นโยบายดำเนินงานกำกับดูแลและการใช้งานปัญญาประดิษฐ์อย่างรับผิดชอบ
(Corporate Responsible AI Governance Policy)

1. บทนำเชิงกลยุทธ์และเจตจำนงขององค์กร (Strategic Introduction & Corporate Intent)

การก้าวกระโดดของเทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence: AI) และ Generative AI ได้เปลี่ยนผ่านจากนวัตกรรมทางเทคโนโลยีไปสู่วาระเชิงกลยุทธ์ขั้นสูงสุด การนำ AI มาประยุกต์ใช้ในองค์กรไม่เพียงแต่เป็นเครื่องมือสร้างมูลค่าทางธุรกิจ เพิ่มประสิทธิภาพการทำงาน และสร้างความได้เปรียบทางการแข่งขัน แต่ยังนำมาซึ่งความเสี่ยงที่ซับซ้อนในหลายมิติ ทั้งความเสี่ยงด้านการปฏิบัติงาน กฎหมาย การคุ้มครองข้อมูลส่วนบุคคล ความมั่นคงปลอดภัยทางไซเบอร์ ตลอดจนจริยธรรมและภาพลักษณ์องค์กร นโยบายการดำเนินงานกำกับดูแล และการใช้งานปัญญาประดิษฐ์อย่างรับผิดชอบฉบับนี้ จัดทำขึ้นเพื่ออ้างอิงเกณฑ์มาตรฐานสากล ISO/IEC 27001:2022 และหลักธรรมาภิบาลปัญญาประดิษฐ์ (AI Governance Center: AIGC) ที่สอดคล้องกับบริบทขององค์กรให้เป็นแนวทางปฏิบัติเชิงกลยุทธ์ เพื่อให้คณะกรรมการและฝ่ายบริหารสามารถกำกับดูแล บูรณาการ และควบคุม การใช้ AI ได้อย่างมีประสิทธิภาพ ปลอดภัย มีจริยธรรม และเกิดความยั่งยืนสูงสุด

1.1 วัตถุประสงค์ ขอบเขต และบริบทเชิงนโยบาย (Purpose, Scope, and Corporate Context)

กรอบการกำกับดูแลและการใช้งานปัญญาประดิษฐ์อย่างรับผิดชอบนี้ กำหนดขึ้นภายใต้เจตจำนงในการสร้างมาตรฐานการกำกับดูแล โดยมีขอบเขตและบริบทเชิงนโยบายครอบคลุมดังต่อไปนี้

- **วัตถุประสงค์ของนโยบาย**
  - เพื่อกำหนดแนวทางปฏิบัติเชิงกลยุทธ์และมาตรการควบคุมในการนำเทคโนโลยี AI และ Generative AI มาประยุกต์ใช้ในกระบวนการทำงานอย่างถูกต้อง เหมาะสม มีประสิทธิภาพ และปลอดภัย
  - เพื่อกำกับดูแลการใช้งาน AI ให้เป็นไปตามกฎหมาย กฎ ระเบียบ ข้อบังคับ มาตรฐานความมั่นคงปลอดภัยสารสนเทศ และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) พร้อมทั้งป้องกันผลกระทบเชิงลบต่อองค์กร สังคม และประเทศชาติ
  - เพื่อปลูกฝังวัฒนธรรมความรับผิดชอบ (Responsible Culture) เสริมสร้างความตระหนักรู้ และกำหนดกรอบจริยธรรมในการใช้ AI ให้สอดคล้องกับค่านิยมและหลักธรรมาภิบาลของบริษัท
- **ขอบเขตการบังคับใช้**
  - นโยบายนี้มีผลบังคับใช้ครอบคลุมการใช้งานเทคโนโลยี AI และ Generative AI ทุกประเภทในการดำเนินงานตามภารกิจของบริษัทฯ โดยบังคับใช้กับ **ผู้ใช้งาน** ทุกกลุ่มอย่างเคร่งครัด ได้แก่ กรรมการบริษัท ผู้บริหาร พนักงานทุกระดับ ลูกจ้าง ผู้ปฏิบัติงาน ตลอดจนหน่วยงานภายนอกและผู้รับจ้าง (Outsourcers, Suppliers, Service Providers, Consultants, Partners) ที่ได้รับสิทธิ์ในการเข้าถึงระบบหรือข้อมูลสารสนเทศของบริษัทฯ
- **เจตจำนงในการปฏิบัติตามกฎหมายและความมั่นคงปลอดภัย**
  - บริษัทมุ่งมั่นยึดถือการคุ้มครองข้อมูลส่วนบุคคล ข้อมูลส่วนบุคคลอ่อนไหว และรักษาความลับขององค์กร เป็นสิ่งสำคัญสูงสุด พร้อมผสานมาตรการความมั่นคงปลอดภัยไซเบอร์เข้ากับระบบเทคโนโลยีเชิงปฏิบัติการ (Operational Technology) เพื่อปกป้องทรัพย์สินสารสนเทศขององค์กรให้รอดพ้นจากภัยคุกคามทุกรูปแบบ

1.2 นิยามศัพท์สำคัญด้านการกำกับดูแล AI และความมั่นคงปลอดภัย (Key Governance & Security Definitions)

