WHA GROUP

Policy

นโยบายความมั่นคงปลอดภัยไซเบอร์ สารสนเทศและการคุ้มครองข้อมูลส่วนบุคคล และการกำกับดูแลปัญญาประดิษฐ์

Cybersecurity, Information Security & Privacy and AI Governance Policy

นโยบายความมั่นคงปลอดภัยไซเบอร์ สารสนเทศและการคุ้มครองข้อมูลส่วนบุคคล และการกำกับดูแลปัญญาประดิษฐ์

(Cybersecurity, Information Security & Privacy and AI Governance Policy)

กลุ่มบริษัทดับบลิวเอชเอตระหนักถึงความสำคัญของเทคโนโลยีสารสนเทศและปัญญาประดิษฐ์ (Artificial Intelligence: AI) มาใช้เป็นกลไกสำคัญในการยกระดับประสิทธิภาพและประสิทธิผลในการดำเนินงานขององค์กร เพื่อสนับสนุนการมุ่งสู่ความเป็นเลิศในการดำเนินธุรกิจ ตลอดจนการขับเคลื่อนองค์กรในยุคดิจิทัล เพื่อนำไปสู่การสร้างสรรค์นวัตกรรม การสร้างคุณค่าอย่างยั่งยืนแก่ผู้มีส่วนได้เสีย และการเติบโตขององค์กรในระยะยาว ทั้งนี้ กลุ่มบริษัทดับบลิวเอชเอยึดมั่นและให้ความสำคัญในการคุ้มครองและรักษาความปลอดภัยของข้อมูลและระบบสารสนเทศ รวมถึงการใช้ การพัฒนา และการประยุกต์ใช้ปัญญาประดิษฐ์ ภายใต้หลักความมั่นคงปลอดภัย ความมีธรรมาภิบาล ความเป็นธรรม ความโปร่งใส และความรับผิดชอบอย่างเคร่งครัด

ด้วยเหตุนี้ กลุ่มบริษัทดับบลิวเอชเอจึงได้กำหนดนโยบายความมั่นคงปลอดภัยไซเบอร์ สารสนเทศและการคุ้มครองข้อมูลส่วนบุคคล และการกำกับดูแลปัญญาประดิษฐ์ฉบับนี้ขึ้น โดยยึดหลักการปฏิบัติให้สอดคล้องกับกฎหมาย ข้อบังคับ แนวปฏิบัติและมาตรฐานสากล เพื่อให้มั่นใจว่าการใช้และการบริหารจัดการเทคโนโลยีดังกล่าวเป็นไปอย่างมีระบบ มีความมั่นคงปลอดภัย โปร่งใส และเชื่อถือได้

1. วัตถุประสงค์ของนโยบาย

1.1 **เพื่อสร้างความเชื่อมั่นและรักษาความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ** โดยการปกป้องข้อมูลและระบบสารสนเทศขององค์กรให้มีความลับ (Confidentiality) ความถูกต้อง (Integrity) และความพร้อมใช้งาน (Availability) สอดคล้องตามมาตรฐาน ISO/IEC 27001

1.2 **เพื่อคุ้มครองสิทธิและข้อมูลส่วนบุคคล** โดยวางรากฐานการบริหารจัดการข้อมูลส่วนบุคคล ให้โปร่งใสและสอดคล้องตามมาตรฐาน ISO/IEC 27701

1.3 **เพื่อการพัฒนาและประยุกต์ใช้ปัญญาประดิษฐ์อย่างมีจริยธรรม** กำหนดกรอบการพัฒนาและใช้งาน AI ให้มีความรับผิดชอบ โปร่งใส ปราศจากอคติและเป็นธรรม ควบคู่ไปกับการรักษาความปลอดภัยและความเป็นส่วนตัวของข้อมูล พร้อมทั้งจัดให้มีระบบธรรมาภิบาลที่สามารถตรวจสอบได้ เพื่อลดความเสี่ยงที่อาจเกิดขึ้นต่อมนุษย์และสังคม สอดคล้องตามมาตรฐาน ISO/IEC 42001

1.4 **เพื่อการปฏิบัติตามกฎหมาย กฎระเบียบ มาตรฐานและแนวปฏิบัติสากล** มุ่งเน้นการดำเนินงานที่สอดคล้องกับกฎหมาย ข้อบังคับ สัญญาจ้างทางธุรกิจ รวมถึงมาตรฐานแนวปฏิบัติสากลอื่น ๆ ที่เกี่ยวข้อง

