



## นโยบายบริษัทฯ ปี 2566 Company Policy 2023

1. นโยบายต่อต้านทุจริตและคอร์รัปชัน .....	1
2. นโยบายการบริหารความเสี่ยงองค์กร .....	6
3. นโยบายการพัฒนาผลิตภัณฑ์ประกันภัยและการกำหนดเบี้ยประกันภัย .....	10
4. นโยบายการเสนอขาย และการเก็บเบี้ยประกันภัย .....	11
5. นโยบายการพิจารณารับประกันภัย .....	12
6. นโยบายการประเมินสำรองประกันภัย .....	13
7. นโยบายการจัดการสินไหมทดแทน .....	14
8. นโยบายการประกันภัยต่อ .....	15
9. นโยบายการลงทุน.....	16
10. นโยบายการบริหารสินทรัพย์และหนี้สิน.....	17
11. นโยบายการจัดจ้างบุคคลภายนอก.....	18
12. นโยบายการบริหารความต่อเนื่องทางธุรกิจ .....	19
13. นโยบายการป้องกันและปราบปรามการฟอกเงิน การสนับสนุนทางการเงินแก่การก่อการร้าย และการแพร่ขยายอาวุธที่มีอานุภาพทำลายล้างสูง.....	20
14. นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ.....	22
15. นโยบายการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ .....	27
16. นโยบายคุ้มครองข้อมูลส่วนบุคคล.....	30
16.1 นโยบายคุ้มครองข้อมูลส่วนบุคคล [ลูกค้าและผู้มุ่งหวัง].....	30
16.2 นโยบายคุ้มครองข้อมูลส่วนบุคคล [คู่ค้า ตัวแทน และนายหน้า].....	35
16.3 นโยบายคุ้มครองข้อมูลส่วนบุคคล [พนักงาน] .....	38
17. นโยบายการบริหารงานคุณภาพและความมั่นคงปลอดภัยสารสนเทศ .....	42
18. นโยบายการควบคุมภายใน .....	43
19. นโยบายการกำกับดูแลข้อมูล .....	45

ประกาศ ณ วันที่ 15 พฤศจิกายน 2565

[ นายชาติชาย ชินเวชกิจวานิชย์ ]  
กรรมการผู้จัดการ

บริษัท เทเวศประกันภัย จำกัด [มหาชน]  
97 และ 99 อาคารเทเวศประกันภัย ถนนราชดำเนินกลาง แขวงบวรนิเวศ  
เขตพระนคร กรุงเทพมหานคร 10200 โทรศัพท์ 0 2080 1599  
เว็บไซต์ <http://www.deves.co.th> อีเมล [dvsins@deves.co.th](mailto:dvsins@deves.co.th)

รวบรวมโดย ... สำนักบริหารความเสี่ยงและสถิติประกันภัย

นโยบายบริษัทฯ ได้รับการพิจารณาและอนุมัติจากการประชุมคณะกรรมการบริษัทฯ เมื่อวันที่ 4 พฤศจิกายน 2565

# 1. นโยบายต่อต้านทุจริตและคอร์รัปชัน

## 1. หลักการและเหตุผล

บริษัท เทเวศรประกันภัย จำกัด [มหาชน] มีอุดมการณ์ดำเนินธุรกิจอย่างมีคุณธรรม และตระหนักถึงการทุจริตและคอร์รัปชัน ซึ่งส่งผลกระทบต่อความสูญเสียต่อระบบเศรษฐกิจและความเสียหายทางสังคม ซึ่งเป็นการกระทำที่ไม่ถูกต้อง ส่งผลกระทบต่อชื่อเสียงด้านจริยธรรมธุรกิจ ความสามารถในการแข่งขัน ทำให้บริษัทฯ ไม่เป็นที่ยอมรับ ตลอดจนลดความเชื่อมั่นของผู้ถือหุ้น ผู้ลงทุน และผู้มีส่วนได้ส่วนเสีย ดังนั้นที่ประชุมคณะกรรมการบริษัทฯ จึงมีมติเข้าเป็น "แนวร่วมต่อต้านคอร์รัปชันของภาคเอกชนไทย" เมื่อวันที่ 10 สิงหาคม 2560 เพื่อแสดงเจตนารมณ์และความมุ่งมั่นในการต่อต้านทุจริตและคอร์รัปชันทุกรูปแบบ ทั้งนี้บริษัทฯ ให้ความสำคัญในการดำเนินธุรกิจตามแนวทางกำกับดูแลกิจการที่ดี [Good Governance] ยึดหลักการดำเนินงานที่เป็นธรรมและถูกต้อง บริหารงานด้วยความซื่อสัตย์สุจริต โปร่งใส ไม่สนับสนุนกิจการ กลุ่มบุคคล หรือบุคคลที่มีส่วนร่วมในการแสวงหาผลประโยชน์ที่ไม่ถูกต้อง ไม่ว่าจะทางตรงหรือทางอ้อม จากการใช้อำนาจหน้าที่โดยมิชอบ ดังนั้นบริษัทฯ จึงได้กำหนดนโยบายเพื่อใช้เป็นแนวทางดำเนินงาน และถือเป็นหลักในการปฏิบัติสำหรับกรรมการ ผู้บริหาร และพนักงานทุกคน ที่ต้องดำเนินการตามคำมั่นและนโยบายที่กำหนดอย่างเคร่งครัด และพัฒนาสู่องค์กรแห่งความยั่งยืนอย่างมีคุณธรรม

นโยบายฉบับนี้บังคับใช้กับคณะกรรมการบริษัทฯ คณะอนุกรรมการทุกคณะ รวมถึงผู้บริหาร พนักงาน และลูกจ้างของบริษัทฯ [รวมเรียกว่า "พนักงาน"] และบริษัทฯ คาดหวังให้คู่ค้าทางธุรกิจที่มีความเกี่ยวข้องหรือกระทำการในนามบริษัทฯ เช่น ตัวแทน นายหน้า คู่ บริษัทสำรวจภัย ฯลฯ ปฏิบัติตามนโยบายฉบับนี้

## 2. คำนิยาม

"คอร์รัปชัน" หมายถึง การติดสินบนไม่ว่าจะอยู่ในรูปแบบใด โดยการเสนอให้ สัญญาว่าจะให้ มอบให้ ให้คำมั่นว่าจะให้ เรียกรับ หรือรับ เงิน ทรัพย์สิน หรือประโยชน์อื่นใด ที่ไม่เหมาะสมกับเจ้าหน้าที่รัฐ หน่วยงานรัฐและเอกชน หรือผู้มีหน้าที่ไม่ว่าทางตรงหรือทางอ้อม เพื่อให้บุคคลดังกล่าวปฏิบัติหรือละเว้นปฏิบัติ อันเป็นการให้ได้มาหรือรักษาไว้ซึ่งธุรกิจ หรือแนะนำธุรกิจให้กับบริษัทฯ หรือเพื่อให้ได้มาซึ่งงานด้านธุรกิจ ความได้เปรียบการแข่งขัน หรือเพื่อรักษาไว้ซึ่งผลประโยชน์อื่นใดที่ไม่เหมาะสมทางธุรกิจ เว้นแต่เป็นกรณีที่กฎหมาย ระเบียบ ประกาศ ข้อบังคับ ขนบธรรมเนียมประเพณีของท้องถิ่นหรือจารีตทางการค้าให้กระทำได้

"การฉ้อฉลประกันภัย" หมายถึง การกระทำหรือการละเว้นการกระทำโดยทุจริต หลอกลวง เพื่อให้ได้รับประโยชน์ที่มีขอบด้วยกฎหมาย ไม่ว่าจะผู้ได้รับประโยชน์จากการฉ้อฉลจะเป็นบุคคลที่กระทำการฉ้อฉลเองหรือบุคคลอื่นที่เกี่ยวข้องก็ตาม

"การฉ้อฉลภายใน" หมายถึง การฉ้อฉลต่อบริษัท ผู้เอาประกันภัย ผู้รับประโยชน์ ผู้มีสิทธิเรียกร้องตามสัญญาประกันภัย หรือผู้เสียหาย โดยกรรมการ ผู้บริหาร พนักงาน หรือลูกจ้าง ไม่ว่าจะโดยลำพังหรือร่วมกับบุคคลอื่นทั้งจากภายในและภายนอกองค์กร

"การฉ้อฉลภายนอก" หมายถึง การฉ้อฉลต่อบริษัท ผู้เอาประกันภัย ผู้รับประโยชน์ ผู้มีสิทธิเรียกร้องตามสัญญาประกันภัย หรือผู้เสียหาย โดยผู้เอาประกันภัย ผู้รับประโยชน์ ผู้มีสิทธิเรียกร้องตามสัญญาประกันภัย ตัวแทนประกันวินาศภัย นายหน้าประกันวินาศภัย บุคคลที่บริษัทมอบหมาย หรือบุคคลอื่นซึ่งมิใช่กรรมการ ผู้บริหาร พนักงาน หรือลูกจ้างของบริษัท

## 3. นโยบายต่อต้านทุจริตและคอร์รัปชัน

กำหนดให้ กรรมการ ผู้บริหาร และพนักงานของบริษัทฯ ต้องไม่เรียกรับ ไม่ยินยอม ไม่จ่าย ไม่มีส่วนเกี่ยวข้อง ต่อต้านผู้เกี่ยวข้อง และไม่ยอมรับการทุจริตและคอร์รัปชันในทุกรูปแบบทั้งทางตรงและทางอ้อม เพื่อประโยชน์ต่อบริษัทฯ ตนเอง ครอบครัว เพื่อน หรือคนรู้จัก หรือเพื่อประโยชน์ทางธุรกิจ และจะไม่ลดตำแหน่ง ลงโทษ หรือให้ผลทางลบต่อพนักงานที่ปฏิเสธการทุจริตและคอร์รัปชัน แม้ว่าการกระทำนั้นจะส่งผลให้บริษัทฯ สูญเสียโอกาสทางธุรกิจก็ตาม ทั้งนี้นโยบายครอบคลุมถึงทุกหน่วยงาน คู่ค้า ลูกค้า และผู้มีส่วนได้ส่วนเสียของบริษัทฯ

กำหนดให้มีการทบทวนนโยบายและประเมินความเสี่ยงต่อการเกิดทุจริตและคอร์รัปชันเป็นประจำทุกปี มีการสอบทานการปฏิบัติตามนโยบายอย่างสม่ำเสมอ ตลอดจนทบทวนแนวทางการปฏิบัติ และข้อกำหนดในการดำเนินการ เพื่อให้สอดคล้องกับการเปลี่ยนแปลงของธุรกิจ ระเบียบ ข้อบังคับ และข้อกำหนดของกฎหมาย ทั้งนี้หากมีการฝ่าฝืนหรือกระทำการใด ๆ อันเป็นการสนับสนุน ช่วยเหลือ หรือให้ความร่วมมือกับการทุจริตและคอร์รัปชัน จะต้องได้รับการพิจารณาโทษตามระเบียบของบริษัทฯ รวมถึงการเลิกจ้าง กรณีที่จำเป็น

## 4. หน้าที่ความรับผิดชอบ

### 4.1 คณะกรรมการบริษัท

4.1.1 พิจารณานโยบายด้านนโยบาย ติดตาม ทบทวน และกำกับดูแลให้มีระบบสนับสนุนต่อต้านทุจริตและคอร์รัปชันที่มีประสิทธิภาพ เพื่อให้มั่นใจว่า ฝ่ายบริหารได้ตระหนักและให้ความสำคัญและปลูกฝังเป็นวัฒนธรรมองค์กร

4.1.2 ปฏิบัติตามมาตรการต่อต้านทุจริตและคอร์รัปชัน รวมถึงให้คำปรึกษา ข้อเสนอ พิจารณาบทลงโทษ และร่วมกันหาวิธีแก้ไขปัญหามา เมื่อได้รับรายงานทุจริตและคอร์รัปชันจากคณะกรรมการตรวจสอบ

### 4.2 คณะกรรมการตรวจสอบ

4.2.1 กำกับดูแลการปฏิบัติ การควบคุมภายใน การจัดทำรายงานทางการเงิน และกระบวนการอื่นที่เกี่ยวข้องกับมาตรการต่อต้านทุจริตและคอร์รัปชัน รวมถึงนำเสนอรายงานความเพียงพอและประสิทธิภาพของมาตรการเสนอต่อคณะกรรมการบริษัท

4.2.2 นำนโยบาย รวมถึงการทบทวนนโยบายประจำปีหรือทบทวนเมื่อมีนัยสำคัญ ที่ได้รับจากฝ่ายจัดการ เสนอต่อคณะกรรมการบริษัท พิจารณานโยบาย

4.2.3 สอบทานรายงานการตรวจสอบระบบควบคุมภายใน และการประเมินความเสี่ยงการทุจริตและคอร์รัปชัน รวมถึงสถิติตามที่สำนักตรวจสอบนำเสนอ เพื่อให้มั่นใจว่าระบบดังกล่าวเป็นไปตามนโยบายที่กำหนดขึ้น หรือมีความเสี่ยงที่จะทำให้เกิดโอกาสทุจริตและคอร์รัปชัน ที่มีผลกระทบต่อฐานะการเงินและผลการดำเนินงานของบริษัทฯ และนำเสนอต่อคณะกรรมการบริษัท

4.2.4 รับเรื่องการแจ้งเบาะแสการกระทำทุจริตและคอร์รัปชันที่คนในองค์กรเกี่ยวข้อง โดยตรวจสอบข้อเท็จจริงที่ได้รับ และเสนอคณะกรรมการบริษัทฯ ร่วมกันพิจารณาลงโทษหรือแก้ไขปัญหามา

### 4.3 คณะกรรมการบริหารความเสี่ยง

4.3.1 กำกับและสนับสนุนให้มีการดำเนินงานด้านการบริหารความเสี่ยงด้านทุจริตและคอร์รัปชัน

4.3.2 ประเมินความเสี่ยงที่อาจเกิดการทุจริตและคอร์รัปชัน รวมทั้งบริหารจัดการและวางนโยบายบริหารความเสี่ยงที่เหมาะสมต่อการป้องกันการเกิดทุจริตและคอร์รัปชัน

### 4.4 ฝ่ายจัดการหรือผู้บริหารระดับสูง

4.4.1 กำหนด/ทบทวนนโยบายเพื่อให้ทันต่อการเปลี่ยนแปลงของธุรกิจ หรือเมื่อมีนัยสำคัญ หรือตามข้อกำหนดของกฎหมายเพื่อเสนอต่อคณะกรรมการตรวจสอบ

4.4.2 ดำเนินการตามนโยบายและมาตรการต่อต้านทุจริตและคอร์รัปชัน รวมถึงสื่อสารไปยังพนักงานและผู้เกี่ยวข้อง

4.4.3 ให้ความช่วยเหลือคณะกรรมการตรวจสอบ ในการรายงานและตรวจสอบข้อเท็จจริงตามที่ได้รับแจ้งหรือได้รับมอบหมายเกี่ยวกับการสอบสวนการทุจริตและคอร์รัปชัน โดยสามารถมอบหมายให้ทีมผู้บริหารที่เห็นว่าสามารถช่วยสืบหาข้อเท็จจริงได้

### 4.5 ผู้อำนวยการสำนักตรวจสอบ

4.5.1 ตรวจสอบและสอบทานการปฏิบัติงานของหน่วยงานต่าง ๆ เช่น งานขาย งานการตลาด งานจ่ายค่าสินไหมทดแทน งานจัดซื้อ งานทำสัญญา ฯลฯ ให้เป็นไปอย่างถูกต้อง ตรงตามนโยบาย ระเบียบปฏิบัติ อำนาจดำเนินการ ข้อกำหนด รวมถึงข้อกำหนดสำนักงาน คปภ. และ ปปง. เพื่อมั่นใจว่า มีระบบควบคุมภายในที่ดี มีความเหมาะสม และเพียงพอต่อความเสี่ยงด้านการทุจริตและคอร์รัปชันที่อาจเกิดขึ้น

4.5.2 ติดตาม ทบทวน และประเมินผล มาตรการทุจริตและคอร์รัปชัน รวมถึงเสนอรายงานผลการตรวจสอบระบบควบคุมภายใน และการประเมินความเสี่ยงที่เกี่ยวข้องกับการทุจริตและคอร์รัปชันให้ผู้บริหารระดับสูงและคณะกรรมการตรวจสอบทราบเพื่อพิจารณาและปรับปรุง

4.5.3 ปฏิบัติตามที่คณะกรรมการตรวจสอบมอบหมาย ในเรื่องการตรวจสอบการทุจริตและคอร์รัปชัน

4.5.4 รับแจ้งเบาะแสและให้คำแนะนำเกี่ยวกับการทุจริตและคอร์รัปชัน รวมถึงจัดเก็บสถิติ เช่น จำนวนเบาะแสที่ได้รับ/ถูกตรวจสอบ ประเภทเบาะแส และรายงานคณะกรรมการตรวจสอบ

### 4.6 ผู้บริหาร

4.6.1 กำกับดูแลและจัดสรรทรัพยากรให้เพียงพอต่อการดำเนินการเกี่ยวกับการทุจริตและคอร์รัปชัน

4.6.2 กำหนดให้มีระบบ มีการส่งเสริม สนับสนุน ควบคุมดูแล และสื่อสารไปยังพนักงานและผู้เกี่ยวข้อง เพื่อให้มั่นใจว่ามีการปฏิบัติตามนโยบายที่กำหนดขึ้น

### 4.7 พนักงาน

4.7.1 นำนโยบายไปปฏิบัติ พร้อมทั้งสอดส่องดูแลและรายงานการพบเห็น หรือการกระทำใดที่สงสัย อาจมีการฝ่าฝืนนโยบายตามช่องทางกรรับแจ้งเบาะแสหรือร้องเรียนตามที่บริษัทฯ กำหนด

## 5. มาตรการและแนวทางการปฏิบัติ

5.1 กรรมการและผู้บริหาร ต้องแสดงความมุ่งมั่น และเป็นแบบอย่างที่ดีในการปฏิบัติตามนโยบาย รวมถึงการตระหนักถึงความสำคัญในการสร้างความเข้าใจและส่งเสริมให้พนักงานยึดถือปฏิบัติอย่างจริงจัง ต่อเนื่อง และเสริมสร้างให้เป็นส่วนหนึ่งของวัฒนธรรมองค์กร

5.2 กรรมการ ผู้บริหาร และพนักงานของบริษัทฯ ต้องปฏิบัติตามนโยบายอย่างเคร่งครัด ไม่เข้าไปเกี่ยวข้องกับไม่เรียกร่อง ไม่รับเงิน ผลประโยชน์ สิ่งของ หรือประโยชน์อื่นใดจากบุคคลหรือนิติบุคคลที่ร่วมทำธุรกิจ ไม่ว่าจะเป็นการเรียกร่อง หรือรับเพื่อตนเองหรือผู้อื่น ที่ส่อไปในทางจงใจให้ปฏิบัติหรือละเว้นปฏิบัติ หรือกระทำผิดกฎหมาย ไม่ว่าจะทางตรงหรือทางอ้อม กรณีพบการกระทำผิดจะต้องได้รับการลงโทษ

5.3 กรรมการ ผู้บริหาร และพนักงานของบริษัทฯ ไม่พึงละเลยหรือเพิกเฉยเมื่อพบเห็นการกระทำหรือพฤติกรรมที่เข้าข่ายทุจริตและคอร์รัปชัน หรือส่อไปในทางทุจริตและคอร์รัปชัน ที่เกี่ยวข้องกับบริษัทฯ ทั้งทางตรงหรือทางอ้อม ผู้พบเห็นต้องแจ้งผู้บังคับบัญชาหรือบุคคลที่รับผิดชอบทราบ และให้ความร่วมมือในการตรวจสอบ หากมีข้อสงสัยหรือซักถาม ให้ปรึกษาผู้บังคับบัญชาหรือบุคคลที่กำหนดให้ทำหน้าที่รับผิดชอบ ผ่านช่องทางที่กำหนด

5.4 บริษัทฯ จะให้ความสำคัญและคุ้มครองพนักงานที่ปฏิเสธหรือแจ้งทุจริตและคอร์รัปชันที่เกี่ยวกับบริษัทฯ โดยใช้มาตรการคุ้มครองผู้ร้องเรียนหรือผู้ความร่วมมือในการแจ้งและรายงาน โดยจะไม่ลดตำแหน่ง ลงโทษ หรือให้ผลทางลบต่อพนักงานที่ปฏิเสธการทุจริตและคอร์รัปชัน แม้การกระทำนั้นจะทำให้สูญเสียโอกาสทางธุรกิจ

5.5 ผู้ที่กระทำการทุจริตและคอร์รัปชัน ถือเป็นกระทำความผิดจรรยาบรรณบริษัทฯ ซึ่งต้องได้รับโทษทางวินัย และอาจได้รับโทษตามกฎหมาย หากการกระทำนั้นเข้าเงื่อนไขการกระทำความผิดทั้งทางอาญาและทางแพ่ง

5.6 บริษัทฯ มุ่งมั่นที่จะสร้างและรักษาวัฒนธรรมองค์กรที่ยึดมั่นว่า การทุจริตและคอร์รัปชัน การให้หรือการรับสินบน เป็นการกระทำที่ยอมรับไม่ได้ ไม่ว่าจะเป็นการกระทำกับบุคคลใดก็ตาม รวมถึงการกระทำธุรกรรมกับภาครัฐและเอกชน ต้องเป็นไปอย่างโปร่งใส ซื่อสัตย์ และต้องดำเนินการให้เป็นไปตามกฎหมายที่เกี่ยวข้อง

5.7 ค่าของขวัญ ค่าเลี้ยงรับรอง [Gift and Hospitality] ที่เกี่ยวข้องกับธุรกิจ สามารถกระทำได้ตามโอกาส ธรรมเนียม ประเพณี หรือตามมารยาทสังคมที่ปฏิบัติโดยทั่วไป ซึ่งต้องดำเนินการด้วยความโปร่งใส การรับหรือการให้ต้องมีมูลค่าที่เหมาะสม ไม่ส่งผลกระทบต่อการตัดสินใจ หรือละเว้นปฏิบัติหน้าที่ และตรวจสอบได้

5.8 การให้ความสนับสนุน [Sponsorship] ตามหลักเกณฑ์ของบริษัทฯ ต้องใช้เงินหรือทรัพย์สินเพื่อสนับสนุนโครงการโดยระบุชื่อในนามบริษัทฯ เท่านั้น เงินสนับสนุนที่จ่ายต้องมีวัตถุประสงค์เพื่อธุรกิจ ภาพลักษณ์ที่ดี และชื่อเสียงของบริษัทฯ โดยมีกระบวนการพิจารณาที่โปร่งใส ปราศจากความขัดแย้งทางผลประโยชน์ การเบิกจ่ายต้องระบุวัตถุประสงค์ที่ชัดเจน มีหลักฐานที่เชื่อถือและตรวจสอบได้ และดำเนินการตามขั้นตอนการขออนุมัติที่สามารถสอบทาน ควบคุม อนุมัติโดยผู้มีอำนาจ รวมถึงการประเมินผลและตรวจสอบได้

5.9 การบริจาค [Donations] บริษัทฯ สนับสนุนการมีส่วนร่วมกับชุมชนและพัฒนาคุณภาพชีวิตของประชาชน เพื่อให้สังคมมีความน่าอยู่และมีสิ่งแวดล้อมที่ดี ดังนั้นบริษัทฯ จะใช้เงินหรือให้ความช่วยเหลือในรูปแบบอื่น ๆ เพื่อเป็นการตอบแทนสังคม โดยมีได้มุ่งหวังผลทางธุรกิจแต่อย่างใด

5.10 การสนับสนุนทางการเมือง [Political Contributions] บริษัทฯ ดำเนินธุรกิจโดยยึดมั่นความเป็นกลางทางการเมือง โดยไม่เข้าไปมีส่วนร่วมหรือฝักใฝ่พรรคการเมืองใด หรือผู้มีอำนาจทางการเมืองคนใด ไม่นำเงินทุนหรือทรัพยากรของบริษัทฯ ไปใช้ช่วยเหลือหรือสนับสนุนไม่ว่าทางตรงหรือทางอ้อมแก่พรรคการเมืองหรือนักการเมืองใด

5.11 การขัดแย้งทางผลประโยชน์ [Conflict of Interest] ห้ามมิให้กรรมการ ผู้บริหาร และพนักงานของบริษัทฯ ประกอบธุรกิจแข่งกับบริษัทฯ หลีกเลี่ยงการดำเนินการที่เกี่ยวข้องกับตนเองที่อาจก่อให้เกิดการขัดแย้งทางผลประโยชน์กับบริษัทฯ ไม่ว่าจะโดยทางตรงหรือทางอ้อม กรณีมีความจำเป็น ต้องแจ้งให้บริษัทฯ ทราบ เพื่อดูแลให้มีความโปร่งใสและยุติธรรม

5.12 การจ่ายค่าอำนวยความสะดวก [Facilitation Payment] บริษัทฯ มีนโยบายไม่จ่ายและรับค่าอำนวยความสะดวกหรือเงินให้สินบนทุกกรณี ที่อาจนำไปสู่การทุจริตและคอร์รัปชัน

5.13 การจ้างพนักงานรัฐ [Revolving Door] บริษัทฯ มีนโยบายไม่มีการจ้างเจ้าหน้าที่รัฐเพื่อแสวงหาผลประโยชน์ใด ๆ จากข้อมูลหรือสายสัมพันธ์ของเจ้าหน้าที่รัฐในการสร้างความได้เปรียบการแข่งขัน

5.14 การจัดซื้อ จัดจ้าง ต้องดำเนินการตามขั้นตอนและระเบียบอย่างเคร่งครัด มีความโปร่งใส ตรวจสอบได้ และเป็นไปตามอำนาจดำเนินการ รวมถึงกำหนดให้มีการระบุข้อกำหนดเกี่ยวกับการต่อต้านทุจริตและคอร์รัปชันในเงื่อนไขสัญญาหรือข้อตกลงการจัดซื้อ จัดจ้าง

5.15 บริษัทฯ ตระหนักถึงความสำคัญในการเผยแพร่ ให้ความรู้ และทำความเข้าใจกับบุคคลอื่นที่ต้องปฏิบัติหน้าที่ที่เกี่ยวข้องกับบริษัทฯ โดยกำหนดให้มีการประชาสัมพันธ์นโยบายแก่กรรมการ ผู้บริหาร พนักงาน ลูกค้า และประชาชนผ่านสื่อต่าง ๆ เช่น เว็บไซต์ อีเมล รายงานประจำปี สื่อสังคมออนไลน์ ฯลฯ รวมถึงคู่มือและตัวแทนทางธุรกิจ เพื่อยึดถือและน่านโยบายไปปฏิบัติ โดยนโยบายดังกล่าวเป็นการปฏิบัติภายใต้กฎหมายประเทศไทย และเพื่อแสดงให้เห็นถึงเจตนารมณ์อันแน่วแน่ในการดำเนินธุรกิจอย่างโปร่งใส

5.16 นโยบายฉบับนี้ให้ครอบคลุมถึงกระบวนการบริหารงานบุคคล [Human Resources] ตั้งแต่การคัดเลือก และสรรหาบุคลากร ฝึกอบรม ประเมินผลการปฏิบัติงาน การให้ผลตอบแทน และเลื่อนตำแหน่ง ที่สะท้อนถึงความมุ่งมั่นของบริษัทฯ ต่อมาตรการต่อต้านทุจริตและคอร์รัปชัน โดยกำหนดให้ผู้บังคับบัญชาทุกระดับสื่อสารและทำความเข้าใจกับพนักงาน เพื่อใช้ในกิจกรรมทางธุรกิจที่อยู่ในความรับผิดชอบและควบคุมดูแลการปฏิบัติให้เป็นไปอย่างมีประสิทธิภาพ

## 6. การรับแจ้งเบาะแสหรือร้องเรียนการทุจริตและคอร์รัปชัน

บริษัทฯ มีความมุ่งมั่นในการดำเนินธุรกิจอย่างโปร่งใสและเป็นธรรม จึงกำหนดให้มีช่องทางการรับแจ้งเบาะแสหรือข้อร้องเรียนเกี่ยวกับการทุจริตและคอร์รัปชัน ที่ผู้มีส่วนได้เสียทุกกลุ่ม เช่น ผู้ถือหุ้น ลูกค้า คู่ค้า คู่แข่งทางการค้า เจ้าหนี้ ภาครัฐบาล ชุมชน สังคม ผู้บริหาร และพนักงาน สามารถติดต่อกับบริษัทฯ ได้ ทั้งนี้ไม่ว่าจะแจ้งด้วยวิธีใดก็ตาม บริษัทฯ จะดำเนินการตามมาตรการคุ้มครองผู้แจ้งเบาะแส โดยจะไม่เปิดเผยและรักษาความลับ

6.1 หากผู้ใดพบเห็นการกระทำของกรรมการ ผู้บริหาร และพนักงานของบริษัทฯ ในเรื่องดังต่อไปนี้

6.1.1 พบเห็นการกระทำทุจริตและคอร์รัปชันที่เกี่ยวข้องกับบริษัทฯ ทั้งทางตรงหรือทางอ้อม เช่น พบเห็นบุคคลในบริษัทฯ ดัดสินบนหรือรับสินบนจากเจ้าหน้าที่ภาครัฐหรือเอกชน

6.1.2 พบเห็นการกระทำที่ผิดขั้นตอนตามระเบียบปฏิบัติของบริษัทฯ หรือมีผลกระทบต่อระบบการควบคุมภายในจนทำให้สงสัยได้ว่า อาจเป็นช่องทางในการทุจริตและคอร์รัปชัน

6.1.3 พบเห็นการกระทำที่ทำให้บริษัทฯ เสียผลประโยชน์ กระทบต่อชื่อเสียง

6.1.4 พบเห็นการกระทำที่ผิดกฎหมาย ผิดศีลธรรม จรรยาบรรณทางธุรกิจ

6.2 คณะกรรมการบริษัทฯ มอบหมายให้คณะกรรมการตรวจสอบเป็นผู้พิจารณาแจ้งเบาะแส ข้อร้องเรียนหรือการกระทำที่สงสัยได้ว่าเป็นการทุจริตและคอร์รัปชันที่เกิดขึ้นกับบริษัทฯ ทั้งทางตรงหรือทางอ้อม โดยผู้ร้องเรียนที่พบเห็นการกระทำตามข้อ 6.1 สามารถแจ้งเบาะแสโดยระบุรายละเอียด พร้อมทั้งข้อมูลและหลักฐานที่เพียงพอต่อการตรวจสอบ รวมถึงแจ้งชื่อ-นามสกุล ที่อยู่ และโทรศัพท์ ส่งมายังช่องทางรับเรื่องดังนี้

6.2.1 แจ้งทางอีเมล [fraud\\_corruption@deves.co.th](mailto:fraud_corruption@deves.co.th) หรือไปรษณีย์ จ่าหน้าซองหรือยื่นโดยตรงที่ประธานคณะกรรมการตรวจสอบ กรรมการผู้จัดการ หรือผู้อำนวยการสำนักตรวจสอบ ที่บริษัท เทเวศประกันภัย จำกัด [มหาชน] 97 และ 99 อาคารเทเวศประกันภัย ถนนราชดำเนินกลาง แขวงบวรนิเวศ เขตพระนคร กรุงเทพฯ 10200

6.2.3 กรณีผู้แจ้งเบาะแสหรือผู้ร้องเรียน มีข้อร้องเรียนต่อคณะกรรมการบริษัทฯ ขอให้ส่งเรื่องร้องเรียนมายังประธานคณะกรรมการตรวจสอบโดยตรง

## 7. มาตรการคุ้มครองและรักษาความลับ

7.1 เพื่อเป็นการคุ้มครองสิทธิผู้ร้องเรียนและผู้ให้ข้อมูลที่กระทำโดยเจตนาสุจริต บริษัทฯ จะปกปิดชื่อ ที่อยู่ หรือข้อมูลที่ระบุตัวผู้ร้องเรียนหรือผู้ให้ข้อมูลและเก็บรักษาไว้เป็นความลับ โดยจำกัดเฉพาะผู้ที่ทำหน้าที่รับผิดชอบในการดำเนินการตรวจสอบเรื่องร้องเรียนเท่านั้นที่สามารถเข้าถึงข้อมูลดังกล่าวได้

7.2 กรณีที่มีการร้องเรียนกรรมการบริษัท คณะกรรมการตรวจสอบจะทำหน้าที่คุ้มครองผู้แจ้งเบาะแส ผู้ร้องเรียน พยาน และบุคคลที่ให้ข้อมูลในการสืบสวน ไม่ให้ได้รับความเดือดร้อน อันตรายใด หรือความไม่ชอบธรรม โดยขอให้ผู้ร้องเรียนส่งเรื่องร้องเรียนมายังประธานคณะกรรมการตรวจสอบโดยตรง

7.3 ประธานคณะกรรมการตรวจสอบ มีหน้าที่ในการใช้ดุลยพินิจสั่งการตามที่เห็นสมควร เพื่อคุ้มครองผู้แจ้งเบาะแส หรือผู้ร้องเรียน พยาน และบุคคลที่ให้ข้อมูลในการสืบสวนหาข้อเท็จจริง ไม่ให้ได้รับความเดือดร้อน อันตรายใด หรือความไม่ชอบธรรม อันเกิดมาจากการแจ้งเบาะแส ร้องเรียน การเป็นพยาน หรือการให้ข้อมูล

