



คปท.

สำนักงานคณะกรรมการกำกับและส่งเสริม
การประกอบธุรกิจประกันภัย(คปท.)

แนวปฏิบัติ

เรื่อง การกำกับดูแลการใช้งานปัญญาประดิษฐ์

สำหรับบริษัทประกันภัย

(AI Governance Guideline)

การใช้งานเทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence: AI) ในธุรกิจประกันภัย ปัจจุบันมีแนวโน้มการนำมาใช้ในรูปแบบที่หลากหลาย ซับซ้อน และเพิ่มขึ้นอย่างต่อเนื่อง ทั้งเพิ่มประสิทธิภาพการดำเนินงาน การให้บริการลูกค้า และการวิเคราะห์ข้อมูลเชิงลึก อย่างไรก็ตาม การใช้งาน AI นำมาซึ่งความเสี่ยงรูปแบบใหม่ที่อาจส่งผลกระทบต่อการทำงานของบริษัท ผู้เอาประกันภัย ประชาชน และผู้มีส่วนได้ส่วนเสีย เช่น ความเสี่ยงด้านจริยธรรม การละเมิดความเป็นส่วนตัว ความน่าเชื่อถือของผลลัพธ์จาก AI ความเสี่ยงเชิงกฎหมาย ความเสี่ยงด้านเทคโนโลยีสารสนเทศ และภัยคุกคามทางไซเบอร์ เป็นต้น

สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (คปภ.) ส่งเสริมและสนับสนุนการใช้นวัตกรรมและเทคโนโลยี ควบคู่กับการให้ความสำคัญกับการคุ้มครองผู้บริโภค (Consumer Protection) และความมั่นคงทางการเงินของบริษัทประกันภัย (Prudential Soundness) จึงได้จัดทำแนวปฏิบัติฉบับนี้ เพื่อเป็นแนวทางการบริหารจัดการความเสี่ยงใหม่จากการใช้ปัญญาประดิษฐ์ (Artificial Intelligence: AI) เพิ่มเติมจากประกาศและแนวปฏิบัติที่เกี่ยวข้องที่บังคับใช้ในปัจจุบัน ครอบคลุมหลักการที่มุ่งเน้นให้บริษัทใช้งาน AI อย่างมีความรับผิดชอบ เป็นธรรม และไม่เป็นอุปสรรคในการเข้าถึงการประกันภัยของประชาชน อย่างไรก็ตาม แนวทางการบริหารจัดการความเสี่ยงฉบับนี้ ยึดหลักการกำกับดูแลตามระดับความเสี่ยง (Risk-Based Proportionality) สอดคล้องกับลักษณะการดำเนินธุรกิจ ความซับซ้อนของเทคโนโลยีที่นำมาใช้ ครอบคลุมกิจกรรมและกระบวนการดำเนินงานที่มีนัยสำคัญของบริษัท โดยเฉพาะการนำ AI ไปใช้กับงานที่ปฏิสัมพันธ์กับลูกค้าและประชาชน หรืองานที่มีความเสี่ยงสูง

แนวปฏิบัติ เรื่อง การกำกับดูแลการใช้งานปัญญาประดิษฐ์ สำหรับบริษัทประกันภัย (AI Governance Guideline) จะเชื่อมโยงกับประกาศหรือแนวปฏิบัติที่เกี่ยวข้อง โดยสาระสำคัญของแนวปฏิบัติฉบับนี้ครอบคลุม ๔ ส่วน ได้แก่ ส่วนที่ ๑ : การกำกับดูแลการใช้งาน AI (AI Governance) ส่วนที่ ๒ : ความทนทานและการรักษาความมั่นคงปลอดภัยระบบ AI (Robustness and AI Security) ส่วนที่ ๓ : ความโปร่งใสและความสามารถในการอธิบาย (Transparency and Explainability) และ ส่วนที่ ๔ : ความเป็นธรรมและการคุ้มครองผู้บริโภค (Fairness and Consumer Protection)

นิยามคำศัพท์	
ปัญญาประดิษฐ์ (Artificial Intelligence: AI)	เทคโนโลยีที่ถูกพัฒนาขึ้นเพื่อให้คอมพิวเตอร์มีคุณสมบัติหรือพฤติกรรมใกล้เคียงมนุษย์ ตามวัตถุประสงค์ที่มนุษย์กำหนด เช่น การเรียนรู้ การรับรู้และตอบสนองต่อสภาพแวดล้อม การเข้าใจภาษา การให้เหตุผล และการแก้ไขปัญหา เป็นต้น โดยครอบคลุมระบบที่มี Machine Learning (ML) หรือ Deep Learning (DL) หรือ Generative AI (Gen AI)
Machine Learning: ML	เทคโนโลยีปัญญาประดิษฐ์ ประเภทหนึ่งที่มีความสามารถในการเรียนรู้ หรือปรับปรุงประสิทธิภาพการทำงานของตน โดยพัฒนาและใช้อัลกอริทึมในการวิเคราะห์ และเรียนรู้จากข้อมูลที่ได้รับจากการฝึกสอน หรือสภาพแวดล้อม
Deep learning: DL	Machine Learning ประเภทหนึ่งที่ออกแบบการทำงานเลียนแบบสมองมนุษย์ หรือการเรียนรู้เชิงลึกที่ใช้โครงข่ายประสาทเทียมหลายชั้น (Deep Neural Networks) เพื่อวิเคราะห์และเรียนรู้จากข้อมูลจำนวนมาก เพื่อให้คอมพิวเตอร์สามารถทำงานที่ซับซ้อนได้
Generative AI: Gen AI	เทคโนโลยีปัญญาประดิษฐ์ ประเภทหนึ่งที่ฝึกละเอียดเรียนรู้จากโครงข่ายประสาท (Neural Network) หลายชุด เพื่อเข้าใจและสร้างข้อความ ภาพ เสียง และวิดีโอ คล้ายมนุษย์ เช่น Large Language Model (LLM) เป็นต้น
โมเดล/ โมเดลปัญญาประดิษฐ์ (Model AI)	โปรแกรม หรือเงื่อนไข ที่ถูกสร้างขึ้นจากอัลกอริทึมและข้อมูลที่ฝึกสอนโดยมนุษย์ นำไปประมวลผลข้อมูลเพื่อให้คอมพิวเตอร์มีคุณสมบัติ หรือพฤติกรรมใกล้เคียงมนุษย์
การใช้งาน AI ที่มีความเสี่ยงสูง	การประยุกต์ใช้ AI ในกระบวนการที่มีนัยสำคัญต่อความมั่นคงปลอดภัย ด้านเทคโนโลยีสารสนเทศและไซเบอร์ของบริษัท ซึ่งรวมถึงการใช้ AI กับข้อมูลส่วนบุคคล ตลอดจนการปฏิสัมพันธ์กับลูกค้า เช่น การพิจารณารับประกันภัย การกำหนดเบี้ยประกันภัย การจัดการค่าสินไหมทดแทนและผลประโยชน์ตามกรมธรรม์ เป็นต้น
หลักจริยธรรมในการใช้งาน AI (AI Ethics)	หลักจริยธรรมในการใช้งาน AI (AI Ethics) เพื่อเป็นแนวทางในการนำ AI มาประยุกต์ใช้ในการดำเนินธุรกิจ ได้แก่ ความรับผิดชอบ (Accountability) ความเป็นธรรม (Fairness) ความโปร่งใสและความสามารถในการอธิบาย (Transparency and Explainability)
หน่วยงานควบคุม (Control Function)	แนวปฏิบัติฉบับนี้หมายความว่าหมายถึงหน่วยงานที่ทำหน้าที่ต่อไปนี้ ๑. งานบริหารความเสี่ยง (Risk Management Function) ๒. งานดูแลการปฏิบัติตามกฎหมาย (Compliance Function) ๓. งานคณิตศาสตร์ประกันภัย (Actuarial Function) ๔. งานตรวจสอบภายใน (Internal Audit Function)

ภาพรวมของแนวปฏิบัติ เรื่อง การกำกับดูแลการใช้งานปัญญาประดิษฐ์ สำหรับบริษัทประกันภัย
(AI Governance Guideline)

การกำกับดูแลตามระดับความเสี่ยง (Risk-Based Proportionality)

การกำกับดูแลการใช้งาน AI (AI Governance)	ความทนทานและการรักษาความมั่นคงปลอดภัยระบบ AI (Robustness and AI Security)	ความโปร่งใสและความสามารถในการอธิบาย (Transparency and Explainability)	ความเป็นธรรมและการคุ้มครองผู้บริโภค (Fairness and Consumer Protection)
- บทบาทหน้าที่คณะกรรมการบริษัท - บทบาทหน้าที่ผู้บริหาร - การบริหารความเสี่ยงการใช้งาน AI - การกำกับดูแลการใช้บริการ AI จากบุคคลภายนอกด้านเทคโนโลยีสารสนเทศ	- การประเมินประสิทธิภาพการทำงานของระบบ AI - การรักษาความมั่นคงปลอดภัยระบบ AI	การอธิบายผลลัพธ์จากระบบ AI	- การบริหารจัดการข้อมูล - การบริหารจัดการอคติของโมเดล - การติดตามและตรวจสอบผลลัพธ์ของระบบ AI - การคุ้มครองผู้บริโภค