คำศัพท์	ความหมายเชิงกลยุทธ์
ปัญญาประดิษฐ์ (Artificial Intelligence: AI)	เทคโนโลยีที่ถูกพัฒนาขึ้นเพื่อให้ระบบประมวลผลของคอมพิวเตอร์ หุ่นยนต์ เครื่องจักร หรืออุปกรณ์อิเล็กทรอนิกส์ต่างๆ มีคุณสมบัติหรือพฤติกรรมใกล้เคียงมนุษย์ตามวัตถุประสงค์ที่มนุษย์กำหนด เช่น การเรียนรู้ การรับรู้และตอบสนองต่อสภาพแวดล้อม การให้เหตุผล และการแก้ไขปัญหา
เทคโนโลยี Generative AI	เทคโนโลยี AI ประเภทหนึ่งที่มีความสามารถในการสร้างเนื้อหาใหม่ในหลากหลายรูปแบบตามข้อความหรือคำสั่ง (Prompt) ที่มนุษย์เป็นผู้กำหนด เช่น ข้อความ ภาพ วิดีโอ เสียง ซอร์สโค้ด หรือรูปแบบอื่น
Responsible AI	แนวทางการพัฒนาและใช้งาน AI โดยคำนึงถึงหลักจริยธรรมและค่านิยมของสังคม มุ่งเน้นการสร้างประโยชน์สูงสุดต่อมนุษย์ สังคม และสิ่งแวดล้อม พร้อมทั้งป้องกันผลกระทบเชิงลบ เช่น ความลำเอียงหรือการเลือกปฏิบัติ
ข้อมูลส่วนบุคคล (Personal Data)	ข้อมูลเกี่ยวกับบุคคลธรรมดาซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ
ข้อมูลส่วนบุคคลอ่อนไหว (Sensitive Personal Data)	ข้อมูลส่วนบุคคลตามที่ถูกบัญญัติไว้ในมาตรา 26 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้แก่ ข้อมูลเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกัน
ระดับการมีส่วนร่วมของมนุษย์ (Level of Human Involvement)	กรอบการกำหนดขอบเขตและอำนาจการควบคุมดูแลของมนุษย์ในกระบวนการทำงานและการตัดสินใจของระบบ AI ตามระดับความเสี่ยง (Human-in-the-loop, Human-over-the-loop, Human-out-of-the-loop)
Recovery Point Objective (RPO)	จุดของข้อมูลล่าสุดที่ต้องสามารถนำกลับคืนมาได้เมื่อเกิดความเสียหายต่อระบบสารสนเทศ (เป้าหมายด้านข้อมูลของการกู้คืนสภาพ)
Recovery Time Objective (RTO)	ระยะเวลาสูงสุดที่ยอมรับได้ในการกู้คืนสภาพจากการหยุดชะงักของการปฏิบัติงานทางธุรกิจ การให้บริการ หรือระบบสารสนเทศ ให้กลับมาให้บริการได้ตามปกติ
ทีมตอบสนองต่อเหตุการณ์ (Incident Response Team)	ทีมที่ได้รับการแต่งตั้งโดยผู้บริหารสูงสุด ซึ่งประกอบด้วยบุคลากรที่มีทักษะและประสบการณ์เพียงพอ ได้รับการจัดสรรทรัพยากรและอุปกรณ์อำนวยความสะดวกอย่างเหมาะสม ทำหน้าที่จัดการงานที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศ และเหตุการณ์ละเมิดความมั่นคงปลอดภัย

การกำหนดรากฐานนิยามศัพท์เชิงกลยุทธ์ข้างต้นสร้างภาษาและความเข้าใจที่ตรงกันทั่วทั้งองค์กร นำไปสู่การวางโครงสร้างอำนาจหน้าที่และการส่งผ่านนโยบายจากระดับคณะกรรมการบริษัทลงสู่ผู้ปฏิบัติงานอย่างสอดคล้องและมีประสิทธิภาพในเสาหลักถัดไป

2. โครงสร้างองค์กรและการกำกับดูแล (Pillar 1: AI Governance Structure & Leadership)

การวางรากฐานโครงสร้างการกำกับดูแลองค์กร (Governance Structure) เป็นเสาหลักแรก (Pillar 1) ในการขับเคลื่อน AI ให้เป็นไปตามหลักธรรมาภิบาล โดยต้องกำหนดสายการบังคับบัญชา หน้าที่ความรับผิดชอบ และกลไกการกำกับดูแลที่ตรวจสอบได้จริงในระดับคณะกรรมการบริษัท และผู้บริหาร โดยมีรายละเอียด ดังนี้

2.1 คณะกรรมการบริษัท (Board of Directors)

บทบาทและภาระหน้าที่ของคณะกรรมการบริษัท (Board of Directors Mandate)

คณะกรรมการบริษัทมีหน้าที่กำกับดูแลการใช้ AI ให้สอดคล้องกับหลักธรรมาภิบาล ความปลอดภัย และจริยธรรม โดยมีพันธกิจสำคัญ 3 ด้าน พร้อมกลไกกำกับดูแลเชิงรุก ดังนี้