7.4 ประธานคณะกรรมการตรวจสอบ สามารถมอบหมายงานให้กับผู้บริหารคนใดคนหนึ่งทำหน้าที่แทนในการใช้ดุลยพินิจสั่งการคุ้มครองความปลอดภัยผู้แจ้งเบาะแส ผู้ร้องเรียน พยาน หรือบุคคลที่ให้ข้อมูล โดยผู้บริหารที่ได้รับมอบหมาย ต้องไม่มีส่วนเกี่ยวข้องกับเรื่องที่ได้รับความแจ้งเบาะแสหรือร้องเรียน ทั้งทางตรงและทางอ้อม [เช่น ผู้ถูกกล่าวหาเป็นผู้บังคับบัญชาโดยตรง] ทั้งนี้ผู้ได้รับข้อมูลจากการปฏิบัติหน้าที่ที่เกี่ยวข้องกับเรื่องร้องเรียน มีหน้าที่เก็บรักษาข้อมูลและเอกสารหลักฐานของผู้ร้องเรียนและผู้ให้ข้อมูลไว้เป็นความลับ ห้ามเปิดเผยข้อมูลแก่บุคคลอื่นที่ไม่มีความเกี่ยวข้อง เว้นแต่เป็นการเปิดเผยตามหน้าที่กฎหมายกำหนด

## 8. การสืบสวน การตรวจสอบ และบทลงโทษ

8.1 เมื่อได้รับแจ้งเบาะแส ประธานคณะกรรมการตรวจสอบเป็นผู้สั่งการสืบสวนข้อเท็จจริง โดยระหว่างดำเนินการ ประธานคณะกรรมการตรวจสอบหรืออาจมอบหมายให้ผู้บริหารระดับสูงแจ้งผลความคืบหน้าเป็นระยะให้ผู้แจ้งเบาะแสหรือผู้ร้องเรียนทราบ โดยกำหนดระยะเวลาการสอบสวนข้อเท็จจริง จนพิจารณาเสร็จสิ้นได้อีกไม่เกิน 30 วัน และสามารถขยายเวลาสืบสวนข้อเท็จจริงและพิจารณาจนเสร็จสิ้นได้อีกไม่เกิน 30 วัน

8.2 กรณีสืบสวนและพบการทุจริตและคอร์รัปชัน หรือการกระทำใดซึ่งส่งผลกระทบต่อฐานะการเงิน ผลการดำเนินงาน หรือชื่อเสียงของบริษัทฯ ให้คณะกรรมการตรวจสอบรายงานต่อคณะกรรมการบริษัทฯ เพื่อดำเนินการแก้ไขภายในระยะเวลาที่เหมาะสมโดยไม่ชักช้า ตามที่คณะกรรมการตรวจสอบเห็นสมควร

8.3 กรณีสืบสวนข้อเท็จจริงแล้วพบว่า ข้อมูลหรือหลักฐานที่มี มีเหตุอันควรเชื่อได้ว่า ผู้ถูกกล่าวหาได้กระทำการทุจริตและคอร์รัปชันจริง บริษัทฯ จะให้สิทธิผู้ถูกกล่าวหาหรือรับทราบข้อกล่าวหาและสิทธิพิสูจน์ตนเองโดยการหาข้อมูลหรือหลักฐานที่แสดงให้เห็นว่าตนเองไม่มีส่วนเกี่ยวข้องกับการกระทำทุจริตและคอร์รัปชันตามที่ได้อ้างกล่าวหา

8.4 กรณีผู้ถูกกล่าวหา ได้กระทำการทุจริตและคอร์รัปชันจริง ถือว่าเป็นการกระทำผิดนโยบายบริษัทฯ ผู้ถูกกล่าวหาต้องได้รับการพิจารณาโทษทางวินัยตามระเบียบที่บริษัทฯ กำหนดไว้ และหากการกระทำการนั้นผิดกฎหมาย ผู้กระทำความผิดอาจได้รับโทษทางกฎหมาย ทั้งนี้คำตัดสินของประธานคณะกรรมการตรวจสอบถือเป็นอันสิ้นสุด

8.5 กรณีที่การทุจริตและคอร์รัปชันนั้นเกี่ยวข้องกับไปยังบุคคลภายนอกหรือคู่ค้าบริษัทฯ บริษัทฯ จะระงับสัญญาหรือระงับการชำระเงินแก่ผู้มีส่วนเกี่ยวข้อง และจะดำเนินคดีตามกฎหมายตามที่บริษัทฯ เห็นสมควร

8.6 การร้องเรียนโดยไม่สุจริต กรณีพิสูจน์ได้ว่าเป็นการกระทำไม่สุจริต ถ้าเป็นพนักงานบริษัทฯ จะได้รับโทษทางวินัย แต่หากเป็นบุคคลภายนอก และบริษัทฯ ได้รับความเสียหาย จะพิจารณาดำเนินคดีตามกฎหมาย

8.7 กรณีร้องเรียนกรรมการบริษัท คณะกรรมการตรวจสอบมีหน้าที่ในการรับเรื่อง หาข้อมูล และตรวจสอบข้อเท็จจริง เพื่อรายงานต่อคณะกรรมการบริษัทฯ ให้ร่วมกันพิจารณาและกำหนดโทษตามที่เห็นสมควร

8.8 กรณีที่มีการละเมิด ฝ่าฝืนนโยบาย มาตรการ หรือแนวปฏิบัติการต่อต้านทุจริตและคอร์รัปชันที่กำหนดขึ้นที่ส่งผลให้บริษัทฯ ได้รับความเสียหาย ผู้ที่ปฏิบัติไม่ถูกต้องจะได้รับโทษทางวินัยตามระเบียบของบริษัทฯ

## 9. การเผยแพร่นโยบายต่อต้านการทุจริตและคอร์รัปชัน

เพื่อให้ทุกคนในบริษัทฯ และคู่ค้า ได้รับทราบถึงนโยบาย มาตรการ และการนำไปปฏิบัติ รวมถึงการเปิดเผยต่อสาธารณชนเกี่ยวกับนโยบายและมาตรการต่อต้านทุจริตและคอร์รัปชัน บริษัทฯ จึงได้ดำเนินการดังนี้

9.1 บริษัทฯ จะสื่อสารนโยบายและมาตรการผ่านช่องทางต่าง ๆ เช่น เว็บไซต์ อีเมล รายงานประจำปี สื่อสังคมออนไลน์ แผ่นพับ หนังสือแจ้ง ฯลฯ

9.2 บริษัทฯ จะจัดให้มีการอบรมนโยบายให้กับพนักงานใหม่

9.3 บริษัทฯ จะมีการทบทวนนโยบายอย่างสม่ำเสมอทุกปี

## 2. นโยบายการบริหารความเสี่ยงองค์กร

ธุรกิจประกันภัยเป็นธุรกิจที่ต้องเผชิญการเปลี่ยนแปลงตลอดเวลาทั้งในปัจจุบันและอนาคต ไม่ว่าจะเป็นปัจจัยภายนอก เช่น สถานะเศรษฐกิจ การเมือง และเทคโนโลยีสารสนเทศ หรือปัจจัยภายใน เช่น การปรับเปลี่ยนกลยุทธ์การดำเนินงาน โครงสร้างองค์กร การบริหารจัดการข้อมูลประกอบกับกรรมการและผู้บริหารได้ตระหนักถึงความสำคัญในการบริหารความเสี่ยง ซึ่งถือเป็นองค์ประกอบในการก้าวไปสู่ระบบการกำกับดูแลกิจการที่ดี พร้อมทั้งสร้างมูลค่าเพิ่มให้กับผู้ที่เกี่ยวข้อง ทั้งนี้องค์กรเชื่อมั่นว่า การบริหารความเสี่ยงเป็นกระบวนการที่ช่วยให้บรรลุวัตถุประสงค์ที่ตั้งไว้ ขณะเดียวกันก็ลดอุปสรรคหรือสิ่งที่ไม่คาดหวังที่อาจเกิดขึ้นทั้งด้านผลกำไร การปฏิบัติงาน และความเชื่อถือจากผู้ถือหุ้นและผู้มีส่วนได้ส่วนเสีย เป็นการป้องกันความเสียหายต่อทรัพยากรองค์กร ตอบสนองต่อการเปลี่ยนแปลงทางธุรกิจอย่างมีประสิทธิภาพ มีระบบจัดการและควบคุมที่ดีตามที่สำนักงาน คปภ. กำหนด รวมทั้งเพิ่มระดับการแข่งขันและสนับสนุนความยั่งยืนขององค์กร ดังนั้นคณะกรรมการบริหารความเสี่ยง จึงได้กำหนดนโยบายขึ้นเพื่อเป็นแนวทางในการบริหารจัดการความเสี่ยงของบริษัทฯ

### แนวทางในการบริหารความเสี่ยง

บริษัท เทเวศประกันภัย จำกัด [มหาชน] ได้กำหนดแนวทางบริหารความเสี่ยง โดยใช้เครื่องมือดัชนีชี้วัดความเสี่ยง [Key Risk Indicators : KRI] ในการติดตามและรายงาน รวมถึงกำหนดให้ครอบคลุม “ขอบเขตการบริหารความเสี่ยงและกิจกรรมหลัก” ตามประกาศที่สำนักงาน คปภ. กำหนด รวมทั้งเรื่องการกำหนดเบี้ยประกันภัย การพัฒนาผลิตภัณฑ์ประกันภัย การพิจารณารับประกันภัย และการลงทุน ต้องสัมพันธ์กันตามนโยบายที่กำหนดไว้ในแต่ละกิจกรรม ทั้งนี้การบริหารความเสี่ยงของกิจกรรมหลัก จะอยู่ในนโยบายของกิจกรรมหลักนั้นๆ นอกจากนี้ตามมาตรฐานระบบบริหารงานคุณภาพ ISO 9001 : 2015 ที่บริษัทฯ ได้รับการรับรองจาก Tuv Nord ตามข้อกำหนด บริษัทฯ ต้องมีการบริหารความเสี่ยง โดยพิจารณาถึงระดับหน่วยงานและ Process การปฏิบัติงานหรือ Procedure เพื่อสร้างความตระหนักให้กับผู้บริหารและพนักงานให้ความสำคัญในการบริหารความเสี่ยงถึงระดับปฏิบัติงาน รวมถึงกำหนดให้มีการรายงานความเสี่ยงด้านต่าง ๆ ในการประชุมสายงาน คณะผู้บริหาร คณะกรรมการตรวจสอบ และคณะกรรมการบริษัทฯ เพื่อบูรณาการกระบวนการในการบริหารจัดการความเสี่ยงของบริษัทฯ ให้มีความยั่งยืนทั่วทั้งองค์กร

### ระดับความเสี่ยงที่ยอมรับได้

บริษัทฯ ได้กำหนดแนวทางการป้องกันและบรรเทาความเสี่ยงจากการดำเนินงานของบริษัทฯ โดยบริหารความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ [Risk Appetite] หรือเบี่ยงเบนไม่เกินกว่าระดับที่องค์กรยอมรับ [Risk Tolerance] รวมทั้งดำรงเงินกองทุนให้เพียงพอตามกฎหมาย และเพื่อหลีกเลี่ยงความเสียหายหรือความสูญเสียที่อาจเกิดขึ้น บริษัทฯ จึงได้กำหนดดัชนีชี้วัดความเสี่ยงในทุกประเภทความเสี่ยงที่ครอบคลุมตามข้อกำหนดของ คปภ. โดยมอบหมายให้หน่วยงานที่เกี่ยวข้อง [Risk Owner] ดำเนินการทบทวน ประเมินความเสี่ยง ติดตาม วิเคราะห์ และกำหนดมาตรการบริหารจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้อย่างสม่ำเสมอ ตามระดับความเสี่ยงที่กำหนดใน คู่มือดัชนีชี้วัดความเสี่ยง [Key Risk Indicators Manual] รวมถึงการรายงานไปยังคณะกรรมการบริหารความเสี่ยงตามที่กำหนด

### หน้าที่ความรับผิดชอบ

- บริษัทฯ กำหนดให้การบริหารความเสี่ยงเป็นหน้าที่ความรับผิดชอบของคณะกรรมการบริษัทฯ คณะกรรมการบริหารความเสี่ยง คณะกรรมการตรวจสอบ คณะกรรมการชุดย่อย หน่วยงานต่างๆ ภายในบริษัทฯ รวมถึงผู้บริหารและพนักงานในทุกระดับชั้นที่ต้องตระหนักถึงความเสี่ยงที่มีในการปฏิบัติงานในหน่วยงานของตนและองค์กร โดยให้ความสำคัญในการบริหารความเสี่ยงด้านต่างๆ ให้อยู่ในระดับที่เพียงพอและเหมาะสม
- บริษัทฯ กำหนดบทบาทหน้าที่ผู้ที่เกี่ยวข้อง รวมทั้งความเชื่อมโยงระหว่างกระบวนการบริหารความเสี่ยง และภาพรวมโครงสร้างการกำกับดูแลการบริหารความเสี่ยง และวัฒนธรรมการบริหารความเสี่ยงไว้ใน “กรอบการบริหารความเสี่ยง [Risk Management Framework]”

### การติดตามความเสี่ยงและดัชนีชี้วัดความเสี่ยง [Key Risk Indicators : KRI]

- บริษัทฯ กำหนดให้มีการติดตามความเสี่ยงตามประกาศของสำนักงาน คปภ. ตามบทบาทหน้าที่ของคณะกรรมการผู้บริหาร และพนักงาน ที่กำหนดไว้ใน “กรอบการบริหารความเสี่ยง [Risk Management Framework]”
- บริษัทฯ กำหนดให้มีการจัดทำดัชนีชี้วัดความเสี่ยง เพื่อประโยชน์ดังนี้
  - ใช้ในการพิจารณาทิศทางของความเสี่ยงว่ามีแนวโน้มเพิ่มขึ้นหรือลดลง
  - เป็นสัญญาณเตือน [Early Warning] เพื่อนำไปสู่การค้นหาสาเหตุและปรับปรุงแก้ไข
  - ใช้สนับสนุนการวัดความเสี่ยงเชิงปริมาณและกิจกรรมการควบคุมภายใน
  - แสดงถึงความสัมพันธ์ของการจัดการความเสี่ยงในด้านต่างๆ ขององค์กร

- บริษัทฯ กำหนดให้มีการทบทวนดัชนีชี้วัดความเสี่ยงทุกปี และกำหนดให้มีระเบียบปฏิบัติงาน [Procedure] เรื่อง การบริหารจัดการความเสี่ยง ตามระบบบริหารงานคุณภาพ [Quality Management System] ISO 9001 เพื่อใช้ในการติดตามความเสี่ยงและดัชนีชี้วัดความเสี่ยงให้เป็นไปตามประกาศของสำนักงาน คปภ.

### การวิเคราะห์ความต่อเนื่อง และการทดสอบภาวะวิกฤต

- บริษัทฯ กำหนดให้มีการวิเคราะห์ความต่อเนื่องในการดำเนินธุรกิจภายใต้สถานการณ์ที่หลากหลายที่บริษัทคาดว่าจะเกิดขึ้นในอนาคต ซึ่งครอบคลุมถึงการทดสอบภาวะวิกฤต ตามระยะเวลาที่สอดคล้องกับแผนธุรกิจและระดับความเสี่ยงที่ยอมรับได้ และดำเนินการอย่างน้อยปีละหนึ่งครั้ง
- บริษัทฯ กำหนดให้การวิเคราะห์ความต่อเนื่องในการดำเนินธุรกิจครอบคลุมถึงความเสี่ยงที่สำคัญทั้งความเสี่ยงเชิงคุณภาพ และความเสี่ยงเชิงปริมาณภายใต้กรอบการบริหารความเสี่ยงแบบองค์รวมและการประเมินความเสี่ยงและความมั่นคงทางการเงินของบริษัท และคำนึงถึงความสัมพันธ์ระหว่างความเสี่ยง รวมถึงการเปลี่ยนแปลงลักษณะความเสี่ยงของบริษัทในอนาคต โดยบริษัทจะประมาณการสถานะทางการเงิน เงินกองทุนที่ต้องดำรงไว้ และอัตราส่วนความเพียงพอของเงินกองทุนของบริษัท
- บริษัทฯ กำหนดสถานการณ์ที่ใช้ในการวิเคราะห์ความต่อเนื่องประกอบไปด้วย สถานการณ์พื้นฐาน [base] สถานการณ์เศรษฐกิจมหภาค [macroeconomic] สถานการณ์วิกฤตทางการเงิน [financial crisis] สถานการณ์มหันตภัย [catastrophe] สถานการณ์ภาวะวิกฤตแบบย้อนกลับ [reverse stress test] และสถานการณ์ที่บริษัทฯ กำหนดขึ้นเอง [self-select]
- บริษัทฯ จัดทำแผนการดำเนินการ [management action] อันเป็นผลมาจากการวิเคราะห์ความต่อเนื่องในการดำเนินธุรกิจเพื่อให้บริษัทมีความสามารถทางการเงินทั้งในเรื่องเงินกองทุนและสภาพคล่อง รวมถึงจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง [Business Continuity Plan: BCP] ในกรณีเกิดเหตุการณ์ที่ทำให้บริษัทไม่สามารถดำเนินธุรกิจประจำวันได้อย่างต่อเนื่องและเป็นไปตามปกติ

### การบริหารความเสี่ยงด้านการฉ้อฉลประกันภัย

- บริษัทฯ กำหนดให้มีการระบุเหตุการณ์และแหล่งที่มาของความเสี่ยงด้านการฉ้อฉล ที่ครอบคลุมถึงการดำเนินงานที่อาจส่งผลกระทบต่อรายได้ เงินกองทุน ชื่อเสียง หรือการดำรงอยู่ของบริษัทฯ เพื่อนำมาประเมินโอกาสและผลกระทบ รวมถึงจัดระดับความเสี่ยง เพื่อบริหารจัดการได้อย่างเหมาะสม
- บริษัทฯ กำหนดให้มีการบริหารจัดการความเสี่ยงด้านการฉ้อฉล ดังนี้
  - มาตรฐานคุณสมบัติและความเหมาะสมของคณะกรรมการบริษัทฯ ผู้บริหาร และพนักงาน โดยมีการประเมินให้สอดคล้องกับตำแหน่งหน้าที่ความรับผิดชอบของแต่ละบุคคลอย่างเหมาะสม
  - หลักเกณฑ์และวิธีการรับลูกค้าและจัดกลุ่มลูกค้า ที่แสดงให้เห็นถึงลักษณะลูกค้าที่มีความผิดปกติ รวมถึงการตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้า [Customer Due Diligence : CDD] ตามประเภทการรับประกันภัยและมาตรการดำเนินการกรณีตรวจพบความผิดปกติ
  - หลักเกณฑ์และวิธีการบริหารจัดการค่าใช้จ่ายหรือค่าสินไหมทดแทนที่ชัดเจน เพื่อลดความเสี่ยงด้านการฉ้อฉลในการเรียกร้องการชดใช้เงินหรือค่าสินไหมทดแทน
  - หลักเกณฑ์และวิธีการพิจารณาคุณสมบัติและความเหมาะสมของตัวแทนและนายหน้า รวมถึงการปฏิบัติตามหลักจรรยาบรรณ โดยคำนึงถึงการปฏิบัติหน้าที่ของตัวแทนและนายหน้าตามกฎหมายและแนวปฏิบัติที่เกี่ยวข้อง เพื่อยับยั้งและป้องกันการฉ้อฉลโดยตัวแทนและนายหน้า
  - ติดตามตรวจสอบผลการดำเนินงานหรือแนวโน้มการดำเนินธุรกิจ รวมทั้งพฤติกรรมที่อาจก่อให้เกิดความเสี่ยงของตัวแทนและนายหน้า เพื่อตรวจหาการฉ้อฉลโดยตัวแทนและนายหน้า
  - กำหนดให้มีนโยบายการใช้บริการจากบุคคลภายนอก และแนวทางคัดเลือกผู้ให้บริการก่อนทำสัญญาใหม่หรือทบทวนสัญญาเก่า รวมทั้งติดตาม ประเมินผล ตรวจสอบ และควบคุมความเสี่ยงจากการใช้บริการ
- บริษัทฯ กำหนดให้มีหลักเกณฑ์ วิธีการ ช่องทางรับแจ้งเบาะแส มาตรการคุ้มครองผู้ร้องเรียน การรักษาความลับ รวมถึงการสืบสวนสอบสวนที่เป็นอิสระจากกิจกรรมที่สงสัย เพื่อค้นหาข้อเท็จจริง จัดการและเยียวยาความเสียหาย และรายงานต่อคณะกรรมการตรวจสอบ ตามที่กำหนดไว้ในนโยบายต่อต้านการทุจริตและคอร์รัปชัน
- จัดทำฐานข้อมูลเกี่ยวกับการฉ้อฉล เพื่อประโยชน์ในการติดตามและบริหารจัดการความเสี่ยงของบริษัทฯ
- ควบคุม ติดตาม และประเมินผลการบริหารจัดการความเสี่ยงด้านการฉ้อฉล เพื่อประกอบการทบทวนนโยบายการบริหารความเสี่ยงด้านการฉ้อฉล อย่างน้อยปีละหนึ่งครั้ง
- จัดทำสรุปรายงานการปฏิบัติตามมาตรการบริหารความเสี่ยงด้านการฉ้อฉล ที่ผ่านการกลั่นกรองจากคณะกรรมการบริหารความเสี่ยง เสนอต่อคณะกรรมการบริษัทฯ พิจารณายกขึ้นอย่างน้อยปีละหนึ่งครั้ง



## การบริหารความเสี่ยงด้านกลยุทธ์ [Strategic Risk]

- บริษัทฯ มีการบริหารความเสี่ยงโดยพิจารณาถึงเป้าหมาย แผนรองรับการขยายงาน ทิศทางการดำเนินงานธุรกิจในอนาคตของบริษัทฯ ตามแผนธุรกิจ ซึ่งผู้บริหารระดับสูงมีส่วนร่วมในการพิจารณาและอนุมัติแผนงานต่างๆ รวมทั้งมีกระบวนการติดตามและรายงานผลการปฏิบัติงานตามแผนงานเป็นประจำทุกเดือน เพื่อให้มั่นใจว่าบริษัทฯ กำลังดำเนินมาในทิศทางที่ถูกต้องและเป็นไปตามเป้าหมายของบริษัทฯ

## การบริหารความเสี่ยงด้านประกันภัย [Insurance Risk]

- บริษัทฯ นำข้อมูลที่เกี่ยวข้องกับบุคคล วัตถุ หรือภัย ที่ถูกเอาประกันภัยมาพิจารณาถึงระดับความเสี่ยงภัยที่รับโอนว่าอยู่ในระดับที่บริษัทฯ ได้รับความเสี่ยงได้หรือไม่ โดยอิงจากคู่มือและอัตราเบี้ยประกันภัยที่กำหนด มีการติดตามและควบคุมการกระจายตัวของความเสี่ยงให้มีความเหมาะสม ไม่กระจุกตัวทั้งในทางภูมิศาสตร์และประเภทของความเสี่ยง สำหรับความเสี่ยงภัยที่อยู่ในระดับสูงเกินกว่าที่บริษัทฯ จะสามารถรับไว้ได้เอง บริษัทฯ ได้มีการจัดการให้มีการถ่ายโอนความเสี่ยงไปยังผู้รับประกันภัยต่อผ่านสัญญาประกันภัยต่อทั้งวิธีที่เป็นสัญญาล่วงหน้ารายปี และวิธีที่เป็นการทำเฉพาะราย เพื่อบริหารพอร์ตการรับประกันภัยให้มีสัดส่วนของการรับประกันภัยอย่างเหมาะสม รวมทั้งมีการติดตามและรายงานผลด้านอัตราส่วนสินไหมทดแทนแยกตามประเภทการรับประกันภัยเป็นประจำทุกเดือน เพื่อให้สอดคล้องกับวัตถุประสงค์และเป้าหมายของบริษัทฯ

## การบริหารความเสี่ยงด้านตลาด [Market Risk]

- บริษัทฯ มีคณะกรรมการลงทุนเป็นผู้กำหนดกรอบนโยบายการลงทุน เพื่อกำกับดูแลการลงทุน ให้เป็นไปตามนโยบายการบริหารความเสี่ยงรวม โดยเน้นการลงทุนหลักทรัพย์ที่มีความเสี่ยงต่ำ มีความมั่นคง ให้ผลตอบแทนในอัตราที่เหมาะสมและสม่ำเสมอ รวมถึงได้มีการกำหนดคู่มือแนวทางบริหารการลงทุน เป็นลายลักษณ์อักษร ซึ่งจะมีการกำหนดกรอบและทิศทางการลงทุนในแต่ละปี โดยระบุขีดจำกัดในการลงทุนทุกประเภทและทุกระดับ ซึ่งพิจารณากำหนดขึ้นจากอัตราผลตอบแทนเป้าหมายและสภาพคล่อง โดยให้เชื่อมโยงและสอดคล้องกับผลกระทบต่อเงินกองทุนที่ต้องดำรงไว้ตามกฎหมายเกณฑ์การดำรงเงินกองทุนตามระดับความเสี่ยง

## การบริหารความเสี่ยงด้านเครดิต [Credit Risk]

- บริษัทฯ ได้กำหนดให้มีระบบการติดตามและรายงานฐานะลูกหนี้เบี้ยประกันภัยค้างชำระเป็นประจำทุกเดือน รวมถึงการควบคุมให้มีการเรียกเก็บเบี้ยประกันภัยเป็นไปตามระเบียบของสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (คปภ.) จัดทำมาตรการควบคุมและป้องกันความเสี่ยง กำหนดหลักเกณฑ์ในการพิจารณาคัดเลือกบริษัทรับประกันภัยต่อและนายหน้า/ตัวแทนอย่างรัดกุม พิจารณาศักยภาพในด้านการขาย สถานะทางการเงิน ประวัติในการประกอบธุรกิจ ความสามารถในการชำระเบี้ย ตลอดจนกำหนดให้ตัวแทนต้องมีหลักทรัพย์หรือบุคคลค้ำประกันในวงเงินเครดิตที่บริษัทฯ กำหนด อีกทั้งเพื่อเป็นการหลีกเลี่ยงความเสี่ยง บริษัทฯ จะเน้นลงทุนในตราสารหนี้ที่ผู้ออกมีคุณภาพสูงมีอันดับเครดิตที่ดี

## การบริหารความเสี่ยงด้านสภาพคล่อง [Liquidity Risk]

- บริษัทฯ มีการบริหารจัดการเงินสดหรือสินทรัพย์ที่เทียบเท่าเงินสดที่มีประสิทธิภาพ สามารถรักษาระดับเงินสดในมือให้อยู่ในระดับที่เหมาะสมตลอดเวลา และมีการติดตามเบี้ยประกันภัยค้างรับให้เป็นไปตามเกณฑ์ที่ คปภ. กำหนดเป็นประจำ รวมทั้งติดตามค่าสินไหมทดแทนค้างรับจากการรับประกันภัยต่ออย่างสม่ำเสมอ ทำให้เชื่อมั่นว่าความเสี่ยงด้านสภาพคล่องอยู่ในระดับที่ควบคุมได้

## การบริหารความเสี่ยงด้านปฏิบัติการ [Operational Risk]

- บริษัทฯ มีการกำหนดนโยบาย แผนงาน ด้านการบริหารความเสี่ยงด้านปฏิบัติการให้สอดคล้องกับนโยบายของบริษัทฯ พร้อมทั้งสื่อสารนโยบายให้ทุกหน่วยงานทราบ และนำไปปฏิบัติอย่างเคร่งครัด โดยพิจารณาขอบเขตการบริหารความเสี่ยงด้านปฏิบัติการให้ครอบคลุม 9 กิจกรรมหลักของบริษัทฯ ดังนี้
  - การพัฒนาผลิตภัณฑ์ประกันภัย และการกำหนดอัตราเบี้ยประกันภัย
  - การเสนอขาย และการเก็บเบี้ยประกันภัย
  - การพิจารณารับประกันภัย
  - การประเมินสำรองประกันภัย
  - การบริหารจัดการค่าสินไหมทดแทน
  - การรับประกันภัยต่อ

- การลงทุนประกอบธุรกิจอื่น
- การบริหารสินทรัพย์และหนี้สิน
- การใช้บริการจากบุคคลภายนอก

### การบริหารความเสี่ยงด้านชื่อเสียง [Reputation Risk]

- บริษัทฯ ได้จัดตั้งหน่วยงานสำนักกำกับดูแล เพื่อทำหน้าที่ติดตามและกำกับกับการปฏิบัติงานของหน่วยงานต่างๆ ภายในบริษัทฯ ให้เป็นไปตามข้อบังคับ ตลอดจนกฎหมายอื่นๆ ที่เกี่ยวข้อง อีกทั้ง บริษัทฯ ยังได้กำหนด "นโยบายต่อต้านทุจริตและคอร์รัปชัน" และ "นโยบายการป้องกันและปราบปรามการฟอกเงิน การสนับสนุนทางการเงินแก่การก่อการร้าย และการแพร่ขยายอาวุธที่มีอานุภาพทำลายล้างสูง" ขึ้น อย่างเป็นลายลักษณ์อักษรซึ่งผ่านความเห็นชอบจากคณะกรรมการบริษัทฯ โดยกำหนด คำนิยาม แนวทางปฏิบัติ และมาตรการต่างๆ เพื่อส่งเสริมและสื่อสารให้เกิดความเข้าใจนำไปสู่การยอมรับและปลูกจิตสำนึกที่ดีให้บุคลากรทุกระดับ รวมถึงมีการติดตามและแก้ไขเรื่องร้องเรียนเป็นประจำทุกเดือน

### การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ [Information Technology Risk]

- บริษัทฯ มีการติดตามความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ ทั้งข่าวสารจากหน่วยงานเอกชน รวมถึงหน่วยงานราชการต่างๆ ที่ได้มีการสื่อสารออกมา เพื่อนำมาวิเคราะห์ผลกระทบ และสื่อสารไปยังบุคลากรในทุกระดับให้รับทราบ รวมทั้งได้นำระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC 27001 : 2013 มาเป็นกรอบการปฏิบัติงานที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศของบริษัทฯ มีการจัดทำ "นโยบายการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ", "นโยบายการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ" และ "นโยบายการบริหารความต่อเนื่องทางธุรกิจ" เพื่อไม่ให้อุปการะหยุดชะงักจากความเสียหายในด้านต่างๆ พร้อมกับการจัดทำ แผนรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ [Cyber Incident Response Plan : CIRP]

### การบริหารความเสี่ยงด้านมหันตภัย [Catastrophe Risk]

- บริษัทฯ มีการติดตามและควบคุมการกระจายตัวของความเสี่ยงให้มีความเหมาะสม ไม่กระจุกตัวทั้งในทางภูมิศาสตร์และประเภทของความเสี่ยง สำหรับความเสี่ยงภัยที่อยู่ในระดับสูงเกินกว่าที่บริษัทฯ จะสามารถรับไหวได้เอง บริษัทฯ ได้มีการจัดการให้มีการถ่ายโอนความเสี่ยงไปยังผู้รับประกันภัยต่อผ่านสัญญาประกันภัยต่อทั้งวิธีที่เป็นสัญญาล่วงหน้ารายปี และวิธีที่เป็นการทำเฉพาะราย รวมทั้งสัญญาประกันภัยต่อการคุ้มครองความเสียหายส่วนเกิน [Excess of Loss Cover]

### การบริหารความเสี่ยงที่เกิดขึ้นใหม่ [Emerging Risk]

- บริษัทฯ มีการติดตามความเสี่ยงที่เกิดขึ้นใหม่อย่างสม่ำเสมอ ในหลากหลายช่องทาง เพื่อนำมาวิเคราะห์ผลกระทบ หากเป็นความเสี่ยงที่มีนัยสำคัญ บริษัทฯ จะมีการทบทวนกรอบการบริหารความเสี่ยง และนโยบายการบริหารความเสี่ยงโดยทันที

### 3. นโยบายการพัฒนาผลิตภัณฑ์ประกันภัยและการกำหนดเบี้ยประกันภัย

- กำหนดให้มีคณะกรรมการผลิตภัณฑ์ ซึ่งประกอบด้วยหน่วยงานต่าง ๆ ตามที่สำนักงานคปภ.กำหนด มีหน้าที่กำหนดนโยบาย เป้าหมาย กลยุทธ์ และอนุมัติผลิตภัณฑ์และบริการใหม่ ให้สอดคล้องกับความเสี่ยง และเงินกองทุนของบริษัท หลักการประกันภัย หลักคณิตศาสตร์ประกันภัย หลักกฎหมาย และหลักศีลธรรมจรรยา ความเหมาะสมและเป็นธรรมต่อลูกค้า
- กำหนดให้มีการดำเนินการตาม Procedure การออกแบบและพัฒนาผลิตภัณฑ์ ตามระบบบริหารงานคุณภาพ ISO 9001 : 2015 โดยมีการรวบรวมข้อมูลต่าง ๆ เพื่อประกอบการพิจารณา การร่างรูปแบบผลิตภัณฑ์และบริการให้เป็นไปตามความต้องการของลูกค้า การบริหารความเสี่ยง การประสานงานกับหน่วยงานภายในและภายนอก และการประเมินผลหลังจากผลิตภัณฑ์ออกสู่ตลาดเพื่อปรับปรุงอย่างต่อเนื่อง รวมถึงติดตามกระบวนการดำเนินงานต่าง ๆ ของบริษัทให้มีความพร้อมและมีประสิทธิภาพก่อนผลิตภัณฑ์ออกจำหน่าย
- กำหนดให้มีสมมติฐานในการคำนวณอัตราเบี้ยประกันภัย โดยมีนักคณิตศาสตร์ประกันภัยเข้ามามีส่วนร่วมในกระบวนการกำหนดอัตราเบี้ยประกันภัย เพื่อตรวจสอบความถูกต้องของข้อมูลสถิติและความเหมาะสมของอัตราเบี้ยประกันภัย
- แบบและข้อความ และอัตราเบี้ยประกันภัยจะต้องผ่านการพิจารณาจากคณะกรรมการพัฒนาผลิตภัณฑ์และได้รับอนุมัติจากสำนักงาน คปภ.
- กำหนดให้มีการทบทวนผลิตภัณฑ์กรณีทีผลิตภัณฑ์นั้น ๆ ให้ผลตอบแทนไม่เป็นไปตามที่คาดหวัง เพื่อกำหนดมาตรการที่เหมาะสม

