CENTRALPATTANA

นโยบายด้านความปลอดภัยสารสนเทศ
และการพัฒนาเทคโนโลยีปัญญาประดิษฐ์อย่างรับผิดชอบ
บริษัท เซ็นทรัลพัฒนา จำกัด (มหาชน)

1. บทนำ

ในยุคที่เทคโนโลยีสารสนเทศและปัญญาประดิษฐ์ (Artificial Intelligence - AI) เข้ามามีบทบาทสำคัญต่อการดำเนินธุรกิจและการสร้างความได้เปรียบทางการแข่งขัน การบริหารจัดการด้านความปลอดภัยของสารสนเทศ (Information Security) และการใช้งาน AI อย่างปลอดภัยจึงถือเป็นหัวใจสำคัญในการสร้างความเชื่อมั่นแก่ผู้มีส่วนได้เสียทุกกลุ่ม ทั้งลูกค้า คู่ค้า ผู้ถือหุ้น และบุคลากรของบริษัท ความผิดพลาดหรือการใช้งานเทคโนโลยีและ AI โดยขาดความระมัดระวัง อาจนำไปสู่ความเสียหายร้ายแรงต่อความมั่นคงทางธุรกิจ ความน่าเชื่อถือ และความปลอดภัยของข้อมูลที่มีความสำคัญ บริษัท เซ็นทรัลพัฒนา จำกัด (มหาชน) และบริษัทย่อย ("บริษัท") ตระหนักถึงความสำคัญของการบริหารจัดการด้านความปลอดภัยของสารสนเทศและการพัฒนาเทคโนโลยีปัญญาประดิษฐ์อย่างรับผิดชอบ เพื่อรองรับการเปลี่ยนแปลงในยุคดิจิทัลและสร้างคุณค่าที่ยั่งยืนแก่ธุรกิจและสังคม โดยมุ่งมั่นที่จะดำเนินงานให้เป็นไปตามมาตรฐานสูงสุดในระดับสากล ผ่านการยึดถือแนวปฏิบัติตามกรอบการกำกับดูแลที่สำคัญ เช่น กฎระเบียบข้อบังคับตามกฎหมายของประเทศไทย รวมถึงกฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDPA) และมาตรฐานสากล เช่น ISO/IEC 27001 รวมถึงแนวปฏิบัติด้านธรรมาภิบาลที่กำหนดโดย IOD

นอกจากนี้ บริษัทยังให้ความสำคัญกับการใช้เทคโนโลยี AI อย่างปลอดภัยและมีจริยธรรม โดยกำหนดมาตรฐานในการป้องกันความเสี่ยงจากการใช้งาน AI เช่น การรั่วไหลของข้อมูล การตัดสินใจที่ไม่เป็นธรรม หรือการถูกโจมตีทางไซเบอร์ที่เกี่ยวข้องกับ AI เพื่อให้การใช้งาน AI สามารถส่งเสริมการดำเนินธุรกิจอย่างมีประสิทธิภาพและยังคงรักษาความไว้วางใจจากผู้มีส่วนได้เสียทุกกลุ่ม

บริษัทมุ่งหวังที่จะสร้างความมั่นใจให้กับทุกภาคส่วน โดยการเสริมสร้างมาตรการและแนวปฏิบัติด้านความปลอดภัยของสารสนเทศและ AI ให้มีประสิทธิภาพสูงสุด เพื่อลดความเสี่ยงในการรั่วไหลหรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต ตลอดจนป้องกันและจัดการภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น พร้อมทั้งพัฒนานโยบายและแนวปฏิบัติให้เหมาะสมกับสภาพแวดล้อมทางธุรกิจและเทคโนโลยีที่เปลี่ยนแปลงอย่างรวดเร็ว ด้วยการยึดมั่นในความโปร่งใส ความน่าเชื่อถือ และการบริหารจัดการอย่างยั่งยืน บริษัทจึงกำหนดนโยบายและแนวปฏิบัติด้านความปลอดภัยสารสนเทศ และการพัฒนาเทคโนโลยีปัญญาประดิษฐ์อย่างรับผิดชอบนี้ขึ้น เพื่อเป็นกรอบการทำงานสำหรับบุคลากรและผู้มีส่วนเกี่ยวข้องทุกฝ่ายในการปฏิบัติงานให้สอดคล้องกับความมุ่งมั่นของบริษัทและมาตรฐานที่ได้รับการยอมรับในระดับสากล

