



บริษัท ผลิตไฟฟ้า จำกัด (มหาชน)

นโยบายด้านปัญญาประดิษฐ์

Artificial Intelligence Policy

ประวัติการปรับปรุงเอกสาร

เวอร์ชัน	คำอธิบายและเหตุผลในการแก้ไข	ผู้แก้ไข	วันที่
1.0	เอกสารเผยแพร่ฉบับแรก		

ลายเซ็นรับรองเอกสาร

หน้าที่	ชื่อ	ลายเซ็น	ตำแหน่ง	วันที่
จัดทำโดย	อาทิตย์ ลออนวล		ผู้จัดการส่วนคุ้มครองข้อมูลและความมั่นคงปลอดภัยไซเบอร์	มิถุนายน 69
ตรวจทาน	วุฒิรัฐ จิ่งแสงสถิตย์พร		ผู้จัดการฝ่ายโครงสร้างพื้นฐานและความมั่นคงปลอดภัยระบบสารสนเทศ	มิถุนายน 69
อนุมัติโดย	ประเสริฐ สินสุขประเสริฐ		ประธานกรรมการ	

1. บทนำ

บริษัท ผลิตไฟฟ้า จำกัด (มหาชน) และบริษัทย่อยที่จดทะเบียนในประเทศไทย (รวมเรียกว่า “กลุ่มเอ็กโก”) ได้จัดให้มีระบบเทคโนโลยีสารสนเทศ ขึ้นเพื่อรองรับการเปลี่ยนผ่านขององค์กรสู่การดำเนินงานในยุคปัญญาประดิษฐ์ (Artificial Intelligence – AI) และส่งเสริมการใช้เทคโนโลยีเป็นเครื่องมือในการเพิ่มประสิทธิภาพ และประสิทธิผลในการทำงาน สนับสนุนการตัดสินใจ และยกระดับนวัตกรรมทางธุรกิจ โดยอยู่ภายใต้กรอบการบริหารจัดการ AI ที่มีความรับผิดชอบ โปร่งใส ปลอดภัย ตรวจสอบได้ และสอดคล้องกับกฎหมาย และระเบียบข้อบังคับของหน่วยงานกำกับที่เกี่ยวข้อง ฝ่ายบริหารจึงเห็นควรให้มีการจัดทำนโยบายด้าน AI เพื่อกำหนดกรอบการใช้เทคโนโลยีดังกล่าวอย่างมีความรับผิดชอบ ภายใต้หลักจรรยาบรรณ ความโปร่งใส และความปลอดภัย

2. วัตถุประสงค์

นโยบายฉบับนี้มีวัตถุประสงค์เพื่อ

- กำหนดเจตนารมณ์ของกลุ่มเอ็กโกต่อการพัฒนา การติดตั้งใช้งาน และการใช้ระบบ AI อย่างมีความรับผิดชอบในทุกกิจกรรมทางธุรกิจ
- จัดให้มีการรอบการบริหารจัดการด้าน AI ที่สอดคล้องกับทิศทางเชิงกลยุทธ์และพันธกิจด้านความยั่งยืนของกลุ่มเอ็กโก
- ทำให้มั่นใจว่าระบบ AI ได้รับการติดตั้งและใช้งานอย่างมีจริยธรรม โปร่งใส ตรวจสอบได้ รับผิดชอบ และสอดคล้องกับข้อกำหนดทางกฎหมายและกฎระเบียบที่ใช้บังคับ
- ส่งเสริมให้ผู้ใช้งานในกลุ่มเอ็กโกและหน่วยงานภายนอกที่เกี่ยวข้องมีวัฒนธรรมการใช้ AI อย่างมีความรับผิดชอบ
- สนับสนุนการบริหารจัดการและปรับปรุงระบบ AI อย่างต่อเนื่อง