1. **การกำหนดและกำกับดูแลกลยุทธ์ AI (AI Strategy Integration)**
   บูรณาการ AI เข้ากับกลยุทธ์ทางธุรกิจ โดยกำหนดวิสัยทัศน์ที่ชัดเจนในการสร้างมูลค่า เพิ่มขีดความสามารถในการแข่งขัน และกำกับดูแล เพื่อควบคุมระบบ AI ทั้งหมดในองค์กร
2. **การจัดสรรงบประมาณและการอนุมัติบริหารความเสี่ยง (Budget Allocation & Risk Oversight)**
   อนุมัติงบประมาณลงทุนในโครงสร้างพื้นฐาน เทคโนโลยี บุคลากร และกำหนดให้มี **"กระบวนการประเมินผลกระทบด้านความเสี่ยง AI (AI Risk & Impact Assessment: ARIA)"** ก่อนอนุมัติปรับใช้ระบบ AI ในกระบวนการทำงานจริง
3. **การสร้างความเข้าใจและการยกระดับสมรรถนะ (Board Capability Building)**
   พัฒนาความรู้ความเข้าใจเกี่ยวกับ AI และภัยคุกคามใหม่ๆ ให้แก่กรรมการทุกคน เพื่อให้สามารถตั้งคำถามเชิงกลยุทธ์และตัดสินใจได้อย่างชาญฉลาด โดยอาจพิจารณาจัดตั้งคณะกรรมการเฉพาะกิจด้าน AI ตามความเหมาะสม

2.2 การแต่งตั้งและการดำเนินงานของคณะทำงาน AI Governance (AI Governance Working Group Setup)

คณะกรรมการอาจพิจารณาแต่งตั้งคณะทำงาน AI Governance แบบข้ามสายงาน (Cross-functional Working Group) ประกอบด้วย ด้านระบบสารสนเทศ ด้านธุรกิจ ด้านกฎหมาย และด้านกำกับดูแลการปฏิบัติงาน (Compliance) เพื่อทำหน้าที่บริหารจัดการ โดยมีรายละเอียดดังนี้

1. **การกำหนดทิศทาง (Direction)** กำหนดกลยุทธ์ AI จัดการความเสี่ยง และอนุมัติผลการประเมิน
2. **การเฝ้าติดตาม (Monitoring)** ติดตามประสิทธิภาพ ความมั่นคงปลอดภัย และการใช้งาน AI ให้เป็นไปตามมาตรฐานสากล
3. **การประเมินผล (Evaluation)** ประเมินผลกระทบ ประสิทธิผลของกลไกการกำกับดูแล (AI Mechanism) และทบทวนความคุ้มค่าเชิงกลยุทธ์
4. **กรณีมีความจำเป็นต้องใช้ Generative AI** ร่วมกับข้อมูลภายในที่มีชั้นความลับ ข้อมูลส่วนบุคคล หรือข้อมูลส่วนบุคคลที่มีความอ่อนไหว ต้องได้รับการพิจารณาอนุมัติจากผู้บริหารสูงสุดในการใช้ผ่านแพลตฟอร์มระดับองค์กรขององค์กรที่บริษัทกำหนดเท่านั้น
5. **กำหนดให้มีการตรวจสอบ และกลั่นกรองการใช้ AI ในสายงาน** ติดตามและควบคุมการทำงานของพนักงานให้ปฏิบัติตามนโยบายอย่างเคร่งครัด
6. **พนักงานทุกคนต้องปฏิบัติตามนโยบายและมาตรการความปลอดภัยอย่างเคร่งครัด** ตรวจสอบผลลัพธ์ของ AI ก่อนนำไปใช้ และรายงานเหตุผิดพลาดหรือช่องโหว่ความปลอดภัยต่อผู้บังคับบัญชาและทีมตอบสนองต่อเหตุการณ์ทันที

2.3 การยกระดับทักษะและการสร้างวัฒนธรรมความรับผิดชอบ (Upskilling & Responsible Culture)

- **การยกระดับสมรรถนะบุคลากร (Upskilling)**
  เสริมสร้างความรู้ ทักษะเชิงเทคโนโลยี และความเข้าใจด้านจริยธรรมให้แก่บุคลากรทุกระดับ เพื่อให้สามารถใช้งานระบบ AI ในการปฏิบัติงานได้อย่างมีประสิทธิภาพและปลอดภัย
- **การสร้างวัฒนธรรมองค์กรแห่งความไว้วางใจ**
  ประเมินผลกระทบของ AI ต่อพนักงาน ยึดมั่นในการใช้ AI เพื่อส่งเสริมศักยภาพมนุษย์ (Human Augmentation) สร้างความยั่งยืน และสร้างความไว้วางใจแก่สาธารณชน
- **การเปิดรับมุมมองที่หลากหลายและการสื่อสาร** รวบรวมข้อมูลจากผู้เชี่ยวชาญข้ามสาขา (นักพัฒนา, นักกฎหมาย, นักจริยธรรม) และสื่อสารสร้างการมีส่วนร่วมกับผู้มีส่วนได้เสียทุกฝ่ายเพื่อรับฟังข้อกังวลเกี่ยวกับ AI อย่างโปร่งใส

การจัดตั้งโครงสร้างองค์กรที่เข้มงวดเป็นฐานรากสำคัญในการขับเคลื่อนวิสัยทัศน์ AI ไปสู่การกำหนดกลยุทธ์การบริหารจัดการความเสี่ยงที่ครอบคลุมทุกมิติในเสาหลักถัดไป

3. กลยุทธ์ปัญญาประดิษฐ์อย่างรับผิดชอบและการบริหารความเสี่ยง (Pillar 2: Responsible AI Strategy & Risk Management Framework)

