

## 1. วัตถุประสงค์ (Purpose)

เพื่อกำหนดแนวทางและโครงสร้างการบริหารความเสี่ยงขององค์กรให้สอดคล้องกับเป้าหมายทางธุรกิจ วิสัยทัศน์ ธรรมนูญ และกลยุทธ์ขององค์กร ดังแนวทางต่อไปนี้

- 1.1 สร้างระบบบริหารความเสี่ยงที่ครอบคลุมทั้งระดับองค์กรและระดับหน่วยธุรกิจ
- 1.2 บูรณาการระบบบริหารความเสี่ยงเข้ากับกระบวนการตัดสินใจเชิงกลยุทธ์และการกำหนดเป้าหมาย (Strategy & Objective Setting)
- 1.3 บูรณาการระบบการบริหารความเสี่ยงเข้ากับกลไกสำคัญ เช่น การควบคุมภายใน (Internal Control), การกำกับดูแลกิจการ (Corporate Governance) สิ่งแวดล้อม สังคม และธรรมนูญ (ESG) ซึ่งเป็นรากฐานสำคัญในการขับเคลื่อนองค์กรสู่ความยั่งยืน (Sustainability) อย่างสัมฤทธิ์ผล
- 1.4 เสริมสร้างและปลูกฝังวัฒนธรรมการบริหารความเสี่ยง (Risk Culture) ในทุกระดับขององค์กร

## 2. ขอบเขต (Scope)

นโยบายฉบับนี้มีผลบังคับใช้กับทุกหน่วยงานในระดับ Corporate Function และ Business Unit (BU) ภายใต้บริษัทบุรีกรุ๊ป

## 3. กรอบแนวคิด (Framework)

องค์กรใช้กรอบการบริหารความเสี่ยงในระดับสากลของ COSO ERM: Enterprise Risk Management – Integrating with Strategy and Performance (2017) เป็นกรอบหลักโดยบูรณาการร่วมกับแนวปฏิบัติของ ISO 31000:2018 เพื่อสร้างความสอดคล้องของธรรมนูญ วัฒนธรรมและการดำเนินงาน ให้เป็นมาตรฐานเดียวกันทั่วทั้งองค์กร

## 4. หลักการสำคัญของการบริหารความเสี่ยงเพื่อความยั่งยืน (Core Principles)

เพื่อให้การบริหารความเสี่ยงขององค์กรเป็นไปอย่างมีประสิทธิภาพ โปร่งใส และสอดคล้องตามหลักธรรมนูญ จึงได้กำหนดหลักการสำคัญขึ้นเป็นแนวทางหลักที่ทุกหน่วยงานและบุคลากรทุกคนต้องถือปฏิบัติและยึดเป็นแนวทางในการดำเนินงาน การตัดสินใจ และการบริหารความเสี่ยงในทุกระดับขององค์กร ดังต่อไปนี้

- 4.1 กำหนดให้การบริหารความเสี่ยงเป็นส่วนหนึ่งในการตัดสินใจควบคู่กับการกำหนดกลยุทธ์ การวางแผนงานและเป้าหมายในทุกระดับขององค์กร รวมถึงการตัดสินใจก่อนการลงทุนในโครงการต่างๆ เพื่อให้มั่นใจว่าการตัดสินใจและการดำเนินงานอยู่ภายใต้กรอบความเสี่ยงที่ยอมรับได้ (Risk Appetite) และสนับสนุนการสร้างคุณค่าและการเติบโตอย่างยั่งยืน
- 4.2 จัดให้มีกระบวนการและกรอบการบริหารความเสี่ยง เพื่อใช้เป็นแนวทาง มาตรการ และเป็นเครื่องมือให้ทุกหน่วยงานนำไปใช้เพื่อคาดการณ์ ประเมินและตอบสนองความเสี่ยงในกลยุทธ์ แผนงานและการดำเนินงานได้อย่างมีประสิทธิภาพ พร้อมทั้งสนับสนุนให้ใช้ข้อมูลและเทคโนโลยีที่ทันสมัยในการวิเคราะห์และติดตามความเสี่ยง เพื่อยกระดับคุณภาพการตัดสินใจด้านความเสี่ยงให้แม่นยำ โปร่งใส ตรวจสอบได้ และสอดคล้องกับกลยุทธ์การพัฒนาด้านดิจิทัลขององค์กร
- 4.3 กำหนดการบริหารความเสี่ยงเป็นความรับผิดชอบของทุกหน่วยงานและบุคลากรทุกคน โดยมีคณะกรรมการและผู้บริหารทำหน้าที่เป็นแบบอย่างในการสร้างวัฒนธรรมความเสี่ยง ส่งเสริมให้พนักงานทุกระดับเปิดเผยข้อมูลความเสี่ยงอย่างโปร่งใส และร่วมมือกันป้องกันความเสียหายก่อนเกิดขึ้น
- 4.4 พิจารณาบริหารความเสี่ยงใหม่ ที่เกี่ยวข้องกับสิ่งแวดล้อม สังคม และธรรมนูญ (ESG) การเปลี่ยนแปลงสภาพภูมิอากาศ (Climate Change) ธรรมนูญข้อมูล (Data Governance) จริยธรรมทางด้านปัญญาประดิษฐ์ (AI Ethics) และความยืดหยุ่นของห่วงโซ่อุปทาน (Supply Chain Resilience) เพื่อสร้างองค์กรที่ยั่งยืนและมีความรับผิดชอบต่อสังคม
- 4.5 กำหนดให้ทุกหน่วยงานทำการประเมินความเสี่ยง จัดทำมาตรการจัดการความเสี่ยง ทบทวนและติดตามผลการบริหารความเสี่ยง และรายงานผลต่อคณะกรรมการบริหารความเสี่ยงอย่างสม่ำเสมอ

