

ประกาศสถาบันข้อมูลขนาดใหญ่ (องค์การมหาชน)  
เรื่อง นโยบายธรรมาภิบาลปัญญาประดิษฐ์

โดยที่เทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence) เป็นกลไกสำคัญในการเพิ่มประสิทธิภาพการบริหารงานและการให้บริการภาครัฐให้มีความแม่นยำและรวดเร็ว อย่างไรก็ตาม การประยุกต์ใช้เทคโนโลยีดังกล่าวจำเป็นต้องคำนึงถึงความเสี่ยง ผลกระทบด้านจริยธรรม ความโปร่งใส และความรับผิดชอบต่อสังคม เพื่อสร้างความเชื่อมั่นในการใช้งานและคุ้มครองสิทธิของประชาชน

เพื่อให้การดำเนินงานด้านปัญญาประดิษฐ์ของสถาบันข้อมูลขนาดใหญ่ (องค์การมหาชน) สอดคล้องกับแนวปฏิบัติจริยธรรมปัญญาประดิษฐ์ (Thailand AI Ethics Guideline) และแผนปฏิบัติการด้านปัญญาประดิษฐ์แห่งชาติเพื่อการพัฒนาประเทศไทย (พ.ศ. ๒๕๖๕ – ๒๕๗๐) รวมถึงมาตรฐานสากลด้านธรรมาภิบาลปัญญาประดิษฐ์ที่มุ่งเน้นความยุติธรรม การปราศจากอคติ และความมั่นคงปลอดภัยไซเบอร์ ประกอบกับพระราชบัญญัติการบริการงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ ที่มุ่งเน้นการบูรณาการข้อมูลและการทำงานภาครัฐอย่างมีธรรมาภิบาล

อาศัยอำนาจตามความในมาตรา ๒๘ แห่งพระราชกฤษฎีกาจัดตั้งสถาบันข้อมูลขนาดใหญ่ (องค์การมหาชน) พ.ศ. ๒๕๖๖ ประกอบกับมติที่ประชุมคณะทำงานธรรมาภิบาลข้อมูลและปัญญาประดิษฐ์ การคุ้มครองข้อมูลส่วนบุคคล และการรักษาความมั่นคงปลอดภัยทางไซเบอร์ เมื่อวันที่ ๑๕ มกราคม ๒๕๖๙ และมติที่ประชุมผู้บริหารระดับสูงสถาบันข้อมูลขนาดใหญ่ ครั้งที่ ๙/๒๕๖๙ เมื่อวันที่ ๑๐ มีนาคม ๒๕๖๙ จึงประกาศนโยบายธรรมาภิบาลปัญญาประดิษฐ์ เพื่อใช้สำหรับยึดถือปฏิบัติภายในสถาบันข้อมูลขนาดใหญ่ (องค์การมหาชน) รายละเอียดปรากฏตามเอกสารแนบท้ายประกาศนี้

จึงประกาศให้ทราบโดยทั่วกัน

ประกาศ ณ วันที่ ๘ มิถุนายน พ.ศ. ๒๕๖๙

(ศาสตราจารย์ธีรณี อจลากุล)

ผู้อำนวยการสถาบันข้อมูลขนาดใหญ่



# นโยบายธรรมาภิบาลปัญญาประดิษฐ์ (AI Governance Policy)

## 1: บทนำ

สถาบันข้อมูลขนาดใหญ่ (องค์การมหาชน) หรือ สขญ. เล็งเห็นถึงศักยภาพของเทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence: AI) ในการยกระดับประสิทธิภาพการดำเนินงานภาครัฐ ทั้งด้านการวิเคราะห์ข้อมูลขนาดใหญ่ การสนับสนุนการตัดสินใจเชิงนโยบาย และการเพิ่มคุณภาพการให้บริการประชาชน ดังนั้น การนำปัญญาประดิษฐ์มาใช้ภายในองค์กร จึงต้องตระหนักถึงจริยธรรม ความปลอดภัย และผลกระทบต่อสังคม