2. ขอบเขตนโยบาย

นโยบายด้านความปลอดภัยสารสนเทศและการพัฒนาเทคโนโลยีปัญญาประดิษฐ์อย่างรับผิดชอบนี้มีผลบังคับใช้กับบุคลากรทุกระดับของ บริษัทรวมถึงพนักงานประจำ พนักงานชั่วคราว ผู้บริหาร คู่ค้า และผู้ที่เกี่ยวข้องที่ได้รับมอบหมายหรือได้รับสิทธิ์ในการเข้าถึงข้อมูลหรือระบบเทคโนโลยี ของบริษัทนโยบายนี้ครอบคลุมการจัดเก็บ การใช้ และการป้องกันข้อมูลทุกประเภทของบริษัททั้งข้อมูลทางการเงิน ข้อมูลการดำเนินธุรกิจ ข้อมูลส่วนบุคคลของลูกค้า คู่ค้า พนักงาน และผู้มีส่วนได้เสียทุกกลุ่ม รวมถึงการพัฒนาและการใช้งานเทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence - AI) อย่างมีจริยธรรมและปลอดภัย

3. วัตถุประสงค์

- เพื่อป้องกันการรั่วไหล การเข้าถึงโดยไม่ได้รับอนุญาต และการถูกโจมตีทางไซเบอร์ที่อาจก่อให้เกิดความเสียหายต่อข้อมูลและระบบเทคโนโลยีของบริษัท
- เพื่อให้การพัฒนาและใช้งาน AI ของบริษัทเป็นไปอย่างปลอดภัย โปร่งใส ยุติธรรม และไม่สร้างผลกระทบในเชิงลบต่อผู้มีส่วนได้เสียทุกกลุ่ม
- เพื่อให้การดำเนินงานด้านความปลอดภัยสารสนเทศและ AI เป็นไปตามกฎหมาย ระเบียบข้อบังคับ และมาตรฐานที่เกี่ยวข้อง เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) มาตรฐาน ISO/IEC 27001 และหลักธรรมาภิบาลที่กำหนดไว้ในคู่มือจรรยาบรรณและหลักการกำกับดูแลกิจการของบริษัท
- เพื่อสร้างความเชื่อมั่นในความโปร่งใสและความน่าเชื่อถือของบริษัทในการจัดการข้อมูลและการใช้เทคโนโลยีอย่างรับผิดชอบ
- เพื่อให้การบริหารจัดการด้านความปลอดภัยสารสนเทศและ AI สอดคล้องกับเป้าหมายการพัฒนาที่ยั่งยืน (SDGs) และส่งเสริมความสามารถทางการแข่งขันของบริษัทในระยะยาว

4. หน้าที่ความรับผิดชอบ

เพื่อให้การบริหารจัดการด้านความปลอดภัยสารสนเทศและการพัฒนาเทคโนโลยีปัญญาประดิษฐ์เป็นไปอย่างมีประสิทธิภาพ ครอบคลุมทุกระดับขององค์กร และสอดคล้องกับทิศทางธุรกิจของบริษัทจึงกำหนดหน้าที่และความรับผิดชอบของหน่วยงานและบุคคลที่เกี่ยวข้อง ดังนี้

4.1 คณะกรรมการบริษัท

- อนุมัติและกำกับดูแลนโยบายด้านความปลอดภัยสารสนเทศและการพัฒนาเทคโนโลยีปัญญาประดิษฐ์อย่างรับผิดชอบให้สอดคล้องกับเป้าหมายเชิงกลยุทธ์และแนวทางธรรมาภิบาลของบริษัท
- ทบทวนนโยบายให้เหมาะสมกับการเปลี่ยนแปลงของสภาพแวดล้อมทางธุรกิจ กฎหมาย และมาตรฐานสากล
- พิจารณารายงานผลการดำเนินงานด้านความปลอดภัยสารสนเทศและ AI รวมถึงการจัดการความเสี่ยงและโอกาสที่สำคัญในแต่ละปี
- ให้คำแนะนำเชิงกลยุทธ์แก่ผู้บริหารระดับสูงเพื่อส่งเสริมความยั่งยืนในด้านเทคโนโลยีและการป้องกันความเสี่ยง