3. ขอบเขตการบังคับใช้

นโยบายฉบับนี้ครอบคลุมผู้ใช้งาน ประกอบด้วย คณะกรรมการบริษัท กรรมการผู้จัดการใหญ่ ผู้บริหาร และพนักงานของกลุ่มเอ็กโก ตลอดจนส่งเสริมให้หน่วยงานภายนอกปฏิบัติตามนโยบายฉบับนี้ อีกทั้ง นโยบายฉบับนี้ใช้บังคับกับระบบ AI ทั้งหมดที่กลุ่มเอ็กโก พัฒนา จัดหา ติดตั้งใช้งาน หรือใช้งาน รวมถึงระบบที่ดำเนินการโดยกลุ่มเอ็กโก หรือดำเนินการในนามของกลุ่มเอ็กโก รวมถึงเป็นระบบที่พัฒนาขึ้นเองหรือจากบุคคลที่สาม

4. นิยามหรือคำจำกัดความ

- 1) “กลุ่มเอ็กโก” หมายถึง บริษัท ผลิตไฟฟ้า จำกัด (มหาชน) และบริษัทย่อยที่จดทะเบียนในประเทศไทย
- 2) “ผู้บริหาร” หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างของกลุ่มเอ็กโก

- 3) “พนักงาน” หมายถึง บุคคลที่ได้รับค่าจ้างหรือเงินเดือนทั้งในระดับปฏิบัติการและระดับบริหาร ซึ่งรวมถึง พนักงานทดลองงาน พนักงานประจำ พนักงานสัญญาจ้างพิเศษ ทุกระดับที่อยู่ภายใต้การจ้างงานของกลุ่มเอ็กโก
- 4) “ผู้ใช้งาน” หมายถึง พนักงานของกลุ่มเอ็กโก รวมไปถึงบุคคลภายนอกที่ได้รับอนุญาตให้มีรหัสเข้าใช้งานในบัญชีรายชื่อผู้สามารถเข้าใช้งาน หรือ/และ มีรหัสผ่านเพื่อเข้าใช้งานอุปกรณ์ประมวลผลสารสนเทศของกลุ่มเอ็กโก
- 5) “หน่วยงานภายนอก” หมายถึง บุคคลหรือหน่วยงานภายนอกที่ดำเนินธุรกิจหรือให้บริการที่อาจได้รับสิทธิเข้าถึงสารสนเทศ และอุปกรณ์ประมวลผลสารสนเทศของกลุ่มเอ็กโก เช่น
 - บริษัทคู่ค้า
 - ผู้รับจ้างปฏิบัติงานให้กับกลุ่มเอ็กโก
 - ผู้รับจ้างพัฒนาระบบหรือจัดหาวัสดุอุปกรณ์ต่าง ๆ
 - ผู้ให้บริการต่าง ๆ
 - ที่ปรึกษา
- 6) “ข้อมูลสารสนเทศ” ซึ่งต่อไปนี้จะเรียกว่า “ข้อมูล” หมายถึง ข้อมูล ข่าวสาร บันทึก ประวัติ ข้อความในเอกสาร โปรแกรมคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ รูปภาพ เสียง เครื่องหมาย และสัญลักษณ์ต่าง ๆ ไม่ว่าจะเก็บไว้ในรูปแบบที่สามารถสื่อความหมายให้บุคคลสามารถเข้าใจได้โดยตรง หรือผ่านคอมพิวเตอร์ หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้
- 7) “ระบบปัญญาประดิษฐ์ (Artificial Intelligence: AI System)” หมายถึง ระบบที่ใช้คอมพิวเตอร์หรือเครื่องจักรในการประมวลผลและวิเคราะห์ข้อมูล เพื่อสร้างข้อคาดการณ์ ข้อเสนอแนะ และสนับสนุนการตัดสินใจหรือการสร้างเนื้อหา โดยสามารถดำเนินการได้โดยอัตโนมัติในระดับหนึ่ง เช่น ระบบแชทบอท (Generative AI) การวิเคราะห์ข้อมูลเพื่อการพยากรณ์ (Predictive Analytics) และระบบวิเคราะห์ภาพ (Computer Vision)
- 8) “ระบบบริหารจัดการปัญญาประดิษฐ์ (AI Management System: AIMS)” หมายถึง ระบบหรือแนวทางที่กลุ่มเอ็กโกใช้จัดการเรื่อง AI ทั้งหมด ตั้งแต่การพัฒนา การนำไปใช้ ไปจนถึงการดูแลและปรับปรุง เพื่อให้การใช้ AI เป็นไปอย่างเหมาะสม มีความรับผิดชอบ และสอดคล้องกับนโยบายและเป้าหมายของกลุ่มเอ็กโก
- 9) “นโยบายด้านปัญญาประดิษฐ์ (AI Policy)” หมายถึง ข้อกำหนดทิศทางและการให้การสนับสนุนการบริหารจัดการระบบ AI ของกลุ่มเอ็กโก ซึ่งผู้บริหารสูงสุดได้แสดงไว้อย่างเป็นทางการเกี่ยวกับการพัฒนา การติดตั้งใช้งาน และการใช้ระบบ AI อย่างมีความรับผิดชอบ

