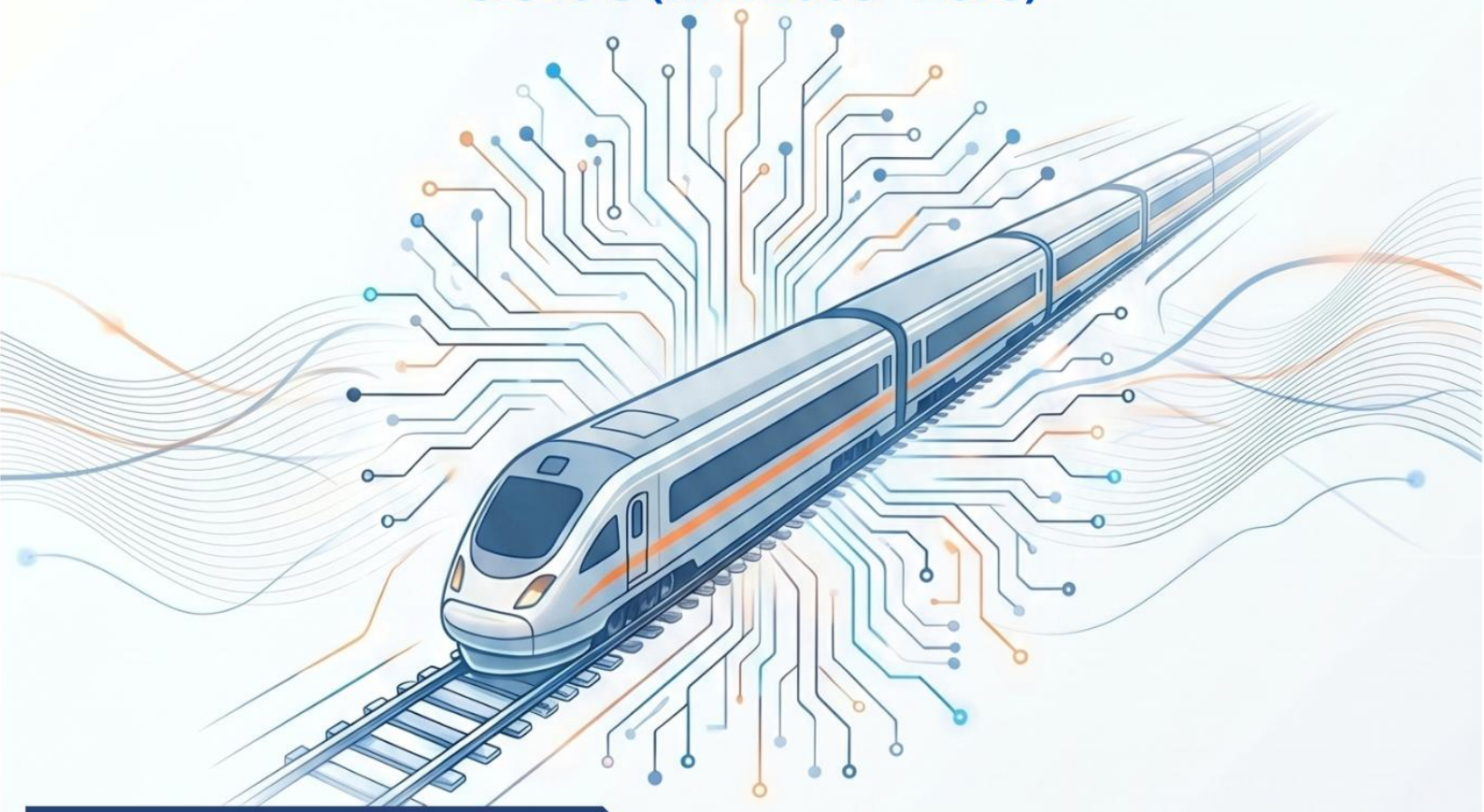
กรมการขนส่งทางราง
Department of Rail Trasport

แผนปฏิบัติการการขับเคลื่อนและบริหารจัดการระบบปัญญาประดิษฐ์ ระยะ 5 ปี (พ.ศ. 2569 - 2573)



กองยุทธศาสตร์และแผนงาน

514/1 Lan Luang Rd., www.drt.go.th facebook/ กรมการขนส่งทางราง

พฤษภาคม 2569

สารบัญ

แผนปฏิบัติการการขับเคลื่อนและบริหารจัดการระบบปัญญาประดิษฐ์ กรมการขนส่งทางราง ระยะ ๕ ปี (พ.ศ. ๒๕๖๙ - ๒๕๗๓)

