นโยบายความมั่นคงปลอดภัยด้านปัญญาประดิษฐ์ (AI Security Policy)

บริษัท สเตคอน กรุ๊ป จำกัด (มหาชน) และบริษัทในเครือ ("บริษัท") สนับสนุนการนำเทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence: AI) มาใช้เพื่อเพิ่มประสิทธิภาพในการดำเนินงาน การวิเคราะห์ข้อมูล การสื่อสาร และการพัฒนากระบวนการดำเนินธุรกิจขององค์กร

อย่างไรก็ตาม การใช้งาน AI การใช้งาน AI อาจก่อให้เกิดความเสี่ยงต่อความมั่นคงปลอดภัยของข้อมูล ความลับทางธุรกิจ ข้อมูลส่วนบุคคล ทรัพย์สินทางปัญญา ตลอดจนความเสี่ยงด้านกฎหมาย และภัยคุกคามด้านข้อมูลและความมั่นคงปลอดภัยทางไซเบอร์ หากมีการใช้งานโดยไม่เหมาะสม

บริษัทจึงกำหนดนโยบายความมั่นคงปลอดภัยด้านปัญญาประดิษฐ์ (AI Security Policy) เพื่อกำหนดหลักเกณฑ์และแนวทางในการใช้งาน AI ให้เป็นไปอย่างเหมาะสม ปลอดภัย และสอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ และนโยบายของบริษัท เพื่อสนับสนุนการใช้ AI เกิดประโยชน์สูงสุด รวมถึงการป้องกันภัยคุกคามด้านข้อมูลและไซเบอร์ที่อาจเกิดขึ้น ควบคู่กับการบริหารจัดการความเสี่ยงและการปกป้องข้อมูลของบริษัท บริษัทในเครือ ลูกค้า คู่ค้า และผู้มีส่วนได้เสีย

วัตถุประสงค์

1. เพื่อให้เกิดความมั่นคงปลอดภัยในการใช้งาน AI
2. เพื่อกำหนดหลักเกณฑ์และแนวทางปฏิบัติสำหรับผู้ใช้งาน AI
3. เพื่อป้องกันความเสี่ยงการรั่วไหล การเปิดเผย หรือการนำข้อมูลสำคัญของบริษัทไปใช้อย่างไม่เหมาะสม
4. เพื่อสร้างความตระหนักด้าน AI Security และลดความเสี่ยงจากการใช้ AI อย่างไม่เหมาะสม
5. เพื่อสนับสนุนการนำ AI มาใช้ในองค์กรอย่างมีประสิทธิภาพ ปลอดภัย และสอดคล้องกับกฎหมาย ระเบียบ และนโยบายของบริษัท

ขอบเขต

1. กรรมการ ผู้บริหาร พนักงาน วิศวกร และลูกจ้างทุกระดับ ของบริษัท
2. AI Tools ที่นำมาใช้ในการปฏิบัติงาน เช่น ChatGPT, Copilot, Gemini, DeepSeek, Grammarly, Claude หรือเครื่องมือ AI อื่นที่มีลักษณะเดียวกัน เป็นต้น
3. ข้อมูลของบริษัทและบริษัทในเครือทุกประเภท รวมถึงข้อมูลโครงการ เช่น Drawing, BOQ, TOR, Cost ราคาประมูล ข้อมูลลูกค้า และข้อมูลอื่นที่เกี่ยวข้องกับการดำเนินธุรกิจของบริษัท
4. การใช้ AI ในการปฏิบัติงานของบริษัททั้งภายในและภายนอกองค์กร
   ทั้งนี้ บริษัทอาจกำหนดให้บุคคลภายนอกที่ปฏิบัติงานให้แก่บริษัทปฏิบัติตามนโยบายฉบับนี้ หรือมาตรการอื่นที่เทียบเท่า ตามเงื่อนไขที่กำหนดในสัญญา ข้อตกลง หรือเอกสารที่เกี่ยวข้อง

โครงสร้างนโยบายความมั่นคงปลอดภัยด้าน AI

นโยบายความมั่นคงปลอดภัยด้าน AI บริษัท สเตคอน กรุ๊ป จำกัด (มหาชน) และบริษัทในเครือ ประกอบด้วย