- 10) “ปัญญาประดิษฐ์อย่างมีความรับผิดชอบ (Responsible AI)” หมายถึง การออกแบบ พัฒนา ติดตั้งใช้งาน และดำเนินงานระบบ AI ในลักษณะที่มีจริยธรรม โปร่งใส ตรวจสอบรับผิดชอบได้ เป็น ธรรม และสอดคล้องกับข้อกำหนด กฎระเบียบ และความคาดหวังของสังคมที่เกี่ยวข้อง
- 11) “ความเป็นส่วนตัวของข้อมูล (บริบท AI)” หมายถึง การคุ้มครองข้อมูลส่วนบุคคลตลอดวงจร ชีวิตทั้งหมดของระบบ AI ซึ่งรวมถึงการเก็บรวบรวมข้อมูล การฝึกสอนโมเดล การอนุมานผล และการเลิกใช้งานระบบ โดยต้องเป็นไปตามกฎหมายคุ้มครองข้อมูลที่ใช้บังคับ รวมถึง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) ของประเทศไทย
- 12) “ความมั่นคงปลอดภัยไซเบอร์ (บริบท AI)” หมายถึง มาตรการรักษาความมั่นคงปลอดภัยที่ใช้ กับระบบ AI เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต เช่น
 - การแทรกแซงเพื่อบิดเบือนข้อมูลฝึกสอน (Data Poisoning)
 - การขโมยหรือการคัดลอกเลียนแบบโมเดล (Model Stealing)
 - การโจมตีแบบคาดเดาหรือสร้างข้อมูลลับที่ใช้ในการฝึกโมเดล (Model Inversion Attacks)
 - การตรวจสอบและกรองคำสั่ง (Prompt Shielding)
 - ภัยคุกคามเฉพาะด้าน AI เช่น การทดสอบเจาะระบบ การเข้ารหัส การเขียนโค้ด อย่างปลอดภัย
- 13) “อคติ (บริบท AI)” หมายถึง การเลือกปฏิบัติอย่างเป็นระบบและไม่เป็นธรรมในผลลัพธ์ของ AI อันเกิดจากอคติในชุดข้อมูลฝึกสอน การออกแบบโมเดล หรือบริบทการนำไปใช้งาน ซึ่งส่งผลให้ บุคคลหรือกลุ่มบุคคลได้รับการปฏิบัติที่ไม่เหมาะสมหรือไม่เป็นธรรม
- 14) “มนุษย์อยู่ในวงจรการตัดสินใจ (Human-in-the-Loop: HITL)” หมายถึง หลักการกำกับดูแลที่ กำหนดให้มนุษย์ยังคงมีบทบาทในการตรวจสอบ ทบทวน หรืออนุมัติการตัดสินใจที่ได้รับ อิทธิพลจากระบบ AI โดยเฉพาะในกรณีที่มีความสำคัญ มีความเสี่ยงสูง หรือไม่สามารถ ย้อนกลับได้ ทั้งนี้ มนุษย์ต้องมีอำนาจในการแทรกแซง ยกเลิก หรือยกระดับประเด็นได้อย่าง ชัดเจน
- 15) “เนื้อหาที่สร้างโดย AI (AI-Generated Content)” หมายถึง เนื้อหาใด ๆ รวมถึงข้อความ ภาพ วิดีโอ เสียง การตัดสินใจ หรือข้อเสนอแนะ ที่ผลิตโดยระบบ AI ซึ่งต้องมีการระบุให้ชัดเจนว่า เป็นเนื้อหาที่สร้างโดย AI เพื่อให้เกิดความโปร่งใสต่อผู้ใช้และผู้ที่ได้รับผลกระทบ
- 16) “กระบวนการตรวจสอบจากหน่วยงานอิสระ AIMS (Artificial Intelligence Management System External Verification)” หมายถึง การประเมินและการรับรองโดยบุคคลที่สาม เพื่อตรวจสอบความ สอดคล้องตามมาตรฐาน หรือกรอบการบริหารจัดการที่เป็นที่ยอมรับ เช่น การตรวจสอบความ สอดคล้องตามมาตรฐาน ISO/IEC 42001 เพื่อให้เกิดความเชื่อมั่นแก่ผู้มีส่วนได้ส่วนเสีย

