นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

(Information Security Policy)

บทนำ

บริษัท กรุงเทพประกันชีวิต จำกัด (มหาชน) " บริษัท " กำหนดให้มีนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ที่ครอบคลุมทั้งด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ และความมั่นคงปลอดภัยทางไซเบอร์ สอดคล้องกับการนำเทคโนโลยีสารสนเทศมาใช้ในการดำเนินธุรกิจ โดยรักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้งานของระบบและข้อมูลสารสนเทศของบริษัท

วัตถุประสงค์

เพื่อให้ระบบสารสนเทศของบริษัท มีการประเมินและจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ มีการควบคุมภายในที่ดี มีความมั่นคงปลอดภัย ถูกต้องและเชื่อถือได้ ตลอดจนข้อมูลและทรัพย์สินสารสนเทศของบริษัท ได้รับการดูแลรักษาอย่างเหมาะสม สอดคล้องตามข้อบังคับ กฎ ระเบียบ กฎหมายด้านความมั่นคงปลอดภัยสารสนเทศ มาตรฐานสากลที่เกี่ยวข้อง และประกาศคำสั่งของหน่วยงานกำกับธุรกิจ

ขอบเขต

บุคลากรของบริษัท กรุงเทพประกันชีวิต จำกัด (มหาชน) และบริษัทย่อย ต้องศึกษา ทำความเข้าใจนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศฉบับนี้ และถือปฏิบัติอย่างเคร่งครัด

คำนิยาม

"**ระบบสารสนเทศ**" (Information Technology) หมายถึง ระบบหรือกระบวนการประมวลผลข้อมูลโดยการใช้เทคโนโลยีคอมพิวเตอร์เข้ามาใช้จัดการข้อมูล (Data) อย่างเป็นระบบ เพื่อให้ได้สารสนเทศ (Information) ที่มีประสิทธิภาพ ในการสนับสนุนธุรกิจ

"**ความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ**" (Information Technology Security) หมายถึง การป้องกันด้านเทคโนโลยีสารสนเทศและทรัพย์สินสารสนเทศจากการเข้าถึง ใช้ เปิดเผย ขัดขวาง เปลี่ยนแปลง แก้ไข ทำให้สูญหาย ทำให้เสียหาย ถูกทำลาย หรือล่วงรู้โดยมิชอบ โดยการธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของเทคโนโลยีสารสนเทศและทรัพย์สินสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิดชอบ (Accountability) การห้ามปฏิเสธความรับผิดชอบ (Non-Repudiation) และความน่าเชื่อถือ (Reliability) รวมถึง การตอบสนองต่อภัยคุกคามและกู้คืนระบบสารสนเทศให้กลับมาเป็นปกติได้รวดเร็ว ไม่ทำให้ธุรกิจหยุดชะงัก (Resilience)

“**การรักษาความมั่นคงปลอดภัยทางไซเบอร์**” (Cyber Security) หมายถึง มาตรการหรือการดำเนินการที่กำหนดขึ้น เพื่อป้องกัน รับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอก อันกระทบต่อความมั่นคงของระบบเทคโนโลยีสารสนเทศ

“**ภัยคุกคามทางไซเบอร์**” (Cyber Threat) หมายถึง การกระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์ โดยมุ่งหมายให้เกิดการประทุษร้าย และส่งผลกระทบด้านการปฏิบัติงาน ต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

“**โปรแกรมไม่ประสงค์ดี**” (Malicious Software) หมายถึง โปรแกรมที่สร้างขึ้น เพื่อให้เกิดผลลัพธ์ที่ไม่พึงประสงค์กับผู้ใช้งานหรือระบบ โดยทำงานในลักษณะที่เป็นการโจมตีระบบ การทำให้ระบบเสียหาย รวมไปถึงการโจรกรรมข้อมูล