## 4. นโยบายการเสนอขาย และการเก็บเบี้ยประกันภัย

- บริษัทฯ มีนโยบายเพิ่มเบี้ยประกันภัยรับ ในระดับที่ไม่ต่ำกว่าอัตราการเจริญเติบโตของอุตสาหกรรมอย่างมีแบบแผน โดยมุ่งเน้นสร้างความสมดุลของที่มาของรายได้และช่องทางการเสนอขาย โดยไม่พึ่งพิงช่องทางใด ช่องทางหนึ่งมากเกินไป และมีการจัดพอร์ตการรับงานให้สมดุลย์ระหว่างการประกันภัยแต่ละประเภท ทั้งนี้บริษัทฯ ได้กำหนดช่องทางการเสนอขายออกเป็น 4 กลุ่มหลัก ดังนี้
  1. ช่องทางลูกค้ากลุ่มองค์กร
  2. ช่องทางลูกค้ารายบุคคล
  3. ช่องทางลูกค้าผ่านตัวแทน นายหน้า
  4. ช่องทางลูกค้าผ่านสถาบันการเงิน
- บริษัทฯ ได้นำระบบบริหารงานคุณภาพ ISO 9001 : 2015 เข้ามาช่วยในการพัฒนากระบวนการทำงาน มีการควบคุมคุณภาพการเสนอขายเพื่อยกระดับมาตรฐานการเสนอขายของบริษัทฯ ไปยังผู้เอาประกันภัยด้วยการบริการที่ดี มีคุณภาพ และได้รับอัตราเบี้ยประกันภัยที่เหมาะสมกับความเสี่ยงภัย รวมถึงการให้บริการหลังการขาย การชดเชยค่าสินไหมทดแทน และการบริหารจัดการข้อร้องเรียน เพื่อให้ลูกค้าได้รับการปฏิบัติด้วยความเป็นธรรม อีกทั้งกำหนดให้มีการปรับปรุงกระบวนการทำงานอย่างต่อเนื่อง เพื่อให้สอดคล้องกับสถานะที่เปลี่ยนแปลงไป
- บริษัทฯ กำหนดให้มีการคัดเลือกคนกลางประกันภัยอย่างมีคุณภาพ มีการบริหารจัดการเพื่อติดตาม ควบคุม ดูแล ตรวจสอบ และประเมินผลอย่างสม่ำเสมอ มีระบบงานที่ช่วยในการควบคุมคุณภาพการเสนอขาย รวมถึงการรายงานการเสนอขายและ Feedback ในทุกช่องทาง เพื่อนำมาปรับปรุงคุณภาพการให้บริการและพัฒนาผลิตภัณฑ์เพื่อตอบสนองความต้องการของลูกค้า โดยคำนึงถึงสิทธิประโยชน์ของผู้เอาประกันภัยอย่างสำคัญ
- บริษัทฯ กำหนดให้มีคณะกรรมการสินเชื่อ [Credit Committee] ในการกำกับดูแล มีการกำหนดวงเงินการขายเบี้ยประกันภัย [Credit Line] ให้กับตัวแทน/นายหน้าในแต่ละรายตามหลักทรัพย์สินค้ำประกันตามระเบียบที่กำหนดไว้ รวมถึงมีการติดตามค่าเบี้ยเงินประกันภัยที่ยอมรับได้ โดยพิจารณาจากอัตราส่วนเบี้ยประกันภัยค้ำประกันราคาประเมินต่อเบี้ยประกันภัยค้ำประกันราคาตามบัญชีไม่ต่ำกว่าเกณฑ์ที่กำหนดไว้ในดัชนีชี้วัดความเสี่ยง
- บริษัทฯ กำหนดให้มีการติดตามการชำระเบี้ยจากผู้เอาประกันภัยและตัวแทน/นายหน้าภายในระยะเวลาที่กำหนด เพื่อให้เป็นไปตามประกาศของสำนักงาน คปภ. โดยกำหนดให้มีการปฏิบัติตามมาตรฐานของกระบวนการที่กำหนดขึ้นอย่างเคร่งครัด มีการติดตามและรายงานกรณีตัวแทน/นายหน้ารายได้ไม่ชำระเบี้ยภายในระยะเวลาที่กำหนด เพื่อสร้างความมั่นใจให้กับลูกค้าของบริษัทฯ

## 5. นโยบายการพิจารณารับประกันภัย

การพิจารณารับประกันภัย หมายถึง บริษัทจะพิจารณารับประกันภัยตามความเสี่ยงของผู้เอาประกันภัยโดยพิจารณาจากปัจจัยเสี่ยงที่เกี่ยวกับบุคคล วัตถุ หรือภัย ที่ถูกเอาประกันภัยมาประเมินความเสี่ยง เพื่อตัดสินใจว่าจะรับประกันภัยภายใต้เงื่อนไขหรือข้อกำหนดอย่างไร หรือปฏิเสธการรับประกันภัย บริษัทฯ จึงได้กำหนดนโยบายไว้ดังนี้

- กำหนดแนวทางการพิจารณารับประกันภัย [Underwriting Guideline] ให้เหมาะสมกับความสามารถในการรับเสี่ยงภัยไว้เอง [Retention Capacity] และระดับความเสี่ยงที่ยอมรับได้ของบริษัทฯ [Risk Appetite] โดยได้รับความเห็นชอบจากกรรมการผู้จัดการ
- กำหนดให้มีระเบียบปฏิบัติงาน [Procedure] พร้อมทั้งสื่อสารและจัดอบรมให้พนักงานรับทราบและเข้าใจ
- กำหนดบทบาทหน้าที่ความรับผิดชอบของหน่วยงานและบุคลากรด้านการพิจารณารับประกันภัย โดยมอบหมายอำนาจหน้าที่การปฏิบัติงาน การอนุมัติ และการควบคุมภายใน ให้สอดคล้องกับระดับอำนาจในการพิจารณารับประกันภัย รวมถึงนโยบายและแนวทางในการพิจารณารับประกันภัย
- กำหนดขอบเขตและระดับอำนาจในการพิจารณารับประกันภัย [Underwriting Authority] ตามอำนาจดำเนินการที่ได้รับอนุมัติ โดยให้ระดับความเสี่ยงที่สูงขึ้นหรือซับซ้อนต้องได้รับการพิจารณาจากผู้มีอำนาจตามระดับตำแหน่งงานที่สูงขึ้น
- จัดให้มีระบบสารสนเทศการประกันภัยเพื่อเชื่อมโยงข้อมูลสำคัญ ได้แก่ ข้อมูลเกี่ยวกับการพิจารณารับประกันภัย อำนาจการพิจารณารับประกันภัย ขีดจำกัดการเอาประกันภัยต่อ และข้อมูลภัยสะสม โดยบริษัทฯ ได้กำหนดสิทธิในการเข้าถึงข้อมูลเพื่อรักษาความปลอดภัยของข้อมูลที่เกี่ยวข้อง

## 6. นโยบายการประเมินสำรองประกันภัย

สำรองประกันภัย คือเงินสำรองประกันภัยที่บริษัทฯ จะต้องจัดสรรไว้ในส่วนของหนี้สินสำหรับกรมธรรม์ประกันภัยที่ยังมีความผูกพันอยู่ตามกรมธรรม์ประกันภัย โดยแบ่งได้เป็น 2 ประเภท ดังนี้

- เงินกองทุนสำหรับความเสี่ยงจากสำรองค่าสินไหมทดแทน
  - เงินกองทุนสำหรับความเสี่ยงจากสำรองเบี้ยประกันภัย
- บริษัทฯ กำหนดให้มีการประเมินสำรองประกันภัยตามหลักคณิตศาสตร์ประกันภัยทุกเดือน และ กำหนดให้นักคณิตศาสตร์ประกันภัยทำการประเมินเงินกองทุนสำหรับความเสี่ยงจากภาระผูกพันสำหรับสัญญาประกันภัยในระยะสั้นทุกในช่วงกลางปีและสิ้นปี
  - บริษัทฯ กำหนดให้มีอัตราส่วนเงินกองทุนสำหรับความเสี่ยงจากสำรองค่าสินไหมทดแทนต่อจำนวนเงินกองทุนที่สามารถนำมาใช้ได้ทั้งหมด และอัตราส่วนเงินกองทุนสำหรับความเสี่ยงจากสำรองเบี้ยประกันภัยต่อจำนวนเงินกองทุนที่สามารถนำมาใช้ได้ทั้งหมด เพื่อใช้ในการติดตาม โดยกำหนดอัตราส่วนขั้นต่ำไว้ในนโยบายบริหารความเสี่ยง
  - บริษัทฯ กำหนดให้มีการรายงานผลของเงินสำรองประกันภัย ซึ่งเป็นส่วนหนึ่งของการจัดทำรายงาน RBC ที่รวมอยู่ในรายงานบริหารความเสี่ยง ต่อคณะกรรมการบริหาร คณะกรรมการตรวจสอบ และคณะกรรมการบริษัทฯ ในทุกไตรมาส

## 7. นโยบายการจัดการสินไหมทดแทน

การบริหารจัดการสินไหมทดแทน หมายถึง กระบวนการที่บริษัทประกันภัยทำการพิจารณาและจ่ายเงินสินไหมทดแทนตามข้อตกลงและเงื่อนไขที่กำหนดในสัญญาประกันภัย บริษัทฯ จึงได้กำหนดนโยบายไว้ดังนี้

- กำหนดให้มีระเบียบปฏิบัติงาน [Procedure] ที่ครอบคลุมกิจกรรมหลักทั้งหมด เช่น การพิจารณาการจ่ายค่าสินไหม การตั้งสำรองค่าสินไหม การสำรวจและการรายงานความเสียหาย การตกลงค่าสินไหม ฯลฯ โดยได้มีการกำหนด KPI และ KRI เพื่อใช้ในการติดตามผลการดำเนินงาน พร้อมทั้งสื่อสารให้พนักงานรับทราบ มีการทบทวนอย่างสม่ำเสมอ เพื่อให้สอดคล้องกับข้อกำหนดของกฎหมายและความเสี่ยงที่เปลี่ยนแปลงไป และปฏิบัติงานได้อย่างมีประสิทธิภาพ
- กำหนดบทบาทหน้าที่ความรับผิดชอบของหน่วยงานและบุคลากรด้านการจ่ายผลประโยชน์ รวมถึงการใช้สิทธิตามสัญญาประกันวินาศภัย โดยแบ่งแยกหน้าที่ของหน่วยงานที่รับผิดชอบการพิจารณาประกันภัย และการจ่ายค่าสินไหมทดแทน รวมถึงขอบเขตอำนาจในการอนุมัติอย่างเป็นลายลักษณ์อักษร โดยพิจารณาประสิทธิภาพ ความรู้ความสามารถ และความชำนาญในตำแหน่งไว้อย่างเหมาะสม
- กำหนดขอบเขตและระดับอำนาจในการพิจารณาจ่ายผลประโยชน์ [Claims Authority] ตามอำนาจดำเนินการที่ได้รับการอนุมัติ โดยระดับอำนาจในการอนุมัติ จำนวนค่าสินไหมทดแทนที่สูงขึ้น หรือรายการที่มีความซับซ้อน ต้องได้รับการพิจารณาจากผู้มีอำนาจตามระดับตำแหน่งงานที่สูงขึ้น

## 8. นโยบายการประกันภัยต่อ

การประกันภัยต่อ หมายถึง การกระจายความเสี่ยงภัยของผู้รับประกันภัยกับผู้รับประกันภัยด้วยตนเอง เนื่องจากความสามารถในการรับเสี่ยงภัยไว้เองของบริษัทมีจำกัด บริษัทจึงพิจารณาการโอนความเสี่ยงภัยบางส่วนหรือทั้งหมดไปให้ผู้รับประกันภัยต่อ หรือการรับโอนความเสี่ยงภัยบางส่วนหรือทั้งหมดจากผู้เอาประกันภัยต่อ

ทั้งนี้การประกันภัยต่อยังช่วยให้บริษัทฯ เพิ่มศักยภาพและขีดความสามารถในการรับประกันภัย และเพื่อให้เกิดเสถียรภาพกับผลการรับประกันภัย บริษัทฯ จึงได้กำหนดนโยบายไว้ดังนี้

- กำหนดกรอบการบริหารการประกันภัยต่อ และได้รับความเห็นชอบจากคณะกรรมการบริษัทฯ
- กำหนดให้มีระเบียบปฏิบัติงาน [Procedure] และจัดอบรมให้พนักงานรับทราบและปฏิบัติได้อย่างถูกต้อง
- กำหนดบทบาทหน้าที่ความรับผิดชอบของหน่วยงานและบุคลากรด้านการประกันภัยต่อ พร้อมมอบหมายอำนาจหน้าที่ด้านการปฏิบัติงาน การอนุมัติ และการควบคุม ให้สอดคล้องกับอำนาจดำเนินการของบริษัทฯ
- ปฏิบัติตามกรอบการบริหารการประกันภัยต่อ หลักเกณฑ์ ข้อกำหนด ข้อบังคับ กฎหมาย และประกาศของคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย [คปภ.] อย่างเคร่งครัด

บริษัทฯ ได้กำหนดนโยบายการบริหารความเสี่ยงไว้ดังนี้

- บริษัทฯ มีนโยบายกระจายความเสี่ยงภัยโดยการจัดทำประกันภัยต่อสำหรับการรับประกันภัยที่มีจำนวนเงินเอาประกันภัยสูงหรือมีความเสี่ยงสูงโดยเป็นไปตามนโยบายรับประกันภัย ทั้งในส่วนของประกันภัยต่อแบบเฉพาะรายและการประกันภัยต่อตามสัญญา รวมถึงการทำประกันภัยต่อตามสัญญาแบบไม่เป็นสัดส่วน [Excess of Loss Treaty] สำหรับรองรับความเสียหายจากมหันตภัย เพื่อคุ้มครองส่วนที่บริษัทรับเสี่ยงภัยไว้เอง [Retention]

แต่ทั้งนี้ในการกระจายความเสี่ยงภัย จะต้องเป็นไปตามกรอบการบริหารความเสี่ยงและการบริหารเงินกองทุนของบริษัทฯ รวมถึงระดับความเสี่ยงภัยที่บริษัทฯ ต้องการรับเสี่ยงภัยไว้เอง และส่วนที่โอนความเสี่ยง ซึ่งจะต้องสอดคล้องกับระดับความเสี่ยงที่ยอมรับได้ รวมถึงเป้าหมายเงินกองทุนของบริษัทฯ

- บริษัทฯ จะจัดทำประกันภัยต่อไปยังผู้รับประกันภัยต่อตามประกาศของคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย [คปภ.] เรื่อง หลักเกณฑ์ วิธีการ และเงื่อนไขในการประกันภัยต่อของบริษัทประกันวินาศภัย โดยบริษัทฯ จะพิจารณาจากอันดับความน่าเชื่อถือและความมั่นคงของผู้รับประกันภัยต่อ และติดตามการจัดอันดับความน่าเชื่อถือของผู้รับประกันภัยต่อทุกราย อย่างไรก็ตามบางกรณีบริษัทฯ อาจจะอนุโลมให้จัดทำประกันภัยต่อไปยังบริษัทรับประกันภัยต่อบางแห่งซึ่งมีรัฐบาลเป็นผู้ถือหุ้นได้

กรณีที่ผู้รับประกันภัยต่อรายใดรายหนึ่งเกิดปัญหาทางการเงินหรือล้มละลายทำให้ไม่สามารถจ่ายค่าสินไหมทดแทนได้ บริษัทฯ จะดำเนินการจัดหาผู้รับประกันภัยต่อทดแทนในสัดส่วนของผู้รับประกันภัยต่อรายนั้น



## 9. นโยบายการลงทุน

บริษัทฯ กำหนดให้มีการบริหารความเสี่ยงด้านการลงทุนและการบริหารเงินกองทุนดังนี้

- บริษัทฯ กำหนดให้กรอบนโยบายการลงทุนต้องสอดคล้องกับนโยบายการบริหารความเสี่ยงรวม การออกแบบผลิตภัณฑ์ การรับประกันภัย การทำสัญญาประกันภัยต่อ การบริหารทรัพย์สินและหนี้สิน ฐานะเงินกองทุนตามระดับความเสี่ยงที่ยอมรับได้ [Risk Appetite] ผลตอบแทนที่คาดหวังและความพร้อมของระบบและบุคลากรในการรองรับการลงทุนตามแผนการลงทุน สัดส่วนการลงทุนตามระยะเวลาของการรับประกันภัยและการทำสัญญาประกันภัยต่อ รวมทั้งอัตราผลตอบแทนและระดับความเสี่ยงที่มีผลกระทบต่อเงินกองทุนรวมของบริษัทฯ รวมถึงการลงทุนในบริษัทที่มีการดำเนินธุรกิจโดยคำนึงถึงสังคม สิ่งแวดล้อม และบรรษัทภิบาล [ESG] โดยทบทวนนโยบายปีละ 1 ครั้ง
- ความเสี่ยงด้านเครดิต [Credit Risk Management Policy] : กำหนดให้มีแนวทางการปฏิบัติในการประเมินความเสี่ยงด้านเครดิตของคู่สัญญา ผู้ออกตราสารหนี้ ที่อาจไม่สามารถปฏิบัติตามภาระที่ตกลงกันได้ รวมถึงโอกาสที่ผู้ออกตราสารหนี้จะถูกปรับลดอันดับความเสี่ยงด้านเครดิต
- ความเสี่ยงด้านตลาด [Market Risk Management Policy]
  - บริษัทฯ มีความเสี่ยงจากการลงทุนในตราสารหนี้ไปแล้วไม่ได้รับชำระเงินต้น และ/หรือโดยตราสารหนี้ที่บริษัทฯ มีการลงทุนสามารถแยกได้เป็น 2 ประเภท คือ 1] ตราสารหนี้ถือครบกำหนด และ 2] ตราสารหนี้เผื่อขาย ทั้งนี้การแยกประเภทขึ้นอยู่กับแผนการลงทุนประจำปีที่ได้รับอนุมัติตามคู่มืออำนาจดำเนินการ โดยกำหนดหลักเกณฑ์ในการเลือกลงทุนในตราสารหนี้และหลักเกณฑ์การ Stop Loss
  - บริษัทฯ มีความเสี่ยงจากการลงทุนในกองทุนรวม จึงต้องมีเกณฑ์การพิจารณาการลงทุนในกองทุนรวม เกณฑ์การพิจารณากองทุนที่จะทำการลงทุน และเกณฑ์ในการ Stop Lossทั้งนี้การดำเนินการในขั้นตอนการคัดเลือก การขายหน่วยลงทุน/เงินลงทุน และหลักเกณฑ์ในการ Stop Loss ให้เป็นไปตามระเบียบว่าด้วยการลงทุนประกอบธุรกิจอื่นที่ได้รับอนุมัติจากผู้มีอำนาจตามที่กำหนดในคู่มืออำนาจดำเนินการของบริษัทฯ
- ความเสี่ยงด้านการกระจุกตัว [Concentration Risk Management Policy] : การลงทุนต้องไม่ละเมิดกฎระเบียบการลงทุนตามประกาศการลงทุนของสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย [คปภ.]

## 10. นโยบายการบริหารสินทรัพย์และหนี้สิน

การบริหารสินทรัพย์ [Assets Management] หมายถึง กระบวนการในการจัดหาและใช้ประโยชน์จากสินทรัพย์อย่างคุ้มค่า รวมทั้งป้องกันมิให้สูญหายหรือเสียหายไป

- การบริหารจัดการสินทรัพย์และหนี้สิน [Asset Liability Management] เป็นเทคนิคเพื่อใช้สำหรับการจัดการความเสี่ยงในการบริหารงานและการลงทุนทุกประเภท บริหารเงินส่วนเกินของสินทรัพย์ [Asset] ที่มีค่ามากกว่าหนี้สิน [Liability] โดยตั้งอยู่ในเกณฑ์ความเสี่ยงที่บริษัทฯ รับผิดชอบได้ ซึ่งหนี้สินจากการรับประกันวินาศภัยส่วนใหญ่เป็นหนี้สินระยะสั้นซึ่งมีความเสี่ยงทางด้านดอกเบี้ยต่ำ
- กลยุทธ์การบริหารสินทรัพย์และหนี้สินของบริษัทฯ จึงเน้นไปทางการรักษาสภาพคล่องทางการเงินให้อยู่ในระดับที่เหมาะสมและเพียงพอ บริษัทฯ จึงมีการประมาณการกระแสเงินสดจ่ายหนี้สินอย่างสม่ำเสมอ และจัดสรรเงินลงทุนที่วันครบกำหนดและอัตราผลตอบแทนที่เหมาะสม เพื่อให้มีกระแสเงินสดรับที่สอดคล้องสัมพันธ์กับกระแสเงินสดจ่ายที่ประมาณการไว้ ซึ่งกระบวนการดังกล่าวได้จัดทำโดยฝ่ายลงทุน โดยใช้ข้อมูลประกอบจากฝ่ายบัญชีและการเงิน และหน่วยงานคณิตศาสตร์ประกันภัย
- กลยุทธ์การบริหารสินทรัพย์และหนี้สินเน้นไปทางการรักษาสภาพคล่องทางการเงินเพื่อให้เพียงพอที่จะจ่ายชำระหนี้สินที่มีต่อผู้ถือกรมธรรม์ จำนวนกรมธรรม์ และหนี้สินตามกรมธรรม์ประกันภัยจึงเป็นสิ่งที่บริษัทฯ นำมาใช้ในการพิจารณาตัดสินใจในการลงทุน ทั้งในเรื่องของระยะเวลาที่จะลงทุน และความเสี่ยงจากอัตราดอกเบี้ย

## 11. นโยบายการจัดจ้างบุคคลภายนอก

บริษัท เทเวศประกันภัย จำกัด [มหาชน] ได้มีการใช้บริการจากบุคคลภายนอกเพื่อลดต้นทุนการดำเนินงานและเพิ่มความคล่องตัวในการประกอบธุรกิจให้มีประสิทธิภาพมากยิ่งขึ้น ดังนั้นเพื่อสนับสนุนให้บริษัทฯ เพิ่มขีดความสามารถในการดำเนินงานและใช้ทรัพยากรของบริษัทฯ ในงานหลักที่สำคัญ รวมถึงการได้รับประโยชน์จากความเชี่ยวชาญเฉพาะด้านและเครือข่ายของผู้ให้บริการภายนอก บริษัทฯ จึงได้กำหนดนโยบายไว้ดังนี้

- กำหนดให้มีการปฏิบัติตามประกาศของสำนักงาน คปภ. เรื่อง แนวทางปฏิบัติในการใช้บริการจากบุคคลภายนอก [Outsourcing] ของบริษัทประกันภัย และแนวปฏิบัติเรื่อง หลักเกณฑ์การกำกับดูแลการใช้บริการจากผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศ ฉบับที่มีผลบังคับใช้ในปัจจุบัน
- การให้บริการงานชุดใช้ค่าสินไหมทดแทนตามกรมธรรม์ประกันภัย จะต้องเป็นไปตามข้อตกลงที่บริษัทฯ กำหนด
- การใช้บริการจากบุคคลภายนอก จะต้องเป็นไปตามหลักเกณฑ์การคัดเลือกและการพิจารณาคุณสมบัติของผู้ให้บริการ และมีกระบวนการว่าจ้างอย่างเหมาะสม ตามระบบบริหารงานคุณภาพ ISO 9001 และระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC 27001
- กำหนดให้มีการตรวจสอบและการบริหารความเสี่ยงด้าน ปปง. สำหรับคู่ค้าและการใช้บริการจากบุคคลภายนอก
- การควบคุมภายใน โดยดำเนินการตามระเบียบปฏิบัติงาน [Procedure] กำหนดให้มีการประเมินผลการดำเนินงานตามระบบบริหารงานคุณภาพ ISO 9001 และระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC 27001 ของบริษัทฯ ซึ่งต้องประเมินและทบทวนทุกปี รวมถึงการตรวจสอบและการควบคุมความเสี่ยงจากการใช้บริการจากบุคคลภายนอกที่อาจเกิดขึ้น
- ผู้ให้บริการบุคคลภายนอกจะต้องรักษาความปลอดภัยข้อมูลของบริษัทฯ และข้อมูลลูกค้า ซึ่งต้องไม่เปิดเผยข้อมูลส่วนบุคคลแก่ผู้อื่นที่ไม่มีส่วนเกี่ยวข้อง ตาม "สัญญาการประมวลผลข้อมูลส่วนบุคคล" รวมถึงการดำเนินการตาม "พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล" รวมถึงประกาศที่เกี่ยวข้อง ฉบับที่มีผลบังคับใช้ในปัจจุบัน
- กำหนดให้มีแผนฉุกเฉินของบริษัทฯ เพื่อรองรับกรณีงานที่ใช้บริการจากบุคคลภายนอกมีปัญหาหยุดชะงัก และไม่สามารถให้บริการได้อย่างต่อเนื่อง รวมถึงการบริหารจัดการในช่วงการเปลี่ยนแปลงจากการดำเนินการเองมาเป็นการใช้บริการจากบุคคลภายนอก มีปัญหาหยุดชะงักและไม่สามารถให้บริการได้อย่างต่อเนื่อง
- ผู้ให้บริการภายนอก จะต้องปฏิบัติตามข้อตกลงระดับการให้บริการ [Service Level Agreement : SLA] ตามที่กำหนด รวมถึงการดำเนินการตามนโยบาย แนวปฏิบัติ ที่บริษัทฯ กำหนด
- การติดตาม ประเมินผล ตรวจสอบ และควบคุมความเสี่ยงจากการใช้บริการจากผู้ให้บริการ
  - จัดให้มีระบบที่ชัดเจนในการกำกับดูแล ติดตาม ตรวจสอบ และประเมินผลผู้ให้บริการอย่างเหมาะสม เพื่อให้มีมาตรฐานการควบคุมภายในและการให้บริการเช่นเดียวกับบริษัทฯ ดำเนินการเอง รวมทั้งต้องตรวจสอบให้แน่ใจว่าทั้งบริษัทฯ เอง และผู้ให้บริการได้ปฏิบัติตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้อง โดยเคร่งครัด
  - จัดให้มีคู่มือการปฏิบัติงานและเอกสารที่เกี่ยวข้องตามระบบบริหารงานคุณภาพ ISO 9001 รวมทั้งปรับปรุงให้ทันสมัยอยู่เสมอ เพื่อประโยชน์ในการติดตามและประเมินผลและบริหารความเสี่ยงของบริษัทฯ
  - จัดให้มีพนักงานหรือหน่วยงานที่มีความเข้าใจในขอบเขต ลักษณะงาน และกระบวนการทำงานของผู้ให้บริการ เพื่อสามารถติดตามและประเมินผลการปฏิบัติงานของผู้ให้บริการได้อย่างถูกต้อง น่าเชื่อถือ
  - จัดให้มีการรายงานปัญหาที่เกิดขึ้นต่อผู้บริหารระดับสูงของบริษัทฯ ทราบทันที เพื่อสามารถแก้ไขปัญหาดังกล่าวได้อย่างทันท่วงที
  - จัดให้มีการทบทวนผู้ให้บริการเป็นระยะตามความเหมาะสม
  - กำหนดให้มีการจัดทำข้อมูลรายละเอียดเกี่ยวกับการใช้บริการจากผู้ให้บริการภายนอก หรือผู้รับจ้างช่วง [ถ้ามี] ให้มีความถูกต้องและเป็นปัจจุบัน เพื่อเตรียมพร้อมไว้สำหรับการตรวจสอบของสำนักงาน คปภ. และหน่วยงานอื่นที่เกี่ยวข้อง

## 12. นโยบายการบริหารความต่อเนื่องทางธุรกิจ

บริษัท เทเวศประกันภัย จำกัด [มหาชน] ได้ตระหนักถึงความสำคัญในการบริหารความต่อเนื่องทางธุรกิจ เนื่องจากปัจจุบันการดำเนินธุรกิจอาจต้องเผชิญกับความเสี่ยงที่สำคัญหลายด้าน เช่น บั๊จจ่ายเสี่ยงจากภัยคุกคามธรรมชาติหรือสิ่งแวดล้อมที่เปลี่ยนแปลงไป ภัยจากการชุมนุมทางการเมือง ภัยก่อการร้าย ภัยวินาศกรรม ภัยคุกคามทางไซเบอร์ [Cybersecurity] เป็นต้น ซึ่งบั๊จจ่ายเสี่ยงดังกล่าวอาจส่งผลกระทบต่อกรดำเนินธุรกิจ ชื่อเสียง และความเชื่อมั่น ของผู้มีส่วนเกี่ยวข้องหรือผู้มีส่วนได้ส่วนเสียกับบริษัทฯ

ดังนั้นบริษัทฯ จึงให้ความสำคัญในการบริหารความต่อเนื่องทางธุรกิจ โดยดำเนินการภายใต้แนวทางปฏิบัติของสำนักงาน คปภ. เรื่อง “การบริหารความต่อเนื่องทางธุรกิจ [Business Continuity Management : BCM] และการจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง [Business Continuity Plan : BCP] ของบริษัทประกันภัย” และ “การรักษาความปลอดภัยและควบคุมความเสี่ยงของระบบเทคโนโลยีสารสนเทศ [Information Technology Risk Management] และความเสี่ยงด้านภัยคุกคามทางไซเบอร์ [Cybersecurity]” เพื่อมั่นใจว่า ระบบการบริหารความต่อเนื่องทางธุรกิจมีประสิทธิภาพ และเมื่อเกิดเหตุการณ์วิกฤต บริษัทฯ สามารถดำเนินการได้อย่างต่อเนื่องหรือกลับมาดำเนินธุรกิจได้ในระยะเวลาที่เหมาะสม โดยมีสาระสำคัญดังนี้

- จัดให้มีกระบวนการในการกำกับดูแลการบริหารความต่อเนื่องทางธุรกิจอย่างต่อเนื่องและสม่ำเสมอ โดยกำหนดเป็นลายลักษณ์อักษร
- จัดให้มีการอบรมหรือเผยแพร่เกี่ยวกับองค์ความรู้ที่เกี่ยวกับการบริหารความต่อเนื่องทางธุรกิจให้กับบุคลากรของบริษัทฯ เพื่อเสริมสร้างความรู้ ความเข้าใจ และความตระหนัก ให้ทราบถึงความจำเป็นและความสำคัญของการบริหารความต่อเนื่องทางธุรกิจเป็นประจำทุกปี
- จัดให้มีคณะกรรมการบริหารจัดการในภาวะวิกฤต [Crisis Management Team : CMT] ซึ่งประกอบด้วยผู้บริหารระดับสูง ที่มีหน้าที่รับผิดชอบโดยตรงในการควบคุมและกำกับดูแลการบริหารความต่อเนื่องทางธุรกิจ รวมถึงผู้จัดการการบริหารความต่อเนื่องทางธุรกิจ [Business Continuity Manager] ที่มีหน้าที่รับผิดชอบในการประสานงานเมื่อเกิดภาวะวิกฤต
- จัดให้มีหน่วยงานซึ่งทำหน้าที่รับผิดชอบโดยตรง เป็นศูนย์กลางการประสานงานและทบทวนการประเมินความเสี่ยง [Risk Assessment : RA] การวิเคราะห์ผลกระทบทางธุรกิจ [Business Impact Analysis : BIA] และแผนความต่อเนื่องทางธุรกิจ [Business Continuity Plan : BCP] สำหรับหน่วยงานต่าง ๆ เป็นประจำทุกปี
- มอบหมายให้หน่วยงานหลักและหน่วยงานสนับสนุนจัดให้มีผู้บริหารและพนักงานรับผิดชอบโดยตรงในการจัดทำและทบทวนการประเมินความเสี่ยง [Risk Assessment : RA] การวิเคราะห์ผลกระทบทางธุรกิจ [Business Impact Analysis : BIA] และแผนความต่อเนื่องทางธุรกิจ [Business Continuity Plan : BCP] ตลอดจนการจัดเตรียมมาตรการรองรับการดำเนินธุรกิจอย่างต่อเนื่องในแต่ละหน่วยงาน
- มอบหมายให้ผู้บริหารสายสารสนเทศและผู้ที่เกี่ยวข้องจัดทำแผนรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ [Cyber Incident Response Plan : CIRP]
- จัดให้มีการทดสอบแผนความต่อเนื่องทางธุรกิจ [Business Continuity Plan : BCP] และแผนรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ [Cyber Incident Response Plan : CIRP] เพื่อทดสอบความพร้อมและซักซ้อมทำความเข้าใจให้กับบุคคลากรที่เกี่ยวข้องเป็นประจำทุกปี
- จัดให้มีการทบทวนแผนความต่อเนื่องทางธุรกิจ [Business Continuity Plan : BCP] แผนรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ [Cyber Incident Response Plan : CIRP] แผนรองรับสถานการณ์ฉุกเฉินทางด้าน IT [IT Contingency Plan] แผนรักษาความปลอดภัยอาคารและสถานที่ [Security Plan] และคู่มือการบริหารจัดการในภาวะวิกฤต [Crisis Management Guideline] เพื่อให้มีความทันสมัยอยู่เสมอเป็นประจำทุกปี

### 13. นโยบายการป้องกันและปราบปรามการฟอกเงิน การสนับสนุนทางการเงินแก่การก่อการร้าย และการแพร่ขยายอาวุธที่มีอานุภาพทำลายล้างสูง

บริษัท เทเวศประกันภัย จำกัด [มหาชน] ได้ตระหนักถึงความสำคัญในการปฏิบัติตามกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงิน และกฎหมายว่าด้วยการป้องกันและปราบปรามการสนับสนุนทางการเงินแก่การก่อการร้ายและการแพร่ขยายอาวุธที่มีอานุภาพทำลายล้างสูง เพื่อให้การปฏิบัติเป็นไปอย่างถูกต้อง ครบถ้วน ลดความเสี่ยงในการปฏิบัติงาน และสอดคล้องกับข้อกฎหมาย บริษัทฯ จึงได้กำหนดนโยบายในการดำเนินการโดยมีสาระสำคัญดังนี้