5. หน้าที่และความรับผิดชอบ

- 5.1. **คณะกรรมการบริษัท:** รับผิดชอบในการจัดให้มีนโยบายด้าน AI ที่ครอบคลุม และทำให้มั่นใจว่ามีการนำระบบบริหารจัดการ AI ที่มีประสิทธิภาพไปใช้ รวมทั้งอนุมัติการใช้นโยบายฉบับนี้
- 5.2. **คณะกรรมการกำกับดูแลกิจการและความยั่งยืน:** รับผิดชอบในการพิจารณาถ่วงดุลและกำกับดูแลนโยบาย ระเบียบ และแนวปฏิบัติของกลุ่มเอ็กโกที่เกี่ยวข้องการใช้ AI อย่างมีความรับผิดชอบ ในด้านการกำกับดูแล จริยธรรม การปฏิบัติตามกฎหมาย ความยั่งยืน และความมั่นคงปลอดภัยไซเบอร์
- 5.3. **คณะกรรมการกำกับความเสี่ยง:** รับผิดชอบในการกำกับดูแลความเสี่ยงที่เกี่ยวข้องกับ AI ภายใต้กรอบการบริหารความเสี่ยงองค์กร ทบทวนผลการประเมินความเสี่ยงด้าน AI และแผนการจัดการความเสี่ยง และทำให้มั่นใจว่าความเสี่ยงด้าน AI ที่สำคัญได้รับการบริหารจัดการอย่างเหมาะสม
- 5.4. **คณะกรรมการกำกับดูแลการพัฒนาเทคโนโลยีสารสนเทศและการรักษาความมั่นคงปลอดภัยไซเบอร์:** รับผิดชอบในการกำกับดูแลการนำระบบบริหารจัดการ AI ไปใช้ ติดตามการปฏิบัติตามนโยบายฉบับนี้ ทบทวนการประเมินผลกระทบด้าน AI และมาตรการควบคุมด้านความมั่นคงปลอดภัยไซเบอร์
- 5.5. **คณะทำงานโครงการเสริมประสิทธิภาพการทำงานด้วย AI:** รับผิดชอบในการจัดทำนโยบาย ดำเนินการประเมินความเสี่ยงและผลกระทบด้าน AI จัดทำและดูแลบริหารจัดการรายการระบบ AI ดำเนินโครงการฝึกอบรม พัฒนาและดูแลมาตรการควบคุมด้าน AI และขั้นตอนการตอบสนองต่อเหตุการณ์ และรายงานต่อคณะกรรมการกำกับดูแลการพัฒนาเทคโนโลยีสารสนเทศและการรักษาความมั่นคงปลอดภัยไซเบอร์
- 5.6. **พนักงาน:** รับผิดชอบในการปฏิบัติตามนโยบายฉบับนี้และขั้นตอนที่เกี่ยวข้อง เข้ารับการอบรมด้านจริยธรรมและความมั่นคงปลอดภัยของ AI ตามที่กำหนด และรายงานข้อกังวลเกี่ยวกับพฤติกรรมของระบบ AI หรือการไม่ปฏิบัติตามข้อกำหนดผ่านช่องทางที่กำหนด

