



# นโยบายการบริหาร ความเสี่ยงในระดับ องค์กร

ฉบับที่ 2/2568 VNG-GOV-ERM-PL-02

วันที่มีผลบังคับใช้: 11 พฤศจิกายน 2568

## นโยบายการบริหารความเสี่ยงในระดับองค์กร บริษัท วนชัย กรุ๊ป จำกัด (มหาชน) และบริษัทย่อย

บริษัท วนชัย กรุ๊ป จำกัด (มหาชน) และบริษัทย่อย (“บริษัท”) ตระหนักถึงความสำคัญของการบริหารความเสี่ยงในฐานะกลไกหลักของการกำกับดูแลกิจการที่ดี (Good Corporate Governance) ซึ่งช่วยให้บริษัทสามารถคาดการณ์และจัดการกับความไม่แน่นอนที่อาจส่งผลกระทบต่อการบรรลุวัตถุประสงค์เชิงกลยุทธ์ การดำเนินงาน และความยั่งยืนขององค์กรได้อย่างมีประสิทธิภาพ

การบริหารความเสี่ยงในระดับองค์กร (Enterprise Risk Management: ERM) มีบทบาทสำคัญในการเสริมสร้างความสามารถในการแข่งขัน ความยืดหยุ่นต่อการเปลี่ยนแปลง (Resilience) และการสร้างคุณค่าอย่างต่อเนื่องให้กับผู้มีส่วนได้เสียทุกกลุ่ม โดยมุ่งเน้นการบริหารจัดการความเสี่ยงเชิงรุก (Proactive Risk Management) เพื่อให้บริษัทสามารถป้องกันและบรรเทาผลกระทบเชิงลบจากเหตุการณ์ที่ไม่คาดคิด ตลอดจนใช้ประโยชน์จากโอกาสทางธุรกิจใหม่ ๆ ที่สอดคล้องกับกลยุทธ์และทิศทางการพัฒนาอย่างยั่งยืนของบริษัท

บริษัทได้นำแนวทางการบริหารความเสี่ยงตามกรอบมาตรฐาน COSO ERM Framework (2017) มาประยุกต์ใช้ เพื่อให้มั่นใจว่าการบริหารความเสี่ยงขององค์กรมีความครอบคลุมทุกมิติ ทั้งด้านกลยุทธ์ การปฏิบัติงาน การเงิน การปฏิบัติตามกฎหมาย และด้านสิ่งแวดล้อม สังคม และธรรมาภิบาล (ESG Risks)

ในการระบุและจัดลำดับความสำคัญของความเสี่ยงและโอกาสด้านความยั่งยืน บริษัทใช้กรอบการประเมินความมีสาระสำคัญและความเสี่ยงแบบบูรณาการของวณชัย (**Vanachai Integrated Materiality and Risk Assessment: V-IMRA**) เป็นเครื่องมือภายในในการประเมินผลกระทบ ความเสี่ยง และโอกาสด้านความยั่งยืนอย่างเป็นระบบ ครอบคลุมการดำเนินงานและห่วงโซ่คุณค่าของบริษัท

ผลลัพธ์จากกระบวนการ V-IMRA ถูกนำมาใช้เป็นข้อมูลนำเข้าที่สำคัญในกระบวนการบริหารความเสี่ยงขององค์กร (Enterprise Risk Management: ERM) เพื่อสนับสนุนการระบุความเสี่ยงด้านความยั่งยืนที่มีสาระสำคัญ การบูรณาการเข้าสู่ทะเบียนความเสี่ยงขององค์กร (Enterprise Risk Register) รวมถึงการติดตามและบริหารจัดการความเสี่ยงดังกล่าวอย่างต่อเนื่องและเป็นระบบ