- บริษัทฯ มีหน้าที่และจรรยาบรรณในการสนับสนุนและพร้อมที่จะปฏิบัติตามกฎหมาย รวมถึงมีความมุ่งมั่นไม่ให้องค์กรเป็นแหล่งในการฟอกเงิน การสนับสนุนทางการเงินแก่การก่อการร้าย และการแพร่ขยายอาวุธที่มีอานุภาพทำลายล้างสูง โดยกำหนดให้มีมาตรการที่เกี่ยวข้อง คู่มือแนวทางการปฏิบัติ ระเบียบวิธีการประเมิน บริหาร และบรรเทาความเสี่ยง รวมถึงการให้ความรู้ความเข้าใจกับบุคลากรในการปฏิบัติตามกฎหมายอย่างเคร่งครัด
- บริษัทฯ กำหนดให้มีการประเมินความเสี่ยงภายในองค์กร โดยนำปัจจัยความเสี่ยงเกี่ยวกับลูกค้า พื้นที่หรือประเทศ ผลิตภัณฑ์หรือบริการ หรือช่องทางในการให้บริการ มาประกอบการพิจารณาประเมินความเสี่ยง โดยมีแนวทางในการพิจารณา ดังต่อไปนี้
  - ความเสี่ยงเกี่ยวกับลูกค้า ให้พิจารณาจากผลการประเมินความเสี่ยงของลูกค้าทั้งหมดภายในองค์กรตามปัจจัยความเสี่ยงที่กำหนดในประกาศสำนักงาน ปปง. เรื่อง แนวทางในการพิจารณาปัจจัยความเสี่ยงด้านการฟอกเงินหรือการสนับสนุนทางการเงินแก่การก่อการร้ายหรือการแพร่ขยายอาวุธที่มีอานุภาพทำลายล้างสูง
  - ความเสี่ยงเกี่ยวกับพื้นที่หรือประเทศ ให้พิจารณาจากสถานที่ตั้ง สาขา พื้นที่ให้บริการ หรือแหล่งที่มาของรายได้ขององค์กร ซึ่งอยู่ในพื้นที่เชิงภูมิศาสตร์หรือประเทศในข้อใดข้อหนึ่งที่จะทำให้เกิดความเสี่ยงสูงตามประกาศสำนักงาน ปปง. เรื่อง แนวทางในการพิจารณาปัจจัยความเสี่ยงด้านการฟอกเงินและการสนับสนุนทางการเงินแก่การก่อการร้ายหรือการแพร่ขยายอาวุธที่มีอานุภาพทำลายล้างสูง และประกาศสำนักงาน ปปง. เรื่อง พื้นที่หรือประเทศที่มีความเสี่ยงสูง ที่ต้องดำเนินการตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้าในระดับเข้มข้นและใช้มาตรการตอบโต้ อาจส่งผลให้องค์กรมีความเสี่ยงสูงขึ้น
  - ความเสี่ยงเกี่ยวกับผลิตภัณฑ์หรือบริการ ให้พิจารณาจากลักษณะผลิตภัณฑ์หรือบริการอย่างน้อยดังต่อไปนี้
    - ผลิตภัณฑ์หรือบริการที่สามารถให้ รับ หรือเปลี่ยนเป็นเงินสดได้ ซึ่งความเสี่ยงจะเพิ่มขึ้นตามจำนวนเงินสดที่ผลิตภัณฑ์หรือบริการนั้นสามารถรองรับได้
    - ผลิตภัณฑ์หรือบริการที่สามารถโอนหรือเปลี่ยนมือให้แก่บุคคลอื่นได้ ซึ่งความเสี่ยงจะเพิ่มขึ้นตามมูลค่า ความถี่ ความรวดเร็ว หรือความสะดวก ในการโอนหรือเปลี่ยนมือ
    - ผลิตภัณฑ์หรือบริการที่สามารถใช้หรือนำไปใช้ในต่างประเทศ ซึ่งความเสี่ยงจะเพิ่มขึ้นหากผลิตภัณฑ์หรือบริการนั้นสามารถใช้ข้ามประเทศได้
  - ความเสี่ยงเกี่ยวกับช่องทางในการให้บริการ โดยการให้บริการเพื่อสร้างความสัมพันธ์ทางธุรกิจหรือการทำธุรกรรมแบบไม่พบหน้าลูกค้า [Non-face-to-face] และแบบพบหน้าลูกค้า [face-to-face]
- บริษัทฯ กำหนดให้มีระเบียบวิธีการในการบริหารและบรรเทาความเสี่ยงภายในองค์กร และให้นำผลการประเมินและบริหารความเสี่ยงตามรายงานการประเมินความเสี่ยงระดับชาติที่ สำนักงาน ปปง. จัดทำขึ้นมาพิจารณาประกอบด้วย เพื่อสนับสนุนการปฏิบัติตามกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงิน และกฎหมายว่าด้วยการป้องกันและปราบปรามการสนับสนุนทางการเงินแก่การก่อการร้ายและการแพร่ขยายอาวุธที่มีอานุภาพทำลายล้างสูง โดยได้กำหนดและดำเนินการตามนโยบายและระเบียบวิธีการที่เป็นลายลักษณ์อักษรซึ่งมีสาระสำคัญ ดังต่อไปนี้
  - ในการรับลูกค้า บริษัทฯ กำหนดให้มีกระบวนการเพื่ออนุมัติการสร้างความสัมพันธ์ทางธุรกิจหรือการทำธุรกรรม หรือปฏิเสธการสร้างความสัมพันธ์ทางธุรกิจหรือการทำธุรกรรมกับลูกค้า โดยปฏิบัติตามหลักเกณฑ์การจัดให้ลูกค้าแสดงตน การระบุตัวตนของลูกค้า และการพิสูจน์ทราบตัวตนของลูกค้าตามกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงิน และการตรวจสอบข้อมูลของลูกค้าและผู้ได้รับผลประโยชน์ที่แท้จริงของลูกค้ากับข้อมูลรายชื่อบุคคลที่ถูกกำหนด ตามกฎหมายว่าด้วยการป้องกันและปราบปรามการสนับสนุนทางการเงินแก่การก่อการร้ายและการแพร่ขยายอาวุธที่มีอานุภาพทำลายล้างสูง ดังนี้
    - เพื่อให้บรรลุตามนโยบายและระเบียบวิธีการในการรับลูกค้า บริษัทฯ กำหนดให้มีแนวทาง หรือวิธีการ หรือคู่มือ เพื่อให้บุคลากรปฏิบัติ
    - การรับลูกค้าเริ่มตั้งแต่ขั้นตอนการขอหรือแสวงหาข้อมูลการแสดงตนของลูกค้า และการระบุตัวตนของลูกค้า การตรวจสอบข้อมูลของลูกค้า การพิสูจน์ทราบตัวตนของลูกค้า การหาผู้ได้รับผลประโยชน์ที่แท้จริงของลูกค้า การตรวจสอบรายชื่อบุคคลที่ถูกกำหนด และการอนุมัติหรือปฏิเสธการสร้างความสัมพันธ์ทางธุรกิจหรือการทำธุรกรรม นับแต่เมื่อได้รับแจ้งความประสงค์จากลูกค้า

- การบริหารและบรรเทาความเสี่ยง บริษัทฯ ได้กำหนดหลักการบริหารความเสี่ยงสำหรับลูกค้าทั้งหมด โดยต้องพิจารณาปัจจัยในการกำหนดความเสี่ยงไม่น้อยกว่าที่กฎหมายกำหนด และต้องดำเนินการบริหารและบรรเทาความเสี่ยงตลอดระยะเวลาที่ยังดำเนินการความสัมพันธ์ทางธุรกิจกับลูกค้าและสิ้นสุดลงเมื่อยุติความสัมพันธ์ทางธุรกิจกับลูกค้า ดังนี้
    - บริษัทฯ ต้องประเมินความเสี่ยงของลูกค้าตามหลักเกณฑ์ที่กฎหมายกำหนดเพื่อให้บรรลุนโยบายและระเบียบวิธีการบริหารความเสี่ยงพร้อมทั้งต้องจัดทำแนวทาง หรือวิธีการ หรือคู่มือเพื่อให้บุคลากรปฏิบัติ ในการบริหารความเสี่ยงของลูกค้าที่สร้างความสัมพันธ์ทางธุรกิจและบริการทุกประเภทและในทุกช่องทางที่ให้บริการ
    - การบริหารความเสี่ยง เริ่มตั้งแต่ขั้นตอนการประเมินเพื่อระบุและพิสูจน์ทราบตัวตนของลูกค้า การกำหนดระดับความเสี่ยงสำหรับลูกค้าแต่ละราย การตรวจสอบความเคลื่อนไหวในการทำธุรกรรมซึ่งสอดคล้องกับระดับความเสี่ยงของลูกค้า การตรวจทานข้อมูลการพิสูจน์ทราบลูกค้าซึ่งสอดคล้องกับระดับความเสี่ยงของลูกค้า การทบทวนการประเมินความเสี่ยง จนถึงการยุติความสัมพันธ์ทางธุรกิจกับลูกค้าแต่ละราย
  - การรายงานธุรกรรมมายังสำนักงาน ปปง. ให้กำหนดประเภทธุรกรรม วิธีการ และขั้นตอนในการรายงานธุรกรรมให้ชัดเจน
  - กำหนดให้มีมาตรการควบคุมภายในที่เหมาะสมกับความเสี่ยง ดังต่อไปนี้
    - กำหนดโครงสร้างในการกำกับดูแลโดยให้มีผลงานหรือพนักงานผู้รับผิดชอบที่ทำหน้าที่ในการกำกับดูแลการปฏิบัติงานให้เป็นไปตามกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงินและกฎหมายว่าด้วยการป้องกันและปราบปรามการสนับสนุนทางการเงินแก่การก่อการร้ายและการแพร่ขยายอาวุธที่มีอานุภาพทำลายล้างสูง และมีพนักงานระดับผู้บริหารเป็นผู้รับผิดชอบในการกำกับดูแลการปฏิบัติงานนั้น
    - การคัดเลือกพนักงานก่อนการว่าจ้างให้ปฏิบัติงานด้านการป้องกันและปราบปรามการฟอกเงิน และการป้องกันและปราบปรามการสนับสนุนทางการเงินแก่การก่อการร้ายและการแพร่ขยายอาวุธที่มีอานุภาพทำลายล้างสูง ให้มีขั้นตอนและวิธีการที่มีมาตรฐานในระดับสูงในการคัดเลือกบุคคล เช่น การตรวจสอบประวัติอาชญากรรม การตรวจสอบรายชื่อบุคคลที่ถูกกำหนด
    - จัดให้มีการอบรมพนักงานที่เกี่ยวข้องกับการปฏิบัติงานด้านการป้องกันและปราบปรามการฟอกเงิน และการป้องกันและปราบปรามการสนับสนุนทางการเงินแก่การก่อการร้ายและการแพร่ขยายอาวุธที่มีอานุภาพทำลายล้างสูง ให้มีความรู้ความเข้าใจเกี่ยวกับการป้องกันและปราบปรามการฟอกเงิน และการป้องกันและปราบปรามการสนับสนุนทางการเงินแก่การก่อการร้ายและการแพร่ขยายอาวุธที่มีอานุภาพทำลายล้างสูงตั้งแต่ก่อนเริ่มปฏิบัติงานและอย่างต่อเนื่องตลอดระยะเวลาที่ปฏิบัติงานนั้น เพื่อให้ปฏิบัติหน้าที่ตามกฎหมายได้อย่างถูกต้อง
    - กำหนดให้มีผลงานหรือพนักงานผู้รับผิดชอบในการตรวจสอบภายในที่เป็นอิสระจากการปฏิบัติงานด้านการป้องกันและปราบปรามการฟอกเงิน และการป้องกันและปราบปรามการสนับสนุนทางการเงินแก่การก่อการร้ายและการแพร่ขยายอาวุธที่มีอานุภาพทำลายล้างสูงภายในองค์กร เพื่อตรวจสอบการดำเนินงานและการปฏิบัติตามกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงินและกฎหมายว่าด้วยการป้องกันและปราบปรามการสนับสนุนทางการเงินแก่การก่อการร้ายและการแพร่ขยายอาวุธที่มีอานุภาพทำลายล้างสูง และจัดให้มีรายงานผลการตรวจสอบภายในต่อพนักงานระดับผู้บริหารที่มีหน้าที่ในการพิจารณาตัดสินใจในการดำเนินธุรกิจทราบด้วย
  - กำหนดให้มีมาตรการในการดำเนินงานเกี่ยวกับการร่วมใช้ข้อมูลระหว่างสำนักงานใหญ่และสาขา
  - กำหนดให้มีมาตรการเกี่ยวกับวิธีการ ขั้นตอน และรายละเอียดในการเก็บรักษาข้อมูลที่เกี่ยวข้องกับการจัดให้ลูกค้าแสดงตน ข้อมูลเกี่ยวกับกระบวนการตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้าและข้อมูลเกี่ยวกับการรายงานธุรกรรม
- บริษัทฯ กำหนดการพัฒนาและปรับปรุงนโยบาย คู่มือปฏิบัติงาน และระเบียบวิธีการที่กำหนดในนโยบาย โดยต้องได้รับการทบทวนเป็นระยะและปรับปรุงให้เป็นปัจจุบันอยู่เสมอ
  - บริษัทฯ กำหนดให้ผู้บริหารระดับสูงดำเนินการด้านการป้องกันและปราบปรามการฟอกเงิน และการสนับสนุนทางการเงินแก่การก่อการร้ายและการแพร่ขยายอาวุธที่มีอานุภาพทำลายล้างสูง โดยให้ความสำคัญดังนี้
    - กำหนดให้ผู้บริหารและพนักงาน รวมถึงตัวแทน/นายหน้าของบริษัทฯ จะต้องปฏิบัติตามนโยบาย และแนวทางปฏิบัติที่บริษัทฯ กำหนดอย่างเคร่งครัด รวมถึงกฎหมายที่เกี่ยวข้อง
    - ผู้บริหารระดับสูงกำหนดให้มีมาตรการควบคุมความเสี่ยงด้านการฟอกเงิน และการสนับสนุนทางการเงินแก่การก่อการร้ายและการแพร่ขยายอาวุธที่มีอานุภาพทำลายล้างสูง ที่อาจเกิดขึ้นจากการใช้ผลิตภัณฑ์หรือบริการต่าง ๆ ของบริษัทฯ
    - ผู้บริหารระดับสูงสนับสนุนและส่งเสริมให้พนักงานมีความตระหนักรู้ มีความรู้ความเข้าใจ รวมถึงจัดสรรทรัพยากรอย่างเหมาะสมในการปฏิบัติตามกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงิน และการสนับสนุนทางการเงินแก่การก่อการร้ายและการแพร่ขยายอาวุธที่มีอานุภาพทำลายล้างสูง ได้อย่างถูกต้อง และมีประสิทธิภาพ
    - ผู้บริหารระดับสูงมอบหมายพนักงานระดับผู้บริหารทำหน้าที่ในการกำกับดูแลการปฏิบัติตามกฎหมาย และติดต่อประสานงานกับสำนักงาน ปปง.

## 14. นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

บริษัท เทเวศประกันภัย จำกัด [มหาชน] ใต้นโยบายสารสนเทศเข้ามาสนับสนุนเพื่อเพิ่มประสิทธิภาพในการดำเนินธุรกิจ แต่หากระบบสารสนเทศไม่สามารถดำเนินการได้หรือมีความผิดพลาดในการให้บริการ ไม่ว่าจะด้วยสาเหตุใดก็ตาม อาจส่งผลกระทบต่อความเสียหายการดำเนินงานของบริษัทฯ ไม่มีความปลอดภัย และส่งผลกระทบต่อชื่อเสียงหรือความน่าเชื่อถือ ดังนั้นเพื่อยกระดับมาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของบริษัทฯ ให้อยู่ในระดับมาตรฐานสากล โดยอ้างอิงจาก ISO/IEC 27001 มาบังคับใช้กับผู้บริหาร พนักงาน และ ลูกจ้าง ซึ่งต้องร่วมมือกันป้องกันไม่ให้เกิดความเสียหาย หรือลดโอกาสที่จะเกิดความเสียหายต่อระบบสารสนเทศและเครือข่ายคอมพิวเตอร์บริษัทฯ จึงได้กำหนดนโยบายว่าด้วยการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขึ้น ซึ่งประกอบด้วย 16 ข้อ โดยมีรายละเอียดดังนี้

### 1. การจัดทำนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ [IT Security]

- สายสารสนเทศร่วมกับสำนักบริหารความเสี่ยง มีหน้าที่ทบทวนนโยบาย ซึ่งต้องได้รับการอนุมัติจากคณะกรรมการกำกับและดูแลความเสี่ยงสารสนเทศ ก่อนนำเสนอคณะกรรมการบริษัทฯ พิจารณานุมัติ ทั้งนี้กำหนดให้มีการทบทวนอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญต่อความมั่นคงปลอดภัยด้านสารสนเทศของบริษัทฯ
- บริษัทฯ กำหนดให้มีการอบรมหรือสื่อสารนโยบายและระเบียบปฏิบัติดังกล่าวไปยังผู้บริหาร พนักงาน ลูกจ้าง และผู้เกี่ยวข้องอย่างสม่ำเสมอเพื่อรับทราบ และสร้างความตระหนักเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ รวมถึงการนำไปปฏิบัติอย่างเคร่งครัด กรณีพนักงานพบผู้ไม่ปฏิบัติตามนโยบายฯ ระเบียบปฏิบัติ หรือกระทำการอันอาจก่อให้เกิดความเสี่ยงด้านความมั่นคงปลอดภัยด้านสารสนเทศ ให้แจ้งไปยังผู้บังคับบัญชาตามสายงาน ประสานงานมายังผู้ช่วยกรรมการผู้จัดการสายสารสนเทศเพื่อกำหนดแนวทางแก้ไขต่อไป

### 2. การบริหารจัดการทรัพย์สินด้านสารสนเทศ [IT Asset Management]

- บริษัทฯ จัดให้มีการบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศที่เหมาะสม โดยต้องมีการจัดทำทะเบียนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศ เพื่อให้สามารถระบุรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศได้อย่างครบถ้วน และสามารถนำไปใช้ในการกำหนดแนวทางการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศได้อย่างเหมาะสม รวมถึงต้องจัดให้มีการบำรุงรักษาทรัพย์สินด้านเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ เพื่อให้มีความพร้อมใช้งานและสามารถรองรับการดำเนินธุรกิจได้อย่างต่อเนื่อง ทั้งนี้ผู้ใช้งานจะต้องปฏิบัติตามข้อกำหนดเพื่อควบคุมไม่ให้เกิดความเสียหายหรือใช้งานผิดวัตถุประสงค์

### 3. การรักษาความมั่นคงปลอดภัยของข้อมูล [Information Security]

- บริษัทฯ จัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูล ทั้งในการรับส่งข้อมูลผ่านเครือข่ายสื่อสารและการจัดเก็บข้อมูลบนระบบงานและสื่อบันทึกข้อมูลต่าง ๆ มีการจัดชั้นความลับของข้อมูล [Information Classification] มีการเก็บรักษาและทำลายข้อมูลให้เหมาะสมกับชั้นความลับ และมีการบริหารจัดการการเข้ารหัสข้อมูล [Cryptography] ที่เชื่อถือได้และเป็นมาตรฐานสากล เพื่อรักษาความมั่นคงปลอดภัยและความลับของข้อมูล

### 4. การควบคุมการเข้าถึง [Access Control]

- บริษัทฯ จัดให้มีการควบคุมการเข้าถึงระบบปฏิบัติการ ระบบงาน และระบบฐานข้อมูล โดยกำหนดให้มีการบริหารจัดการสิทธิและตรวจสอบยืนยันตัวตนตามสิทธิที่กำหนดไว้ตามความจำเป็นในการใช้งานและระดับความเสี่ยง เพื่อป้องกันการเข้าถึงและเปลี่ยนแปลงระบบหรือข้อมูลโดยผู้ที่ไม่มีความรู้หรือไม่ได้ได้รับอนุญาต

### 5. การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม [Physical and Environmental Security]

- บริษัทฯ จัดให้มีการรักษาความมั่นคงปลอดภัยของศูนย์คอมพิวเตอร์ สถานที่ปฏิบัติงานที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ และพื้นที่ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศที่สำคัญ รวมทั้งมีระบบการป้องกันและกระบวนการในการบำรุงรักษาอุปกรณ์คอมพิวเตอร์ และระบบสาธารณูปโภค [Facility] ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นจากการบุกรุกหรือจากภัยธรรมชาติ และให้ความพร้อมใช้งานสามารถรองรับการดำเนินธุรกิจอย่างต่อเนื่อง

## 6. การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร [Communications Security]

- บริษัทฯ จัดให้มีการรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสารของบริษัทฯ เพื่อให้ระบบเครือข่ายสื่อสารและข้อมูลที่มีการรับส่งผ่านเครือข่ายสื่อสารมีความมั่นคงปลอดภัย และสามารถป้องกันการบุกรุกหรือภัยคุกคามที่อาจเกิดขึ้น

## 7. การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ [IT Operations Security]

บริษัทฯ จัดให้มีการรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ เพื่อให้การปฏิบัติงานด้านเทคโนโลยีสารสนเทศมีความมั่นคงปลอดภัย โดยต้องครอบคลุมในเรื่องดังต่อไปนี้

- การบริหารจัดการขีดความสามารถของระบบ และระบบสาธารณูปโภค [Capacity Management] เช่น การประเมินแนวโน้มการใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศ เพื่อให้สามารถบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศได้อย่างเพียงพอต่อการรองรับการดำเนินธุรกิจและสามารถวางแผนการจัดการเทคโนโลยีสารสนเทศให้รองรับการใช้งานในอนาคต
- การรักษาความมั่นคงปลอดภัยของเครื่องแม่ข่าย [Server] และอุปกรณ์ที่ใช้ปฏิบัติงานของผู้ใช้เทคโนโลยีสารสนเทศ [Endpoint] เช่น การติดตั้งโปรแกรมป้องกันไวรัส หรือระบบตรวจจับการแฝงตัวของโปรแกรมไม่ประสงค์ดี [Malware] หรือการโจมตีด้วยรูปแบบต่าง ๆ เพื่อป้องกันการรั่วไหลของข้อมูลหรือการเข้าใช้งานโดยไม่ได้รับอนุญาต
- การสำรองข้อมูล [Data Backup] ด้วยวิธีการและระยะเวลาที่เหมาะสม เช่น การสำรองข้อมูลประจำวัน เพื่อให้มีข้อมูลสำรองที่มีความพร้อมใช้งานในกรณีที่ระบบและข้อมูลหลักเกิดเหตุขัดข้องหรือได้รับความเสียหาย
- การจัดเก็บข้อมูลบันทึกเหตุการณ์ [Logging] ของเครื่องแม่ข่าย ระบบงาน และอุปกรณ์เครือข่ายที่สำคัญ เช่น การจัดเก็บและสอบทานบันทึกการเข้าถึงระบบ [Access Log] และบันทึกการดำเนินงาน [Activity Log] เพื่อให้สามารถติดตามและตรวจสอบการเข้าถึงและการใช้งานระบบหรือข้อมูลและใช้เป็นหลักฐานการทำธุรกรรมทางอิเล็กทรอนิกส์ให้แก่ผู้ใช้บริการ
- การติดตามดูแลระบบและเฝ้าระวังภัยคุกคาม [Security Monitoring] โดยมีกระบวนการหรือเครื่องมือในการตรวจจับเหตุการณ์ผิดปกติหรือภัยคุกคามที่มีผลกระทบต่อความมั่นคงปลอดภัยของระบบที่สำคัญ เช่น เครื่องมือในการติดตามและวิเคราะห์ภัยคุกคามทางไซเบอร์อย่างต่อเนื่อง เพื่อให้สามารถตรวจจับ ป้องกัน และรับมือเหตุการณ์ผิดปกติและภัยคุกคามได้อย่างทันท่วงที
- การบริหารจัดการช่องโหว่ [Vulnerability Management] ของระบบที่เหมาะสมตามระดับความเสี่ยง เพื่อให้ทราบถึงช่องโหว่และสามารถดำเนินการแก้ไขและป้องกันภัยคุกคามที่อาจเกิดขึ้นได้อย่างทันการณ์ โดยบริษัทฯ ต้องมีการประเมินช่องโหว่ของระบบงานสำคัญทุกระบบอย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ
- การทดสอบเจาะระบบ [Penetration Test] โดยจัดให้มีผู้เชี่ยวชาญภายใน หรือภายนอกที่มีความเป็นอิสระทำหน้าที่ทดสอบเจาะระบบ โดยเฉพาะระบบงาน [Application] และระบบเครือข่าย [Network] ที่มีการเชื่อมต่อกับระบบเครือข่ายสื่อสารสาธารณะ [Internet Facing] สม่ำเสมออย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เพื่อให้ทราบถึงช่องโหว่และสามารถดำเนินการแก้ไขและป้องกันภัยคุกคามที่อาจเกิดขึ้นได้อย่างทันการณ์
- การบริหารจัดการการเปลี่ยนแปลง [Change Management] โดยจัดให้มีกระบวนการในการบริหารจัดการการเปลี่ยนแปลงและควบคุมการเปลี่ยนแปลงอย่างรัดกุมและเพียงพอ เช่น การนำระบบขึ้นใช้งานจริง [System Deployment] การตั้งค่าระบบ [System Configuration] การติดตั้ง Patch เพื่อให้การเปลี่ยนแปลงเป็นไปตามวัตถุประสงค์ที่กำหนดไว้อย่างถูกต้องครบถ้วน และป้องกันการเปลี่ยนแปลงโดยที่ไม่ได้รับอนุญาต
- การบริหารจัดการการตั้งค่าระบบ [System Configuration Management] โดยจัดให้มีกระบวนการในการควบคุมการตั้งค่าของระบบที่ใช้งานจริง และมีการสอบทานการตั้งค่าอย่างสม่ำเสมอ เพื่อป้องกันข้อผิดพลาดในการปฏิบัติงาน
- การบริหารจัดการ Patch [Patch Management] โดยจัดให้มีกระบวนการในการควบคุมการติดตั้ง Patch ของระบบที่ใช้งานจริง เพื่อให้สามารถติดตั้ง Patch ที่สำคัญในการรักษาความมั่นคงปลอดภัยได้อย่างทันการณ์

## 8. การจัดหาและการพัฒนาระบบ [System Acquisition and Development]

- การจัดหาระบบ [System Acquisition] มีการกำหนดหลักเกณฑ์ที่ชัดเจนและเหมาะสม ในการคัดเลือกระบบและผู้ให้บริการ เช่น ความน่าเชื่อถือของระบบและผู้ให้บริการ การได้รับการรับรองตามมาตรฐานสากลหรือมาตรฐานด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้องที่ได้รับการยอมรับโดยทั่วไป [Certificate] ความมั่นคงปลอดภัยของระบบ การสนับสนุนและการบำรุงรักษาระบบ ข้อตกลงระดับการให้บริการ [Service Level Agreement : SLA] และบทปรับเพื่อให้มั่นใจว่าระบบและผู้ให้บริการสามารถตอบสนองต่อความต้องการในการดำเนินธุรกิจของบริษัทฯ ได้ รวมถึงต้องคำนึงถึงความยืดหยุ่นในการเปลี่ยนแปลงผู้ให้บริการ การเปลี่ยนแปลงเทคโนโลยี หรือการเปลี่ยนแปลงกลยุทธ์ในการดำเนินธุรกิจในอนาคต



- การพัฒนาระบบ [System Development] มีการออกแบบ พัฒนา และทดสอบระบบ เพื่อให้มั่นใจว่าระบบมีความถูกต้อง มั่นคงปลอดภัย เชื่อถือได้ พร้อมใช้งาน และมีความยืดหยุ่นเพียงพอที่จะรองรับการปรับปรุงเปลี่ยนแปลงระบบในอนาคต โดยต้องจัดให้มือน้อยในเรื่องดังต่อไปนี้
  - เอกสารความต้องการของระบบงาน [Requirement] และเอกสารรายละเอียดคุณสมบัติทางเทคนิค [Technical Specification] โดยครอบคลุมถึงเรื่องการรักษาความมั่นคงปลอดภัยของระบบงาน ข้อมูลต่างๆ รวมทั้งข้อมูลส่วนบุคคล กระบวนการในการทดสอบการดูแล และการติดตามความมั่นคงปลอดภัยในการใช้งาน
  - กระบวนการหรือเครื่องมือในการควบคุมเวอร์ชันของคำสั่งในการเขียนโปรแกรม [Source Code Version Control]
  - การแบ่งแยกบทบาทหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องในกระบวนการพัฒนาระบบ เช่น การแบ่งแยกระหว่างผู้พัฒนาระบบและผู้บำรุงระบบขึ้นใช้งานจริง
  - การแบ่งแยกสภาพแวดล้อมของระบบงานที่ใช้สำหรับการพัฒนา [Development] และการทดสอบ [Testing] ออกจากระบบงานที่ให้บริการจริง [Production]
  - การทดสอบระบบก่อนการใช้งานจริง เช่น ทดสอบการทำงานของแต่ละระบบ [Unit Test] ทดสอบการทำงานร่วมกันของระบบต่าง ๆ [System Integration Test] ทดสอบความพร้อมใช้งานตามกระบวนการและความต้องการของผู้ใช้งาน [User Acceptance Test] และทดสอบความปลอดภัยของระบบ [Security Test] ตามกระบวนการในการรักษาความมั่นคงปลอดภัยที่กำหนดในเอกสารรายละเอียดคุณสมบัติทางเทคนิค [Technical Specification]
  - การพัฒนาหรือการเปลี่ยนแปลงระบบที่เกี่ยวข้องกับการให้บริการหรือการทำธุรกรรมทางอิเล็กทรอนิกส์ ต้องจัดให้มีการทดสอบประสิทธิภาพ [Performance Test]
  - แนวทางในการควบคุมการรักษาความมั่นคงปลอดภัยและความลับของข้อมูลสำคัญที่นำไปใช้ในการทดสอบ
  - การจัดทำคู่มือและอบรมผู้ใช้งานระบบและผู้ดูแลระบบ

## 9. การบริหารจัดการเหตุการณ์ผิดปกติและปัญหา [IT Incident and Problem Management]

- บริษัทฯ จัดให้มีการบริหารจัดการเหตุการณ์ผิดปกติและปัญหาที่เกิดจากการใช้เทคโนโลยีสารสนเทศอย่างเหมาะสมและทันท่วงที โดยมีการบันทึก วิเคราะห์ และรายงานเหตุการณ์ผิดปกติและปัญหา และการแก้ไข ให้คณะกรรมการที่ได้รับมอบหมาย หรือผู้บริหารระดับสูงที่ได้รับมอบหมาย ทราบในระยะเวลาที่เหมาะสม นอกจากนี้ ต้องมีการวิเคราะห์สาเหตุที่แท้จริง [Root Cause] ของปัญหา เพื่อหาแนวทางแก้ไขจากสาเหตุที่แท้จริง และป้องกันไม่ให้เกิดเหตุการณ์ผิดปกติซ้ำในอนาคต

## 10. การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ [Business Continuity Plan]

- กำหนดให้มีคณะทำงานหรือหน่วยงานที่รับผิดชอบในการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษรให้เป็นไปตามนโยบายที่กำหนดไว้ และแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศดังกล่าวต้องได้รับอนุมัติโดยคณะกรรมการที่ได้รับมอบหมาย
- ในการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ ต้องคำนึงถึงลักษณะการดำเนินธุรกิจ ปริมาณธุรกรรม ความซับซ้อนของเทคโนโลยีสารสนเทศ และความเสี่ยงที่เกี่ยวข้องในการดำเนินธุรกิจ รวมทั้งการบริหารความเสี่ยงที่อาจเกิดจากเหตุการณ์ความเสียหายต่างๆ และความเสี่ยงทั่วไป เช่น ความเสี่ยงด้านปฏิบัติการ [Operational Risk] ความเสี่ยงด้านชื่อเสียง [Reputational Risk] และความเสี่ยงอื่นที่เกี่ยวข้อง เช่น ความเสี่ยงจากการพึ่งพาองค์กรอื่นในการดำเนินธุรกิจ [Interdependency Risk] ความเสี่ยงจากการกระจุกตัวของระบบงานหรือทรัพยากรที่สำคัญ [Concentration Risk] และความเสี่ยงที่มีผลกระทบต่อบริษัทฯ ผู้ให้บริการ ผู้มีส่วนได้เสีย และระบบบริษัทฯ [Systemic Risk]
- แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศต้องมีความเป็นไปได้ในทางปฏิบัติ สามารถนำมาใช้รองรับความเสียหายที่เกิดขึ้นได้จริง และสอดคล้องกับแนวปฏิบัติของสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย [คปภ.] โดยแผนฉุกเฉินดังกล่าวต้องครอบคลุมถึงการกำหนดระยะเวลาในการกู้คืนระบบ [Recovery Time Objective : RTO] และระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย [Recovery Point Objective : RPO] ที่สอดคล้องกับความสำคัญของระบบ รวมทั้งการกำหนดระยะเวลาสูงสุดที่ยอมให้ธุรกิจหยุดชะงัก [Maximum Tolerance Period Of Disruption : MTPD] เพื่อรองรับการดำเนินธุรกิจอย่างต่อเนื่องของบริษัทฯ และรองรับการเกิดเหตุการณ์ผิดปกติต่างๆ ที่อาจส่งผลให้เกิดการหยุดชะงักหรือเกิดความเสียหายต่อระบบ เช่น ภัยคุกคามทางไซเบอร์ ภัยธรรมชาติ เพื่อให้บริษัทฯ ดำเนินการกู้ระบบและกลับสู่การทำงานได้ตามปกติให้เร็วที่สุด
- ต้องจัดทำคู่มือหรือเอกสารประกอบการดำเนินการตามแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ รวมทั้งประชาสัมพันธ์แผนและฝึกอบรมเพื่อให้พนักงานทุกคนที่มีส่วนเกี่ยวข้องกับการดำเนินการตามแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศมีความเข้าใจและสามารถปฏิบัติตามแผนได้
- จัดให้มีการทบทวนและทดสอบการปฏิบัติตามแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศอย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