6. ข้อกำหนด

นโยบายด้าน AI มีรายละเอียดดังต่อไปนี้

1. กำหนดวัตถุประสงค์ด้าน AI ให้สอดคล้องกับกลยุทธ์ทางธุรกิจ ค่านิยม วัฒนธรรม และระดับความเสี่ยงที่ยอมรับได้ของกลุ่มเอ็กโก เพื่อสนับสนุนการพัฒนาและการใช้ AI อย่างมีความรับผิดชอบ และยั่งยืน
2. ปฏิบัติตามข้อกำหนดทางกฎหมาย และแนวปฏิบัติสากลที่เกี่ยวข้อง รวมถึงแนวทางตามมาตรฐาน ISO/IEC 42001

3. พัฒนา และดำเนินงานระบบ AI อย่างมีความรับผิดชอบตลอดวงจรชีวิต ตั้งแต่การออกแบบ การพัฒนา การตรวจยืนยัน การนำไปใช้งาน การติดตาม การตรวจสอบ และการยกเลิกหรือปลดระวางระบบ โดยกำหนดขอบเขต และข้อจำกัดของแต่ละระบบ AI อย่างชัดเจนว่าระบบสามารถดำเนินการใดได้ จัดให้มีการกำกับดูแล ตรวจสอบ โดยมีมนุษย์อยู่ในวงจรการตัดสินใจ และมีกลไกในการตรวจจับและแก้ไขความคลาดเคลื่อนหรือการเสื่อมประสิทธิภาพของโมเดลที่อาจเกิดขึ้นเมื่อเวลาผ่านไป
4. ระบุ และบริหารจัดการความเสี่ยงที่เกิดจากการพัฒนา การนำไปใช้ และการใช้งาน AI รวมถึงความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคล ความมั่นคงปลอดภัยทางไซเบอร์ อคติของ AI ความโปร่งใส ความรับผิดชอบ และผลกระทบด้านสิ่งแวดล้อม โดยดำเนินการให้สอดคล้องตามกรอบการบริหารความเสี่ยงของกลุ่มเอ็กโก
5. ประเมิน และบริหารผลกระทบของระบบ AI ต่อผู้มีส่วนได้เสียที่เกี่ยวข้อง ได้แก่ พนักงาน ลูกค้า ชุมชน และสังคม เพื่อให้มั่นใจว่ากิจกรรมที่เกี่ยวข้องกับ AI ไม่ก่อให้เกิดความเสียหาย และมีช่องทางให้ผู้ที่ได้รับผลกระทบสามารถร้องขอให้มีการทบทวนหรืออุทธรณ์การตัดสินใจที่ขับเคลื่อนด้วย AI
6. กำหนด และคงไว้ซึ่งกระบวนการในการจัดการกรณีไม่เป็นไปตามนโยบายนี้หรือการได้รับยกเว้นจากนโยบาย รวมถึงการกำหนดทรัพยากรที่จำเป็นสำหรับระบบ AI เช่น ข้อมูล เครื่องมือ โครงสร้างพื้นฐาน และขีดความสามารถของบุคลากร พร้อมทั้งจัดให้มีการประเมินผลกระทบของระบบ AI ก่อนนำไปใช้งาน และทบทวนประเมินตามระยะเวลาที่กำหนด
7. ปรับปรุงและพัฒนากระบวนการบริหารจัดการ AI อย่างต่อเนื่อง ผ่านการทบทวนตามแผน การประเมินของฝ่ายบริหาร ผลการตรวจสอบการติดตามผลการดำเนินงานของระบบ AI และการติดตามการเปลี่ยนแปลงด้านกฎหมาย ระเบียบ และแนวปฏิบัติที่เกี่ยวข้อง
8. จัดทำและปฏิบัติตามนโยบายและแนวปฏิบัติของกลุ่มเอ็กโก ตลอดจนทบทวนและตรวจสอบตามระยะเวลาที่กำหนด
9. สื่อสาร และจัดให้มีการฝึกอบรมให้แก่ผู้ใช้งานที่เกี่ยวข้องเกี่ยวกับการใช้ AI อย่างมีความรับผิดชอบ ประเด็นจริยธรรม การคุ้มครองข้อมูลส่วนบุคคล และความมั่นคงปลอดภัยของระบบ AI พร้อมทั้งเผยแพร่นโยบายฉบับนี้ให้ผู้มีส่วนได้เสียทุกกลุ่มสามารถเข้าถึงและรับทราบได้