การกำหนดกลยุทธ์ AI ขององค์กร ต้องขับเคลื่อนด้วยหลักธรรมาภิบาลและความรับผิดชอบ ควบคู่กับการนำกรอบบริหารจัดการความเสี่ยงเชิงรุกมาประยุกต์ใช้ตลอดวงจรชีวิต AI เพื่อปกป้องคุณค่าและทรัพย์สินขององค์กร

3.1 หลักการสำคัญ 6 ประการของ Responsible AI และคุณค่าองค์กร (6 Core Responsible AI Principles)

การขับเคลื่อน Responsible AI ยึดมั่นในหลักสากล 6 ประการ ซึ่งช่วยลดความเสี่ยงเชิงโครงสร้างและสร้างความได้เปรียบทางการแข่งขัน

1. **ความโปร่งใส (Transparency)**
   มุ่งเน้นการสร้างระบบ AI ที่สามารถอธิบายเหตุผลของการตัดสินใจและกระบวนการทำงานได้ (Explainable AI) เพื่อให้ผู้มีส่วนได้เสียเข้าใจที่มาของผลลัพธ์ ช่วยสร้างความเชื่อมั่น ลดข้อสงสัย และยกระดับความไว้วางใจในการใช้บริการ
2. **ความยุติธรรม (Fairness)**
   ตรวจสอบและขจัดอคติในชุดข้อมูล และขั้นตอนหรือวิธี (อัลกอริทึม/Algorithm) เพื่อป้องกันการเลือกปฏิบัติอย่างไม่เป็นธรรมต่อบุคคลหรือกลุ่มคน ช่วยยกระดับคุณภาพการวางกลยุทธ์ วางรากฐานการบริการที่เท่าเทียม และปราศจากอคติทางสังคม
3. **ความปลอดภัยและความน่าเชื่อถือ (Safety & Reliability)**
   พัฒนาและทดสอบระบบ AI ให้มีความแม่นยำ เสถียร ปลอดภัย และให้ผลลัพธ์ที่เชื่อถือได้สม่ำเสมอ ช่วยลดความผิดพลาดในการปฏิบัติงานและป้องกันภัยคุกคามทางไซเบอร์
4. **ความเป็นส่วนตัว (Privacy)**
   ปกป้องข้อมูลส่วนบุคคลอย่างเข้มงวดตลอดกระบวนการประมวลผลของ AI ตามกฎหมาย PDPA ช่วยลดความเสี่ยงจากการละเมิดกฎหมายและป้องกันการรั่วไหลของข้อมูลความลับ
5. **ความรับผิดชอบ (Accountability)**
   กำหนดตัวบุคคลหรือหน่วยงานรับผิดชอบ (Ownership) ที่ชัดเจนสำหรับผลลัพธ์และการทำงานของ AI ช่วยให้เกิดกลไกการแก้ไขปัญหาที่รวดเร็วและเพิ่มความได้เปรียบในการบริหารจัดการ

6. **ผลกระทบต่อสังคม (Social Impact)**

ประเมินผลกระทบรอบด้านทั้งต่อพนักงาน สังคม เศรษฐกิจ และสิ่งแวดล้อม ช่วยป้องกันการตกเป็นเป้าโจมตีทางสังคมและส่งเสริมการเติบโตอย่างยั่งยืน

3.2 การระบุ และการประเมินความเสี่ยงจาก AI (AI Risk Identification & Assessment Framework)

องค์กรต้องระบุและประเมินความเสี่ยงจาก AI เชิงรุก โดยเชื่อมโยงความเสี่ยงทางเทคโนโลยีเข้ากับผลกระทบทางธุรกิจเชิงกลยุทธ์ 5 มิติหลัก ดังนี้

1. **คุณภาพของข้อมูล (Data Quality Risk) การตัดสินใจผิดพลาด การหยุดชะงักของระบบ**
   ความเสี่ยงจากข้อมูลที่ป้อนเข้าสู่ AI มีความบิดเบือน ไม่สมบูรณ์ หรือเก่าเกินไป นำไปสู่การประมวลผลผิดพลาดส่งผลกระทบต่อการตัดสินใจเชิงธุรกิจ
2. **อคติและการเลือกปฏิบัติ (Bias & Discrimination Risk) การถูกฟ้องร้อง การละเมิดสิทธิมนุษยชน**
   ขั้นตอนหรือวิธี (อัลกอริทึม/Algorithm) ที่ประมวลผลบนชุดข้อมูลที่มีอคติ ส่งผลให้เกิดการตัดสินใจที่เอนเอียง ก่อให้เกิดการฟ้องร้อง และละเมิดกฎหมาย
3. **ช่องโหว่ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk) การสูญเสียทรัพย์สินทางปัญญา ระบบถูกโจมตี**
   การถูกโจมตีผ่านเทคนิค Prompt Injection, Data Poisoning หรือการเจาะช่องโหว่ระบบ AI ที่เชื่อมต่อกับระบบเทคโนโลยีเชิงปฏิบัติการ (OT/SCADA) ก่อให้เกิดการหยุดชะงักในกระบวนการผลิตหรือการสูญเสียความคุ้มครองทางทรัพย์สินทางปัญญา
4. **การละเมิดความเป็นส่วนตัวและการขัดต่อกฎหมาย (Privacy & Non-compliance Risk) โทษปรับรุนแรงตาม PDPA**
   การนำข้อมูลส่วนบุคคลหรือข้อมูลอ่อนไหวตาม PDPA มาตรา 26 ไปเทรนโมเดลโดยไม่ได้รับยินยอม นำไปสู่โทษปรับทางอาญาและแพ่งรุนแรง
5. **ความเสี่ยงด้านชื่อเสียงและจริยธรรม (Reputational Risk) ภาพลักษณ์องค์กรเสียหาย ขาดความเชื่อมั่น**
   การที่ AI Gen เนื้อหาเท็จ (Hallucination/Misinformation) หรือสร้างข้อความที่ขัดต่อจริยธรรม นำไปสู่วิกฤตความเชื่อมั่นต่อแบรนด์หรือชื่อเสียงขององค์กร

