

## กฎบัตรคณะกรรมการกำกับดูแลและบริหารจัดการงานด้านเทคโนโลยีสารสนเทศ

บริษัท กรุงเทพประกันชีวิต จำกัด (มหาชน)

### 1. วัตถุประสงค์

กฎบัตรคณะกรรมการกำกับดูแลและบริหารจัดการงานด้านเทคโนโลยีสารสนเทศ (IT Steering Committee) จัดทำขึ้นเพื่อเป็นกรอบการกำกับดูแล ส่งเสริม และบริหารจัดการงานด้านเทคโนโลยีและนวัตกรรมดิจิทัล เพื่อช่วยให้คณะกรรมการกำกับดูแลและบริหารจัดการงานด้านเทคโนโลยีสารสนเทศสามารถดำเนินงานต่าง ๆ ให้บรรลุและสำเร็จตามวัตถุประสงค์ และ/หรือ เป้าหมายที่กำหนดไว้ โดยให้การบริหารจัดการงานเป็นไปตามมาตรฐานด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ สอดคล้องกับนโยบายของบริษัท แนวทางมาตรฐานสากล ประกาศของหน่วยงานกำกับดูแลธุรกิจ ด้านการกำกับดูแลการบริหารโครงการเทคโนโลยีสารสนเทศ และเป็นไปตามที่กฎหมายกำหนด

### 2. องค์ประกอบ คุณสมบัติ การแต่งตั้ง และวาระการดำรงตำแหน่ง

- 2.1 คณะกรรมการบริษัทแต่งตั้งคณะกรรมการกำกับดูแลและบริหารจัดการงานด้านเทคโนโลยีสารสนเทศอย่างน้อย 3 ท่าน โดยแต่งตั้งจากกรรมการบริษัทและ/หรือผู้ทรงคุณวุฒิจากภายนอกที่มีความรู้ ความสามารถ มีประสบการณ์ และ/หรือเชี่ยวชาญเฉพาะด้าน โดยคณะกรรมการบริษัทแต่งตั้งกรรมการท่านหนึ่งทำหน้าที่ประธาน
- 2.2 คณะกรรมการบริษัทและ/หรือคณะกรรมการกำกับดูแลและบริหารจัดการงานด้านเทคโนโลยีสารสนเทศแต่งตั้งกรรมการและ/หรือผู้บริหาร จำนวน 1 ท่าน เพื่อทำหน้าที่เลขานุการคณะกรรมการ
- 2.3 กรรมการที่เป็นกรรมการบริษัทมีวาระการดำรงตำแหน่งให้เป็นไปตามระยะเวลาการดำรงตำแหน่งกรรมการบริษัท และกรรมการผู้ทรงคุณวุฒิจากภายนอกมีวาระการดำรงตำแหน่ง 3 ปี และเมื่อพ้นจากตำแหน่งแล้วอาจได้รับแต่งตั้งอีกได้
- 2.4 มีคุณสมบัติ ไม่มีลักษณะต้องห้ามตามพระราชบัญญัติประกันชีวิต พระราชบัญญัติมหาชน จำกัด และกฎหมายอื่นที่เกี่ยวข้อง รวมทั้งมีความรู้ ความสามารถ ความเข้าใจเกี่ยวกับธุรกิจ มีประสบการณ์ด้านเทคโนโลยีดิจิทัล และ/หรือมีประสบการณ์ในหลากหลายสาขาวิชาชีพที่เป็นประโยชน์ต่อการดำเนินงานของบริษัท สามารถกำหนดทิศทางและกำกับดูแลการใช้เทคโนโลยีดิจิทัลให้สอดคล้องกับกลยุทธ์ในการดำเนินธุรกิจ

