

นโยบายการใช้งานปัญญาประดิษฐ์ (Artificial Intelligence Policy)

บทนำ

เนื่องด้วยเทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence “AI”) ได้พัฒนาก้าวหน้าอย่างรวดเร็วและมีศักยภาพในการเพิ่มประสิทธิภาพการดำเนินงานของบริษัทฯ อีกทั้งมีความจำเป็นที่ต้องรักษาความปลอดภัยของข้อมูลและปฏิบัติตามกฎหมายที่เกี่ยวข้อง บริษัทฯ จึงได้กำหนดนโยบายการใช้งานปัญญาประดิษฐ์ฉบับนี้ เพื่อให้การใช้งานเป็นไปอย่างมีระบบ มีประสิทธิภาพ และสอดคล้องกับหลักธรรมาภิบาลที่ดี

วัตถุประสงค์

นโยบายฉบับนี้มีวัตถุประสงค์เพื่อ

- กำหนดกรอบการใช้งานปัญญาประดิษฐ์ให้เป็นไปอย่างเหมาะสม ปลอดภัย และก่อให้เกิดประโยชน์สูงสุดต่อบริษัทฯ
- ส่งเสริมการใช้งานเทคโนโลยีปัญญาประดิษฐ์เพื่อเพิ่มขีดความสามารถในการแข่งขันและการพัฒนานวัตกรรม
- ป้องกันความเสี่ยงที่อาจเกิดขึ้นจากการใช้งานปัญญาประดิษฐ์ รวมถึงการละเมิดความเป็นส่วนตัว การรั่วไหลของข้อมูล ความลับทางการค้า และการไม่ปฏิบัติตามกฎหมาย
- สร้างมาตรฐานการปฏิบัติงานที่เป็นเอกภาพและสามารถตรวจสอบได้ในการใช้งานเทคโนโลยีปัญญาประดิษฐ์

ขอบเขตการใช้บังคับ

นโยบายนี้ใช้บังคับกับ

- พนักงานทุกระดับของบริษัทฯและบริษัทในเครือ รวมถึงผู้บริหาร พนักงานประจำ พนักงานชั่วคราว และลูกจ้างตามสัญญาจ้าง
- ผู้รับเหมา ผู้ให้บริการ ที่ปรึกษา และคู่ค้าทางธุรกิจที่มีการเข้าถึงหรือใช้งานระบบปัญญาประดิษฐ์ของบริษัทฯ
- การใช้งานปัญญาประดิษฐ์ทุกรูปแบบ ไม่ว่าจะเป็นการใช้งานผ่านระบบภายในบริษัทฯ บริการออนไลน์ หรือแอปพลิเคชันของบุคคลที่สาม
- การประมวลผลข้อมูลทุกประเภทที่เกี่ยวข้องกับการดำเนินงานของบริษัทฯ ไม่ว่าจะเป็ข้อมูลการผลิต ข้อมูลลูกค้า ข้อมูลพนักงาน หรือข้อมูลทางการค้า

กฎหมายและข้อบังคับที่เกี่ยวข้อง

บริษัทฯ ได้คำนึงถึงการปฏิบัติตามกฎหมายและข้อบังคับที่เกี่ยวข้องดังต่อไปนี้

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และประกาศของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้อง ในส่วนที่เกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลด้วยระบบปัญญาประดิษฐ์
- พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และกฎกระทรวงที่เกี่ยวข้อง ในส่วนของการป้องกันภัยคุกคามทางไซเบอร์ต่อระบบปัญญาประดิษฐ์
- พระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537 และที่แก้ไขเพิ่มเติม ในส่วนของการสร้างผลงานโดยใช้ปัญญาประดิษฐ์และการเคารพทรัพย์สินทางปัญญาของผู้อื่น

