นโยบายกำกับดูแลด้านเทคโนโลยีสารสนเทศ

นโยบายกำกับดูแลด้านเทคโนโลยีสารสนเทศ

บริษัท อมรินทร์ คอร์เปอเรชั่นส์ จำกัด (มหาชน) (“บริษัท”) ตระหนักถึงความสำคัญของเทคโนโลยีสารสนเทศ ซึ่งเป็นเครื่องมือสำคัญที่ช่วยสนับสนุนการเพิ่มสมรรถนะขององค์กร ทั้งในด้านการบริหารจัดการและการดำเนินธุรกิจ ดังนั้น เพื่อให้การดำเนินการด้านเทคโนโลยีสารสนเทศของบริษัทและบริษัทย่อย (รวมเรียกว่า “กลุ่มบริษัท”) เป็นไปอย่างมีประสิทธิภาพ มีความมั่นคงปลอดภัยและน่าเชื่อถือ โดยข้อมูลสารสนเทศและสินทรัพย์ในระบบเทคโนโลยีสารสนเทศของกลุ่มบริษัทได้รับการดูแลรักษาอย่างเหมาะสม คงไว้ซึ่งการรักษาความลับ (Confidentiality) ความถูกต้องสมบูรณ์ (Integrity) และความพร้อมใช้งาน (Availability) ตลอดจนเพื่อให้การดำเนินการด้านเทคโนโลยีสารสนเทศของกลุ่มบริษัทสอดคล้องกับกฎหมาย หลักเกณฑ์ แนวปฏิบัติ หรือมาตรฐานสากลที่เกี่ยวข้องบริษัท จึงกำหนดนโยบายกำกับดูแลด้านเทคโนโลยีสารสนเทศขึ้น เพื่อเป็นแนวปฏิบัติแก่ฝ่ายงานและบุคลากรทุกระดับของกลุ่มบริษัท

1. **วัตถุประสงค์**

   นโยบายกำกับดูแลด้านเทคโนโลยีสารสนเทศฉบับนี้กำหนดขึ้น เพื่อวัตถุประสงค์ดังนี้

   - กำหนดกรอบการกำกับดูแล การดำเนินงาน และการบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กร เพื่อให้ผู้ที่เกี่ยวข้องทั้งบุคลากรภายในองค์กรและผู้ที่เกี่ยวข้องภายนอกองค์กรมีกรอบการปฏิบัติงานที่ชัดเจน
   - สร้างความรู้ความเข้าใจแก่บุคลากรของกลุ่มบริษัทเพื่อให้สามารถปฏิบัติตามกฎหมาย นโยบาย แนวปฏิบัติ หรือข้อกำหนดที่เกี่ยวข้องด้านเทคโนโลยีสารสนเทศของหน่วยงานกำกับดูแลและของกลุ่มบริษัทได้อย่างถูกต้อง
   - เพื่อป้องกันปัญหาหรือความเสียหายต่อทรัพย์สิน ผลกระทบต่อการประกอบธุรกิจ หรือชื่อเสียงความน่าเชื่อถือของกลุ่มบริษัทที่อาจจะเกิดขึ้นจากการใช้งานเทคโนโลยีสารสนเทศอย่างไม่เหมาะสม หรือจากสถานการณ์ฉุกเฉิน หรือจากภัยคุกคามต่าง ๆ

2. **ขอบเขต**

   นโยบายฉบับนี้ใช้กับกรรมการ ผู้บริหาร และพนักงานทุกระดับของบริษัทและบริษัทย่อย รวมถึงผู้ให้บริการภายนอก (Outsource) ที่บริษัทหรือบริษัทย่อยว่าจ้างให้ดำเนินการด้านเทคโนโลยีสารสนเทศ ตลอดจนบุคคลภายนอกหรือหน่วยงานภายนอกที่ได้รับอนุญาตให้เข้าถึง ให้บริการ หรือใช้งานระบบเครือข่าย ระบบงาน หรือสินทรัพย์ใด ๆ ในระบบเทคโนโลยีสารสนเทศของกลุ่มบริษัท

3. **นิยามที่เกี่ยวข้อง**

   - **บริษัท** หมายถึง บริษัท อมรินทร์ คอร์เปอเรชั่นส์ จำกัด (มหาชน)
   - **บริษัทย่อย** หมายถึง กิจการที่บริษัท อมรินทร์ คอร์เปอเรชั่นส์ จำกัด (มหาชน) ถือหุ้นทางตรงหรือทางอ้อมมากกว่าร้อยละ 50 ของจำนวนหุ้นทั้งหมดที่มีสิทธิออกเสียง หรือมีอำนาจควบคุมกิจการ
   - **กลุ่มบริษัท** หมายถึง บริษัท อมรินทร์ คอร์เปอเรชั่นส์ จำกัด (มหาชน) และบริษัทย่อย
   - **สารสนเทศ** หมายถึง ข้อมูล ข้อเท็จจริง ข่าวสาร และความรู้ที่ได้มีการบันทึก ประมวลผล หรือดำเนินการด้วยวิธีใด ๆ ซึ่งสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ

- **สินทรัพย์ในระบบเทคโนโลยีสารสนเทศ** หมายถึง ทรัพย์สินหรือสิ่งที่อยู่ภายในหรือใช้งานกับระบบเทคโนโลยีสารสนเทศของกลุ่มบริษัท ทั้งที่เป็นทรัพย์สินที่มีตัวตน เช่น ฮาร์ดแวร์ อุปกรณ์คอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่าย และที่เป็นทรัพย์สินไม่มีตัวตน เช่น สิทธิการใช้ ซอฟต์แวร์ หมายเลขไอพี โดเมนเนม
- **ข้อมูลภายใน** หมายถึง ข้อมูลความลับทางธุรกิจของกลุ่มบริษัท ข้อมูลที่เป็นความลับ หรือข้อมูลสำคัญของกลุ่มบริษัท รวมถึงข้อมูลอื่นใดที่เกี่ยวข้องกับการดำเนินธุรกิจ ข้อมูลทางการเงิน หรือชื่อเสียงของกลุ่มบริษัท ที่ยังไม่เปิดเผยต่อสาธารณะ
- **ปัญญาประดิษฐ์** (Artificial Intelligence : AI) หมายถึง เทคโนโลยีที่ถูกพัฒนาขึ้นเพื่อให้ระบบประมวลผลของคอมพิวเตอร์ หุ่นยนต์เครื่องจักร หรืออุปกรณ์อิเล็กทรอนิกส์ต่าง ๆ มีคุณสมบัติหรือพฤติกรรมใกล้เคียงมนุษย์ ตามวัตถุประสงค์ที่มนุษย์กำหนด เช่น การเรียนรู้ การรับรู้และตอบสนองต่อสภาพแวดล้อม การให้เหตุผล การเลียนแบบพฤติกรรม และการแก้ไขปัญหา เป็นต้น ทั้งนี้ บริษัทเป็นผู้จัดหาและนำ AI ให้ผู้บริหารและพนักงานของกลุ่มบริษัทนำไปใช้งาน

4. หน้าที่และความรับผิดชอบ

เพื่อให้การบริหารจัดการตามนโยบายกำกับดูแลด้านเทคโนโลยีสารสนเทศฉบับนี้เป็นไปอย่างมีประสิทธิภาพ บริษัทจึงกำหนดหน้าที่และความรับผิดชอบของฝ่ายงานและบุคคลที่เกี่ยวข้อง ดังนี้

(1) คณะกรรมการบริษัท: อนุมัติและกำกับดูแลนโยบายให้สอดคล้องกับเป้าหมายเชิงกลยุทธ์และหลักการกำกับดูแลกิจการที่ดีของบริษัท รวมทั้งทบทวนนโยบายให้เหมาะสมกับการเปลี่ยนแปลงของสภาพแวดล้อมทางธุรกิจและกฎหมายที่เกี่ยวข้อง

(2) ผู้บริหารระดับสูง:

- จัดสรรบุคลากร งบประมาณ และเทคโนโลยีให้เพียงพอและเหมาะสมต่อการดำเนินงานที่เกี่ยวข้องกับการกำกับดูแลเทคโนโลยีสารสนเทศเพื่อให้บรรลุตามวัตถุประสงค์ของนโยบายฉบับนี้
- ติดตามและกำกับดูแลให้ฝ่ายงานที่เกี่ยวข้องดำเนินการตามนโยบาย รวมทั้งกำหนดแนวปฏิบัติ หลักเกณฑ์ และระเบียบปฏิบัติที่เกี่ยวข้องกับการกำกับดูแลเทคโนโลยีสารสนเทศ
- ส่งเสริมการให้ความรู้และสร้างความเข้าใจแก่บุคลากรของกลุ่มบริษัท เพื่อให้ปฏิบัติตามนโยบายกำกับดูแลด้านเทคโนโลยีสารสนเทศได้อย่างถูกต้องเหมาะสม

(3) ฝ่ายเทคโนโลยีสารสนเทศ:

- ควบคุม ติดตาม ให้คำแนะนำ และประเมินผลแก่บุคลากรของกลุ่มบริษัทในการปฏิบัติตามนโยบายฉบับนี้ รวมถึงกฎหมายและนโยบายหรือแนวปฏิบัติอื่นที่เกี่ยวข้องกับการกำกับดูแลเทคโนโลยีสารสนเทศ
- ติดตามแนวโน้มเทคโนโลยีและภัยคุกคาม การเปลี่ยนแปลงกฎหมายและมาตรฐานที่เกี่ยวข้อง เพื่อจัดทำหรือเสนอแนะแนวทางในการพัฒนาระบบเทคโนโลยีสารสนเทศของกลุ่มบริษัทให้มีประสิทธิภาพและมีความมั่งคงปลอดภัย
- สนับสนุนการจัดอบรมหรือกิจกรรมทบทวนความรู้และแนวปฏิบัติที่เกี่ยวข้องกับการกำกับดูแลเทคโนโลยีสารสนเทศแก่บุคลากรของกลุ่มบริษัท

(4) พนักงานของกลุ่มบริษัท:

- ปฏิบัติตามนโยบายกำกับดูแลด้านเทคโนโลยีสารสนเทศ รวมถึงกฎหมายและนโยบายอื่นที่เกี่ยวข้องกับการกำกับดูแลเทคโนโลยีสารสนเทศ
- แจ้งผู้บังคับบัญชาหรือฝ่ายเทคโนโลยีสารสนเทศ เมื่อพบการกระทำที่ขัดต่อกฎหมาย นโยบายฉบับนี้ หรือขัดต่อนโยบาย และ/หรือแนวปฏิบัติอื่นของกลุ่มบริษัทที่เกี่ยวข้องกับการกำกับดูแลเทคโนโลยีสารสนเทศ
- เข้ารับการอบรมหรือกิจกรรมทบทวนความรู้และแนวปฏิบัติที่เกี่ยวข้องกับการกำกับดูแลเทคโนโลยีสารสนเทศ ซึ่งฝ่ายเทคโนโลยีสารสนเทศหรือฝ่ายทรัพยากรบุคคลของบริษัทหรือบริษัทย่อยได้จัดขึ้น

ทั้งนี้ กรณีข้อมูลสารสนเทศและระบบเทคโนโลยีสารสนเทศของกลุ่มบริษัทเกิดความเสียหาย อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายกำกับดูแลเทคโนโลยี รวมถึงกฎหมายและนโยบายหรือแนวปฏิบัติที่เกี่ยวข้องกับการกำกับดูแลเทคโนโลยี ถือเป็นความผิดซึ่งต้องถูกดำเนินการทางวินัยตามข้อบังคับหรือระเบียบของบริษัทหรือบริษัทย่อย หรือตามข้อตกลงในสัญญาจ้าง รวมทั้งอาจได้รับโทษตามที่กำหนดในกฎหมาย กฎ ระเบียบ หรือคำสั่งที่เกี่ยวข้อง