ส่วนที่ ๑ บทนำและบริบทเชิงยุทธศาสตร์ (Introduction and Strategic Context)

๑.๑ ความเป็นมาและความสำคัญ

โครงสร้างพื้นฐานระบบขนส่งทางรางของประเทศไทยกำลังขยายตัวอย่างก้าวกระโดด ทั้งระบบรถไฟฟ้าในเขตเมือง รถไฟทางคู่ และโครงการรถไฟความเร็วสูง กรมการขนส่งทางราง (ขร.) ในฐานะหน่วยงานส่วนกลางที่มีภารกิจในการเสนอแนะนโยบาย ยุทธศาสตร์ แผนการพัฒนา และกำกับดูแลมาตรฐานความปลอดภัยและการประกอบกิจการขนส่งทางราง จำเป็นต้องยกระดับขีดความสามารถในการบริหารจัดการข้อมูลและโครงข่ายขนส่งเทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence: AI) และปัญญาประดิษฐ์เชิงสร้างสรรค์ (Generative AI) ได้กลายเป็นเครื่องมือสำคัญในการขับเคลื่อนนวัตกรรมการบริหารภาครัฐและการขนส่งอัจฉริยะ (Smart Mobility) อย่างไรก็ตาม การประยุกต์ใช้ AI ในภารกิจระดับโครงสร้างพื้นฐานวิกฤต (Critical Infrastructure) จำเป็นต้องคำนึงถึงความเสี่ยงรอบด้าน ทั้งด้านเสถียรภาพ ความมั่นคงปลอดภัยไซเบอร์ ความเป็นส่วนตัวของข้อมูล และหลักธรรมาภิบาล เพื่อป้องกันผลกระทบอันอาจเกิดต่อความปลอดภัยในชีวิตและทรัพย์สินของประชาชน

๑.๒ วัตถุประสงค์

๑. เพื่อเป็นกรอบแนวทางเชิงยุทธศาสตร์และการปฏิบัติในการนำเทคโนโลยี AI มาใช้ยกระดับการบริหารราชการ การกำหนดนโยบาย และการกำกับดูแลระบบขนส่งทางรางของประเทศ

๒. เพื่อสร้างระบบบริหารจัดการและธรรมาภิบาลปัญญาประดิษฐ์ (AI Governance) ที่สอดคล้องกับมาตรฐานสากลและบริบทของกฎหมายไทย

๓. เพื่อสร้างกลไกการรักษาความมั่นคงปลอดภัยในการพัฒนาและใช้งาน AI ป้องกันภัยคุกคามไซเบอร์รูปแบบใหม่ที่มุ่งเป้ามายังระบบวิกฤตสารสนเทศทางการขนส่ง

๔. เพื่อพัฒนาศักยภาพบุคลากรและโครงสร้างพื้นฐานดิจิทัลของกรมการขนส่งทางรางให้พร้อมรองรับระบบขนส่งทางรางอัจฉริยะในอนาคต

๑.๓ กรอบแนวคิดและเอกสารอ้างอิงหลัก

แผนปฏิบัติการฉบับนี้จัดทำขึ้นโดยการบูรณาการหลักการสำคัญจากแนวทางการกำกับดูแลและรักษาความมั่นคงปลอดภัยระบบ AI ของประเทศไทย ๓ ฉบับหลัก ได้แก่

๑. แนวทางการประยุกต์ใช้ปัญญาประดิษฐ์อย่างมีธรรมาภิบาลสำหรับผู้บริหารองค์กร (AI Governance Guideline for Executive) ของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) มุ่งเน้นการจัดโครงสร้างองค์กร ความรับผิดชอบ (Accountability) ความโปร่งใส (Transparency) และความเป็นธรรม (Fairness)

๒. แนวทางการประยุกต์ใช้ Generative AI อย่างมีธรรมาภิบาลสำหรับองค์กร (Generative AI Governance Guideline for Organizations) ของ สพธอ. มุ่งเน้นการควบคุมความเสี่ยงเฉพาะของ Generative AI เช่น การรั่วไหลของข้อมูล (Data Leakage) ความถูกต้องของข้อมูล (Hallucination) และสิทธิ์ในทรัพย์สินทางปัญญา

๓. แนวปฏิบัติการใช้ปัญญาประดิษฐ์อย่างมั่นคงปลอดภัย ของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) มุ่งเน้นการรักษาความมั่นคงปลอดภัยตลอดวงจรชีวิตระบบ AI

(Secure AI Lifecycle) การป้องกันการโจมตีแบบ Adversarial Machine Learning และการบูรณาการร่วมกับระบบ Sectoral CERT