สขญ. จึงจัดทำนโยบายธรรมาภิบาลปัญญาประดิษฐ์ (AI Governance Policy) ฉบับนี้ขึ้น เพื่อเป็นกรอบการกำกับดูแลการนำปัญญาประดิษฐ์มาใช้ในการปฏิบัติงานขององค์กรได้อย่างมีประสิทธิภาพ และมีความรับผิดชอบต่อองค์กร ผู้มีส่วนเกี่ยวข้อง และสังคมโดยรวม โดยยึดหลักจริยธรรมปัญญาประดิษฐ์ (AI Ethics Principles) การปฏิบัติให้สอดคล้องกับกฎหมายและข้อกำหนดที่เกี่ยวข้อง (Laws and Regulations) รวมถึงการบริหารจัดการความเสี่ยงและผลกระทบที่อาจเกิดขึ้นจากการใช้ปัญญาประดิษฐ์อย่างเหมาะสม (AI Risk and Impact Management)

## 2: วัตถุประสงค์ของนโยบาย

นโยบายธรรมาภิบาลปัญญาประดิษฐ์ฉบับนี้จัดทำขึ้นเพื่อกำหนดทิศทาง กลไกการกำกับดูแล และแนวปฏิบัติที่เป็นมาตรฐานสำหรับการพัฒนา การนำไปใช้ และการบริหารจัดการระบบปัญญาประดิษฐ์ของ สขญ. โดยมีวัตถุประสงค์ดังต่อไปนี้

- เพื่อกำหนดหลักเกณฑ์และมาตรฐานในการบริหารจัดการการใช้ปัญญาประดิษฐ์ ของ สขญ. ให้สอดคล้องกับหลักจริยธรรมและกฎหมายที่เกี่ยวข้อง
- เพื่อระบุความรับผิดชอบของบุคลากรที่เกี่ยวข้องในการกำกับดูแลระบบปัญญาประดิษฐ์
- เพื่อบริหารจัดการความเสี่ยงที่อาจเกิดขึ้นจากการใช้ปัญญาประดิษฐ์ รวมถึงการคุ้มครองสิทธิขั้นพื้นฐานและความเป็นส่วนตัวของเจ้าของข้อมูล
- เพื่อส่งเสริมวัฒนธรรมการใช้ปัญญาประดิษฐ์อย่างสร้างสรรค์ ปลอดภัย และมีธรรมาภิบาลภายในองค์กร

### 3: ขอบเขตการบังคับใช้

นโยบายธรรมาภิบาลปัญญาประดิษฐ์ฉบับนี้ มีผลบังคับใช้กับผู้ปฏิบัติงานของ สขญ. รวมถึงบุคคลหรือหน่วยงานภายนอก ที่เกี่ยวข้องกับการพัฒนาและการใช้งานระบบปัญญาประดิษฐ์ของ สขญ. โดยครอบคลุมดังต่อไปนี้

#### 3.1 บุคคลและหน่วยงานที่อยู่ภายใต้ขอบเขตนโยบาย

นโยบายฉบับนี้ใช้บังคับกับบุคคลทุกประเภทที่เกี่ยวข้องกับการดำเนินงานด้านปัญญาประดิษฐ์ของ สขญ. ซึ่งในนโยบายนี้จะเรียกว่า “ผู้ใช้งาน” ได้แก่

- 1) ผู้ปฏิบัติงานทุกระดับของ สขญ. ได้แก่ ผู้บริหาร เจ้าหน้าที่ ที่ปรึกษา ผู้เชี่ยวชาญหรือลูกจ้าง
- 2) ผู้รับจ้าง ผู้พัฒนาระบบ ผู้ให้บริการ และคู่ค้าทางเทคโนโลยี ที่ให้บริการหรือปฏิบัติงานเกี่ยวข้องกับระบบปัญญาประดิษฐ์ในทุกส่วนงานของ สขญ.
- 3) บุคคลหรือหน่วยงานอื่นใด ที่เข้าถึงข้อมูล ทรัพยากร หรือระบบที่เกี่ยวข้องกับเทคโนโลยี AI ของ สขญ.

