


นโยบายการบริหารจัดการทรัพย์สินสารสนเทศ

IT Asset Management Policy

รุ่นเอกสาร	1.1	เลขที่เอกสาร	ISMS-PL-11
สายงาน	บริหารความมั่นคงปลอดภัยระบบสารสนเทศ		
กลุ่ม	ดิจิทัลทรานส์ฟอร์มเมชัน		
ผู้รับผิดชอบ	นายณัฐชัย สมภักดี		
อนุมัติโดย			
นโยบายนี้ให้มีผลใช้บังคับ ตั้งแต่วันที่ 22 สิงหาคม 2566 เป็นต้นไป ตามมติที่ประชุมคณะกรรมการกำกับดูแลการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ ครั้งที่ 3 เมื่อวันที่ 22 สิงหาคม 2566			
ลงนามโดย			
			
คุณเคียน อิน ลิ้ม			
(President)			

ประวัติการแก้ไข

รุ่นเอกสาร	วันที่	รายละเอียด	ทบทวนโดย
1.0	10/08/2022	จัดทำเอกสาร	นายสุวัฒน์ชัย สันตินรงค์ดี
1.1	16/05/2023	ทบทวนเอกสาร	น.ส.เมกรินทร์ วุฒิชยา

นโยบายการบริหารจัดการทรัพย์สินสารสนเทศ

1. บทนำ

1.1 วัตถุประสงค์

เพื่อรักษาความมั่นคงปลอดภัยของทรัพย์สินสารสนเทศของบริษัทฯ

1.2 ขอบเขต

นโยบายนี้ครอบคลุมการบริหารจัดการทรัพย์สินสารสนเทศของทางบริษัทฯ

1.3 คำจำกัดความ

ทรัพย์สิน (Asset) หมายถึง สิ่งใดๆ ก็ตามทั้งที่มีตัวตน หรือไม่มีตัวตน อันมีมูลค่าหรือคุณค่าสำหรับบริษัท ไทยประกันชีวิต จำกัด (มหาชน) (“บริษัทฯ”) เช่น อุปกรณ์คอมพิวเตอร์ ข้อมูล ข้อมูลส่วนบุคคล ความมั่นคงปลอดภัยของทรัพย์สินสารสนเทศ หมายถึง การอ้างไว้ซึ่งการรักษาความลับ (Confidential) การรักษาความถูกต้องครบถ้วนสมบูรณ์ (Integrity) การรักษาสภาพพร้อมใช้งาน (Availability) ของทรัพย์สินสารสนเทศ รวมถึงต้องมีความรับผิดชอบ (Accountability) มีความน่าเชื่อถือ (Reliability)

2. นโยบาย

- 2.1 บริษัทฯ ต้องมีการบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ ต้องมีการจัดทำทะเบียนรายการทรัพย์สิน เพื่อให้สามารถระบุรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศได้อย่างครบถ้วน และสามารถนำไปใช้ในการกำหนดแนวทางการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศได้อย่างเหมาะสม และต้องมีการบำรุงรักษาทรัพย์สินด้านเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ เพื่อให้มีความพร้อมใช้งาน ความปลอดภัย และสามารถรองรับการดำเนินธุรกิจได้อย่างต่อเนื่อง
- 2.2 ต้องมีการประเมินความเสี่ยงทรัพย์สินด้านเทคโนโลยีสารสนเทศอย่างน้อยปีละ 1 ครั้ง หรือทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ
- 2.3 มีการกำหนดผู้รับผิดชอบทรัพย์สินด้านเทคโนโลยีสารสนเทศของแต่ละหน่วยงาน ระบุผู้รับผิดชอบหน่วยงานผู้รับผิดชอบ ประเภทของทรัพย์สิน ระบุปีที่ทรัพย์สินอยู่ในความดูแลให้เหมาะสม ตามกระบวนการหรือขั้นตอนบริหารจัดการทรัพย์สินที่บริษัทฯ กำหนด
- 2.4 การจัดหมวดหมู่ทรัพย์สินด้านเทคโนโลยีสารสนเทศต้องสอดคล้องและเป็นไปในทิศทางเดียวกันกับขั้นตอนการจัดชั้นความลับสารสนเทศของทางบริษัทฯ

3. การทบทวนและปรับปรุงนโยบาย

นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศทั้งหมด รวมถึงระเบียบและคำสั่งต่างๆ ที่เกี่ยวข้อง ต้องได้รับการทบทวนและประเมินผลเพื่อปรับปรุงเนื้อหา หรือยืนยันเนื้อหาเดิมโดยผู้บริหารอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าเนื้อหาของนโยบายยังคงไว้ซึ่งความครบถ้วนสมบูรณ์ มีประสิทธิภาพ และสามารถนำไปใช้งานได้อย่างเหมาะสม

4. บทลงโทษ

การละเมิด ฝ่าฝืน ละเลย หรือไม่ปฏิบัติตามนโยบาย ตลอดจนวิธีการปฏิบัติงาน และเอกสารสนับสนุนต่างๆ ที่เกี่ยวข้อง ไม่ว่าจะโดยเจตนาหรือไม่ก็ตาม ถือเป็นความผิดทางวินัย ซึ่งจะต้องพิจารณาลงโทษทางวินัยตามกฎหมายระเบียบของบริษัทฯ และหากการละเมิดหรือฝ่าฝืนนโยบายนั้นเข้าข่ายการกระทำที่ผิดกฎหมาย ผู้ละเมิดต้องได้รับการดำเนินคดีตามที่กฎหมายระบุไว้

End of Document