7. ระยะเวลาการทบทวน

กลุ่มเอ็กโกจัดให้มีการปรับปรุงและทบทวนนโยบายการใช้ AI อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ เพื่อให้การกำกับดูแล AI กำหนดขอบเขตการนำไปใช้งานและความรับผิดชอบที่เกี่ยวข้องยังคงมีความถูกต้องเหมาะสมและสอดคล้องกับการเปลี่ยนแปลงตามความต้องการทางธุรกิจของกลุ่มเอ็กโก

ทั้งนี้ ให้มีผลตั้งแต่วันที่ 26 มิถุนายน 2569 เป็นต้นไป

ประกาศ ณ วันที่ 26 มิถุนายน 2569



(นายประเสริฐ สินสุขประเสริฐ)

ประธานกรรมการ

บริษัท ผลิตไฟฟ้า จำกัด (มหาชน)



บริษัท ผลิตไฟฟ้า จำกัด (มหาชน)

แนวปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยี
สารสนเทศสำหรับผู้ใช้งาน

1. การใช้งานปัญญาประดิษฐ์ (Artificial Intelligence - AI)

เพื่อเป็นแนวทางการใช้งานปัญญาประดิษฐ์สาธารณะ (Public AI) และปัญญาประดิษฐ์สำหรับองค์กร (Corporate AI) อย่างมีความรับผิดชอบและเป็นไปตามกฎหมาย โดยคำนึงถึงผลกระทบที่อาจเกิดขึ้นต่อบุคคลอื่น สังคม บริษัท และกฎหมาย

■ หลักการสำคัญการใช้งาน ดังนี้

- 1) ควรใช้งานในทางสร้างสรรค์สิ่งที่ดีและผลงานที่เป็นประโยชน์ และไม่ขัดต่อกฎหมาย
- 2) ความปลอดภัยในการใช้งานต้องไม่ก่อให้เกิดอันตรายหรือความเสียหายต่อบุคคลหรือทรัพย์สินหรือบริษัท
- 3) ต้องมีการตรวจสอบความถูกต้องของข้อมูลที่สร้างขึ้นก่อนนำไปใช้งาน
- 4) การใช้งานต้องเคารพสิทธิในความเป็นส่วนตัวของบุคคลอื่น ไม่นำข้อมูลมาใช้ในทางที่ไม่เหมาะสม
- 5) ความรับผิดชอบต่อการนำข้อมูลไปใช้งานต้องอย่างถูกต้องและเหมาะสม

1.1 แนวทางการใช้เทคโนโลยีระบบปัญญาประดิษฐ์ที่ยอมรับได้

1.1.1 การใช้งานที่ยอมรับได้ ผู้ใช้งานต้องประยุกต์ใช้เทคโนโลยีระบบปัญญาประดิษฐ์เพื่อช่วยสนับสนุนการดำเนินงานในบริบทที่กำหนด ดังต่อไปนี้