ส่วนที่ ๒ กรอบแนวคิดการบริหารจัดการและสถาปัตยกรรมธรรมาภิบาล AI ของ ขร. (Governance & Security Architecture)

๒.๑ โครงสร้างการกำกับดูแล (AI Governance Structure)

ขร. จัดตั้ง คณะกรรมการกำกับดูแลการประยุกต์ใช้ปัญญาประดิษฐ์ (AI Governance Council) โดยมีรองอธิบดีที่ได้รับมอบหมายเป็นประธาน และมีผู้อำนวยการกอง/กลุ่มงานที่เกี่ยวข้อง ร่วมเป็นกรรมการ โดยมีหน้าที่ ดังนี้

๑. กำหนดนโยบายและแนวปฏิบัติการใช้งาน AI และ Generative AI ของ ขร.

๒. อนุมัติการดำเนินโครงการจัดซื้อจัดจ้างระบบ AI ที่มีระดับความเสี่ยงสูง

๓. ตรวจสอบและประเมินผลกระทบด้านจริยธรรมและความปลอดภัยของระบบ AI เป็นรายปี

๒.๒ การจำแนกประเภทความเสี่ยงของระบบ AI ในภารกิจระบบราง

ขร. กำหนดเกณฑ์การประเมินความเสี่ยงระบบ AI ออกเป็น ๔ ระดับ เพื่อการควบคุมที่เหมาะสม ตามแนวทาง สพธอ. และ สกมช. ดังนี้

ระดับความเสี่ยง	คำจำกัดความตามบริบทระบบราง	ตัวอย่างระบบงาน	มาตรการควบคุมขั้นบังคับ
๑. Unacceptable Risk (ยอมรับไม่ได้)	ระบบ AI ที่ส่งผลกระทบโดยตรงต่อความปลอดภัยในชีวิตของประชาชน หรือละเมิดสิทธิขั้นพื้นฐานอย่างรุนแรง	ระบบควบคุมการเดินรถอัตโนมัติที่ไม่มีระบบ Manual สำรอง หรือระบบคัดกรองบุคคลเข้าสถานีด้วยอคติทางชาติพันธุ์	ห้ามใช้งาน หรือต้องระงับโครงการเพื่อทบทวนเชิงโครงสร้างทันที
๒. High Risk (ความเสี่ยงสูง)	ระบบ AI ที่ใช้ในโครงสร้างพื้นฐานวิกฤตการบังคับใช้กฎหมาย การวิเคราะห์ข้อมูลผู้โดยสารจำนวนมากหรือระบบที่มีผลต่อการตัดสินใจเชิงนโยบาย	- AI ตรวจสอบรอยร้าวของรางและระบบอาณัติสัญญาณ - AI วิเคราะห์สถิติอุบัติเหตุเพื่อกำหนดงบประมาณ - ระบบตั๋วร่วมอัจฉริยะ (EMV/ABT)	- ต้องผ่านการประเมิน AI Risk Assessment - มีกลไก Human-in-the-loop - ทดสอบความมั่นคงปลอดภัยตามแนวทาง สกมช.
๓. Limited Risk (ความเสี่ยงจำกัด)	ระบบ AI ที่ปฏิสัมพันธ์กับบุคคลทั่วไป หรือใช้ประมวลผลข้อมูลภายในที่ไม่กระทบต่อความปลอดภัยทางกายภาพ	- Chatbot ตอบคำถามประชาชนเกี่ยวกับเส้นทางและค่าโดยสาร - Generative AI สำหรับช่วยร่างเอกสารราชการภายใน	- ประกาศให้ผู้ใช้ทราบว่าเป็น AI (Transparency) - ห้ามใส่ข้อมูลชั้นความลับราชการ/ข้อมูลส่วนบุคคล (PDPA)
๔. Minimal Risk (ความเสี่ยงต่ำสุด)	ระบบ AI ที่ใช้สนับสนุนงานสำนักงานทั่วไปที่ไม่มีความเสี่ยงด้านความปลอดภัยหรือข้อมูลบุคคล	- ระบบคัดแยกคำผิดในเอกสาร - AI จัดตารางการประชุมอัจฉริยะ	- ปฏิบัติตามแนวปฏิบัติการใช้งานไอทีทั่วไปของ ขร.