4.2 ผู้บริหารระดับสูง

- จัดสรรทรัพยากร เช่น บุคลากร งบประมาณ และเทคโนโลยีให้เพียงพอและเหมาะสมต่อการดำเนินงานด้านความปลอดภัยสารสนเทศและ AI
- ติดตามความคืบหน้าของการดำเนินงานและการจัดการภัยคุกคาม รวมถึงการตรวจสอบระบบและการประเมินความปลอดภัยอย่างสม่ำเสมอ
- สนับสนุนการพัฒนากระบวนการจัดการ AI อย่างมีจริยธรรม และตรวจสอบให้แน่ใจว่าการพัฒนา AI สอดคล้องกับแนวทางของบริษัท
- ส่งเสริมการสร้างความรู้ ความเข้าใจ และความตระหนักแก่พนักงานและคู่ค้า โดยเน้นถึงความสำคัญของความปลอดภัยสารสนเทศและการใช้งาน AI อย่างมีจริยธรรม
- รายงานการดำเนินงานและความท้าทายที่สำคัญด้านความปลอดภัยสารสนเทศให้คณะกรรมการบริษัทหรือคณะกรรมการชุดย่อยที่เกี่ยวข้องทราบเป็นระยะ

4.3 หน่วยงานที่เกี่ยวข้อง

- พัฒนาระบบจัดเก็บและจัดการข้อมูลสารสนเทศและข้อมูลที่เกี่ยวข้องกับ AI ให้มีความปลอดภัยและเป็นไปตามข้อกำหนด
- ดำเนินการตรวจสอบและติดตามภัยคุกคามทางไซเบอร์ รวมถึงการพัฒนาแผนรับมือที่เหมาะสม
- ประสานงานกับผู้บริหารและหน่วยงานภายนอกที่เกี่ยวข้องในการจัดการความเสี่ยงและข้อพิพาทที่เกิดขึ้น
- ติดตามแนวโน้มเทคโนโลยีและภัยคุกคามที่เกี่ยวข้องกับความปลอดภัยสารสนเทศและ AI เพื่อเสนอแนะแนวทางการพัฒนาที่ทันสมัย
- อบรมบุคลากรที่เกี่ยวข้องให้มีความเข้าใจในระบบและเครื่องมือที่เกี่ยวข้องกับการจัดการความปลอดภัย

4.4 พนักงาน

- ปฏิบัติตามนโยบาย แนวปฏิบัติ และมาตรการด้านความปลอดภัยสารสนเทศและ AI ที่บริษัทกำหนด
- ใช้ข้อมูลและเทคโนโลยีของบริษัทอย่างเหมาะสม โดยหลีกเลี่ยงการกระทำที่อาจนำไปสู่ความเสียหายหรือการละเมิดสิทธิ์
- แจ้งผู้บังคับบัญชาในกรณีที่พบเห็นภัยคุกคามทางไซเบอร์ การละเมิดข้อมูล หรือการใช้งาน AI ที่ไม่เหมาะสม
- เข้าร่วมการอบรมหรือกิจกรรมที่เกี่ยวข้องกับความปลอดภัยสารสนเทศและ AI เพื่อเพิ่มความรู้และความตระหนักในบทบาทที่สำคัญ

5. นโยบายและแนวปฏิบัติ

5.1) บุคลากรทุกคนต้องปฏิบัติตามนโยบายและมาตรการด้านความปลอดภัยสารสนเทศที่กำหนดไว้ โดยต้องปกป้องข้อมูลที่เป็นความลับของบริษัท ลูกค้า คู่ค้า และพนักงาน ไม่ให้เกิดการรั่วไหลหรือการนำไปใช้โดยไม่ได้รับอนุญาต

5.2) ห้ามนำข้อมูลภายในของบริษัทไปใช้หรือเปิดเผยเพื่อผลประโยชน์ส่วนตัวหรือบุคคลที่สาม โดยไม่ได้รับการอนุมัติล่วงหน้า

