บริษัท เอพี (ไทยแลนด์) จำกัด (มหาชน) และบริษัทในเครือ

ประกาศที่ AP-HOBPI-060/2566

นโยบาย

เรื่อง การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

เพื่อให้การดำเนินงานด้านเทคโนโลยีสารสนเทศของ บริษัท เอพี (ไทยแลนด์) จำกัด (มหาชน) และบริษัทในเครือ (ต่อไปนี้เรียกว่า "บริษัท") มีความมั่นคงปลอดภัย และรองรับมาตรการคุ้มครองข้อมูลส่วนบุคคล บริษัทจึงได้กำหนดนโยบายฉบับนี้ เพื่อใช้เป็นกรอบให้พนักงาน ผู้บริหาร และผู้ดูแลระบบบริหารจัดการระบบเทคโนโลยีสารสนเทศ ดำเนินงานได้อย่างมีประสิทธิภาพ และเป็นไปตามมกฎหมายและข้อบังคับของหน่วยงานราชการและหน่วยงานกำกับที่กำหนด โดยให้ยกเลิกประกาศเลขที่ 051/2555 และใช้ประกาศฉบับนี้ทดแทน โดยมีรายละเอียด ดังต่อไปนี้

1. ขอบเขต

ครอบคลุมการดำเนินงานด้านเทคโนโลยีสารสนเทศ บริษัท เอพี (ไทยแลนด์) จำกัด (มหาชน) และบริษัทในเครือ โดยครอบคลุมถึงทรัพย์สินของบริษัททุกประเภท (ไม่ว่าทรัพย์สินนั้นจะตั้งอยู่ในบริษัทหรือไม่ก็ตาม) ได้แก่

- ข้อมูล (ฐานข้อมูล, เอกสาร, อีเมล์ เป็นต้น) รวมถึงข้อมูลส่วนบุคคล
- ซอฟต์แวร์ลิขสิทธิ์ หรือโปรแกรมที่พัฒนาขึ้น
- ทรัพย์สินทางกายภาพ (ห้องคอมพิวเตอร์, อุปกรณ์คอมพิวเตอร์, โน้ตบุ๊ค, แท็บเล็ต, เครื่องพิมพ์, พื้นที่ทำงาน เป็นต้น)
- พนักงานและบุคลากรที่บริษัทว่าจ้าง
- งานบริการต่าง ๆ (ระบบสำรองไฟฟ้า, การสื่อสาร, ระบบเครือข่าย เป็นต้น)

2. คำจำกัดความ

- **การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ** หมายถึง การรักษาไว้ซึ่งความลับของข้อมูล (Confidentiality) ความถูกต้องครบถ้วนของข้อมูล (Integrity) และข้อมูลมีสภาพพร้อมใช้งาน (Availability) เพื่อป้องกันข้อมูลถูกเข้าถึงโดยไม่ได้รับอนุญาติ หรือ ถูกแก้ไขเปลี่ยนแปลง หรือ ข้อมูลสูญหายจนไม่สามารถใช้งานได้
- **มาตรการการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ** หมายถึง กระบวนการระบุบริบทที่เกี่ยวข้องกับความเสี่ยงด้านสารสนเทศ (Identify) การปกป้องทรัพย์สินสารสนเทศ (Protect) การตรวจจับเหตุการณ์ผิดปกติ (Detect) การรับมือเหตุการณ์ผิดปกติ (Response) และการกู้คืนสินทรัพย์สารสนเทศจากความเสียหายเพื่อให้ธุรกิจสามารถดำเนินได้อย่างต่อเนื่อง (Recovery)

3. รายละเอียด

บริษัทกำหนดนโยบายในภาพรวมเพื่อการบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศ โดยจัดแบ่งสาระสำคัญออกเป็น 14 หมวด ดังต่อไปนี้

1) การกำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy) : บริษัทจัดให้มีการกำหนดนโยบายความมั่นคงปลอดภัยด้านสารสนเทศเป็นลายลักษณ์อักษร และต้องสื่อสารนโยบายดังกล่าวแก่พนักงานและหน่วยงานภายนอกที่เกี่ยวข้อง เพื่อสร้างความเข้าใจและสามารถปฏิบัติตามได้อย่างถูกต้อง ตลอดจนทบทวนนโยบายตามรอบระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญต่อองค์กร

