บริษัท บี.กริม เพาเวอร์ จำกัด (มหาชน) สำนักงานใหญ่
B.Grimm Power Public Company Limited (Head Office)
5 ถนนกรุงเทพกรีฑา แขวงหัวหมาก เขตบางกะปิ กรุงเทพฯ 10240
5 Krungthepkreetha Road, Huamark, Bangkapi, Bangkok 10240
Tel. +66 (0) 2710 3400, Fax +66 (0) 2379 4257
เลขประจำตัวผู้เสียภาษีอากร 0107559000427

นโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ

บริษัทบี.กริม เพาเวอร์ จำกัด (มหาชน) ได้กำหนดนโยบายและขั้นตอนด้านความปลอดภัยของสารสนเทศ เพื่อให้มั่นใจว่าระบบเทคโนโลยีสารสนเทศมีความเหมาะสม มีประสิทธิภาพ ปลอดภัย และสามารถปฏิบัติงานได้อย่างต่อเนื่อง มาตรการเหล่านี้มีจุดมุ่งหมายเพื่อป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้ระบบเทคโนโลยีสารสนเทศที่ไม่เหมาะสม รวมถึงการเผชิญกับภัยคุกคามทางไซเบอร์ที่อาจส่งผลกระทบต่อความมั่นคงขององค์กร ด้วยเหตุนี้ บี.กริม เพาเวอร์ จึงมีการกำหนดนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ โดยกำหนดมาตรฐานและขั้นตอนความปลอดภัยของระบบเทคโนโลยีสารสนเทศและป้องกันภัยคุกคามต่าง ๆ อย่างเหมาะสม

ขอบเขต

นโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ มีผลบังคับใช้ครอบคลุมทั่วทั้งกลุ่มบริษัท บี.กริม เพาเวอร์ บริษัทย่อย รวมไปถึงกิจการร่วมค้าและผู้รับเหมาที่อยู่ภายใต้การดูแลควบคุมของบี.กริม เพาเวอร์ ซึ่งได้รับสิทธิ์ในการเข้าถึงใช้ระบบเครือข่าย ระบบคอมพิวเตอร์ และฮาร์ดแวร์ทั้งหมดของบี.กริม เพาเวอร์

วัตถุประสงค์

- เพื่อรักษาความลับของข้อมูลสำคัญ ให้มั่นใจในความสมบูรณ์และความถูกต้องของข้อมูล และมีความพร้อมใช้งาน ทำให้สามารถใช้ข้อมูลได้อย่างต่อเนื่องตามการอนุญาต และสามารถดำเนินธุรกิจได้อย่างต่อเนื่อง
- เพื่อบริหารจัดการความปลอดภัยสารสนเทศให้เป็นไปตามมาตรฐานสากลและมีการปรับปรุงและพัฒนาอย่างต่อเนื่อง
- เพื่อให้มั่นใจว่าความเสี่ยงและภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศของบี.กริม เพาเวอร์ ได้รับการระบุ ป้องกัน ตรวจจับ ตอบสนองและกู้คืนได้อย่างมีประสิทธิภาพ ซึ่งจะช่วยลดผลกระทบที่อาจเกิดขึ้นต่อโอกาสทางธุรกิจและบี.กริม เพาเวอร์ ให้เหลือน้อยที่สุด
- เพื่อสนับสนุนการเติบโตอย่างยั่งยืนของบี.กริม เพาเวอร์ ในการดำเนินธุรกิจในยุคดิจิทัลที่เปลี่ยนแปลงตลอดเวลา