2. คำนิยาม

2.1 “กลุ่มบริษัทดับบลิวเอชเอ” หรือ “องค์กร” หมายความว่า บริษัท ดับบลิวเอชเอ คอร์ปอเรชั่น จำกัด (มหาชน) และบริษัทย่อย รวมทั้งบริษัทร่วมที่บริษัทมีอำนาจควบคุมสั่งการและกำหนดนโยบาย

2.2 “นโยบาย” หมายความว่า นโยบายความมั่นคงปลอดภัยไซเบอร์ สารสนเทศและการคุ้มครองข้อมูลส่วนบุคคลและการกำกับดูแลปัญญาประดิษฐ์ ฉบับนี้ (รวมถึงที่ได้มีการแก้ไขเพิ่มเติม) ตลอดจนนโยบาย ระเบียบวิธีปฏิบัติ แนวปฏิบัติ หรือมาตรฐานการทำงานอื่น ๆ ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ สารสนเทศ ความเป็นส่วนตัว และการกำกับดูแลปัญญาประดิษฐ์ (AI) ที่กลุ่มบริษัทดับบลิวเอชเอ กำหนดขึ้น โดยได้รับ

ความเห็นชอบจากประธานเจ้าหน้าที่บริหารกลุ่มบริษัท และ/หรือประธานเจ้าหน้าที่บริหารของบริษัทย่อยที่ได้มีการลงนามประกาศบังคับใช้

2.3 “แนวปฏิบัติ” หมายความว่า ข้อปฏิบัติเกี่ยวกับการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ สารสนเทศ ความเป็นส่วนตัว และการกำกับดูแลปัญญาประดิษฐ์ (AI) ที่กลุ่มบริษัทดับบลิวเอชเอกำหนดขึ้นและประกาศใช้งานเพื่อให้ผู้ใช้งานปฏิบัติตามโดยเคร่งครัด

2.4 “กิจการที่องค์กรมีอำนาจบริหาร” หมายความว่า กิจการที่องค์กรสามารถควบคุมและสั่งการได้ ไม่ว่าจะเป็นการถือหุ้นที่มีสิทธิออกเสียงเกินกว่าร้อยละ 50 หรือการมีอำนาจควบคุมคะแนนเสียงส่วนใหญ่ในที่ประชุมผู้ถือหุ้น อำนาจบริหารนี้รวมถึงการตัดสินใจและดูแลการดำเนินงานขององค์กร และมีการใช้ระบบเทคโนโลยีสารสนเทศและ/หรือระบบเครือข่ายและคอมพิวเตอร์ การใช้งานเทคโนโลยีปัญญาประดิษฐ์ (AI) ร่วมกัน

2.5 “ห่วงโซ่อุปทาน” หมายความว่า เครือข่ายความสัมพันธ์ระหว่างองค์กร คู่ค้าขององค์กร ผู้รับจ้างของคู่ค้าที่เกี่ยวข้องกับการดำเนินงานบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ สารสนเทศ ความเป็นส่วนตัว และการกำกับดูแลปัญญาประดิษฐ์ (AI) ขององค์กร และกิจการที่องค์กรมีอำนาจบริหารที่เกี่ยวข้อง

2.6 “สารสนเทศ” หมายความว่า ข้อมูล ข่าวสาร บันทึก ประวัติ ข้อความในเอกสาร โปรแกรมคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ รูปภาพ เสียง เครื่องหมาย และสัญลักษณ์ต่าง ๆ ไม่ว่าจะเก็บไว้ในรูปแบบที่สามารถสื่อความหมายให้บุคคลสามารถเข้าใจได้โดยตรง หรือผ่านคอมพิวเตอร์ หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้

2.7 “ระบบสารสนเทศ” หมายความว่า ระบบที่รวบรวม จัดเก็บ ประมวลผล และแจกจ่ายข้อมูล เพื่อให้เกิดสารสนเทศที่เป็นประโยชน์ต่อการตัดสินใจและการดำเนินงานของบุคคลหรือองค์กร ระบบนี้ประกอบด้วยองค์ประกอบสำคัญหลายอย่าง ได้แก่ ฮาร์ดแวร์, ซอฟต์แวร์, ข้อมูล, บุคคล, กระบวนการ, และเครือข่าย หน้าที่หลักคือการแปลงข้อมูลดิบให้เป็นสารสนเทศที่มีความหมาย เพื่อช่วยในการบริหารจัดการและบรรลุเป้าหมายขององค์กร