### 3. อำนาจหน้าที่ และความรับผิดชอบ

- 3.1 กำกับดูแลและให้ความเห็นชอบทิศทาง กลยุทธ์ และแผนงานด้านเทคโนโลยีสารสนเทศและนวัตกรรมดิจิทัลของบริษัท เพื่อให้สอดคล้องและสนับสนุนกลยุทธ์การดำเนินธุรกิจของบริษัท และมีความยืดหยุ่นเพียงพอที่จะรองรับการเปลี่ยนแปลงของเทคโนโลยีและสภาพแวดล้อมทางธุรกิจ รวมทั้งกำกับดูแลให้การดำเนินงานด้านเทคโนโลยีสารสนเทศเป็นไปตามนโยบายของบริษัท กฎหมาย และหลักเกณฑ์ของหน่วยงานกำกับดูแลที่เกี่ยวข้อง
- 3.2 กำกับดูแลให้การจัดสรรและบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศ ซึ่งครอบคลุมถึงการจัดสรรทรัพยากรให้เพียงพอต่อการดำเนินธุรกิจ และมีแนวทางรองรับในกรณีที่ไม่สามารถจัดสรรทรัพยากรได้เพียงพอตามที่กำหนดไว้
- 3.3 กำกับดูแลให้มีการกำหนดนโยบายด้านการรักษาความมั่นคงปลอดภัย การบริหารความเสี่ยงที่เกี่ยวข้องกับภัยด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ โดยคณะกรรมการทำหน้าที่พิจารณากลับกรอนโยบายก่อนเสนอขออนุมัติต่อคณะกรรมการบริษัท รวมทั้งให้คณะกรรมการมีหน้าที่อนุมัติกรอบการปฏิบัติงานที่เกี่ยวข้อง และกำกับดูแลให้มีการนำไปปฏิบัติอย่างเหมาะสม ตลอดจนกำหนดให้มีการทบทวนนโยบาย กรอบการปฏิบัติงาน และมาตรฐานที่เกี่ยวข้องอย่างน้อยปีละหนึ่งครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ
- 3.4 กำกับดูแลให้มีการกำหนดกรอบการบริหารจัดการโครงการและโครงสร้างการกำกับดูแลโครงการ (Project Governance) เพื่อให้เกิดการบริหารจัดการโครงการด้านเทคโนโลยีสารสนเทศอย่างเหมาะสมตามกรอบการปฏิบัติงาน โดยให้มีการประเมินความเสี่ยงและผลกระทบของโครงการ การจัดลำดับความสำคัญของโครงการ และการพิจารณาอนุมัติโครงการที่สำคัญที่มีผลกระทบต่อการดำเนินงานตามแผนกลยุทธ์ หรือมีความเสี่ยงอย่างมีนัยสำคัญต่อการดำเนินธุรกิจในภาพรวม หรือโครงการที่มีการนำเทคโนโลยีมาใช้ครั้งแรกและมีความเสี่ยงต่อการดำเนินธุรกิจของบริษัท ทั้งนี้เพื่อให้โครงการสามารถดำเนินการได้ตามแผนที่กำหนด และสอดคล้องกับกลยุทธ์การดำเนินธุรกิจของบริษัท
- 3.5 กำกับดูแลให้มีการกำหนดนโยบายและกรอบการปฏิบัติงาน การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และกำกับดูแลให้มีกระบวนการ การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่มีประสิทธิภาพและเป็นไปตามมาตรฐานสากลด้านระบบการจัดการความมั่นคงปลอดภัยของข้อมูล (ISO/IEC 27001 : Information Security Management System - ISMS)