บี.กริม เพาเวอร์ จึงมีการกำหนดนโยบายเพื่อให้สอดคล้องกับวัตถุประสงค์ดังนี้

1. **นโยบายความมั่นคงปลอดภัยด้านบุคลากร**

   ฝ่ายทรัพยากรบุคคลต้องดำเนินการตรวจสอบประวัติผู้สมัคร กำหนดเงื่อนไขการจ้างงาน และแจ้งข้อมูลการเปลี่ยนแปลงสถานะพนักงานต่อฝ่ายเทคโนโลยีสารสนเทศอย่างทันท่วงที พนักงานใหม่ต้องได้รับการฝึกอบรมด้านระบบสารสนเทศและความปลอดภัยข้อมูล พร้อมจัดให้มีการอบรมและสร้างความตระหนักรู้แก่พนักงานอย่างสม่ำเสมอ ทั้งนี้ พนักงานทุกคนต้องปฏิบัติตามนโยบาย กฎหมาย และข้อกำหนดด้านความปลอดภัยของบี.กริม เพาเวอร์ อย่างเคร่งครัด

บริษัท บี.กริม เพาเวอร์ จำกัด (มหาชน) สำนักงานใหญ่
B.Grimm Power Public Company Limited (Head Office)
5 ถนนกรุงเทพกรีฑา แขวงหัวหมาก เขตบางกะปิ กรุงเทพฯ 10240
5 Krungthepkreetha Road, Huamark, Bangkapi, Bangkok 10240
Tel. +66 (0) 2710 3400, Fax +66 (0) 2379 4257
เลขประจำตัวผู้เสียภาษีอากร 0107559000427

2. **นโยบายความมั่นคงทางกายภาพและสภาพแวดล้อม**

   บี.กริม เพาเวอร์ ต้องกำหนดมาตรการควบคุมพื้นที่ระบบเทคโนโลยีสารสนเทศโดยแบ่งตามระดับความสำคัญ พร้อมควบคุมการเข้าถึงของบุคคลและอุปกรณ์อย่างเข้มงวด รวมถึงมีการป้องกันภัยคุกคามทางกายภาพและสิ่งแวดล้อมอย่างเหมาะสม และต้องมีการบันทึก ตรวจสอบ และรายงานเหตุการณ์ด้านความปลอดภัยตามระยะเวลาและขั้นตอนที่กำหนด.

3. **นโยบายการควบคุมการเข้าถึง**

   บี.กริม เพาเวอร์ กำหนดมาตรการควบคุมการเข้าถึงข้อมูล ระบบสารสนเทศ และอุปกรณ์จัดเก็บข้อมูลให้เหมาะสมกับบทบาทหน้าที่ โดยยึดหลักการยืนยันตัวตน การบริหารสิทธิ์อย่างเป็นระบบ และการใช้รหัสผ่านที่ปลอดภัย พร้อมทั้งควบคุมการเข้าถึงระยะไกล การเข้ารหัสข้อมูล และการใช้งานอุปกรณ์อย่างรัดกุม เพื่อป้องกันความเสี่ยงและรักษาความมั่นคงปลอดภัยของข้อมูลในทุกขั้นตอน

4. **นโยบายการรักษาความมั่นคงปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย**

   บี.กริม เพาเวอร์ กำหนดแนวทางควบคุมและรักษาความมั่นคงปลอดภัยของเครือข่ายอย่างรัดกุม ครอบคลุมการควบคุมการเข้าถึง การใช้งาน การป้องกันมัลแวร์ การเข้ารหัสข้อมูล รวมถึงการบริหารจัดการกุญแจเข้ารหัส การตรวจสอบความปลอดภัย และการสำรองข้อมูล ทั้งนี้เพื่อป้องกันภัยคุกคามและรับมือกับเหตุการณ์ที่ไม่พึงประสงค์อย่างมีประสิทธิภาพ พร้อมส่งเสริมการอบรมและสร้างความตระหนักรู้ด้านความปลอดภัยแก่บุคลากรในองค์กร