- 1) การวิเคราะห์ข้อมูล การคาดการณ์แนวโน้ม และการสร้างรายงาน
- 2) การเขียนและทวนสอบชุดคำสั่งหรือโปรแกรม
- 3) การจัดทำร่างหนังสือหรือเอกสารร่าง ๆ
- 4) การให้คำแนะนำหรือเป็นผู้ช่วยในการแก้ปัญหาเบื้องต้น
- 5) การสนับสนุนงานวิจัยและวิชาการ เช่น การช่วยทบทวนบทความ วรรณกรรม เป็นต้น
- 6) การสร้างเนื้อหาเพื่อการสื่อสารและการประชาสัมพันธ์
- 7) ดำเนินงานอื่น ๆ ที่ได้รับมอบหมายจากผู้บังคับบัญชา

1.1.2 ข้อห้ามในการใช้งาน

- 1) ห้ามใช้ปัญญาประดิษฐ์ในการตัดสินใจที่สำคัญ (High-Stakes Decisions) เช่น การอนุมัติ การพิจารณาด้านวินัย เป็นต้น โดยปราศจากการตรวจสอบและอนุมัติโดยมนุษย์
- 2) ห้ามป้อนข้อมูลที่ไม่ได้รับการตรวจสอบความถูกต้อง หรือข้อมูลที่อาจบิดเบือนการทำงานของโมเดล (Data Poisoning) เข้าสู่ระบบปัญญาประดิษฐ์
- 3) ห้ามใช้ระบบปัญญาประดิษฐ์ในทางที่ผิด (Misuse) หรือจงใจใช้เป็นเครื่องมือเพื่อสร้างการโจมตีทางไซเบอร์โดยไม่ได้รับอนุญาตเด็ดขาด ซึ่งรวมถึงแต่ไม่จำกัดเพียงการใช้ AI เพื่อค้นหาช่องโหว่ในระบบอื่น การสร้างโค้ดสำหรับมัลแวร์ การสร้างสื่อสังเคราะห์ปลอม (Deepfake) เพื่อใช้ในการหลอกลวงหรือเขียนข้อความฟิชชิ่ง (Phishing) ที่มีความแม่นยำสูง
- 4) ห้ามนำข้อมูลของบริษัท หรือข้อมูลส่วนบุคคลเข้าสู่ Public AI เช่น การป้อนข้อมูลบริษัท หรือข้อมูลส่วนบุคคลเพื่อสอบถามและป้องกันการรั่วไหลของข้อมูลที่สำคัญ
- 5) ห้ามใช้เพื่อสร้างเนื้อหาที่ผิดกฎหมาย ละเมิดศีลธรรม หรืออาจสร้างความเสียหายต่อบุคคล องค์กรและสังคม
- 6) ห้ามสร้างเนื้อหาที่เป็นอันตราย เช่น เผยแพร่เนื้อหาที่เกี่ยวข้องกับความรุนแรง การก่อการร้าย การลวงละเมิดทางเพศ การเหยียดเชื้อชาติ การเกลียดชัง หรือการกระทำผิดกฎหมาย
- 7) ห้ามใช้เพื่อสร้างเนื้อหาที่ละเมิดลิขสิทธิ์หรือทรัพย์สินทางปัญญาของผู้อื่น

- 8) ไม่ควรเปิดเผยข้อมูลส่วนบุคคลโดยไม่จำเป็น เช่น การแสดกนใบหน้า ภาพถ่าย วิดีโอ การบันทึกเสียง หากมีติดต่อกับ หรือการแอบอ้างจากบุคคล หรือหน่วยงานที่น่าเชื่อถือ ควรมีการตรวจสอบความถูกต้องของแหล่งต้นทางให้แน่ชัดเสียก่อน เพื่อป้องกันการนำข้อมูลส่วนบุคคลไปใช้ในประโยชน์ในทางที่ไม่ถูกต้อง เช่น การสร้างข้อมูลปลอมด้วยปัญญาประดิษฐ์ที่สมจริง เพื่อหลอกลวง หรืออาจทำให้เข้าใจผิดและบิดเบือนข้อมูลได้ จนอาจนำไปสู่การทำผิดกฎหมายได้