#### 3.2 ระบบปัญญาประดิษฐ์ที่อยู่ภายใต้ขอบเขตนโยบาย

นโยบายฉบับนี้ครอบคลุมระบบปัญญาประดิษฐ์ทุกประเภท ไม่ว่าจะผ่านการพัฒนาเองโดย สขญ. หรือจัดหาจากผู้ให้บริการภายนอก ระบบปัญญาประดิษฐ์ที่ให้บริการผ่านคลาวด์ ระบบปัญญาประดิษฐ์ที่บูรณาการเข้ากับระบบเดิมของ สขญ. ครอบคลุมถึงข้อมูล กระบวนการทำงาน ระบบงาน หรือแพลตฟอร์มใด ๆ ที่ใช้เทคโนโลยีปัญญาประดิษฐ์หรือมีการเชื่อมโยงหรือบูรณาการกับระบบปัญญาประดิษฐ์ หรือการดำเนินการอาจได้รับผลกระทบจากการใช้ปัญญาประดิษฐ์ ในการประมวลผล ตัดสินใจ หรือให้บริการ โดยรวมถึงแต่ไม่จำกัดเฉพาะ

- Machine Learning และแบบจำลองเชิงพยากรณ์ (Predictive Models)
- Natural Language Processing (NLP)
- Computer Vision
- ระบบหุ่นยนต์หรือระบบอัตโนมัติที่ใช้ปัญญาประดิษฐ์ (Robotics/Automation)
- ระบบสนับสนุนการตัดสินใจ (Decision Support Systems)
- เครื่องมือ AI สำหรับการใช้งานภายใน สขญ. (Internal AI Tools)
- Generative AI

### 4: โครงสร้างการกำกับดูแลด้านปัญญาประดิษฐ์

สขญ. กำหนดให้การกำกับดูแลด้านปัญญาประดิษฐ์เป็นภารกิจสำคัญระดับองค์กร โดยมีโครงสร้างการกำกับดูแลผ่านคณะทำงานด้านธรรมาภิบาลข้อมูลและปัญญาประดิษฐ์ การคุ้มครองข้อมูลส่วนบุคคล

และการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (“คณะทำงาน”) ซึ่งได้รับมอบหมายให้ทำหน้าที่กำกับดูแลเทคโนโลยีปัญญาประดิษฐ์ในทุกมิติอย่างครอบคลุม และมีหน้าที่รายงานการดำเนินการที่มีนัยสำคัญหรือผลกระทบที่สำคัญต่อคณะผู้บริหารระดับสูง (TopEX)

โดยคณะทำงานฯ ประกอบด้วยผู้บริหารระดับสูง ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (DCIO) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO) ผู้เชี่ยวชาญเฉพาะด้านที่จำเป็น ผู้แทนจากฝ่าย/ส่วนงาน และมีเลขานุการ/ผู้ช่วยเลขานุการที่ทำหน้าที่ประสานงานและสนับสนุนการดำเนินงานให้เป็นไปตามมติและแนวทางของคณะทำงานฯ อย่างมีประสิทธิภาพและต่อเนื่อง

#### 4.1 บทบาทและความรับผิดชอบของคณะทำงานฯ

คณะทำงานชุดนี้ทำหน้าที่เป็นกลไกกำกับดูแลด้านปัญญาประดิษฐ์ของ สขญ. โดยมีหน้าที่และความรับผิดชอบในการกำหนดนโยบายและแนวทางการบริหารจัดการเกี่ยวกับการใช้ปัญญาประดิษฐ์ตลอดวงจรชีวิตของระบบปัญญาประดิษฐ์ของ สขญ. รวมถึงการจัดทำมาตรฐาน แนวปฏิบัติ หลักเกณฑ์ด้านเทคนิคและการบริหารจัดการ เพื่อให้การใช้ปัญญาประดิษฐ์เป็นไปอย่างปลอดภัย มีความรับผิดชอบ ตรวจสอบได้ และสอดคล้องกับภารกิจและกฎหมายที่เกี่ยวข้อง