ประกาศ / แนวปฏิบัติที่เกี่ยวข้อง

ส่วนที่ ๑ : การกำกับดูแลการใช้งาน AI (AI Governance)

การกำกับดูแลการใช้งาน AI โดยคณะกรรมการบริษัทและผู้บริหาร มีบทบาทหน้าที่และความรับผิดชอบในการกำกับดูแลการใช้งาน AI ยึดหลักจริยธรรมการใช้งาน AI และการคุ้มครองผู้บริโภค รวมทั้งดูแลให้มีการบริหารจัดการและควบคุมความเสี่ยง เพื่อให้มั่นใจว่าระบบ AI สามารถให้ผลลัพธ์ที่ถูกต้อง

๑.๑ บทบาทหน้าที่คณะกรรมการบริษัท

บทบาทหน้าที่คณะกรรมการบริษัทต้องให้ความสำคัญในการกำกับดูแลการใช้งาน AI อย่างมีความรับผิดชอบ และเข้าใจความเสี่ยงที่อาจเกิดขึ้นจากการใช้งาน AI โดยคำนึงถึงหลักจริยธรรมในการใช้งาน ครอบคลุมเรื่อง ความเป็นธรรม ความโปร่งใส การอธิบายได้ และบริหารจัดการความเสี่ยงที่เกิดจากการใช้งาน AI โดยสามารถมอบหมายหน้าที่กำกับดูแลให้แก่คณะกรรมการชุดย่อย ดำเนินการแทนได้ ในเรื่องดังต่อไปนี้

๑.๑.๑ จัดให้มีนโยบายกำกับดูแลการใช้งาน AI และการบริหารจัดการความเสี่ยง สอดคล้องตามกรอบการบริหารความเสี่ยงแบบองค์กรรวม (Enterprise Risk Management: ERM)

๑.๑.๒ ดูแลให้มีการกำหนดหน้าที่ ความรับผิดชอบในการกำกับและบริหารความเสี่ยง ตลอดจนวงจรชีวิตการใช้งานและพัฒนา AI ตามหลักการการกำกับดูแลการปฏิบัติงานแบบ 3 Lines of Defense (LoD)

๑.๒ บทบาทหน้าที่ผู้บริหาร

บทบาทหน้าที่ผู้บริหารในการวางแนวทางเกี่ยวกับการใช้งาน AI ภายในบริษัท ครอบคลุมในเรื่องดังต่อไปนี้

๑.๒.๑ กำหนดกระบวนการหรือแนวปฏิบัติการใช้งาน AI ภายในบริษัทครอบคลุมการใช้งาน AI ทุกรูปแบบ ตั้งแต่ การออกแบบพัฒนาระบบ หรือการเลือกใช้บริการจากบุคคลภายนอกด้านเทคโนโลยีสารสนเทศ การทดสอบ การบริหารจัดการข้อมูล การประเมินความเสี่ยง ขั้นตอนการอนุมัติการประยุกต์ใช้ AI ตลอดจนการ

ติดตามผลลัพธ์ จากการใช้งาน AI และความเสี่ยงที่อาจเกิดขึ้นโดยให้สอดคล้องกับนโยบายกำกับดูแลการใช้งาน AI และการบริหารจัดการความเสี่ยงของบริษัท

กรณีการใช้งาน AI ที่ไม่สามารถอธิบายกระบวนการตัดสินใจหรือเหตุผลของผลลัพธ์ได้อย่างชัดเจน เช่น ระบบที่มีความซับซ้อนสูงหรือมีข้อจำกัดด้านความโปร่งใส บริษัทควรประเมินระดับความเสี่ยงจากข้อจำกัดดังกล่าว เพื่อใช้ประกอบการกำหนดกระบวนการควบคุมและแนวปฏิบัติในการใช้งาน AI ให้เหมาะสมกับลักษณะและความสำคัญของระบบ

๑.๒.๒ ส่งเสริมความรู้ความเข้าใจเกี่ยวกับหลักจริยธรรม และความเสี่ยงในการใช้งาน AI ให้แก่บุคลากรทุกระดับ ทั้งนี้ สำหรับผู้ปฏิบัติงานในหน่วยงานควบคุม (Control Function) ควรอบรมให้ความรู้ เพื่อสามารถปฏิบัติหน้าที่ได้สอดคล้องตามบทบาทความรับผิดชอบ

๑.๓ การบริหารจัดการความเสี่ยงการใช้งาน AI

ครอบคลุมในเรื่องดังต่อไปนี้

๑.๓.๑ การประเมินความเสี่ยงตามลักษณะการใช้งาน AI^๑ และผลกระทบเชิงลบที่อาจเกิดขึ้น โดยเฉพาะที่มีความเสี่ยงทางด้านพฤติกรรมทางการตลาด (Market Conduct) และความเสี่ยงด้านความมั่นคงทางการเงิน (Prudential Risk) สอดคล้องกับการกำกับดูแลตามระดับความเสี่ยง (Risk-Based Proportionality) ทั้งนี้ บริษัทควรพิจารณาความเสี่ยงที่มีโอกาสเกิดขึ้นจากการใช้งาน AI เช่น

- การปกป้องข้อมูลและการรักษาความมั่นคงปลอดภัย (Data Protection and Security) เมื่อระบบ AI มีการประมวลผลข้อมูลสำคัญ เช่น ข้อมูลส่วนบุคคล ข้อมูลทางการเงิน เป็นต้น ควรมีการป้องกันความปลอดภัย ตามระดับความเสี่ยงอย่างเหมาะสม

- ผลลัพธ์ที่มีอคติ (Bias Outcome) เกิดจากข้อมูลที่ใช้ฝึกสอนมีอคติ เช่น เชื้อชาติ เผ่าพันธุ์ ข้อมูลในอดีตที่มีอคติที่กำหนดความเสี่ยงปัจจุบัน เป็นต้น รวมถึงการออกแบบโมเดลอาจจะส่งผลให้เกิดความไม่เป็นธรรม^๒

- ความเสี่ยงของโมเดลและการอธิบายผลลัพธ์ของโมเดล (Model Risk/ Explainability) เกิดจากโมเดลไม่สามารถปรับตัวต่อการเปลี่ยนแปลงของข้อมูล หรือการใช้ระบบ AI ที่มีความซับซ้อนสูง ส่งผลกระทบต่อความเข้าใจของผู้ใช้งาน และความสามารถในการอธิบายการประมวลผล ทำให้ผลลัพธ์ขาดความน่าเชื่อถือ

- การไม่สามารถเข้าถึงการประกันภัย (Uninsurability) เมื่อนำมาใช้กับการพิจารณารับประกันภัย การกำหนดเบี้ยประกันภัย ผลลัพธ์ของโมเดลอาจทำให้ความเสี่ยงของคนบางกลุ่มสูงเกินจริง ส่งผลให้ไม่สามารถเข้าถึงการประกันภัย

- การปรับแต่งอัตรากำไรส่วนบุคคล (Personalising Profit Margins) จากการนำระบบ AI มาประมวลผลข้อมูลพฤติกรรมลูกค้า โดยไม่ได้พิจารณาตามหลักคณิตศาสตร์ประกันภัย ส่งผลให้ผู้เอาประกันภัยจ่ายเบี้ยประกันภัยสูงเกินความเสี่ยงที่แท้จริง

^๑ ตัวอย่างความเสี่ยงที่เกี่ยวข้องกับการใช้งาน AI ในภาคประกันภัย มาตรการควบคุมความเสี่ยง และตัวอย่างหัวข้อการรายงานความเสี่ยงจากการใช้งาน AI ปรากฏในภาคผนวก ก.

^๒ ผลลัพธ์ที่มีอคติจากข้อมูลฝึกหรือการออกแบบโมเดล อาจก่อให้เกิดความไม่เป็นธรรมและความเสี่ยงด้านจริยธรรม (Ethical Risk) ที่ต้องได้รับการประเมินและควบคุมตามหลักจริยธรรมในการใช้งาน AI

- การละเมิดทรัพย์สินทางปัญญา (Intellectual Property Infringement) ข้อมูลที่ระบบ AI นำมาใช้ อาจมีการละเมิดทรัพย์สินทางปัญญานำไปสู่การละเมิดทางกฎหมายได้

- การรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) ระบบ AI มีความเสี่ยงต่อการโจมตีทางไซเบอร์ ซึ่งอาจส่งผลกระทบต่อความการรักษาความลับ ความถูกต้อง และความพร้อมใช้ของระบบ AI เช่น การโจมตีแบบ Data Poisoning การคัดลอกโมเดลโดยไม่ได้รับอนุญาต (Model Extraction) เป็นต้น

- การกระจุกตัวของความเสี่ยง (Concentration Risk) เกิดจากบริษัทประกันภัยใช้บริการจากผู้ให้บริการรายใดรายหนึ่งมากเกินไป หากผู้ให้บริการถูกโจมตีทางไซเบอร์ หรือไม่สามารถให้บริการได้ อาจกระทบการดำเนินงานหรือความมั่นคงปลอดภัยไซเบอร์ของบริษัทประกันภัย

