกับค่านิยมและวัตถุประสงค์ขององค์กร เป็นลำดับแรก

2. ขอบเขต

2.1. การบังคับใช้

นโยบายนี้ใช้สำหรับพนักงานทุกระดับ และบุคคลที่สามที่เกี่ยวข้องกับการใช้ระบบ AI ภายในบริษัท

2.2. เครื่องมือและแอปพลิเคชัน

นโยบายนี้ใช้ควบคุมการใช้ระบบ AI ของบุคคลที่สาม หรือระบบ AI ที่เปิดให้ใช้เป็นสาธารณะ ครอบคลุม แพลตฟอร์มและแอปพลิเคชันที่คล้ายคลึงกัน ที่ออกแบบมาเพื่อจำลองสติปัญญาของมนุษย์ในการสร้าง การตอบสนอง การคิด การคำนวณ การวิเคราะห์ การช่วยสร้างผลงาน หรือช่วยทำภารกิจใดโดยเฉพาะ ตามรายการในภาคผนวก ก. นอกจากนี้ยังรวมถึงแอปพลิเคชันหรือระบบ AI ใด ๆ ที่ได้รับการออกแบบเพื่อทำหน้าที่ที่คล้ายคลึงกันที่อาจเกิดขึ้นในอนาคต

3. คุณสมบัติของระบบ AI ที่นำมาใช้ปฏิบัติงาน

ในการเลือกระบบ AI เพื่อใช้ในการปฏิบัติงานของบริษัท นอกจากต้องคำนึงถึงประสิทธิภาพและวัตถุประสงค์ขององค์กรแล้ว ยังต้องคำนึงถึงหลักการจริยธรรม AI รวมถึงกฎหมายที่เกี่ยวข้อง บริษัทจึงกำหนดแนวทางพิจารณา ระบบ AI ที่สอดคล้องตามหลักจริยธรรม ดังนี้ โดยต้องพิจารณาควบคู่กับบริบท ความเสี่ยง และผลกระทบที่อาจเกิดจากการประยุกต์ใช้ระบบ AI

- (1) ความเท่าเทียม หลากหลาย ครอบคลุม และเป็นธรรม (Fairness) ของผลลัพธ์จากการทำงานของระบบ AI หมายถึง ระบบ AI ที่สามารถประมวลผลได้อย่างเป็นธรรม เที่ยงตรง และปราศจากอคติ
- (2) ความโปร่งใส (Transparency) ในการทำงานของระบบ AI หมายถึง การที่สามารถอธิบายเหตุการณ์ การกระทำ กระบวนการทำงาน และกิจกรรมต่าง ๆ ที่เกิดขึ้นย้อนหลังได้ เพื่อให้ผู้ใช้งานระบบ AI สามารถตรวจสอบกิจกรรมต่าง ๆ ว่าดำเนินไปด้วยความถูกต้องและสามารถคาดการณ์การกระทำต่าง ๆ ได้
- (3) ความน่าเชื่อถือ (Reliability) ในการทำงานของระบบ AI หมายถึง ความสามารถและคุณภาพของระบบ AI ที่มีความน่าเชื่อถือต่อผู้ใช้งานระบบ AI เช่น ความถูกต้องแม่นยำ ความสมบูรณ์ ความเป็นปัจจุบัน ความเกี่ยวข้องของข้อมูลและความสามารถในการนำไปใช้

- (4) ความมั่นคงปลอดภัยและความเป็นส่วนตัว (Security and Privacy) ของระบบ AI หมายถึง ระบบ AI ที่มีความมั่นคงปลอดภัย ทำให้สามารถลดช่องโหว่และป้องกันภัยคุกคามต่าง ๆ ที่อาจก่อให้เกิดผลทางด้านลบ และมีความสอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้อง

4. แนวปฏิบัติสำหรับผู้ใช้งานระบบ AI ในการปฏิบัติงาน

4.1. สิ่ง que ผู้ใช้งานระบบ AI ควรปฏิบัติ:

- ✓ ศึกษาความรู้ทั่วไปเกี่ยวกับประโยชน์ และทักษะที่จำเป็นในการใช้ระบบ AI เพื่อให้สามารถปฏิบัติงานร่วมกับระบบ AI ได้อย่างถูกต้อง
- ✓ เลือกใช้ระบบ AI ที่มีประสิทธิภาพและสอดคล้องตามวัตถุประสงค์ในการปฏิบัติงานของบริษัท
- ✓ ติดตามข่าวสารที่เกี่ยวข้องกับเทคโนโลยี AI อย่างสม่ำเสมอ เพื่อให้ทราบถึงองค์ความรู้ใหม่และสามารถรับมือกับภัยคุกคามต่าง ๆ ได้
- ✓ ให้ความสำคัญกับการใช้งานระบบ AI โดยคำนึงถึงจริยธรรมและความเป็นธรรม
- ✓ ตระหนักว่าระบบ AI สามารถใช้เป็นประโยชน์ได้ แต่ไม่ควรใช้แทนที่วิจารณญาณและความคิดสร้างสรรค์ของมนุษย์
- ✓ ตระหนักถึงความเป็นไปได้ว่าผลลัพธ์จากการใช้ระบบ AI อาจเกิดความคลาดเคลื่อน รวมถึง ภาพลวงตา ข้อมูลเท็จ หรือข้อมูลที่ไม่สมบูรณ์ ดังนั้น ผู้ใช้งานต้องทำการตรวจสอบผลการตอบสนองอย่างละเอียดอย่างสม่ำเสมอ
- ✓ ตรวจสอบให้แน่ใจว่าผลลัพธ์จากระบบ AI ที่จะนำมาใช้อ้างอิงในการปฏิบัติงานนั้นมีความถูกต้อง ปราศจากอคติ สอดคล้องกับกฎหมายทรัพย์สินทางปัญญาและกฎหมายคุ้มครองข้อมูลส่วนบุคคล และไม่ขัดต่อนโยบายของบริษัท
- ✓ เมื่อใช้ระบบ AI สำหรับการออกแบบ ให้ตรวจสอบว่าผลงานนั้นเป็นต้นฉบับและไม่ละเมิดลิขสิทธิ์ที่มีอยู่แล้ว ทั้งนี้ แนวคิดการออกแบบต้องสอดคล้องกับแนวโน้มตลาดปัจจุบันและความพึงพอใจของลูกค้า
- ✓ ปฏิบัติต่อข้อมูลทั้งหมดที่ให้ไว้กับระบบ AI ในฐานะข้อมูลสาธารณะ ไม่ว่าจะเป็นการตั้งค่าเครื่องมือ หรือการรับรองจากผู้สร้าง
- ✓ ตระหนักถึงการรับผิดชอบต่อ (Accountability) ของตนเองในการใช้งานระบบ AI
- ✓ แจ้งหัวหน้างานเมื่อมีการใช้ระบบ AI เพื่อช่วยในการปฏิบัติงาน
- ✓ ได้รับอนุญาตเป็นลายลักษณ์อักษรจากหัวหน้างานและฝ่ายไอทีของบริษัท ก่อนดำเนินการรวมระบบ (Integrate) ระบบ AI กับซอฟต์แวร์ของบริษัท

4.2. สิ่ง que ผู้ใช้งานระบบ AI ควรปฏิบัติ หากมีคำถามหรือพบสิ่งผิดปกติ:

- ✓ รายงานคำถามหรือกิจกรรมที่ผิดปกติที่เกี่ยวข้องกับนโยบายความปลอดภัยของระบบ AI ต่อทีมรักษาความปลอดภัยด้านไอทีทันที โดยเฉพาะอย่างยิ่งหากกิจกรรมที่ผิดปกตินั้นเกี่ยวข้องกับการเข้าถึงโดยไม่ได้รับอนุญาต การรั่วไหลของข้อมูล หรือการละเมิดนโยบาย

4.3. สิ่งที่ใช้งานระบบ AI ไม่ควรปฏิบัติ:

- ✘ พึ่งพาอัลกอริทึมและระบบ AI เพียงอย่างเดียว โดยไม่มีมนุษย์คอยกำกับดูแลและแทรกแซงในกระบวนการตัดสินใจที่สำคัญ
- ✘ ใช้ระบบ AI ในการตัดสินใจที่เกี่ยวกับการจ้างงาน ของผู้สมัครหรือพนักงาน รวมถึงการสรรหาการจัดจ้าง การติดตามผลการปฏิบัติงาน และการเลิกจ้าง
- ✘ บ่อนข้อมูลที่เป็นการลับ มีกรรมสิทธิ์ หรือข้อมูลที่ละเอียดอ่อนของบริษัทลงในระบบ AI ใด ๆ เช่น รหัสผ่าน ข้อมูลด้านสุขภาพ ข้อมูลบุคลากร หรือข้อมูลใด ๆ ที่อาจนำไปสู่การละเมิดกฎหมายคุ้มครองข้อมูลส่วนบุคคล
- ✘ ถ่ายโอน (Upload) ข้อมูลส่วนบุคคลที่เกี่ยวข้องกับบุคคลใด ๆ รวมถึงชื่อ ที่อยู่ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลในทำนองเดียวกัน ในระบบ AI
- ✘ แอบอ้างผลงานที่สร้างโดยระบบ AI ว่าเป็นผลงานที่สร้างเอง
- ✘ ใช้ระบบ AI ที่ไม่รวมอยู่ในรายการที่ได้รับอนุมัติจากแผนกไอที เนื่องจากแชทบอท (Chatbot) ที่เป็นอันตรายอาจส่งผลกระทบต่อความปลอดภัยของข้อมูล
- ✘ ยอมรับผลงานออกแบบใด ๆ ที่สร้างโดยระบบ AI โดยไม่ตรวจสอบความเป็นไปได้ในแง่ของความสามารถในการผลิตและข้อจำกัดด้านวัสดุ

5. การละเมิด

การละเมิดนโยบายความปลอดภัยในการใช้ AI นี้ อาจส่งผลให้มีการลงโทษทางวินัย ซึ่งรวมถึงแต่ไม่จำกัดเพียงการตำหนิ การฝึกอบรมเพิ่มเติม การระงับสิทธิ์การใช้งานระบบ AI หรือการเลิกจ้าง ขึ้นอยู่กับความรุนแรงและความถี่ของการละเมิด

6. ความรับผิดชอบ

นโยบายความปลอดภัยในการใช้ AI นี้ มีวัตถุประสงค์เพื่อให้คำแนะนำและหลักการทั่วไปสำหรับการใช้ระบบ AI อย่างมีจริยธรรมและมีความรับผิดชอบภายในบริษัท ทีซีเอ็ม คอร์ปอเรชั่น จำกัด (มหาชน) เท่านั้น โดยไม่ถือเป็นคำแนะนำทางกฎหมาย และบริษัทขอสงวนสิทธิ์ในการแก้ไขหรือปรับปรุงนโยบายนี้ตามความจำเป็น เพื่อรองรับข้อกำหนดทางกฎหมายที่เปลี่ยนแปลง เทคโนโลยีที่พัฒนาขึ้น หรือตามความจำเป็นขององค์กร

ตามมติที่ประชุมคณะกรรมการบริษัท วันที่ 14 สิงหาคม 2567

บริษัท ทีซีเอ็ม คอร์ปอเรชั่น จำกัด (มหาชน)

|||||

นายพิมล ศรีวิกรม์
ประธานกรรมการบริษัท

ภาคผนวก ก.

รายชื่อระบบ AI และแอปพลิเคชันที่ได้รับการอนุมัติ

สำหรับงานออกแบบ

1. NedGraphics
2. Textronics Design Systems
3. Design2Fab
4. Poincare
5. Digital Weaving Norway (DWN)
6. Photoshop
7. Illustrator
8. MidJourney

สำหรับงานขายและการตลาด

1. HubSpot
2. Salesforce Einstein
3. Marketo
4. Conversica

สำหรับการผลิตและการดำเนินงาน

1. GE Predix
2. Spark Cognition
3. Uptake
4. Sight Machine

สำหรับการใช้งานทั่วไป

1. OpenAI's ChatGPT
2. Google Assistant Gemini
3. Amazon Alexa
4. Canva
5. Gamma
6. Grammarly

สำหรับการวิเคราะห์ข้อมูล

1. Claude AI
2. Perplexity AI
3. Blackbox AI
4. NotebookLM

สำหรับการเรียนรู้และอบรมเรื่อง AI

1. Colab
2. Kaggle

สำหรับการเขียนโปรแกรม Coding

1. Lovable
2. Cursor
3. Google Antigravity

อื่นๆ

1. BOTNOI VOICE – สำหรับการพากย์เสียงลงบนสื่อดิจิทัลสำหรับการอบรมพนักงาน
2. DeepL – สำหรับการแปล
3. Kling AI – สำหรับสร้าง Movie