ที่ กส. 2566/021

ประกาศ
เรื่อง นโยบายบริหารความมั่นคงปลอดภัยสารสนเทศ

1. **วัตถุประสงค์** (Objective)

   1.1 เพื่อรักษาซึ่งความมั่นคงปลอดภัยของข้อมูลอันประกอบไปด้วย การรักษาความลับของข้อมูล (Confidential) การรักษาความถูกต้องสมบูรณ์ของข้อมูล (Integrity) และความพร้อมใช้งานของข้อมูล (Availability)

   1.2 เพื่อให้มีการกำหนดทิศทางการบริหารจัดการและการสนับสนุนด้านความมั่นคงปลอดภัยสารสนเทศโดยสอดคล้องกับความต้องการทางธุรกิจและกฎหมาย รวมถึงระเบียบข้อบังคับที่เกี่ยวข้อง

2. **การบังคับใช้** (Enforcement)

บังคับใช้กับบริษัท บีเคไอ โฮลดิ้งส์ จำกัด (มหาชน) และบริษัทย่อย รวมถึงพนักงาน ผู้ให้บริการภายนอก ที่อยู่ในขอบเขตระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศของบริษัทฯ

3. **นิยาม** (Define)

บริษัท/บริษัทฯ หมายถึง บริษัท บีเคไอ โฮลดิ้งส์ จำกัด (มหาชน)

พนักงาน หมายถึง ทรัพยากรด้านบุคลากรของบริษัทฯ

ผู้ให้บริการภายนอก หมายถึง นิติบุคคลหรือตัวแทนนิติบุคคลที่ปฏิบัติงานให้กับบริษัทฯ โดยมีการว่าจ้างตามระเบียบบริษัทฯ ซึ่งมีระยะเวลาปฏิบัติงานตามช่วงเวลาที่ระบุในสัญญาจ้าง

ทรัพย์สินด้านสารสนเทศ หมายถึง ฐานข้อมูล ไฟล์ข้อมูล ซอฟต์แวร์ เครื่องมือในการพัฒนาอุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย อุปกรณ์สื่อสาร สื่อบันทึกข้อมูลภายนอก และอุปกรณ์ต่อพ่วงทุกชนิด

ระบบสารสนเทศ หมายถึง ระบบที่มีการนำฮาร์ดแวร์ ซอฟต์แวร์ บุคลากร แนวปฏิบัติ และข้อมูล ซึ่งทำงานประสานกันเพื่อจัดเตรียมสารสนเทศให้กับบริษัทฯ

สารสนเทศ หมายถึง ข้อมูลต่าง ๆ ที่ได้ผ่านการเปลี่ยนแปลง ประมวลผล หรือวิเคราะห์สรุปผลด้วยวิธีการต่าง ๆ แล้วเก็บรวบรวมไว้ เพื่อนำมาใช้ประโยชน์ตามต้องการ การประมวลผลเป็นการนำข้อมูลจากแหล่งต่าง ๆ ที่เก็บรวบรวมไว้มาผ่านกระบวนการต่าง ๆ เพื่อแปรสภาพข้อมูลให้เป็นระบบที่อยู่ในรูปแบบที่ต้องการและนำไปใช้งานกับธุรกิจของบริษัทฯ

บมจ. บีเคไอ โฮลดิ้งส์
BKI Holdings PCL.
25 Bangkok Insurance Building, Floor 5
Sathon Tai Road, Thung Maha Mek,
Sathon, Bangkok 10120
25 อาคารกรุงเทพประกันภัย ชั้น 5
ถนนสาทรใต้ แขวงทุ่งมหาเมฆ เขตสาทร
กรุงเทพมหานคร 10120
T 0 2285 7008
bkiholdings.com

4. บทนำ

นโยบายบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy: IS Policy) ของบริษัท บีเคไอ โฮลดิ้งส์ จำกัด (มหาชน) จัดตั้งขึ้นเพื่อให้มีการกำหนดทิศทางการบริหารจัดการ และการสนับสนุนด้านความมั่นคงปลอดภัยสารสนเทศ โดยสอดคล้องกับความต้องการทางธุรกิจและกฎหมาย รวมถึงระเบียบข้อบังคับที่เกี่ยวข้องโดยมีการกำหนดนโยบายในแต่ละด้าน เผยแพร่ และบังคับใช้กับพนักงาน ผู้ให้บริการภายนอก ที่อยู่ในขอบเขตระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศของบริษัทฯ รวมถึงมีการทบทวนนโยบายบริหารความมั่นคงปลอดภัยสารสนเทศอย่างน้อยปีละ 1 ครั้งหรือมีการเปลี่ยนแปลงที่มีนัยสำคัญ