2.8 “เทคโนโลยีสารสนเทศ” หมายความว่า เทคโนโลยีที่นำมาใช้ในการดำเนินธุรกิจ ซึ่งครอบคลุมถึงข้อมูลหรือสารสนเทศ (DATA/Information) ระบบปฏิบัติการ (Operating System) ระบบงาน (Application System) ระบบฐานข้อมูล (Database System) อุปกรณ์คอมพิวเตอร์และเครือข่าย (Hardware) และระบบเครือข่ายสื่อสาร (Communication System) เป็นต้น

2.9 “ความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ” หมายความว่า การปกป้องระบบสารสนเทศและข้อมูลให้มีความลับ (Confidentiality) ถูกต้องครบถ้วน (Integrity) และพร้อมใช้งาน (Availability) อยู่เสมอ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปลี่ยนแปลง หรือการทำลายข้อมูล โดยอาศัยมาตรการต่าง ๆ ทั้งด้านการบริหาร เทคนิค และกายภาพ เพื่อรับมือกับภัยคุกคามต่าง ๆ

2.10 “ไซเบอร์” หมายความว่า ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการบริการปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกันที่เชื่อมต่อกันเป็นการทั่วไป

2.11 “ความมั่นคงปลอดภัยทางไซเบอร์” หมายความว่า มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทุกรูปแบบทั้งจากภายในและภายนอกองค์กร ที่ส่งผลกระทบต่อการดำเนินธุรกิจขององค์กร ความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ

2.12 “ภัยคุกคามทางไซเบอร์” หมายความว่า การกระทำหรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์ โดยมุ่งหมายให้เกิดความเสียหายหรือผิดปกติต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

2.13 “ปัญญาประดิษฐ์ (Artificial Intelligence: AI)” หมายความว่า เทคโนโลยีที่ถูกพัฒนาขึ้นเพื่อให้ระบบประมวลผลของคอมพิวเตอร์ หุ่นยนต์ เครื่องจักร หรืออุปกรณ์อิเล็กทรอนิกส์ต่าง ๆ มีคุณสมบัติหรือพฤติกรรมใกล้เคียงมนุษย์ตามวัตถุประสงค์ที่มนุษย์กำหนด เช่น การเรียนรู้ การรับรู้และตอบสนองต่อสภาพแวดล้อม การให้เหตุผล และการแก้ไขปัญหา เป็นต้น

3. ขอบเขตของนโยบาย

3.1 นโยบายฉบับนี้ให้มีผลบังคับใช้กับคณะกรรมการบริษัท ผู้บริหาร พนักงาน ผู้ปฏิบัติงานทุกระดับของกลุ่มบริษัทดับบลิวเอชเอ ตลอดจนกิจการที่องค์กรมีอำนาจในการบริหารจัดการ ทั้งนี้ครอบคลุมถึงทรัพย์สินและระบบสารสนเทศทั้งหมดขององค์กร ได้แก่ ระบบเทคโนโลยีสารสนเทศ ข้อมูลและทรัพย์สินดิจิทัล อุปกรณ์ และระบบใด ๆ ที่มีการเชื่อมต่อหรือเข้าถึงเครือข่ายขององค์กร โดยไม่จำกัดสถานที่ เวลา หรือรูปแบบการใช้งาน

3.2 นโยบายฉบับนี้ครอบคลุมถึงบุคคลภายนอก คู่ค้า ผู้รับจ้าง ผู้ให้บริการ และผู้มีส่วนได้ส่วนเสีย ที่ได้รับอนุญาตให้เข้าถึง ใช้งาน ระบบสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลส่วนบุคคล สินทรัพย์ด้านเทคโนโลยีสารสนเทศ ระบบปัญญาประดิษฐ์ หรือบริการใด ๆ ของ กลุ่มบริษัทดับบลิวเอชเอ โดยองค์กรมีความมุ่งมั่นที่จะนำหลักเกณฑ์ตามนโยบายฉบับนี้ไปประยุกต์ใช้กับบุคคลต่าง ๆ ดังกล่าวผ่านจรรยาบรรณธุรกิจของคู่ค้า ข้อกำหนดในสัญญา ข้อตกลงระดับการให้บริการ ข้อกำหนดและเงื่อนไขของการให้บริการ หรือแนวปฏิบัติตามความเหมาะสม