ในกรณีที่นำระบบ AI มาใช้ในงานที่มีความเสี่ยงสูง เช่น การพิจารณาประกันภัย การกำหนดเบี้ยประกันภัย การจัดการค่าสินไหมทดแทนและผลประโยชน์ตามกรมธรรม์ เป็นต้น บริษัทควรพิจารณาให้มนุษย์มีส่วนร่วมในการตัดสินใจหรือดำเนินการ (Human in the loop^๓ / Human over the loop^๔) เพื่อป้องกันการปฏิบัติอย่างไม่เป็นธรรมหรือไม่เหมาะสมต่อลูกค้าหรือประชาชน การเลือกปฏิบัติที่ไม่เหมาะสม ไม่ถูกต้องตามกฎหมาย (Unlawful Discrimination) ส่งผลให้ประชาชนบางกลุ่มเข้าไม่ถึงการประกันภัยอย่างเป็นธรรม

๑.๓.๒ ผู้บริหารควรจัดให้มีการรายงานผลการบริหารความเสี่ยง ต่อคณะกรรมการบริหารความเสี่ยง และคณะกรรมการบริษัท อย่างน้อยปีละ ๑ ครั้ง โดยเฉพาะการใช้งาน AI ที่มีความเสี่ยงสูง เพื่อให้ทราบถึงสถานะความเสี่ยง รวมทั้งประสิทธิภาพของมาตรการควบคุมที่ดำเนินการ เพื่อการทบทวนปรับปรุงให้เหมาะสม

๑.๔ การกำกับดูแลการใช้บริการ AI จากบุคคลภายนอกด้านเทคโนโลยีสารสนเทศ

ครอบคลุมในเรื่องดังต่อไปนี้

๑.๔.๑ บริษัทควรมีมาตรการควบคุมและติดตามการใช้งาน AI จากการใช้บริการจากบุคคลภายนอกด้านเทคโนโลยีสารสนเทศ ตามการกำกับดูแลและบริหารจัดการความเสี่ยงจากบุคคลภายนอกด้านเทคโนโลยีสารสนเทศที่สำนักงาน คปภ. กำหนด และดำเนินการเพิ่มเติมในเรื่องดังต่อไปนี้

กรณีบริษัทประกันภัยเลือกใช้บริการจากบุคคลภายนอกด้านเทคโนโลยีสารสนเทศ เช่น Generative AI บริษัทสามารถพิจารณามาตรการควบคุมตามความเหมาะสม และควรกำหนดขอบเขตการใช้งานภายในบริษัท และข้อกำหนดเกี่ยวกับสิ่งที่ควรและไม่ควรปฏิบัติในการใช้งาน AI ของบริษัท

กรณีจ้างผู้ให้บริการภายนอกพัฒนาระบบ AI บริษัทควรประเมินความเสี่ยงและข้อจำกัดจากการใช้งานระบบ AI และข้อมูลของบุคคลภายนอก ตลอดจนการพิจารณาข้อกำหนดในสัญญาผู้ให้บริการ เช่น การพัฒนาระบบ AI บนหลักจริยธรรม ความโปร่งใสของโมเดล แหล่งข้อมูลที่ใช้ฝึกสอนโมเดล สิทธิในการตรวจสอบข้อกำหนดการให้บริการ และกระบวนการในการปรับปรุงโมเดล เป็นต้น

^๓ Human in the loop: ระดับการมีส่วนร่วมที่มนุษย์ควบคุมการทำงานหรือตัดสินใจทั้งหมด โดยมี AI ทำหน้าที่ในการให้คำแนะนำหรือข้อมูล แต่ไม่สามารถทำงานหรือตัดสินใจในการดำเนินการใดๆ ได้โดยปราศจากมนุษย์ อ้างอิง ETDA: แนวทางการประยุกต์ใช้ปัญญาประดิษฐ์อย่างมีธรรมาภิบาล

^๔ Human over the loop: ระดับการมีส่วนร่วมที่ AI สามารถทำงานหรือตัดสินใจได้โดยอัตโนมัติ แต่ยังจำเป็นต้องมีมนุษย์ในการกำกับดูแล อีกทั้งมนุษย์สามารถเข้าควบคุมหรือระงับการทำงานได้ อ้างอิง ETDA: แนวทางการประยุกต์ใช้ปัญญาประดิษฐ์อย่างมีธรรมาภิบาล

๑.๔.๒ ประเมินระดับการพึ่งพาผู้ให้บริการ AI จากผู้ให้บริการภายนอกอย่างสม่ำเสมอ โดยคำนึงถึงความเสี่ยงด้านปฏิบัติการ (Operational Risk) และความเสี่ยงด้านการกระจุกตัว (Concentration Risk) ของผู้ให้บริการ AI ซึ่งอาจส่งผลกระทบต่อธุรกิจเกิดการหยุดชะงัก

๑.๔.๓ กำหนดมาตรการควบคุมความเสี่ยงเพิ่มเติม ตามลักษณะการใช้งานและความเสี่ยงของระบบ เช่น การพิจารณาความจำเป็นของระบบสำรอง การกำกับดูแลการใช้ข้อมูลของระบบ AI การติดตั้งกลไก คำสั่ง หรือ กระบวนการที่สามารถปิดหรือหยุดการทำงานของระบบ AI ได้ทันที (Kill Switch) เพื่อหยุดการทำงานของระบบภายใต้เงื่อนไขที่กำหนด การจัดทำและทดสอบแผนฉุกเฉิน (Contingency Plan) รวมถึงการเปลี่ยนไปใช้ระบบอื่นตามความจำเป็น และการจัดทำแผนการสิ้นสุดการใช้บริการ (Exit Plan)

ส่วนที่ ๒ : ความทนทานและการรักษาความมั่นคงปลอดภัยระบบ AI (Robustness and AI Security)

ระบบ AI มีความสามารถในการเรียนรู้และปรับตัวจากข้อมูลได้อย่างต่อเนื่อง บริษัทจึงควรมีมาตรการกำกับดูแลเพื่อให้ระบบสามารถทำงานได้ถูกต้องตามวัตถุประสงค์ และการรักษาความมั่นคงปลอดภัยของระบบ AI ควรมีแนวทางการควบคุมความเสี่ยงในเรื่องดังต่อไปนี้

๒.๑ การประเมินประสิทธิภาพการทำงานของระบบ AI

บริษัทควรประเมินประสิทธิภาพในการทำงานของระบบ AI อย่างสม่ำเสมอ โดยคำนึงถึงวัตถุประสงค์การใช้งาน วิเคราะห์ความถูกต้องของโมเดลและข้อมูล เช่น การวิเคราะห์ความไวของโมเดลต่อการเปลี่ยนแปลงของข้อมูล (Sensitivity Analysis) การทดสอบความสามารถของโมเดลในการรับมือกับข้อมูลที่ผิดปกติ (Adversarial Testing) และการเปลี่ยนแปลงแนวคิดของโมเดล (Concept Drift) เป็นต้น

ทั้งนี้ กรณีที่เป็นการใช้งาน AI ที่มีความเสี่ยงสูง หรือส่งผลกระทบต่อผู้เอาประกันภัย บริษัทควรทดสอบประสิทธิภาพของระบบ AI ให้สอดคล้องกับระดับความเสี่ยงและผลกระทบที่อาจเกิดขึ้น และแจ้งผลการทดสอบไปยังผู้พัฒนาระบบและผู้เกี่ยวข้องเพื่อดำเนินการแก้ไข

๒.๒ การรักษาความมั่นคงปลอดภัยระบบ AI

บริษัทควรมีแนวทางการรักษาความมั่นคงปลอดภัยระบบ ตามวงจรชีวิตของการใช้งาน AI โดยมีแนวทางการป้องกันและควบคุมความเสี่ยง อย่างน้อยในเรื่องดังต่อไปนี้

๒.๒.๑ ดูแลให้กระบวนการพัฒนาระบบ AI คำนึงถึงความมั่นคงปลอดภัยตั้งแต่ขั้นตอนการออกแบบ และพัฒนาระบบ (Secure by Design) หากพบข้อบกพร่องควรดำเนินการแก้ไขก่อนนำไปใช้งานจริง รวมถึงเฝ้าระวังความมั่นคงปลอดภัยของโมเดลและระบบ AI อย่างต่อเนื่อง

๒.๒.๒ ทดสอบความมั่นคงปลอดภัยและบริหารจัดการช่องโหว่ของระบบ AI (Vulnerability Management) โดยอ้างอิงมาตรฐานหรือแนวปฏิบัติสากลที่เกี่ยวข้อง เช่น OWASP Top 10 for LLM Applications, OWASP Machine Learning Security Top 10 เป็นต้น รวมทั้ง การทดสอบรูปแบบการโจมตีที่อาจเกิดขึ้นและส่งผลกระทบต่อระบบแสดงข้อมูลที่ไม่ควรเปิดเผยหรือข้อมูลเชิงลบ เช่น การทำ Data Poisoning หรือ Adversarial Testing เป็นต้น ตามความเหมาะสมกับระดับความเสี่ยงของระบบ AI