5. **นโยบายการรักษาความปลอดภัยสำหรับอินเทอร์เน็ต**

   บี.กริม เพาเวอร์ กำหนดแนวปฏิบัติในการใช้งานอินเทอร์เน็ตภายในองค์กรอย่างชัดเจน เพื่อควบคุมการใช้งานที่เหมาะสม ป้องกันการเข้าถึงหรือเผยแพร่ข้อมูลที่อาจก่อให้เกิดความเสียหายต่อ บี.กริม เพาเวอร์ และรักษาความปลอดภัยของข้อมูล ทั้งนี้รวมถึงข้อห้ามการใช้งานในเชิงพาณิชย์ การเปิดเผยข้อมูลลับ การใช้โซเชียลมีเดียอย่างมีความรับผิดชอบ และการห้ามนำข้อมูลใส่ในระบบ Generative AI โดยมิได้รับอนุญาต

6. **นโยบายการพัฒนาระบบอย่างมั่นคงปลอดภัย**

   บี.กริม เพาเวอร์ กำหนดแนวปฏิบัติด้านความปลอดภัยสำหรับการพัฒนาและปรับปรุงระบบสารสนเทศ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การรั่วไหลของข้อมูล และการพัฒนาซอฟต์แวร์ที่อาจก่อให้เกิดความเสี่ยง โดยครอบคลุมการควบคุมการเข้าถึงซอร์สโค้ด การแยกสภาพแวดล้อมการพัฒนา การปฏิบัติตามมาตรฐานความปลอดภัย รวมถึงข้อห้ามที่ชัดเจนในการพัฒนาเครื่องมือที่มีผลกระทบต่อระบบ

7. **นโยบายการตอบสนองต่อเหตุการณ์ข้อมูลรั่วไหล**

   บี.กริม เพาเวอร์ กำหนดมาตรการด้านการบริหารจัดการเพื่อควบคุมและจำกัดการเข้าถึงข้อมูล โดยประเมินและตอบสนองต่อเหตุการณ์ข้อมูลรั่วไหลอย่างเป็นระบบ โดยแผนกความปลอดภัยทางด้านไซเบอร์ (Cyber Security) รับผิดชอบในการตรวจสอบ ประสานงาน และประเมินความเสี่ยง พร้อมทั้งจัดเก็บบันทึกและรักษาความลับของเหตุการณ์ รวมถึงพิจารณาการรายงานต่อหน่วยงานภายนอกตามความเหมาะสม

บริษัท บี.กริม เพาเวอร์ จำกัด (มหาชน) สำนักงานใหญ่
B.Grimm Power Public Company Limited (Head Office)
5 ถนนกรุงเทพกรีฑา แขวงหัวหมาก เขตบางกะปิ กรุงเทพฯ 10240
5 Krungthepkreetha Road, Huamark, Bangkapi, Bangkok 10240
Tel. +66 (0) 2710 3400, Fax +66 (0) 2379 4257
เลขประจำตัวผู้เสียภาษีอากร 0107559000427

8. นโยบายการเก็บรักษาและการลบทำลายข้อมูล

บี.กริม เพาเวอร์ กำหนดให้มีการจัดเก็บข้อมูลอย่างปลอดภัย โดยควบคุมการเข้าถึงเอกสารหรือสื่อข้อมูลที่สำคัญหรือเป็นความลับ และกำหนดให้มีการทำลายข้อมูลอย่างเหมาะสมตามประเภทและระดับชั้นความลับ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตและลดความเสี่ยงจากการละเมิดข้อมูล

9. นโยบายการจัดการชั้นความลับข้อมูล

นโยบายการจัดชั้นความลับข้อมูลมีวัตถุประสงค์เพื่อแบ่งประเภทข้อมูลสำคัญของบี.กริม เพาเวอร์ เป็น 4 ระดับ ได้แก่ ข้อมูลสาธารณะ ข้อมูลใช้ภายใน ข้อมูลความลับ และข้อมูลหวงห้ามเฉพาะ เพื่อกำหนดเกณฑ์ความอ่อนไหวและผลกระทบในด้านการเงิน กฎหมาย ชื่อเสียง และลูกค้าอย่างชัดเจน โดยช่วยให้บี.กริม เพาเวอร์ สามารถบริหารจัดการความปลอดภัยข้อมูลได้เหมาะสมและปฏิบัติตามข้อกฎหมายได้อย่างมีประสิทธิภาพ

