นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและธรรมาภิบาลปัญญาประดิษฐ์

บริษัท มิสเตอร์. ดี.ไอ.วาย. โฮลดิ้ง (ประเทศไทย) จำกัด (มหาชน) และบริษัทย่อย

7 สิงหาคม 2569

ฉบับที่ 1

อนุมัติโดยที่ประชุมคณะกรรมการบริษัท: 7 สิงหาคม 2569

นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและธรรมาภิบาลปัญญาประดิษฐ์

บริษัท มิสเตอร์. ดี.ไอ.วาย. โฮลดิ้ง (ประเทศไทย) จำกัด (มหาชน) ("**บริษัท**") รวมถึงบริษัทย่อย เรียกรวมกันว่า ("**กลุ่มบริษัท**") ได้นำระบบเทคโนโลยีสารสนเทศมาใช้ในการดำเนินงานเพื่อสนับสนุนการดำเนินธุรกิจ เพิ่มประสิทธิภาพในการปฏิบัติงาน และอำนวยความสะดวกให้แก่ผู้มีส่วนได้เสียที่เกี่ยวข้อง

เพื่อให้การใช้งานระบบเทคโนโลยีสารสนเทศเป็นไปอย่างเหมาะสม มีความมั่นคงปลอดภัย และสามารถป้องกันความเสี่ยงหรือภัยคุกคามทางไซเบอร์ที่อาจส่งผลกระทบต่อการดำเนินงานและข้อมูลของ กลุ่มบริษัท กลุ่มบริษัทจึงกำหนดนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และธรรมาภิบาลปัญญาประดิษฐ์ฉบับนี้ขึ้น เพื่อเป็นกรอบแนวทางในการกำกับดูแลและแนวทางปฏิบัติ สำหรับพนักงาน คู่ค้าและพันธมิตรทางธุรกิจ ผู้ให้บริการ ที่ปรึกษา และบุคคลภายนอกที่มีปฏิสัมพันธ์กับระบบหรือข้อมูลของกลุ่มบริษัท

วัตถุประสงค์

นโยบายฉบับนี้มีวัตถุประสงค์เพื่อ:

- คุ้มครองทรัพย์สินด้านข้อมูลและสนับสนุนความต่อเนื่องในการดำเนินธุรกิจของบริษัท
- กำหนดกรอบและความคาดหวังด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศที่ชัดเจนสำหรับบุคคลและองค์กรภายนอกที่เกี่ยวข้อง
- ส่งเสริมให้มีการปฏิบัติตามกฎหมาย ระเบียบ และข้อบังคับที่เกี่ยวข้องกับการคุ้มครองข้อมูลอย่างเหมาะสม
- รักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งาน (Availability) ของข้อมูลและระบบสารสนเทศของบริษัท
- ลดและป้องกันความเสี่ยงด้านความมั่นคงปลอดภัยจากการเข้าถึง การใช้ หรือการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต
- ส่งเสริมให้การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศและการคุ้มครองข้อมูลเป็นส่วนหนึ่งของระบบการบริหารความเสี่ยงและการกำกับดูแลการปฏิบัติตามกฎหมายของกลุ่มบริษัท
- ส่งเสริมการใช้ปัญญาประดิษฐ์ (AI Governance) อย่างปลอดภัย (Safety) มีความรับผิดชอบ (Accountability) และป้องกันการใช้งานในทางที่ผิดหรือไม่เหมาะสม (Misuse)

ขอบเขตการบังคับใช้

นโยบายฉบับนี้ใช้บังคับกับบุคคลและองค์กรทุกประเภทที่เข้าเงื่อนไขดังต่อไปนี้:

- ผู้ที่เข้าถึงระบบหรือเครือข่ายเทคโนโลยีสารสนเทศของกลุ่มบริษัท
- ผู้ที่จัดการ ประมวลผล หรือมีความเกี่ยวข้องกับข้อมูลสำคัญของกลุ่มบริษัท
- คู่ค้าหรือพันธมิตรทางธุรกิจ ผู้ให้บริการ ที่ปรึกษา หรือบุคคลภายนอก ที่ให้บริการด้านเทคโนโลยีสารสนเทศการประมวลผลข้อมูล หรือบริการที่เกี่ยวข้องอื่นๆ แก่กลุ่มบริษัท
- ผู้ที่ปฏิบัติงานภายใต้โครงการหรือสัญญาของบริษัทที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศของกลุ่มบริษัท
- คู่ค้าและพันธมิตรทางธุรกิจ ผู้ให้บริการ ที่ปรึกษา หรือบุคคลภายนอก ทางธุรกิจทุกฝ่ายต้องปฏิบัติตามนโยบายฉบับนี้เป็นเงื่อนไขหนึ่งของการเข้าถึงระบบและข้อมูลของกลุ่มบริษัท