5. การบริหารจัดการโครงการด้านเทคโนโลยีสารสนเทศ (Project Management)

พนักงาน ที่อยู่ในขอบเขตระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศของบริษัทฯ ต้องมีการควบคุมการบริหารจัดการโครงการด้านเทคโนโลยีสารสนเทศได้อย่างมั่นคงปลอดภัยตั้งแต่ก่อนเริ่มจัดตั้งโครงการจนกระทั่งถึงโครงการเสร็จสิ้น

6. ความมั่นคงปลอดภัยสำหรับทรัพยากรบุคคล (Human Resource Security)

พนักงาน ผู้ให้บริการภายนอก ที่อยู่ในขอบเขตระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศของบริษัทฯ ต้องเข้าใจในหน้าที่ความรับผิดชอบของตนเอง และมีความเหมาะสมตามบทบาทของตนเองที่ได้รับการพิจารณา ตระหนักและปฏิบัติตามหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศของตนเอง และเพื่อป้องกันผลประโยชน์ของบริษัทฯ ซึ่งเป็นส่วนหนึ่งของกระบวนการเปลี่ยนหรือสิ้นสุดการจ้างงาน

ทั้งนี้ความมั่นคงปลอดภัยในการบริหารงานทรัพยากรบุคคล ได้แก่ กระบวนการบริหารจัดการก่อนการจ้างงาน กระบวนการบริหารจัดการพนักงาน และผู้ให้บริการภายนอกในระหว่างการจ้างงาน และกระบวนการบริหารจัดการเมื่อมีการสิ้นสุด หรือเปลี่ยนการจ้างงาน

7. การบริหารจัดการทรัพย์สิน (Asset Management)

พนักงาน ผู้ให้บริการภายนอก ที่อยู่ในขอบเขตระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศของบริษัทฯ ต้องมีการระบุทรัพย์สินของบริษัทฯ และกำหนดหน้าที่ความรับผิดชอบในการป้องกันทรัพย์สินตามระดับการป้องกันที่เหมาะสม และเพื่อป้องกันการเปิดเผยโดยไม่ได้รับอนุญาต การเปลี่ยนแปลง การขนย้าย การลบหรือการทำลายข้อมูลและสารสนเทศที่จัดเก็บอยู่บนสื่อบันทึกข้อมูล

ทั้งนี้การบริหารจัดการทรัพย์สินสารสนเทศให้มีความมั่นคงปลอดภัย ต้องรวมถึงการระบุหน้าที่ความรับผิดชอบต่อทรัพย์สินสารสนเทศของบริษัทฯ การจัดชั้นความลับของข้อมูลและสารสนเทศ และการจัดการสื่อบันทึกข้อมูล

8. **การควบคุมการเข้าถึง** (Access Control)

พนักงาน ผู้ให้บริการภายนอก ที่อยู่ในขอบเขตระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศของบริษัทฯ ต้องควบคุมการเข้าถึงสารสนเทศ อุปกรณ์ประมวลผลสารสนเทศ และระบบงานสารสนเทศของบริษัทฯ เฉพาะผู้ที่ได้รับอนุญาต และป้องกันการเข้าถึงระบบและบริการโดยไม่ได้รับอนุญาต และเพื่อให้ผู้ใช้งานมีความรับผิดชอบในการป้องกันข้อมูลการพิสูจน์ตัวตน

9. **การเข้ารหัสข้อมูล** (Cryptography)

พนักงาน ผู้ให้บริการภายนอก ที่อยู่ในขอบเขตระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศของบริษัทฯ ต้องกำหนดให้มีเข้ารหัสข้อมูล เพื่อให้มีการใช้การเข้ารหัสข้อมูลอย่างเหมาะสม ได้ผล และป้องกันความลับ การปลอมแปลง หรือความถูกต้องของสารสนเทศ

10. **ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม** (Physical and environmental Security)