- จัดให้มีศูนย์คอมพิวเตอร์สำรอง [Disaster Recovery Site] ที่มีความพร้อมใช้งานและสามารถปฏิบัติงานทดแทนได้เมื่อศูนย์คอมพิวเตอร์หลัก [Primary Site] หยุดชะงัก โดยพิจารณาให้ศูนย์คอมพิวเตอร์สำรองอยู่ห่างจากศูนย์คอมพิวเตอร์หลักเพียงพอที่จะมิให้เกิดปัญหาหรือได้รับผลกระทบในลักษณะเดียวกันในช่วงเวลาเดียวกัน เช่น ระบบไฟฟ้าขัดข้อง และภัยธรรมชาติ

## 11. การบริหารจัดการผู้ให้บริการสารสนเทศภายนอก [IT Third Party Management]

การจัดจ้างผู้ให้บริการสารสนเทศภายนอก หรือมีพันธมิตรทางธุรกิจที่มีการเชื่อมต่อกับระบบเทคโนโลยีสารสนเทศของบริษัทฯ ที่สามารถเข้าถึงข้อมูลสำคัญของบริษัทหรือของลูกค้าของบริษัทฯ และมีผลต่อการดำเนินธุรกิจของบริษัทแบบมีนัยสำคัญ ต้องมีการดำเนินการดังต่อไปนี้

- บริษัทฯ จัดให้มีการกำกับดูแลและการบริหารจัดการความเสี่ยงจากการใช้บริการจากผู้ให้บริการสารสนเทศภายนอก รวมถึงการใช้บริการระบบคลาวด์ โดยกำหนดกลยุทธ์ที่ชัดเจนในการตัดสินใจใช้บริการจากผู้ให้บริการภายนอก กำกับดูแลและพิจารณาให้เห็นชอบการใช้บริการ IT outsourcing ของบริษัทฯ ให้สอดคล้องกับกลยุทธ์ในการดำเนินธุรกิจ โดยคำนึงขนาดปริมาณธุรกรรมความซับซ้อนของงานเทคโนโลยีสารสนเทศที่ใช้บริการและความเสี่ยงที่เกี่ยวข้องกับการใช้บริการ
- บริษัทฯ มีการกำหนดกระบวนการและหลักเกณฑ์ที่ชัดเจนในการคัดเลือกผู้ให้บริการภายนอก และมีการตรวจสอบความพร้อม และพิจารณาความเหมาะสมของผู้ให้บริการภายนอก เพื่อให้มั่นใจว่าผู้ให้บริการภายนอกจะสามารถให้บริการได้อย่างต่อเนื่อง และสามารถตอบสนองความต้องการของบริษัทได้ ทั้งนี้ การตัดสินใจในการใช้บริการที่มีความเสี่ยงหรือมีนัยสำคัญต้องได้รับความเห็นชอบจากคณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมาย
- บริษัทฯ จัดให้มีการจัดทำสัญญาการใช้บริการจากผู้ให้บริการภายนอก หรือมีการจัดทำข้อตกลงการให้บริการ [service level agreement: SLA] เป็นลายลักษณ์อักษร และเงื่อนไขในการให้บริการอย่างชัดเจน เช่น การรักษาความมั่นคงปลอดภัยทางสารสนเทศตามมาตรฐาน ISO/IEC 27001:2013 การทำลายข้อมูลของบริษัทฯ หรือของลูกค้าทั้งหมดเมื่อสิ้นสุดสัญญาหรือเลิกใช้บริการ ความรับผิดชอบต่อการรั่วไหลของข้อมูลอันเนื่องมาจากการนำข้อมูลไปใช้นอกเหนือจากที่ระบุไว้ในสัญญาหรือข้อตกลงการให้บริการโดยรายละเอียดของสัญญาและข้อตกลงการให้บริการ โดยพิจารณาให้ครอบคลุมตามระดับความเสี่ยงและความมีนัยสำคัญของการใช้บริการ
- บริษัทฯ จัดให้มีการติดตามการใช้บริการจากผู้ให้บริการภายนอกโดยครอบคลุมเรื่อง การรายงานเหตุการณ์ผิดปกติ การทบทวนเพื่อประเมินประสิทธิภาพ และความเสี่ยงจากการใช้บริการของผู้ให้บริการภายนอกอย่างสม่ำเสมอ
- บริษัทฯ จัดให้มีแนวทางในการบริหารจัดการเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ อันเนื่องมาจากการใช้บริการจากผู้ให้บริการสารสนเทศภายนอก
- บริษัทฯ จัดให้มีแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง [business continuity plan: BCP] ที่ครอบคลุมถึงการใช้บริการจากผู้ให้บริการสารสนเทศภายนอก
- บริษัทฯ จัดให้มีการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศในการใช้บริการจากผู้ให้บริการสารสนเทศภายนอกโดยคำนึง 3 ด้าน CIA การรักษาความลับ [Confidentiality], ความถูกต้องเชื่อถือได้ [Integrity] และ ความพร้อมใช้งาน [Availability]

## 12. การบริหารจัดการความมั่นคงปลอดภัย ด้านทรัพยากรบุคคล [Human Resource Security]

- บริษัทฯ จัดให้มีกระบวนการคัดเลือกบุคลากร โดยระบุข้อกำหนดหรือเงื่อนไขในสัญญาจ้างงานของบุคลากรในเรื่องความรับผิดชอบเกี่ยวกับการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของบริษัทฯ

## 13. การบริหารจัดการความมั่นคงปลอดภัยทางไซเบอร์ [Cyber Security Management]

- บริษัทฯ จัดให้มีการ ตั้งคณะทำงานที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์โดยกำหนดบทบาทหน้าที่ให้ เป็นไปตามกรอบปฏิบัติการตามที่สากลยอมรับ หรือใช้กรอบปฏิบัติการ NIST CyberSecurity Framework
- โดยคณะทำงานจัดทำประเมินความเสี่ยงทางไซเบอร์ และจัดทำแผนรับมือภัยทางไซเบอร์และทบทวนแผนรวมทั้งซ้อมแผนรับมือภัยทางไซเบอร์อย่างน้อยปีละ 1 ครั้ง
- คณะทำงานมีแผนงานการอบรมความรู้เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ให้บุคลากรของบริษัทฯ อย่างน้อยปีละ 1 ครั้ง

## 14. การแบ่งแยกหน้าที่สารสนเทศ [Segregation of Duties]

- บริษัทฯ จัดให้มีการแบ่งแยกหน้าที่ความรับผิดชอบและการควบคุมของผู้ปฏิบัติงานสารสนเทศให้ชัดเจนไม่ทับซ้อนกัน หรือเอื้อต่อการทุจริต เพื่อลดโอกาสที่จะเกิดความผิดพลาดจากการปฏิบัติงานและโอกาสการทุจริตของผู้ปฏิบัติงานโดยมีสาเหตุจากที่ไม่ได้จำกัดสิทธิในการเข้าถึงระบบงาน โปรแกรม และข้อมูล

## 15. การปฏิบัติตามข้อกำหนด [Compliance]

- บริษัทฯ จัดให้มีขั้นตอนปฏิบัติที่เหมาะสม เพื่อให้มั่นใจว่าสอดคล้องกับกฎหมายกฎหมาย ระเบียบข้อบังคับ ข้อกำหนด หรือข้อผูกพันตามสัญญาที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศ และข้อกำหนดด้านความมั่นคงปลอดภัยใด ๆ ก็ตาม รวมถึงสิทธิในทรัพย์สินทางปัญญา และการใช้ซอฟต์แวร์ที่มีกรรมสิทธิ์ [Intellectual property rights] โดยต้องมีการนำไปปฏิบัติและมีการดำเนินงานตามนโยบายและขั้นตอนปฏิบัติงานของบริษัทฯ

## 16. บทกำหนดโทษ

- เพื่อให้นโยบายการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศของบริษัทฯ ดำเนินการได้อย่างมีประสิทธิภาพ จึงกำหนดโทษสำหรับผู้กระทำการฝ่าฝืนข้อห้ามและข้อกำหนดต่างๆ ดังนี้ ถ้าพนักงานผู้ใดกระทำการฝ่าฝืนตามข้อห้ามในนโยบายการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ ต้องได้รับโทษทางวินัยตามข้อบังคับของบริษัทฯ รวมถึงต้องระวางโทษตามที่ระบุไว้ในพระราชบัญญัติลิขสิทธิ์ และพระราชบัญญัติคอมพิวเตอร์ ฉบับที่มีผลบังคับใช้ในปัจจุบัน

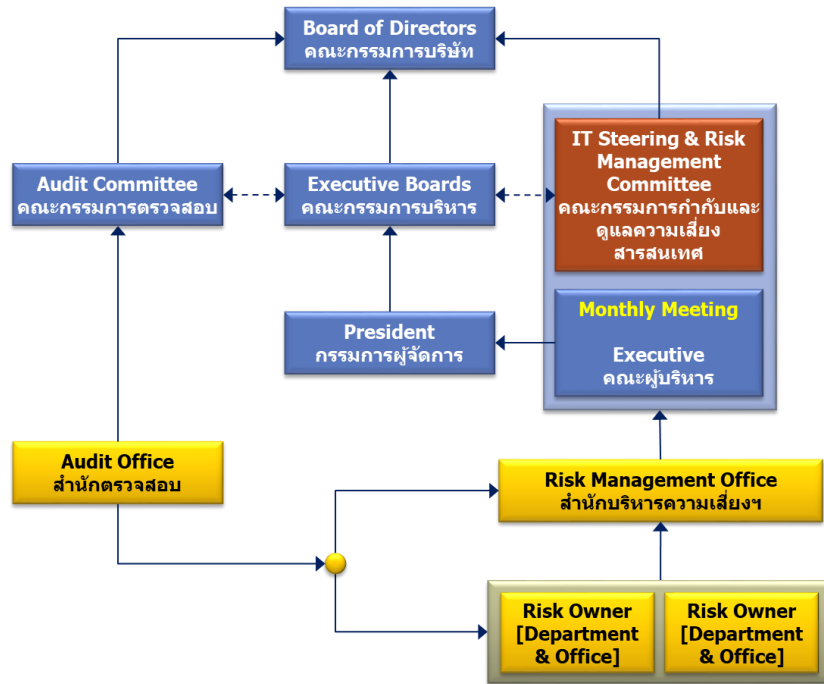
## 15. นโยบายการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ปัจจุบันเทคโนโลยีสารสนเทศได้เข้ามามีบทบาทสำคัญต่อการดำเนินธุรกิจของบริษัทฯ ในด้านต่างๆ อย่างไรก็ดี แม้ว่าการใช้เทคโนโลยีสารสนเทศจะช่วยให้การดำเนินธุรกิจมีประสิทธิภาพมากขึ้น และช่วยลดตอบสนองความต้องการของลูกค้าได้ดีขึ้น แต่หากขาดการบริหารจัดการความเสี่ยงที่ดี การใช้เทคโนโลยีสารสนเทศดังกล่าวอาจก่อให้เกิดความเสี่ยงด้านเทคโนโลยีสารสนเทศ [IT Risk] และภัยคุกคามทางไซเบอร์ [Cyber Threat] ที่ส่งผลกระทบต่อบริษัทฯ ทั้งในด้านความเสียหายที่เป็นจำนวนเงินและความเสียหายด้านชื่อเสียง ดังนั้นบริษัทฯ จึงได้กำหนดนโยบายการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ [IT Risk Management] โดยแบ่งเป็น 7 หมวด ดังนี้

### 1. หน้าที่และความรับผิดชอบ

- คณะกรรมการบริษัทฯ มีหน้าที่ ดังต่อไปนี้
  - กำกับดูแลการใช้เทคโนโลยีสารสนเทศให้สอดคล้องกับกลยุทธ์ในการดำเนินธุรกิจให้มีความยืดหยุ่นเพียงพอที่จะรองรับการเปลี่ยนแปลงด้านเทคโนโลยีสารสนเทศ และคำนึงถึงการเปลี่ยนแปลงการดำเนินธุรกิจในอนาคต รวมทั้งความพร้อมในการรับมือภัยคุกคามทางไซเบอร์
  - กำกับดูแลให้มีการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ และความเสี่ยงจากภัยคุกคามทางไซเบอร์ ที่อาจเกิดขึ้นจากการนำเทคโนโลยีสารสนเทศมาใช้ดำเนินธุรกิจ โดยให้ถือเป็นความเสี่ยงหลักที่สำคัญในภาพรวมระดับองค์กร และให้เป็นส่วนหนึ่งของการบริหารความเสี่ยงแบบองค์รวม
  - กำกับดูแลให้มีการกำหนดนโยบายที่เกี่ยวข้องกับการกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ และความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่เป็นลายลักษณ์อักษร ซึ่งมีรายละเอียดอย่างน้อย ดังต่อไปนี้
    - นโยบายการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ [IT Risk Management Policy]
    - นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ [IT Security Policy] ซึ่งต้องมีแผนงานหรือแนวทางในการดำเนินการที่อย่างน้อยต้องครอบคลุมในเรื่อง ดังต่อไปนี้
      - แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ [IT Continuity]
      - แผนหรือแนวทางในการกำกับดูแลและบริหารจัดการความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
  - กำกับดูแลให้บริษัทมีนโยบายที่ได้รับรองอนุมัติมาจัดทำแนวปฏิบัติในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ รวมถึงดูแลให้มีการนำไปปฏิบัติอย่างเหมาะสม และมีการทบทวนนโยบายและแนวทางปฏิบัติอย่างน้อยปีละหนึ่งครั้ง หรือทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ
  - กำกับดูแลให้มีการรายงานต่อคณะกรรมการบริษัทฯ หรือคณะกรรมการชุดย่อยที่ได้รับมอบหมาย อย่างน้อยในเรื่อง ดังต่อไปนี้
    - การรายงานผลการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศในภาพรวมของบริษัท ต้องมอบหมายให้หัวหน้าหน่วยงานบริหารความเสี่ยงเป็นผู้รายงานต่อคณะกรรมการบริษัทฯ หรือคณะกรรมการชุดย่อยที่ได้รับมอบหมาย
    - ข้อมูลเกี่ยวกับปัญหาหรือเหตุการณ์ด้านเทคโนโลยีสารสนเทศที่สำคัญ หรือที่อาจส่งผลกระทบต่อธุรกิจในวงกว้าง หรือส่งผลกระทบต่อชื่อเสียงของบริษัท หรือต่อการดำเนินการและการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ
    - ผลการทดสอบและการปฏิบัติตามแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ
- คณะกรรมการกำกับและดูแลความเสี่ยงสารสนเทศ มีหน้าที่ในการจัดทำและทบทวนนโยบาย นำเสนอคณะกรรมการบริษัทฯ เพื่อพิจารณาอนุมัติ โดยกำหนดให้มีการทบทวนนโยบายอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญต่อความเสี่ยงด้านเทคโนโลยีสารสนเทศ ทั้งนี้ให้คณะกรรมการกำกับและดูแลความเสี่ยงสารสนเทศ มีหน้าที่ทบทวนการระบุความเสี่ยง การประเมินความเสี่ยง การติดตามตัวชี้วัด และรายงานผลการบริหารจัดการความเสี่ยงต่อคณะกรรมการบริษัทฯ อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญต่อความเสี่ยงด้านเทคโนโลยีสารสนเทศ
- ผู้บริหารสายสารสนเทศและผู้ที่เกี่ยวข้อง มีหน้าที่ระบุความเสี่ยงในงานที่เกี่ยวข้อง เพื่อประเมินความเสี่ยงและจัดลำดับในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ พร้อมทั้งกำหนดมาตรการบริหารจัดการความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้ และจัดทำรายงานผล นำเสนอต่อผู้ช่วยกรรมการผู้จัดการสายสารสนเทศพิจารณา ก่อนขอความเห็นชอบร่วมกับคณะกรรมการกำกับและดูแลความเสี่ยงสารสนเทศ

## โครงสร้างการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ



### 2. กระบวนการในการประเมินความเสี่ยงและจัดการความเสี่ยง

- การระบุความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ [IT-Related Risk]
  - กำหนดให้ผู้บริหารสายสารสนเทศหรือผู้บริหารที่เกี่ยวข้อง ทำการระบุความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ รวมถึงภัยคุกคามทางไซเบอร์ และช่องโหว่ต่าง ๆ โดยให้มีรายละเอียดดังนี้
    - ผู้กระทำให้เกิดความเสี่ยงและเหตุการณ์ความเสี่ยง เช่น ผู้ไม่ประสงค์ดี ภัยคุกคาม หรือช่องโหว่ เป็นต้น
    - ประเภทของความเสี่ยง เช่น ความเสี่ยงด้านการปฏิบัติงานเทคโนโลยีสารสนเทศ ความเสี่ยงด้านโปรแกรม ความเสี่ยงด้านข้อมูล ความเสี่ยงด้านบุคลากร ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ ความเสี่ยงด้านการบริหารโครงการ เป็นต้น
    - วัน เวลา สถานที่ ช่วงเวลาหรือระยะเวลาที่เกิดเหตุการณ์ผิดปกติหรือความเสี่ยงด้านเทคโนโลยีสารสนเทศ [ถ้ามี]
    - สาเหตุของการเกิดเหตุการณ์ เช่น กระบวนการปฏิบัติงาน ระบบงาน บุคลากร บั๊กจ๊ายภายนอก เป็นต้น
    - ผลกระทบต่อทรัพย์สิน ทรัพยากร การปฏิบัติงานด้านเทคโนโลยีสารสนเทศ และการดำเนินธุรกิจของบริษัทฯ
- ผู้บริหารสายสารสนเทศหรือผู้บริหารที่เกี่ยวข้องประเมินความเสี่ยงที่ครอบคลุมถึงโอกาสหรือความถี่ที่จะเกิดความเสี่ยงและผลกระทบที่จะเกิดขึ้นเพื่อจัดลำดับความสำคัญในการบริหาร และกำหนดวิธีการหรือเครื่องมือในการบริหารจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

### 3. ระดับความเสี่ยงที่ยอมรับได้ [IT risk appetite]

- ผู้บริหารสายสารสนเทศหรือผู้บริหารที่เกี่ยวข้อง รับผิดชอบการกำหนดระดับความเสี่ยง และช่วงเบี่ยงเบนที่ยอมรับได้ของความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ โดยพิจารณาจากสถิติข้อมูลย้อนหลัง [ถ้ามี]

### 4. เกณฑ์การประเมินความเสี่ยง

เพื่อการบริหารจัดการความเสี่ยงอย่างเหมาะสม จึงกำหนดให้ปฏิบัติดังนี้

- กำหนดเจ้าของความเสี่ยงด้านเทคโนโลยีสารสนเทศ [Risk Owner]
- ระบุการควบคุมที่มีอยู่ในปัจจุบัน [Existing Control]
- พิจารณาและค้นหาสาเหตุและสถานการณ์ที่เป็นไปได้
- วิเคราะห์ผลกระทบที่เกิดขึ้นจากเหตุการณ์ความเสี่ยงด้านเทคโนโลยีสารสนเทศ
- การประเมินความเสี่ยงและจัดลำดับในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ให้ปฏิบัติดังนี้
  - กำหนดเกณฑ์การประเมินความเสี่ยงด้านโอกาสและผลกระทบ เช่น ด้านการเงิน ด้านปฏิบัติการ เป็นต้น
  - กำหนดระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ยอมรับได้ [IT Risk Appetite]
  - ประเมินค่าโอกาสและผลกระทบของเหตุการณ์ความเสี่ยงที่อาจเกิดขึ้น เพื่อระบุระดับค่าความเสี่ยงของแต่ละเหตุการณ์ความเสี่ยงด้านเทคโนโลยีสารสนเทศ

- จัดลำดับความเสี่ยงด้านเทคโนโลยีสารสนเทศแสดงในแผนภาพความเสี่ยงด้านเทคโนโลยีสารสนเทศ

## 5. วิธีการในการบริหารและจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

เพื่อให้ความเสี่ยงที่เหลืออยู่ [Residual Risk] อยู่ในระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ยอมรับได้ [IT Risk Appetite] ให้ปฏิบัติดังนี้

- กำหนดแนวทางในการจัดการและควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยการเลือกแนวทางการจัดการและควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศ ควรพิจารณาถึงความคุ้มค่าและวิธีการที่เหมาะสมสำหรับบริษัทฯ
- ระบุรายละเอียดของงานที่ต้องดำเนินการ ผู้รับผิดชอบ ระยะเวลาที่ใช้ในการดำเนินการ
- ประเมินระดับค่าความเสี่ยงที่เหลืออยู่ [Residual Risk] ว่าอยู่ในระดับความเสี่ยงที่ยอมรับได้
- จัดทำแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยจัดลำดับความสำคัญในการดำเนินการ
- นำเสนอและขออนุมัติแผนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ
- ดำเนินการสื่อสารแผนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

## 6. การกำหนดดัชนีชี้วัดความเสี่ยง [IT risk indicator]

ผู้บริหารสายสารสนเทศหรือผู้บริหารที่เกี่ยวข้อง รับผิดชอบในการกำหนดดัชนีชี้วัดความเสี่ยงด้านเทคโนโลยีสารสนเทศ [IT Key Risk Indicators] และทบทวนความเสี่ยงด้านเทคโนโลยีสารสนเทศให้อยู่ภายใต้ระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ยอมรับได้ [IT Risk Appetite] โดยจัดให้มีการจัดเก็บและบันทึกข้อมูลอย่างเป็นระบบเพื่อใช้ติดตามและทบทวนความเสี่ยงได้อย่างมีประสิทธิภาพ โดยให้ปฏิบัติดังนี้

- ดำเนินงานตามแผนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างต่อเนื่อง
- ประสานงานร่วมกับผู้รับผิดชอบและผู้บริหารถึงสถานะดำเนินงาน อุปสรรคและข้อจำกัดที่เกิดขึ้น
- ศึกษาและวิเคราะห์เหตุการณ์ความเสี่ยงที่เกิดขึ้น รวมทั้งติดตามแนวโน้มของเหตุการณ์ความเสี่ยงด้านเทคโนโลยีสารสนเทศที่อาจเกิดขึ้นกับบริษัทฯ
- รายงานความคืบหน้าของแผนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

## 7. การรายงานความเสี่ยง [risk reporting]

คณะกรรมการกำกับและดูแลความเสี่ยงสารสนเทศ รับผิดชอบในการติดตาม และรายงานผลการประเมินการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศโดยเชื่อมโยงกับความเสี่ยงในระดับองค์กร และรายงานแนวโน้มความเสี่ยงด้านเทคโนโลยีสารสนเทศที่อาจจะเกิดขึ้นต่อคณะกรรมการที่ได้รับมอบหมาย อย่างน้อยไตรมาสละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เพื่อให้มั่นใจว่าบริษัทฯ มีการบริหารความเสี่ยง ด้านเทคโนโลยีสารสนเทศที่เหมาะสมและต่อเนื่อง โดยการรายงานมีรายละเอียดดังนี้

- สถานะและผลลัพธ์การดำเนินงานตามแผนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศประจำปี
- ผลการประเมินและการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยเชื่อมโยงกับความเสี่ยงระดับองค์กร
- รายงานดัชนีชี้วัดความเสี่ยงด้านเทคโนโลยีสารสนเทศและรายงานสรุปเหตุการณ์ผิดปกติ
- แนวโน้มความเสี่ยงด้านเทคโนโลยีสารสนเทศที่อาจจะเกิดขึ้นกับบริษัทฯ
- ความคืบหน้าของการดำเนินงานตามแผนการบริหารจัดการความเสี่ยง

## 16. นโยบายคุ้มครองข้อมูลส่วนบุคคล

### 16.1 นโยบายคุ้มครองข้อมูลส่วนบุคคล [ลูกค้าและผู้มุ่งหวัง]

บริษัท เทเวศประกันภัย จำกัด [มหาชน] ตระหนักดีถึงสิทธิในความเป็นส่วนตัวและความรับผิดชอบของบริษัทฯ เกี่ยวกับการเก็บรวบรวม การใช้ การเปิดเผย ["การประมวลผล"] ข้อมูลส่วนบุคคลของท่าน บริษัทฯ จึงได้จัดทำ นโยบายคุ้มครองข้อมูลส่วนบุคคล [นโยบายฯ] ฉบับนี้ขึ้นมา เพื่อแจ้งรายละเอียดเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลของท่านตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ["พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล"]

#### 1. บทนิยาม

**"ข้อมูลส่วนบุคคล"** หมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

**"ข้อมูลส่วนบุคคลที่มีความอ่อนไหว"** หมายถึง ข้อมูลตามที่กำหนดไว้ในมาตรา 26 พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล และฉบับปรับปรุงแก้ไขตามที่จะมีการแก้ไขเป็นคราว ๆ กฎหมายและกฎระเบียบที่ใช้บังคับอื่น รวมถึงข้อมูลบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในตนเองเดียวกัน

**"พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล"** หมายถึง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 รวมถึงกฎหมายลำดับรองที่อาศัยอำนาจ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลในการตราขึ้น และตามที่จะมีการแก้ไขเป็นครั้งคราว

**"คณะกรรมการ"** หมายถึง คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

**"สำนักงาน"** หมายถึง สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย

#### 2. ข้อมูลส่วนบุคคลใดบ้างที่บริษัทฯ จะเก็บรวบรวม

บริษัทฯ จะประมวลผลข้อมูลส่วนบุคคล ซึ่งอาจรวมถึงข้อมูลส่วนบุคคลที่มีความอ่อนไหวของท่านดังต่อไปนี้

##### 2.1 ข้อมูลส่วนบุคคลทั่วไป

[ก] ข้อมูลส่วนบุคคลที่เกี่ยวกับท่านเป็นการทั่วไป เช่น ชื่อ นามสกุล เลขบัตรประจำตัวประชาชน วันเกิด อายุ อาชีพ เพศ สถานภาพทางการสมรส รูปถ่าย หมายเลขโทรศัพท์บ้าน หมายเลขโทรศัพท์เคลื่อนที่ ที่อยู่ตามทะเบียนบ้าน ที่อยู่เพื่อจัดส่งไปรษณีย์ เลขที่หนังสือเดินทาง อีเมล และรายละเอียดข้อมูลติดต่ออื่น ๆ

[ข] ข้อมูลเกี่ยวกับการทำงานของท่าน เช่น ตำแหน่งงาน สถานที่ทำงาน ประวัติเกี่ยวกับการทำงานของท่าน ซึ่งอาจรวมถึงชื่อและที่อยู่ของนายจ้างของท่าน

[ค] ข้อมูลทางการเงิน เช่น รายได้ แหล่งที่มาของรายได้ เลขบัญชีธนาคาร ข้อมูลเกี่ยวกับภาษี รายละเอียดเกี่ยวกับการเคลื่อนไหวของบัญชีธนาคาร รายละเอียดเกี่ยวกับเงินกู้ ข้อมูลเกี่ยวกับการลงทุน รายละเอียดเกี่ยวกับบัตรเครดิต และรายละเอียดหรือข้อมูลเกี่ยวกับการชำระเงินอื่น ๆ

[ง] รายละเอียดผลิตภัณฑ์และ/หรือบริการต่าง ๆ ได้แก่ รายละเอียดผลิตภัณฑ์และ/หรือบริการต่าง ๆ ที่ท่านเคยซื้อจากบริษัทฯ หรือผู้ประกอบการธุรกิจประกันภัยอื่น ๆ เช่น หมายเลขกรมธรรม์ จำนวนเงินเอาประกันภัย การเปลี่ยนแปลง/การทำธุรกรรมเกี่ยวกับกรมธรรม์ วิธีการจ่ายเบี้ยประกัน ประวัติการชำระเบี้ยประกัน หรือประวัติเกี่ยวกับการกู้ยืมเงิน ผู้รับประโยชน์ การเรียกร้องค่าสินไหมทดแทน รวมถึงการใช้สิทธิต่าง ๆ ภายใต้กรมธรรม์ หรือผลิตภัณฑ์ หรือบริการอื่น ๆ ของบริษัทฯ หรือผู้ประกอบการธุรกิจประกันภัยอื่น ๆ

[จ] สถานะทางกฎหมาย เช่น สถานะเกี่ยวกับการป้องกันและปราบปรามการฟอกเงินและการป้องกันและปราบปรามการสนับสนุนเงินแก่การก่อการร้าย และภาวะล้มละลาย กฎหมายสหรัฐอเมริกาว่าด้วยการป้องกันมิให้บุคคลธรรมดาและนิติบุคคลที่มีสถานะเป็นบุคคลอเมริกันหลีกเลี่ยงภาษี [Foreign Account Tax Compliance Act : FACTA]

[ฉ] ข้อมูลทางเทคนิค และกิจกรรมส่วนบุคคล/ลักษณะการใช้งานที่ท่านชอบ เมื่อท่านใช้เว็บไซต์ แอปพลิเคชันของบริษัทฯ และอาจรวมถึงแพลตฟอร์มสื่อสังคมออนไลน์ของผู้ให้บริการอื่น เช่น ชื่อเรียกตัวตนเฉพาะของลูกค้าที่ใช้บนแพลตฟอร์มสื่อสังคมออนไลน์ ที่อยู่ไอพี [IP Address] ประเภทและเวอร์ชันของเบราว์เซอร์ การตั้งค่าเขตเวลา ระบบปฏิบัติการและแพลตฟอร์ม ข้อมูลผู้ใช้ [User Profile] ข้อมูลเกี่ยวกับอุปกรณ์ ซึ่งรวมถึงข้อมูลเกี่ยวกับอุปกรณ์เคลื่อนที่ ข้อมูลเครือข่ายไร้สายและข้อมูลเครือข่ายทั่วไป

[ช] ข้อมูลที่ได้จากระบบบันทึกอัตโนมัติต่าง ๆ เช่น เว็บคูกี้ ประวัติการใช้บริการผ่านช่องทางอิเล็กทรอนิกส์ บันทึกเสียงการสนทนา ภาพถ่าย ภาพเคลื่อนไหวจากกล้องวงจรปิด เป็นต้น

## 2.2 ข้อมูลส่วนบุคคลที่มีความอ่อนไหว

บริษัทมีความจำเป็นต้องเก็บรวบรวมข้อมูลส่วนบุคคลที่มีความอ่อนไหว [Sensitive Personal Data] เช่น ประวัติสุขภาพ เพื่อการซื้อหรือใช้ผลิตภัณฑ์ของบริษัทฯ กล่าวคือ ข้อมูลดังกล่าวจำเป็นต้องการพิจารณาปรับประกันภัย ตลอดจนการให้บริการและการจ่ายค่าสินไหมทดแทน หรือเพื่อการดำเนินการตามกฎหมายที่เกี่ยวข้อง หากท่านไม่ยินยอมให้บริการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวดังกล่าว บริษัทฯ จะไม่สามารถให้บริการ และให้บริการใด ๆ แก่ท่านได้

ในกรณีที่บริษัทฯ มีความจำเป็นต้องเก็บรวบรวมข้อมูลส่วนบุคคลของท่าน เพื่อปฏิบัติหน้าที่ตามกฎหมาย หรือการเข้าทำสัญญากับท่าน หากท่านไม่ให้ข้อมูลส่วนบุคคลบางอย่างที่จำเป็นต้องดำเนินการตามงาน บริษัทฯ อาจไม่สามารถดำเนินการตามวัตถุประสงค์ด้านล่างหรือให้บริการแก่ท่านได้อย่างเต็มรูปแบบ หรือท่านอาจจะไม่สามารถใช้บริการของบริษัทฯ ได้อย่างเหมาะสม และอาจส่งผลกระทบต่อการใช้บริการของบริษัทฯ ใด ๆ ที่บริษัทฯ หรือท่านมีหน้าที่ต้องปฏิบัติตาม

หากท่านให้ข้อมูลส่วนบุคคลของบุคคลที่สามแก่บริษัทฯ ท่านต้องปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ไม่ว่าจะเป็นการขอความยินยอม หรือแจ้งนโยบายฉบับนี้แก่บุคคลที่สามในนามบริษัทฯ เพื่อให้บริษัทฯ สามารถปฏิบัติตามต่อไปได้ตามวัตถุประสงค์ที่กำหนดในนโยบายฉบับนี้และนโยบายการคุ้มครองข้อมูลส่วนบุคคลของสำนักงาน

## 3. บริษัทฯ เก็บรวบรวมข้อมูลส่วนบุคคลของท่านอย่างไร

บริษัทฯ อาจเก็บรวบรวมข้อมูลส่วนบุคคลของท่านโดยวิธีต่อไปนี้

3.1 เมื่อท่านแสดงเจตนาจะซื้อหรือใช้ประกันส่วนบุคคล ประกันกลุ่ม รวมทั้งผลิตภัณฑ์และบริการ และ/หรือเมื่อท่านเข้าถึงหรือใช้เว็บไซต์ หรือแอปพลิเคชัน และ/หรือบริการต่าง ๆ ทางออนไลน์ บนอุปกรณ์เคลื่อนที่ หรือทางโทรศัพท์ หรือบริการอื่น ๆ ของบริษัทฯ ["ผลิตภัณฑ์" หรือ "บริการ"]

3.2 เมื่อท่านส่งเอกสารและใบคำขอเอาประกันเพื่อซื้อหรือใช้ หรือเมื่อท่านให้ข้อมูล ขณะที่พิจารณาจะซื้อหรือใช้ ผลิตภัณฑ์หรือบริการต่าง ๆ ของบริษัทฯ

3.3 เมื่อท่านติดต่อสื่อสารกับบริษัทฯ ไม่ว่าจะเป็นการสื่อสารเป็นหนังสือหรือวาจา โดยไม่คำนึงว่าฝ่ายใดจะเป็นผู้ติดต่อฝ่ายนั้นก่อนหรือไม่ก็ตาม

3.4 เมื่อท่านส่งคำร้องขอให้มีการเปลี่ยนแปลงหรือปรับปรุงผลิตภัณฑ์ที่ท่านซื้อหรือบริการที่ท่านใช้ หรือคำร้องขออื่นใดเกี่ยวกับผลิตภัณฑ์ที่ท่านซื้อหรือบริการที่ท่านใช้ รวมถึงการส่งแบบฟอร์มและเอกสารเกี่ยวกับการขอรับบริการที่เกี่ยวข้องกับผลิตภัณฑ์ของบริษัทฯ

3.5 เมื่อท่านติดต่อกับบุคลากร เจ้าหน้าที่บริการลูกค้า พนักงานขาย ตัวแทน นายหน้า คนกลางประกันภัย ผู้รับจ้าง คู่ค้า ผู้ให้บริการ ผู้รับมอบอำนาจ ผู้กระทำการแทน หรือบุคคลอื่นหรือหน่วยงานอื่นที่เกี่ยวข้องของบริษัทฯ [เรียกรวมกันว่า "บุคลากรและคู่ค้าของบริษัทฯ"] ผ่านทางเว็บไซต์ แอปพลิเคชัน สื่อสังคมออนไลน์ โทรศัพท์ อีเมล การพบปะกันโดยตรง การสัมภาษณ์ ข้อความสั้น [SMS] โทรสาร ไปรษณีย์ หรือโดยวิธีการอื่นใด

3.6 เมื่อบริษัทฯ ได้รับความแนะนำท่าน หรือเมื่อบริษัทฯ เก็บรวบรวมข้อมูลส่วนบุคคลจากบุคลากรและคู่ค้าของบริษัทฯ

3.7 เมื่อท่านส่งข้อมูลส่วนบุคคลให้แก่บริษัทฯ เพื่อเข้าร่วมในกิจกรรมทางการตลาด การประกวด การจับฉลากชิงโชค งานอีเว้นท์ หรือการแข่งขันต่าง ๆ ที่จัดขึ้นโดยหรือในนามของบริษัทฯ และ/หรือบุคลากรและคู่ค้าของบริษัทฯ

3.8 เมื่อบริษัทฯ ได้รับความข้อมูลส่วนบุคคลจากบุคคลภายนอกเกี่ยวกับท่าน ซึ่งรวมถึงแต่ไม่จำกัดเพียงการได้รับข้อมูลจากการตรวจสอบจากแหล่งข้อมูลที่เป็นสาธารณะ แหล่งข้อมูลส่วนตัว หรือแหล่งข้อมูลเชิงพาณิชย์ เว็บไซต์ แหล่งข้อมูลสื่อสังคมออนไลน์ ผู้ให้บริการข้อมูล [Data Providers] แหล่งข้อมูลทางการแพทย์ สถานบริการสาธารณสุข โรงพยาบาล แพทย์ บุคลากรผู้ประกอบวิชาชีพสาธารณสุขอื่น ผู้ประกอบธุรกิจประกันภัยอื่น สมาคมหรือสหพันธ์ของธุรกิจที่เกี่ยวข้องกับผลิตภัณฑ์ที่ท่านซื้อหรือบริการที่ท่านใช้ ใบคำขอเอาประกันสำหรับผลิตภัณฑ์ที่ท่านซื้อหรือบริการที่ท่านใช้ การรับประกันความเสี่ยงของผลิตภัณฑ์ที่ท่านซื้อ การร้องเรียนเกี่ยวกับผลิตภัณฑ์ และ/หรือผลิตภัณฑ์และบริการของบริษัทฯ ที่ซื้อหรือใช้โดยท่าน ["แหล่งข้อมูลที่เป็นบุคคลภายนอก"]

3.9 เมื่อบริษัทฯ ได้รับความข้อมูลส่วนบุคคลจากบุคคลภายนอกเกี่ยวกับท่านเพื่อวัตถุประสงค์ในการปฏิบัติตามกฎหมายและเพื่อวัตถุประสงค์เกี่ยวกับการกำกับดูแลในประการอื่น ๆ ตลอดจนเพื่อวัตถุประสงค์อื่น ๆ ที่ชอบด้วยกฎหมาย เช่น บริษัทฯ อาจได้รับความข้อมูลส่วนบุคคลของท่านจากคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย [คปภ.]