- 3.6 รับทราบสรุปภาพรวมการดำเนินการที่เกี่ยวข้องด้านการบริหารความเสี่ยงเทคโนโลยีสารสนเทศ ความเสี่ยงภัยไซเบอร์ ซึ่งอาจก่อให้เกิดผลกระทบต่อแผนงานด้านเทคโนโลยีสารสนเทศและนวัตกรรมดิจิทัลของบริษัท เพื่อให้รู้เท่าทันต่อความเสี่ยงและบริหารจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้
- 3.7 คณะกรรมการ รับทราบประเด็นสำคัญ ให้คำแนะนำหรือความเห็นต่อการดำเนินการในเรื่องดังนี้
- ผลการตรวจสอบด้านเทคโนโลยีสารสนเทศที่อาจมีผลกระทบต่อการบริหารจัดการเทคโนโลยีสารสนเทศของบริษัท และการดำเนินการแก้ไขประเด็นเพื่อปิดประเด็นผลตรวจ
  - การรายงานเหตุการณ์ด้านเทคโนโลยีสารสนเทศและภัยคุกคามทางไซเบอร์ที่เกิดขึ้นต่อบริษัทอย่างมีนัยสำคัญ การแก้ไขปัญหาเหตุการณ์ที่เกิดผลกระทบ และการรายงานต่อหน่วยงานกำกับธุรกิจ หรือหน่วยงานตามที่กฎหมายกำหนด ตามระยะเวลาและหลักเกณฑ์ที่หน่วยงานนั้นกำหนด
- 3.8 ส่งเสริมและสนับสนุนการบริหารจัดการบุคลากรด้านเทคโนโลยีสารสนเทศให้มีเครื่องมือที่เหมาะสมในการปฏิบัติงาน มีความรู้ทันต่อเทคโนโลยีที่เปลี่ยนแปลงไปอย่างรวดเร็ว และทันต่อภัยคุกคามทางไซเบอร์ใหม่ๆ ที่อาจเกิดขึ้น เพื่อสนับสนุนต่อความสำเร็จในการใช้เทคโนโลยีสารสนเทศและนวัตกรรมดิจิทัลของบริษัท รวมถึงส่งเสริมการเรียนรู้การใช้เทคโนโลยีสารสนเทศและนวัตกรรมดิจิทัลเพื่อการดำเนินธุรกิจให้กับผู้บริหารและพนักงานในบริษัท เพื่อนำไปประยุกต์ใช้ในการปฏิบัติงานได้อย่างมีประสิทธิภาพ
- 3.9 คณะกรรมการกำกับดูแลและบริหารงานด้านเทคโนโลยีสารสนเทศมีอำนาจในการแต่งตั้งอนุกรรมการ และ/หรือคณะทำงาน และ/หรือบุคคลใด ๆ เพื่อให้ดำเนินงานอันเป็นประโยชน์ต่อการปฏิบัติหน้าที่และอยู่ภายในขอบเขตแห่งอำนาจหน้าที่ของคณะกรรมการกำกับดูแลและบริหารงานด้านเทคโนโลยีสารสนเทศ
- 3.10 กำหนดให้มีการประชุมกรรมการอย่างน้อยปีละ 4 ครั้ง และให้รายงานผลการดำเนินงานด้านเทคโนโลยีสารสนเทศและนวัตกรรมดิจิทัลต่อคณะกรรมการบริษัทอย่างน้อยปีละหนึ่งครั้ง หรือเมื่อเกิดเหตุการณ์ที่ส่งผลกระทบต่ออย่างมีนัยสำคัญ

#### 4. การประชุม

ในการประชุมคณะกรรมการกำกับดูแลและบริหารจัดการงานด้านเทคโนโลยีสารสนเทศต้องมีกรรมการมาประชุมจำนวนไม่น้อยกว่า 3 ใน 4 ของจำนวนกรรมการที่ได้รับการแต่งตั้ง จึงจะถือว่าครบองค์

ประชุม โดยในการออกเสียงในการประชุมให้ถือว่าคณะกรรมการ 1 ท่านมี 1 เสียง และในการลงคะแนนเสียง หากปรากฏว่ามีคะแนนเสียงเท่ากันก็ให้ประธานในที่ประชุมออกเสียงเพิ่มขึ้นอีก 1 เสียงเป็นเสียงชี้ขาด

5. การประเมินผลของคณะกรรมการ

คณะกรรมการกำกับดูแลและบริหารจัดการงานด้านเทคโนโลยีสารสนเทศต้องมีการประเมินผลการปฏิบัติงานในปีที่ผ่านมาโดยกรรมการทุกท่านที่ดำรงตำแหน่งในขณะนี้ เพื่อทบทวนผลการปฏิบัติงาน ปัญหา และอุปสรรค ตลอดจนนำข้อเสนอแนะมาปรับปรุงและพัฒนาการปฏิบัติงานต่อไป

กฎบัตรคณะกรรมการกำกับดูแลและบริหารจัดการงานด้านเทคโนโลยีสารสนเทศ ฉบับนี้ได้รับการอนุมัติจากที่ประชุมคณะกรรมการบริษัท ครั้งที่ 5/2569 เมื่อวันที่ 13 พฤษภาคม 2569



(ดร.ศิริ การเจริญดี)

ประธานกรรมการ