#### 4.2 การกำกับติดตามและการประเมินผล

- 1) สขญ. ให้ความสำคัญกับการกำกับดูแลการใช้ปัญญาประดิษฐ์ของ สขญ. ให้สอดคล้องกับกรอบธรรมาภิบาลข้อมูล การคุ้มครองข้อมูลส่วนบุคคล และการรักษาความมั่นคงปลอดภัยทางไซเบอร์ เพื่อป้องกันความเสี่ยงที่เกี่ยวข้องกับ ข้อมูลส่วนบุคคล ข้อมูลสำคัญของ สขญ. และภัยคุกคามทางไซเบอร์
- 2) มีการกำหนดมาตรการในการตรวจทานและกำกับดูแลการใช้ปัญญาประดิษฐ์ ทั้งในเชิงนโยบายและการปฏิบัติ เพื่อให้มั่นใจว่าทุกส่วนงานภายในองค์กรต้องปฏิบัติตามหลักธรรมาภิบาลปัญญาประดิษฐ์ที่ สขญ. กำหนดไว้ และมีการบริหารจัดการความเสี่ยงอย่างรอบด้าน
- 3) จัดให้มีระบบติดตาม ประเมินผล และรายงานผลการดำเนินงานด้าน AI Governance ทั้งในมิติความเสี่ยง ประสิทธิภาพ และผลกระทบ เพื่อสนับสนุนการตัดสินใจของผู้บริหาร และเสริมสร้างความโปร่งใสในการใช้ปัญญาประดิษฐ์ ภายใน สขญ.

### 5: นโยบายธรรมาภิบาลปัญญาประดิษฐ์ (AI Governance Policy)

การพัฒนา จัดทำ ประยุกต์ใช้ และบริหารจัดการระบบปัญญาประดิษฐ์ของ สขญ. ต้องคำนึงถึงหลักการที่สำคัญในทุกกระบวนการที่เกี่ยวข้อง ดังต่อไปนี้

- 1) **ความเป็นธรรม (Fairness):** การพัฒนาและใช้งานปัญญาประดิษฐ์ต้องดำเนินการอย่างเป็นกลาง เป็นธรรม และไม่เลือกปฏิบัติ โดยต้องพิจารณาและลดความเสี่ยงจากอคติ (Bias) ที่อาจเกิดจากการใช้ปัญญาประดิษฐ์