๒.๒.๓ บันทึกเหตุการณ์ (Log) ของระบบ AI อย่างเหมาะสม เพื่อใช้ในการตรวจสอบเหตุการณ์ย้อนหลัง เมื่อเกิดปัญหา และระยะเวลาในการจัดเก็บควรสอดคล้องกับวัตถุประสงค์ของการใช้งาน AI โดยเฉพาะระบบ AI ที่มีความเสี่ยงสูงควรมีการบันทึกเหตุการณ์ที่เหมาะสมกับความเสี่ยง เช่น กิจกรรมของผู้ใช้งานระบบ กิจกรรมของโมเดล และกิจกรรมด้านความมั่นคงปลอดภัยทางไซเบอร์และข้อมูลส่วนบุคคล เป็นต้น

๒.๒.๔ สำรองข้อมูลและการกู้คืน (Backup and Recovery) จัดให้มีระบบสำรองข้อมูลและแผนการกู้คืนที่มีประสิทธิภาพ เพื่อรองรับเหตุการณ์ฉุกเฉินและรักษาความต่อเนื่องทางธุรกิจที่เกี่ยวข้องกับระบบ AI

๒.๒.๕ จัดทำแผนรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan: CIRP) จัดทำหรือทบทวนแผนรับมือภัยคุกคามทางไซเบอร์ให้ครอบคลุมเหตุการณ์ที่เกี่ยวข้องกับระบบ AI เพื่อให้บริษัทสามารถตอบสนองและแก้ไขสถานการณ์ฉุกเฉินได้อย่างทันท่วงที

๒.๒.๖ แบ่งแยกสภาพแวดล้อมของระบบ AI ตามระดับความเสี่ยง เพื่อป้องกันภัยคุกคามที่โจมตีระบบ AI เพื่อจำกัดผลกระทบหากระบบใช้งานไม่ได้ (Single Point of Failure)

๒.๒.๗ กรณีใช้งาน Generative AI ควรมีมาตรการลดความเสี่ยงจากการที่ระบบอาจแสดงผลลัพธ์หรือให้ข้อมูลที่ไม่เป็นความจริง (Hallucination) เพื่อให้บริหารจัดการความเสี่ยงที่เกิดขึ้นจากการใช้งาน Generative AI ได้อย่างมีประสิทธิภาพ

ส่วนที่ ๓ : ความโปร่งใสและความสามารถในการอธิบาย (Transparency and Explainability)

ความโปร่งใสและความสามารถในการอธิบายเป็นปัจจัยสำคัญในการสร้างความเชื่อมั่น และความรับผิดชอบต่อผลลัพธ์ของระบบ AI โดยเฉพาะความเสี่ยงและผลกระทบที่อาจเกิดขึ้นกับผู้เอาประกันภัย ดังนั้น การนำระบบ AI มาใช้งาน ควรยึดหลักจริยธรรมในการใช้งาน AI สามารถอธิบายการทำงาน กระบวนการพัฒนา การตัดสินใจของระบบได้อย่างชัดเจน เพื่อสามารถปฏิบัติต่อลูกค้าได้อย่างเป็นธรรม ควรมีแนวทางการควบคุม ความเสี่ยงในเรื่องดังต่อไปนี้

การอธิบายผลลัพธ์จากระบบ AI

การนำระบบ AI มาใช้งาน บริษัทต้องสามารถอธิบายการตัดสินใจหรือผลลัพธ์ได้ โดยเฉพาะการใช้งานที่อาจส่งผลกระทบต่อผู้บริโภค ความมั่นคงทางการเงิน หรือข้อกำหนดทางกฎหมาย สำหรับกรณีใช้ระบบ AI ที่มีความซับซ้อนและยากต่อการอธิบาย ควรพิจารณามาตรการควบคุมเพิ่มเติมที่เหมาะสม รวมถึงการแสดงกระบวนการคิดของ AI หรือลำดับความคิดอย่างเป็นขั้นตอน (Chain of Thought) หรือจัดให้มีการกำกับดูแลโดยมนุษย์ ตลอดจนการพิจารณาเลือกใช้โมเดลที่มีความซับซ้อนน้อยลง

ทั้งนี้ บริษัทควรบันทึกข้อสรุปและความสัมพันธ์เชิงเหตุผล ตลอดจนข้อจำกัดของระบบ เพื่อให้สามารถอธิบาย ตรวจสอบ ความสอดคล้องของผลลัพธ์ได้ และการจัดทำคำอธิบายผลลัพธ์ของระบบ AI ควรใช้ภาษาที่ผู้ใช้งานเข้าใจง่าย

อย่างไรก็ตาม ระบบ AI ควรมีมาตรการป้องกันข้อผิดพลาด และแจ้งไปยังผู้รับผิดชอบให้ดำเนินการปรับปรุงแก้ไข (Fail-Safe) หรือมีกระบวนการให้มนุษย์เข้ามาแทรกแซงการทำงานกรณีระบบ AI ทำงานในสภาพแวดล้อมใหม่ หรือข้อมูลมีความผิดปกติจนส่งผลกระทบต่อผลลัพธ์ เพื่อป้องกันและลดความเสี่ยงที่อาจส่งผลกระทบต่อผู้เอาประกันภัย

ส่วนที่ ๔ : ความเป็นธรรมและการคุ้มครองผู้บริโภค (Fairness and Consumer Protection)

การพัฒนา การบริหารจัดการและใช้งาน AI บริษัทควรยึดหลักความเป็นธรรม และการคุ้มครองผู้บริโภค หลีกเลี่ยงการใช้ข้อมูลที่มีอคติ หรือการออกแบบโมเดลที่อาจนำไปสู่การเลือกปฏิบัติอย่างไม่เหมาะสม เช่น การปฏิบัติต่อผู้เอาประกันภัยอย่างไม่เท่าเทียม หรือการตัดสินใจที่ส่งผลกระทบต่อชีวิตและสิทธิของบุคคล เป็นต้น ครอบคลุมในเรื่องดังต่อไปนี้

๔.๑ การบริหารจัดการข้อมูล

การกำกับดูแลคุณภาพของข้อมูลที่นำมาใช้งานกับ AI เพื่อให้ผลลัพธ์ที่ได้มีความถูกต้อง และลดความเสี่ยงจากอคติของข้อมูล (Data Bias) เพื่อป้องกันการปฏิบัติต่อลูกค้าอย่างไม่เป็นธรรม ควรมีแนวทางการควบคุมความเสี่ยงด้านข้อมูล ในเรื่องดังต่อไปนี้

๔.๑.๑ การจัดเตรียมชุดข้อมูล กำหนดคุณสมบัติและคุณภาพของข้อมูลให้เหมาะสมกับวัตถุประสงค์ของการพัฒนาระบบ AI โดยพิจารณาประเภทของข้อมูล ความถูกต้องของข้อมูล ความหลากหลายของข้อมูล แหล่งที่มาของข้อมูล และความสัมพันธ์ระหว่างข้อมูล เช่น ที่อยู่ อาชีพ พฤติกรรมการบริโภค อาจเชื่อมโยงกับเพศของลูกค้าโดยไม่เจตนา ซึ่งอาจส่งผลให้เกิดอคติแฝงในโมเดลหรือการตัดสินใจ

ทั้งนี้ การพัฒนาและใช้งานระบบ AI ที่มีผลต่อการตัดสินใจ ส่งผลกระทบต่อผู้เอาประกันภัย ลูกค้าหรือประชาชน บริษัทควรให้ความสำคัญกับการจัดเตรียมและบริหารจัดการชุดข้อมูล อย่างน้อยในเรื่องดังต่อไปนี้

- ชุดข้อมูลสำหรับการฝึกสอนโมเดล (Training Dataset)
- ชุดข้อมูลสำหรับการตรวจสอบความถูกต้องของโมเดล (Validation Dataset)
- ชุดข้อมูลสำหรับการทดสอบประสิทธิภาพของโมเดล (Testing Dataset)

๔.๑.๒ การเก็บรวบรวมข้อมูล พิจารณาเลือกใช้ข้อมูลจากแหล่งที่มีความน่าเชื่อถือ มีความหลากหลาย และมีการปรับปรุงให้เป็นปัจจุบันอย่างต่อเนื่อง

๔.๑.๓ การบริหารจัดการข้อมูลเพื่อรองรับการใช้งาน AI พิจารณาจัดกลุ่มข้อมูลตามประเภทระดับความสำคัญหรือวัตถุประสงค์ในการใช้งาน เช่น ข้อมูลลูกค้า ข้อมูลส่วนบุคคล ข้อมูลทางการเงิน ข้อมูลกรมธรรม์ เป็นต้น ตลอดจนการแยกข้อมูลบริษัทออกจากข้อมูลสาธารณะ เช่น การทำ Data Boundary เป็นต้น และการจัดทำคลังข้อมูลที่รวบรวมโมเดลที่นำมาใช้ภายในบริษัท

๔.๑.๔ การจัดทำเอกสารแสดงแหล่งที่มาของข้อมูล แสดงรายละเอียดเกี่ยวกับการพัฒนา^๕ การฝึกสอน การตรวจสอบ และการทดสอบระบบ AI

๔.๑.๕ การติดตามและตรวจสอบข้อมูลที่น่าไปใช้ในระบบ AI โดยกำหนดแนวทางการติดตามและตรวจสอบข้อมูลที่ใช้ในระบบ AI อย่างสม่ำเสมอ เพื่อให้มั่นใจว่า ข้อมูลมีความถูกต้อง เป็นปัจจุบัน และสอดคล้องกับวัตถุประสงค์การใช้งาน ทั้งในด้านการวิเคราะห์ การตัดสินใจ และการเรียนรู้ของระบบ เพื่อป้องกันความเสี่ยงการใช้ข้อมูลที่ทำให้เกิดการเลือกปฏิบัติที่ไม่ชอบด้วยกฎหมาย

๔.๒ การบริหารจัดการอคติของโมเดล

กำหนดแนวทางควบคุมและประเมินประสิทธิภาพของโมเดลอย่างเป็นระบบทั้งก่อนและหลังใช้งาน เพื่อติดตามความถูกต้อง ความน่าเชื่อถือของผลลัพธ์อย่างต่อเนื่อง และป้องกันผลลัพธ์ที่มีอคติจากการออกแบบระบบ

^๕ ตัวอย่างการจัดทำเอกสารและรายละเอียด ปรากฏในภาคผนวก ก.