นโยบายฉบับนี้ครอบคลุมการดำเนินงานทั้งหมดของกลุ่มบริษัท รวมถึงพนักงาน คู่ค้าและพันธมิตรทางธุรกิจ ผู้ให้บริการ ผู้ประมวลผลข้อมูล ที่ปรึกษา และบุคคลภายนอกที่เกี่ยวข้องกับการเข้าถึง การใช้ หรือการประมวลผลข้อมูลของกลุ่มบริษัท

แนวปฏิบัติ

1. **บทบาท หน้าที่และความรับผิดชอบ**

1.1 คณะกรรมการบริษัท

มีบทบาทในการกำกับดูแลภาพรวมด้านความมั่นคงปลอดภัยสารสนเทศของบริษัท โดยรับทราบประเด็นความเสี่ยงและประเด็นสำคัญที่มีนัยสำคัญต่อการดำเนินธุรกิจ และให้คำแนะนำในระดับนโยบายตามความเหมาะสม

1.2 คณะกรรมการตรวจสอบและบริหารความเสี่ยง

มีบทบาทในกำกับดูแล ทบทวน และประเมินความเสี่ยงด้านไซเบอร์ รวมถึงผลกระทบที่อาจเกิดขึ้นตลอดจนกำกับให้มีการรายงานความคืบหน้าต่อคณะกรรมการบริษัทอย่างสม่ำเสมอ

1.3 ประธานเจ้าหน้าที่บริหาร

มีบทบาทในการกำกับดูแลและสนับสนุนการดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศในระดับองค์กร โดยทำหน้าที่กำหนดทิศทางและสร้างความตระหนักถึงความสำคัญของความมั่นคงปลอดภัยสารสนเทศให้สอดคล้องกับกลยุทธ์และการดำเนินธุรกิจของบริษัท รวมถึงสนับสนุนให้มีการจัดสรรทรัพยากรที่เหมาะสม และติดตามประเด็นสำคัญด้านความเสี่ยงที่อาจส่งผลกระทบต่อการดำเนินงานของบริษัท

1.4 **ฝ่ายเทคโนโลยีสารสนเทศ** มีบทบาทและหน้าที่ความรับผิดชอบ ดังนี้

(1) กำหนดและดูแลให้มีการนำมาตรการด้านความมั่นคงปลอดภัยสารสนเทศไปใช้ให้เหมาะสมกับลักษณะการดำเนินงานและระดับความเสี่ยงขององค์กร

(2) บริหารจัดการและดูแลทรัพย์สินด้านเทคโนโลยีสารสนเทศของบริษัท เพื่อสนับสนุนการดำเนินธุรกิจและการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศ

(3) ติดตาม ประเมินผล และปรับปรุงการดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศอย่างต่อเนื่อง เพื่อให้มีประสิทธิผลและสอดคล้องกับการเปลี่ยนแปลงของความเสี่ยงและเทคโนโลยี

(4) ประสานงานกับหน่วยงานที่เกี่ยวข้อง พนักงาน และคู่ค้าและพันธมิตรทางธุรกิจ ผู้ให้บริการ ที่ปรึกษา ผู้ประมวลผลข้อมูล หรือบุคคลภายนอก เพื่อส่งเสริมการใช้ระบบเทคโนโลยีสารสนเทศอย่างเหมาะสม ปลอดภัย และเป็นไปตามข้อกำหนดที่เกี่ยวข้อง

(5) ส่งเสริมและสนับสนุนการสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศให้แก่พนักงานและผู้ที่เกี่ยวข้อง

(6) รายงานประเด็นหรือความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศที่มีนัยสำคัญต่อฝ่ายบริหารตามความเหมาะสม

(7) สนับสนุนการปฏิบัติตามกฎหมาย ระเบียบ และข้อบังคับที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยสารสนเทศ

1.5 **พนักงาน**

มีบทบาทในการใช้ระบบเทคโนโลยีสารสนเทศและทรัพยากรที่เกี่ยวข้องอย่างเหมาะสมและปลอดภัย โดยต้องปฏิบัติตามนโยบายและข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศของกลุ่มบริษัท พนักงานทุกคนมีหน้าที่รับผิดชอบในการปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศตามบทบาทหน้าที่ของตน รวมถึงร่วมป้องกัน ตรวจพบ และรายงานเหตุการณ์หรือความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศที่อาจเกิดขึ้น

1.6 **บุคคลภายนอก**

มีบทบาทในการปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศของกลุ่มบริษัทและเงื่อนไขตามสัญญาที่เกี่ยวข้องอย่างเคร่งครัด โดยเฉพาะอย่างยิ่งคู่ค้าและพันธมิตรทางธุรกิจ ผู้ให้บริการ ผู้ประมวลผลข้อมูล ที่ปรึกษา และบุคคลภายนอก ที่มีการเข้าถึง เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศหรือข้อมูลของกลุ่มบริษัท โดยสามารถใช้ข้อมูลและระบบของกลุ่มบริษัทเพื่อวัตถุประสงค์ทางธุรกิจที่ได้รับอนุญาตเท่านั้น และให้ความร่วมมือในการดำเนินมาตรการด้านความมั่นคงปลอดภัยสารสนเทศตามที่กลุ่มบริษัทกำหนด

2. แนวทางการบริหารจัดการด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

2.1 การควบคุมการเข้าถึงข้อมูลและทรัพยากรด้านเทคโนโลยีสารสนเทศ

(1) กำหนดให้มีการพิสูจน์ตัวตนของผู้ใช้งานก่อนการเข้าถึงระบบสารสนเทศ ข้อมูล และทรัพยากรด้านเทคโนโลยีสารสนเทศของบริษัท

(2) กำหนดสิทธิการเข้าถึงข้อมูลและระบบตามบทบาทหน้าที่ ความรับผิดชอบ และความจำเป็นในการปฏิบัติงานของผู้ใช้งาน โดยยึดหลักการให้สิทธิเท่าที่จำเป็น (Least Privilege)

(3) ควบคุมและจำกัดการเข้าถึงข้อมูลและระบบที่มีความสำคัญหรือมีความอ่อนไหว เพื่อป้องกันการเข้าถึงหรือการใช้งานโดยไม่ได้รับอนุญาต

(4) จัดให้มีการบริหารจัดการบัญชีผู้ใช้งานตลอดวงจรการใช้งาน ตั้งแต่การอนุมัติสิทธิ การเปลี่ยนแปลงสิทธิ ไปจนถึงการเพิกถอนสิทธิเมื่อสิ้นสุดความจำเป็นในการใช้งาน

(5) ทบทวนสิทธิการเข้าถึงข้อมูลและระบบสารสนเทศเป็นระยะ หรือเมื่อมีการเปลี่ยนแปลงบทบาทหน้าที่ สถานะการจ้างงาน หรือโครงการที่เกี่ยวข้อง

(6) กำหนดให้มีการบันทึกและติดตามการใช้งานระบบสารสนเทศอย่างเหมาะสม เพื่อให้สามารถตรวจสอบและระบุความรับผิดชอบของผู้ใช้งานได้ในกรณีที่เกิดเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ

2.2 ความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม

(1) จำกัดการเข้าถึงพื้นที่ที่เกี่ยวข้องกับระบบสารสนเทศ โครงสร้างพื้นฐาน และอุปกรณ์สำคัญ เฉพาะบุคคลที่ได้รับอนุญาตและมีความจำเป็นตามหน้าที่

(2) จัดให้มีมาตรการป้องกันความเสี่ยงด้านสภาพแวดล้อมที่อาจส่งผลกระทบต่อระบบสารสนเทศและอุปกรณ์ เช่น อัคคีภัย ไฟฟ้าขัดข้อง หรือเหตุฉุกเฉินอื่น ๆ

(3) คุ้มครองอุปกรณ์และโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศจากความเสียหายหรือการเข้าถึงโดยไม่ได้รับอนุญาต

2.3 ความมั่นคงปลอดภัยด้านการปฏิบัติงานเทคโนโลยีสารสนเทศ

(1) กำหนดให้การใช้งานระบบสารสนเทศและทรัพยากรด้านเทคโนโลยีสารสนเทศเป็นไปตามวัตถุประสงค์ในการดำเนินธุรกิจและเป็นไปตามนโยบาย ระเบียบ และข้อกำหนดของบริษัท