4. ความปลอดภัย อาชีวอนามัย และสภาพแวดล้อมในการทำงาน พ.ศ. 2554 ในส่วนของการใช้ปัญญาประดิษฐ์ในการควบคุมระบบการผลิตและการรักษาความปลอดภัยของพนักงาน
5. มาตรฐานผลิตภัณฑ์อุตสาหกรรม มาตรฐานการจัดการคุณภาพ และข้อกำหนดทางเทคนิคอื่นๆ ที่เกี่ยวข้องกับการประกันคุณภาพของกระบวนการผลิต

คณะกรรมการ หน้าที่และความรับผิดชอบ

คณะกรรมการที่เกี่ยวข้องกับการใช้งานปัญญาประดิษฐ์ ประกอบด้วยคณะกรรมการ ดังต่อไปนี้

1. คณะกรรมการกำกับดูแลและขับเคลื่อนปัญญาประดิษฐ์ (“คณะกรรมการ AI”) - AI Committee

ประกอบด้วย ประธานกรรมการและผู้บริหารระดับสูงขององค์กร เพื่อเป็นตัวแทนและมีบทบาทในการกำหนดนโยบาย ทิศทางและกำกับดูแลการนำเทคโนโลยีปัญญาประดิษฐ์มาใช้ให้สอดคล้องกับเป้าหมายทางธุรกิจ โดยครอบคลุมการดำเนินงานในทุกด้านของบริษัทฯ อย่างครบถ้วน

2. คณะทำงานปฏิบัติการปัญญาประดิษฐ์ (“คณะทำงาน AI”) - AI Working Team

ประกอบด้วย ผู้บริหารและตัวแทนจากทุกกลุ่มงานในองค์กร เพื่อให้ครอบคลุมทุกกระบวนการทำงานภายในบริษัทฯ ทั้งด้านธุรกิจ เทคโนโลยีสารสนเทศ การกำกับดูแล และความปลอดภัยของข้อมูล โดยมีหน้าที่ในการขับเคลื่อนการนำ AI มาใช้ในบริษัทฯ อย่างเป็นระบบ ตั้งแต่การคัดเลือกโครงการ การพัฒนาและนำไปใช้งานจริง ตลอดจนการติดตามและปรับปรุงอย่างต่อเนื่อง โดยมุ่งให้สอดคล้องกับกลยุทธ์ทางธุรกิจและสร้างประโยชน์สูงสุดต่อองค์กร

3. คณะทำงานกำกับดูแลและบริหารความเสี่ยงด้านปัญญาประดิษฐ์ (“คณะทำงานบริหารความเสี่ยง AI”) – AI Risk and Information Security Working Team

ประกอบด้วย ผู้แทนจากหน่วยงานหลักที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศภายในบริษัทฯ โดยมีผู้บริหารหรือผู้แทนจากหน่วยงานเทคโนโลยีสารสนเทศ (IT) กฎหมาย (Legal/Compliance) และตรวจสอบภายใน (Internal Audit) เป็นองค์ประกอบสำคัญ โดยมีหน้าที่ในการกำกับดูแลและบริหารความเสี่ยงจากการพัฒนาและใช้งาน AI ให้เป็นไปอย่างเหมาะสม ปลอดภัย และสอดคล้องกับนโยบาย กฎหมาย และข้อกำหนดที่เกี่ยวข้อง โดยครอบคลุมการระบุ ประเมิน ควบคุม และติดตามความเสี่ยงที่สำคัญ เช่น ความเป็นส่วนตัวของข้อมูล และความมั่นคงปลอดภัยของระบบ พร้อมทั้งให้คำแนะนำและรายงานสถานะความเสี่ยงต่อคณะกรรมการที่เกี่ยวข้อง เพื่อสนับสนุนการตัดสินใจและส่งเสริมการใช้ AI อย่างมีความรับผิดชอบและยั่งยืนในบริษัทฯ