- 2) **ความโปร่งใส (Transparency & Explainability):** ต้องเปิดเผยการใช้ปัญญาประดิษฐ์อย่างเหมาะสม โดยเฉพาะกรณีที่ปัญญาประดิษฐ์มีผลต่อการให้บริการ การวิเคราะห์ การให้คำแนะนำ หรือการตัดสินใจที่เกี่ยวข้องกับบุคคลหรือสาธารณะ เพื่อให้ผู้เกี่ยวข้องสามารถเข้าใจ ตรวจสอบ หรือขอคำอธิบายได้ตามความเหมาะสม
- 3) **ความรับผิดชอบ (Accountability):** ต้องคำนึงถึงความรับผิดชอบต่อผลการนำผลลัพธ์จากปัญญาประดิษฐ์ไปใช้ในการปฏิบัติงาน โดยถือว่าปัญญาประดิษฐ์ไม่สามารถเป็นผู้รับผิดชอบแทนมนุษย์ได้ และก่อนนำผลลัพธ์ไปใช้ต้องตรวจสอบความถูกต้อง ความเหมาะสม และความสอดคล้องกับข้อเท็จจริง กฎหมาย ระเบียบ และนโยบายขององค์กร รวมถึงควรเก็บหลักฐานหรือบันทึกที่จำเป็น เช่น แหล่งที่มาของข้อมูล วิธีการใช้งาน หรือผลลัพธ์ที่นำไปใช้ เพื่อให้สามารถตรวจสอบย้อนหลังได้ (Auditability) เมื่อจำเป็น
- 4) **ความมั่นคงปลอดภัย (Safety & Security):** การใช้งานระบบหรือเครื่องมือปัญญาประดิษฐ์ต้องคำนึงถึงการรักษาความมั่นคงปลอดภัย และต้องปฏิบัติตามมาตรการด้านความมั่นคงปลอดภัยที่องค์กรกำหนดอย่างเคร่งครัด และห้ามใช้ปัญญาประดิษฐ์ในลักษณะที่อาจทำให้ระบบข้อมูล หรือทรัพยากรขององค์กรเกิดความเสียหาย รั่วไหล ถูกเข้าถึงโดยไม่ได้รับอนุญาต หรือถูกนำไปใช้ผิดวัตถุประสงค์ หากพบความผิดปกติของระบบ ผลลัพธ์ที่อาจเป็นอันตราย หรือเหตุการณ์ด้านความปลอดภัยต้องรายงานส่วนงานหรือผู้ที่เกี่ยวข้องโดยเร็ว
- 5) **การคุ้มครองข้อมูลส่วนบุคคล (Privacy Protection):** การใช้ข้อมูลในระบบปัญญาประดิษฐ์ต้องเป็นไปตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล นโยบายธรรมาภิบาลข้อมูล และข้อกำหนดด้านความมั่นคงปลอดภัยขององค์กร โดยต้องใช้ข้อมูลเท่าที่จำเป็น มีวัตถุประสงค์ที่ชัดเจน ควบคุมการเข้าถึง ลดการระบุตัวตน หรือขจัดตัวตนของข้อมูลตามความเหมาะสม ทั้งนี้ ต้องคำนึงถึงความปลอดภัยของข้อมูลตลอดวงจรชีวิตของระบบปัญญาประดิษฐ์
- 6) **ความเป็นมนุษย์เป็นศูนย์กลาง (Human-Centric AI):** การใช้ปัญญาประดิษฐ์ต้องยึดถือศักดิ์ศรี สิทธิ เสรีภาพ ความปลอดภัย และประโยชน์ของมนุษย์เป็นสำคัญ ต้องจัดให้มีการกำกับดูแลโดยมนุษย์ในระดับที่เหมาะสม และไม่ใช้ผลลัพธ์จากระบบปัญญาประดิษฐ์เป็นข้อสรุปสุดท้ายโดยปราศจากการพิจารณาของมนุษย์
- 7) **ประสิทธิภาพและความยั่งยืน (Efficiency & Sustainability):** การพัฒนาและใช้งานปัญญาประดิษฐ์ต้องคำนึงถึงความจำเป็น ความเหมาะสม ความคุ้มค่า และประสิทธิภาพในการใช้ทรัพยากรขององค์กร รวมถึงผลกระทบต่อผู้มีส่วนเกี่ยวข้อง สังคม และสิ่งแวดล้อม ทั้งนี้ องค์กรต้องทบทวนและประเมินผลการใช้ปัญญาประดิษฐ์ เพื่อให้มั่นใจว่าใช้งานปัญญาประดิษฐ์ยังคงเหมาะสม ปลอดภัย เกิดคุณค่าตามวัตถุประสงค์ และไม่ก่อให้เกิดผลกระทบเกินกว่าระดับที่องค์กรยอมรับได้

นอกจากนี้ ในการกำกับดูแลปัญญาประดิษฐ์ควรคำนึงถึงการกำกับดูแลตามมาตรฐานสากล ได้แก่ OECD AI Principles, UNESCO Recommendation on the Ethics of AI, NIST AI Risk Management Framework รวมถึงแนวทางกำกับดูแลด้านปัญญาประดิษฐ์ของประเทศไทย เพื่อใช้เป็นกรอบกำกับดูแลการพัฒนา การจัดหา และการใช้ปัญญาประดิษฐ์ของ สสว. ให้เป็นไปอย่างปลอดภัย โปร่งใส และรับผิดชอบ

## 6: ข้อปฏิบัติในการใช้งานปัญญาประดิษฐ์สำหรับบุคคลที่อยู่ภายใต้ขอบเขตนโยบายนี้

เพื่อให้การพัฒนา จัดทำ ประยุกต์ใช้ และบริหารจัดการระบบปัญญาประดิษฐ์ของ สขญ. เป็นไปอย่างปลอดภัย โปร่งใส ตรวจสอบได้ และคำนึงถึงสิทธิของประชาชน ผู้ปฏิบัติงานและบุคคลที่อยู่ภายใต้ขอบเขตของนโยบายนี้ต้องปฏิบัติตามข้อปฏิบัติในการใช้งานปัญญาประดิษฐ์ ดังต่อไปนี้