5. นโยบาย

5.1 การจัดสรรและบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศ

เพื่อให้การจัดสรรและบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศสอดคล้องกับกลยุทธ์องค์กร บริษัทกำหนดให้ผู้บริหารระดับสูง ฝ่ายเทคโนโลยีสารสนเทศ และฝ่ายงานที่เกี่ยวข้องของบริษัทหรือบริษัทย่อยดำเนินการดังนี้

(1) กำหนดหลักเกณฑ์และปัจจัยในการจัดลำดับความสำคัญของแผนงานด้านเทคโนโลยีสารสนเทศเพื่อให้สอดคล้องกับกลยุทธ์องค์กรหรือเป้าหมายในการดำเนินธุรกิจ

(2) กำหนดหน้าที่และความรับผิดชอบของฝ่ายงานและบุคลากรฝ่ายเทคโนโลยีสารสนเทศ เพื่อจัดสรรและบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศ

(3) จัดทำและอนุมัติงบประมาณด้านเทคโนโลยีสารสนเทศที่สอดคล้องกับงบประมาณและกลยุทธ์องค์กร

(4) จัดให้มีทรัพยากรบุคคลสำหรับงานด้านเทคโนโลยีสารสนเทศอย่างเพียงพอและมีการพัฒนาทักษะบุคลากรดังกล่าวอย่างต่อเนื่อง รวมทั้งพิจารณาจัดจ้างบุคลากรด้านเทคโนโลยีสารสนเทศจากภายนอก เมื่อมีความจำเป็น

5.2 การบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

(1) กำหนดให้มีการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศตามนโยบายบริหารความเสี่ยงองค์กร

(2) กำหนดให้มีการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ เพื่อให้ระบบสารสนเทศของกลุ่มบริษัทพร้อมใช้งานอยู่เสมอ ซึ่งเป็นส่วนหนึ่งของการบริหารความต่อเนื่องทางธุรกิจของกลุ่มบริษัท

(3) กำหนดให้มีการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ โดยกำหนดขั้นตอนบริหารจัดการและผู้รับผิดชอบที่ชัดเจน เพื่อให้เหตุการณ์ดังกล่าวได้รับการแก้ไขหรือดำเนินการอย่างถูกต้อง มีประสิทธิภาพ ภายในระยะเวลาที่เหมาะสม

(4) กำหนดให้มีการบริหารจัดการทรัพย์สินในระบบเทคโนโลยีสารสนเทศ โดยระบุผู้รับผิดชอบและหน้าที่ความรับผิดชอบ เพื่อให้ทรัพย์สินในระบบเทคโนโลยีสารสนเทศที่มีความสำคัญได้รับการป้องกันอย่างเหมาะสม

5.3 ความมั่นคงปลอดภัยสารสนเทศ ความมั่นคงปลอดภัยไซเบอร์ และการคุ้มครองข้อมูล

บริษัทกำหนดให้มีนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ เพื่อใช้ควบคุม ดูแล และกำหนดมาตรฐานในการใช้งานหรือการปฏิบัติงานที่เกี่ยวข้องกับสารสนเทศและระบบเทคโนโลยีสารสนเทศ (“ระบบ IT”) ของกลุ่มบริษัท รวมทั้งเป็นแนวทางให้พนักงานของกลุ่มบริษัทและผู้ที่เกี่ยวข้องถือปฏิบัติ ครอบคลุมในเรื่องต่าง ๆ ดังนี้

(1) การควบคุมการเข้าถึงและการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ

(1.1) การเข้าใช้งาน ระบบ IT ของกลุ่มบริษัท มีการควบคุมและจำกัดสิทธิในการเข้าถึงจากฝ่ายเทคโนโลยีสารสนเทศ (“ฝ่าย IT”) โดยให้เป็นไปตามความจำเป็นในการดำเนินงาน มีความเหมาะสมแบบเป็นลำดับขั้นและตามสิทธิที่พึงมีในการเข้าถึงเท่านั้น ตลอดจนมีการดูแล จัดเก็บ ป้องกันระบบงานและข้อมูลที่สำคัญตามนโยบายของกลุ่มบริษัทและถูกต้องตามกฎหมายที่เกี่ยวข้อง รวมทั้งมีการเก็บหลักฐานการร้องขอสิทธิที่สามารถตรวจสอบได้

(1.2) การเข้าสู่ระบบ IT ของกลุ่มบริษัท ต้องมีการลงทะเบียนผู้ใช้งานซึ่งผ่านการพิสูจน์ตัวตน โดยใช้บัญชีชื่อและรหัสผ่าน (Username และ Password) ของตนเองเท่านั้น ห้ามไม่ให้พนักงานใช้บัญชีชื่อและรหัสผ่านร่วมกับพนักงานผู้อื่น รวมถึงห้ามให้สิทธิ มอบสิทธิ หรือยินยอมให้พนักงานอื่นหรือผู้อื่นใช้บัญชีชื่อและรหัสผ่านของตนเองในทุกกรณี นอกจากนี้ ต้องกำหนดรหัสผ่านอย่างปลอดภัยเพื่อให้สามารถยืนยันตัวตนในการใช้ระบบงาน สามารถระบุผู้รับผิดชอบต่อการบันทึกรายการนั้น ๆ ในระบบงานได้ และใช้เพื่อกำหนดการเข้าถึงข้อมูลแบบเป็นลำดับขั้นตามสิทธิที่พึงมีในการเข้าถึง ตลอดจนใช้เพื่อระบุตัวตนในการใช้งานเส้นทางจราจรในระบบเครือข่ายของกลุ่มบริษัท