ประเภทการใช้งานปัญญาประดิษฐ์

การใช้งานปัญญาประดิษฐ์ สามารถแบ่งได้เป็น 4 ประเภท ดังนี้

1. การใช้งานประเภทที่ 1 (ความเสี่ยงต่ำ - อนุญาตให้ใช้งานได้ทันที)

การใช้งานในประเภทนี้ หมายถึง การใช้งานปัญญาประดิษฐ์ที่ไม่ก่อให้เกิดความเสี่ยงต่อความมั่นคงปลอดภัยของข้อมูล ไม่กระทบต่อการดำเนินธุรกิจหลักของบริษัทฯ และไม่เกี่ยวข้องกับการตัดสินใจที่สำคัญ ได้แก่ การใช้งานเพื่อวิเคราะห์แนวโน้มการผลิตจากข้อมูลที่ไม่เป็นความลับ การสร้างเอกสารคู่มือการปฏิบัติงานทั่วไป การแปลเอกสารทางเทคนิค สำหรับการสื่อสารกับคู่ค้าต่างประเทศ และการจำลองสถานการณ์การผลิตในสภาพแวดล้อมที่ไม่เชื่อมต่อกับระบบการผลิตจริง

2. การใช้งานประเภทที่ 2 (ความเสี่ยงปานกลาง - ต้องได้รับอนุมัติก่อนใช้งาน)

การใช้งานในประเภทนี้ หมายถึง การใช้งานที่อาจก่อให้เกิดความเสี่ยงในระดับปานกลางต่อบริษัทฯ อาจเกี่ยวข้องกับข้อมูลภายในบริษัทฯ แต่ไม่ถึงระดับข้อมูลลับทางการค้า หรือเกี่ยวข้องกับการตัดสินใจที่มีผลกระทบต่อการดำเนินธุรกิจ ได้แก่ การใช้งานเพื่อช่วยในการออกแบบผลิตภัณฑ์หรือกระบวนการผลิตใหม่ การพยากรณ์อุปสงค์ของตลาดหรือการวิเคราะห์แนวโน้มทางธุรกิจ และการเสนอแนะแนวทางการปรับปรุงประสิทธิภาพการผลิต การใช้งานในประเภทนี้จะต้องได้รับการอนุมัติจากหัวหน้าส่วนงานที่เกี่ยวข้องและหัวหน้าฝ่ายเทคโนโลยีสารสนเทศ พร้อมทั้งมีการประเมินความเสี่ยงเบื้องต้น อนุญาตให้นำข้อมูลลับทางการค้า ข้อมูลทางการเงินเชิงลึก หรือกลยุทธ์ทางธุรกิจ ไปใช้กับระบบปัญญาประดิษฐ์ภายนอกบริษัทฯ

3. การใช้งานประเภทที่ 3 (ความเสี่ยงสูง - ต้องได้รับอนุมัติพิเศษ)

การใช้งานในประเภทนี้ หมายถึง การใช้งานที่มีความเสี่ยงสูงและอาจส่งผลกระทบต่อบริษัทฯ พนักงาน หรือผู้มีส่วนได้เสีย ซึ่งรวมถึงการใช้งานที่เกี่ยวข้องกับข้อมูลลับทางการค้า ข้อมูลเชิงกลยุทธ์ หรือข้อมูลสำคัญต่อความสามารถในการแข่งขันของบริษัทฯ ได้แก่ การใช้ปัญญาประดิษฐ์ในการควบคุมเครื่องจักรหรือระบบการผลิตโดยตรง การตัดสินใจทางการเงินที่สำคัญ เช่น การลงทุนหรือการจัดซื้อวัตถุดิบ การจัดการห่วงโซ่อุปทานและการคัดเลือกหรือประเมินผู้จำหน่าย และการวิจัยพัฒนาผลิตภัณฑ์หรือเทคโนโลยีใหม่ การใช้งานในประเภทนี้จะต้องได้รับการอนุมัติจากคณะกรรมการกำกับดูแลปัญญาประดิษฐ์ของบริษัทฯ มีการประเมินความเสี่ยงอย่างละเอียด และมีแผนการทดลองใช้งานในขอบเขตจำกัดก่อนนำไปใช้ในวงกว้าง