3.3 ในกรณีที่มีประกาศ หลักเกณฑ์ คำสั่ง หรือแนวปฏิบัติอื่นใดขององค์กรที่มีเนื้อหาขัดหรือแย้งกับนโยบายฉบับนี้ ให้ถือนโยบายฉบับนี้เป็นหลักในการบังคับใช้

4. โครงสร้างการกำกับดูแลและแนวปฏิบัติหลักของนโยบาย

4.1 เพื่อให้การบริหารจัดการเป็นไปอย่างมีประสิทธิภาพ กลุ่มบริษัทดับบลิวเอชเอกำหนดลำดับชั้นของเอกสารกำกับดูแล ดังนี้

4.1.1 **นโยบายแม่บท** (Master Policy) หมายถึง นโยบายฉบับนี้ที่กำหนดทิศทาง วิสัยทัศน์หลักและหลักการพื้นฐานในการดำเนินงานขององค์กร เพื่อเป็นกรอบความคิดหลักในการตัดสินใจและกำหนดระเบียบปฏิบัติในระดับถัดไป

4.1.2 **มาตรฐาน** (Standards) หมายถึง ข้อกำหนดทางเทคนิคและหลักเกณฑ์ขั้นต่ำที่ต้องปฏิบัติอย่างเคร่งครัดเพื่อให้การดำเนินงานเป็นไปตามมาตรฐานที่กลุ่มบริษัทดับบลิวเอชเอกำหนด เช่น มาตรฐานการรักษาความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ (Cybersecurity and Information Security Management Standard) หรือ มาตรฐานการบริหารจัดการ และกำกับดูแลการใช้งานเทคโนโลยีปัญญาประดิษฐ์ (AI Management Standard)

4.1.3 **ระเบียบปฏิบัติและแนวทางปฏิบัติ** (Procedures & Guidelines) หมายถึงขั้นตอนการทำงานโดยละเอียด (Work Instructions) และคำแนะนำในการปฏิบัติงาน เพื่อให้ผู้ปฏิบัติงานสามารถนำนโยบายและมาตรฐานไปประยุกต์ใช้ในหน้างานจริงได้อย่างถูกต้องและสอดคล้องกัน

4.2 เพื่อให้การปฏิบัติงานเป็นไปตามนโยบายฉบับนี้ กลุ่มบริษัทดับบลิวเอชเอ จะดำเนินการจัดทำ กำหนดและ/หรือทบทวนมาตรการ มาตรฐานและแนวนโยบายการปฏิบัติงาน ในเรื่องต่าง ๆ ดังต่อไปนี้

4.2.1 นโยบายความเป็นส่วนตัว “Privacy Policy”

4.2.2 มาตรฐานบริหารจัดการด้านความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ “Cybersecurity and Information Security Management Standard”

4.2.3 มาตรฐานการบริหารจัดการ และกำกับดูแลการใช้งานเทคโนโลยีปัญญาประดิษฐ์ “AI Management Standard” และ

4.2.4 มาตรฐาน มาตรการ คู่มือ ระเบียบปฏิบัติหรือแนวปฏิบัติอื่น ๆ ที่เกี่ยวข้องและจำเป็น

4.3 กลุ่มบริษัทดับบลิวเอชเอ จะดำเนินการตรวจสอบและปรับปรุงมาตรการต่าง ๆ ให้สอดคล้องกับกฎหมาย กฎระเบียบ ข้อบังคับของรัฐ ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ ข้อมูลส่วนบุคคล และเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ

4.4 บรรดาแนวปฏิบัติใด ๆ ที่เกี่ยวข้องซึ่งได้มีการทำขึ้นและ/หรือประกาศใช้งานก่อนวันที่ของนโยบายฉบับนี้ ให้ถือเป็นแนวปฏิบัติที่ออกภายใต้ข้อ 4 ของนโยบายฉบับนี้

5. บทบาท หน้าที่ และความรับผิดชอบ

5.1 กำหนดให้คณะกรรมการบริหารความเสี่ยงและความมั่นคงปลอดภัยสารสนเทศ มีหน้าที่กำกับดูแลการดำเนินงานให้เป็นไปตามนโยบาย