5.3) มีการจัดการและควบคุมการเข้าถึงข้อมูลอย่างเหมาะสม โดยใช้ระบบรักษาความปลอดภัยที่ทันสมัยและสอดคล้องกับมาตรฐานที่เกี่ยวข้อง

5.4) บุคลากรทุกคนต้องใช้ระบบและอุปกรณ์เทคโนโลยีของบริษัทเพื่อวัตถุประสงค์ในการทำงานเท่านั้น ห้ามนำไปใช้ในทางที่อาจก่อให้เกิดความเสียหายหรือความเสี่ยงต่อความปลอดภัย

5.5) ห้ามติดตั้ง ซอฟต์แวร์ หรือโปรแกรมใด ๆ บนอุปกรณ์ของบริษัทโดยไม่ได้รับอนุญาต เพื่อป้องกันความเสี่ยงจากมัลแวร์หรือไวรัสคอมพิวเตอร์

5.6) การพัฒนาและใช้งาน AI ต้องดำเนินการอย่างมีความรับผิดชอบ โดยคำนึงถึงความโปร่งใส ความเป็นธรรม และไม่สร้างผลกระทบเชิงลบต่อผู้มีส่วนได้เสีย

5.7) บุคลากรต้องหลีกเลี่ยงการใช้ AI ในลักษณะที่ก่อให้เกิดความลำเอียงหรือการเลือกปฏิบัติ และต้องประเมินผลกระทบของ AI ต่อความเป็นส่วนตัวของข้อมูล

5.8) การใช้งาน AI ต้องได้รับการตรวจสอบและประเมินผลอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าเป็นไปตามหลักจริยธรรมและกฎหมายที่เกี่ยวข้อง

5.9) บริษัทมีมาตรการป้องกันภัยคุกคามทางไซเบอร์อย่างเข้มงวด เช่น การตรวจสอบระบบอย่างสม่ำเสมอ การเข้ารหัสข้อมูล และการพัฒนาแผนรับมือในกรณีที่เกิดเหตุไม่คาดฝัน

5.10) บุคลากรมีหน้าที่รายงานเหตุการณ์ที่เกี่ยวข้องกับภัยคุกคามหรือการละเมิดความปลอดภัยของระบบทันทีที่พบ

5.11) บุคลากรทุกคนมีหน้าที่ปฏิบัติตามมาตรการและแนวทางที่กำหนด รวมถึงเข้าร่วมการฝึกอบรมที่เกี่ยวข้อง เพื่อพัฒนาความรู้ความเข้าใจในด้านความปลอดภัยของข้อมูลและ AI

5.12) ส่งเสริมให้บุคลากรมีจิตสำนึกและความระมัดระวังในการใช้ข้อมูลและเทคโนโลยีของบริษัท

5.13) การจัดการข้อมูลส่วนบุคคลต้องเป็นไปตามกฎหมายที่เกี่ยวข้อง โดยมีมาตรการคุ้มครองความเป็นส่วนตัว (Privacy) ของข้อมูลในทุกกระบวนการ

5.14) บริษัทมุ่งมั่นที่จะปฏิบัติตามมาตรฐานระดับสากลในการบริหารจัดการข้อมูลและเทคโนโลยี

5.15) บริษัทจะดำเนินการตรวจสอบและปรับปรุงนโยบายและมาตรการด้านความปลอดภัยสารสนเทศและ AI อย่างสม่ำเสมอ เพื่อให้ทันต่อการเปลี่ยนแปลงทางเทคโนโลยีและธุรกิจ

6. การฝึกอบรม

บริษัทมีความมุ่งมั่นในการส่งเสริมความรู้ ความเข้าใจ และการปฏิบัติตามนโยบายด้านความปลอดภัยสารสนเทศและการพัฒนาเทคโนโลยีปัญญาประดิษฐ์อย่างรับผิดชอบแก่คณะกรรมการ ผู้บริหาร และพนักงานทุกระดับ ผ่านกิจกรรมต่าง ๆ เช่น การฝึกอบรม การประชุมเชิงปฏิบัติการ และเวิร์กช็อป โดยเนื้อหาจะครอบคลุมถึงหลักการรักษาความปลอดภัยข้อมูล การใช้งาน AI อย่างมีจริยธรรม การป้องกันภัยคุกคามทางไซเบอร์ และการจัดการข้อมูลส่วนบุคคลให้ปลอดภัย เนื้อหาการฝึกอบรมจะถูกออกแบบให้สอดคล้องกับลักษณะงานและความต้องการขององค์กร เพื่อให้บุคลากรสามารถนำไปปรับใช้ในกระบวนการทำงานได้อย่างเหมาะสม บริษัทยังมุ่งเน้นการติดตามและประเมินผลการถ่ายทอดความรู้ เพื่อให้มั่นใจว่าบุคลากรทุกคนมีความเข้าใจชัดเจนและสามารถปฏิบัติตามแนวทางขององค์กรได้อย่างมีประสิทธิภาพ