- 1) ผู้ใช้งานต้องมีการตรวจสอบและประเมินผลลัพธ์ก่อนนำไปใช้งาน (Human Oversight Requirement ) ห้ามใช้ผลลัพธ์จากระบบปัญญาประดิษฐ์เป็นข้อสรุปขั้นสุดท้ายโดยปราศจากการพิจารณาหรือการกำกับดูแลโดยมนุษย์ โดยเฉพาะกรณีที่มีผลกระทบต่อสิทธิ เสรีภาพ สวัสดิภาพ หรือสถานะของประชาชน และต้องตรวจสอบแหล่งที่มาและอ้างอิงข้อมูลอย่างเหมาะสม
- 2) ห้ามใช้ระบบปัญญาประดิษฐ์สร้างหรือเผยแพร่ข้อมูลที่ขัดต่อกฎหมาย จริยธรรม หรือระเบียบของหน่วยงาน เช่น ข้อมูลเท็จ ข่าวดปลอม หรือข้อมูลบิดเบือน เนื้อหาอันเป็นการหมิ่นประมาท ดูหมิ่น หรือสร้างความเสียหายแก่บุคคลอื่น เนื้อหาที่เข้าข่ายละเมิดลิขสิทธิ์ ทรัพย์สินทางปัญญา หรือข้อมูลที่มีข้อจำกัดทางกฎหมาย เนื้อหาที่อาจก่อให้เกิดความแตกแยก ความเกลียดชัง หรือการเลือกปฏิบัติ
- 3) ห้ามบ่อน เปิดเผย อัปโหลด หรือส่งต่อข้อมูลส่วนบุคคล ข้อมูลอ่อนไหว ข้อมูลภายในของ สขญ. ข้อมูลลับราชการ ข้อมูลเชิงยุทธศาสตร์ หรือข้อมูลที่มีข้อจำกัดทางกฎหมายเข้าสู่ระบบปัญญาประดิษฐ์ที่ไม่ใช่ระบบที่ สขญ. จัดทำไว้ให้หรือไม่ได้อนุมัติ ทั้งนี้ การใช้ข้อมูลกับระบบปัญญาประดิษฐ์ต้องเป็นไปตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ และกฎหมาย ระเบียบ หรือนโยบายที่เกี่ยวข้องอย่างเคร่งครัด
- 4) ผู้ใช้งานต้องใช้งานเฉพาะระบบปัญญาประดิษฐ์ เครื่องมือปัญญาประดิษฐ์ แพลตฟอร์ม หรือซอฟต์แวร์ที่ สขญ. พิจารณาและอนุมัติให้ใช้งานเท่านั้น เพื่อให้การใช้งานอยู่ภายใต้กรอบความมั่นคงปลอดภัยและการกำกับดูแลขององค์กร การใช้ระบบปัญญาประดิษฐ์จากแหล่งภายนอกต้องได้รับอนุญาตเป็นลายลักษณ์อักษร และต้องผ่านการประเมินความเสี่ยงด้านข้อมูลและความมั่นคงปลอดภัยไซเบอร์ตามที่ สขญ. กำหนด
- 5) ผู้ใช้งานต้องระมัดระวังไม่ให้เกิดการใช้ระบบปัญญาประดิษฐ์ละเมิดลิขสิทธิ์ เครื่องหมายการค้า ความลับทางการค้า สิทธิในข้อมูล หรือทรัพย์สินทางปัญญาของบุคคลอื่น รวมถึงต้องไม่ใช้ระบบปัญญาประดิษฐ์เพื่อคัดลอก ดัดแปลง หรือเผยแพร่ผลงานของผู้อื่นโดยไม่มีสิทธิหรือไม่ได้รับอนุญาตตามกฎหมาย
- 6) ในกรณีที่มีการใช้ระบบปัญญาประดิษฐ์ในงานสำคัญ งานที่มีผลต่อการตัดสินใจ งานที่เกี่ยวข้องกับประชาชน หรือการจัดทำเอกสารทางการ ผู้ใช้งานควรจัดเก็บหลักฐานที่จำเป็นตามความเหมาะสม เช่น เครื่องมือที่ใช้ วันที่ใช้งาน ข้อมูลนำเข้าในระดับที่ไม่ละเมิดความลับ ผลลัพธ์ที่ได้รับ การตรวจทานของผู้ใช้งาน และแหล่งอ้างอิง เพื่อให้สามารถตรวจสอบย้อนหลังได้
- 7) ผู้ใช้งานต้องศึกษาหรือเข้ารับการอบรมเกี่ยวกับการใช้งานระบบปัญญาประดิษฐ์ เพื่อให้เข้าใจความสามารถ ข้อจำกัด ความเสี่ยง ข้อห้าม และข้อควรระวังในการใช้งาน รวมถึงต้องติดตามแนว