4. การใช้งานที่ห้ามอย่างเด็ดขาด

บริษัทฯ ห้ามการใช้งานปัญญาประดิษฐ์ในกรณีดังต่อไปนี้ การนำข้อมูลลับของบริษัทฯ หรือความลับทางการค้าไม่ว่าทั้งหมดหรือบางส่วนไปใช้ ป้อน หรือประมวลผลผ่านระบบปัญญาประดิษฐ์ภายนอกบริษัทฯ รวมถึงการประมวลผลข้อมูลส่วนบุคคลของลูกค้า พนักงาน หรือบุคคลอื่น โดยไม่ได้รับความยินยอมหรือไม่มีฐานทางกฎหมายที่ชัดเจน การนำข้อมูลทางการเงิน กลยุทธ์การขาย กลยุทธ์การตลาด แผนธุรกิจ เงื่อนไขทางการค้า หรือข้อมูลสัญญาไปใช้กับระบบปัญญาประดิษฐ์สาธารณะหรือบริการของบุคคลที่สาม การสร้างหรือดัดแปลงเนื้อหาที่อาจละเมิดลิขสิทธิ์หรือทรัพย์สินทางปัญญาของบุคคลอื่น การใช้งานกับข้อมูลความลับทางการค้าหรือข้อมูลที่เป็นความลับของบริษัทฯ โดยไม่มีมาตรการรักษาความปลอดภัยที่เหมาะสม และการใช้ผลลัพธ์จากปัญญาประดิษฐ์เพื่อการตัดสินใจด้านความปลอดภัยในการทำงานที่อาจส่งผลกระทบต่อชีวิตและความปลอดภัยของพนักงานหรือบุคคลอื่น

มาตรการรักษาความปลอดภัยและการป้องกันข้อมูล

1. หลักการจัดการข้อมูล

บริษัทฯ ถือปฏิบัติตามหลักการลดข้อมูลให้น้อยที่สุด (Data Minimization) โดยใช้เพียงข้อมูลที่จำเป็นต่อวัตถุประสงค์การใช้งานปัญญาประดิษฐ์เท่านั้น ข้อมูลทุกประเภทที่ส่งไปยังระบบปัญญาประดิษฐ์จะต้องผ่านการเข้ารหัสด้วยมาตรฐานการเข้ารหัสที่บริษัทฯ กำหนด มีการปิดบังข้อมูลที่สามารถระบุตัวตนได้ (Anonymization) ก่อนการประมวลผล และมีการกำหนดระยะเวลาการเก็บรักษาข้อมูลและวิธีการลบข้อมูลอย่างปลอดภัยเมื่อสิ้นสุดการใช้งาน

2. การควบคุมการเข้าถึงระบบ

บริษัทฯ จะดำเนินการควบคุมการเข้าถึงระบบปัญญาประดิษฐ์ผ่านระบบการควบคุมการเข้าถึงตามบทบาท (Role-based Access Control) โดยกำหนดสิทธิ์การเข้าถึงตามหน้าที่และความจำเป็นในการใช้งาน มีระบบการยืนยันตัวตนแบบหลาย

Ch

ขั้นตอน (Multi-Factor Authentication) สำหรับการเข้าถึงข้อมูลที่มีความสำคัญ มีการบันทึกประวัติการใช้งานอย่างครบถ้วน เพื่อการตรวจสอบ และมีการทบทวนสิทธิ์การเข้าถึงเป็นประจำทุก 6 เดือน