5.2 กำหนดให้มีการทบทวนนโยบาย อย่างน้อยปีละ 1 ครั้งหรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญด้านกฎหมาย เทคโนโลยี หรือภัยคุกคามที่เกี่ยวข้อง เพื่อให้มั่นใจว่าหลักการของนโยบายนี้สอดคล้องกับบริบทขององค์กร และธุรกิจในขณะนั้น

5.3 กำหนดให้ประธานเจ้าหน้าที่บริหารกลุ่มบริษัท ประธานเจ้าหน้าที่บริหารของบริษัทย่อย ประธานเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ และ/หรือประธานเจ้าหน้าที่ฝ่ายกฎหมาย มีอำนาจในการพิจารณา ทบทวนและอนุมัติมาตรฐาน และแนวปฏิบัติต่าง ๆ ที่เกี่ยวข้องซึ่งออกภายใต้นโยบายฉบับนี้

5.4 พนักงานและบุคลากรทุกคนของกลุ่มบริษัทดับบลิวเอชเอ มีหน้าที่รายงานเหตุการณ์ทางไซเบอร์ที่ผิดปกติ การรั่วไหลของข้อมูล หรือการใช้งาน AI ที่ไม่เหมาะสมต่อทีมงานด้านความปลอดภัยสารสนเทศ หรือ Incident Response Team (IRT) ทันทีที่พบเห็น ทั้งนี้ในกรณีที่ข้อมูลที่รั่วไหลเป็นข้อมูลส่วนบุคคล ต้องดำเนินการแจ้งเหตุการณ์ดังกล่าวให้กับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ด้วยในเวลาเดียวกัน เพื่อเข้าสู่กระบวนการตอบสนองต่อเหตุการณ์ (Incident Response) ตามมาตรฐานที่กำหนด

6. การตรวจสอบและการปฏิบัติตาม

กลุ่มบริษัทดับบลิวเอชเอสงวนสิทธิ์ในการตรวจสอบ (Right to Audit) การใช้งานระบบสารสนเทศ ข้อมูล และ AI ภายในขอบเขตที่กฎหมายอนุญาต เพื่อให้มั่นใจว่าการปฏิบัติงานสอดคล้องกับนโยบายนี้และป้องกันภัยคุกคามที่อาจเกิดขึ้น

7. การสร้างความตระหนักรู้และฝึกอบรม

กลุ่มบริษัทดับบลิวเอชเอจะจัดให้มีการฝึกอบรมและทดสอบความรู้ด้าน Cybersecurity, Privacy และ AI Ethics ให้แก่พนักงานและผู้เกี่ยวข้องอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่าทุกคนมีความเข้าใจและตระหนักถึงหน้าที่ความรับผิดชอบ

8. บทลงโทษ

การละเมิด ฝ่าฝืน หรือไม่ปฏิบัติตามนโยบายหรือแนวปฏิบัติที่เกี่ยวข้อง ถือเป็นความผิดทางวินัยและจะได้รับการพิจารณาลงโทษตามข้อบังคับเกี่ยวกับการทำงานของกลุ่มบริษัท ทั้งนี้ หากการกระทำดังกล่าวก่อให้เกิดความเสียหายหรือเข้าข่ายเป็นความผิดทางกฎหมาย กลุ่มบริษัทจะดำเนินการทางแพ่งและทางอาญาต่อผู้กระทำผิด

นโยบายความมั่นคงปลอดภัยไซเบอร์ สารสนเทศและการคุ้มครองข้อมูลส่วนบุคคล และการกำกับดูแลปัญญาประดิษฐ์ฉบับนี้ ได้ผ่านการพิจารณาและเห็นชอบจากคณะกรรมการบริหารความเสี่ยงและความมั่นคงปลอดภัยสารสนเทศ ครั้งที่ 3/2569 เมื่อวันที่ 23 กรกฎาคม 2569 และได้ผ่านการพิจารณาและอนุมัติจากที่ประชุมคณะกรรมการบริษัท ครั้งที่ 5/2569 เมื่อวันที่ 10 สิงหาคม 2569

(นายสมคิด จาตุศรีพิทักษ์)
ประธานคณะกรรมการบริษัท
บริษัท ดับบลิวเอชเอ คอร์ปอเรชั่น จำกัด (มหาชน)