ส่วนที่ ๓ แผนปฏิบัติการ ๕ ปี แยกตามระยะ

เพื่อให้เกิดการขับเคลื่อนที่เป็นรูปธรรม แผนปฏิบัติการจะแบ่งออกเป็น ๓ ระยะหลัก เริ่มตั้งแต่การวางรากฐานทางกฎหมายและนโยบาย การขยายผลสู่ระบบงานหลัก จนถึงการก้าวสู่การเป็นศูนย์กลางข้อมูลและนโยบายระบบรางที่ขับเคลื่อนด้วย AI อย่างสมบูรณ์

ระยะ	แผนดำเนินการ	เป้าหมายหลัก	ช่วงเวลา
ระยะที่ ๑ (ระยะสั้น)	การเตรียมความพร้อมด้านบุคลากรและระเบียบปฏิบัติ	บุคลากร ข้อมูล และระเบียบปฏิบัติ	ปีที่ ๑–๑.๕
ระยะที่ ๒ (ระยะกลาง)	การเริ่มนำระบบเข้าสู่กระบวนการทำงานจริง	นำร่องและบริหารความเสี่ยง	ปีที่ ๑.๕–๓
ระยะที่ ๓ (ระยะยาว)	การยกระดับประสิทธิภาพและการกำกับดูแลต่อเนื่อง	บูรณาการและตรวจสอบผลสัมฤทธิ์	ปีที่ ๔-๕

๓.๑ ระยะที่ ๑ การเตรียมความพร้อมด้านบุคลากรและระเบียบปฏิบัติ (ปีที่ ๑ – ๑.๕)

เป้าหมาย วางโครงสร้างการทำงาน สร้างความพร้อมของบุคลากร ข้อมูล และการกำกับดูแล

๑. การจัดตั้งกลไกขับเคลื่อน แต่งตั้งแต่งคณะกรรมการกำกับดูแลการประยุกต์ใช้ปัญญาประดิษฐ์ (AI Governance Council) เพื่อทำหน้าที่กำหนดนโยบาย คัดเลือกโครงการ และอนุมัติการนำ AI มาใช้ในหน่วยงาน พร้อมกำหนดผู้รับผิดชอบที่ชัดเจน

๒. จัดทำคู่มือมาตรฐานการปฏิบัติงาน (Standard Operating Procedures) ครอบคลุมกระบวนการจัดหา พัฒนา ทดสอบ และใช้งาน AI เพื่อให้ทุกหน่วยงานปฏิบัติในทิศทางเดียวกันและตรวจสอบได้

๓. การเตรียมความพร้อมของข้อมูล สำรวจและจัดระเบียบชุดข้อมูล (Data Audit & Cleaning) ในแต่ละหน่วยงาน โดยกำหนดมาตรฐานข้อมูล (Data Standards) และโครงสร้างการจัดเก็บที่รองรับการประมวลผลด้วย AI

๔. การประยุกต์ใช้ในงานวิชาการและนโยบาย ใช้ AI ในการจัดทำรายงานสถิติการขนส่งทางรางและการพยากรณ์ข้อมูลเบื้องต้นเพื่อประกอบการตัดสินใจของผู้บริหาร

๕. การเพิ่มทักษะการทำงานร่วมกับ AI จัดอบรมเชิงปฏิบัติการให้เจ้าหน้าที่รู้วิธีการใช้ AI ในการร่างเอกสาร สรุปรายงาน หรือวิเคราะห์ข้อมูลเบื้องต้น

๖. กำหนดกรอบจริยธรรม AI (AI Ethics Framework) และแนวทางการใช้ AI อย่างมีความรับผิดชอบ สอดคล้องกับมาตรฐานสากลและนโยบายภาครัฐ

๓.๒ ระยะที่ ๒: การเริ่มนำระบบเข้าสู่กระบวนการทำงานจริง (ปีที่ ๑.๕ - ๓)

เป้าหมาย ดำเนินโครงการนำร่อง บริหารความเสี่ยง และสร้างระบบกำกับดูแล AI ตลอดวงจรชีวิต

๑. การปรับปรุงกระบวนการบริการประชาชน นำระบบ AI มาช่วยในงานบริการข้อมูล เช่น Chatbot หรือระบบสืบค้นอัตโนมัติ เพื่อลดภาระงานประจำของเจ้าหน้าที่

๒. การกำกับดูแลตลอดวงจรชีวิต (Lifecycle Management) เริ่มใช้ระบบตรวจจับและทดสอบระบบ AI (Testing & Validation) ก่อนนำไปใช้งานจริง เพื่อให้มั่นใจว่าระบบทำงานได้ถูกต้องตามวัตถุประสงค์

๓. บังคับใช้ Human-in-the-Loop อย่างเข้มงวด โดยกำหนดให้เจ้าหน้าที่ผู้รับผิดชอบทบทวนและรับรองผลลัพธ์จาก AI ก่อนนำไปใช้ประกาศ เผยแพร่ หรืออ้างอิงทางราชการ