3. การป้องกันการรั่วไหลของข้อมูล

บริษัทฯ ห้ามใช้บริการปัญญาประดิษฐ์แบบสาธารณะที่ไม่มีค่าใช้จ่าย (Free Public AI Services) สำหรับการประมวลผลข้อมูลที่เป็นความลับหรือมีความสำคัญต่อบริษัทฯ การใช้งานจะต้องผ่านเฉพาะ โซลูชันระดับองค์กร (Enterprise Solutions) ที่มีการรับประกันความปลอดภัยและการปกป้องข้อมูลอย่างเหมาะสม มีกระบวนการตรวจสอบและประเมินผลลัพธ์จากระบบปัญญาประดิษฐ์ก่อนนำไปใช้งานจริง และมีระบบสำรองข้อมูลที่แยกออกจากระบบปัญญาประดิษฐ์เพื่อป้องกันการสูญหายของข้อมูล

กระบวนการขออนุมัติการใช้งาน

สำหรับการใช้งานประเภทที่ 2 และ 3 ผู้ขออนุมัติจะต้องส่งคำขออนุมัติผ่านระบบที่บริษัทฯ กำหนดพร้อมกับรายละเอียดวัตถุประสงค์การใช้งาน ประเภทข้อมูลที่จะใช้ และมาตรการรักษาความปลอดภัย ขณะทำงาน AI จะดำเนินการประเมินความเสี่ยงเบื้องต้นและเสนอความเห็นต่อหัวหน้าส่วนงานที่เกี่ยวข้องและหัวหน้าฝ่ายเทคโนโลยีสารสนเทศเพื่อพิจารณาอนุมัติ สำหรับการใช้งานประเภทที่ 3 ผู้ขออนุมัติจะต้องจัดทำเอกสารเหตุผลความจำเป็นทางธุรกิจและการประเมินความเสี่ยงอย่างละเอียด นำเสนอต่อคณะกรรมการ AI พิจารณา เมื่อได้รับอนุมัติแล้ว จะต้องมีการทดลองใช้งานในขอบเขตจำกัดก่อนและมีการประเมินผลก่อนขยายการใช้งานในวงกว้าง

การบริหารความเสี่ยงและแผนการตอบสนองเหตุการณ์ฉุกเฉิน

1. กรณีเกิดการรั่วไหลหรือการใช้งานข้อมูลอย่างไม่เหมาะสม

เมื่อมีการตรวจพบหรือได้รับแจ้งเหตุการณ์การรั่วไหลของข้อมูลหรือการใช้งานข้อมูลอย่างไม่เหมาะสม คณะทำงานความเสี่ยง AI จะต้องดำเนินการหยุดการใช้งานระบบที่เกี่ยวข้องทันทีภายใน 1 ชั่วโมงนับจากเวลาที่ทราบเหตุ ประเมินขอบเขตและความรุนแรงของความเสียหายภายใน 4 ชั่วโมง และรายงานต่อคณะกรรมการ AI ภายใน 8 ชั่วโมง หากเหตุการณ์มีความรุนแรงและอาจกระทบต่อข้อมูลส่วนบุคคล บริษัทฯ จะแจ้งต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ภายใน 3 วัน และแจ้งต่อเจ้าของข้อมูลที่ได้รับผลกระทบภายใน 30 วัน

2. กรณีระบบปัญญาประดิษฐ์ทำงานผิดปกติหรือให้ผลลัพธ์ที่ไม่ถูกต้อง

เมื่อตรวจพบว่าระบบปัญญาประดิษฐ์ทำงานผิดปกติหรือให้ผลลัพธ์ที่ไม่ถูกต้อง ผู้ใช้งานหรือผู้ตรวจสอบจะต้องหยุดการใช้งานทันทีและย้อนกลับสู่ระบบเดิมหรือกระบวนการปกติ ฝ่ายเทคโนโลยีสารสนเทศจะดำเนินการตรวจสอบสาเหตุและประเมินผลกระทบต่อการทำงานของบริษัทฯ มีการปรับปรุงแก้ไขระบบและทดสอบการทำงานให้ถูกต้องก่อนนำกลับมาใช้งานใหม่ และจัดทำรายงานสรุปเหตุการณ์พร้อมมาตรการป้องกันเพื่อป้องกันไม่ให้เกิดเหตุการณ์ซ้ำ