(2) ป้องกันการใช้งานระบบสารสนเทศในลักษณะที่อาจก่อให้เกิดความเสียหายต่อระบบข้อมูล หรือการดำเนินงานของบริษัท

(3) กำกับดูแลการปฏิบัติงานด้านเทคโนโลยีสารสนเทศให้อยู่ภายใต้แนวทางและมาตรการด้านความมั่นคงปลอดภัยที่เหมาะสม

(4) ส่งเสริมให้ระบบสารสนเทศมีความพร้อมใช้งานอย่างเหมาะสม เพื่อสนับสนุนความต่อเนื่องในการดำเนินธุรกิจ

(5) ติดตาม ตรวจจับ ประเมิน และตอบสนองต่อภัยคุกคามด้านความมั่นคงปลอดภัยสารสนเทศอย่างเหมาะสมและทันท่วงที

2.4 การจัดการเหตุการณ์และความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ

(1) จัดให้มีช่องทางและกระบวนการที่เหมาะสมสำหรับการรายงานและรับรู้เหตุการณ์หรือเหตุอันควรสงสัยที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ

(2) ดำเนินการจัดการ แก้ไข และลดผลกระทบจากเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ รวมถึงการวิเคราะห์และทบทวนเหตุการณ์ตามความเหมาะสม

(3) จัดให้มีแนวทางรองรับเหตุขัดข้องและการเตรียมความพร้อมของระบบและข้อมูลในภาพรวม เพื่อสนับสนุนความต่อเนื่องในการดำเนินธุรกิจของบริษัท

(4) ทบทวนและปรับปรุงแนวทางการจัดการเหตุการณ์และการรองรับเหตุขัดข้องอย่างเหมาะสมอย่างต่อเนื่อง

2.5 การสร้างความตระหนักด้านเทคโนโลยีสารสนเทศ

(1) ส่งเสริมให้บุคลากรเข้าใจบทบาท หน้าที่ และความรับผิดชอบของตนเองด้านความมั่นคงปลอดภัยสารสนเทศ โดยกำหนดให้บุคคลที่เกี่ยวข้องกับการใช้งานหรือการเข้าถึงทรัพยากรสารสนเทศต้องได้รับการให้ข้อมูลหรือการสื่อสารที่เหมาะสมก่อนการเข้าถึงระบบ

(2) กำหนดให้พนักงานใหม่ได้รับการปฐมนิเทศเกี่ยวกับนโยบายด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศของบริษัท เพื่อสร้างความเข้าใจในการใช้งานระบบสารสนเทศและการคุ้มครองข้อมูล

(3) สนับสนุนการเสริมสร้างความตระหนักด้านความเสี่ยงเทคโนโลยีสารสนเทศให้แก่บุคลากรที่มีสิทธิเข้าถึงข้อมูลหรือระบบภายในองค์กร เพื่อป้องกันความเสี่ยงที่อาจเกิดขึ้นจากการใช้งานระบบหรือข้อมูลโดยไม่เหมาะสม

2.6 การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ

(1) กำหนดให้มีการระบุและบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศที่ใช้ในการดำเนินงานของบริษัทอย่างเหมาะสม

(2) ดูแลและบำรุงรักษาทรัพย์สินด้านเทคโนโลยีสารสนเทศให้อยู่ในสภาพพร้อมใช้งานและลดความเสี่ยงที่อาจส่งผลกระทบต่อระบบและข้อมูล

(3) สนับสนุนให้มีการทบทวนและปรับปรุงข้อมูลเกี่ยวกับทรัพย์สินด้านเทคโนโลยีสารสนเทศตามความเหมาะสม เพื่อใช้ประกอบการบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ

2.7 **การบริหารจัดการความสัมพันธ์กับคู่ค้าและบุคคลภายนอก**

(1) กำหนดให้การเข้าถึงระบบสารสนเทศหรือข้อมูลของบริษัทโดยคู่ค้าและบุคคลภายนอกเป็นไปตามขอบเขตงานและวัตถุประสงค์ที่ได้รับอนุญาต

(2) สนับสนุนให้มีการกำหนดบทบาท หน้าที่ และความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศของคู่ค้าและบุคคลภายนอกอย่างเหมาะสม

(3) กำหนดให้มีการดูแลและติดตามการเข้าถึงระบบและข้อมูลของคู่ค้าและบุคคลภายนอกตามความจำเป็น เพื่อป้องกันความเสี่ยงที่อาจส่งผลกระทบต่อบริษัท