7. การร้องเรียนและการแจ้งเบาะแส

บริษัทเปิดช่องทางให้พนักงานและผู้มีส่วนได้เสียสามารถร้องเรียนหรือแจ้งเบาะแสเกี่ยวกับการละเมิดนโยบายด้านความปลอดภัยสารสนเทศและการพัฒนาเทคโนโลยีปัญญาประดิษฐ์อย่างรับผิดชอบ โดยกระบวนการดังกล่าวจะดำเนินการตามนโยบายการแจ้งเบาะแสของบริษัทพร้อมทั้งรับประกันความปลอดภัยและความลับของข้อมูลตลอดจนสิทธิของผู้ร้องเรียน เพื่อป้องกันการตอบโต้หรือผลกระทบที่อาจเกิดขึ้นในระหว่างกระบวนการสอบสวน บริษัทให้ความสำคัญกับความโปร่งใส ความซื่อสัตย์ และการสร้างวัฒนธรรมองค์กรที่ตระหนักถึงความรับผิดชอบต่อความปลอดภัยของข้อมูลและการพัฒนาเทคโนโลยีอย่างมีจริยธรรม

8. การกำหนดบทลงโทษ

บริษัทยืนยันความสำคัญของการปฏิบัติตามนโยบายด้านความปลอดภัยสารสนเทศและการพัฒนาเทคโนโลยีปัญญาประดิษฐ์อย่างรับผิดชอบ อย่างเคร่งครัด พนักงานทุกคนต้องให้ความร่วมมือในกระบวนการตรวจสอบและสอบสวนกรณีการละเมิดนโยบายอย่างเต็มที่ หากพบว่ามีการกระทำผิดหรือฝ่าฝืนนโยบาย บริษัทจะดำเนินการลงโทษตามระเบียบวินัยของบริษัทอย่างเหมาะสม เพื่อสร้างมาตรฐานการปฏิบัติงานที่โปร่งใส สนับสนุนการพัฒนาเทคโนโลยีที่ปลอดภัยและมีจริยธรรม ตลอดจนรักษาความเชื่อมั่นจากผู้มีส่วนได้เสีย

9. การทบทวนและปรับปรุงนโยบาย

บริษัทกำหนดให้มีการตรวจสอบและปรับปรุงนโยบายด้านความปลอดภัยสารสนเทศและการพัฒนาเทคโนโลยีปัญญาประดิษฐ์อย่างรับผิดชอบ อย่างต่อเนื่อง อย่างน้อยปีละหนึ่งครั้ง หรือเมื่อมีการเปลี่ยนแปลงด้านกฎหมาย กฎระเบียบ หรือแนวปฏิบัติที่เกี่ยวข้อง เพื่อให้มั่นใจว่านโยบายดังกล่าวยังคงเหมาะสมและมีประสิทธิภาพในการตอบสนองต่อการเปลี่ยนแปลงทางธุรกิจและเทคโนโลยี นอกจากนี้ บริษัทมุ่งเน้นการพัฒนากระบวนการจัดการด้านความปลอดภัยและ AI ที่สามารถตอบสนองต่อความต้องการของผู้มีส่วนได้เสีย รวมถึงสนับสนุนการเติบโตอย่างยั่งยืนและการดำเนินธุรกิจที่มีความรับผิดชอบในระยะยาว

ทั้งนี้ ให้นโยบายด้านความปลอดภัยสารสนเทศ และการพัฒนาเทคโนโลยีปัญญาประดิษฐ์อย่างรับผิดชอบฉบับนี้ มีผลตั้งแต่วันที่ 2 พฤษภาคม 2568 เป็นต้นไป