เมื่อท่านให้ข้อมูลส่วนบุคคลใด ๆ ที่เกี่ยวข้องกับบุคคลภายนอกแก่บริษัทฯ [ซึ่งบุคคลภายนอกดังกล่าวรวมถึงแต่ไม่จำกัดเพียงผู้เอาประกัน สมาชิกในครอบครัว ผู้ชำระเงินตามกรมธรรม์ หรือผู้รับประโยชน์] ท่านรับรองและรับประกันความถูกต้องของข้อมูลส่วนบุคคลนั้น พร้อมทั้งรับรองและรับประกันว่าท่านได้แจ้งให้บุคคลเหล่านั้นทราบอย่างครบถ้วนแล้วเกี่ยวกับรายละเอียดตามนโยบายฯ ฉบับนี้



#### 4. วัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคลของท่าน

บริษัทฯ จะประมวลผลข้อมูลส่วนบุคคลของท่านเพื่อวัตถุประสงค์ดังต่อไปนี้

4.1 เพื่อการเก็บรวบรวม ใช้ และ/หรือเปิดเผยข้อมูลส่วนบุคคลต่อสำนักงาน เพื่อประโยชน์ในการกำกับดูแล และส่งเสริมธุรกิจประกันภัยตามกฎหมายว่าด้วยคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย และกฎหมายว่าด้วยการประกันวินาศภัย ตามนโยบายคุ้มครองข้อมูลส่วนบุคคลของสำนักงาน ซึ่งสามารถตรวจดูได้ที่ เว็บไซต์ของสำนักงาน [<https://www.oic.or.th>]

4.2 เพื่อดำเนินการเกี่ยวกับการเข้าทำสัญญาประกันภัย และการดำเนินการตามสัญญา กล่าวคือ [ก] เพื่อเสนอขาย ขาย จัดให้ บริหารจัดการ ดำเนินการ ปฏิบัติตามขั้นตอนกระบวนการ และจัดการเกี่ยวกับผลิตภัณฑ์และ/หรือบริการของบริษัทฯ ให้แก่ท่าน [ข] เพื่อปฏิบัติตามขั้นตอนกระบวนการ จัดการ ทำให้แล้วเสร็จ ซึ่งการให้บริการ หรือ ผลิตภัณฑ์ของบริษัทฯ และการแนะนำผลิตภัณฑ์และบริการที่เหมาะสมให้แก่ท่าน การปฏิบัติตามขั้นตอนกระบวนการเกี่ยวกับใบคำขอเอาประกันสำหรับผลิตภัณฑ์ การจัดการเกี่ยวกับผลิตภัณฑ์ที่ท่านซื้อ การเก็บเบี้ยประกัน และเงินค่าชำระจากท่าน การสืบสวน วิเคราะห์ ประมวลผล การเวนคืนกรมธรรม์ และการจ่ายค่าสินไหมทดแทน/การจ่ายผลประโยชน์ตามกรมธรรม์ภายใต้กรมธรรม์ของท่าน และการต่ออายุ ปรับปรุงแก้ไข ยกเลิกกรมธรรม์ของท่าน ตลอดจนจนถึงการใช้สิทธิใด ๆ ภายใต้กรมธรรม์ของท่าน ซึ่งรวมถึงสิทธิในการรับช่วงสิทธิ และสิทธิที่ได้รับช่วงมาด้วย [หากมี]

4.3 เพื่อการจัดการเกี่ยวกับการประกันภัยของบริษัทฯ ได้แก่ การออกแบบผลิตภัณฑ์และ/หรือบริการใหม่ของบริษัทฯ หรือการเสริมเพิ่มเติมผลิตภัณฑ์และ/หรือบริการที่มีอยู่ของบริษัทฯ การดำเนินการเพื่อทำประกันภัยต่อสำหรับผลิตภัณฑ์และ/หรือบริการของบริษัทฯ ให้แก่ท่าน

4.4 เพื่อการติดต่อสื่อสารกับท่าน ซึ่งรวมถึงการสื่อสารข้อมูลเกี่ยวกับการจัดการและข้อมูลอื่น ๆ เกี่ยวกับผลิตภัณฑ์หรือบัญชีใด ๆ ที่ท่านอาจมีกับบริษัทฯ การให้การสนับสนุนทางเทคนิคเกี่ยวกับเว็บไซต์และแอปพลิเคชันของบริษัทฯ หรือการสื่อสารเกี่ยวกับการเปลี่ยนแปลงใด ๆ ที่จะมีขึ้นต่อนโยบายฯ ฉบับนี้ในอนาคต

4.5 เพื่อการวิเคราะห์และจัดทำสถิติ ได้แก่ การทำวิจัยทางการตลาด การวิเคราะห์ข้อมูลขั้นสูง และการทำวิจัยเชิงสถิติหรือคณิตศาสตร์ประกันภัย การรายงานหรือการประเมินผลทางการเงินที่จัดทำขึ้นโดยบริษัทฯ กลุ่มบริษัท บุคลากรและลูกค้าของบริษัทฯ หรือหน่วยงานกำกับดูแลที่เกี่ยวข้องกับบริษัทฯ

4.6 เพื่อการป้องกันการฉ้อโกง ได้แก่ การสืบสวนหรือป้องกันการกระทำที่เกี่ยวกับการฉ้อโกง การปกปิดข้อความจริง และการกระทำผิดอื่น ๆ ไม่ว่าจะเป็นการกระทำผิดจริงหรือการกระทำที่สงสัยว่าจะเป็นการกระทำผิด โดยเฉพาะอย่างยิ่งเพื่อการติดต่อสื่อสารกับบริษัทต่าง ๆ ในธุรกิจบริการทางการเงินและการประกันภัย ตลอดจนเพื่อการติดต่อสื่อสารกับหน่วยงานกำกับดูแลที่เกี่ยวข้องกับบริษัทฯ

4.7 เพื่อการปรับโครงสร้างของบริษัทฯ กล่าวคือ เพื่อวัตถุประสงค์ในการปรับโครงสร้างองค์กรของบริษัทฯ และเพื่อการทำธุรกรรมของบริษัทฯ รวมถึงการซื้อ หรือ ขายธุรกิจไม่ว่าส่วนใดส่วนหนึ่งของบริษัทฯ [หากมี]

4.8 เพื่อการให้บริการช่องทางการสื่อสารทางอิเล็กทรอนิกส์ เช่น เพื่อให้ท่านสามารถเข้าถึงเนื้อหาในเว็บไซต์ แอปพลิเคชัน หรือแพลตฟอร์มสื่อสังคมออนไลน์ หรือบริการอย่างใดอย่างหนึ่งเป็นการเฉพาะ โดยบริษัทฯ อาจประมวลผลพฤติกรรมการใช้เว็บไซต์ แอปพลิเคชัน หรือแพลตฟอร์มสื่อสังคมออนไลน์ เพื่อการวิเคราะห์การใช้งานเว็บไซต์ แอปพลิเคชัน หรือแพลตฟอร์มสื่อสังคมออนไลน์ของท่าน และการทำความเข้าใจลักษณะการใช้งานที่ท่านชอบ เพื่อจัดทำให้เว็บไซต์ แอปพลิเคชัน หรือแพลตฟอร์มสื่อสังคมออนไลน์เหล่านั้นตอบสนองอย่างเหมาะสมกับท่านโดยเฉพาะ เพื่อการประเมิน หรือดำเนินการ และการปรับปรุงเว็บไซต์ แอปพลิเคชัน หรือแพลตฟอร์มสื่อสังคมออนไลน์เหล่านั้น หรือผลิตภัณฑ์และ/หรือบริการของบริษัทฯ การแก้ไขปัญหาต่าง ๆ การแนะนำผลิตภัณฑ์และ/หรือบริการที่เกี่ยวข้อง และการจัดโฆษณาบนเว็บไซต์ แอปพลิเคชัน และช่องทางอื่น ๆ ตามกลุ่มเป้าหมาย

4.9 เพื่อการปฏิบัติตามกฎหมาย และนโยบายบริษัทฯ ได้แก่ การดำเนินการใด ๆ [ก] เพื่อการปฏิบัติตามกฎหมาย และการตรวจสอบธุรกิจของบริษัทฯ ไม่ว่าจะเป็นการตรวจสอบภายใน หรือการตรวจสอบจากบุคคลภายนอก [ข] เพื่อดำเนินการให้เป็นไปตามข้อกำหนดของกฎหมาย กฎ ระเบียบ ข้อตกลง หรือนโยบายที่ใช้บังคับ ซึ่งกำหนดขึ้นโดยหน่วยงานกำกับดูแลของรัฐ หน่วยงานที่มีหน้าที่บังคับใช้กฎหมาย หน่วยงานรัฐ หน่วยงานที่มีหน้าที่ระงับข้อพิพาท หรือหน่วยงานที่ดูแลธุรกิจประกันภัย ไม่ว่าหน่วยงานใดก็ตาม [ค] เพื่อวัตถุประสงค์ของการบังคับใช้กฎหมาย หรือการให้ความช่วยเหลือ ให้ความร่วมมือ การสืบสวนโดยบริษัทฯ หรือในนามของบริษัทฯ โดยเจ้าหน้าที่ตำรวจ หรือโดยหน่วยงานรัฐหรือหน่วยงานกำกับดูแลอื่น ๆ ในประเทศ และการดำเนินการตามหน้าที่ในการรายงาน และข้อกำหนดต่าง ๆ ตามที่กฎหมายกำหนด หรือ ตามที่มีการตกลงเห็นชอบกับหน่วยงานรัฐหรือหน่วยงานกำกับดูแลอื่น ๆ ในประเทศหรือเขตการปกครองใด ๆ หรือการดำเนินการตามคำสั่งโดยชอบด้วยกฎหมายของพนักงานเจ้าหน้าที่ หรือหน่วยงานของรัฐ และ [ง] เพื่อดำเนินการให้เป็นไปตามข้อกำหนดภายใต้นโยบายภายในของบริษัทฯ ที่ยึดถือปฏิบัติ

4.10 เพื่อการบริหารจัดการข้อมูล ได้แก่ เพื่อวัตถุประสงค์ในการบริหารจัดการ จัดเก็บ บันทึกรวบรวม หรือทำลายข้อมูลส่วนบุคคล

4.11 เพื่อพัฒนาการผลิตภัณฑ์และการให้บริการของบริษัทฯ รวมถึงการตรวจสอบและเพิ่มคุณภาพ รวมทั้งการฝึกอบรม เมื่อมีการบันทึกการติดต่อสื่อสารของบริษัทฯ

4.12 เพื่อการดำเนินการส่งเสริมการขาย รวมถึงการดำเนินการให้ข้อมูลเกี่ยวกับ ผลิตภัณฑ์ และการบริการที่เหมาะสมแก่ท่าน ซึ่งอาจรวมถึงการให้คำแนะนำและข้อมูลในเรื่องต่าง ๆ ซึ่งรวมถึงการประกัน ตลอดจนจนถึงกิจกรรมส่งเสริมการขายผลิตภัณฑ์และการบริการ เช่น โพรแกรมให้รางวัล/ให้ผลประโยชน์สำหรับการเป็นลูกค้าที่มีความภักดี

ต่อแบรนด์/ให้สิทธิพิเศษ กิจกรรมการกุศล/กิจกรรมที่ไม่หวังผล และการจัดกิจกรรมทางการตลาด งานอีเว้นท์ และกิจกรรมอื่น ๆ ซึ่งท่านเลือกที่จะเข้าร่วม

ในกรณีนี้ บริษัทฯ จะดำเนินการต่อเมื่อท่านให้ความยินยอมเท่านั้น และท่านมีสิทธิในการถอนความยินยอมเกี่ยวกับการประมวลผลเพื่อการส่งเสริมการขายได้ตลอดโดยผ่านช่องทางการติดต่อตั้งระบุในนโยบายฯ ฉบับนี้ หรือ กดปุ่ม Unsubscribe หรือ Opt-Out ในช่องทางการสื่อสารต่าง ๆ เช่น SMS หรือ Email ที่ท่านได้รับ

4.13 อื่น ๆ กล่าวคือ เพื่อการดำเนินการอื่น ๆ ที่จำเป็น ซึ่งเกี่ยวข้องกับวัตถุประสงค์ใด ๆ ข้างต้น

เว้นแต่กฎหมายและกฎระเบียบที่ใช้บังคับ รวมถึง พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลจะอนุญาตให้กระทำเป็นอย่างอื่น บริษัทฯ จะแจ้งและขอความยินยอมจากท่าน หากบริษัทฯ ประสงค์จะใช้ข้อมูลส่วนบุคคลของท่านเพื่อวัตถุประสงค์อื่นใดนอกเหนือไปจากที่ระบุไว้ในนโยบายฯ ฉบับนี้ หรือนอกเหนือไปจากวัตถุประสงค์ที่เกี่ยวข้องโดยตรงกับนโยบายฯ นี้

## 5. บุคคลใดบ้างที่อาจจะได้รับข้อมูลส่วนบุคคลของท่านจากบริษัทฯ

ในการดำเนินการตามวัตถุประสงค์ต่าง ๆ ข้างต้น บริษัทฯ อาจเปิดเผยข้อมูลส่วนบุคคลของท่านให้แก่บุคคลต่าง ๆ ตามที่ระบุด้านล่างนี้ โดยบริษัทฯ จะดำเนินการใด ๆ ที่จำเป็นเพื่อคุ้มครองข้อมูลส่วนบุคคลของท่านตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล

5.1 บุคคลใดก็ตามที่ได้รับอนุญาตให้กระทำการในฐานะบุคลากรและคู่ค้าของบริษัทฯ เพื่อทำการเชิญชวน ชักชวน ชี้ช่อง จัดการให้ทำ เสนอขาย ขาย จัดจำหน่าย หรือให้บริการเกี่ยวกับผลิตภัณฑ์และ/หรือบริการที่เสนอโดยบริษัทฯ หรือบริษัทในกลุ่มบริษัทให้แก่ท่าน รวมถึงส่งมอบผลิตภัณฑ์และ/หรือบริการของบริษัทฯ ที่มี การเสนอ/ขาย ให้แก่ท่าน เช่น บริษัทประกันภัยต่อ บริษัทจัดการการลงทุน สถาบันจัดอันดับความน่าเชื่อถือ บริษัทต่าง ๆ ซึ่งทำการสืบสวน หรือคู่ค้ารายอื่น ๆ

5.2 ผู้ถือกรรมสิทธิ์ ในกรณีของผลิตภัณฑ์ประกันแบบกลุ่ม

5.3 บุคคลใดก็ตามที่ได้รับการว่าจ้าง หรือเข้าทำสัญญาเพื่อปฏิบัติงานให้แก่บุคลากรและคู่ค้าของบริษัทฯ ดังกล่าว เพื่อทำการเชิญชวน ชักชวน ชี้ช่อง จัดการให้ทำ เสนอขาย ขาย จัดจำหน่าย หรือให้บริการเกี่ยวกับผลิตภัณฑ์และ/หรือบริการที่เสนอโดยบริษัทฯ หรือบริษัทในกลุ่มบริษัทให้แก่ท่าน

5.4 บุคลากรและคู่ค้าของบริษัทฯ ไม่ว่าจะรายใดก็ตาม ซึ่งให้บริการเกี่ยวกับการจัดการต่าง ๆ การให้บริการประมวลผลข้อมูล บริการเกี่ยวกับกระบวนการทางธุรกิจ บริการเกี่ยวกับการชำระเงิน การทวงหนี้ หรือการหักบัญชี หลักทรัพย์ บริการโทรคมนาคม บริการด้านเทคโนโลยี บริการคลาวด์ บริการจัดหาผู้รับจ้างปฏิบัติงาน บริการคอลเซ็นเตอร์ บริการจัดเก็บของ การดำเนินการเกี่ยวกับเอกสาร บริการเก็บบันทึกข้อมูล บริการสแกนเอกสาร บริการรับส่งไปรษณีย์ บริการจัดพิมพ์ บริการส่งพัสดุหรือบริการรับส่งพัสดุโดยพนักงานรับส่งพัสดุ บริการวิเคราะห์ข้อมูล บริการทำการตลาด บริการทำการวิจัย บริการบริหารจัดการเหตุฉุกเฉิน บริการทางกฎหมาย หรือบริการอื่น ๆ ที่เกี่ยวข้องกับการดำเนินธุรกิจของบริษัทฯ หรือการจัดให้มีการบริหารจัดการ การดำเนินการ การปฏิบัติตามขั้นตอน หรือการจัดการต่าง ๆ เกี่ยวกับผลิตภัณฑ์หรือบริการของบริษัทฯ ให้แก่ท่าน

5.5 ผู้ประกอบธุรกิจประกันอื่น ๆ

5.6 สมาคมหรือสมาพันธ์ในภาคธุรกิจประกัน

5.7 แหล่งข้อมูลที่เป็นบุคคลภายนอก [ตามรายละเอียดข้างต้น]

5.8 หน่วยงานที่มีหน้าที่บังคับใช้กฎหมาย คณะกรรมการต่าง ๆ ที่จัดตั้งขึ้นตามกฎหมาย หน่วยงานรัฐหรือหน่วยงานกำกับดูแล หน่วยงานที่มีหน้าที่ระงับข้อพิพาท หรือบุคคลอื่นใดในประเทศที่บริษัทฯ หรือบริษัทในกลุ่มบริษัทต้องเปิดเผยข้อมูลให้ [ก] ตามหน้าที่ตามกฎหมายและ/หรือตามหน้าที่ในการปฏิบัติตามกฎระเบียบในประเทศไทย และอาจรวมถึงหน่วยงานของรัฐในประเทศที่กลุ่มบริษัทตั้งอยู่ หรือ [ข] ตามข้อตกลงหรือนโยบายระหว่างบริษัทฯ ในกลุ่มบริษัท กับรัฐ หน่วยงานกำกับดูแล หรือบุคคลอื่น ๆ ที่เกี่ยวข้อง

5.9 บริษัทใด ๆ ในกลุ่มบริษัท

5.10 ผู้ให้คำปรึกษาของบริษัทฯ ซึ่งเป็นผู้ประกอบวิชาชีพ อาทิเช่น ทนายความ แพทย์ ผู้ตรวจสอบบัญชี หรือที่ปรึกษา

5.11 บุคคลหรือหน่วยงานใด ๆ ที่ท่านให้ความยินยอมให้เปิดเผยข้อมูลส่วนบุคคลของท่านต่อบุคคลหรือหน่วยงานนั้น ๆ ได้

5.12 ผู้เข้าทำธุรกรรม หรือจะเข้าทำธุรกรรมกับบริษัทฯ โดยข้อมูลส่วนบุคคลของท่านอาจเป็นส่วนหนึ่งของการซื้อหรือขาย หรือเป็นส่วนหนึ่งของการเสนอซื้อหรือเสนอขายของกิจการของบริษัทฯ [หากมี]

5.13 บุคคลหรือหน่วยงานอื่นใดที่ได้รับอนุญาตตามกฎหมายที่ใช้บังคับ

## 6. การโอนข้อมูลไปยังประเทศต่างประเทศ

ข้อมูลส่วนบุคคลของท่านอาจถูกโอนไป ถูกจัดเก็บไว้ หรือประมวลผลโดยบริษัทฯ หรืออาจถูกส่งให้แก่บุคคลหรือหน่วยงานใด ๆ ตามรายละเอียดข้างต้น ซึ่งอาจมีที่ตั้งหรืออาจให้บริการอยู่ในประเทศไทยหรือนอกประเทศไทย ทั้งนี้ข้อมูลส่วนบุคคลของท่าน จะถูกโอนไปยังสถานที่อื่น ๆ ตามเงื่อนไขเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ดังที่ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลกำหนด โดยหากเป็นการโอนข้อมูลส่วนบุคคลของท่านระหว่างกลุ่มบริษัท บริษัทฯ จะ

ดำเนินการตามนโยบายคุ้มครองข้อมูลส่วนบุคคลภายในกลุ่มบริษัท [Binding Corporate Rules] ที่ได้รับการอนุมัติจากคณะกรรมการ [หากมี]

## 7. การเก็บรักษาข้อมูลส่วนบุคคล

บริษัทฯ จะเก็บรักษาข้อมูลส่วนบุคคลของท่านไว้ トラบเท่าที่จำเป็นต้องเก็บเพื่อการดำเนินการให้บรรลุตามวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลของท่านตามที่ระบุข้างต้น ทั้งนี้บริษัทฯ จะเก็บรักษาข้อมูลส่วนบุคคลของท่านไม่เกิน 10 ปี นับแต่วันที่ท่านสิ้นสุดความสัมพันธ์ หรือการติดต่อครั้งสุดท้ายกับบริษัทฯ บริษัทฯ อาจเก็บรักษาข้อมูลส่วนบุคคลของท่านนานกว่าที่กำหนดหากมีความจำเป็นทางด้านกฎหมาย

บริษัทฯ จะดำเนินการตามขั้นตอนที่เหมาะสม เพื่อทำการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลของท่านเป็นข้อมูลที่ไม่สามารถระบุตัวท่าน ตามระยะเวลาเก็บรักษาข้อมูลส่วนบุคคลข้างต้น

## 8. สิทธิของท่านเกี่ยวกับข้อมูลส่วนบุคคล

ท่านมีสิทธิดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลของท่านดังต่อไปนี้

8.1 เพิกถอนหรือร้องขอให้เปลี่ยนแปลงขอบเขตความยินยอมของท่านใดให้ไว้กับบริษัทฯ

8.2 ตรวจสอบว่าบริษัทฯ มีข้อมูลส่วนบุคคลใด ๆ เกี่ยวกับท่านหรือไม่ ตลอดจนสิทธิในการเข้าถึง หรือขอรับสำเนาของข้อมูลใด ๆ ดังกล่าว และ/หรือเข้าถึงข้อมูลว่าบริษัทฯ ประมวลผลข้อมูลส่วนบุคคลของท่านอย่างไร

8.3 ขอให้บริษัทฯ ทำการแก้ไขข้อมูลส่วนบุคคลใด ๆ ที่เกี่ยวข้องกับท่าน ให้ถูกต้อง

8.4 ขอให้ลบหรือทำลายข้อมูลส่วนบุคคลของท่านในบางสถานการณ์

8.5 ขอให้จำกัดการดำเนินการประมวลผลข้อมูลส่วนบุคคลของท่านในบางสถานการณ์

8.6 ขอให้บริษัทฯ โอนย้ายข้อมูลส่วนบุคคลของท่านในบางสถานการณ์

8.7 ขอให้ระงับการประมวลผลข้อมูลส่วนบุคคลของท่านเป็นการชั่วคราวในบางสถานการณ์

ทั้งนี้ ขอสงวนสิทธิไม่ปฏิบัติตามคำร้องขอใช้สิทธิของท่าน ตามความเหมาะสมและเท่าที่กฎหมายที่ใช้บังคับจะอนุญาต

นอกจากสิทธิของท่านตามที่ระบุข้างต้น ท่านมีสิทธิที่จะเสนอข้อร้องเรียนเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลของบริษัทฯ ต่อคณะกรรมการผู้เชี่ยวชาญตามขั้นตอนที่กำหนดใน พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล เท่าที่กฎหมายและกฎระเบียบที่ใช้บังคับอนุญาต บริษัทฯ อาจมีสิทธิเรียกเก็บค่าใช้จ่ายที่สมเหตุสมผล สำหรับการดำเนินการเกี่ยวกับคำร้องขอใช้สิทธิข้างต้น

## 9. การแก้ไขเปลี่ยนแปลงนโยบายฯ ฉบับนี้

บริษัทฯ ขอสงวนสิทธิในการแก้ไข เพิ่มเติม เปลี่ยนแปลง ปรับปรุง หรือปรับเปลี่ยนนโยบายฯ ฉบับนี้ เท่าที่กฎหมายอนุญาต หากเป็นการเปลี่ยนแปลงในสาระสำคัญของนโยบายฯ ฉบับนี้ บริษัทฯ จะแจ้งการแก้ไข การเปลี่ยนแปลง การปรับปรุง หรือการปรับเปลี่ยนนโยบายฯ ให้ท่านทราบ และ/หรือจะขอความยินยอมจากท่าน [หากกฎหมายกำหนดให้ต้องได้รับความยินยอม]

## 10. ช่องทางการติดต่อ

หากท่านมีข้อสงสัยเกี่ยวกับเนื้อหาส่วนใด ๆ ในนโยบายฯ ฉบับนี้ หรือต้องการข้อมูลเพิ่มเติมเกี่ยวกับแนวทางปฏิบัติของบริษัทฯ เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของท่าน หรือต้องการใช้สิทธิเกี่ยวกับข้อมูลส่วนบุคคลของท่าน กรุณาติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล [Data Protection Officer : DPO] ของบริษัทฯ ดังนี้

สำนักกำกับดูแล

บริษัท เทเวศประกันภัย จำกัด [มหาชน]

97 และ 99 อาคารเทเวศประกันภัย ถนนราชดำเนินกลาง แขวงบวรนิเวศ เขตพระนคร กรุงเทพฯ 10200

โทรศัพท์ 1291 ต่อ 8202, 8203 เวลาทำการ วันจันทร์ – วันศุกร์ เวลา 8.30 – 17.00 น.