10. นโยบายการตอบสนองต่อเหตุการณ์

นโยบายการตอบสนองต่อเหตุการณ์มีเป้าหมายเพื่อจัดตั้งกระบวนการที่ชัดเจน ครอบคลุมตั้งแต่การเตรียมความพร้อม การตรวจจับ การจัดการเหตุการณ์ การสื่อสารภายในและภายนอก ตลอดจนการประเมินผลและปรับปรุงอย่างต่อเนื่อง โดยมอบหมายบทบาทและความรับผิดชอบอย่างชัดเจนแก่ผู้ใช้งาน หน่วยงานเทคโนโลยีสารสนเทศ และหน่วยงานที่เกี่ยวข้อง เพื่อให้สามารถรับมือกับเหตุการณ์ด้านความปลอดภัยสารสนเทศได้อย่างมีประสิทธิภาพและสอดคล้องตามข้อกำหนดขององค์กร

11. นโยบายการบริหารความต่อเนื่องทางธุรกิจด้านความปลอดภัยของข้อมูล

เพื่อให้การดำเนินธุรกิจของบี.กริม เพาเวอร์ มีความต่อเนื่องแม้เกิดเหตุการณ์ไม่คาดคิด ฝ่ายเทคโนโลยีสารสนเทศต้องประเมินผลกระทบ พัฒนาและทบทวนแผนความต่อเนื่องทางธุรกิจ (BCP) และแผนกู้คืนจากความเสียหาย (DRP) อย่างน้อยปีละ 1 ครั้ง รวมถึงทดสอบแผนดังกล่าวเป็นประจำ โดยครอบคลุมเหตุการณ์ด้านความปลอดภัยทาง Cyber และจัดทำรายงานเสนอต่อผู้บริหารระดับสูงเพื่อประกอบการตัดสินใจ

12. นโยบายความสัมพันธ์กับผู้ให้บริการภายนอก

บี.กริม เพาเวอร์ มีการกำหนดข้อกำหนดด้านความปลอดภัยของข้อมูลร่วมกับผู้ให้บริการภายนอก โดยระบุประเด็นสำคัญในสัญญา ได้แก่ ข้อกำหนดตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) ความรับผิดชอบจากการรับเหมาช่วง และการจัดการความเสี่ยง พร้อมทั้งมีการติดตาม ตรวจสอบ และทบทวนการให้บริการตามสัญญาอย่างสม่ำเสมอ และการเปลี่ยนแปลงใด ๆ ต้องได้รับความยินยอมร่วมกันจากทั้งสองฝ่าย

13. นโยบายคุ้มครองข้อมูลส่วนบุคคล

บี.กริม เพาเวอร์ ดำเนินการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลตามกฎหมายอย่างโปร่งใสและเป็นธรรม โดยอาศัยความยินยอมจากเจ้าของข้อมูล หรือเป็นไปตามข้อยกเว้นที่กฎหมายบัญญัติ ข้อมูลที่เก็บรวมถึงข้อมูลทั่วไป ข้อมูลอ่อนไหว ข้อมูลการติดต่อ ข้อมูลทางการเงิน และข้อมูลสารสนเทศต่าง ๆ ทั้งนี้ บี.กริม เพาเวอร์ กำหนดมาตรการรักษาความปลอดภัยของข้อมูลอย่างรัดกุม เก็บรักษาข้อมูลตามระยะเวลาที่จำเป็นตามวัตถุประสงค์ และให้สิทธิแก่เจ้าของข้อมูลในการเข้าถึง แก้ไข ลบ หรือคัดค้านการใช้ข้อมูล ทั้งนี้ บี.กริม เพาเวอร์ อาจปรับปรุงนโยบายเป็นระยะเพื่อให้สอดคล้องกับกฎหมายและแนวปฏิบัติที่เปลี่ยนแปลง