๔. พัฒนาระบบบันทึกการตัดสินใจ (Decision Log) และเส้นทาง Audit Trail เพื่อให้การใช้ AI ทุกครั้งสามารถตรวจสอบย้อนหลังได้อย่างโปร่งใส

๓.๓ ระยะที่ ๓ การยกระดับประสิทธิภาพและการกำกับดูแลต่อเนื่อง (ปีที่ ๔ - ๕)

เป้าหมาย เชื่อมโยงงานแบบบูรณาการ ตรวจสอบผลสัมฤทธิ์ และเสริมสร้างความมั่นคงปลอดภัย

๑. การเชื่อมโยงระบบงานระหว่างหน่วยงาน พัฒนาระบบแลกเปลี่ยนข้อมูลการวิเคราะห์ระหว่างหน่วยงานภายในและหน่วยงานภายนอกที่เกี่ยวข้อง ผ่านแพลตฟอร์มกลางที่รองรับ AI

๒. การติดตามผลและตรวจสอบการทำงาน (Monitoring & Audit) จัดตั้งระบบติดตามประสิทธิภาพของ AI (Performance Dashboard) เพื่อดูความแม่นยำและแจ้งเตือนเมื่อระบบเริ่มทำงานคลาดเคลื่อน

๓. การประเมินผลสัมฤทธิ์และพัฒนาต่อเนื่อง ประเมินความคุ้มค่าและผลกระทบของการใช้ AI ต่อภารกิจของกรมการขนส่งทางราง พร้อมปรับปรุงโมเดลและนโยบายให้ทันสมัยตามเทคโนโลยี

๔. การรักษาความมั่นคงปลอดภัยในการทำงาน พัฒนามาตรการรับมือเหตุการณ์ผิดปกติ (Incident Response Plan) ในกรณีที่ระบบ AI ขัดข้องหรือถูกโจมตีทางไซเบอร์

ส่วนที่ ๔ รายละเอียดแนวทางการดำเนินการตามกรอบธรรมาภิบาลและความมั่นคงปลอดภัย

เพื่อให้แผนปฏิบัติการข้างต้นมีรายละเอียดเทียบเท่าเอกสารแม่บทระดับประเทศ ขร. จึงกำหนดแนวทางการปฏิบัติตามหลักการสำคัญของ ๓ เอกสารอ้างอิงหลักไว้ ดังนี้

๔.๑ การประยุกต์ใช้ AI Governance Guideline for Executive (ETDA)

ขร. จะยึดหลักการ ๔ มิติหลักในการบริหารระบบ AI ดังนี้

๑. ความรับผิดชอบที่ตรวจสอบได้ (Accountability & Auditability)

- ทุกระบบ AI จะต้องระบุ “เจ้าของระบบงาน” (System Owner) เป็นข้าราชการระดับชำนาญการขึ้นไป เพื่อรับผิดชอบต่อผลลัพธ์ของ AI

- มีการเก็บบันทึกประวัติการทำงานของระบบ (System Logs) และข้อมูลที่ใช้ในการตัดสินใจของ AI ไว้อย่างน้อย ๑๐ ปี เพื่อรองรับการตรวจสอบย้อนหลังทางกฎหมาย

๒. ความเป็นธรรมและไม่เลือกปฏิบัติ (Fairness & Bias Mitigation)

- ในการวิเคราะห์ข้อมูลผู้โดยสารและการจัดบริการขนส่งมวลชน ขร. จะตรวจสอบชุดข้อมูลฝึกสอน (Training Data) เพื่อให้มั่นใจว่าจะไม่มีอคติหรือการเลือกปฏิบัติต่อกลุ่มบุคคลตามปัจจัยด้านรายได้ อายุ เพศ หรือความทุพพลภาพ

๓. ความโปร่งใสและการอธิบายได้ (Transparency & Explainability)

- ถ้าระบบ AI ถูกนำมาใช้ในการพิจารณาออกใบอนุญาตผู้ประจำหน้าที่รถไฟ/รถไฟฟ้า หรือการพิจารณาเปรียบเทียบปรับผู้ประกอบการขนส่งทางราง ระบบนั้นต้องพัฒนาบนสถาปัตยกรรมที่สามารถอธิบายเหตุผลทางตรรกะได้ (Explainable AI: XAI) ไม่เป็นกล่องดำ (Black Box)

๔. ความเป็นส่วนตัวและความปลอดภัยของข้อมูล (Data Privacy & Protection)

- การนำข้อมูลดิบจากระบบตั๋วร่วม (EMV/ABT) มาใช้งาน จะต้องผ่านกระบวนการแปลงข้อมูลเพื่อไม่ให้ระบุตัวบุคคลได้ (Anonymization) เสมอ เพื่อให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (PDPA)