พนักงาน ผู้ให้บริการภายนอก ที่อยู่ในขอบเขตระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศของบริษัทฯ ต้องป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต ความเสียหาย และการแทรกแซงการทำงานที่มีต่อสารสนเทศ อุปกรณ์ประมวลผลสารสนเทศ และระบบงานสารสนเทศของบริษัทฯ รวมทั้งป้องกันการหยุดชะงักต่อการดำเนินงานของบริษัทฯ

11. **ความมั่นคงปลอดภัยสำหรับการดำเนินงาน** (Operations Security)

พนักงาน ผู้ให้บริการภายนอก ที่อยู่ในขอบเขตระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศของบริษัทฯ ต้องปฏิบัติตามขั้นการปฏิบัติงานและหน้าที่ความรับผิดชอบ เพื่อให้การปฏิบัติงานกับสารสนเทศ อุปกรณ์ประมวลผลสารสนเทศ และระบบงานสารสนเทศของบริษัทฯ เป็นไปอย่างถูกต้อง มั่นคงปลอดภัย ได้รับการป้องกันจากโปรแกรมไม่ประสงค์ดี ได้รับการป้องกันการสูญหายของข้อมูล เพื่อให้ระบบงานสารสนเทศมีการบันทึกเหตุการณ์และจัดทำหลักฐาน มีการทำงานที่ถูกต้อง และมีการป้องกันการใช้ประโยชน์จากช่องโหว่ทางเทคนิค และเพื่อลดผลกระทบของกิจกรรมการตรวจประเมินบนระบบให้บริการ

12. **ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล** (Communications security)

พนักงาน ผู้ให้บริการภายนอก ที่อยู่ในขอบเขตระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศของบริษัทฯ ต้องมีการป้องกันสารสนเทศในเครือข่ายและอุปกรณ์ประมวลผลสารสนเทศ เพื่อให้มีการรักษาความมั่นคงปลอดภัยของสารสนเทศที่มีการถ่ายโอนภายในบริษัทฯ หรือถ่ายโอนกับหน่วยงานภายนอก

13. **ความมั่นคงปลอดภัยไซเบอร์** (Cyber Security Policy)

พนักงาน ผู้ให้บริการภายนอก ที่อยู่ในขอบเขตระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศของบริษัทฯ ต้องปฏิบัติตามคำแนะนำรวมถึงกฎหมายที่เกี่ยวกับระบบคอมพิวเตอร์ได้อย่างถูกต้อง และเหมาะสม เพื่อป้องกันไม่ให้ระบบคอมพิวเตอร์ และข้อมูลสารสนเทศของบริษัท โดนบุกรุก ขโมย ทำลาย แทรกแซงการทำงาน หรือโจรกรรมในรูปแบบต่าง ๆ ที่อาจจะสร้างความเสียหายต่อการดำเนินธุรกิจของบริษัท

14. **การจัดหา การพัฒนา และการบำรุงรักษาระบบ** (System acquisition, development and maintenance)

พนักงาน ผู้ให้บริการภายนอก ที่อยู่ในขอบเขตระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศของบริษัทฯ ต้องพัฒนาระบบอย่างมั่นคงปลอดภัย เพื่อให้ความมั่นคงปลอดภัยสารสนเทศเป็นองค์ประกอบสำคัญหนึ่งของระบบตลอดวงจรชีวิตของการพัฒนาระบบ ซึ่งรวมถึงความต้องการด้านระบบที่มีการให้บริการผ่านเครือข่ายสาธารณะด้วย

15. **ความสัมพันธ์กับผู้ให้บริการภายนอก** (Supplier relationships)

พนักงาน ผู้ให้บริการภายนอก ที่อยู่ในขอบเขตระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศของบริษัทฯ ต้องมีการป้องกันทรัพย์สินของบริษัทฯ ที่มีการเข้าถึงโดยผู้ให้บริการภายนอก และเพื่อให้มีการรักษาไว้ซึ่งระดับความมั่นคงปลอดภัยและระดับการให้บริการตามที่ตกลงกันไว้ในข้อตกลงการให้บริการของผู้ให้บริการภายนอก

16. **การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ** (Information Security Incident Management)

พนักงาน ผู้ให้บริการภายนอก ที่อยู่ในขอบเขตระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศของบริษัทฯ ต้องบริหารจัดการเหตุละเมิดความมั่นคงปลอดภัยสารสนเทศและการปรับปรุง รวมถึงการติดต่อกับหน่วยงานผู้มีอำนาจ และกลุ่มที่มีความสนใจเป็นพิเศษในเรื่องเดียวกัน เพื่อให้มีวิธีการที่สอดคล้องกันและได้ผลสำหรับการบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ ซึ่งรวมถึงการแจ้งสถานการณ์ความมั่นคงปลอดภัยสารสนเทศและจุดอ่อนความมั่นคงปลอดภัยสารสนเทศให้ได้รับทราบ