(1.3) การเข้าถึงข้อมูลตามระดับชั้นความสำคัญและการจัดเก็บข้อมูลสารสนเทศในระบบงาน ต้องมีการจัดลำดับชั้นความสำคัญของข้อมูล มีการแบ่งประเภทของข้อมูลออกตามหน้าที่ ภารกิจ ฝ่ายงานหรือหน่วยงาน รวมทั้งมีการกำหนดวิธีการบริหารจัดการและการดูแลปกป้องข้อมูลแต่ละประเภท รวมถึงการเข้าถึงและดูแลปกป้องข้อมูลส่วนบุคคลที่มีความอ่อนไหว (ตามคำนิยามในกฎหมายคุ้มครองข้อมูลส่วนบุคคล) และให้มีการกำหนดขั้นตอนและวิธีปฏิบัติกับข้อมูลสำคัญ ก่อนการจำหน่ายออก หรือการเปลี่ยน หรือนำอุปกรณ์กลับมาใช้งานใหม่

(1.4) การควบคุมการเข้าถึงห้องเซิร์ฟเวอร์ เพื่อควบคุมรักษาความปลอดภัยของระบบงาน ระบบเครือข่ายและข้อมูลของกลุ่มบริษัท โดยกำหนดให้จำกัดการเข้าถึงห้องที่มีการติดตั้ง และจัดเก็บอุปกรณ์ที่ใช้ในระบบเครือข่าย หรืออุปกรณ์ที่ใช้กับระบบไอทีของกลุ่มบริษัท ในกรณีผู้ไม่มีหน้าที่เกี่ยวข้องจำเป็นต้องเข้าถึงห้องดังกล่าวจะต้องมีการจัดเก็บบันทึกรายชื่อ เวลา และระบุเหตุผลที่ต้องเข้าสู่พื้นที่ดังกล่าว เพื่อใช้ในการตรวจสอบในภายหลังได้ และต้องมีผู้มีหน้าที่รับผิดชอบห้องเซิร์ฟเวอร์เป็นผู้คอยดูแลควบคุมการเข้าเยือนในพื้นที่ดังกล่าว

(1.5) การรักษาความปลอดภัยของห้องเซิร์ฟเวอร์ กำหนดให้มีการติดตั้งระบบดับเพลิงชนิดที่ใช้กับอุปกรณ์คอมพิวเตอร์และอุปกรณ์อิเล็กทรอนิกส์ในห้องดังกล่าว เพื่อทำความเสียหายต่ออุปกรณ์ให้น้อยที่สุดเมื่อมีความจำเป็นต้องใช้งาน รวมทั้งกำหนดให้มีการติดตั้งระบบสำรองเครื่องปรับอากาศ และระบบสำรองไฟฟ้าฉุกเฉิน

ให้เพียงพอตามระดับความสำคัญของระบบงานต่าง ๆ และกำหนดให้มีรอบการบำรุงรักษาอุปกรณ์ เพื่อให้ระบบงานและระบบเครือข่ายสามารถให้บริการได้อย่างต่อเนื่อง

(1.6) การควบคุมการเข้าถึงเครือข่ายทั้งจากเครือข่ายภายในและเครือข่ายภายนอก กำหนดให้ผู้ที่จะเข้าใช้งานต้องได้รับการอนุมัติในการให้สิทธิการเข้าถึงจากฝ่าย IT ก่อน ต้องมีขั้นตอนการพิสูจน์ยืนยันตัวตน (Authentication) โดยมีการใส่บัญชีชื่อ (Username) เพื่อแสดงตัวตนด้วยชื่อผู้ใช้งานและใส่รหัสผ่านในโดเมนก่อนเข้าใช้งาน และให้มีการบังคับเส้นทางเชื่อมต่อระหว่างเครือข่ายคอมพิวเตอร์ของกลุ่มบริษัทกับระบบอินเทอร์เน็ตให้ผ่านระบบควบคุม ระบบตรวจสอบ และระบบรักษาความปลอดภัยตามที่กลุ่มบริษัทกำหนด และมีการออกแบบระบบเครือข่ายโดยแบ่งเขตแดน (Zone) ในการใช้งาน เพื่อให้สามารถป้องกันภัยคุกคามได้อย่างปลอดภัย มีประสิทธิภาพ และสามารถตรวจสอบได้ในกรณีที่มีเหตุการณ์ผิดปกติเกิดขึ้น

(1.7) การควบคุมการเข้าถึงเครือข่ายไร้สาย เพื่อป้องกันการเข้าถึงระบบไอทีของกลุ่มบริษัท ต้องมีขั้นตอนการพิสูจน์ยืนยันตัวตน (Authentication) โดยมีการใส่บัญชีชื่อ (Username) เพื่อแสดงตัวตนด้วยชื่อผู้ใช้งาน และใส่รหัสผ่านในโดเมนก่อนเข้าใช้งาน หรือในกรณีเป็นผู้มาติดต่องานกับกลุ่มบริษัท (Guest) จำเป็นต้องมีการขออนุมัติใช้งาน ผ่านระบบลงทะเบียนขอใช้งานระบบเครือข่ายไร้สายของกลุ่มบริษัท (Guest Wi-Fi) หรือการนำ MAC Address (Media Access Control Address) ของอุปกรณ์เชื่อมต่อ มาแจ้งขออนุมัติและทำการลงทะเบียนกับฝ่าย IT ก่อนนำไปใช้งาน