๔.๒ การประยุกต์ใช้ Generative AI Governance Guideline (ETDA)

ในการประยุกต์ใช้ Generative AI ในงานสนับสนุนและการวิเคราะห์ข้อมูลราชการ ขร. กำหนดกรอบการควบคุมดังนี้

๑. มาตรการสกัดกั้นข้อมูลรั่วไหล (Data Leakage Prevention) ขร. จะทำการบล็อกการเข้าถึงเว็บไซด์บริการ Generative AI สาธารณะที่ไม่ระบุเงื่อนไขการคุ้มครองข้อมูลผู้ใช้ สัญญาว่าจะไม่นำข้อมูลของ ขร. ไปใช้เทรนโมเดลต่อ

๒. การตรวจสอบความถูกต้องและข้อเท็จจริง (Fact-Checking Workflow) กำหนดให้ผลลัพธ์ใดๆ ที่ได้จาก Generative AI ไม่ว่าจะเป็นการสรุปข้อกฎหมาย การร่างหนังสือราชการ หรือการวิเคราะห์สถิติต่างๆ จะต้องได้รับการตรวจสอบ คัดกรอง และลงนามกำกับโดยเจ้าหน้าที่ที่เป็นมนุษย์เสมอ (Human-in-the-loop) ห้ามมิให้ส่งต่อผลลัพธ์จาก AI เข้าสู่กระบวนการพิจารณาโดยตรง

๓. การเคารพทรัพย์สินทางปัญญา (Intellectual Property Protection) ในการใช้ Generative AI สร้างสรรค์ภาพสื่อประชาสัมพันธ์ หรือโค้ดโปรแกรมสารสนเทศ เจ้าหน้าที่ต้องตรวจสอบที่มาและข้อกำหนดสิทธิ์ (Licensing) เพื่อป้องกันการละเมิดลิขสิทธิ์ของบุคคลภายนอก

๔.๓ การประยุกต์ใช้แนวปฏิบัติการใช้ AI อย่างมั่นคงปลอดภัย (สกมช.)

เพื่อปกป้องระบบไอทีและระบบควบคุมการเดินรถซึ่งถือเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) ขร. จะดำเนินการตามวงจรชีวิต AI ที่มั่นคงปลอดภัย (Secure AI Lifecycle) ดังนี้

๑. Securing the Training Data ในโครงการที่ ขร. ต้องพัฒนาโมเดลเอง เช่น ตรวจจับภาพวัตถุกีดขวางทางรถไฟ ชุดข้อมูลรูปภาพทั้งหมดต้องผ่านการตรวจสอบความถูกต้องทางดิจิทัล (Digital Signature) เพื่อให้มั่นใจว่าไม่ถูกแทรกแซงหรือปรับเปลี่ยนภาพโดยผู้ไม่หวังดี (Data Poisoning Mitigation)

๒. Model Hardening and Adversarial Defense ระบบ AI สำหรับภารกิจวิกฤตจะต้องได้รับการทดสอบด้วยเทคนิค Adversarial Testing เช่น การใส่สัญญาณรบกวน (Noise) เข้าไปในข้อมูลนำเข้า เพื่อดูว่าระบบยังคงตัดสินใจได้ถูกต้องหรือไม่ และมีการวางระบบสำรอง (Fail-Safe Rule-Based System) ที่จะเข้าควบคุมการทำงานทันทีหากโมเดล AI เกิดสภาวะล้มเหลวหรือไม่เสถียร

๓. Access Control & Continuous Monitoring การเข้าถึงระบบจัดการโมเดล AI (MLOps Platform) ต้องใช้การพิสูจน์ตัวตนแบบหลายปัจจัย (Multi-factor Authentication) และสิทธิ์ขั้นต่ำที่จำเป็น (Principle of Least Privilege) พร้อมระบบเฝ้าระวังความผิดปกติของ Input/Output ของ AI สม่ำเสมอ

ส่วนที่ ๕ แผนผังการดำเนินงานรายปี (Implementation Roadmap)

เพื่อให้สามารถติดตามความก้าวหน้าของแผนปฏิบัติการได้อย่างมีประสิทธิภาพ จึงสรุปกิจกรรมหลัก งบประมาณโดยประมาณ และหน่วยงานรับผิดชอบหลักไว้ในตาราง ดังต่อไปนี้