การพัฒนาบุคลากรและการฝึกอบรม

1. หลักสูตรการฝึกอบรมบังคับ

พนักงานทุกคนจะต้องเข้ารับการฝึกอบรมหลักสูตรความตระหนักรู้เกี่ยวกับปัญญาประดิษฐ์ ซึ่งครอบคลุมหลักการพื้นฐานของเทคโนโลยีปัญญาประดิษฐ์ ความเสี่ยงและข้อจำกัดในการใช้งาน การปกป้องข้อมูลส่วนบุคคลและการปฏิบัติตามกฎหมายที่เกี่ยวข้อง และการรักษาความปลอดภัยทางไซเบอร์ การฝึกอบรมจะจัดขึ้นเป็นประจำทุกปีและมีการประเมินผลเพื่อให้แน่ใจว่าพนักงานมีความรู้ความเข้าใจที่เพียงพอ

Ch

2. หลักสูตรสำหรับผู้ใช้งานปัญญาประดิษฐ์

พนักงานที่ได้รับอนุมัติให้ใช้งานปัญญาประดิษฐ์จะต้องเข้ารับการฝึกอบรมเพิ่มเติมในหัวข้อเทคนิคการสร้างคำสั่งที่มีประสิทธิภาพ (Prompt Engineering) จริยธรรมในการใช้งานปัญญาประดิษฐ์และการตัดสินใจอย่างมีความรับผิดชอบ การตรวจสอบคุณภาพและความถูกต้องของผลลัพธ์จากระบบปัญญาประดิษฐ์ และกรณีศึกษาการใช้งานที่ดีและข้อผิดพลาดที่ควรหลีกเลี่ยง

3. หลักสูตรสำหรับผู้บริหารและผู้กำกับดูแล

ผู้บริหารระดับสูงและสมาชิกคณะกรรมการ AI จะต้องเข้ารับการฝึกอบรมในหัวข้อการกำกับดูแลปัญญาประดิษฐ์ระดับองค์กร กลยุทธ์การนำเทคโนโลยีปัญญาประดิษฐ์มาใช้เพื่อสร้างความได้เปรียบทางการแข่งขัน การบริหารจัดการความเสี่ยงที่เกี่ยวข้องกับปัญญาประดิษฐ์ และความเข้าใจเชิงลึกเกี่ยวกับกฎหมายและข้อบังคับที่เกี่ยวข้อง รวมถึงแนวโน้มการเปลี่ยนแปลงในอนาคต

การกำหนดโทษและมาตรการทางวินัย

1. ระดับความร้ายแรงของการฝ่าฝืน

1.1 การฝ่าฝืนนโยบายระดับเบา ได้แก่ การใช้งานโดยไม่ได้รับอนุมัติในกรณีที่ไม่ก่อให้เกิดความเสียหายหรือความเสี่ยงต่อบริษัทฯ การไม่เข้าร่วมการฝึกอบรมตามกำหนดเวลาโดยไม่มีเหตุผลอันสมควร หรือการไม่ปฏิบัติตามขั้นตอนการใช้งานในรายละเอียดย่อยที่ไม่ส่งผลกระทบต่อความปลอดภัย สำหรับกรณีเหล่านี้ บริษัทฯจะดำเนินการตักเตือนด้วยวาจาและจัดให้มีการฝึกอบรมเพิ่มเติม