๔.๓ การติดตามและตรวจสอบผลลัพธ์ของระบบ AI

การติดตาม และตรวจสอบผลลัพธ์ของระบบ AI ครอบคลุมในเรื่องดังต่อไปนี้

๔.๓.๑ การนำระบบ AI มาใช้งาน ควรมีแนวทางในการติดตามประสิทธิภาพการทำงานของระบบ ข้อมูลและผลลัพธ์ที่เกิดขึ้น เพื่อให้ผู้พัฒนาระบบหรือผู้ให้บริการดำเนินการตรวจสอบความถูกต้อง และสามารถแก้ไข ปรับปรุงระบบได้อย่างต่อเนื่อง (Feedback Loop) ทั้งนี้ กรณีใช้งาน AI ที่มีความเสี่ยงสูง ควรมีการประเมิน ผลลัพธ์ของโมเดลที่เกี่ยวข้องกับความเป็นธรรมต่อผู้บริโภค เช่น การเปิดเผยข้อมูลประกอบการตัดสินใจ ของระบบ AI เป็นต้น

๔.๓.๒ หากระบบ AI หรือบริการที่เกี่ยวข้องไม่สามารถบรรลุเป้าหมายที่กำหนดไว้ หรือใช้เทคโนโลยี ที่ไม่เหมาะสม บริษัทสามารถพิจารณายุติการใช้งานหรือเปลี่ยนไปใช้โมเดลใหม่ที่เหมาะสมกว่า โดยต้องพิจารณา ปัจจัยที่เกี่ยวข้องอย่างรอบคอบ รวมถึงผลกระทบที่อาจเกิดขึ้นต่อผู้ใช้งาน ผู้มีส่วนได้ส่วนเสีย และระบบงาน ที่เกี่ยวข้อง

๔.๔ การคุ้มครองผู้บริโภค

บริษัทต้องให้ความสำคัญต่อการใช้งานระบบ AI ตามหลักจริยธรรมการใช้งาน AI มีการพิจารณาให้ มนุษย์มีส่วนร่วมในการตัดสินใจหรือดำเนินการ (Human in the loop/ Human over the loop) เพื่อป้องกันการ ปฏิบัติอย่างไม่เป็นธรรม โดยควรพิจารณาดำเนินการอย่างน้อยในเรื่องดังต่อไปนี้

๔.๔.๑ กรณีที่ใช้ระบบ AI ในงานที่ปฏิสัมพันธ์กับลูกค้าโดยตรง ให้แสดงข้อความ เพื่อแจ้งและเปิดเผย ให้ประชาชนหรือลูกค้าทราบโดยใช้ข้อความที่เข้าใจง่าย ไม่คลุมเครือ นอกจากนี้ บริษัทต้องจัดให้มีทางเลือกให้ ผู้ใช้บริการสามารถเปลี่ยนไปใช้บริการจากพนักงานแทนระบบ AI ได้

๔.๔.๒ จัดให้มีช่องทางการติดต่อ หรือการรายงานข้อผิดพลาดจากการใช้งาน ทั้งจากผู้ใช้งาน ในบริษัท และลูกค้า เพื่อสามารถปรับปรุงระบบและมีแนวทางการป้องกันไม่ให้เกิดซ้ำในอนาคต

๔.๔.๓ มีกระบวนการรองรับให้ผู้บริโภคสามารถแจ้งปรับปรุง เพิ่มเติม แก้ไขข้อมูล และแหล่งข้อมูล ที่ระบบ AI ใช้ได้ รวมทั้งให้สิทธิแก่ผู้บริโภคปรับปรุงข้อมูลให้มีความถูกต้องเป็นปัจจุบัน เพื่อที่ระบบ AI สามารถ ทำงานและให้ผลลัพธ์ได้อย่างถูกต้อง

๔.๔.๔ กรณีที่มีการใช้งานระบบ AI ที่มีความเสี่ยงสูง หรือบริหารจัดการเรื่องร้องเรียน บริษัทควรจัดทำ คำอธิบายปัจจัยสำคัญที่มีผลต่อการตัดสินใจของระบบ AI อย่างชัดเจน (Determinative Factors) เพื่อเป็นข้อมูล ประกอบในการอธิบายต่อผู้เอาประกันภัย

๔.๔.๕ กรณีที่บริษัทใช้งานระบบ AI เพื่อคำนวณเบี้ยประกันภัยแบบละเอียด (Granular Risk-Based Pricing) หรือการพิจารณารับประกันภัย ควรตั้งอยู่บนพื้นฐานความเป็นธรรมและการคุ้มครองผู้บริโภค เพื่อลด ผลกระทบทางสังคมที่อาจเกิดขึ้น ทั้งนี้ การคำนวณเบี้ยประกันแบบละเอียดสามารถช่วยให้ประชาชนบางกลุ่มที่ ปัจจุบันไม่สามารถเข้าถึงการประกันภัย สามารถเข้าถึงบริการทางการเงินได้ (Financial Inclusion) ในทางกลับกัน อาจส่งผลให้กลุ่มเปราะบางได้รับเบี้ยประกันภัยที่ไม่เหมาะสม และถูกจำกัดการเข้าถึงการประกันภัย

ดังนั้น บริษัทควรคำนึงถึงความเป็นธรรมต่อผู้บริโภค โดยมีมาตรการควบคุมความเสี่ยงจากการใช้งาน AI ให้เหมาะสม เช่น การออกแบบโมเดล (Fairness by Design) การติดตามผลลัพธ์ การประเมินผลกระทบทางสังคม จากการใช้ระบบ AI การประเมินปัจจัยเสี่ยงที่ก่อให้เกิดการเลือกปฏิบัติและทบทวนข้อมูลที่อาจส่งผลให้เกิดการ ปฏิบัติที่ไม่เป็นธรรมต่อผู้บริโภค จัดทำเอกสารอธิบายเหตุผลเชิงสาเหตุ และทดสอบความถูกต้องของผลลัพธ์ เป็นต้น รวมถึงการมีช่องทางให้ผู้บริโภคสามารถร้องขอคำอธิบาย หรือขอให้มนุษย์เข้ามาตรวจสอบได้ ตลอดจนมีแนว ทางแก้ไขหากเกิดความไม่เป็นธรรม

ตัวอย่าง รายละเอียดการจัดทำเอกสารแหล่งที่มาของข้อมูล (Data Resource Documentation)