3. **แนวทางการบริหารจัดการด้านปัญญาประดิษฐ์** (AI)

กลุ่มบริษัทเล็งเห็นถึงความสำคัญของการนำปัญญาประดิษฐ์มาใช้งานหรือพัฒนาเพื่อสนับสนุนการดำเนินงานให้มีประสิทธิภาพมากยิ่งขึ้น ทั้งนี้ เพื่อให้การใช้งานหรือการพัฒนาเป็นไปอย่างเหมาะสม ถูกต้อง มีธรรมาภิบาล และสอดคล้องกับหลักจริยธรรม กลุ่มบริษัทจึงกำหนดแนวทางการดำเนินงาน ดังนี้

(1) กลุ่มบริษัทจะใช้หรือประยุกต์ใช้ AI อย่างเหมาะสม ปลอดภัย โปร่งใส และเป็นไปตามกฎหมาย มาตรฐานที่เกี่ยวข้อง และหลักจริยธรรม

(2) กลุ่มบริษัทจะคุ้มครองข้อมูลส่วนบุคคลและความเป็นส่วนตัวในการใช้หรือพัฒนา AI

(3) กลุ่มบริษัทจะดูแลความปลอดภัยของระบบ AI และข้อมูลที่เกี่ยวข้อง เพื่อป้องกันการเข้าถึงการใช้งาน หรือการเปิดเผยโดยไม่ได้รับอนุญาต

(4) กลุ่มบริษัทจะใช้ AI โดยคำนึงถึงความเป็นธรรม ลดความเสี่ยงจากอคติหรือการเลือกปฏิบัติที่อาจเกิดจากผลลัพธ์หรือการทำงานของระบบ AI และกำหนดให้การใช้ AI ในเรื่องที่มีนัยสำคัญต้องอยู่ภายใต้การกำกับดูแลของมนุษย์อย่างเหมาะสม รวมทั้งสามารถตรวจสอบ ทบทวน หรือแทรกแซงได้เมื่อจำเป็น

(5) กลุ่มบริษัทจะกำหนดวัตถุประสงค์ ขอบเขตการใช้งาน และผู้รับผิดชอบสำหรับการใช้และกำกับดูแล AI อย่างชัดเจน รวมทั้งสื่อสารข้อจำกัดและอธิบายผลลัพธ์ของ AI ให้ผู้ที่เกี่ยวข้องทราบตามความเหมาะสม

(6) กลุ่มบริษัทจะไม่ใช้ AI ในทางที่ก่อให้เกิดการหลอกลวง เอาเปรียบ หรือกระทบต่อบุคคลอย่างไม่เหมาะสม

4. **การตรวจสอบและประเมินผลด้านความมั่นคงปลอดภัยสารสนเทศ**

(1) กลุ่มบริษัทดำเนินการตรวจสอบภายในหรือทบทวนการปฏิบัติตามนโยบายด้านความมั่นคงปลอดภัยสารสนเทศเป็นระยะ เพื่อประเมินความเพียงพอและประสิทธิผลของมาตรการควบคุมที่เกี่ยวข้อง

(2) กลุ่มบริษัทดำเนินการประเมินหรือทบทวนการปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศของคู่ค้า ผู้ให้บริการ ผู้ประมวลผลข้อมูล หรือบุคคลภายนอก ตามความเหมาะสมและระดับความเสี่ยง

5. **การทบทวนนโยบาย**

ให้ฝ่ายเทคโนโลยีสารสนเทศมีการทบทวนนโยบายฉบับนี้อย่างน้อยปีละหนึ่งครั้ง หากกรณีมีความจำเป็นต้องปรับปรุงแก้ไข นโยบายฉบับนี้จะต้องเสนอไปยังคณะกรรมการพิจารณาอนุมัติต่อไป

นโยบายฉบับนี้ มีผลบังคับใช้ตั้งแต่วันที่ 7 สิงหาคม 2569 เป็นต้นไป ตามที่คณะกรรมการบริษัทได้พิจารณาและมีมติอนุมัติในการประชุมคณะกรรมการบริษัท ครั้งที่ 3/2569

_____

(นายออง ชู จิน เอเดรียน)

ประธานกรรมการ

บริษัท มิสเตอร์. ดี.ไอ.วาย. โฮลดิ้ง (ประเทศไทย) จำกัด (มหาชน)