1. คำนิยาม
2. อำนาจและหน้าที่
3. การใช้งาน AI อย่างปลอดภัย
   - 3.1. การควบคุมข้อมูล (Data Handling)
   - 3.2. การคุ้มครองข้อมูลส่วนบุคคล
   - 3.3. การตรวจสอบผลลัพธ์ (Output Validation)
   - 3.4. การป้องกัน Prompt Injection
   - 3.5. การใช้ AI อย่างมีความรับผิดชอบ
   - 3.6. การรายงานเหตุการณ์ผิดปกติ

4. การทบทวนนโยบาย
5. บทลงโทษและการบังคับใช้

1. **คำนิยาม**

"AI" หรือ "AI Tools" หมายถึง ระบบหรือเครื่องมือที่สามารถเรียนรู้ วิเคราะห์ สร้างข้อมูล หรือทำงานสนับสนุนการปฏิบัติงานของมนุษย์ได้ เช่น ChatGPT, Copilot, Gemini, DeepSeek, Claude หรือ เครื่องมือ AI อื่นที่มีลักษณะเดียวกันเป็นต้น

"AI สาธารณะ" หมายถึง AI/AI Tools ที่เปิดให้บุคคลทั่วไปสามารถลงทะเบียนใช้งานและสามารถนำข้อมูลของผู้ใช้งานไปเผยแพร่ต่อได้ หรือไม่มีการปกปิดข้อมูลของผู้ใช้งาน โดยส่วนมากคือ AI/AI Tools ที่เปิดให้ใช้งานฟรี หรือ AI/AI Tools ที่ไม่ใช่รูปแบบแพ็กเกจองค์กร

"ข้อมูลสำคัญ" หมายถึง ข้อมูลที่หากหลุด รั่วไหล ถูกเปิดเผย หรือถูกนำไปใช้โดยไม่ได้รับอนุญาตแล้ว อาจก่อให้เกิดความเสียหายต่อบริษัท บริษัทในเครือ ลูกค้า คู่ค้า พนักงาน หรือผู้มีส่วนได้เสีย เช่น ข้อมูลโครงการ/โครงการก่อสร้างแบบก่อสร้าง ราคาประมูล ข้อมูลลูกค้า ข้อมูลทางการเงิน ข้อมูลทางกฎหมาย และข้อมูลอื่นที่เกี่ยวข้องกับการดำเนินธุรกิจของบริษัท เป็นต้น

"ข้อมูลส่วนบุคคล" หมายถึง ข้อมูลเกี่ยวกับบุคคลธรรมดาที่สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม ตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

"Prompt" หมายถึง ข้อมูล ข้อความ คำสั่ง รูปภาพ ไฟล์ หรือ ข้อมูลอื่นใดที่ส่งให้ AI ประมวลผลหรือดำเนินการ

"Data Masking" หมายถึง การปกปิด หรือการแปลงข้อมูลสำคัญ เพื่อไม่ให้ข้อมูลจริงถูกเปิดเผย แต่ยังสามารถนำไปใช้กับ AI ได้ เช่นการเปลี่ยนข้อมูลจาก โครงการรถไฟฟ้าสายสีชมพู เป็น โครงการ A หรือ การลบข้อมูลที่สำคัญออก เช่น การลบข้อมูลราคาประมูลโครงการ หรือการทำให้ข้อมูลมีความกว้างขึ้น เช่น ข้อมูลจริง 2,485 ล้าน แปลงเป็น 3,000 ล้าน เป็นต้น

"Anonymization" หมายถึงการแปลงข้อมูลให้เป็นข้อมูลที่ไม่ระบุตัวตน หรือเป็นชื่อกลาง เพื่อไม่ให้ข้อมูลจริงถูกเปิดเผย แต่ยังสามารถนำไปใช้กับ AI ได้ เช่นการลบชื่อคน หรือชื่อบริษัทออก หรือเปลี่ยนไปใช้คำเรียกกลางเช่น ลูกค้า หรือ ผู้รับเหมา แทนการระบุชื่อลูกค้าและชื่อผู้รับเหมา เป็นต้น