หัวข้อ	ตัวอย่าง รายละเอียดที่ควรจัดทำ หรือควรระบุไว้ในเอกสาร
๑. แหล่งที่มาของข้อมูล	- ระบุแหล่งที่มาของข้อมูล (ภายใน / ภายนอกบริษัท) - ระบุชื่อหน่วยงานหรือบุคคลที่เป็นเจ้าของข้อมูล
๒. วันที่ปรับปรุงข้อมูลล่าสุด	- ระบุวันที่ล่าสุดในการปรับปรุงข้อมูล
๓. ประเภทข้อมูลตามการใช้งาน	- ระบุชุดข้อมูลตามการใช้งาน เช่น ข้อมูลที่ใช้ในการฝึกสอนโมเดล ข้อมูลที่ใช้ในการตรวจสอบ และข้อมูลสำหรับการทดสอบ เป็นต้น - ระบุวัตถุประสงค์ของชุดข้อมูล เช่น ใช้สำหรับการฝึกสอนโมเดล การตรวจสอบ หรือการทดสอบระบบ AI เป็นต้น
๔. ลักษณะของข้อมูลทั่วไป	- ระบุประเภทข้อมูล เช่น ข้อมูลที่มีโครงสร้าง (Structured Data) ข้อมูลไม่มีโครงสร้าง (Unstructured Data) ข้อมูลรูปภาพ ข้อมูลสถิติ เป็นต้น
๕. การติดป้ายกำกับข้อมูล	- ระบุเกณฑ์หรือแนวทางในการ ติดป้ายกำกับข้อมูล (Label) ข้อมูลการตรวจสอบความถูกต้องของป้ายกำกับข้อมูล (Label) เป็นต้น - ระบุแนวทางหรือเกณฑ์ที่ใช้ในการติดป้ายกำกับข้อมูล และวิธีการตรวจสอบความถูกต้องของป้ายกำกับข้อมูล
๖. วัตถุประสงค์ในการใช้ข้อมูล	- ระบุวัตถุประสงค์ของการนำข้อมูลไปใช้ เช่น การวิเคราะห์ การพัฒนาโมเดล AI การจัดทำรายงาน หรือการตรวจสอบความถูกต้องของข้อมูล (Reconciliation) เป็นต้น
๗. คุณภาพของข้อมูล	- ระบุแนวทางการตรวจสอบคุณภาพข้อมูลก่อนนำไปใช้จริง เช่น การตรวจสอบความสอดคล้อง การตรวจสอบความเอนเอียงของข้อมูล ที่อาจนำไปสู่การตัดสินใจที่ไม่เป็นธรรม และความถูกต้องของข้อมูล เป็นต้น
๘. ระยะเวลาเก็บข้อมูล	- ระบุระยะเวลาจัดเก็บข้อมูล เช่น จัดเก็บข้อมูลเป็นระยะเวลา ๓ ปี หลังจากการใช้งาน และมีแนวทางการลบหรือทำลายข้อมูลอย่างเหมาะสม เป็นต้น
๙. อคติในข้อมูล (Bias)	- อธิบายแหล่งที่มาของข้อมูล ตัวอย่างข้อมูลที่มีลักษณะก่อให้เกิดผลที่เป็นอคติ (Bias) - ระบุแนวทางในการตรวจจับ และการจัดการกับข้อมูลที่มีอคติ (Bias)
๑๐. การเตรียมข้อมูล (Data Preparation)	- ระบุขั้นตอนในการเตรียมข้อมูล ก่อนนำไปใช้งาน เช่น - การลบ แก้ไข หรือจัดการข้อมูลที่ผิดพลาด ไม่สมบูรณ์ ซ้ำซ้อน หรือไม่สัมพันธ์กัน - การทำให้ข้อมูลไม่สามารถระบุตัวตนได้ เช่น การลบหรือการเข้ารหัสข้อมูลส่วนบุคคล (Personally Identifiable Information: PII) เป็นต้น

ตัวอย่าง หัวข้อการรายงานความเสี่ยงจากการใช้งาน AI

หัวข้อการรายงานความเสี่ยงจากการใช้งาน AI	รายละเอียด
๑. ระดับความเสี่ยงของการใช้งาน AI ที่มีนัยสำคัญและความเสี่ยงที่อาจเกิดขึ้น	รายงานระดับความเสี่ยงของการใช้งาน AI ที่มีความสำคัญโดยพิจารณาความเสี่ยงที่อาจเกิดขึ้น เช่น - ความเสี่ยงจากอคติของโมเดล (Model Bias) - ความเสี่ยงจากความน่าเชื่อถือหรือข้อเสียน - ความเสี่ยงทางกฎหมาย ระเบียบ ข้อบังคับ (Regulatory/Compliance Risk) - ความเสี่ยงจากการใช้ผู้ให้บริการภายนอก เป็นต้น
๒. รายงานสรุปเกี่ยวกับการใช้งาน AI ที่มีนัยสำคัญ	รายงานตามบริบทการใช้งาน (In-house, Third-party, Hybrid) และระบุความเสี่ยงหรือผลกระทบที่เกี่ยวข้องกับกิจกรรมหลัก หรือห่วงโซ่อุปทานของธุรกิจประกันภัย
๓. แนวโน้มความเสี่ยงในอนาคตของเทคโนโลยี AI	รายงานแนวโน้มความเสี่ยงในอนาคตที่ส่งผลต่อการใช้งาน AI ในบริษัท เช่น - การเปลี่ยนแปลงของเทคโนโลยี AI พัฒนาไปอย่างรวดเร็วทำให้ไม่สามารถควบคุมเทคโนโลยีได้ทัน - การปรับปรุง เพิ่มเติม กฎระเบียบ ข้อบังคับที่เกี่ยวข้องกับการใช้งาน AI เพื่อเป็นการเตรียมความพร้อมต่อกฎหมายและกฎระเบียบใหม่ เป็นต้น
๔. ระดับความเสี่ยงในภาพรวมขององค์กร (Risk Profile) เพื่อทบทวนและติดตามผลที่ได้ยังคงเป็นไปตามเป้าหมายที่กำหนด และใช้เป็นข้อมูลในการปรับปรุงกระบวนการพิจารณาตัดสินใจในครั้งต่อไป	รายงานระดับความเสี่ยงที่ได้รับผลกระทบจากการนำ AI มาใช้ในภาพรวมของบริษัท เช่น - ความเสี่ยงจากการละเมิดข้อมูลส่วนบุคคล - ความเสี่ยงจากข้อมูลสำคัญรั่วไหล - ความเสี่ยงจากภัยคุกคามทางไซเบอร์ - ความเสี่ยงอื่นๆ ที่อาจกระทบต่อกลยุทธ์การดำเนินธุรกิจในการพิจารณาตัดสินใจนำ AI ไปใช้ เป็นต้น
๕. สถานะปัจจุบันในการใช้บริการผู้ให้บริการจากภายนอก (Third Party AI) และความเสี่ยงที่เกิดขึ้นจากการใช้บริการผู้ให้บริการจากภายนอก AI (Third Party AI)	รายงานการให้บริการจากผู้ให้บริการภายนอก ตัวอย่างหัวข้อการรายงาน เช่น - รายงานระดับการให้บริการจากผู้ให้บริการภายนอกสอดคล้องกับที่กำหนดไว้ในสัญญา หรือไม่ - รายงานผลการปฏิบัติงาน
๖. ความเสี่ยงในการปฏิบัติตามกฎหมาย ระเบียบที่เกี่ยวข้อง	การระบุความเสี่ยงจากการไม่ปฏิบัติตามกฎหมายที่เกี่ยวข้องกับ AI เช่น - พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล ความเสี่ยงจากการละเมิดกฎหมายการคุ้มครองข้อมูลส่วนบุคคลที่เกิดจากการใช้ AI ในการประมวลผลข้อมูล - การปฏิบัติตามข้อกำหนดของสำนักงาน คปภ. ความเสี่ยงจากการไม่ปฏิบัติตามข้อกำหนดที่สำนักงาน คปภ. หรือหน่วยงานกำกับดูแลอื่นๆ กำหนด - การประเมิน Gap ในการปฏิบัติตามกฎหมายที่เกี่ยวข้องกับการใช้งาน AI และการดำเนินการเพื่อปิด Gap

ตัวอย่าง ความเสี่ยงที่เกี่ยวข้องกับการใช้งาน AI ในภาคประกันภัย

ความเสี่ยงต่อ	ผลกระทบ	ตัวอย่าง ความเสี่ยงที่อาจเกิดขึ้น	ตัวอย่าง มาตรการควบคุมความเสี่ยง
ผลลัพธ์ที่ได้จากการใช้งาน AI			
ผู้เอาประกันภัย	การพิจารณารับประกันภัย	ความเสี่ยงต่อการที่ AI ใช้พิจารณารับประกันภัย ซึ่งอาจมีผลกระทบต่อผู้เอาประกันภัย <u>ตัวอย่างเช่น</u> บริษัทประกันภัยใช้ระบบ AI ในกระบวนการพิจารณารับประกันภัย ส่งผลให้ผลการพิจารณากรรมธรรม์ อยู่ในระดับความเสี่ยงสูง	- การพิจารณาข้อมูลประกอบการรับประกันภัย ผ่านเจ้าหน้าที่เพื่อพิจารณาเงื่อนไข ข้อมูล ก่อนที่จะนำไปให้ AI ประมวลผลต่อ - กำหนดเกณฑ์ หรือกรณีที่จะใช้งาน AI โดยคำนึงถึงความเสี่ยง และความเป็นไปได้ในกรณีนั้นๆ
	การเลือกปฏิบัติที่ไม่เหมาะสม ไม่ถูกต้องตามกฎหมาย (Unlawful Discrimination)	ความเสี่ยงที่เกิดจากการใช้งาน AI กระทบในทางลบต่อการเลือกปฏิบัติที่ไม่เหมาะสม ไม่ถูกต้องตามกฎหมาย ส่งผลต่อการรับประกันภัย <u>ตัวอย่างเช่น</u> บริษัทประกันภัยใช้ระบบ AI วิเคราะห์ข้อมูลลูกค้าเพื่อกำหนดเบี้ยประกัน และพิจารณารับประกันระบบเรียนรู้จากข้อมูลที่มีอคติแฝง ระบบจึงแนะนำให้ปฏิเสธรับประกันหรือคิดเบี้ยสูงผิดปกติ	- การพิจารณาข้อมูลประกอบการรับประกันภัย ผ่านเจ้าหน้าที่เพื่อพิจารณาเงื่อนไข ข้อมูล ก่อนที่จะนำไปให้ AI ประมวลผลต่อ - กำหนดเกณฑ์ หรือกรณีที่จะใช้งาน AI โดยคำนึงถึงความเสี่ยง และความเป็นไปได้ในกรณีนั้น ๆ
	ความเป็นธรรม (Fairness)	AI มีส่วนร่วมในการรับผิดชอบต่อผลลัพธ์ และต่อผู้บริโภค และประชาชน <u>ตัวอย่างเช่น</u> บริษัทประกันภัยใช้ AI เพื่อช่วยประเมินความเสี่ยง และคำนวณเบี้ยประกัน อาจส่งผลให้ AI เลือกปฏิบัติและปฏิเสธการรับประกันภัย จากข้อมูลที่มีอคติ	- กำหนดหลักเกณฑ์พิจารณาการใช้ AI ให้สอดคล้องกับหลักจริยธรรมในการใช้งาน AI - ข้อมูลที่ใช้ฝึกสอน ควรเป็นข้อมูลที่มีคุณภาพ ไม่เอนเอียง และปราศจากอคติในข้อมูล และมีการวิเคราะห์ข้อมูลจากมนุษย์/ ผู้ที่มีหน้าที่รับผิดชอบ - กำหนดช่องทางการรับเรื่องร้องเรียน เพื่อนำมาปรับปรุงกระบวนการให้เหมาะสม