อีเมล [dpo@deves.co.th](mailto:dpo@deves.co.th)

## 16.2 นโยบายคุ้มครองข้อมูลส่วนบุคคล [คู่ค้า ตัวแทน และนายหน้า]

บริษัท เทเวศประกันภัย จำกัด [มหาชน] ตระหนักดีถึงสิทธิในความเป็นส่วนตัวและความรับผิดชอบของบริษัทฯ เกี่ยวกับการเก็บรวบรวม การใช้ การเปิดเผย ["การประมวลผล"] ข้อมูลส่วนบุคคลของท่าน บริษัทฯ จึงได้จัดทำ นโยบายคุ้มครองข้อมูลส่วนบุคคล [นโยบายฯ] ฉบับนี้ขึ้นมา เพื่อแจ้งรายละเอียดเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลของท่านตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ["พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล"]

### 1. บทนิยาม

"ข้อมูลส่วนบุคคล" หมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

"ข้อมูลส่วนบุคคลที่มีความอ่อนไหว" หมายถึง ข้อมูลตามที่กำหนดไว้ในมาตรา 26 พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล และฉบับปรับปรุงแก้ไขตามที่จะมีการแก้ไขเป็นคราว ๆ กฎหมายและกฎระเบียบที่ใช้บังคับอื่น รวมถึงข้อมูลบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกัน

"พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล" หมายถึง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 รวมถึงกฎหมายลำดับรองที่อาศัยอำนาจ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลในการตราขึ้น และตามที่มีการแก้ไขเป็นครั้งคราว

"คณะกรรมการ" หมายถึง คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

### 2. ข้อมูลส่วนบุคคลใดบ้างที่บริษัทฯ จะเก็บรวบรวม

ข้อมูลส่วนบุคคลที่บริษัทฯ อาจเก็บรวบรวมประกอบไปด้วยข้อมูลของท่านดังต่อไปนี้

#### 2.1 กรณีที่ท่านดำเนินการในนามของตนเอง

[ก] ข้อมูลที่ใช้ระบุตัวบุคคล อาทิ ชื่อ-นามสกุล ที่อยู่ตามทะเบียนบ้าน ที่อยู่ปัจจุบัน เบอร์โทรศัพท์บ้านหรือมือถือ หรือรายละเอียดการติดต่ออื่น ๆ เพศ สัญชาติ สถานภาพการสมรส วันเกิด เลขที่หนังสือเดินทาง/บัตรประจำตัวประชาชน

[ข] ข้อมูลเกี่ยวกับคุณวุฒิและประวัติการทำงานของท่าน อาทิ คุณวุฒิการศึกษาจากโรงเรียนหรือมหาวิทยาลัย รวมถึงหนังสือรับรองและหนังสืออ้างอิงจากสถานศึกษา

[ค] ข้อมูลเกี่ยวกับการสมัครของท่าน ตัวอย่างเช่น ประวัติส่วนตัว ข้อมูลการสัมภาษณ์งาน และหลักฐานหรือหนังสืออ้างอิงต่าง ๆ

[ง] รายละเอียดการทำงานพื้นฐาน ตัวอย่างเช่น รายละเอียดสถานที่ทำงานของท่าน หมายเลขใบอนุญาตตัวแทน/ นายหน้าประกันวินาศภัย รายละเอียดหน่วยงานต้นสังกัด ตำแหน่ง สายการบังคับบัญชา และข้อตกลงและเงื่อนไขของการเป็นตัวแทน/ นายหน้าประกันวินาศภัย

[จ] ประวัติเกี่ยวกับประสิทธิภาพการทำงาน รวมถึงการประเมินผลการปฏิบัติงาน รางวัลที่เคยได้รับ ประวัติการถูกร้องเรียน บันทึกการสอบสวน การถูกพักสัญญาตัวแทน/นายหน้าประกันวินาศภัย และโทษทางวินัย รวมถึงการตรวจสอบและการประเมินความเสี่ยง

[ฉ] ข้อมูลเกี่ยวกับผลประโยชน์และค่าตอบแทน ตัวอย่างเช่น รายละเอียดเกี่ยวกับค่าบำเหน็จ และ/ หรือผลประโยชน์อื่น ๆ ที่ท่านได้รับ เลขบัญชีธนาคาร กองทุนประกันสังคม ข้อมูลทางภาษี ข้อมูลของบุคคลภายนอก ผู้ได้รับผลประโยชน์

#### 2.2 กรณีที่ท่านดำเนินการแทนหรือเพื่อนิติบุคคลของท่าน

กรณีที่คู่สัญญาของบริษัทฯ เป็นนิติบุคคล บริษัทฯ อาจประมวลผลข้อมูลส่วนบุคคลของท่านในฐานะที่ท่านเป็นพนักงาน ผู้รับจ้าง หรือผู้มีอำนาจกระทำการแทนนิติบุคคลของท่าน

[ก] ข้อมูลที่ใช้ระบุตัวบุคคล อาทิ ชื่อ-นามสกุล ที่อยู่ตามทะเบียนบ้าน ที่อยู่ปัจจุบัน เบอร์โทรศัพท์บ้านหรือมือถือ อีเมล เลขที่หนังสือเดินทางหรือเลขบัตรประจำตัวประชาชน

[ข] ข้อมูลของท่านที่ปรากฏในหนังสือรับรองบริษัท บัญชีรายชื่อผู้ถือหุ้น หรือเอกสารเกี่ยวกับนิติบุคคลอื่นใดที่มีข้อมูลส่วนบุคคลของท่าน

[ค] ประวัติเกี่ยวกับการล้มละลาย การฟอกเงิน หรือการให้การสนับสนุนทางการเงินแก่ผู้ก่อการร้าย

[ง] ข้อมูลอื่นใดที่บริษัทฯ ร้องขอจากนิติบุคคลของท่าน หรือจากท่านเพื่อใช้ในการประกอบการเข้าทำสัญญา การบริการ หรือการดำเนินการอื่นใดที่เกี่ยวข้อง ตามที่บริษัทฯ ได้แจ้งหรือร้องขอไปยังท่าน

ทั้งนี้หากท่านดำเนินการเกี่ยวกับการเสนอขาย หรือกระทำการเป็นตัวแทนหรือนายหน้าประกันด้วย บริษัทฯ จะประมวลผลข้อมูลส่วนบุคคลของท่านตามรายละเอียดในข้อ 2.1 ด้วย

นอกจากข้อมูลส่วนบุคคลตามที่ระบุข้างต้น บริษัทฯ อาจประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหว [Sensitive Personal Data] ของท่าน เช่น ประวัติอาชญากรรม เพื่อประกอบการตรวจสอบในการเข้าทำสัญญากับบริษัทฯ เช่น ตรวจสอบเพื่อการป้องกันและปราบปรามการฟอกเงินและการให้การสนับสนุนแก่ผู้ก่อการร้าย เป็นต้น

ในกรณีที่ท่านได้ให้ข้อมูลส่วนบุคคลเกี่ยวกับบุคคลอื่นแก่บริษัทฯ ท่านรับทราบและรับรองว่าได้นำเสนอ นโยบายฯ นี้แก่บุคคลดังกล่าว พร้อมทั้งได้รับความยินยอมจากบุคคลนั้น ๆ แล้วในการเปิดเผยข้อมูลแก่บริษัทฯ

### 3. บริษัทฯ เก็บรวบรวมข้อมูลส่วนบุคคลของท่านอย่างไร

โดยทั่วไปบริษัทฯ จะเก็บรวบรวมข้อมูลส่วนบุคคลของท่านโดยตรงจากท่าน เว้นแต่บางกรณีที่บริษัทฯ อาจเก็บรวบรวมข้อมูลของท่านจากบุคคลอื่นที่แนะนำท่านให้บริษัทฯ จากแหล่งข้อมูลสาธารณะ แหล่งข้อมูลเกี่ยวกับ ธุรกิจของท่าน หรือแหล่งข้อมูลทางการค้า

### 4. วัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคลของท่าน

4.1 บริษัทฯ ประมวลผลข้อมูลส่วนบุคคลของท่านเพื่อการเข้าทำสัญญากับท่าน และเพื่อการปฏิบัติตามสิทธิหน้าที่ที่มีตามสัญญาที่บริษัทฯ เข้าทำกับท่าน

4.2 เพื่อการตรวจสอบและยืนยันตัวตนของท่าน

4.3 เพื่อการตรวจสอบประวัติก่อนและระหว่างเข้าทำสัญญา และอาจมีการตรวจสอบรายละเอียดดังกล่าวระหว่างระยะเวลาตามสัญญา

4.4 ในกรณีที่ท่านดำเนินการเป็นตัวแทนหรือนายหน้าประกัน ข้อมูลส่วนบุคคลของท่านจะถูกใช้เพื่อวัตถุประสงค์ในการบริหารจัดการธุรกิจตัวแทนประกันวินาศภัยและ/หรือนายหน้าประกันวินาศภัย รวมถึงแต่ไม่จำกัดอยู่เพียงการวางแผนกำลังคน การจ่ายผลประโยชน์ ค่าตอบแทน การคิดค่าตอบแทนที่จูงใจ ข้อเสนอ รางวัล การประเมินผลการปฏิบัติงานที่ การรายงานหรือตรวจสอบภายใน การวิเคราะห์ข้อมูล การแข่งขันการขายต่าง ๆ การติดต่อสื่อสาร การประกาศ การทำแบบสำรวจ สถิติ ตรวจสอบข้อร้องเรียนและประเด็นของการประทุติตัวไม่เหมาะสม หรือเป็นส่วนหนึ่งของกระบวนการทางวินัย การตรวจสอบข้อมูลของท่านทางกฎหมาย ความสามารถในการทำงาน การร้องขอข้อมูลใด ๆ โดยรัฐบาลไม่ว่าจะเพื่อเหตุใด ตลอดจนเพื่อการประกอบกิจการของกลุ่มบริษัท ซึ่งรวมถึงแต่ไม่จำกัดเพียง จัดทำบันทึกข้อมูลตัวแทน การทำประกัน การตรวจสอบการอ้างถึงและประวัติโดยสมาชิกใด ๆ ของกลุ่มบริษัทหรือบุคคลอื่น การหลีกเลี่ยงการขัดกันของผลประโยชน์ หรือหลีกเลี่ยงแนวโน้มที่จะเกิดการขัดกันของผลประโยชน์ และการตรวจสอบโดยสมาชิกใด ๆ ของกลุ่มบริษัท นอกจากนี้ข้อมูลส่วนบุคคลของท่านยังอาจจะถูกใช้เพื่อวัตถุประสงค์เพื่อปฏิบัติตามกฎหมายและกฎเกณฑ์ที่ใช้บังคับ และการปฏิบัติตามข้อกำหนดของหน่วยงานกำกับดูแลตามกฎหมายทั้งในและนอกประเทศของท่าน แล้วแต่กรณี

4.5 เพื่อการปฏิบัติตามกฎหมาย รวมถึงแต่ไม่จำกัดเฉพาะประกาศ ระเบียบ และคำสั่งโดยชอบด้วยกฎหมายของหน่วยงานรัฐและเจ้าหน้าที่รัฐที่เกี่ยวข้อง เช่น คณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย [คปภ.] และคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

4.6 เพื่อการก่อตั้ง ใช้ โต้แย้ง หรือดำเนินการตามสิทธิเรียกร้องของบริษัทฯ

4.7 เพื่อการติดต่อ และการดำเนินธุรกิจของบริษัทฯ ตลอดระยะเวลาที่บริษัทฯ ยังมีความสัมพันธ์กับท่าน

### 5. บุคคลใดบ้างที่อาจจะได้รับข้อมูลส่วนบุคคลของท่านจากบริษัทฯ

บริษัทฯ อาจมีการเปิดเผย และ/หรือ โอนข้อมูลส่วนบุคคลของท่านไปยังบุคคลดังต่อไปนี้ โดยที่บุคคลดังกล่าวอาจอยู่ในประเทศไทย หรือนอกประเทศไทยก็ได้

5.1 สมาชิกใด ๆ ของกลุ่มบริษัท

5.2 ตัวแทน/นายหน้าประกันวินาศภัยของบริษัทฯ เพื่อวัตถุประสงค์ในการส่งเสริมหรือกระตุ้นให้เกิดการแข่งขัน สร้างผลงานหรือสร้างแรงจูงใจ

5.3 ที่ปรึกษาหรือผู้เชี่ยวชาญ ภายในหรือภายนอกของบริษัทฯ

5.4 ผู้ให้บริการใด ๆ หรือตัวแทนผู้ให้บริการ [รวมไปถึงผู้ให้บริการช่วง] ของบริษัทฯ

5.5 องค์กรที่เกี่ยวข้องกับการประกันภัย เช่น สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย [คปภ.] สมาคมหรือสภาอุตสาหกรรมประกันภัย

5.6 หน่วยงานรัฐใด ๆ ทางด้านภาษี กฎเกณฑ์ หรือผู้ซึ่งมีอำนาจเหนือบริษัทฯ ตามที่กฎหมายกำหนด หรือตามที่มีการร้องขอให้เปิดเผยเพื่อผลประโยชน์ของบริษัทฯ หรือเปิดเผยเพื่อประโยชน์สาธารณะ

5.7 ผู้รับโอนหรือผู้สืบทอดในบางส่วนใด ๆ ของบริษัทฯ เนื่องจากการซื้อหรือขายที่เกิดขึ้นจริงหรือการเสนอซื้อหรือขายบริษัท หรือกลุ่มบริษัท ทั้งหมดหรือบางส่วน

5.8 บุคคลอื่นใดที่ท่านได้ให้ความยินยอมโดยชัดแจ้งหรือโดยปริยาย เพื่อให้บรรลุเป้าหมายตามวัตถุประสงค์ที่กล่าวมาแล้วข้างต้น

## 6. การโอนข้อมูลไปยังประเทศอื่น/การโอนข้อมูลข้ามประเทศ

ข้อมูลส่วนบุคคลของท่านอาจถูกโอนไป ถูกจัดเก็บไว้ หรือประมวลผลโดยบริษัทฯ หรืออาจถูกส่งให้แก่บุคคลหรือหน่วยงานใด ๆ ตามรายละเอียดข้างต้น ซึ่งอาจมีที่ตั้งหรืออาจให้บริการอยู่ในประเทศไทยหรือนอกประเทศไทย ทั้งนี้ข้อมูลส่วนบุคคลของท่าน จะถูกโอนไปยังสถานที่อื่น ๆ ตามเงื่อนไขเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ดังที่ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลกำหนด โดยหากเป็นการโอนข้อมูลส่วนบุคคลของท่านระหว่างกลุ่มบริษัท บริษัทฯ จะดำเนินการตามนโยบายคุ้มครองข้อมูลส่วนบุคคลภายในกลุ่มบริษัท [Binding Corporate Rules] ที่ได้รับการอนุมัติจากคณะกรรมการ [หากมี]

## 7. การเก็บรักษาข้อมูลส่วนบุคคล

บริษัทฯ อาจเก็บรักษาข้อมูลส่วนบุคคลของท่านไว้ นานเท่าที่จำเป็นต้องเก็บเพื่อการดำเนินการให้บรรลุตามวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลของท่านตามที่ระบุข้างต้น ทั้งนี้บริษัทฯ จะเก็บรักษาข้อมูลส่วนบุคคลของท่านไม่เกิน 10 ปี นับแต่วันที่ท่านสิ้นสุดความสัมพันธ์ หรือการติดต่อครั้งสุดท้ายกับบริษัทฯ บริษัทฯ อาจเก็บรักษาข้อมูลส่วนบุคคลของท่านนานกว่าที่กำหนดหากมีความจำเป็นทางด้านกฎหมาย

บริษัทฯ จะดำเนินการตามขั้นตอนที่เหมาะสม เพื่อทำการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลของท่านเป็นข้อมูลที่ไม่สามารถระบุตัวท่าน ตามระยะเวลาเก็บรักษาข้อมูลส่วนบุคคลข้างต้น

## 8. สิทธิของท่านเกี่ยวกับข้อมูลส่วนบุคคล

ท่านมีสิทธิดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลของท่านดังต่อไปนี้

8.1 เพิกถอน หรือร้องขอให้เปลี่ยนแปลงขอบเขตความยินยอมของท่านได้ให้ไว้กับบริษัทฯ

8.2 ตรวจสอบว่าบริษัทฯ มีข้อมูลส่วนบุคคลใด ๆ เกี่ยวกับท่านหรือไม่ ตลอดจนสิทธิในการเข้าถึง หรือขอรับสำเนาของข้อมูลใด ๆ ดังกล่าว และ/หรือเข้าถึงข้อมูลว่าบริษัทฯ ประมวลผลข้อมูลส่วนบุคคลของท่านอย่างไร

8.3 ขอให้บริษัทฯ ทำการแก้ไขข้อมูลส่วนบุคคลใด ๆ ที่เกี่ยวข้องกับท่าน ให้ถูกต้อง

8.4 ขอให้ลบหรือทำลายข้อมูลส่วนบุคคลของท่านในบางสถานการณ์

8.5 ขอให้จำกัดการดำเนินการประมวลผลข้อมูลส่วนบุคคลของท่านในบางสถานการณ์

8.6 ขอให้บริษัทฯ โอนย้ายข้อมูลส่วนบุคคลของท่านในบางสถานการณ์

8.7 ขอให้ระงับการประมวลผลข้อมูลส่วนบุคคลของท่านเป็นการชั่วคราวในบางสถานการณ์

ทั้งนี้ บริษัทฯ ขอสงวนสิทธิไม่ปฏิบัติตามคำร้องขอใช้สิทธิของท่าน ตามความเหมาะสมและเท่าที่กฎหมายที่ใช้อยู่บังคับจะอนุญาต

นอกจากสิทธิเกี่ยวกับข้อมูลส่วนบุคคลที่ระบุข้างต้น ท่านมีสิทธิที่จะเสนอข้อร้องเรียนเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลของบริษัทฯ ต่อคณะกรรมการผู้เชี่ยวชาญตามขั้นตอนที่กำหนดใน พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลเท่าที่กฎหมายและกฎระเบียบที่ใช้อยู่บังคับอนุญาต บริษัทฯ อาจมีสิทธิเรียกเก็บค่าใช้จ่ายที่สมเหตุสมผล สำหรับการดำเนินการเกี่ยวกับคำร้องขอใช้สิทธิข้างต้น

## 9. การแก้ไขเปลี่ยนแปลงนโยบายฯ ฉบับนี้

บริษัทฯ ขอสงวนสิทธิในการแก้ไข เพิ่มเติม เปลี่ยนแปลง ปรับปรุง หรือปรับเปลี่ยนนโยบายฯ ฉบับนี้ เท่าที่กฎหมายอนุญาต หากเป็นการเปลี่ยนแปลงในสาระสำคัญของนโยบายฯ ฉบับนี้ บริษัทฯ จะแจ้งการแก้ไข การเปลี่ยนแปลง การปรับปรุง หรือการปรับเปลี่ยนนโยบายฯ ให้ท่านทราบ และ/หรือจะขอความยินยอมจากท่าน [หากกฎหมายกำหนดให้ต้องได้รับความยินยอม]

## 10. ช่องทางการติดต่อ

หากท่านมีข้อสงสัยเกี่ยวกับเนื้อหาส่วนใด ๆ ในนโยบายฯ ฉบับนี้ หรือต้องการข้อมูลเพิ่มเติมเกี่ยวกับแนวทางปฏิบัติของบริษัทฯ เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของท่าน หรือต้องการใช้สิทธิเกี่ยวกับข้อมูลส่วนบุคคลของท่าน กรุณาติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล [Data Protection Officer : DPO] ของบริษัทฯ ดังนี้

สำนักกำกับดูแล

บริษัท เทเวศประกันภัย จำกัด [มหาชน]

97 และ 99 อาคารเทเวศประกันภัย ถนนราชดำเนินกลาง แขวงบวรนิเวศ เขตพระนคร กรุงเทพฯ 10200

โทรศัพท์ 1291 ต่อ 8202, 8203 เวลาทำการ วันจันทร์ – วันศุกร์ เวลา 8.30 – 17.00 น.

อีเมล [dpo@deves.co.th](mailto:dpo@deves.co.th)

## 16.3 นโยบายคุ้มครองข้อมูลส่วนบุคคล [พนักงาน]

บริษัท เทเวศประกันภัย จำกัด [มหาชน] ตระหนักดีถึงสิทธิในความเป็นส่วนตัวและความรับผิดชอบของบริษัทฯ เกี่ยวกับการเก็บรวบรวม การใช้ การเปิดเผย ["การประมวลผล"] ข้อมูลส่วนบุคคลของท่าน บริษัทฯ จึงได้จัดทำ นโยบายคุ้มครองข้อมูลส่วนบุคคล [นโยบายฯ] ฉบับนี้ขึ้นมา เพื่อแจ้งรายละเอียดเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลของท่านตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ["พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล"]

### 1. บทนิยาม

"ข้อมูลส่วนบุคคล" หมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

"ข้อมูลส่วนบุคคลที่มีความอ่อนไหว" หมายถึง ข้อมูลตามที่กำหนดไว้ในมาตรา 26 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล และฉบับปรับปรุงแก้ไขตามที่จะมีการแก้ไขเป็นคราว ๆ กฎหมายและกฎระเบียบที่ใช้บังคับอื่น รวมถึงข้อมูลบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในท่านเองเดียวกัน

"พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล" หมายถึง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 รวมถึงกฎหมายลำดับรองที่ออกโดยอำนาจ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลในการตราขึ้น และตามที่มีการแก้ไขเป็นครั้งคราว

"คณะกรรมการ" หมายถึง คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

### 2. ข้อมูลส่วนบุคคลที่บริษัทอาจทำการเก็บรวบรวม

#### 2.1 กรณีที่ท่านเป็นผู้สมัครงาน

[ก] ข้อมูลที่ใช้ระบุตัวบุคคล เช่น ชื่อ ที่อยู่ หรือรายละเอียดของสถานที่ติดต่ออื่น เพศ อายุ สัญชาติ สถานภาพการสมรส วันเดือนปีเกิด รายละเอียดบัญชีธนาคาร เลขที่หนังสือเดินทาง/บัตรประจำตัวประชาชน ข้อมูลเกี่ยวกับผู้ที่อยู่ในการดูแลของท่าน และภาพถ่าย

[ข] ข้อมูลเกี่ยวกับคุณวุฒิและประวัติการทำงานของท่าน เช่น ประกาศนียบัตรจากโรงเรียน/มหาวิทยาลัย ประวัติการศึกษา การทดสอบทางวิชาการหรือภาษา ใบอนุญาตประกอบอาชีพหรือวิชาชีพ [เช่น ใบอนุญาตตัวแทน/นายหน้าประกันวินาศภัย] หนังสือรับรองและหนังสืออ้างอิง

[ค] ข้อมูลส่วนบุคคลที่มีความอ่อนไหว เช่น ข้อมูลสุขภาพ ประวัติอาชญากรรม เป็นต้น โดยบริษัทฯ จะเก็บรวบรวมข้อมูลส่วนบุคคลที่มีความอ่อนไหวเหล่านี้ต่อเมื่อท่านได้ผ่านการสัมภาษณ์งานแล้ว โดยบริษัทฯ จำเป็นต้องเก็บรวบรวมข้อมูลส่วนบุคคลที่มีความอ่อนไหวเหล่านี้เพื่อพิจารณาประกอบการเข้าทำสัญญา และประเมินความพร้อมในการเข้าทำงานของท่าน

#### 2.2 กรณีที่ท่านเป็นพนักงาน

หากท่านได้รับพิจารณาและเข้าทำสัญญาเป็นพนักงานของบริษัทฯ บริษัทฯ จะเก็บรวบรวม และประมวลผลข้อมูลส่วนบุคคลของท่านที่ไว้ตั้งแต่ขั้นตอนการสมัครงาน และจะเก็บรวบรวมข้อมูลส่วนบุคคลอื่น ๆ ของท่านเพิ่มเติม ดังนี้

[ก] รายละเอียดการทำงานพื้นฐาน เช่น หมายเลขพนักงาน ตำแหน่งงาน รายละเอียดของงาน สายการบังคับบัญชา ชั่วโมงการทำงานระเบียบและเงื่อนไขของการจ้างงาน

[ข] ข้อมูลทั่วไปที่เก็บรวบรวมจากการปฏิบัติงาน เช่น ประวัติส่วนตัว ประวัติการเกณฑ์ทหาร ข้อมูลการสัมภาษณ์งาน และหลักฐานอ้างอิงต่าง ๆ ข้อมูลจากระบบเฝ้าระวังและควบคุมการเข้า-ออกอาคารและสถานที่ กล้องวงจรปิด เทปบันทึกและการบันทึกข้อมูลการใช้โทรศัพท์ อีเมล และการบันทึกข้อมูลการใช้อินเทอร์เน็ตที่มีความเกี่ยวข้องกับการทำงานของท่านกับบริษัทฯ เท่าที่ไม่ขัดกับกฎหมาย

[ค] ข้อมูลเกี่ยวกับผลประโยชน์และค่าจ้าง เช่น รายละเอียดการจ่ายเงินเดือนและผลประโยชน์อื่นของท่าน ประกันสังคม ข้อมูลเกี่ยวกับการเกษียณอายุ/บำนาญ กองทุนสำรองเลี้ยงชีพ ข้อมูลทางภาษี และข้อมูลของบุคคลภายนอกผู้ได้รับผลประโยชน์

[ง] ประวัติเกี่ยวกับประสิทธิภาพของการทำงาน รวมถึงการประเมิน ผลตอบรับ ข้อมูลเกี่ยวกับระเบียบข้อบังคับการทำงานหรือการร้องทุกข์ ประวัติวันหยุดประจำปี ประวัติการลาป่วยหรือขาดงาน หรือข้อมูลที่เกี่ยวข้องกับการทำงานในสถานประกอบการและความปลอดภัย รวมถึงการตรวจสอบและการประเมินความเสี่ยง

[จ] ข้อมูลส่วนบุคคลที่มีความอ่อนไหว เช่น ประวัติสุขภาพ ทั้งนี้เป็นไปเพื่อการให้สวัสดิการแก่ท่าน เช่น การทำประกันสุขภาพ หรือการเบิกจ่ายค่ารักษาพยาบาล เป็นต้น

[ฉ] ข้อมูลที่ได้จากระบบบันทึกอัตโนมัติต่าง ๆ เช่น ภาพถ่าย ภาพเคลื่อนไหวจากกล้องวงจรปิด ข้อมูลจราจรคอมพิวเตอร์ เป็นต้น

ในกรณีที่ท่านได้ให้ข้อมูลส่วนบุคคลของบุคคลอื่นแก่บริษัทฯ เช่น สมาชิกในครอบครัว หรือญาติ เพื่อวัตถุประสงค์สำหรับกรณีเหตุฉุกเฉิน หรือเพื่อจัดการผลประโยชน์ ท่านรับทราบและยืนยันว่าได้แจ้งรายละเอียดที่เกี่ยวข้องตามนโยบายฯ นี้แก่บุคคลดังกล่าว และในกรณีที่บริษัทจำเป็นต้องได้รับความยินยอมในการประมวลผล

ข้อมูลส่วนบุคคล ท่านจะต้องดำเนินการใด ๆ ที่จำเป็นเพื่อให้บริษัทประมวลผลข้อมูลส่วนบุคคลของบุคคลเหล่านั้นได้อย่างถูกต้องตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล

### 3. บริษัทฯ เก็บรวบรวมข้อมูลส่วนบุคคลของท่านอย่างไร

โดยทั่วไป บริษัทฯ จะเก็บรวบรวมข้อมูลส่วนบุคคลของท่านโดยตรงจากท่าน และในบางกรณีบริษัทอาจจะต้องเก็บรวบรวมข้อมูลส่วนบุคคลของท่านจากแหล่งอื่น หรือบุคคลอื่น เช่น บุคคลที่แนะนำท่านให้กับบริษัทฯ บริษัทจัดหางานโรงพยาบาล หน่วยงานของรัฐที่เกี่ยวข้อง หรือบุคคลอื่น ๆ แล้วแต่กรณี

### 4. วัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคลของท่าน

#### 4.1 สำหรับผู้สมัครงาน

เพื่อพิจารณาและดำเนินการกระบวนการต่าง ๆ ที่จำเป็นในการรับสมัครงาน เช่น การพิจารณาประวัติของท่าน การสัมภาษณ์งาน การเตรียมเอกสารประกอบการรับสมัครงาน การจัดการเกี่ยวกับการตรวจสอบสุขภาพ และการดำเนินการอื่น ๆ ที่เกี่ยวข้อง

#### 4.2 สำหรับพนักงาน

[ก] เพื่อการพิจารณาข้อตกลงเกี่ยวกับการจ้าง การเตรียมเอกสารเพื่อเข้าทำสัญญาจ้าง รวมถึงการเข้าทำสัญญาจ้างกับบริษัทฯ

[ข] เพื่อการปฏิบัติตามสิทธิและหน้าที่ตามสัญญาจ้างระหว่างท่านกับบริษัทฯ

[ค] เพื่อบริหารจัดการการทำงาน สวัสดิการให้แก่ท่านและ/หรือบุคคลภายนอก [หากมี] ตามสัญญาระหว่างบริษัทฯ กับท่าน ซึ่งรวมถึงการการวัด/ ประเมินผล การฝึกอบรมเกี่ยวกับการจ้างงานและบริหารจัดการทรัพยากรบุคคลของบริษัทฯ เช่น การตรวจสอบข้อมูลของท่านตามกฎหมาย ข้อมูลทางกายภาพ การช่วยเหลือพนักงานในการปรับตัวเข้ากับงานใหม่ การจัดสวัสดิการ จัดทำบันทึกข้อมูลลูกจ้าง การทำประกัน ประวัติทางการแพทย์และแผนประกัน การวางแผนและการดำเนินการเกี่ยวกับการจ้างพนักงานและการฝึกอบรม การเลื่อนขั้น การย้ายงาน การมอบหมายให้พนักงานไปปฏิบัติงานที่อื่น และเพื่อปฏิบัติตามกระบวนการ กฎหมายและกฎเกณฑ์ที่ใช้บังคับ รวมถึงการวางแผนกำลังคน ข้อกำหนดการจ่ายค่าจ้าง ค่าชดเชย ผลประโยชน์ แผนค่าตอบแทน ข้อเสนอในอนาคต รางวัล บัญชีค่าตอบแทน การประเมินผลการปฏิบัติงาน การรายงานภายใน การวิเคราะห์ข้อมูล และการจัดการงานในการจ้างงานรายเดือนหรือรายวัน การติดต่อสื่อสารภายใน การแจ้งการนัดหมายแก่บุคคลทั้งภายในและภายนอก การประเมินใบสมัครงานสำหรับโอกาสในงานใหม่และการตัดสินใจในการจ้างงาน รวมถึงการประเมินการเลื่อนตำแหน่ง ความสามารถในการทำงานของท่าน การตรวจสอบโอกาสที่เท่าเทียมกัน

[ง] เพื่อการทําวินิจฉัย การวิเคราะห์ข้อมูล และการทําวินิจฉัยสถิติเกี่ยวกับการจ้างงาน การวัด/ ประเมินผล หรือกระบวนการที่คล้ายคลึงที่เกี่ยวกับการจ้างงานและบริหารจัดการทรัพยากรบุคคลของบริษัทฯ ซึ่งรวมถึงการทำแบบสำรวจ สถิติของรัฐบาล หรือการตอบแบบฟอร์มคำร้องใด ๆ ของรัฐ

[จ] เพื่อการดำเนินการให้เป็นไปตามข้อกำหนดภายใต้นโยบายภายในของบริษัทฯ ที่ยึดถือปฏิบัติ

[ฉ] เพื่อวัตถุประสงค์ในการบริหารจัดการ จัดเก็บ บันทึก สํารอง หรือทำลายข้อมูลส่วนบุคคล

[ช] เพื่อการติดตามพฤติกรรมของท่าน รวมถึงการตรวจสอบและสืบสวนข้อร้องเรียนเกี่ยวกับความประพฤติที่ไม่เหมาะสม การกระทำความผิดทางวินัย และ/หรือกฎหมาย ไม่ว่าจะเป็นการสืบสวนภายใน หรือการให้ความร่วมมือกับหน่วยงานรัฐที่มีอำนาจ

[ซ] เพื่อวิเคราะห์และจัดอบรมให้แก่ท่าน เพื่อพัฒนาศักยภาพและความสามารถในการทำงานของท่าน

[ฌ] เพื่อการปฏิบัติตามกฎหมาย และการตรวจสอบธุรกิจของบริษัทฯ ไม่ว่าจะเป็นการตรวจสอบภายใน หรือการตรวจสอบจากบุคคลภายนอก

[ญ] เพื่อดำเนินการให้เป็นไปตามข้อกำหนดของกฎหมาย กฎ ระเบียบ ข้อตกลง หรือนโยบายที่ใช้บังคับ ซึ่งกำหนดขึ้นโดยหน่วยงานกำกับดูแลของรัฐ หน่วยงานที่มีหน้าที่บังคับใช้กฎหมาย หน่วยงานรัฐ หน่วยงานที่มีหน้าที่ระงับข้อพิพาท หรือหน่วยงานที่ดูแลธุรกิจประกันภัย ไม่ว่าจะหน่วยงานใดก็ตาม

[ฎ] เพื่อวัตถุประสงค์ของการบังคับใช้กฎหมาย หรือการให้ความช่วยเหลือ ให้ความร่วมมือ การสืบสวนโดยบริษัทฯ หรือในนามของบริษัทฯ โดยเจ้าหน้าที่ตำรวจ หรือโดยหน่วยงานรัฐหรือหน่วยงานกำกับดูแลอื่น ๆ ในประเทศ และการดำเนินการตามหน้าที่ในการรายงาน และข้อกำหนดต่าง ๆ ตามที่กฎหมายกำหนด หรือตามที่มีการตกลงเห็นชอบกับหน่วยงานรัฐหรือหน่วยงานกำกับดูแลอื่น ๆ ในประเทศหรือเขตการปกครองใด ๆ หรือการดำเนินการตามคำสั่งโดยขอด้วยกฎหมายของพนักงานเจ้าหน้าที่ หรือหน่วยงานของรัฐ

[ฏ] เพื่อจัดระบบรักษาความปลอดภัยให้แก่ท่าน พนักงานคนอื่น หรือบุคคลอื่น ๆ ที่เข้าออกบริเวณอาคารของบริษัทฯ

[ฐ] เพื่อวัตถุประสงค์ในการปรับโครงสร้างองค์กรของบริษัทฯ และเพื่อการทำธุรกรรมของบริษัทฯ

[ฑ] เพื่อการเข้าซื้อหรืออาจจำหน่ายหนึ่ง หรือมากกว่าหนึ่งธุรกิจ [บางส่วนของธุรกิจ] ของบริษัทฯ

[ฒ] เพื่อการดำเนินการอื่น ๆ ที่จำเป็น ซึ่งเกี่ยวข้องโดยตรงกับวัตถุประสงค์ใด ๆ ข้างต้น

เว้นแต่กฎหมายและกฎระเบียบที่ใช้บังคับ รวมถึง พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลจะอนุญาตให้กระทำเป็นอย่างอื่น บริษัทฯ จะแจ้งและขอความยินยอมจากท่าน หากบริษัทฯ ประสงค์จะใช้ข้อมูลส่วนบุคคลของท่านเพื่อ



วัตถุประสงค์อื่นใดนอกเหนือไปจากที่ระบุไว้ในนโยบายฯ ฉบับนี้ หรือนอกเหนือไปจากวัตถุประสงค์ที่เกี่ยวข้องโดยตรงกับนโยบายฯ นี้

## 5. การเปิดเผยข้อมูลส่วนบุคคลของท่าน

ในการประมวลผลข้อมูลส่วนบุคคลเพื่อให้บรรลุวัตถุประสงค์ข้างต้น บริษัทอาจจำเป็นต้องเปิดเผยข้อมูลส่วนบุคคลของท่านให้แก่บุคคลภายนอก ดังนี้

[ก] บริษัทในเครือ

[ข] ที่ปรึกษาภายในหรือภายนอก ผู้เชี่ยวชาญ หรือที่ปรึกษาอื่นใดของบริษัทในเครือ

[ค] ผู้ให้บริการใด ๆ ซึ่งเป็นคู่สัญญาฝ่ายที่สาม หรือตัวแทนผู้ให้บริการใด ๆ ที่จำเป็นในการดำเนินการตามวัตถุประสงค์ในการประมวลผลข้างต้น เช่น ตัวแทน/นายหน้าประกันภัย บริษัทผู้รับประกันภัย ผู้สรรหาบุคลากร ผู้ให้บริการสนับสนุน และ/หรือดูแลรักษาระบบเทคโนโลยีสารสนเทศของบริษัทฯ หรือโปรแกรมที่ช่วยในการสรรหาบุคลากร ระบบบัญชีค่าตอบแทน ผลประโยชน์ และระบบของฝ่ายทรัพยากรบุคคลอื่น ๆ

[ง] หน่วยงานของรัฐ หรือเจ้าพนักงานด้านภาษี กฎเกณฑ์ หรือเจ้าพนักงานรัฐใด ๆ หรือผู้รับมอบอำนาจซึ่งมีอำนาจเหนือสมาชิกใด ๆ ของบริษัทในเครือตามที่กฎหมายกำหนด หรือตามที่มีการร้องขอให้เปิดเผยผลประโยชน์ของบริษัทในเครือหรือเปิดเผยเพื่อประโยชน์สาธารณะ

[จ] ผู้รับโอนหรือ ผู้สืบทอดในส่วนตัว ๆ ของบริษัทฯ ในเครือหรือผู้ที่อาจเป็นในอนาคต หรือในบริบทของการปรับโครงสร้างองค์กรที่จะเป็นส่วนหนึ่งของการซื้อหรือขายกิจการหรือการเสนอซื้อหรือขาย

[ฉ] บุคคลอื่นใดที่ท่านได้ให้ความยินยอมโดยชัดแจ้งหรือโดยปริยาย

[ช] กองทุนสำรองเลี้ยงชีพ เพื่อให้บรรลุเป้าหมายตามวัตถุประสงค์ที่กล่าวมาแล้วข้างต้น

## 6. การโอนข้อมูลไปยังต่างประเทศ

ข้อมูลส่วนบุคคลของท่านอาจถูกโอนไป ถูกจัดเก็บไว้ หรือประมวลผลโดยบริษัทฯ หรืออาจถูกส่งให้แก่บุคคลหรือหน่วยงานใด ๆ ตามรายละเอียดข้างต้น ซึ่งอาจมีที่ตั้งหรืออาจให้บริการอยู่นอกประเทศไทย ทั้งนี้ข้อมูลส่วนบุคคลของท่าน จะถูกโอนไปยังสถานที่อื่น ๆ ตามเงื่อนไขเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ดังที่ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลกำหนด โดยหากเป็นการโอนข้อมูลส่วนบุคคลของท่านระหว่างกลุ่มบริษัท บริษัทฯ จะดำเนินการตามนโยบายคุ้มครองข้อมูลส่วนบุคคลภายในกลุ่มบริษัท [Binding Corporate Rules] ที่ได้รับการอนุมัติจากคณะกรรมการ [หากมี]