2. **อำนาจและหน้าที่**

2.1 ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ มีหน้าที่ดังต่อไปนี้

- กำกับดูแลและสนับสนุนการดำเนินการตามนโยบายความมั่นคงปลอดภัยด้าน AI ของบริษัท ให้คำปรึกษาและคำแนะนำเกี่ยวกับการใช้งาน AI อย่างปลอดภัย
- พิจารณาให้คำแนะนำเกี่ยวกับ AI Tools ที่เหมาะสมกับการใช้งานของบริษัท
- รับแจ้งและประสานงานกรณีพบเหตุการณ์ผิดปกติ หรือความเสี่ยงด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับการใช้งาน AI

2.2 ผู้ใช้งาน AI มีหน้าที่ดังต่อไปนี้

- ศึกษาและทำความเข้าใจ AI ก่อนใช้งาน
- ใช้งาน AI อย่างปลอดภัย และปฏิบัติตามนโยบายความมั่นคงปลอดภัยด้าน AI อย่างเคร่งครัด

- ตรวจสอบข้อมูลก่อนนำเข้าสู่ AI และตรวจสอบผลลัพธ์จาก AI ก่อนนำไปใช้งานจริง
- แจ้งผู้บังคับบัญชาหรือฝ่ายเทคโนโลยีสารสนเทศโดยเร็ว หากพบเหตุการณ์ผิดปกติหรือความเสี่ยงที่เกี่ยวข้องกับการใช้งาน AI

3. <u>การใช้งาน AI อย่างปลอดภัย</u>

3.1 การควบคุมข้อมูล (Data Handling)

1) ห้ามนำข้อมูลลับ หรือข้อมูลสำคัญ เช่น Drawing, BOQ ราคาประมูล ข้อมูลลูกค้า ข้อมูลคู่ค่า หรือข้อมูลโครงการ ใส่ใน AI สาธารณะ
2) หากมีความจำเป็นต้องใช้ข้อมูลประกอบการใช้งาน AI ต้องดำเนินการ Data Masking หรือ Anonymization ก่อนทุกครั้ง
3) ให้ใช้เฉพาะข้อมูลตัวอย่าง (Dummy Data) หรือข้อมูลที่ไม่สามารถระบุตัวตนบุคคล องค์กร ลูกค้า คู่ค้า โครงการ หรือผู้เกี่ยวข้องได้
4) ห้าม Upload ไฟล์โครงการ เอกสารสำคัญ เอกสารสัญญา หรือข้อมูลอื่นใดของบริษัทเข้าสู่ AI สาธารณะ เว้นแต่ได้รับอนุญาตและได้ดำเนินการตามมาตรการที่บริษัทกำหนด

3.2 การคุ้มครองข้อมูลส่วนบุคคล

1) ห้ามนำข้อมูลส่วนบุคคลของกรรมการ ผู้บริหาร พนักงาน ลูกค้า คู่ค้า ผู้รับเหมา หรือบุคคลภายนอกเข้าสู่ AI สาธารณะ เว้นแต่เป็นไปตามกฎหมายและนโยบายของบริษัท
2) หากมีความจำเป็นต้องใช้ข้อมูลส่วนบุคคลประกอบการใช้งาน AI ต้องดำเนินการ Anonymization หรือ Data Masking ให้เพียงพอก่อนใช้งาน
3) ผู้ใช้งานต้องใช้ความระมัดระวังเป็นพิเศษในการใช้ข้อมูลที่สามารถระบุตัวบุคคลได้ เช่น ชื่อ นามสกุล เลขประจำตัวประชาชน ข้อมูลติดต่อ ข้อมูลพนักงาน ข้อมูลลูกค้า หรือข้อมูลอื่นที่เกี่ยวข้องกับบุคคลธรรมดา

3.3 การตรวจสอบผลลัพธ์ (Output Validation)

1) ผลลัพธ์จาก AI ต้องได้รับการตรวจสอบความถูกต้อง ความครบถ้วน และความเหมาะสม ก่อนนำไปใช้งานจริง
2) หลีกเลี่ยงการใช้ผลลัพธ์ AI ที่อาจทำให้บริษัทได้รับผลกระทบหรือเสียหายทางธุรกิจหากเกิดข้อผิดพลาด