ความเสี่ยงต่อ	ผลกระทบ	ตัวอย่าง ความเสี่ยงที่อาจเกิดขึ้น	ตัวอย่าง มาตรการควบคุมความเสี่ยง
	ปริมาณ/ประเภท ของลูกค้าที่ได้รับ ผลกระทบ (Volume /Type of Customers Affected)	การใช้งาน AI อาจมีผลกระทบ ในทางบวก และทางลบต่อ ลูกค้าจำนวนมาก โดยเฉพาะ กลุ่มลูกค้าที่เปราะบาง เช่น ผู้ ที่มีรายได้น้อย ผู้สูงอายุหรือผู้ ที่มีข้อจำกัดในการเข้าถึง เทคโนโลยี	- พิจารณาการใช้ AI ให้สอดคล้อง กับหลักจริยธรรมในการใช้งาน AI - บริษัทประกันภัยมีการตรวจสอบ ความโปร่งใส ในการประมวลผล ของ AI - จัดทำคำอธิบายกลไกการ พิจารณาเงื่อนไขของ AI โดย แสดงถึงความโปร่งใสของเหตุผล ที่ทำให้เกิดการตัดสินใจ เช่น ทำไมการสมัครประกันถูกปฏิเสธ หรือเบี้ยประกันสูงเกินไป
	การดำเนินงานทาง ธุรกิจ	AI ถูกนำไปใช้ในกิจกรรมที่ สำคัญต่อการเข้าถึงการ ประกันภัยของลูกค้า	- พิจารณาการใช้ AI ให้สอดคล้อง กับหลักจริยธรรมในการใช้งาน AI - หากมีผลกระทบต่อลูกค้าจำนวน มาก หรือมีข้อมูลสำคัญ ข้อมูล อ่อนไหว ควรพิจารณาให้มี เจ้าหน้าที่ที่เกี่ยวข้อง เข้ามา พิจารณาข้อมูลประกอบ - จัดให้มีการประเมินความเสี่ยงให้ ครอบคลุมผลกระทบที่อาจ เกิดขึ้น
	กระบวนการที่ เกี่ยวข้องกับการ แก้ไข หรือ ปรับเปลี่ยนผลลัพธ์ ที่ไม่ถูกต้อง หรือไม่ เป็นธรรม	บริษัทใช้งาน AI ในการ ตัดสินใจที่มีผลกระทบต่อ ผู้บริโภค เช่น การปฏิเสธคำ ขอประกันภัย หรือการ คำนวณค่าสินไหมทดแทน และผลประโยชน์ตาม กรมธรรม์	- จัดทำเอกสารประกอบการใช้งาน ระบบ AI เพื่อแสดงรายละเอียด ที่ AI ใช้ประมวลผล - จัดเก็บ Log การใช้งานระบบ AI เพื่อใช้ตรวจสอบเหตุการณ์ที่ เกิดขึ้นและป้องกันข้อผิดพลาดที่ อาจเกิดขึ้นซ้ำในอนาคต
บริษัทประกันภัย	กิจกรรมการ ประกันภัยที่สำคัญ (Critical Core Insurance Function)	ระดับการบริการที่ใช้ AI หยุดชะงักในกิจกรรมธุรกิจที่ สำคัญ เช่น เช่น การพิจารณา รับประกันภัย การกำหนดเบี้ย ประกันภัย การจัดการค่า สินไหมทดแทนและ ผลประโยชน์ตามกรมธรรม์	- กำหนดเกณฑ์ หรือกรณีที่จะใช้ งาน AI โดยคำนึงถึงความเสี่ยง และความเป็นไปได้ในกรณีนั้น ๆ - จัดทำแผนสำรอง เมื่อระบบ สำคัญที่ใช้งาน AI หยุดชะงัก พร้อมมีการทดสอบแผนเพื่อให้ สามารถใช้งานจริงได้

ความเสี่ยงต่อ	ผลกระทบ	ตัวอย่าง ความเสี่ยงที่อาจเกิดขึ้น	ตัวอย่าง มาตรการควบคุมความเสี่ยง
	ผลกระทบทางการเงิน (Financial Impact)	ความขัดข้องของระบบ AI ส่งผลกระทบอย่างมีนัยสำคัญต่อสถานะการเงินของบริษัท ทำให้ผู้รับประกันภัยขาดความเชื่อถือในบริษัท เช่น ความล้มเหลวของ AI ในการคำนวณค่าสินไหมทดแทน และผลประโยชน์ตามกรมธรรม์อาจทำให้บริษัทประกันภัยต้องจ่ายเงินมากเกินไป หรือ จ่ายค่าสินไหมทดแทนและผลประโยชน์ตามกรมธรรม์ที่ต่ำเกินไป ซึ่งจะส่งผลกระทบต่อ ความมั่นคงทางการเงินของบริษัท หากจ่ายค่าชดเชยมากเกินไป อาจทำให้บริษัทต้องแบกรับภาระทางการเงินที่เพิ่มขึ้น	- จัดให้มีการประเมินความเสี่ยงให้ครอบคลุมผลกระทบที่อาจเกิดขึ้น - จัดทำแผนสำรอง เมื่อระบบสำคัญที่ใช้งาน AI หยุดชะงัก พร้อมมีการทดสอบแผนเพื่อให้สามารถใช้งานจริงได้ - ทดสอบแผนสำรองให้ครอบคลุมระบบงานสำคัญ - มีมาตรการควบคุมตั้งแต่กระบวนการพัฒนา การทดสอบการใช้งาน ตลอดจนการบำรุงรักษาระบบ ให้มีความพร้อมใช้งานอยู่เสมอ
	ผลกระทบทางกฎหมาย (Legal Impact)	ความขัดข้องของระบบ AI ส่งผลกระทบอาจทำให้เกิดการละเมิดข้อผูกพันทางกฎหมาย ต่อผู้รับประกันภัย ตัวอย่างเช่น ระบบ AI ใช้ข้อมูลที่ไม่เหมาะสมหรือ พบข้อผิดพลาดในการประมวลผลข้อมูล เช่น การคำนวณเบี้ยประกันภัยที่ไม่เหมาะสม หรือการปฏิเสธการเคลมที่ไม่เป็นธรรม บริษัทประกันภัยอาจละเมิดข้อกำหนดทางกฎหมาย ที่เกี่ยวข้องกับการคุ้มครองผู้บริโภค หรือการคุ้มครองข้อมูลส่วนบุคคล	- กำหนดนโยบาย และแนวทางการใช้งาน AI ในบริษัท ประกันภัย ครอบคลุมไปถึงหลักจริยธรรมในการใช้งาน AI - จัดให้มีการประเมินความเสี่ยงให้ครอบคลุมผลกระทบที่อาจเกิดขึ้น