นโยบายฉบับนี้จัดทำขึ้นเพื่อเป็นกรอบการดำเนินงานที่ชัดเจน ครอบคลุม และสอดคล้องกับวัตถุประสงค์เชิงกลยุทธ์ของบริษัท รวมถึงข้อกำหนดของตลาดหลักทรัพย์แห่งประเทศไทย และมาตรฐานสากลด้านความยั่งยืน โดยมีเป้าหมายในการส่งเสริมให้ทุกหน่วยงานและบุคลากรทุกระดับมีส่วนร่วมในการบริหารความเสี่ยงอย่างมีระบบและต่อเนื่อง เพื่อสร้างวัฒนธรรมองค์กรแห่งการคาดการณ์ การเตรียมพร้อม และความรับผิดชอบร่วมกัน

## 1) วัตถุประสงค์

การบริหารความเสี่ยงในระดับองค์กร มีวัตถุประสงค์เพื่อสร้างระบบการบริหารจัดการที่มีประสิทธิภาพ ครอบคลุมทุกมิติของความเสี่ยง เพื่อให้บริษัทสามารถบรรลุเป้าหมายเชิงกลยุทธ์และดำเนินธุรกิจได้อย่างมั่นคง โปร่งใส และยั่งยืน

- **เสริมสร้างการกำกับดูแลกิจการที่ดี:** กำหนดกรอบการบริหารความเสี่ยงที่เชื่อมโยงกับหลักธรรมาภิบาล เพื่อให้การตัดสินใจของคณะกรรมการและผู้บริหารอยู่บนพื้นฐานของข้อมูล ความเสี่ยง และโอกาสอย่างสมดุล ส่งเสริมความโปร่งใสและความรับผิดชอบต่อผู้มีส่วนได้เสียทุกกลุ่ม
- **ป้องกันและลดผลกระทบจากความเสียหาย:** สร้างกระบวนการบริหารความเสี่ยงเชิงรุก (Proactive Risk Management) ที่สามารถระบุ ประเมิน และจัดการความเสี่ยงที่อาจเกิดขึ้นได้ทันที่ เพื่อป้องกันหรือบรรเทาผลกระทบทางธุรกิจ การเงิน การปฏิบัติงาน กฎหมาย รวมถึงความเสี่ยงด้านสิ่งแวดล้อม สังคม และธรรมาภิบาล (ESG Risks)
- **สร้างวัฒนธรรมองค์กรแห่งการบริหารความเสี่ยง:** ส่งเสริมให้พนักงานทุกระดับมีความเข้าใจ ตระหนัก และมีส่วนร่วมในการบริหารความเสี่ยงขององค์กร โดยบูรณาการแนวคิดการบริหารความเสี่ยงเข้ากับกิจกรรมการทำงาน การวางแผน และการตัดสินใจ เพื่อให้การบริหารความเสี่ยงเป็นส่วนหนึ่งของวัฒนธรรมองค์กรอย่างแท้จริง
- **สนับสนุนการดำเนินกลยุทธ์และการตัดสินใจเชิงกลยุทธ์:** บูรณาการการบริหารความเสี่ยงเข้ากับการวางแผนกลยุทธ์ การจัดสรรทรัพยากร และการบริหารโครงการ เพื่อให้มั่นใจว่าการตัดสินใจเชิงกลยุทธ์ของบริษัทอยู่ภายใต้ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) และสามารถสร้างคุณค่าอย่างต่อเนื่องให้แก่ผู้มีส่วนได้เสีย
- **เสริมสร้างความสามารถในการปรับตัวและความยืดหยุ่นขององค์กร:** เพิ่มขีดความสามารถของบริษัทในการรับมือกับเหตุการณ์ไม่คาดคิด (Emerging Risks) เช่น การเปลี่ยนแปลงสภาพภูมิอากาศ ภัยธรรมชาติ การคุกคามทางไซเบอร์ และความผันผวนของตลาด เพื่อให้สามารถดำเนินธุรกิจต่อเนื่อง (Business Continuity) และรักษาความเชื่อมั่นของผู้มีส่วนได้เสียในระยะยาว