3.4 การป้องกัน Prompt Injection

1) หลีกเลี่ยงการใช้ข้อมูลจากแหล่งที่ไม่น่าเชื่อถือ
2) ไม่ปฏิบัติตามคำสั่งจาก AI ที่ขอข้อมูลลับ ข้อมูลสำคัญ ข้อมูลส่วนบุคคล หรือข้อมูลเพิ่มเติมโดยไม่มีเหตุอันสมควร
3) หากพบพฤติกรรมผิดปกติของ AI ให้หยุดใช้งานทันทีและแจ้งเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ

3.5 การใช้ AI อย่างมีความรับผิดชอบ

1) ห้ามใช้ AI เพื่อสร้างข้อมูลเท็จ ข้อมูลบิดเบือน หรือข้อมูลที่ทำให้เข้าใจผิด
2) ห้ามใช้ AI ในกิจกรรมที่ผิดกฎหมาย หรือขัดต่อจริยธรรม หรืออาจก่อให้เกิดความเสียหายต่อบริษัท บริษัทในเครือ ลูกค้า คู่ค้า พนักงาน หรือผู้มีส่วนได้เสีย
3) ห้ามใช้ AI เพื่อสร้าง เผยแพร่ หรือส่งต่อเนื้อหาที่ละเมิดลิขสิทธิ์ เครื่องหมายการค้า ความลับทางการค้า หรือทรัพย์สินทางปัญญาของผู้อื่น
4) ต้องระบุเมื่อมีการใช้ AI ในการจัดทำเอกสารสำคัญ (ถ้ามีผลกระทบต่อการตัดสินใจ)
5) ห้าม Upload ไฟล์โครงการหรือเอกสารสำคัญขึ้นระบบ AI สาธารณะ

3.6 การรายงานเหตุการณ์ผิดปกติ

1) ในกรณีที่พบความผิดปกติจากการใช้งาน AI อันอาจก่อให้เกิดความเสียหายต่อบริษัท บริษัทในเครือ ลูกค้า คู่ค้า พนักงาน หรือผู้มีส่วนได้เสีย ผู้พบความผิดปกติต้องแจ้งผู้ที่เกี่ยวข้อง และผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ เพื่อประเมินความเสี่ยง และจัดการรับมือต่อความเสียหายที่อาจเกิดขึ้นอย่างเหมาะสม

4. <u>การทบทวนนโยบาย</u>

บริษัทจะทบทวนนโยบายฉบับนี้เป็นระยะ หรือเมื่อมีการเปลี่ยนแปลงด้านกฎหมาย เทคโนโลยี ความเสี่ยงด้านความมั่นคงปลอดภัย หรือแนวปฏิบัติที่เกี่ยวข้อง เพื่อให้นโยบายมีความเหมาะสมและสอดคล้องกับการดำเนินธุรกิจของบริษัท

5. <u>บทลงโทษและการบังคับใช้</u>

การฝ่าฝืนนโยบายฉบับนี้ หรือการใช้งาน AI ในลักษณะที่อาจก่อให้เกิดความเสี่ยงหรือความเสียหายต่อบริษัท บริษัทในเครือ ลูกค้า คู่ค้า พนักงาน หรือผู้มีส่วนได้เสีย ถือเป็นการกระทำผิดวินัย บริษัทอาจพิจารณาดำเนินการลงโทษตามความเหมาะสม ตามข้อกำหนดหรือระเบียบบริษัท

นโยบายความมั่นคงปลอดภัยด้านปัญญาประดิษฐ์ฉบับนี้ อนุมัติโดยที่ประชุมคณะกรรมการบริษัท ครั้งที่ 4/2569 เมื่อวันที่ 14 สิงหาคม 2569 และให้มีผลใช้บังคับตั้งแต่วันที่ 14 สิงหาคม 2569 เป็นต้นไป

ลงชื่อ .....

(นายวัลลภ รุ่งกิจวรเสถียร)
ประธานกรรมการบริษัท
บริษัท สเตคอน กรุ๊ป จำกัด (มหาชน)