(1.8) การควบคุมการเข้าถึงระบบงาน ระบบปฏิบัติการ ฐานข้อมูล โปรแกรมประยุกต์ และโปรแกรมอรรถประโยชน์ต่าง ๆ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต กำหนดให้ผู้ที่จะเข้าใช้งานต้องได้รับการอนุมัติจากฝ่าย IT ก่อน ต้องมีขั้นตอนในการพิสูจน์ยืนยันตัวตน (Authentication) โดยมีการใส่บัญชีชื่อ (Username) เพื่อแสดงตัวตนด้วยชื่อผู้ใช้งาน และใส่รหัสผ่านก่อนเข้าใช้งาน โดยการเข้าถึงระบบงานที่สำคัญ ต้องให้สิทธิเฉพาะการปฏิบัติงานในขอบเขตหน้าที่ โดยได้รับอนุมัติจากผู้บังคับบัญชา หรือผู้มีสิทธิในการอนุมัติเป็นลายลักษณ์อักษร หรือร้องขอสิทธิจากระบบแจ้งร้องขอสิทธิของกลุ่มบริษัท เพื่อบันทึกไว้เป็นหลักฐานในการตรวจสอบ มีการยกเลิกสิทธิการใช้งาน เมื่อเปลี่ยนแปลงหน้าที่รับผิดชอบหรือลาออก และให้มีการทบทวนสิทธิที่ได้รับอย่างสม่ำเสมอ รวมถึงคอมพิวเตอร์ของกลุ่มบริษัทที่มีการเชื่อมต่อกับระบบอินเทอร์เน็ต ให้มีการติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ มีการบังคับเส้นทางเชื่อมต่อกับระบบอินเทอร์เน็ตให้ผ่านระบบควบคุม ตรวจสอบและระบบรักษาความปลอดภัย

(1.9) กำหนดให้มีการรักษาความมั่นคงปลอดภัยของระบบจดหมายอิเล็กทรอนิกส์ (อีเมล) ของกลุ่มบริษัท รวมทั้งมีการกำหนดหน้าที่และความรับผิดชอบของผู้ใช้งานในการใช้ระบบอีเมลของกลุ่มบริษัท โดยพนักงานต้องใช้ระบบอีเมลของกลุ่มบริษัทเท่านั้นในการติดต่องานที่เกี่ยวข้องกับภารกิจของกลุ่มบริษัท ตลอดจนมีการกำหนดข้อห้าม ข้อควรระวัง ตลอดจนสิทธิในการใช้งานโดยฝ่าย IT โดยคำนึงถึงความมั่นคงปลอดภัยของระบบ IT ของกลุ่มบริษัท

(1.10) เพื่อป้องกันการเข้าถึงระบบ IT ของกลุ่มบริษัทโดยไม่ได้รับอนุญาต รวมถึงป้องกันการเปิดเผยหรือการขโมยข้อมูล กำหนดให้พนักงานของกลุ่มบริษัทมีหน้าที่รับผิดชอบในการตั้งและเปลี่ยนค่ารหัสผ่านสำหรับการเข้าสู่ระบบ IT ของกลุ่มบริษัทให้ถูกต้องตามนโยบายควบคุมของฝ่าย IT รวมทั้งไม่เปิดหน้าจอเครื่องคอมพิวเตอร์ค้างไว้ โดยไม่มีการป้องกันผู้อื่นเข้ามาใช้งานแทน ตลอดจนการเก็บรักษาดูแลสินทรัพย์ในระบบ IT ของกลุ่มบริษัท

ไว้ในที่ปลอดภัย เพื่อป้องกันไม่ให้ผู้ไม่ประสงค์ดีนำสินทรัพย์ดังกล่าวไปใช้ในทางที่ทำให้เกิดความเสียหายต่อกลุ่มบริษัทได้

(1.11) เพื่อป้องกันความเสี่ยงจากช่องโหว่ที่อาจถูกใช้ในการโจมตีระบบงาน กำหนดให้ฝ่าย IT บริหารจัดการการติดตั้งแพตช์ของระบบปฏิบัติการอย่างต่อเนื่อง ทั้งนี้ ในระบบงาน ERP ซึ่งเป็นระบบงานสำคัญของบริษัท ให้ดำเนินการบริหารจัดการเพื่อติดตั้งแพตช์ทั้งส่วนซอฟต์แวร์และระบบปฏิบัติการที่จำเป็นภายในระยะเวลาที่เหมาะสม โดยมีการทดสอบในสภาพแวดล้อมที่ปลอดภัยก่อนนำไปใช้งานจริง ในกรณีระบบงานสำคัญไม่สามารถแพตช์ได้ ให้ฝ่าย IT ระบุในรายการข้อยกเว้นด้านความมั่นคงปลอดภัยของระบบงาน IT เพื่อใช้ในการติดตามและบริหารจัดการความเสี่ยงตามกระบวนการจัดการที่กำหนด

(1.12) เพื่อเฝ้าระวังให้การแพตช์ในระบบงาน ERP เป็นไปอย่างต่อเนื่องและมีประสิทธิภาพ กำหนดให้ฝ่าย IT ดำเนินการหรือประสานงานเพื่อตรวจสอบผลการประเมินช่องโหว่ของซอฟต์แวร์และระบบปฏิบัติการอย่างน้อยปีละ 1 ครั้ง และส่งรายงานผลการประเมินผลให้ผู้บริหารลงนามรับทราบ เพื่อพิจารณาบริหารจัดการตามความเหมาะสม

(2) การสำรองระบบข้อมูลและการเตรียมความพร้อมรับมือกับสถานการณ์ฉุกเฉินและภัยคุกคามทางไซเบอร์

(2.1) กำหนดให้มีการจัดทำระบบสำรองข้อมูลที่สำคัญในระบบ IT ของกลุ่มบริษัท เพื่อสามารถให้บริการได้อย่างต่อเนื่อง มีเสถียรภาพ มีความปลอดภัย รวมทั้งกำหนดให้มีการตรวจสอบและดูแลระบบสำรองให้อยู่ในสภาพพร้อมนำมาใช้งานอยู่เสมอ โดยเรียงลำดับความสำคัญในการสำรองข้อมูลในระบบ IT ของกลุ่มบริษัทตามความจำเป็น จากมากไปน้อย ตลอดจนกำหนดหน้าที่ความรับผิดชอบให้กับเจ้าหน้าที่ผู้ตรวจสอบและดูแลระบบการสำรองข้อมูล