## 7. การเก็บรักษาข้อมูลส่วนบุคคล

บริษัทฯ มีนโยบายที่จะเก็บรักษาข้อมูลส่วนบุคคลตราบเท่าที่จำเป็น เพื่อบรรลุวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลตามที่กำหนดข้างต้น โดยบริษัทมีนโยบายเก็บรักษาข้อมูลส่วนบุคคลของท่านตลอดระยะเวลาการจ้างงาน หรือตลอดระยะเวลาที่มีนิติสัมพันธ์ต่อกัน และเมื่อสิ้นสุดนิติสัมพันธ์ต่อกันแล้ว บริษัทฯ จะเก็บรักษาข้อมูลส่วนบุคคลของท่านต่อไปอีกเป็นระยะเวลา 10 ปี เว้นแต่กฎหมายที่ใช้บังคับกำหนดหรืออนุญาต สำหรับการเก็บรักษาในระยะเวลาที่ยาวกว่าที่ระบุข้างต้น

## 8. สิทธิของท่านเกี่ยวกับข้อมูลส่วนบุคคล

ท่านมีสิทธิดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลของท่านดังต่อไปนี้

[ก] เพิกถอน หรือร้องขอให้เปลี่ยนแปลงขอบเขตความยินยอมของท่านได้ให้ไว้กับบริษัทฯ

[ข] ตรวจสอบว่าบริษัทฯ มีข้อมูลส่วนบุคคลใด ๆ เกี่ยวกับท่านหรือไม่ ตลอดจนสิทธิในการเข้าถึง หรือขอรับสำเนาของข้อมูลใด ๆ ดังกล่าว และ/หรือเข้าถึงข้อมูลว่าบริษัทฯ ประมวลผลข้อมูลส่วนบุคคลของท่านอย่างไร

[ค] ขอให้บริษัทฯ ทำการแก้ไขข้อมูลส่วนบุคคลใด ๆ ที่เกี่ยวข้องกับท่าน ให้ถูกต้อง

[ง] ขอให้ลบหรือทำลายข้อมูลส่วนบุคคลของท่านในบางสถานการณ์

[จ] ขอให้จำกัดการดำเนินการประมวลผลข้อมูลส่วนบุคคลของท่านในบางสถานการณ์

[ฉ] ขอให้บริษัทฯ โอนย้ายข้อมูลส่วนบุคคลของท่านในบางสถานการณ์

[ช] ขอให้ระงับการประมวลผลข้อมูลส่วนบุคคลของท่านเป็นการชั่วคราวในบางสถานการณ์

ทั้งนี้ บริษัทฯ ขอสงวนสิทธิไม่ปฏิบัติตามคำร้องขอใช้สิทธิของท่าน ตามความเหมาะสมและเท่าที่กฎหมายที่ใช้บังคับจะอนุญาต

นอกจากสิทธิเกี่ยวกับข้อมูลส่วนบุคคลที่ระบุข้างต้น ท่านมีสิทธิที่จะเสนอข้อร้องเรียนเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลของบริษัทฯ ต่อคณะกรรมการผู้เชี่ยวชาญตามขั้นตอนที่กำหนดใน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลเท่าที่กฎหมายและกฎระเบียบที่ใช้บังคับอนุญาต บริษัทฯ อาจมีสิทธิเรียกเก็บค่าใช้จ่ายที่สมเหตุสมผล สำหรับการดำเนินการเกี่ยวกับคำร้องขอใช้สิทธิข้างต้น

## 9. การแก้ไขเปลี่ยนแปลงนโยบายฯ ฉบับนี้

บริษัทฯ ขอสงวนสิทธิ์ในการแก้ไข เพิ่มเติม เปลี่ยนแปลง ปรับปรุง หรือปรับเปลี่ยนนโยบายฯ ฉบับนี้ เท่าที่กฎหมายอนุญาต หากเป็นการเปลี่ยนแปลงในสาระสำคัญของนโยบายฯ ฉบับนี้ บริษัทจะแจ้งการแก้ไข การเปลี่ยนแปลง การปรับปรุง หรือการปรับเปลี่ยนนโยบายฯ ให้ท่านทราบ และ/หรือ จะขอความยินยอมจากท่าน [หากกฎหมายกำหนดให้ต้องได้รับความยินยอม]

## 10. ช่องทางการติดต่อ

หากท่านมีข้อสงสัยเกี่ยวกับเนื้อหาส่วนใด ๆ ในนโยบายฯ ฉบับนี้ หรือต้องการข้อมูลเพิ่มเติมเกี่ยวกับแนวทางปฏิบัติของบริษัทฯ เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของท่าน หรือต้องการใช้สิทธิเกี่ยวกับข้อมูลส่วนบุคคลของท่าน กรุณาติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล [Data Protection Officer : DPO] ของบริษัทฯ ดังนี้

สำนักกำกับดูแล

บริษัท เทเวศประกันภัย จำกัด [มหาชน]

97 และ 99 อาคารเทเวศประกันภัย ถนนราชดำเนินกลาง แขวงบวรนิเวศ เขตพระนคร กรุงเทพฯ 10200

โทรศัพท์ 1291 ต่อ 8202, 8203 เวลาทำการ วันจันทร์ – วันศุกร์ เวลา 8.30 – 17.00 น.

อีเมล [dpo@deves.co.th](mailto:dpo@deves.co.th)

## 17. นโยบายการบริหารงานคุณภาพและความมั่นคงปลอดภัยสารสนเทศ

บริษัท เทเวศรประกันภัย จำกัด [มหาชน] ได้ให้ความสำคัญต่อกระบวนการปฏิบัติงาน และความมั่นคงปลอดภัยสารสนเทศ เพื่อปรับปรุงระบบงานให้มีประสิทธิภาพยิ่งขึ้น มีการบริการที่ดี มีคุณภาพและมั่นคงปลอดภัย สามารถสร้างความพึงพอใจและตอบสนองความต้องการของลูกค้าได้อย่างต่อเนื่องและเป็นธรรม บริษัทฯ จึงได้นำระบบบริหารงานคุณภาพเข้ามาประยุกต์ใช้ในการปฏิบัติงาน จนได้รับการรับรองมาตรฐานระบบบริหารงานคุณภาพ ISO 9001 ตั้งแต่ปี 2542 เป็นต้นมา รวมทั้งนำระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC 27001:2013 มาเป็นกรอบการปฏิบัติงานที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศของบริษัทฯ และเพื่อให้ผู้บริหารและพนักงานมีปรัชญาและอุดมการณ์เป็นไปในแนวทางเดียวกัน บริษัทฯ จึงได้กำหนดนโยบายการบริหารงานคุณภาพและความมั่นคงปลอดภัยสารสนเทศไว้ดังนี้

มุ่งมั่นพัฒนาด้วยนวัตกรรมด้านบริการและผลิตภัณฑ์ที่มีคุณภาพและมั่นคงปลอดภัย เพื่อเพิ่มประสิทธิภาพ และสร้างความพึงพอใจให้แก่ลูกค้าและพันธมิตรทางธุรกิจ

ตามปณิธานข้างต้น ถือเป็นหน้าที่และความรับผิดชอบร่วมกันของผู้บริหารและพนักงานทุกคน ที่มีภาระผูกพันในการดำรงรักษาไว้ซึ่งระบบบริหารงานคุณภาพและระบบบริหารความมั่นคงปลอดภัยสารสนเทศ โดยพัฒนาอย่างยั่งยืนตลอดไป บริษัทฯ จะให้ความรู้เกี่ยวกับระบบบริหารงานคุณภาพและระบบบริหารความมั่นคงปลอดภัยสารสนเทศ เผยแพร่นโยบายการบริหารงานคุณภาพและระบบบริหารความมั่นคงปลอดภัยสารสนเทศ เพื่อให้ผู้บริหารและพนักงานรับทราบ เข้าใจ นำไปปฏิบัติอย่างจริงจัง และปรับปรุงคุณภาพการดำเนินงานอย่างต่อเนื่อง

บริษัทฯ กำหนดให้มีกระบวนการและช่องทางการรับข้อร้องเรียน รวมถึงบริหารจัดการข้อร้องเรียนด้วยความเป็นธรรม สอดคล้องตามประกาศที่สำนักงาน คปภ. กำหนด และมีการรายงานไปยังคณะกรรมการที่ได้รับมอบหมายเพื่อรับทราบผลการดำเนินการอย่างสม่ำเสมอ

ผู้บริหารมีหน้าที่ควบคุมดูแลให้พนักงานปฏิบัติและดำรงรักษาไว้ซึ่งระบบบริหารงานคุณภาพและระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ให้มีการพัฒนาอย่างต่อเนื่องและยั่งยืน ในส่วนของพนักงานก็มีหน้าที่รับทราบและปฏิบัติตามเจตนารมณ์ของนโยบายการบริหารงานคุณภาพและระบบบริหารความมั่นคงปลอดภัยสารสนเทศ เข้าใจในบทบาทหน้าที่ของตนเองในการสนับสนุนให้บริษัทฯ บรรลุตามเจตจำนงดังนี้

บริษัทฯ ได้กำหนดวัตถุประสงค์คุณภาพและความมั่นคงปลอดภัยสารสนเทศ เพื่อให้สอดคล้องกับนโยบายคุณภาพและความมั่นคงปลอดภัยสารสนเทศไว้ดังนี้

- “มุ่งมั่นพัฒนาด้วยนวัตกรรมด้านบริการและผลิตภัณฑ์ที่มีคุณภาพและมั่นคงปลอดภัย เพื่อเพิ่มประสิทธิภาพ” ประกอบด้วย
  - นวัตกรรมใหม่ ๆ เพื่อเพิ่มประสิทธิภาพระบบการดำเนินงานของบริษัทฯ อย่างมีคุณภาพและมั่นคงปลอดภัย
  - บุคลากรที่มีคุณภาพและมีการปฏิบัติงานอย่างมั่นคงปลอดภัย
  - บริการและผลิตภัณฑ์ที่มีคุณภาพและมั่นคงปลอดภัย
- “สร้างความพึงพอใจให้แก่ลูกค้าและพันธมิตรทางธุรกิจ” ประกอบด้วย
  - ลูกค้าภายใน ได้แก่ หน่วยงานต่าง ๆ ภายในบริษัทฯ
  - ลูกค้าภายนอก ได้แก่ ผู้ซื้อกรมธรรม์ คู่ค้า และผู้ให้บริการต่าง ๆ
  - พันธมิตรธุรกิจ ได้แก่ บริษัทประกันภัยต่อ บริษัทสำรวจภัย คู่ รานอะไหล่ ฯลฯ

ดังนั้นเพื่อการบริการที่มีคุณภาพและมั่นคงปลอดภัย ฝ่ายบริหารจึงได้กำหนดให้หน่วยงานต่าง ๆ จัดทำแผนงานที่เกี่ยวข้องดังนี้

- การพัฒนาคุณภาพบุคลากรให้เป็นไปตามข้อกำหนด Competency Model ของบริษัทฯ
- การพัฒนากระบวนการดำเนินงานอย่างมีคุณภาพและมั่นคงปลอดภัย มีประสิทธิภาพและประสิทธิผล
- การพัฒนาผลิตภัณฑ์และบริการใหม่ ๆ อย่างมีคุณภาพและมั่นคงปลอดภัย
- การจัดทำแผนงานที่เชื่อมโยงกันระหว่างระบบบริหารงานคุณภาพ บริหารความมั่นคงปลอดภัยสารสนเทศ และการบริหารความเสี่ยงของบริษัทฯ รวมถึงกำหนดให้มีวัตถุประสงค์คุณภาพและความมั่นคงปลอดภัยสารสนเทศระดับหน่วยงาน กำหนดผู้รับผิดชอบ ประเมินผลและรายงานในที่ประชุมคณะต่าง ๆ อย่างสม่ำเสมอ

## 18. นโยบายการควบคุมภายใน

การควบคุมภายในที่มีประสิทธิภาพจะช่วยสนับสนุนการตัดสินใจในการจัดการความเสี่ยงและสามารถป้องกันความเสียหายที่จะเกิดขึ้นได้อย่างทันกาล เพื่อให้บริษัทประกันภัยมีโครงสร้างองค์กรและมาตรการที่เกี่ยวข้องกับการควบคุมภายในที่เหมาะสม สำหรับการดำเนินกิจกรรมทางการเงินและกิจการหลักของบริษัทประกันภัยให้มีความมั่นคง โปร่งใส และมีความเชื่อมั่นต่อผู้เอาประกันภัย

เพื่อให้การควบคุมภายในของบริษัทประกันภัยมีประสิทธิภาพและประสิทธิผล สำนักงาน คปภ. จึงได้ออกประกาศ คปภ. ว่าด้วยเรื่อง หลักเกณฑ์ วิธีการ และเงื่อนไขในการรับเงิน การจ่ายเงิน การตรวจสอบและการควบคุมภายใน ซึ่งกำหนดให้บริษัทฯ ต้องมีการติดตาม ประเมินความเพียงพอและประสิทธิภาพของระบบควบคุมภายในอย่างสม่ำเสมอ รวมถึงบริษัทฯ ต้องมีการทบทวนความเพียงพอของระบบควบคุมภายในของหน่วยงานต่าง ๆ เป็นระยะอย่างน้อยปีละหนึ่งครั้ง ทั้งนี้ บริษัทฯ ได้จัดให้มีการประเมินการควบคุมภายในตามแนวทาง การประเมินการควบคุมภายใน ที่คปภ.กำหนด สำหรับบริษัทประกันภัย และรายงานผลการประเมินการควบคุมภายในของบริษัทฯ โดยรวมต่อ คณะกรรมการบริษัท โดยให้คณะกรรมการตรวจสอบแสดงความเห็นประกอบการรายงานทุกครั้ง

นอกจากนี้ สำนักงาน คปภ. ได้จัดทำแนวทางการประเมินการควบคุมภายในของบริษัทประกันภัย เพื่อให้บริษัทฯ ได้นำไปปรับใช้สำหรับการประเมินหรือทบทวนการควบคุมภายในของบริษัทฯ และคาดหวังว่าผลจาก แนวทางฯ ดังกล่าว จะทำให้บริษัทประกันภัย คณะกรรมการบริษัท คณะกรรมการตรวจสอบ รวมถึงผู้บริหารของบริษัทประกันภัยสามารถนำผลจากการประเมินฯ ไปใช้ประกอบการทบทวนกลยุทธ์ และการบริหารความเสี่ยงของบริษัทฯ ว่าควรมีการพัฒนา หรือปรับปรุงการควบคุมภายในของบริษัทฯ ตามกิจกรรมการดำเนินงานที่สำคัญ และสอดคล้องกับโครงสร้างหน่วยงานของบริษัทฯ ที่ดูแลเกี่ยวกับการควบคุมการปฏิบัติงาน ซึ่งมีผลทำให้การดำเนินงานมีประสิทธิภาพ อันจะทำให้ธุรกิจประกันภัยมีความเข้มแข็ง มีการกำกับดูแลกิจการที่ดี และมีการบริหารความเสี่ยงแบบองค์รวมที่เข้มแข็งและเป็นที่ยอมรับของประชาชน

คณะกรรมการบริษัทจึงได้กำหนดให้มีนโยบายการควบคุมภายใน เพื่อมุ่งสู่การเป็นองค์กรแห่งการกำกับดูแลกิจการที่ดี และมีการปรับปรุงการควบคุมภายในอย่างต่อเนื่อง เพื่อสร้างให้เป็นวัฒนธรรมในการดำเนินงานของบริษัทฯ และสอดคล้องกับมาตรฐานสากล/กรอบการควบคุมภายในตามแนวทางของ COSO

### องค์ประกอบของการควบคุมภายใน

#### 1. สภาพแวดล้อมการควบคุม [Control Environment]

บริษัทฯ ต้องมีสภาพแวดล้อมของการควบคุมที่เหมาะสม รวมทั้ง มีการส่งเสริมวัฒนธรรมการบริหารความเสี่ยง และควบคุมความเสี่ยงของบริษัทฯ ให้อยู่ในระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) เพื่อให้มั่นใจได้ว่าการดำเนินการของบริษัทฯ ได้รับการบริหารจัดการและควบคุมอย่างระมัดระวัง โดยสภาพแวดล้อมของการควบคุมประกอบด้วยปัจจัยที่สำคัญคือ คณะกรรมการและผู้บริหารของบริษัทฯ การควบคุมทางด้านโครงสร้างและวิธีการปฏิบัติงานการตรวจสอบอย่างเป็นอิสระ โดยสื่อสารให้พนักงานทุกคนในบริษัทฯ เข้าใจ ตระหนักถึงความสำคัญของนโยบายด้านการควบคุมภายในของบริษัทฯ โดยบริษัทฯ ได้จัดให้มีแนวทางการควบคุม ดังนี้

- บริษัทฯ ต้องยึดหลักความซื่อสัตย์สุจริต จรรยาบรรณ และจริยธรรมทางธุรกิจซึ่งต้องมีการดำเนินการที่แสดงให้เห็นถึงความรับผิดชอบต่อความซื่อสัตย์สุจริตและจริยธรรมของทั้งองค์กร
- คณะกรรมการบริษัทมีความเป็นอิสระจากฝ่ายบริหาร และมีการกำกับดูแลการควบคุมภายในของบริษัทฯ
- ฝ่ายบริหารได้จัดให้มีโครงสร้างสายการรายงาน การกำหนดอำนาจในการสั่งการ และความรับผิดชอบที่เหมาะสมภายใต้การกำกับดูแลของคณะกรรมการบริษัทเพื่อให้บริษัทฯ บรรลุวัตถุประสงค์หรือเป้าหมายในการดำเนินธุรกิจ
- บริษัทฯ มีกระบวนการที่จูงใจและรักษาบุคลากรที่มีศักยภาพ เพื่อสนับสนุนการดำเนินการของบริษัทฯ ให้เป็นไปตามเป้าหมาย หรือวัตถุประสงค์ในการดำเนินธุรกิจ
- บริษัทฯ มีการกำหนดให้บุคลากรทุกตำแหน่งงาน รับผิดชอบต่อการควบคุมภายใน ตามวัตถุประสงค์ที่บริษัทฯ กำหนด

#### 2. การบริหารความเสี่ยง [Risk Assessments]

เนื่องจากธุรกิจประกันภัยเป็นธุรกิจที่เกี่ยวข้องโดยตรงกับการบริหารความเสี่ยง ทั้งนี้ บริษัทฯ จึงพึงมีระบบการบริหารความเสี่ยงที่มีประสิทธิภาพ เพื่อสนับสนุนการตัดสินใจและการวิเคราะห์เชิงกลยุทธ์ ซึ่งรวมไปถึงกรอบการบริหารความเสี่ยง นโยบายการบริหารความเสี่ยง ที่สามารถเชื่อมโยงกลยุทธ์ทางธุรกิจ และการดำรงเงินกองทุน การประเมินความมั่นคงทางการเงิน และการกำกับดูแลกิจการที่ดี ที่มีประสิทธิภาพ เหมาะสมกับขนาด ลักษณะ และความซับซ้อนของกิจกรรมการดำเนินธุรกิจของบริษัทฯ โดยต้องเป็นไปตาม ประกาศ คปภ. ว่าด้วยเรื่อง หลักเกณฑ์ วิธีการ และเงื่อนไขในการกำกับการบริหารความเสี่ยงแบบองค์รวม และการประเมินความเสี่ยงและความมั่นคงทางการเงินของบริษัทประกันวินาศภัย โดยบริษัทฯ ได้จัดให้มีแนวทางการควบคุม ดังนี้

- บริษัทฯ มีการกำหนดเป้าหมายอย่างชัดเจนและเพียงพอที่จะช่วยในการระบุและประเมินความเสี่ยงที่ส่งผลกระทบต่อการบรรลุเป้าหมายหรือวัตถุประสงค์ในการดำเนินธุรกิจของบริษัทฯ
- บริษัทฯ มีการระบุและวิเคราะห์ความเสี่ยงอย่างครอบคลุมเพื่อพิจารณาวิธีการจัดการความเสี่ยงที่เหมาะสม
- บริษัทฯ มีการพิจารณาโอกาสที่จะเกิดการทุจริต และการฉ้อฉล ซึ่งส่งผลกระทบต่อการบรรลุเป้าหมายหรือวัตถุประสงค์ในการดำเนินธุรกิจของบริษัทฯ
- บริษัทฯ มีการระบุและประเมินการเปลี่ยนแปลงที่อาจจะกระทบต่อการควบคุมภายในอย่างมีนัยสำคัญ

### 3. กิจกรรมควบคุม [Control Activities]

กิจกรรมการควบคุม เป็นกลไกในการดำเนินการผ่านการใช้นโยบายหรือวิธีปฏิบัติที่มุ่งเน้นให้ บริษัทฯ สามารถบรรลุวัตถุประสงค์ในการดำเนินธุรกิจ และสนับสนุนให้มีการรายงานและการปฏิบัติตามกฎหมายได้อย่างมีประสิทธิภาพ เพื่อให้บริษัทฯ สามารถดำเนินธุรกิจได้อย่างมั่นคง และคำนึงถึงผลประโยชน์ของผู้เอาประกันภัยได้อย่างรอบด้าน โดยบริษัทฯ ได้จัดให้มีแนวทางการควบคุม ดังนี้

- บริษัทฯ มีการกำหนด และพัฒนากิจกรรมการควบคุม เพื่อให้มีกระบวนการบรรเทาความเสี่ยง และสามารถดำเนินธุรกิจให้เป็นไปตามเป้าหมาย หรือวัตถุประสงค์ที่ตั้งไว้
- บริษัทฯ มีการกำหนด และพัฒนากิจกรรมควบคุมที่เหมาะสมกับการใช้เทคโนโลยีของบริษัทฯ และมีการพัฒนาระบบเทคโนโลยีเพื่อใช้สนับสนุนด้านการควบคุมภายใน และการบริหารความเสี่ยง
- บริษัทฯ มีกิจกรรมควบคุมผ่านการกำหนดนโยบายหรือขั้นตอนในการปฏิบัติงานที่เหมาะสม

ทั้งนี้ กิจกรรมควบคุมที่เหมาะสมเพื่อให้มั่นใจได้ว่าบริษัทฯ จะสามารถดำเนินธุรกิจได้บรรลุตามวัตถุประสงค์หรือเป้าหมายที่ตั้งไว้ได้ เช่น การพัฒนาผลิตภัณฑ์ และกำหนดเบี้ยประกันภัย , การเสนอขาย และ การเก็บเบี้ยประกันภัย , การพิจารณารับประกันภัย , การประเมินสำรองประกันภัย , การบริหารจัดการค่าสินไหมทดแทน , การประกันภัยต่อ , การลงทุนประกอบธุรกิจอื่น , การบริหารสินทรัพย์และหนี้สิน และการใช้บริการจากบุคคลภายนอก

### 4. สารสนเทศและการสื่อสาร [Information and Communication]

ระบบสารสนเทศ คือ กระบวนการประมวลผลข้อมูลเกี่ยวกับการดำเนินงานของบริษัทฯ และความเสี่ยงที่บริษัทฯ กำลังประสบอยู่หรืออาจจะประสบในอนาคต และรายงานข้อมูลที่ได้จากการประมวลผลในรูปแบบที่ทำให้บุคลากรในบริษัทฯ สามารถใช้ในการติดตาม สอบทานและปฏิบัติงานตามความรับผิดชอบของตน รวมถึงการจัดทำรายงานต่อบุคคลภายนอก เช่น ผู้เอาประกันภัย ผู้ถือหุ้น และหน่วยงานกำกับดูแล เป็นต้น นอกจากนี้ บริษัทฯ ต้องมีการสอบทานระบบสารสนเทศอย่างเป็นประจำเพื่อประเมินความเหมาะสมและความเป็นปัจจุบันของรายงาน รวมถึงคุณภาพของการประมวลผลข้อมูล โดยบริษัทฯ ได้จัดให้มีแนวทางการควบคุม ดังนี้

- บริษัทฯ มีข้อมูลที่ใช้เป็นเพื่อใช้ในการสนับสนุนการดำเนินการด้านการควบคุมภายในของบริษัทฯ
- บริษัทฯ มีการสื่อสารข้อมูลที่จำเป็น รวมถึงเป้าหมายและความรับผิดชอบที่เกี่ยวข้องกับการควบคุมภายใน เพื่อสนับสนุนการดำเนินงานได้อย่างต่อเนื่องและมีประสิทธิภาพของระบบควบคุมภายในของบริษัทฯ
- บริษัทฯ มีการสื่อสารกับหน่วยงานภายนอก ในประเด็นที่อาจกระทบต่อการควบคุมภายใน

ทั้งนี้ บริษัทฯ ต้องมีการปฏิบัติตามประกาศ คปภ. เรื่อง หลักเกณฑ์การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัทฯ ประกันวินาศภัย เพื่อให้บริษัทฯ มีการกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยคุกคามทางไซเบอร์ได้อย่างเหมาะสม และเป็นระบบ รวมทั้งมีการควบคุมและรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศได้อย่างเหมาะสม สอดคล้องกับมาตรฐานสากล ISO 27001 : 2013 ตลอดจนการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง โดยจัดให้มีการว่าจ้างผู้ตรวจสอบระบบเทคโนโลยีสารสนเทศ ดำเนินการตามหลักเกณฑ์ที่คปภ.กำหนด

### 5. กิจกรรมการกำกับติดตามและประเมินผล [Monitoring Activities]

บริษัทฯ มีกระบวนการในการติดตามและประเมินประสิทธิผลของระบบการควบคุมภายในและสภาพแวดล้อมของการควบคุม โดยบริษัทฯ ได้จัดให้มีหน่วยงานตรวจสอบภายในและผู้สอบบัญชีภายนอก ทำหน้าที่สอบทานหรือประเมินผล อย่างเป็นอิสระ เพื่อให้บริษัทฯ เชื่อมั่นได้ว่า องค์ประกอบของการควบคุมภายในของบริษัทฯ จะสามารถดำเนินการได้อย่างต่อเนื่องและมีประสิทธิภาพ รวมถึงบริษัทฯ สามารถดำเนินธุรกิจได้อย่างมั่นคง ต่อเนื่อง และสามารถทนทานต่อสภาพแวดล้อมในการดำเนินธุรกิจที่เปลี่ยนแปลงไป และรับผิดชอบต่อผู้เอาประกันภัยและประชาชน โดยบริษัทฯ ได้จัดให้มีแนวทางการควบคุม ดังนี้

- บริษัทฯ มีการติดตามและประเมินผลการควบคุมภายใน เพื่อให้มั่นใจได้ว่าระบบควบคุมภายในของบริษัทฯ จะสามารถดำเนินการได้อย่างต่อเนื่องและมีประสิทธิภาพ
- บริษัทฯ มีการประเมินและสื่อสารประเด็นที่ต้องมีการปรับปรุงของการควบคุมภายในอย่างทันกาลและเหมาะสม

## 19. นโยบายการกำกับดูแลข้อมูล

ข้อมูลเป็นทรัพย์สินที่สำคัญของบริษัทฯ การนำเทคโนโลยีมาประยุกต์เพื่อใช้ประโยชน์จากข้อมูลในการขับเคลื่อนการดำเนินธุรกิจมีเพิ่มมากขึ้น เพื่อให้มั่นใจว่า บริษัทฯ มีการกำกับดูแลและบริหารจัดการข้อมูลได้อย่างมีคุณภาพและมีความมั่นคงปลอดภัยเป็นมาตรฐานสากล รวมทั้งเป็นไปการกฎเกณฑ์และกฎหมายที่เกี่ยวข้อง จึงได้กำหนดนโยบายการกำกับดูแลข้อมูล [Data Governance] ดังนี้

- บริษัทฯ มีการกำหนดโครงสร้างการกำกับดูแลข้อมูลตามหลัก Three lines of Defense เพื่อให้แบ่งแยกหน้าที่กันอย่างชัดเจน โดยประกอบไปด้วย
  - คณะกรรมการกำกับดูแลข้อมูล ทำหน้าที่กำหนดนโยบาย ทิศทางและกรอบแนวทางการดำเนินงาน โดยจัดให้มีคณะทำงานทำหน้าที่กลั่นกรองและเป็นบริกรข้อมูลร่วมกับส่วนงานที่เกี่ยวข้อง และรายงานต่อคณะกรรมการกำกับดูแลข้อมูล
  - กำหนดให้มีส่วนงานจัดทำกรอบและกระบวนการบริหารความเสี่ยงให้ครอบคลุมความเสี่ยงด้านข้อมูล สนับสนุนให้มีการประเมินความเสี่ยงด้านข้อมูล ให้คำปรึกษา ติดตามและทบทวนความเสี่ยงด้านข้อมูลให้อยู่ในระดับที่ยอมรับได้ นอกจากนี้จะต้องทำหน้าที่กำกับการปฏิบัติตามกฎเกณฑ์และกฎหมาย กำกับดูแลการปฏิบัติงานที่เกี่ยวข้องกับข้อมูล เพื่อป้องกันการละเมิดหรือไม่ปฏิบัติตามกฎเกณฑ์และกฎหมายที่เกี่ยวข้อง
  - กำหนดให้มีส่วนงานทำหน้าที่ตรวจสอบการปฏิบัติงานและการบริหารความเสี่ยงที่เกี่ยวข้องกับข้อมูลเพื่อสอบทานให้มั่นใจว่า เป็นไปตามนโยบาย มาตรฐาน และระเบียบวิธีปฏิบัติการกำกับดูแลข้อมูล
  - มีการทบทวนและประเมินประสิทธิภาพของนโยบายอย่างน้อยปีละ 1 ครั้งหรือทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ
- จัดให้มีการสื่อสารเสริมสร้างความตระหนักรู้ด้านการกำกับดูแลข้อมูลให้กับพนักงานทุกระดับรวมถึงจัดให้มีกระบวนการควบคุมดูแล บุคคลภายนอกที่อาจจ่าง ให้เข้าใจ รับทราบและลงนามยอมรับเงื่อนไขการว่าจ้างที่ครอบคลุมการรักษาความมั่นคงปลอดภัยด้านข้อมูล และ ข้อตกลงการไม่เปิดเผยข้อมูลก่อนเริ่มปฏิบัติงาน โดยประกาศใช้อย่างเป็นทางการ และมีผลให้ทุกคนในองค์กรถือปฏิบัติ
- จัดให้มีการบริหารจัดการข้อมูล [Data Management] โดยประกอบไปด้วย
  - การบริหารวงจรชีวิตข้อมูล [Data Life Cycle] ได้แก่การสร้างหรือการได้มาซึ่งข้อมูล การประมวลผล การจัดเก็บ การใช้งาน การเผยแพร่ และการทำลายข้อมูล
  - การบริหารจัดการคำอธิบายชุดข้อมูล [Metadata Management] เพื่อให้คำอธิบายชุดข้อมูลสามารถนำข้อมูลไปใช้วิเคราะห์เชื่อมโยงความสัมพันธ์ของระบบที่เกี่ยวข้องได้อย่างครบถ้วนถูกต้อง รวมถึงมีกระบวนการการควบคุม การเข้าถึง การกำหนดสิทธิ์ ปรับปรุงแก้ไข คำอธิบายชุดข้อมูล และมีการปรับปรุงให้เป็นปัจจุบันอย่างต่อเนื่อง โดยมีการสอบทานอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง
  - การบริหารจัดการคุณภาพของข้อมูล [Data Quality Management] เพื่อให้ข้อมูลมีคุณภาพ น่าเชื่อถือ สามารถนำไปใช้ประกอบการวิเคราะห์และตัดสินใจทางธุรกิจได้อย่างถูกต้องเหมาะสม โดยมีการกำหนดมาตรฐานหลักเกณฑ์ การประเมิน การปรับปรุง และควบคุมติดตาม คุณภาพของข้อมูล
  - การบริหารจัดการความเสี่ยงด้านข้อมูล [Data Risk Management] โดยครอบคลุม เกณฑ์ในการประเมินความเสี่ยงอันได้แก่ ความถูกต้อง[Accuracy] ความครบถ้วน[Completeness] ความสอดคล้อง[Consistency] ความเป็นปัจจุบัน[Timeliness] ตรงกับความต้องการของผู้ใช้งาน[Relevancy] และความพร้อมใช้งาน[Availability]
  - การรักษาความมั่นคงปลอดภัยของข้อมูล [Data Security] ครอบคลุมตามหลักการ CIA ซึ่งประกอบด้วย การรักษาความลับ[Confidentiality] การรักษาความครบถ้วน[Integrity] และการรักษาสภาพพร้อมใช้งาน[Availability] รวมถึงการรับส่งข้อมูลผ่านเครือข่ายการสื่อสาร การจัดเก็บหรือใช้ข้อมูลบนระบบงานและสื่อบันทึกต่างๆ การเก็บรักษาและการทำลายข้อมูล
  - การรักษาความเป็นส่วนตัวของข้อมูล [Data Privacy] มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเท่าที่จำเป็นภายใต้วัตถุประสงค์ที่กำหนดไว้ ทั้งที่อยู่ในรูปแบบกระดาษและอิเล็กทรอนิกส์ โดยให้ปฏิบัติตามกฎหมายหรือหลักเกณฑ์ที่เกี่ยวข้อง
  - การประเมินระดับการกำกับดูแลข้อมูล [Data Governance Maturity Assessment] เพื่อวัดประสิทธิภาพและทราบถึงสถานะของระดับการกำกับดูแลข้อมูลของบริษัทในปัจจุบัน เพื่อนำผลการประเมินมาเป็นข้อมูลประกอบการพิจารณา พัฒนา นโยบายและการบริหารจัดการข้อมูลให้มีประสิทธิภาพยิ่งขึ้น