“**โปรแกรมป้องกันไวรัส**” (Antivirus Software) หมายถึง โปรแกรมที่สร้างขึ้น เพื่อคอยตรวจจับป้องกัน และกำจัดโปรแกรมไม่ประสงค์ดีหรือโปรแกรมคุกคามทางคอมพิวเตอร์ ซึ่งหมายถึง ไวรัส เวิร์ม โทรจัน สปายแวร์ แอดแวร์ และซอฟต์แวร์คุกคามประเภทอื่น ๆ

ข้อกำหนดด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ

นโยบายฉบับนี้มีข้อกำหนด ดังต่อไปนี้

1. จัดให้มีกรอบการปฏิบัติงานความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่เหมาะสมและรัดกุม ครอบคลุมถึงผู้ให้บริการภายนอกที่มีการใช้บริการ
2. จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ เพื่อธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) สภาพพร้อมใช้งาน (Availability) ของระบบสารสนเทศภายในบริษัท และความต่อเนื่องในการดำเนินธุรกิจ (Business Continuity)
3. จัดให้มีการบริหารจัดการทรัพย์สินสารสนเทศ มีการจำแนกประเภททรัพย์สินสารสนเทศและจัดระดับชั้นความลับ มีมาตรการป้องกันระบบและข้อมูลสารสนเทศของบริษัทจากการเข้าถึงโดยไม่ได้รับอนุญาต เพื่อไม่ให้เกิดข้อมูลรั่วไหล หรือการแสวงหาประโยชน์จากตำแหน่งหน้าที่โดยมิชอบ
4. จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม มีมาตรการควบคุมการใช้งานของผู้ใช้งานและผู้ดูแลระบบ มีมาตรการป้องกันและรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ รวมทั้งมีแนวทางในการกำกับดูแลความเสี่ยงและความมั่นคงปลอดภัยทางไซเบอร์

5. จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยด้านการสื่อสารข้อมูลสารสนเทศ มีมาตรการการเข้ารหัสข้อมูล เพื่อควบคุมการรับส่งหรือแลกเปลี่ยนข้อมูลสารสนเทศ รวมถึงมีแนวปฏิบัติที่ดีในการจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศ
6. จัดให้มีมาตรการป้องกันโปรแกรมไม่ประสงค์ดี ภัยคุกคามที่มีต่อระบบสารสนเทศ และภัยคุกคามทางไซเบอร์ รวมถึงมีการบริหารจัดการโปรแกรมป้องกันไวรัส การบริหารจัดการช่องโหว่ทางเทคนิค หรือการทดสอบความมั่นคงปลอดภัยของระบบสารสนเทศอย่างต่อเนื่อง หรืออย่างน้อยปีละ 1 ครั้ง
7. จัดให้มีการบริหารโครงการด้านเทคโนโลยีสารสนเทศที่มีประสิทธิภาพ มีการจัดทำแผนบริหารความต่อเนื่องในการดำเนินธุรกิจ และแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ เพื่อเตรียมความพร้อมและสามารถรับมือภัยหรือเหตุการณ์ต่าง ๆ ที่อาจส่งผลกระทบต่อการดำเนินธุรกิจ และการปฏิบัติงานด้านเทคโนโลยีสารสนเทศได้อย่างทันท่วงที
8. จัดให้มีการสื่อสารและนำไปปฏิบัติให้เกิดประสิทธิผลทั่วทั้งบริษัท ส่งเสริมและพัฒนาให้เกิดความตระหนักรู้ด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศให้กับบุคลากรอย่างสม่ำเสมอ

การทบทวนนโยบาย

บริษัททบทวนนโยบายอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีสาระสำคัญ

บริษัท กรุงเทพประกันชีวิต จำกัด (มหาชน) 1415 ถนนกรุงเทพ-นนทบุรี แขวงวงศ์สว่าง เขตบางซื่อ กรุงเทพฯ 10800
Bangkok Life Assurance Public Company Limited 1415 Krungthep - Nonthaburi Road, Wongsawang, Bang Sue, Bangkok 10800
Tel. 02-777-8888 Fax 02-777-8889 Call Center 02-777-8888 www.bangkoklife.com ISO 9001 Certified เลขประจำตัวผู้เสียภาษีอากร / ทะเบียนเลขที่ 0107550000238