(2.2) กำหนดให้มีการสำรองข้อมูลในระบบงานที่สำคัญในระบบ IT ของกลุ่มบริษัทเป็นประจำ โดยพิจารณาจำนวนรอบในการสำรองข้อมูล วิธีการ และเทคโนโลยีที่นำมาใช้ในการสำรองข้อมูลให้เหมาะสมกับความสำคัญของข้อมูลในระบบงานของกลุ่มบริษัท ตลอดจนพิจารณาจัดเก็บระบบงานและข้อมูลที่สำคัญของกลุ่มบริษัทไว้ให้พร้อมใช้งาน ณ สถานที่ปลอดภัยอีกแห่งหนึ่งแทน ตลอดจนให้จัดทำแผนเตรียมความพร้อมในสถานการณ์ฉุกเฉิน (IT Contingency Plan) และจัดเตรียมระบบประมวลผลสำรองรองรับ เพื่อให้ธุรกรรมหลักของกลุ่มบริษัทสามารถดำเนินต่อไปได้อย่างต่อเนื่อง

(2.3) กำหนดให้ฝ่าย IT หรือให้ตกลงกับฝ่ายงานเจ้าของข้อมูลในการกำหนดรอบระยะเวลาการสำรองข้อมูลระยะเวลาในการจัดเก็บรักษาข้อมูล ซึ่งต้องมั่นใจได้ว่าข้อมูลและฐานข้อมูลของกลุ่มบริษัทได้มีการสำรองข้อมูลอย่างสม่ำเสมอ ครบถ้วน และต่อเนื่อง พร้อมที่จะนำกลับมาใช้งานภายในเวลาที่กำหนดไว้ เมื่อเกิดเหตุการณ์ฉุกเฉินขึ้น

(2.4) มีการกำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ฝ่าย IT ในการสำรองข้อมูล ตรวจสอบข้อมูลที่สำรอง และการกู้คืนข้อมูล รวมถึงหน้าที่ในการประเมินและทบทวนแผนเตรียมความพร้อมกรณีเกิดสถานการณ์ฉุกเฉิน ตลอดจนมีการกำหนดหน้าที่ความรับผิดชอบและวิธีปฏิบัติในการจัดการกับสถานการณ์ฉุกเฉินที่เกิดขึ้น โดยการเข้าถึงข้อมูลสำรองของกลุ่มบริษัทและการเรียกข้อมูลกลับมาใช้งาน ให้กระทำโดยผู้ได้รับอนุญาตจากกลุ่มบริษัทและผู้ดูแลระบบงานเท่านั้น

(2.5) กำหนดให้มีการทดสอบสื่อและระบบที่ใช้ในการเก็บสำรองข้อมูลและฐานข้อมูลที่สำคัญของกลุ่มบริษัทเป็นประจำอย่างน้อยปีละ 1 ครั้ง และรายงานผลทดสอบให้ผู้บริหารระดับสูงของฝ่าย IT รับทราบ เพื่อให้มั่นใจว่าสามารถนำระบบงานและข้อมูลกลับมาใช้งานได้ตลอดเวลาหรือเมื่อเกิดสถานการณ์ฉุกเฉินขึ้น

(2.6) พนักงานมีหน้าที่รับผิดชอบในการเก็บรักษาข้อมูลของกลุ่มบริษัทไว้ในที่ที่กำหนดไว้อย่างปลอดภัย เพื่อให้ระบบสำรองข้อมูลสามารถกู้คืนข้อมูลของกลุ่มบริษัทกลับมาได้ และป้องกันไม่ให้ผู้ไม่ประสงค์ดีนำข้อมูลดังกล่าวไปใช้ในทางที่ทำให้เกิดความเสียหายต่อกลุ่มบริษัท โดยห้ามพนักงานสำรองข้อมูลส่วนตัวหรือข้อมูลที่ไม่เกี่ยวข้องกับการปฏิบัติงานของกลุ่มบริษัทลงในระบบข้อมูลของกลุ่มบริษัท

(2.7) กำหนดให้จัดทำแผนขั้นตอนการบริหารจัดการเหตุข้อมูลรั่วไหล (Data Breach) และเหตุละเมิดข้อมูลส่วนบุคคล (Personal Data Breach) ที่เหมาะสม ครอบคลุมการแจ้งเหตุ การรายงาน การประเมินผลกระทบ การควบคุมความเสียหายและการดำเนินการตามกฎหมายหรือข้อกำหนดที่เกี่ยวข้อง รวมถึงต้องสื่อสารและสร้างความเข้าใจเกี่ยวกับขั้นตอนดังกล่าวให้แก่พนักงานและผู้ที่เกี่ยวข้อง เพื่อให้สามารถรายงานและตอบสนองต่อเหตุการณ์ได้อย่างถูกต้องและทันท่วงที

(2.8) พนักงานและผู้ที่เกี่ยวข้องมีหน้าที่เฝ้าระวัง แจ้งรายงาน และให้ความร่วมมือในการดำเนินการตามขั้นตอนการบริหารจัดการเหตุข้อมูลรั่วไหล (Data Breach) และเหตุละเมิดข้อมูลส่วนบุคคล (Personal Data Breach) ของกลุ่มบริษัท เมื่อพบหรือสงสัยว่าอาจเกิดเหตุการณ์ดังกล่าวต้องแจ้งต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO) และฝ่าย IT โดยไม่ล่าช้า เพื่อให้สามารถประเมินผลกระทบ ควบคุมความเสียหาย และดำเนินการตามกฎหมายและข้อกำหนดที่เกี่ยวข้องได้อย่างทันท่วงที