1.2 การฝ่าฝืนนโยบายระดับกลาง ได้แก่ การใช้งานข้อมูลโดยไม่ปฏิบัติตามมาตรการรักษาความปลอดภัยที่กำหนด การไม่รายงานเหตุการณ์ที่เกิดขึ้นหรือความผิดปกติที่ตรวจพบ การใช้งานบริการปัญญาประดิษฐ์ที่ไม่ได้รับอนุมัติจากบริษัทฯ หรือการไม่ปฏิบัติตามคำแนะนำด้านความปลอดภัยอย่างต่อเนื่อง สำหรับกรณีเหล่านี้ บริษัทฯจะดำเนินการตักเตือนเป็นลายลักษณ์อักษรและระงับสิทธิ์การใช้งานระบบปัญญาประดิษฐ์เป็นเวลา 30 วัน

1.3 การฝ่าฝืนนโยบายระดับหนัก ได้แก่ การใช้งานปัญญาประดิษฐ์ในลักษณะที่อาจส่งผลกระทบต่อความปลอดภัยของพนักงานหรือบุคคลอื่น การเปิดเผยหรือนำข้อมูลความลับทางการค้าไปใช้กับระบบภายนอกโดยไม่ได้รับอนุมัติ การละเมิดกฎหมายคุ้มครองข้อมูลส่วนบุคคลอย่างจงใจหรือด้วยความประมาทเลินเล่ออย่างร้ายแรง หรือการใช้งานเพื่อสร้างเนื้อหาที่ผิดกฎหมายหรือขัดต่อศีลธรรม สำหรับกรณีเหล่านี้ บริษัทฯอาจพิจารณาการลงโทษทางวินัยระดับร้ายแรง รวมถึงการเลิกจ้าง

2. กระบวนการพิจารณาทางวินัย

เมื่อมีการตรวจพบหรือได้รับรายงานเกี่ยวกับการฝ่าฝืนนโยบาย บริษัทฯ จะจัดตั้งคณะกรรมการสอบสวนซึ่งประกอบด้วยตัวแทนจากฝ่ายทรัพยากรบุคคล ฝ่ายเทคโนโลยีสารสนเทศ และฝ่ายงานที่เกี่ยวข้อง จะดำเนินการสอบสวนข้อเท็จจริงอย่างเป็นธรรมและครบถ้วน การสอบสวนอาจรวมถึงการรวบรวมและตรวจสอบพยานหลักฐานที่เกี่ยวข้อง ทั้งในรูปแบบเอกสาร ข้อมูลอิเล็กทรอนิกส์ บันทึกการใช้งานระบบ รายงานจากเครื่องมือปัญญาประดิษฐ์ หรือข้อมูลทางเทคนิคอื่นใด โดยต้องดำเนินการโดยคำนึงถึงการรักษาความลับ ความปลอดภัยของข้อมูล และการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายที่เกี่ยวข้อง โดยให้โอกาสผู้ที่ถูกกล่าวหาได้ชี้แจงข้อเท็จจริงและนำเสนอหลักฐานเพื่อแก้ต่าง การพิจารณาทางวินัยจะคำนึงถึงความร้ายแรงของการกระทำ ลักษณะและขอบเขตของการฝ่าฝืนนโยบาย ผลกระทบที่เกิดขึ้นต่อบริษัทฯ ถูกค้า หรือบุคคลภายนอก ประวัติการทำงานของผู้กระทำผิด รวมถึงเจตนาและพฤติการณ์แห่งการกระทำ โดยคำสั่งลงโทษ

Ch

ทางวินัยจะออกเป็นลายลักษณ์อักษรพร้อมระบุเหตุผล และบริษัทฯ อาจกำหนดให้มีการติดตาม ตรวจสอบ หรือกำหนด มาตรการแก้ไข ปรับปรุง หรืออบรมเพิ่มเติม เพื่อป้องกันมิให้เกิดการฝ่าฝืนนโยบายในลักษณะเดียวกันอีกในอนาคต