ปีที่	กิจกรรมหลัก	ผลลัพธ์ที่คาดหวัง	แนวทางอ้างอิง	หน่วยงานรับผิดชอบ
ปีที่ ๑ – ๑.๕ (๒๕๖๙-๒๕๗๐)	๑. จัดตั้งคณะกรรมการกำกับดูแลการประยุกต์ใช้ปัญญาประดิษฐ์ (AI Governance Council)	๑. คำสั่งแต่งตั้งคณะกรรมการกำกับดูแลการประยุกต์ใช้ปัญญาประดิษฐ์ (AI Governance Council)	- ETDA Executive Guideline - ETDA GenAI Guideline	คณะกรรมการกำกับดูแลการประยุกต์ใช้ปัญญาประดิษฐ์ (AI Governance Council)/ กยร. ฝ่ายเลขานุการ
	๒. จัดทำคู่มือมาตรฐานการปฏิบัติงาน (Standard Operating Procedures)	๒. คู่มือมาตรฐานการปฏิบัติงาน (Standard Operating Procedures)		
	๓. การเตรียมความพร้อมของข้อมูล สำรวจและจัดระเบียบชุดข้อมูล (Data Audit & Cleaning) ในแต่ละหน่วยงาน โดยกำหนดมาตรฐานข้อมูล (Data Standards) และโครงสร้างการจัดเก็บที่รองรับการประมวลผลด้วย AI	๓.๑ กำหนดมาตรฐานข้อมูล ๓.๒ กำหนดโครงสร้างการจัดเก็บ		
	๔. การประยุกต์ใช้ในงานวิชาการและนโยบาย ใช้ AI ในการจัดทำรายงานสถิติการขนส่งทางรางและการพยากรณ์ข้อมูลเบื้องต้นเพื่อประกอบการตัดสินใจของผู้บริหาร	๔. มีการนำ AI มาช่วยทำงาน		
	๕. แผนจัดอบรมเชิงปฏิบัติการให้บุคลากรวิธีการใช้ AI	๕. บุคลากรผ่านการอบรม > ๘๐%		สลร.สท./กยร.ยส.
	๖. กำหนดกรอบจริยธรรม AI (AI Ethics Framework) และแนวทางการใช้ AI อย่างมีความรับผิดชอบ สอดคล้องกับมาตรฐานสากลและนโยบายภาครัฐ	๖.๑ กรอบจริยธรรม AI (AI Ethics Framework) ๖.๒ แนวทางการใช้ AI อย่างมีความรับผิดชอบ		

ปีที่	กิจกรรมหลัก	ผลลัพธ์ที่คาดหวัง	แนวทางอ้างอิง	หน่วยงานรับผิดชอบ
ปีที่ ๑.๕ - ๓ (๒๕๗๐-๒๕๗๑)	๑. นำระบบ AI มาช่วยในงานบริการข้อมูล	๑. แพลตฟอร์มที่ช่วยในงานบริการข้อมูล	- ETDA Executive Guideline - ETDA GenAI Guideline	คณะกรรมการกำกับดูแลการประยุกต์ใช้ปัญญาประดิษฐ์ (AI Governance Council)/ กยร. ฝ่ายเลขานุการ
	๒. เริ่มใช้ระบบตรวจรับและทดสอบระบบ AI (Testing & Validation) ก่อนนำไปใช้งานจริง	๓. แพลตฟอร์มระบบตรวจรับและทดสอบระบบ AI		
	๓. กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบทบทวนและรับรองผลลัพธ์จาก AI ก่อนนำไปใช้ประกาศ เผยแพร่ หรืออ้างอิงทางราชการ	๔. มีการกำหนดเจ้าที่ผู้รับผิดชอบอย่างชัดเจน		
	๔. พัฒนาระบบบันทึกการตัดสินใจ (Decision Log) และเส้นทาง Audit Trail	๕. แพลตฟอร์มระบบบันทึกการตัดสินใจและเส้นทาง Audit Trail		
ปีที่ ๕ (๒๕๗๒-๒๕๗๓)	๑. การเชื่อมโยงระบบงานระหว่างหน่วยงาน พัฒนาระบบแลกเปลี่ยนข้อมูลการวิเคราะห์ระหว่างหน่วยงาน	๑. แพลตฟอร์มกลางสำหรับการเชื่อมโยงข้อมูล		
	๒. การติดตามผลและตรวจสอบการทำงาน (Monitoring & Audit) จัดตั้งระบบติดตามประสิทธิภาพของ AI (Performance Dashboard)	๒. แพลตฟอร์มระบบติดตามประสิทธิภาพของ AI (Performance Dashboard)		
	๓. การประเมินผลสัมฤทธิ์และพัฒนาต่อเนื่อง ประเมินความคุ้มค่าและผลกระทบของการใช้ AI ต่อภารกิจของกรมการขนส่งทางราง พร้อมปรับปรุงโมเดลและนโยบายให้ทันสมัยตามเทคโนโลยี	๓. รายงานผลผลสัมฤทธิ์และพัฒนาประเมินความคุ้มค่าและผลกระทบของการใช้ AI ต่อภารกิจของ ขร.		
	๔. การรักษาความมั่นคงปลอดภัยในการทำงาน พัฒนามาตรการรับมือเหตุการณ์ผิดปกติ (Incident Response Plan) ในกรณีที่ระบบ AI ขัดข้องหรือถูกโจมตีทางไซเบอร์	๔. จัดทำมาตราการรับมือเหตุการณ์ผิดปกติในกรณีที่ระบบ AI ขัดข้องหรือถูกโจมตีทางไซเบอร์		