ปฏิบัติหรือประกาศที่เกี่ยวข้องซึ่งอาจมีการปรับปรุงให้สอดคล้องกับเทคโนโลยีและความเสี่ยงที่เปลี่ยนแปลงไป

- 8) ผู้ใช้งานต้องใช้งานระบบปัญญาประดิษฐ์ด้วยความรับผิดชอบ รอบคอบ และคำนึงถึงประโยชน์สาธารณะ หากพบความผิดปกติ ผลลัพธ์คลาดเคลื่อน การใช้งานที่อาจไม่เหมาะสม ความเสี่ยงด้านข้อมูล ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ หรือเหตุการณ์ที่อาจก่อให้เกิดผลกระทบต่อ สขญ. ประชาชน หรือผู้เกี่ยวข้อง ผู้ใช้งานต้องรายงานต่อผู้บังคับบัญชาหรือหน่วยงานที่รับผิดชอบทันที

## 7: การทบทวนและปรับปรุงนโยบาย (Policy Review and Amendment)

นโยบายฉบับนี้ต้องได้รับการทบทวนอย่างน้อยปีละ 1 ครั้ง เพื่อประเมินความทันสมัย ความเหมาะสม และความสอดคล้องกับกฎหมาย มาตรฐาน และบริบททางเทคโนโลยีที่เปลี่ยนแปลงไป หรือทบทวนหากมีเหตุการณ์สำคัญ เช่น การประกาศใช้กฎหมายหรือมาตรฐานใหม่ เหตุการณ์ด้านข้อมูลหรือความมั่นคงปลอดภัย การค้นพบความเสี่ยงใหม่ หรือการนำระบบปัญญาประดิษฐ์ที่มีความเสี่ยงสูงมาใช้งาน นโยบายนี้ต้องได้รับการปรับปรุงทันทีตามความจำเป็น

## 8: เอกสารอื่นที่เกี่ยวข้อง (Related Documents)

- 1) นโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy)
- 2) นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy)
- 3) ระเบียบปฏิบัติการจัดการชั้นความลับของเอกสารและข้อมูล (Document and Data Classification Procedure)
- 4) ระเบียบปฏิบัติการเก็บรักษาและการลบทำลายข้อมูล (Data Retention & Disposal Procedure)
- 5) ระเบียบปฏิบัติการประยุกต์ใช้ Generative AI (Generative AI Utilization Procedure)
- 6) ระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยระบบปัญญาประดิษฐ์ (AI Security Procedure)

## 9: แหล่งอ้างอิง (References)

- 1) OECD. OECD Principles on Artificial Intelligence. Organization for Economic Cooperation and Development.
- 2) UNESCO. Recommendation on the Ethics of Artificial Intelligence. United Nations Educational, Scientific and Cultural Organization.

- 3) NIST. Artificial AI Intelligence Risk Management Framework (AI RMF 1.0). Nation AI Institute of Standards and Technology, U.S. Department of Commerce.
- 4) ENISA. AI Cybersecurity Guidelines. European Union Agency for Cybersecurity.
- 5) ISO/IEC 27001: Information Security Management Systems (ISMS). International AI Organization for Standardization.
- 6) ISO/IEC 23894: Guidance on Risk Management for AI. International AI Organization for Standardization.
- 7) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และประกาศ/แนวปฏิบัติที่เกี่ยวข้องจากสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)
- 8) สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) แนวทางและกรอบมาตรการด้านความมั่นคงปลอดภัยไซเบอร์ เช่น SSDLC และมาตรการควบคุมระบบสารสนเทศที่สำคัญ
- 9) สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA). แนวทาง มาตรฐาน และหลักปฏิบัติที่เกี่ยวข้อง:
  - Thailand AI Governance Framework (กรอบธรรมาภิบาลปัญญาประดิษฐ์ประเทศไทย)
  - AI Readiness Assessment Framework