## 5. ประเภทของความเสียหาย (Risk Categories)

เพื่อให้การบริหารจัดการความเสี่ยงครอบคลุมและสอดคล้องกับทุกมิติของการดำเนินธุรกิจอย่างยั่งยืน องค์กรจึงได้กำหนดประเภทความเสี่ยงหลักที่ต้องประเมินและบริหารความเสี่ยงไว้ ดังต่อไปนี้

- 5.1 **ความเสี่ยงเชิงกลยุทธ์ (Strategic Risks)** ปัจจัยที่ส่งผลกระทบต่อการบรรลุวิสัยทัศน์ และวัตถุประสงค์เชิงกลยุทธ์รวมถึงการตัดสินใจในการบริหารจัดการธุรกิจ เช่น การเปลี่ยนแปลงนโยบายภาครัฐ กฎหมาย ภาวะเศรษฐกิจที่ส่งผลกระทบต่อ การดำเนินธุรกิจ พฤติกรรมผู้บริโภค การหยุดชะงักของห่วงโซ่อุปทาน เป็นต้น
- 5.2 **ความเสี่ยงด้านการปฏิบัติการ (Operational Risks)** ปัจจัยจากบุคคลากร กระบวนการทำงาน ระบบงาน หรือจากเหตุการณ์ภายนอกที่ส่งผลกระทบต่อการทำงานประจำวัน เช่น การหยุดชะงักของระบบงานสำคัญ คุณภาพการบริการไม่เป็นไปตามมาตรฐาน เป็นต้น
- 5.3 **ความเสี่ยงด้านการเงิน (Financial Risks)** ปัจจัยจากความผันผวนของปัจจัยทางการเงิน ซึ่งส่งผลกระทบต่อรายได้ สภาพคล่อง และมูลค่าสินทรัพย์ขององค์กร เช่น สภาพคล่องทางการเงิน เครดิตลูกค้า/คู่ค้า ความผันผวนของอัตราดอกเบี้ย เป็นต้น
- 5.4 **ความเสี่ยงด้านการกำกับดูแลและกฎหมาย (Compliance & Legal Risks)** ปัจจัยจากการไม่ปฏิบัติตามกฎหมาย กฎระเบียบ ข้อบังคับ หรือข้อกำหนดตามสัญญาที่เกี่ยวข้องกับธุรกิจ เช่น การขอและต่อใบอนุญาต การปฏิบัติตาม PDPA การปฏิบัติตามกฎหมายและระเบียบต่างๆ ทางด้านแรงงาน ภาษีอากร อาหารและสิ่งแวดล้อม เป็นต้น
- 5.5 **ความเสี่ยงด้านเทคโนโลยีและไซเบอร์ (IT & Cyber Risks)** ปัจจัยที่เกี่ยวข้องกับความมั่นคงปลอดภัยของข้อมูล ความพร้อมใช้งานของระบบเทคโนโลยีสารสนเทศ เช่น การใช้ AI ภัยคุกคามทางไซเบอร์ ความล้มเหลวของระบบสารสนเทศหลัก เป็นต้น
- 5.6 **ความเสี่ยงด้าน ESG และความยั่งยืน (ESG & Sustainability Risks)** ปัจจัยที่เกิดจากผลกระทบด้านสิ่งแวดล้อม สังคม และธรรมาภิบาล ซึ่งส่งผลกระทบต่อชื่อเสียงและมูลค่าระยะยาวขององค์กร เช่น การจัดการการปล่อยก๊าซคาร์บอน (Carbon Emission), ผลกระทบต่อชุมชน, การเปลี่ยนแปลงสภาพภูมิอากาศ (Climate Change) เป็นต้น
- 5.7 **ความเสี่ยงด้านโครงการและการลงทุน (Project & Investment Risks)** ปัจจัยที่เกี่ยวข้องกับการวางแผน การดำเนินงาน และผลลัพธ์ของโครงการสำคัญหรือการลงทุนเชิงกลยุทธ์ เช่น ผลตอบแทนจากการลงทุน (ROI) การปฏิบัติตามสัญญาของลูกค้า/ผู้รับเหมา การบริหารจัดการงบประมาณและเวลาโครงการ เป็นต้น