4. การปฏิบัติการและการควบคุมความมั่นคงปลอดภัยสารสนเทศ (Pillar 3: AI Operation & Information Security Controls)

การดำเนินงานระบบ AI (Pillar 3) ต้องได้รับการควบคุมตามกรอบมาตรฐาน เพื่อรับประกันว่าสินทรัพย์สารสนเทศ โครงสร้างพื้นฐาน IT มีความมั่นคงปลอดภัยตลอดวงจรธุรกิจ

4.1 การบริหารจัดการวงจรชีวิต AI และผู้ให้บริการภายนอก (AI Lifecycle & Vendor Risk Management)

- **การจัดการวงจรชีวิต AI (AI Lifecycle Management)** ควบคุมกระบวนการตั้งแต่การออกแบบ การจัดหาการทดสอบ การติดตั้งใช้งาน จนถึงการยกเลิกใช้งาน โดยต้องประเมินความเสี่ยง และบันทึกใน AI Asset Register ทุกขั้นตอน
- **การกำกับดูแลผู้ให้บริการภายนอก (Vendor Risk Management)** ตรวจสอบและประเมินความเสี่ยงของ Outsourcers, Suppliers และ Service Providers ที่นำบริการ AI มาใช้ โดยต้องระบุข้อตกลงระดับการให้บริการ (SLA) มาตรการคุ้มครองข้อมูล และสิทธิ์ในการเข้าตรวจสอบ (Right to Audit) อย่างชัดเจน

4.2 การบูรณาการมาตรการควบคุม 4 ด้าน โดยอิงแนวทางมาตรฐาน ISO/IEC 27001:2022 (Four Control Domains Integration) เพื่อเป็นการเพิ่มประสิทธิภาพ

1. มาตรการควบคุมด้านองค์กร (Organizational Controls)

- กำหนดนโยบาย ทบทวน และประเมินความเสี่ยงด้านความมั่นคงปลอดภัยของ AI อย่างน้อยปีละ 1 ครั้ง
- จัดทำทะเบียนสินทรัพย์ AI (AI Asset Register) และบริหารความสัมพันธ์กับคู่ค้าที่เข้าถึงระบบ AI ให้สอดคล้องกับนโยบายความมั่นคงปลอดภัยสารสนเทศของบริษัท

2. มาตรการควบคุมด้านบุคลากร (People Controls)

- จัดให้มีกระบวนการคัดกรองบุคลากร (Background Checks) ก่อนมอบหมายหน้าที่รับผิดชอบระบบ AI และข้อมูลความลับ
- กำหนดเงื่อนไขการรักษาความลับ (NDA) และจัดอบรมสร้างความตระหนักรู้ด้านความปลอดภัยไซเบอร์และการใช้ AI อย่างรับผิดชอบแก่บุคลากรทุกระดับ
- จัดการและยกเลิกสิทธิ์การเข้าถึงระบบ AI ทันทีเมื่อบุคลากรเปลี่ยนตำแหน่งหรือสิ้นสุดการจ้างงาน

3. มาตรการควบคุมทางกายภาพ (Physical Controls)

- กำหนดเขตความปลอดภัยทางกายภาพ (Physical Security Perimeters) สำหรับห้องเซิร์ฟเวอร์ (Server) ศูนย์ข้อมูล (Data Center) และพื้นที่ติดตั้งระบบควบคุม AI
- ใช้มาตรการควบคุมการเข้าออกที่เข้มงวด เช่น บัตรผ่าน และกล้องวงจรปิด (CCTV)
- กำจัดและทำลายสื่อบันทึกข้อมูล อุปกรณ์ประมวลผล AI ที่ไม่ใช้งานแล้วอย่างปลอดภัยตามมาตรฐาน

4. มาตรการควบคุมทางเทคโนโลยี (Technological Controls)

- **การยึดหลัก** ปกป้องความลับ (Confidentiality), ความถูกต้องครบถ้วน (Integrity), และความพร้อมใช้งาน (Availability) ของข้อมูล โมเดล AI และระบบสารสนเทศ
- **การบริหารจัดการสิทธิ์และการเข้ารหัส** ใช้หลักสิทธิ์เท่าที่จำเป็น (Least Privilege), เข้ารหัสข้อมูลทั้งขณะจัดเก็บ (Data at Rest) และขณะรับส่ง (Data in Transit)
- **การป้องกันความปลอดภัยของ API Key และซอร์สโค้ด:** ห้ามนำ API Key, Credentials, รายละเอียดการตั้งค่าระบบ ไปใส่ใน Generative AI สาธารณะ และต้องทำการตรวจสอบความปลอดภัย (Code Security Review /Vulnerability Scan) ซอร์สโค้ดที่เจนโดย AI อย่างถี่ถ้วนก่อนนำไปปรับใช้
- Network Segmentation แยกออกจากเครือข่าย IT สาธารณะเพื่อป้องกันภัยคุกคามทางไซเบอร์ที่ส่งผลหยุดชะงักต่อสายการผลิต
- **การสำรองข้อมูลและการกู้คืนระบบ** กำหนดมาตรการสำรองข้อมูลโมเดล AI และตั้งค่า Recovery Point Objective (RPO) และ Recovery Time Objective (RTO) ให้สอดคล้องกับแผนบริหารความต่อเนื่องทางธุรกิจ (BCP)