17. **ความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ** (Information security aspects of business continuity management)

พนักงาน ผู้ให้บริการภายนอก ที่อยู่ในขอบเขตระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศของบริษัทฯ ต้องบริหารจัดการความต่อเนื่องของระบบสารสนเทศ รวมถึงการเตรียมการอุปกรณ์ประมวลผลสำรองเพื่อให้ระบบสารสนเทศของบริษัทฯ สามารถให้บริการได้อย่างต่อเนื่อง และเพื่อจัดเตรียมสภาพความพร้อมใช้ของอุปกรณ์ประมวลผลสารสนเทศของบริษัทฯ

18. **ความสอดคล้อง** (Compliance)

พนักงาน ผู้ให้บริการภายนอก ที่อยู่ในขอบเขตระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศของบริษัทฯ ต้องปฏิบัติตามกฎหมาย มาตรฐาน และ ข้อบังคับ เพื่อหลีกเลี่ยงการละเมิดข้อผูกพันในกฎหมาย ระเบียบข้อบังคับ หรือสัญญาจ้าง ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ และเพื่อให้มีการปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศอย่างสอดคล้องกับนโยบายและขั้นตอนปฏิบัติขององค์กร

19. **ความมั่นคงปลอดภัยสำหรับผู้ใช้งานระบบเทคโนโลยีสารสนเทศ** (End user oriented topics)

พนักงาน ผู้ให้บริการภายนอก ที่อยู่ในขอบเขตระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศของบริษัทฯ ต้องปฏิบัติตามขั้นตอนสำหรับผู้ใช้งานระบบเทคโนโลยีสารสนเทศ เพื่อให้มีกฎเกณฑ์การใช้งานสารสนเทศ ทรัพย์สินที่เกี่ยวข้องกับสารสนเทศ อุปกรณ์ประมวลผลสารสนเทศอย่างเหมาะสม มีการป้องกันการเข้าถึงทางกายภาพต่อเอกสารและข้อมูลสำคัญของบริษัทฯ มีการรักษาความมั่นคงปลอดภัยของสารสนเทศที่มีการถ่ายโอนภายในบริษัทฯ หรือถ่ายโอนกับหน่วยงานภายนอก มีกฎเกณฑ์ควบคุมการติดตั้งซอฟต์แวร์โดยผู้ใช้งาน และเพื่อรักษาความมั่นคงปลอดภัยของการปฏิบัติงานจากระยะไกลและของการใช้งานอุปกรณ์คอมพิวเตอร์แบบพกพา

20. **การลงโทษทางวินัย**

หากพบการกระทำความผิดฝ่าฝืนนโยบายฉบับนี้ บริษัทฯ จะพิจารณาลงโทษทางวินัย ซึ่งอาจรวมไปถึงการถูกดำเนินคดีตามกฎหมายได้ ซึ่งมีโทษทั้งจำทั้งปรับ

21. ข้อยกเว้น

หากพนักงาน หรือผู้ให้บริการภายนอก ที่อยู่ในขอบเขตระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศของบริษัทฯ ไม่สามารถปฏิบัติตามได้ ให้ชี้แจงเหตุผล และทำหนังสือขออนุญาตให้ผู้มีอำนาจอนุมัติเป็นกรณีไป ซึ่งข้อยกเว้นนั้นต้องมีระบบรักษาความปลอดภัยที่เหมาะสมมาทดแทนด้วย

ประกาศ ณ วันที่ 22 กันยายน 2566

(ดร.อภิสิทธิ์ อนันตนาถรัตน)

ประธานคณะผู้บริหาร

บมจ. บีเคไอ โฮลดิ้งส์
BKI Holdings PCL.

25 Bangkok Insurance Building, Floor 5
Sathon Tai Road, Thung Maha Mek,
Sathon, Bangkok 10120

25 อาคารกรุงเทพประกันภัย ชั้น 5
ถนนสาทรใต้ แขวงทุ่งมหาเมฆ เขตสาทร
กรุงเทพมหานคร 10120

T 0 2285 7008
bkiholdings.com