(2.9) กำหนดให้จัดทำแผนบริหารความต่อเนื่องและการกู้คืนระบบเทคโนโลยีสารสนเทศจากเหตุภัยพิบัติเพื่อเป็นแนวทางปฏิบัติ รวมถึงจัดเตรียมระบบประมวลผลสำรองและทรัพยากรที่จำเป็นต้องใช้ในการเชื่อมต่อเข้าสู่เครือข่ายหลักและเครือข่ายสำรอง เพื่อให้ธุรกรรมหลักของกลุ่มบริษัทสามารถดำเนินงานต่อไปได้อย่างต่อเนื่อง

(2.10) เพื่อตอบสนองต่อสถานการณ์ฉุกเฉินของระบบ IT ที่มีผลกระทบต่อการดำเนินธุรกิจของกลุ่มบริษัท กำหนดให้มีการจัดตั้งคณะทำงานและบุคลากรเพื่อทำหน้าที่บริหารจัดการเมื่อเกิดสถานการณ์ฉุกเฉินขึ้น โดยมีการกำหนดบทบาท ความรับผิดชอบ ขั้นตอนดำเนินการที่จำเป็น และวิธีการสื่อสารที่ชัดเจน เพื่อปฏิบัติตามแผนที่จัดเตรียมไว้

(2.11) กำหนดให้จัดทำแผนรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ (Cyber Incident Response Plan) และพัฒนาแผนให้ครอบคลุมทั้งข้อมูลสารสนเทศ รวมถึงองค์ประกอบโครงสร้างพื้นฐานของระบบงานและระบบเครือข่ายที่สำคัญและพึงต้องมีตามกิจกรรมทางธุรกิจหลักของกลุ่มบริษัท รวมทั้งกำหนดให้มีการซ้อมและทบทวนเป็นประจำทุกปี เพื่อให้มั่นใจว่าจะสามารถนำไปใช้ในสถานการณ์จริงได้อย่างมีประสิทธิภาพ โดยฝ่ายบริหารและพนักงานที่เกี่ยวข้องต้องรับทราบและเข้าใจวิธีดำเนินการตามที่กำหนด

(2.12) เพื่อตอบสนองต่อเหตุการณ์ที่เป็นภัยคุกคามทางไซเบอร์อย่างมีประสิทธิภาพ กำหนดให้มีการจัดตั้งคณะทำงานและบุคลากรเพื่อทำหน้าที่รับมือและตอบสนองต่อเหตุโจมตีทางไซเบอร์ โดยมีการกำหนดบทบาท

ความรับผิดชอบ ขั้นตอนดำเนินการที่จำเป็น และวิธีการสื่อสารที่ชัดเจน เพื่อให้พนักงานที่มีส่วนเกี่ยวข้องเข้าใจในบทบาทหน้าที่ของตนเอง สามารถปฏิบัติหน้าที่ได้อย่างถูกต้องและรวดเร็วเมื่อเกิดภัยคุกคามทางไซเบอร์ขึ้น

(3) การตรวจสอบ การประเมินความเสี่ยง และการควบคุมข้อมูลภายใน

(3.1) บริษัทกำหนดให้มีการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศของกลุ่มบริษัท โดยจัดให้มีผู้ตรวจสอบภายในของกลุ่มบริษัท หรือผู้ตรวจสอบอิสระจากภายนอก (External Auditor) อย่างน้อยปีละ 1 ครั้ง เพื่อให้บริษัทและฝ่ายงานได้รับทราบถึงระดับความเสี่ยงและความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของกลุ่มบริษัท

(3.2) บริษัทกำหนดให้ทุกฝ่ายงานจัดระบบงาน สถานที่ปฏิบัติงาน เพื่อเก็บรักษาข้อมูลภายในของกลุ่มบริษัท ไม่ให้ข้อมูลเหล่านั้นถูกเปิดเผยไปยังบุคคลที่ไม่เกี่ยวข้องหรือบุคคลที่ไม่จำเป็นต้องล่วงรู้ สำหรับการใช้ข้อมูลภายในหรือการส่งข้อมูลภายใน ให้กระทำโดยผู้มีหน้าที่รับผิดชอบหรือได้รับอนุญาตจากผู้มีอำนาจอนุมัติเท่านั้น โดยกระบวนการดังกล่าวจะต้องได้รับการตรวจสอบจากหน่วยงานตรวจสอบระบบสารสนเทศ (IT Audit)

(3.3) ห้ามพนักงานที่ปฏิบัติงานเกี่ยวข้องกับข้อมูลภายในของกลุ่มบริษัท เปิดเผยข้อมูลภายในไม่ว่าทางตรงหรือทางอ้อมแก่บุคคลใด ๆ เว้นแต่จะได้รับมอบหมายเป็นหน้าที่รับผิดชอบและได้รับอนุญาตจากผู้มีอำนาจอนุมัติเท่านั้น

(4) การสร้างความตระหนักและระเบียบการรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ

(4.1) จัดอบรมแนวปฏิบัติการรักษาความมั่นคงปลอดภัยสารสนเทศ ความมั่นคงปลอดภัยไซเบอร์ และการคุ้มครองข้อมูล ตามนโยบายกำกับดูแลด้านเทคโนโลยีสารสนเทศของกลุ่มบริษัทอย่างสม่ำเสมอ และให้ความรู้ด้านกฎหมายและกฎระเบียบที่เกี่ยวข้องกับการใช้งาน

(4.2) เผยแพร่นโยบายกำกับดูแลด้านเทคโนโลยีสารสนเทศ ทางอินทราเน็ตของกลุ่มบริษัท เพื่อให้พนักงานกลุ่มบริษัททุกคนสามารถเข้าถึงได้โดยสะดวก

(4.3) จัดให้มีมาตรการเชิงป้องกัน โดยการให้ความรู้เกี่ยวกับแนวปฏิบัติในลักษณะวิธีใช้ ข้อควรระวังในการใช้งานระบบ IT ของกลุ่มบริษัท รวมถึงกำหนดบทลงโทษแก่พนักงาน เมื่อพบว่ามีการกระทำผิด หรือมีการใช้งานระบบ IT ที่ไม่ถูกต้อง เช่น การระงับการเข้าถึงหรือการระงับสิทธิในการใช้งาน