ความเสี่ยงต่อ	ผลกระทบ	ตัวอย่าง ความเสี่ยงที่อาจเกิดขึ้น	ตัวอย่าง มาตรการควบคุมความเสี่ยง
การบริหารจัดการระบบ AI /โมเดล			
ขีดความสามารถ ของบริษัท (Capability)	ความรู้และ ทรัพยากร (Knowledge & Resource)	บริษัทประกันภัยขาด ผู้เชี่ยวชาญ และมีทรัพยากรที่ จำกัดสำหรับระบบ AI	- ส่งเสริมความรู้และทักษะด้าน AI ให้กับพนักงานที่มีหน้าที่เกี่ยวข้อง - จัดหาผู้เชี่ยวชาญ ที่ปรึกษา หรือ ผู้ให้บริการภายนอกเฉพาะด้าน AI - บริหารจัดการทรัพยากรให้รองรับการใช้งาน AI อย่างเหมาะสม
	ความสามารถในการ ปรับตัว (Adaptability)	ระบบ AI สามารถปรับตัวเอง ได้อัตโนมัติ โดยเมื่อมีข้อมูล ใหม่เข้ามา อาจส่งผลกระทบต่อ โมเดล <u>ตัวอย่างเช่น</u> การใช้ AI ในการ พิจารณารับประกันภัย การ กำหนดเบี้ยประกันภัย การ จัดการค่าสินไหมทดแทนและ ผลประโยชน์ตามกรมธรรม์ อาจทำให้เกิดความเสี่ยงจาก อคติที่ไม่ตั้งใจ เมื่อโมเดลเกิด การเบี่ยงเบนจากเวอร์ชันที่ ได้รับการอนุมัติ หรือการที่ไม่ สามารถควบคุมการ ประมวลผลของโมเดลได้	- จัดทำคำอธิบายกลไกการ พิจารณาเงื่อนไขของ AI โดย แสดงถึงความโปร่งใสของระบบ ในการประมวลผลข้อมูล พร้อม แสดงเวอร์ชันอย่างชัดเจน - มีกระบวนการจัดการ เปลี่ยนแปลง (Change Management) เพื่อควบคุม เวอร์ชันการใช้งานของ AI
	คุณภาพข้อมูล (Data Quality)	ข้อมูลที่นำมาฝึกสอนโมเดล ไม่เหมาะสม ข้อมูลมีอคติ ข้อมูล และไม่สามารถแสดงถึง ลักษณะของกลุ่มข้อมูลที่ตรง ตามวัตถุประสงค์ในการใช้งาน	- กำกับดูแลคุณภาพของข้อมูลที่ นำมาใช้งานกับ AI - เตรียมชุดข้อมูลเพื่อทดสอบ คุณภาพข้อมูลก่อนการนำไปใช้ จริง - ประเมินความเสี่ยงด้านข้อมูล
	ความโปร่งใส/ ความสามารถในการ อธิบาย (Transparency/ Explainability)	การทำให้ผลลัพธ์ หรือ กระบวนการตัดสินใจของ ระบบ AI สามารถอธิบายได้ หรือมีการจัดทำเอกสาร ประกอบ โดยอธิบายลักษณะ ของข้อมูลนำเข้า วัตถุประสงค์ของข้อมูล และ	- จัดทำคำอธิบายกลไกการ พิจารณาเงื่อนไขของ AI โดย แสดงถึงความโปร่งใสของระบบ ในการประมวลผลข้อมูล รวมไปถึง การจัดทำเอกสารทางเทคนิค ประกอบ

ความเสี่ยงต่อ	ผลกระทบ	ตัวอย่าง ความเสี่ยงที่อาจเกิดขึ้น	ตัวอย่าง มาตรการควบคุมความเสี่ยง
		ผลกระทบความเสี่ยงที่อาจเกิดขึ้นต่อผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องได้ เพื่อให้เข้าใจผลลัพธ์ หรือการตัดสินใจของระบบได้	
การใช้งาน (Implementation)	ระดับความอัตโนมัติที่ AI สามารถทำงานได้เอง (Autonomy)	ระดับความอัตโนมัติที่ AI สามารถทำงานได้เอง <u>ตัวอย่างเช่น</u> การใช้งาน AI ที่สามารถประมวลผลข้อมูลและแสดงผลลัพธ์กับลูกค้า ได้ อัตโนมัติ อาจส่งผลกระทบในเรื่องความถูกต้อง ครบถ้วนของข้อมูล	- กำหนดเกณฑ์ที่มนุษย์มีส่วนร่วมในการตัดสินใจ (Human in loop/ Human over the loop) - จัดให้มีการประเมินความเสี่ยงให้ครอบคลุมผลกระทบที่อาจเกิดขึ้น
	การพึ่งพาบุคคลภายนอก (Third Party Reliance) - โมเดล /ระบบ - แหล่งข้อมูลสำรอง	<u>ตัวอย่างเช่น</u> บริษัทประกันภัยใช้บริการจากผู้ให้บริการรายใดรายหนึ่งมากเกินไป หากผู้ให้บริการถูกโจมตีทางไซเบอร์ หรือไม่สามารถให้บริการได้ อาจกระทบการดำเนินงานหรือความมั่นคงปลอดภัยไซเบอร์ของบริษัทประกันภัย	- จัดให้มีการประเมินความเสี่ยงให้ครอบคลุมผลกระทบที่อาจเกิดขึ้นตั้งแต่ก่อนใช้บริการ ระหว่างการให้บริการ และเมื่อสิ้นสุดการให้บริการ - จัดทำเกณฑ์การประเมินบุคคลภายนอกเพื่อประเมินการให้บริการก่อนการให้บริการ - จัดทำเกณฑ์การให้บริการ Services Level Agreement (SLA) ตลอดจนการทำสัญญาการให้บริการ - จัดทำแผนสำรองฉุกเฉิน/ ระบบสำรอง

เอกสารอ้างอิง

กฎหมาย ประกาศ คปภ. และแนวปฏิบัติที่เกี่ยวข้อง

- ๑) พระราชบัญญัติประกันวินาศภัย พ.ศ. ๒๕๓๕ และพระราชบัญญัติประกันชีวิต พ.ศ. ๒๕๓๕ และที่แก้ไขเพิ่มเติม
- ๒) ประกาศ คปภ. ว่าด้วยเรื่อง หลักเกณฑ์ วิธีการ และเงื่อนไขในการกำกับการบริหารความเสี่ยงแบบองค์รวม และการประเมินความเสี่ยงและความมั่นคงทางการเงินของบริษัทประกันวินาศภัย/ประกันชีวิต
- ๓) ประกาศ คปภ. ว่าด้วยเรื่อง หลักเกณฑ์การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัทประกันชีวิต/ประกันวินาศภัย
- ๔) ประกาศ คปภ. ว่าด้วยเรื่อง การกำกับดูแลกิจการที่ดีของบริษัทประกันชีวิต และบริษัทประกันวินาศภัย
- ๕) ประกาศ คปภ. ว่าด้วยเรื่อง หลักเกณฑ์ วิธีการออก และเสนอขายกรมธรรม์ประกันของบริษัทประกันวินาศภัย/ประกันชีวิต และการดำเนินการของตัวแทนประกันวินาศภัย/ ประกันชีวิต นายหน้าประกันวินาศภัย และธนาคาร
- ๖) ประกาศ คปภ. ว่าด้วยเรื่อง หลักเกณฑ์ วิธีการออก และเสนอขายกรมธรรม์ประกันภัย และการขอใช้เงิน หรือค่าสินไหมทดแทนตามสัญญาประกันภัย โดยใช้วิธีการทางอิเล็กทรอนิกส์
- ๗) ประกาศสำนักงาน คปภ. ว่าด้วยเรื่อง หลักเกณฑ์ วิธีการ และเงื่อนไขการขึ้นทะเบียนกิจกรรมทางอิเล็กทรอนิกส์ การขอรับความเห็นชอบการใช้บริการบุคคลภายนอก และการรับรองระบบสารสนเทศ สำหรับธุรกิจประกันวินาศภัย/ ประกันชีวิต
- ๘) ประกาศนายทะเบียน ว่าด้วยเรื่อง มาตรฐานขั้นต่ำในการบริหารจัดการความเสี่ยงเกี่ยวกับการพัฒนาผลิตภัณฑ์ประกันภัยและการกำหนดเบี้ยประกันภัยของบริษัทประกันวินาศภัย/ประกันชีวิต
- ๙) แนวปฏิบัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของลูกค้าสำหรับธุรกิจประกันวินาศภัย/ประกันชีวิต
- ๑๐) แนวปฏิบัติว่าด้วยเรื่อง หลักเกณฑ์การกำกับดูแล การบริหารจัดการความเสี่ยงจากบุคคลภายนอกด้านเทคโนโลยีสารสนเทศ
- ๑๑) แนวปฏิบัติว่าด้วยเรื่อง การกำกับดูแลข้อมูล (Data Governance Guideline)

เอกสารอ้างอิงอื่นๆ

- ๑) IAIS - Application Paper on the Supervision of Artificial Intelligence July 2025
- ๒) NIST- Artificial Intelligence Risk Management Framework (AI RMF 1.0) 2022
- ๓) ISO/IEC 42001:2023 AI Management System 2023
- ๔) กรอบการกำกับดูแลการใช้งาน ปัญญาประดิษฐ์ (Artificial Intelligence) และการเรียนรู้ของเครื่อง (Machine Learning) ในตลาดทุน โดยสำนักงานคณะกรรมการกำกับและตลาดหลักทรัพย์ ๒๕๖๖
- ๕) ETDA-Generative AI Governance Guideline for Organization แนวทางการประยุกต์ใช้ Generative AI อย่างมีธรรมาภิบาล สำหรับองค์กร ๒๐๒๔
- ๖) แผนนโยบายธนาคารแห่งประเทศไทย เรื่อง การบริหารจัดการความเสี่ยงของการใช้งานปัญญาประดิษฐ์ (Guiding Principles for Artificial Intelligence Risk Management) ๒๕๖๘



สำนักงานคณะกรรมการกำกับและส่งเสริม
การประกอบธุรกิจประกันภัย(คปภ.)
Office of Insurance Commission