## 2) ความสอดคล้องของนโยบายและมาตรฐานสากล

นโยบายนี้จัดทำขึ้นให้สอดคล้องกับกรอบการกำกับดูแลกิจการและมาตรฐานสากล เพื่อให้กระบวนการบริหารความเสี่ยงของบริษัทมีความโปร่งใส ตรวจสอบได้ และเทียบเท่ามาตรฐานระดับสากล โดยอ้างอิงจากกรอบแนวทางดังต่อไปนี้

- **มาตรฐาน GRI:** GRI 102-15, 102-29, 102-30, 102-33, 102-34 ว่าด้วยการระบุ วิเคราะห์ และเปิดเผยความเสี่ยงและโอกาสที่มีนัยสำคัญ

- **COSO Enterprise Risk Management (ERM) Framework (2017):** เพื่อใช้เป็นแนวทางในการบริหารความเสี่ยงเชิงกลยุทธ์และการบูรณาการความเสี่ยงเข้ากับกระบวนการตัดสินใจขององค์กร
- **ISO 31000: Risk Management Principles and Guidelines:** เป็นแนวทางสำหรับการจัดการความเสี่ยงอย่างเป็นระบบ ครอบคลุมทุกระดับขององค์กร
- **UN Global Compact Principle 10 และ SDG 16:** ส่งเสริมความโปร่งใส ความยุติธรรม และสถาบันที่เข้มแข็งในการดำเนินธุรกิจ
- **FTSE Russell ESG Indicators:**
  - **GRM04:** กรอบการบริหารความเสี่ยงและโครงสร้างการบริหารความเสี่ยง
  - **GRM05:** กลไกการกำกับดูแลและควบคุมความเสี่ยง
  - **GRM12:** Risk Disclosure and Transparency
  - **GRM20:** การเปิดเผยข้อมูลและความโปร่งใสด้านความเสี่ยง
- ความเสี่ยงและโอกาสที่เกี่ยวข้องกับความยั่งยืนได้รับการระบุผ่านกระบวนการประเมินภายในของบริษัท รวมถึงการใช้กรอบการประเมินความมีสาระสำคัญและความเสี่ยงแบบบูรณาการของวงชัย (**Vanachai Integrated Materiality and Risk Assessment: V-IMRA**) และได้รับการบริหารจัดการตามกรอบและมาตรฐานที่อ้างอิงข้างต้นอย่างเป็นระบบ

### 3) ขอบเขตของนโยบาย

นโยบายนี้ครอบคลุม:

- **คณะกรรมการบริษัท และคณะกรรมการย่อยที่เกี่ยวข้อง:** มีหน้าที่กำกับดูแลและติดตามผลการบริหารความเสี่ยงให้อยู่ในระดับที่เหมาะสมและสอดคล้องกับกลยุทธ์ขององค์กร
- **ผู้บริหารทุกระดับ:** ต้องบูรณาการการบริหารความเสี่ยงเข้าสู่การวางแผน การตัดสินใจ และการดำเนินงานประจำวัน รวมถึงกำหนดมาตรการลดความเสี่ยงภายในหน่วยงานของตน
- **พนักงานทุกระดับ:** มีหน้าที่ระบุ วิเคราะห์ และรายงานความเสี่ยงที่อาจเกิดขึ้นในขอบเขตความรับผิดชอบของตน พร้อมปฏิบัติตามมาตรการควบคุมที่กำหนดไว้อย่างเคร่งครัด
- **หน่วยงานสนับสนุน เช่น หน่วยตรวจสอบภายใน หน่วยงานบริหารความยั่งยืน และหน่วยงานบริหารความเสี่ยง:** มีหน้าที่สนับสนุนด้านข้อมูล เครื่องมือ และระบบบริหารจัดการ เพื่อเสริมสร้างประสิทธิภาพการบริหารความเสี่ยงขององค์กร
- **บริษัทย่อยและพันธมิตรทางธุรกิจ:** ต้องดำเนินการภายใต้หลักการและกรอบการบริหารความเสี่ยงเดียวกันกับบริษัท เพื่อรักษาความสอดคล้องและมาตรฐานธรรมาภิบาลของกลุ่มบริษัท
- **กิจกรรมทั้งหมดขององค์กร:** ครอบคลุมตั้งแต่การวางแผนเชิงกลยุทธ์ การจัดการทางการเงิน การดำเนินงาน การจัดซื้อจัดจ้าง โครงการลงทุน การบริหารบุคลากร การบริหารความปลอดภัย การบริหารความต่อเนื่องทางธุรกิจ ตลอดจนการบริหารความเสี่ยงด้านสิ่งแวดล้อม สังคม และธรรมาภิบาล (ESG Risks)