## 6. บทบาทและความรับผิดชอบ (Roles & Responsibilities)

การบริหารความเสี่ยงอย่างมีประสิทธิภาพต้องได้รับความร่วมมือ และความรับผิดชอบร่วมกันของบุคลากรทุกระดับ องค์กรจึงกำหนดบทบาท หน้าที่และความรับผิดชอบของหน่วยงานต่างๆ เพื่อเกิดความชัดเจนและบริหารความเสี่ยงไปในทิศทางเดียวกัน โดยมีรายละเอียดดังนี้

ระดับ / หน่วยงาน	ความรับผิดชอบหลัก
คณะกรรมการบริษัท (Board of Directors)	กำกับดูแลภาพรวมและอนุมัตินโยบายการบริหารความเสี่ยง รวมทั้งกำหนดขีดความสามารถในการรับความเสี่ยง (Risk Appetite) ตลอดจนติดตามผลการจัดการความเสี่ยงระดับสูงสุด (Top Risks) ที่อาจส่งผลกระทบต่อเป้าหมายขององค์กร
คณะกรรมการบริหารความเสี่ยง (Risk Committee)	กำหนดแนวทาง กลยุทธ์และกรอบการบริหารความเสี่ยงขององค์กร พร้อมทั้งกำกับดูแลการจัดการความเสี่ยงที่มีนัยสำคัญ (Top Risks) และเสนอแนะแนวทางปรับปรุงระบบให้มีประสิทธิภาพ รวมถึงการส่งเสริมการใช้เทคโนโลยีสารสนเทศที่ทันสมัย และรายงานผลต่อคณะกรรมการบริษัท
ประธานเจ้าหน้าที่บริหารและคณะผู้บริหารระดับสูง (CEO & Executives)	เป็นผู้นำเพื่อขับเคลื่อนนโยบายการบริหารความเสี่ยงสู่การปฏิบัติ และบูรณาการความเสี่ยงเข้ากับการวางแผนกลยุทธ์ การดำเนินงาน และการตัดสินใจในทุกๆระดับขององค์กร พร้อมทั้งจัดสรรทรัพยากรที่จำเป็นอย่างเพียงพอ ทั้งด้านบุคลากร งบประมาณ และเทคโนโลยี เพื่อสนับสนุนให้การบริหารจัดการความเสี่ยงมีประสิทธิภาพและต่อเนื่อง
หัวหน้าหน่วยงานองค์กรและหน่วยงานธุรกิจ	บริหารและติดตามความเสี่ยงในกระบวนการดำเนินงานของหน่วยงาน รวมทั้งดำเนินการมาตรการควบคุมภายในให้สอดคล้องกับนโยบายการบริหารความเสี่ยงขององค์กร

ระดับ / หน่วยงาน	ความรับผิดชอบหลัก
(Corporate Unit and Business Unit Heads)	
พนักงานทุกคน (All Employees)	ปฏิบัติตามมาตรการควบคุมความเสี่ยงที่กำหนด และรายงานเหตุการณ์หรือความเสี่ยงที่พบต่อหัวหน้างานหรือหน่วยงานที่เกี่ยวข้อง เพื่อร่วมกันลดผลกระทบที่อาจเกิดขึ้นต่อองค์กร
แผนกบริหารความเสี่ยง (Corporate Risk Management)	พัฒนาและปรับปรุงกรอบการบริหารความเสี่ยงองค์กรอย่างต่อเนื่อง รวบรวม วิเคราะห์ และรายงานความเสี่ยงระดับองค์กร นำเสนอเทคโนโลยีที่ทันสมัย พร้อมส่งเสริมและพัฒนาความรู้ด้านการบริหารความเสี่ยงให้กับบุคลากรทุกระดับเพื่อสร้างวัฒนธรรมและความตระหนักรู้ด้านความเสี่ยงทั่วทั้งองค์กร
แผนกตรวจสอบภายใน (Internal Audit)	ให้ความเชื่อมั่นอย่างเป็นอิสระ (Independent Assurance) โดยประเมินความเพียงพอ ความเหมาะสม และประสิทธิผลของระบบควบคุมภายใน และกระบวนการบริหารความเสี่ยง พร้อมรายงานผลต่อคณะกรรมการตรวจสอบ

#### 7. การทบทวนและปรับปรุง (Review & Update)

คณะกรรมการบริหารความเสี่ยง (Risk Committee) เป็นผู้รับผิดชอบหลักในการทบทวนและปรับปรุงนโยบายบริหารความเสี่ยงอย่างยั่งยืนและนำเสนออนุมัติต่อคณะกรรมการบริษัท (Board of Directors) เพื่อให้สอดคล้องกับสภาพแวดล้อมทางธุรกิจที่เปลี่ยนแปลง และรักษามาตรฐานการบริหารความเสี่ยงในระดับสากลอย่างสม่ำเสมอ

ประกาศให้มีผลบังคับใช้ตั้งแต่วันที่ 1 มกราคม 2569 เป็นต้นไปจนกว่าจะมีการเปลี่ยนแปลง