4.3 การเฝ้าระวังและการตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัย (Monitoring & Incident Response)

- **การเฝ้าระวังและบันทึกข้อมูล (Logging & Monitoring)** ติดตั้งระบบบันทึก Log การใช้งาน AI และเฝ้าระวังพฤติกรรมสุ่มเสี่ยงหรือการพยายามเจาะระบบตลอด 24 ชั่วโมง
- **ขั้นตอนการตอบสนองต่อเหตุการณ์ (Incident Response Procedure)** หากพบเหตุการณ์ละเมิดความปลอดภัย หรือความผิดพลาดจาก AI ผู้ใช้งานต้องรายงานต่อผู้บังคับบัญชาทันที และให้**ทีมตอบสนองต่อเหตุการณ์ละเมิดความมั่นคงปลอดภัยด้านสารสนเทศ (Incident Response**

Team) ดำเนินการระงับเหตุ ควบคุมความเสียหายตรวจสอบ และกู้คืนระบบตามมาตรการที่กำหนด

มาตรการควบคุมความมั่นคง

ปลอดภัยทางเทคโนโลยีข้างต้น จะถูกแปลงเป็นแนวทางปฏิบัติการใช้งาน Generative AI สำหรับผู้ปฏิบัติงานในส่วนถัดไป

5. แนวทางปฏิบัติการใช้งาน Generative AI สำหรับองค์กร (Generative AI Acceptable Use Guidelines)

องค์กรกำหนดแนวทางการใช้งาน Generative AI ที่ยอมรับได้ (Acceptable Use Policy: Generative AI) เพื่อให้บุคลากรนำเครื่องมือ AI มาใช้ยกระดับประสิทธิภาพการทำงาน โดยไม่ละเมิดข้อบังคับ กฎหมาย หรือสร้างความเสี่ยงต่อบริษัท

5.1 ลักษณะการใช้งานที่ยอมรับได้และซอฟต์แวร์ที่แนะนำ (Acceptable Use Cases & Approved Tools)

บริษัทอนุญาตให้ผู้ใช้งานประยุกต์ใช้ Generative AI เพื่อสนับสนุนการปฏิบัติงานตามภารกิจ โดยต้องใช้ซอฟต์แวร์และแอปพลิเคชันตามหมวดหมู่ที่บริษัทประกาศกำหนด ดังต่อไปนี้

หมวดหมู่แอปพลิเคชัน Generative AI	ตัวอย่างแอปพลิเคชัน/ บริการที่แนะนำ	ขอบเขตลักษณะการใช้งานที่อนุญาต
เครื่องมือสร้างข้อความ (Text Generation)	**ChatGPT, Claude, Gemini**	การวิเคราะห์ข้อมูล, การสรุปรายงาน, การร่างบันทึกข้อความ/เอกสารภายใน, การคิดหัวข้อประชาสัมพันธ์ และการอ้างอิงข้อมูลเบื้องต้น
เครื่องมือสร้างภาพ (Image Generation)	**DALL-E, Midjourney, Stable Diffusion**	การออกแบบสื่อกราฟิกภายใน, การจัดทำภาพประกอบการนำเสนอ (Internal Presentation) และงานสร้างสรรค์โฆษณา
เครื่องมือช่วยเขียนโค้ด (Code Generation)	**GitHub Copilot, Codeium, Tabnine**	การร่างชุดคำสั่งโปรแกรม, การตรวจสอบความถูกต้องของโค้ด และการปรับปรุงประสิทธิภาพโปรแกรม (Refactoring)
เครื่องมือสร้างเสียงและวิดีโอ (Audio & Video Generation)	**ElevenLabs, RunwayML**	การสร้างสื่อมัลติมีเดียเพื่อการสื่อสารภายในองค์กร งานฝึกอบรม และสื่อประชาสัมพันธ์

หมายเหตุ: การใช้งานซอฟต์แวร์ข้างต้นต้องดำเนินงานผ่านบัญชีผู้ใช้หรือแพลตฟอร์มที่ได้รับการอนุมัติจากฝ่ายไอทีของบริษัทเท่านั้น

5.2 ข้อห้ามเด็ดขาดในการใช้งาน (Strict Prohibitions & Restrictions)

เพื่อป้องกันความเสียหายต่อบุคคลและองค์กร ห้ามมิให้ผู้ใช้งานกระทำการดังต่อไปนี้

- **ห้ามใช้ตัดสินใจแทนมนุษย์ในงานความเสี่ยงสูง** ห้ามใช้ AI ทำหน้าที่ตัดสินใจชี้ขาดแทนมนุษย์ในงานด้านกฎหมาย การเงิน การประเมินผลงาน หรือการตัดสินใจที่กระทบต่อสิทธิเสรีภาพ ทรัพย์สิน และชีวิตของบุคคล
- **เงื่อนไขการใช้ข้อมูลลับและข้อมูลส่วนบุคคล** ห้ามนำข้อมูลความลับ ข้อมูลภายใน เอกสารสัญญา API Key รหัสผ่าน ข้อมูลส่วนบุคคล หรือข้อมูลส่วนบุคคลอ่อนไหวตาม PDPA มาตรา 26 ใส่ลงในระบบ Generative AI สาธารณะโดย เด็ดขาด **เว้นแต่เป็นการใช้งานผ่านแพลตฟอร์มระดับองค์กร (Enterprise Edition) ที่บริษัทประกาศกำหนด และต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจาก "ผู้บังคับบัญชาสูงสุดในสายงาน" (Highest Line Executive) ก่อนนำมาใช้งานทุกกรณี**