(สอดคล้องกับเกณฑ์ FTSE Russell GRM04 – Risk Management Framework, GRI 102-15, GRI 102-29, SDG 16.6 และ SDG 17 – Partnerships for the Goals)

#### 4) คำจำกัดความและเอกสารอ้างอิง

- **เหตุการณ์ (Event):** เหตุการณ์ที่อาจเกิดขึ้นและส่งผลกระทบต่อความสามารถของบริษัทในการบรรลุวัตถุประสงค์ โดยอาจเป็นได้ทั้งผลลัพธ์เชิงบวก (โอกาส) หรือเชิงลบ (ความเสี่ยง) ซึ่งต้องได้รับการประเมิน วิเคราะห์ และจัดการอย่างเหมาะสม
- **ความเสี่ยง (Risk):** ความเป็นไปได้ที่เหตุการณ์หนึ่ง ๆ จะเกิดขึ้นและส่งผลกระทบต่อวัตถุประสงค์ของบริษัท ซึ่งอาจเกิดจากปัจจัยภายในหรือภายนอกองค์กร การบริหารความเสี่ยงมุ่งลดความไม่แน่นอนและผลกระทบจากความเสี่ยงให้อยู่ในระดับที่ยอมรับได้
- **การบริหารความเสี่ยง (Risk Management):** กระบวนการบูรณาการที่ครอบคลุมการระบุ การประเมิน การตอบสนอง การติดตาม และการสื่อสารความเสี่ยง เพื่อสนับสนุนการตัดสินใจเชิงกลยุทธ์และการดำเนินงานอย่างมีประสิทธิภาพ
- **การบริหารความเสี่ยงระดับองค์กร (Enterprise Risk Management – ERM):** ระบบการบริหารจัดการที่มุ่งบูรณาการการบริหารความเสี่ยงในทุกระดับขององค์กร เพื่อเพิ่มความสามารถในการสร้างคุณค่า ปกป้องคุณค่า และรักษาความสามารถในการแข่งขันของบริษัทในระยะยาว ตามแนวทาง COSO ERM Framework (2017)
- **ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite):** ระดับของความเสี่ยงที่องค์กรยอมรับได้ในการดำเนินธุรกิจ เพื่อให้การตัดสินใจและแผนงานต่าง ๆ อยู่ภายในขอบเขตที่สมดุลระหว่างโอกาสและความเสี่ยงที่ยอมรับได้
- **ความเสี่ยงที่เกิดขึ้นใหม่ (Emerging Risks):** ความเสี่ยงที่เพิ่งปรากฏหรือยังไม่เป็นที่เข้าใจอย่างชัดเจน แต่มีแนวโน้มที่จะส่งผลกระทบต่อในอนาคต เช่น ความเสี่ยงจากการเปลี่ยนแปลงสภาพภูมิอากาศ ภัยคุกคามทางไซเบอร์ หรือการเปลี่ยนแปลงของกฎระเบียบ
- **ความยืดหยุ่นขององค์กร (Organizational Resilience):** ความสามารถของบริษัทในการคาดการณ์ ตอบสนอง และฟื้นฟูจากเหตุการณ์ที่ไม่คาดคิด เพื่อให้สามารถดำเนินธุรกิจต่อเนื่องและบรรลุวัตถุประสงค์เชิงกลยุทธ์ได้อย่างยั่งยืน
- **ความเสี่ยงด้านสิ่งแวดล้อม สังคม และธรรมาภิบาล (ESG Risks):** ความเสี่ยงที่เกิดจากผลกระทบต่อด้านสิ่งแวดล้อม การเปลี่ยนแปลงทางสังคม และประเด็นธรรมาภิบาล ที่อาจกระทบต่อชื่อเสียง ความเชื่อมั่น และความยั่งยืนขององค์กร
- **การประเมินความมีสาระสำคัญและความเสี่ยงแบบบูรณาการของวนชัย (Vanachai Integrated Materiality and Risk Assessment: V-IMRA):** กรอบการประเมินภายในของบริษัทที่ใช้ในการระบุ วิเคราะห์ ประเมิน และจัดลำดับความสำคัญของผลกระทบ ความเสี่ยง และโอกาสที่เกี่ยวข้องกับความยั่งยืนตลอดการดำเนินงานและห่วงโซ่คุณค่าของบริษัท โดย V-IMRA บูรณาการการพิจารณาความมีสาระสำคัญเชิงผลกระทบ (Impact Materiality) และความมีสาระสำคัญเชิงการเงิน (Financial Materiality) และทำหน้าที่เป็นข้อมูลนำเข้าที่มี