2) โครงสร้างองค์กร บทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ (Organization of Information Security) : บริษัทจัดให้มีการกำหนดหน้าที่ความรับผิดชอบในการปฏิบัติงานที่ชัดเจน และต้องกำกับดูแล การประเมิน และการติดตามผลการปฏิบัติงานที่เกี่ยวกับมาตรการด้านความปลอดภัยในระบบสารสนเทศ

3) ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human Resources Security) : บริษัทกำหนดให้มีมาตรการในการควบคุมความมั่นคงปลอดภัยเกี่ยวกับการบริหารจัดการบุคคลกร และการให้ความรู้เกี่ยวกับความมั่นคงปลอดภัยให้แก่บุคลากรที่เหมาะสม เพื่อให้มั่นใจได้ว่าพนักงานของบริษัท และบุคลากรอื่น ๆ ที่บริษัทได้ว่าจ้างมาทำงานให้บริษัท มีความตระหนักและปฏิบัติตามนโยบายของบริษัท รวมถึงการถอดถอนสิทธิในการเข้าถึงระบบและการคืนทรัพย์สิน เมื่อสิ้นสุดการจ้างงาน

4) การจัดหมวดหมู่และการควบคุมทรัพย์สินขององค์กร (Asset Management) : บริษัทจัดให้มีการจัดทำบัญชีทรัพย์สินที่ระบุผู้ถือครองหรือดูแลทรัพย์สิน โดยกำหนดหลักเกณฑ์ในการใช้งาน และส่งการคืนทรัพย์สินรวมถึงการทำลายสื่อบันทึก

ข้อมูลที่เหมาะสมตามระดับชั้นความลับของข้อมูลที่อยู่ในสื่อนั้น และจัดทำป้ายชื่อเพื่อการบริหารจัดการทรัพย์สินตามที่ได้จัดหมวดหมู่ไว้เพื่อป้องกันทรัพย์สินสารสนเทศของบริษัทให้มีความมั่นคงปลอดภัยตามมาตรการการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

5) การควบคุมการเข้าถึง (Access Control) : บริษัทจัดให้มีการควบคุมการเข้าถึงระบบสารสนเทศทั้งภายในและภายนอกบริษัทอย่างปลอดภัย โดยต้องกำหนดรหัสผ่าน การกำหนดสิทธิในการใช้งาน การทบทวนสิทธิการใช้งาน และต้องได้รับอนุญาตตามระเบียบของบริษัท

6) การเข้ารหัสข้อมูลสำหรับข้อมูลที่เป็นความลับ (Encryption) : บริษัทจัดให้มาตรการเข้ารหัสข้อมูลตามความเหมาะสมเพื่อรักษาข้อมูลสำคัญที่เป็นความลับโดยให้ข้อมูลนั้นเข้าถึงหรือใช้งานได้โดยบุคคลที่ได้รับอนุญาตเท่านั้น โดยอาศัยกระบวนการทำงานด้วยคอมพิวเตอร์เพื่อเข้ารหัส (Encrypt) ให้อยู่ในรูปของข้อมูลที่ไม่สามารถอ่านได้โดยตรง และข้อมูลนั้นจะถูกถอดรหัส (Decrypt) ในรูปแบบและวิธีการที่ถูกต้องก่อนจึงจะสามารถอ่านข้อมูลได้

7) ความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environmental Security) : บริษัทกำหนดให้มีมาตรการในการควบคุมเกี่ยวกับความปลอดภัยด้านสถานที่และสภาพแวดล้อม การควบคุมการเข้าออกสถานที่ที่ติดตั้งระบบคอมพิวเตอร์ ระบบสำรองไฟ ระบบปรับอากาศ ระบบป้องกันอื่น ๆ (เช่น ระบบสแกนนิ้วมือ กล้องวงจรปิด ระบบดับเพลิงอัตโนมัติ) เพื่อป้องกันไม่ให้ผู้ที่ไม่เกี่ยวข้องเข้าถึงและก่อให้เกิดความเสียหายกับทรัพย์สินสารสนเทศ ร่วมถึงการบำรุงรักษาอุปกรณ์ต่าง ๆ ให้อยู่ในสภาวะที่เหมาะสมและพร้อมใช้งาน

8) ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operations Security) : บริษัทจัดให้มีวางแผนด้านทรัพยากรสารสนเทศให้สามารถพร้อมใช้งาน มีระบบป้องกันที่เหมาะสม ระบบบันทึกเหตุการณ์ผิดปกติ การตรวจสอบการใช้งานระบบ ระบบสำรองข้อมูล การรับส่งหรือการแลกเปลี่ยนข้อมูล (เช่น อีเมล์, อินเตอร์เน็ต) รวมถึงการควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบ (Change Management) เพื่อให้มั่นใจว่าระบบสารสนเทศของบริษัทมีความมั่นคงปลอดภัย

9) ความมั่นคงปลอดภัยในการสื่อสารข้อมูล (Communications Security) : บริษัทกำหนดให้มีมาตรการการควบคุมการเข้าถึงระบบเครือข่ายให้มีความมั่นคงปลอดภัย การจัดแบ่งเครือข่ายระหว่างผู้ใช้งานภายในและผู้ใช้ภายนอกที่ติดต่อกับบริษัท และการควบคุมการเข้าถึงระบบเครือข่ายจากภายนอก (VPN) ต้องได้รับการอนุมัติจากผู้มีอำนาจก่อนทุกครั้ง, กรณีนำอุปกรณ์คอมพิวเตอร์ส่วนตัวมาต่อเชื่อมกับเครือข่ายบริษัทต้องได้รับอนุมัติก่อนการใช้งานและให้สิทธิ์เท่าที่จำเป็นเท่านั้น รวมถึงกำหนดให้มีวิธีการที่ปลอดภัยที่ใช้ในการถ่ายโอนข้อมูลระหว่างหน่วยงานและองค์กรภายนอก

10) การจัดหา, การพัฒนาและการบำรุงรักษาระบบ (Systems Acquisition, Development and Maintenance) บริษัทต้องกำหนดให้มีมาตรการด้านความมั่นคงปลอดภัยของระบบสารสนเทศในทุกขั้นตอนตลอดวงจรชีวิตการพัฒนาระบบซึ่งครอบคลุมถึงกระบวนในการพัฒนา การทดสอบ และข้อมูลสำหรับใช้ทดสอบ รวมถึงการตรวจสอบความมั่นคงปลอดภัยของข้อมูลที่ใช้นำเข้า หรือนำออกไปใช้ นอกจากนี้มาตรการดังกล่าวให้ถือเป็นส่วนหนึ่งในการพิจารณาหรือจัดจ้างจากผู้ให้บริการภายนอกด้วย

11) ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier Relationships) : บริษัทต้องกำหนดให้มีมาตรการป้องกันทรัพย์สินด้านสารสนเทศที่สามารถเข้าถึงโดยผู้ให้บริการภายนอก ต้องมีข้อตกลงเป็นลายลักษณ์อักษร สัญญาการใช้บริการ สัญญารักษาความลับ ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล กับผู้ให้บริการภายนอกที่สามารถเข้าถึงระบบ การประมวลผล การจัดเก็บและการสื่อสารสารสนเทศ ที่ผู้ให้บริการภายนอกต้องปฏิบัติ และการบริหารจัดการด้านการเปลี่ยนแปลงที่เกิดขึ้นในการให้บริการจากผู้ให้บริการภายนอก

12) การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management) : บริษัทต้องจัดให้มีผู้รับผิดชอบและกำหนดขั้นตอนปฏิบัติ เพื่อรับมือกับเหตุการณ์ที่กระทบกับความปลอดภัยระบบสารสนเทศ และการละเมิดมาตรการคุ้มครองข้อมูลส่วนบุคคลของบริษัท รวมถึงการรายงานเหตุการณ์ที่ผิดปกติและจุดอ่อนที่เกี่ยวกับความปลอดภัย รวมถึงข้อมูลส่วนบุคคลรั่วไหล ต่อผู้บริหารฝ่ายระบบเทคโนโลยีสารสนเทศและหน่วยงานกำกับที่เกี่ยวข้อง

13) ความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ (Business Continuity Management) : บริษัทจัดให้มีแผนงานด้านความต่อเนื่องในการดำเนินธุรกิจในฝ่ายระบบสารสนเทศ เพื่อรองรับกรณีที่เกิดหตุการณ์วิกฤตหรือภัยพิบัติซึ่งทำให้ระบบสารสนเทศหรือระบบเครือข่ายไม่สามารถใช้งานได้ตามปกติ บริษัทจะสามารถจัดการกับปัญหาเหล่านี้เพื่อให้สามารถให้บริการกับลูกค้าได้ตามแผนงานและต้องจัดให้มีการทดสอบแผนความต่อเนื่องทางธุรกิจอย่างน้อยปีละ 1 ครั้ง หรือตามความเหมาสม เพื่อนำผลลัพธ์ไปปรับปรุงแผนงานให้เหมาะสมกับการดำเนินธุรกิจ

14) การปฏิบัติตามข้อกำหนด (Compliance) : บริษัทจัดให้มีการปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ ของหน่วยงานราชการและหน่วยงานกำกับที่กำหนดไว้ รวมถึงข้อกำหนดด่าง ๆ ในสัญญาที่ผูกพันกับบริษัท

4. บทบาทและความรับผิดชอบ

1) **IT Steering Committee** มีหน้าที่รับผิดชอบในฐานะเป็นผู้กำหนดทิศทาง และมาตรการการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ รวมถึงให้การสนับสนุนเพื่อให้การดำเนินการต่าง ๆ เป็นไปตามนโยบายของบริษัท

2) **Chief Information Technology Officer** มีหน้าที่กำกับดูแลให้การปฏิบัติงานเป็นไปตามนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศที่บริษัทฯ ได้ประกาศไว้

3) **ผู้บริหารของแต่ละหน่วยงาน** มีหน้าที่รับผิดชอบทรัพย์สินและข้อมูลต่าง ๆ ที่อยู่ภายใต้การดูแลของหน่วยงานตามนโยบายของบริษัทให้อยู่ในสภาพที่มีความมั่นคงปลอดภัย รวมถึงประสานงานกับหน่วยงาน IT ในการร่วมตรวจสอบ และประเมินผลของมาตรการด้านความมั่นคงปลอดภัยด้านสารสนเทศที่ได้นำมาปฏิบัติ

4) **พนักงาน, ผู้จัดจำหน่าย, คู่สัญญา และที่ปรึกษา** มีหน้าที่ปฏิบัติตามนโยบายความมั่นคงปลอดภัย, มาตรฐาน, วิธีปฏิบัติ และแนวทางในการดำเนินงานที่เกี่ยวข้อง เพื่อให้เกิดความมั่นคงปลอดภัยด้านสารสนเทศในการปฏิบัติงาน

5. การบังคับใช้และบทลงโทษ

นโยบายฉบับนี้ ถือเป็นส่วนหนึ่งของระเบียบบริษัท หากพนักงานฝ่าฝืนหรือไม่ปฏิบัติตามอาจได้รับโทษทางวินัยตามที่ระบุในระเบียบข้อบังคับในการทำงาน ซึ่งบริษัทฯ จะพิจารณาลงโทษทางวินัยตามดุลยพินิจต่อไป

ให้ประกาศนี้มีผลตั้งแต่ วันที่ 10 กรกฎาคม พ.ศ. 2566 เป็นต้นไป

เห็นชอบโดย

(คุณสมชาย วัฒนเสาวภาคย์)
Chief Information Technology Officer

อนุมัติโดย

(คุณพิเชษฐ วิภาศุภกร)
IT Steering Committee

เสนอโดย _____ คุณเจือกิพย์ แย้มไสย (Director: Business Process Management and Improvement (Head of)

_____ คุณดนัย คุมตะวิชัย (Director: IT Infrastructure and Security Management (Head of)