- **ห้ามใช้สร้างข้อมูลเท็จและละเมิดทรัพย์สินทางปัญญา** ห้ามใช้ AI สร้างข้อมูลอันเป็นเท็จ (Misinformation/(Disinformation) สร้างเนื้อหาที่ละเมิดลิขสิทธิ์ เครื่องหมายการค้า หรือทรัพย์สินทางปัญญาของผู้อื่น
- **สิทธิในทรัพย์สินทางปัญญา** ผลงาน คำสั่ง (prompts) ข้อมูล หรือชิ้นงานที่สร้างสรรค์ขึ้นโดย AI จากการปฏิบัติงานของพนักงาน ถือเป็นทรัพย์สินทางปัญญาของบริษัทแต่เพียงผู้เดียว พนักงานไม่สามารถอ้างสิทธิ์ส่วนบุคคลเมื่อพ้นสภาพการเป็นพนักงานของบริษัท
- **ห้ามใช้ในทางที่ขัดต่อกฎหมายและจริยธรรม** ห้ามสร้างเนื้อหาที่เหยียดเชื้อชาติ ศาสนา เพศ วัย ความพิการ หรือสร้างความขัดแย้งในสังคม

5.3 ตารางแนวทางพฤติกรรมที่ควรทำและไม่ควรทำ (Do's and Don'ts Matrix)

พฤติกรรมที่ควรทำ (Do's)	พฤติกรรมที่ไม่ควรทำ (Don'ts)
ตรวจสอบความถูกต้อง: ตรวจสอบความถูกต้อง แม่นยำ และความสมเหตุสมผลของผลลัพธ์จาก AI ก่อนนำไปใช้งานทุกครั้ง	**เชื่อมั่นผลลัพธ์ทันที:** นำข้อมูลหรือซอร์สโค้ดจาก AI ไปใช้งานทันทีโดยไม่มีการตรวจสอบและทดสอบความปลอดภัย
อนุมัติข้อมูลลับก่อนใช้: ใช้อนุญาตจากผู้บังคับบัญชาสูงสุดในสายงานเมื่อต้องใช้ข้อมูลลับ/ข้อมูลส่วนบุคคลกับ Enterprise AI	**เปิดเผยความลับสาธารณะ:** นำข้อมูลความลับ ข้อมูลส่วนบุคคล **PDPA มาตรา 26 คือ** กฎหมายที่บัญญัติห้ามมิให้เก็บรวบรวม ใช้ หรือเปิดเผย **"ข้อมูลส่วนบุคคลอ่อนไหว" (Sensitive Personal Data)** โดยปราศจากความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูล เว้นแต่จะมีข้อยกเว้นตามที่กฎหมายกำหนดไว้ **ประเภทของข้อมูลส่วนบุคคลอ่อนไหว** ข้อมูลที่ได้รับความคุ้มครองเป็นพิเศษตามมาตรานี้ ได้แก่: เชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนา หรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม
	ข้อมูลความพิการหรือข้อมูลสุขภาพ ข้อมูลสหภาพแรงงาน พันธุกรรม ไบโอเมตริกซ์ (เช่น ข้อมูลจำลองใบหน้า ลายพิมพ์นิ้วมือ) หรือข้อมูลอื่นใดที่กระทบในทำนองเดียวกันตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด อ่อนไหว หรือ API Key ใส่ลงใน Generative AI สาธารณะ
อ้างอิงการใช้ AI: ระบุข้อความชัดเจนว่า "เนื้อหานี้ได้รับการช่วยเหลือจากเทคโนโลยี Generative AI" ตามความเหมาะสม	**ปกปิดและแอบอ้าง:** ปกปิดการใช้ AI หรือแอบอ้างว่าผลงานที่สร้างจาก AI เป็นผลงานที่ตนเองสร้างสรรค์ขึ้นทั้งหมด

พฤติกรรมที่ควรทำ (Do's)	พฤติกรรมที่ไม่ควรทำ (Don'ts)
อ้างอิงแหล่งที่มา: ตรวจสอบและอ้างอิงแหล่งที่มาต้นฉบับของข้อมูลเพื่อความถูกต้องโปร่งใส	**ละเมิดทรัพย์สินทางปัญญา:** นำผลงานที่มีลิขสิทธิ์ของผู้อื่นมาดัดแปลงผ่าน AI โดยไม่ได้รับอนุญาต
ใช้เครื่องมือที่อนุมัติ: ใช้เฉพาะแอปพลิเคชันและบริการ Generative AI ตามรายการที่บริษัทประกาศกำหนด	**ใช้เครื่องมือไม่อนุมัติ:** ลักลอบใช้ซอฟต์แวร์ AI นอกเหนือรายการที่ได้รับอนุมัติ
รายงานเหตุผิดพลาด: รายงานผู้บังคับบัญชาและทีม Incident Response ทันทีเมื่อพบข้อผิดพลาดหรือภัยคุกคาม	**ปกปิดข้อผิดพลาด:** ปกปิดซ่อนเร้นข้อผิดพลาดจากการประมวลผลของ AI ที่ส่งผลกระทบต่อองค์กร