โครงสร้างสำหรับระบบบริหารความเสี่ยงขององค์กร (Enterprise Risk Management: ERM) การวางแผนกลยุทธ์ และการรายงานด้านความยั่งยืน  
(สอดคล้องกับ FTSE Russell GRM04-GRM11, COSO ERM, ISO 31000, GRI 102-15, GRI 102-29, GRI 102-33, SDG 9, SDG 13, และ SDG 16)

## 5) การกำกับดูแลและความรับผิดชอบ

- **คณะกรรมการบริษัท:** มีบทบาทเป็นผู้กำกับดูแลสูงสุดในการบริหารความเสี่ยงขององค์กร โดยอนุมัติกรอบนโยบายบริหารความเสี่ยง ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) และแนวทางการติดตามผล เพื่อให้มั่นใจว่าระบบบริหารความเสี่ยงมีความเหมาะสม ครบคลุม และสอดคล้องกับกลยุทธ์ของบริษัท คณะกรรมการยังติดตามประสิทธิผลของระบบบริหารความเสี่ยงเป็นประจำ รับทราบรายงานความเสี่ยงที่มีนัยสำคัญ และส่งเสริมวัฒนธรรมองค์กรที่เน้นการบริหารความเสี่ยงและการตัดสินใจบนพื้นฐานข้อมูลที่ครบถ้วนและรอบคอบ
- **คณะกรรมการบริหารความเสี่ยงและกำกับดูแลกิจการ:** มีหน้าที่วางกรอบนโยบาย กลยุทธ์ และแนวทางการบริหารความเสี่ยงให้สอดคล้องกับแผนกลยุทธ์องค์กร รวมถึงกำหนดระดับความเสี่ยงที่ยอมรับได้ ติดตามความเสี่ยงหลัก และพิจารณาความเสี่ยงใหม่ที่มีผลกระทบต่อองค์กร คณะกรรมการชุดนี้ทบทวนรายงานผลการบริหารความเสี่ยงจากคณะทำงานบริหารความเสี่ยง เสนอข้อแนะนำต่อคณะกรรมการบริษัท และส่งเสริมให้มีการบูรณาการแนวคิดการบริหารความเสี่ยงแบบองค์รวม (ERM) เข้ากับกระบวนการตัดสินใจและการดำเนินงานทั่วทั้งองค์กร
- **คณะกรรมการบริหาร:** มีหน้าที่นำแนวทางการบริหารความเสี่ยงไปปฏิบัติในระดับหน่วยงานให้สอดคล้องกับนโยบายขององค์กร ตรวจสอบให้มั่นใจว่าทรัพยากรที่จำเป็นสำหรับการบริหารความเสี่ยงได้รับการจัดสรรอย่างเพียงพอ และรายงานความคืบหน้า ปัญหา หรือความเสี่ยงที่สำคัญต่อคณะกรรมการบริหารความเสี่ยงและกำกับดูแลกิจการ เพื่อให้มั่นใจว่าการบริหารความเสี่ยงดำเนินไปอย่างต่อเนื่องและมีประสิทธิผล
- **คณะทำงานบริหารความเสี่ยง:** ทำหน้าที่ระบุ วิเคราะห์ และประเมินความเสี่ยงหลักขององค์กร ทั้งในเชิงกลยุทธ์ การดำเนินงาน การเงิน และความเสี่ยงเกิดใหม่ ตลอดจนติดตามและประเมินประสิทธิผลของมาตรการจัดการความเสี่ยงที่มีอยู่ คณะทำงานจะจัดทำรายงานสรุปผลการบริหารความเสี่ยงรายไตรมาสเสนอคณะกรรมการบริหารความเสี่ยงและกำกับดูแลกิจการ พร้อมส่งเสริมการสื่อสารและแลกเปลี่ยนความรู้ด้านการบริหารความเสี่ยงในทุกระดับขององค์กร
- **ผู้บริหารและหัวหน้างานทุกระดับ:** รับผิดชอบการบริหารความเสี่ยงภายในหน่วยงานของตน โดยบูรณาการการบริหารความเสี่ยงเข้ากับกิจกรรมประจำวัน ระบุและรายงานความเสี่ยงที่อาจส่งผลกระทบต่อการทำงาน กำหนดมาตรการควบคุมและลดความเสี่ยง รวมถึงส่งเสริมให้

