บริษัท เอ็ม บี เค จำกัด (มหาชน)
MBK Public Company Limited
444 ชั้น 8 อาคาร เอ็ม บี เค เซ็นเตอร์ ถนนพญาไท แขวงวังใหม่ เขตปทุมวัน กรุงเทพฯ 10330 ทะเบียนเลขที่ 0107537001102
444 8th Fl., MBK Center, Phayathai Rd., Wangmai, Pathumwan, Bangkok 10330 Thailand Registration No. 0107537001102
โทรศัพท์ (Telephone): +66 (0) 2853 9000 โทรสาร (Fascimile): +66 (0) 2853 7000 www.mbkgroup.co.th

# นโยบายความปลอดภัยสำหรับระบบสารสนเทศ กลุ่มบริษัท เอ็ม บี เค

เนื่องด้วยกลุ่มบริษัท เอ็ม บี เค (MBK GROUP) (“องค์กร”) ได้มีการนำระบบเทคโนโลยีสารสนเทศมาใช้เป็นเครื่องมือเพื่อช่วยดำเนินธุรกิจเป็นเวลานาน ดังนั้น จึงมีข้อมูลที่มีความสำคัญซึ่งถือเป็นทรัพย์สินอย่างหนึ่ง (Information Asset) ของกลุ่มบริษัท เอ็ม บี เค อยู่เป็นจำนวนมาก ทางผู้บริหารกลุ่มบริษัท เอ็ม บี เค ได้เล็งเห็นถึงความสำคัญดังกล่าว จึงให้มีการกำหนดนโยบายความปลอดภัยสำหรับระบบสารสนเทศ เพื่อให้การใช้งานระบบสารสนเทศต่างๆ ของกลุ่มบริษัท เอ็ม บี เค เป็นไปด้วยความปลอดภัย ให้สอดคล้องกับข้อบังคับ กฎ ระเบียบ กฎหมายด้านความมั่นคงปลอดภัยสารสนเทศในปัจจุบัน โดยมีรายละเอียด ดังต่อไปนี้

## 1. วัตถุประสงค์

เพื่อให้การดำเนินการบริหารจัดการงานด้านเทคโนโลยีสารสนเทศของกลุ่มบริษัท เอ็ม บี เค มีความมั่นคงปลอดภัยและเชื่อถือได้ ตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากล และสอดคล้องกับข้อบังคับ กฎ ระเบียบ กฎหมายด้านความมั่นคงปลอดภัยสารสนเทศ รวมถึงมีกรอบการบริหารจัดการการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศที่ดี จึงกำหนดวัตถุประสงค์และเป้าหมายหลัก 3 ประการในการบริหารจัดการด้านความมั่นคงปลอดภัย คือ

1.1 เพื่อปกป้องและดูแลความปลอดภัยของข้อมูลที่สำคัญของกลุ่มบริษัท เอ็ม บี เค พนักงานและลูกค้า

1.2 เพื่อเป็นมาตรฐานในการปฏิบัติงาน และสอดคล้องกับข้อบังคับ กฎ ระเบียบ กฎหมายด้านความมั่นคงปลอดภัยสารสนเทศที่ได้ประกาศไว้ในปัจจุบัน

1.3 เพื่อเพิ่มประสิทธิภาพการใช้งานระบบเทคโนโลยีสารสนเทศ โดยให้ปลอดภัยจากการถูกคุกคามต่างๆ ทั้งจากภายในและภายนอกองค์กร

## 2. คำนิยาม

ไม่มี

## 3. ขอบเขต

ระเบียบปฏิบัติฉบับนี้ใช้เป็นแนวทางสำหรับพนักงานของกลุ่มบริษัท เอ็ม บี เค

## 4. ระเบียบหรือแนวทางปฏิบัติ

4.1 นโยบายความปลอดภัยสำหรับระบบสารสนเทศ

4.1.1 การตรวจสอบและประเมินความเสี่ยง

กลุ่มบริษัท เอ็ม บี เค ต้องจัดให้มีกระบวนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยให้ครอบคลุมถึงการระบุความเสี่ยง การประเมินความเสี่ยง และการควบคุมความเสี่ยงให้อยู่ในเกณฑ์ที่องค์กรยอมรับได้ รวมถึงจัดให้มีผู้รับผิดชอบในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม

4.1.2 การบริหารจัดการทรัพยากรด้านเทคโนโลยีสารสนเทศ

กลุ่มบริษัท เอ็ม บี เค ต้องจัดให้มีกระบวนการในการบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศให้สอดคล้องกับแผนกลยุทธ์ขององค์กรที่เพียงพอต่อการดำเนินงานด้านเทคโนโลยีสารสนเทศ รวมถึงจัดให้มีการจัดการความเสี่ยงสำคัญในกรณีที่ไม่สามารถจัดสรรทรัพยากรได้เพียงพอต่อการดำเนินงานด้านเทคโนโลยีสารสนเทศ

4.1.3 การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ

กลุ่มบริษัท เอ็ม บี เค ต้องกำหนดให้มีการควบคุมเข้าถึงและการใช้งานระบบสารสนเทศขององค์กรให้เหมาะสมกับประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล และจัดให้มีการป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก รวมถึงจากโปรแกรมที่ไม่พึงประสงค์ที่จะสร้างความเสียหายให้แก่ข้อมูลขององค์กร

4.1.4 การจดโดเมนเนมเพื่อการดำเนินธุรกิจ

บริษัทในกลุ่มบริษัท เอ็ม บี เค ที่มีการใช้งานจดหมายอิเล็กทรอนิกส์ (E-Mail) ในการติดต่อประสานงานเรื่องที่เกี่ยวข้องกับการดำเนินธุรกิจของกลุ่มบริษัท เอ็ม บี เค ต้องดำเนินการ ดังนี้