การกำหนดแนวทางปฏิบัติการใช้งานข้างต้นจะสำเร็จได้ ต้องอาศัยกลไกการบังคับใช้นโยบาย การฝึกอบรมบุคลากร และการกำกับดูแลอย่างต่อเนื่องในส่วนสุดท้าย

6. การบังคับใช้ การฝึกอบรม และการกำกับดูแลอย่างต่อเนื่อง (Enforcement, Training, & Continuous Oversight)

เพื่อให้กรอบการกำกับดูแลมีผลบังคับใช้จริงในทางปฏิบัติ องค์กรได้กำหนดกลไกขับเคลื่อน การฝึกอบรมภาคบังคับ บทลงโทษทางวินัยที่เด็ดขาด และกระบวนการปรับปรุงมาตรฐานให้ทันสมัยอยู่เสมอ

- การบังคับใช้นโยบาย & กำกับดูแล
- การฝึกอบรม อย่างน้อยปีละ 1 ครั้ง
- การรายงาน & บทลงโทษ (วินัยร้ายแรง/ยกเลิกสัญญา)
- การพัฒนาปรับปรุงต่อเนื่อง (ทบทวนตามหลักทางสากล และกฎหมาย

6.1 ข้อกำหนดการฝึกอบรมและการสร้างความตระหนักรู้ (Mandatory Training Program)

- การอบรมภาคบังคับประจำปี บริษัทกำหนดให้พนักงานทุกระดับ ลูกจ้าง ผู้ปฏิบัติงาน และผู้รับจ้างทุกคน ต้องเข้ารับการฝึกอบรมเรื่องการใช้งาน Generative AI อย่างรับผิดชอบ ความเสี่ยง ความมั่นคงปลอดภัย และแนวทาง Do's & Don'ts อย่างน้อยปีละ 1 ครั้ง
- เผยแพร่สื่อสารสร้างความตระหนักรู้ ผ่านช่องทางการสื่อสารต่างๆ ขององค์กร

6.2 กระบวนการรายงานเหตุผิดพลาดและบทลงโทษ (Reporting Mechanisms & Penalties)

- **การรายงานเหตุการณ์ทันที (Immediate Reporting)** หากผู้ใช้งานพบการใช้งาน AI ที่ไม่เหมาะสม การรั่วไหลของข้อมูล หรือข้อผิดพลาดที่อาจก่อให้เกิดความเสียหาย **ต้องรายงานต่อผู้บังคับบัญชาและทีม Incident Response ทราบทันที**
- **บทลงโทษที่เด็ดขาด (Mandatory Discipline & Enforcement)** การไม่ปฏิบัติตามนโยบายฉบับนี้ถือเป็นการฝ่าฝืนคำสั่งและข้อบังคับการทำงานของบริษัท โดยจะได้รับการพิจารณาโทษดังนี้
  - **สำหรับพนักงานและลูกจ้าง** ถือเป็นความผิดทางวินัย และจะถูกดำเนินการลงโทษทางวินัยขั้นเด็ดขาดตามข้อบังคับเกี่ยวกับการทำงานของบริษัท ตั้งแต่การตักเตือน การตัดค่าจ้าง การพักงาน จนถึงการเลิกจ้างโดยไม่จ่ายชดเชยตามแต่กรณีความรุนแรง

- **สำหรับผู้รับจ้างและหน่วยงานภายนอก** ถือเป็นการผิดสัญญาอย่างร้ายแรง บริษัทมีสิทธิ์บอกเลิกสัญญาจ้างหรือสัญญาให้บริการทันที พร้อมเรียกร้องค่าเสียหายที่เกิดขึ้นทางแพ่งและอาญาตามที่กฎหมายสูงสุดบัญญัติไว้

6.3 การทบทวนและพัฒนาอย่างต่อเนื่อง (Continuous Improvement & Policy Review)

- **การติดตามและประเมินผลการกำกับดูแล** คณะทำงาน AI Governance และผู้บริหารระดับสูง ต้องติดตามตรวจสอบ Log การใช้งาน และประเมินประสิทธิผลของกรอบการกำกับดูแลนี้อย่างสม่ำเสมอ
- **การปรับปรุงนโยบายให้ทันสมัย** องค์กรจะทำการทบทวนนโยบายฉบับนี้อย่างน้อยปีละ 1 ครั้ง หรือทันทีที่มีการเปลี่ยนแปลงทางเทคโนโลยี กฎหมาย PDPA หรือการประกาศมาตรฐานใหม่จากศูนย์ธรรมาภิบาลปัญญาประดิษฐ์ (AIGC) และระบบมาตรฐาน เพื่อรักษามาตรฐานความมั่นคงปลอดภัยและธรรมาภิบาลขั้นสูงสุดขององค์กรสืบไป

ทั้งนี้ ให้มีผลบังคับใช้ตั้งแต่วันที่ 15 ตุลาคม 2569 เป็นต้นไป

(นางสาวทิพวรรณ อุทัยสาง)
ประธานกรรมการ