ส่วนที่ ๖ ตัวชี้วัดความสำเร็จและการบริหารความเสี่ยง (KPIs and Risk Management)

การประเมินความสำเร็จของการดำเนินงานตามแผนปฏิบัติการ ๕ ปี จะวัดจาก ๓ มิติหลัก ดังนี้

๑. มิติด้านธรรมาภิบาลและการปฏิบัติตามเกณฑ์ (Governance & Compliance)

- KPI ๑: ร้อยละ ๑๐๐ ของระบบ AI ระดับความเสี่ยงสูง (High Risk) ต้องได้รับการประเมินผลกระทบด้านธรรมาภิบาลและผ่านการอนุมัติจาก AI Governance Council ก่อนการติดตั้งใช้งาน

- KPI ๒: อัตราการเกิดเหตุการณ์ข้อมูลราชการรั่วไหลผ่านระบบ Generative AI สาธารณะเป็น **ศูนย์ (๐ ครั้ง)** ตลอดระยะเวลาของแผน

๒. มิติด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity & Resilience)

- KPI ๓: ระบบ AI ที่จัดเป็นโครงสร้างพื้นฐานสารสนเทศวิกฤต (CII) ต้องผ่านการทดสอบ Vulnerability Assessment และ Penetration Testing และได้รับการปิดช่องโหว่ระดับวิกฤต (Critical Vulnerabilities) ร้อยละ ๑๐๐ ภายใน ๖๐ วันหลังตรวจพบ

- KPI ๔: เวลาที่ใช้ในการตรวจจับและตอบสนองต่อภัยคุกคามไซเบอร์บนระบบ AI (Mean Time to Detect and Respond) ผ่านระบบเชื่อมโยง Rail Sectoral CERT ต้องลดลงไม่น้อยกว่าร้อยละ ๓๐ ภายในปี พ.ศ. ๒๕๗๓

๓. มิติด้านผลกระทบต่อภารกิจและการพัฒนาบุคลากร (Impact & Capacity Building)

- KPI ๕: ความแม่นยำของระบบ AI นำร่องต้องไม่ต่ำกว่าร้อยละ ๘๕

- KPI ๖: บุคลากรของกรมการขนส่งทางรางในกลุ่มวิชาการคอมพิวเตอร์และนโยบาย ได้รับการพัฒนาทักษะเฉพาะด้านการบริหารจัดการและการรักษาความปลอดภัย AI ไม่น้อยกว่า ๑ หลักสูตรต่อคนต่อปี

ส่วนที่ ๗ ปัจจัยความสำเร็จในการปฏิบัติงาน

๑. การสนับสนุนจากผู้บริหาร เพื่อให้นโยบายการนำ AI มาใช้ได้รับงบประมาณและทรัพยากรที่เพียงพอ

๒. ความเชื่อมโยงของข้อมูล ข้อมูลในทุกหน่วยงานต้องถูกต้อง เป็นปัจจุบัน และมีโครงสร้างที่มาตรฐาน พร้อมกำหนดผู้รับผิดชอบด้านข้อมูล (Data Steward) ในแต่ละหน่วยงาน

๓. การทำงานร่วมกันอย่างใกล้ชิด ระหว่างบุคลากรผู้ใช้งานจริงและเจ้าหน้าที่ผู้พัฒนาระบบเพื่อให้ AI ตอบโจทย์การทำงานจริง

๔. ความยืดหยุ่นของระเบียบปฏิบัติ สามารถปรับปรุงขั้นตอนการทำงานได้ตามพัฒนาการของเทคโนโลยี

๕. การกำกับดูแลด้านจริยธรรมและความปลอดภัย มีกลไกทบทวนด้านจริยธรรม AI อย่างต่อเนื่อง เพื่อป้องกันความเสี่ยงด้านความลำเอียง ความเป็นส่วนตัว และผลกระทบที่อาจเกิดขึ้น

.....