4.1.4.1 จัดให้มีการจดโดเมน (Domain Name) สำหรับจดหมายอิเล็กทรอนิกส์ ในรูปแบบ .co.th หรือ .com ซึ่งมีการแสดงชื่อสื่อถึงบริษัทหรือธุรกิจของบริษัท

4.1.4.2 จัดให้มีการกำหนดผู้ดูแลโดเมน (Domain Name) ซึ่งมีหน้าที่คอยตรวจสอบความถูกต้อง ดูแลเรื่องความปลอดภัย (Security) การต่ออายุ รวมถึงดำเนินการเปลี่ยนแปลงข้อมูลและประสานงานกับหน่วยงานที่เกี่ยวข้องต่างๆ

4.1.4.3 จัดให้มีการเก็บรายละเอียดของข้อมูลต่างๆ ที่เกี่ยวกับการจดทะเบียนของโดเมน (Domain Name) ในรูปของเอกสาร และสามารถให้ผู้มีสิทธิ์ตรวจสอบข้อมูลสอบถามได้ตลอดเวลาเมื่อมีการร้องขอ

4.1.5 การจัดทำระบบสำรองและแผนรองรับกรณีเกิดเหตุฉุกเฉิน

กลุ่มบริษัท เอ็ม บี เค ต้องจัดให้มีระบบสำรองที่เหมาะสมและอยู่ในสภาพพร้อมใช้งาน โดยคัดเลือกระบบสารสนเทศที่สำคัญ รวมทั้งจัดทำแผนรองรับกรณีเกิดเหตุฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนรองรับกรณีเกิดเหตุฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ และให้มีการทดสอบแผนรองรับกรณีเกิดเหตุฉุกเฉิน รวมถึงปรับปรุงให้สอดคล้องกับการใช้งานอย่างสม่ำเสมอ

4.1.6 การจัดทำระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

กลุ่มบริษัท เอ็ม บี เค ต้องจัดให้มีระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่ได้ประกาศใช้งาน และดำเนินการประกาศระเบียบปฏิบัติดังกล่าวให้ผู้เกี่ยวข้องรับทราบ โดยระเบียบปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศต้องครอบคลุมเนื้อหาสำคัญอย่างน้อย ดังนี้

4.1.6.1 การจัดโครงสร้างความมั่นคงปลอดภัยของระบบสารสนเทศ (Organization of Information Security)

4.1.6.2 การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร (Human Resource Security)

4.1.6.3 การบริหารจัดการทรัพย์สินสารสนเทศ (Asset Management)

4.1.6.4 การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ (Access Control)

4.1.6.5 การเข้ารหัสข้อมูล (Cryptography)

4.1.6.6 การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม (Physical and Environmental Security)

4.1.6.7 การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ(Operations Security)

4.1.6.8 การรักษาความมั่นคงปลอดภัยด้านการสื่อสารผ่านระบบเครือข่ายคอมพิวเตอร์ (Communications Security)

4.1.6.9 การจัดหา การพัฒนา และการบำรุงรักษาระบบ (System Acquisition, Development and Maintenance)

4.1.6.10 การใช้บริการระบบสารสนเทศจากผู้ให้บริการภายนอก (Supplier Relationships)

4.1.6.11 การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Incident Management)

4.1.6.12 การบริหารความต่อเนื่องทางธุรกิจในด้านความมั่นคงปลอดภัยของระบบสารสนเทศ Information Security Aspects of Business Continuity Management)

4.1.6.13 การปฏิบัติตามกฎหมาย และระเบียบปฏิบัติ (Compliance)

4.1.6.14 กลุ่มบริษัท เอ็ม บี เค ต้องจัดให้มีการทบทวนนโยบายความปลอดภัยสำหรับระบบสารสนเทศ และระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ รวมถึงระเบียบอื่นๆ ที่เกี่ยวข้องให้เป็นปัจจุบัน อย่างน้อยปีละ 1 ครั้ง

4.1.7 การปรับปรุง และหรือการจัดทำเว็บไซต์ (Web Site), เว็บแอพพลิเคชั่น (Web Application) ขึ้นใหม่ให้มีเนื้อหาตาม พรบ.คุ้มครองข้อมูลส่วนบุคคล ดังนี้

4.1.7.1 มีระบบ Cookie Consent คือระบบการขอความยินยอมเพื่อจัดเก็บไฟล์คุ้กกี้ และข้อมูลต่างๆ จากผู้ใช้งานเว็บไซต์

4.1.7.2 มีนโยบายคุ้กกี้ (Cookie Policy) แสดงบนเว็บไซต์ เพื่อแสดงวัตถุประสงค์ของการใช้งานคุ้กกี้ (Cookie) บนเว็บไซต์นั้นๆ

4.1.7.3 มีนโยบายความเป็นส่วนตัว (Privacy Policy) แสดงบนเว็บไซต์ เพื่อแจ้งเจ้าของข้อมูลส่วนบุคคล ถึงรายละเอียด และวัตถุประสงค์ของการจัดเก็บ และประมวลผลข้อมูลส่วนบุคคล

4.1.7.4 มีประกาศความเป็นส่วนตัว (Privacy Notice) ตามมาตรา 23 แห่ง พรบ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยเป็นการแจ้งเจ้าของข้อมูลส่วนบุคคลทราบถึงเงื่อนไขเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด

5. **ข้อยกเว้นการปฏิบัติ**

   ไม่มี

6. **บทลงโทษ**

   อ้างถึงข้อบังคับเกี่ยวกับการทำงานของบริษัท