1.1.3 การรักษาความลับและคุ้มครองข้อมูลส่วนบุคคล

- 1) ห้ามนำข้อมูลภายในเอ็กโก กรุ๊ป และข้อมูลที่มีชั้นความลับ เช่น รหัสผ่าน เอกสารสัญญา ข้อมูลโครงการ ไปใช้ร่วมกับ Public AI
- 2) ข้อมูลของบริษัทให้ใช้ Corporate AI ในการใช้งาน เนื่องจาก Corporate AI มีข้อกำหนดด้านการป้องกันข้อมูลของบริษัทและการเข้ารหัส และจะไม่นำข้อมูลไปใช้ในการฝึกอบรมโมเดลพื้นฐานใน Public AI

1.1.4 การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

- 1) ต้องตรวจสอบซอร์สโค้ดหรือชุดคำสั่งที่สร้างโดยปัญญาประดิษฐ์ ก่อนนำมาใช้งานจริงเสมอ เพื่อหาช่องโหว่และข้อผิดพลาด
- 2) หากพบพฤติกรรมของปัญญาประดิษฐ์ ที่ผิดปกติ น่าสงสัย หรืออาจเป็นช่องโหว่ด้านความมั่นคงปลอดภัย ต้องแจ้งผู้บังคับบัญชาหรือฝ่ายโครงสร้างพื้นฐานและความมั่นคงปลอดภัยระบบสารสนเทศ (ผคม.) ทันที

1.1.5 การตรวจสอบผลลัพธ์และลดอคติ

- 1) ผู้ใช้งานต้องตรวจสอบเนื้อหาและผลลัพธ์ที่สร้างหรือวิเคราะห์โดยปัญญาประดิษฐ์ก่อนนำไปใช้งานหรือเผยแพร่เสมอ เพื่อลดหรือหลีกเลี่ยงการเกิดอคติหรือการเลือกปฏิบัติอย่างไม่เป็นธรรม
- 2) ต้องใช้ความระมัดระวังในการใช้ปัญญาประดิษฐ์ที่เกี่ยวข้องกับการประเมินหรือการตัดสินใจเกี่ยวกับบุคคลเพื่อไม่ให้เกิดผลกระทบต่อสิทธิและความเสมอภาค

1.1.6 หน้าที่และความรับผิดชอบ

- 1) ผู้ใช้งานมีหน้าที่และความรับผิดชอบต่อการตัดสินใจขั้นสุดท้ายที่เกิดขึ้นจากการใช้ข้อมูล คำแนะนำหรือผลลัพธ์จากระบบปัญญาประดิษฐ์
- 2) ผู้ใช้งานต้องตรวจสอบผลลัพธ์จากปัญญาประดิษฐ์ก่อนนำไปใช้งานหรือเผยแพร่เสมอ เนื่องจากสามารถทำให้เกิดอคติหรือความไม่ถูกต้องของข้อมูลได้ โดยต้องพิจารณาถึงความถูกต้อง ผลกระทบทางกฎหมาย ความเท่าเทียม และความมั่นคงปลอดภัยสารสนเทศ
- 3) ผู้ใช้งานต้องรายงานให้ผู้บังคับบัญชาทราบทันที หากพบว่าระบบปัญญาประดิษฐ์ทำงานผิดพลาด ให้ผลลัพธ์ที่มีอคติ หรืออาจส่งผลกระทบเชิงลบ
- 4) การนำเนื้อหาที่ได้รับความช่วยเหลือจากปัญญาประดิษฐ์มาใช้งานต้องมีการระบุที่มาตามความเหมาะสมเพื่อความโปร่งใส
- 5) ตระหนักถึงขีดจำกัดและข้อจำกัดในการใช้งานที่ยังไม่สามารถคิดและตอบสนองได้เหมือนมนุษย์ อีกทั้งอาจยังมีความคลาดเคลื่อนของข้อมูลได้

- 6) สามารถใช้เป็นเครื่องมือในการช่วยทำงานได้ แต่ไม่ควรพึ่งพาข้อมูลทั้งหมด ควรตรวจสอบและแก้ไขข้อมูลทุกครั้ง