(4.4) พนักงานมีหน้าที่ดำเนินการให้เป็นไปตามนโยบายที่กำหนดขึ้นนี้อย่างเคร่งครัด ผู้ที่ฝ่าฝืนไม่ปฏิบัติตามนโยบายฉบับนี้ไม่ว่าข้อหนึ่งข้อใด หรือละเมิดลิขสิทธิ์ในการใช้โปรแกรมคอมพิวเตอร์ของกลุ่มบริษัทเพื่อผลประโยชน์ของตนเองหรือบุคคลอื่น รวมทั้งใช้ระบบ IT ของกลุ่มบริษัทนอกเหนือจากหน้าที่รับผิดชอบของตน หรือไม่ใช่เพื่อผลประโยชน์ของกลุ่มบริษัท ถือเป็นการผิดวินัยพนักงาน

(4.5) กรณีเครื่องคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์ใด ๆ เกิดความเสียหาย หรือสูญหาย ให้พนักงานผู้ใช้งาน ผู้รับผิดชอบครอบครอง หรือผู้ได้รับมอบหมาย แจ้งให้ผู้บริหารหรือบุคคลที่ได้รับมอบหมายให้ทำหน้าที่แทนทราบโดยทันที เพื่อดำเนินการแก้ไขหรือบรรเทาความเสียหายต่อไป

(5) การปฏิบัติเกี่ยวกับโปรแกรมคอมพิวเตอร์ที่กลุ่มบริษัทหรือพนักงานจัดหา สร้างสรรค์ พัฒนา

(5.1) การสร้างสรรค์หรือพัฒนาโปรแกรมคอมพิวเตอร์เพื่อนำมาใช้งานของกลุ่มบริษัท จะต้องได้รับการพิจารณาเห็นชอบเป็นลายลักษณ์อักษรจากผู้บริหารหรือผู้มีอำนาจที่ได้รับมอบหมายจากกลุ่มบริษัท

(5.2) โปรแกรมคอมพิวเตอร์ที่พนักงานได้สร้างสรรค์หรือพัฒนาขึ้นในฐานะพนักงานของกลุ่มบริษัท ให้ลิขสิทธิ์โปรแกรมคอมพิวเตอร์นั้นเป็นของกลุ่มบริษัท

(5.3) การประมวลผลข้อมูลแบบกลุ่ม (Batch Processing) จะต้องดำเนินการภายใต้การควบคุมที่เหมาะสม โดยกำหนดตารางเวลาในการประมวลผล (Batch schedule) และการตรวจสอบความถูกต้องของข้อมูลหลังการประมวลผล รวมถึงต้องมีมาตรการสำรองข้อมูลและระบบเฝ้าระวังเพื่อป้องกันความเสียหายที่อาจเกิดขึ้นจากความผิดพลาดในการประมวลผล

(5.4) การนำโปรแกรมคอมพิวเตอร์ที่เกี่ยวข้องกับปัญญาประดิษฐ์ (Artificial Intelligence : "AI") มาใช้ในการทำงาน ให้ปฏิบัติตามนโยบายและแนวปฏิบัติการใช้ปัญญาประดิษฐ์ โดยคำนึงถึงความปลอดภัยของข้อมูล ห้ามใช้หรือเปิดเผยข้อมูลภายใน ข้อมูลความลับ เอกสารสำคัญ หรือข้อมูลที่อาจส่งผลกระทบต่อการดำเนินงานของกลุ่มบริษัท รวมถึงข้อมูลส่วนบุคคลในการใช้งาน AI นอกจากนี้ ต้องตรวจสอบความถูกต้องของข้อมูลที่ได้จาก AI ก่อนนำไปใช้งาน และต้องปฏิบัติตามขั้นตอนในการขออนุมัติเพื่อนำ AI ที่ปลอดภัยมาใช้งานในกลุ่มบริษัท

(6) การบริหารจัดการผู้ให้บริการเทคโนโลยีสารสนเทศภายนอก

(6.1) เพื่อให้มั่นใจว่าการดำเนินงานของผู้ให้บริการระบบงาน ERP หรือระบบงานอื่นที่บริษัทประเมินว่าเป็นระบบงานสำคัญเทียบเท่าที่ใช้ในการดำเนินธุรกิจ สามารถปฏิบัติตามข้อกำหนดความปลอดภัยตามนโยบายบริษัทได้ ทั้งนี้ ก่อนที่จะเลือกใช้บริการหรือทำสัญญา กำหนดให้ฝ่าย IT มีสิทธิในการเข้าถึงในการตรวจสอบและประเมินสัญญาให้บริการ เพื่อให้บริการที่ได้รับเป็นไปตามข้อกำหนดด้านความมั่นคงปลอดภัยของบริษัท

(6.2) กำหนดให้มีการบริหารจัดการ ติดตาม ตรวจสอบ และประเมินผลการให้บริการของผู้ให้บริการระบบงาน ERP หรือระบบงานอื่นที่บริษัทประเมินว่าเป็นระบบงานสำคัญเทียบเท่าที่ใช้ในการดำเนินธุรกิจอย่างสม่ำเสมอ เพื่อป้องกันความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินงานของผู้ให้บริการภายนอก

6. การทบทวนนโยบาย

บริษัทกำหนดให้มีการทบทวนนโยบายกำกับดูแลด้านเทคโนโลยีสารสนเทศนี้เป็นประจำทุกปี หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ และให้นำเสนอต่อคณะกรรมการบริษัทพิจารณาอนุมัติหากมีการปรับปรุงหรือเปลี่ยนแปลงนโยบาย

ให้นโยบายกำกับดูแลด้านเทคโนโลยีสารสนเทศฉบับนี้ มีผลบังคับใช้ตั้งแต่วันที่ 14 สิงหาคม 2569 เป็นต้นไป