การทบทวนและปรับปรุงนโยบาย

1. กำหนดเวลาการทบทวน

นโยบายฉบับนี้ จะได้รับการทบทวนอย่างสม่ำเสมอเป็นประจำทุกสัปดาห์ โดยคณะกรรมการ AI เพื่อประเมินความ เหมาะสมและประสิทธิผลของการนำไปปฏิบัติ วิเคราะห์ความเปลี่ยนแปลงในเทคโนโลยี กฎหมาย และสภาพแวดล้อมทาง ธุรกิจ และพิจารณาการปรับปรุงแก้ไขให้สอดคล้องกับความเปลี่ยนแปลงดังกล่าว นอกจากนี้ จะมีการทบทวนเร่งด่วนใน กรณีที่มีการประกาศใช้กฎหมายใหม่ที่เกี่ยวข้อง การเกิดเหตุการณ์สำคัญที่ส่งผลกระทบต่อบริษัทฯ หรือการเปลี่ยนแปลง เทคโนโลยีอย่างมีนัยสำคัญ

2. กระบวนการปรับปรุงนโยบาย

การทบทวนและปรับปรุงนโยบายจะดำเนินการ โดยการรวบรวมข้อมูลป้อนกลับจากผู้ใช้งาน ผู้บริหาร และผู้มีส่วนได้เสียที่ เกี่ยวข้อง การวิเคราะห์ช่องว่างระหว่างนโยบายกับการปฏิบัติจริงและผลกระทบที่เกิดขึ้น การศึกษาแนวปฏิบัติที่ดีจาก บริษัทฯ ชำนาญในอุตสาหกรรมเดียวกันและอุตสาหกรรมอื่นที่เกี่ยวข้อง การร่างนโยบายใหม่หรือการแก้ไขเพิ่มเติมโดยทีม ผู้เชี่ยวชาญ การปรึกษาหารือกับหน่วยงานกำกับดูแลที่เกี่ยวข้องและผู้เชี่ยวชาญภายนอกตามความจำเป็น และการนำเสนอ ร่างนโยบายที่ปรับปรุงแล้วต่อคณะกรรมการบริหารเพื่อพิจารณาอนุมัติ

บทสุดท้าย

1. การมีผลใช้บังคับ

นโยบายฉบับนี้มีผลใช้บังคับตั้งแต่วันที่ประกาศเป็นต้นไป ในกรณีที่มีข้อสงสัยหรือข้อขัดแย้งในการตีความ ให้ถือตามคำ วินิจฉัยของคณะกรรมการ AI เป็นที่สุด

2. การแจ้งให้ทราบและการเข้าถึงนโยบาย

บริษัทฯ จะดำเนินการแจ้งให้พนักงานทุกคนทราบถึงนโยบายฉบับนี้ผ่านช่องทางการสื่อสารภายในบริษัทที่หลากหลาย จัดให้มีการเผยแพร่ นโยบายในระบบสารสนเทศภายในบริษัทที่พนักงานสามารถเข้าถึงได้สะดวก และจัดให้มีสำเนา นโยบายในรูปแบบเอกสารไว้ที่หน่วยงานทรัพยากรบุคคลและหน่วยงานที่เกี่ยวข้อง

3. การติดต่อและสอบถาม

พนักงานสามารถติดต่อสอบถามข้อมูลเพิ่มเติมหรือรายงานเหตุการณ์ที่เกี่ยวข้องกับการใช้งานปัญญาประดิษฐ์ได้ที่ คณะทำงาน AI ฝ่ายเทคโนโลยีสารสนเทศ หรือผ่านช่องทางที่บริษัทฯ กำหนด การรายงานจะได้รับการคุ้มครองความลับ และการปกป้องผู้รายงานตามนโยบายการแจ้งเบาะแสของบริษัทฯ

นโยบายนี้ให้มีผลบังคับใช้ตั้งแต่วันที่ 1 พฤษภาคม 2569 เป็นต้นไป



นายสนั่น อังอุบลกุล

กรรมการผู้จัดการ

บริษัท ศรีไทยซูเปอร์แวร์ จำกัด (มหาชน)