พนักงานมีส่วนร่วมในการประเมินและจัดการความเสี่ยงอย่างต่อเนื่อง เพื่อให้หน่วยงานดำเนินการได้อย่างมีประสิทธิภาพและปลอดภัยต่อองค์กรโดยรวม

- **พนักงานทุกระดับ:** มีหน้าที่ปฏิบัติงานโดยตระหนักถึงความเสี่ยงที่อาจเกิดขึ้นจากการปฏิบัติงานของตนเอง พร้อมทั้งรายงานเหตุการณ์ผิดปกติหรือความเสี่ยงผ่านช่องทางที่กำหนดโดยไม่ต้องกังวลต่อการถูกตอบโต้ พนักงานต้องปฏิบัติตามนโยบายและมาตรการควบคุมความเสี่ยงของบริษัทอย่างเคร่งครัด และร่วมกันสร้างวัฒนธรรมองค์กรที่โปร่งใสและมุ่งเน้นการบริหารความเสี่ยงร่วมกันในทุกระดับ
- **หน่วยตรวจสอบภายใน:** ทำหน้าที่ตรวจสอบและประเมินความเสี่ยงพหุของระบบบริหารความเสี่ยงและการควบคุมภายใน เพื่อให้มั่นใจว่ามีความเหมาะสมและมีประสิทธิภาพ หน่วยงานนี้รายงานผลการตรวจสอบต่อคณะกรรมการตรวจสอบ พร้อมเสนอแนวทางการปรับปรุงเพื่อเสริมสร้างความแข็งแกร่งของระบบบริหารความเสี่ยง และให้คำแนะนำเพิ่มเติมในการพัฒนาเครื่องมือหรือแนวทางควบคุมตามมาตรฐานสากล

(สอดคล้องกับเกณฑ์ FTSE Russell GRM04-05, GRM11, GRI 102-29, GRI 102-30, GRI 102-33, GRI 205-2, และ SDG 8.8, SDG 9.1, SDG 16.5, SDG 16.7, SDG 16.6)

## 6) พันธสัญญาและหลักการ

มุ่งมั่นดำเนินการบริหารความเสี่ยงในระดับองค์กร (Enterprise Risk Management: ERM) อย่างเป็นระบบ ครบคลุม และสอดคล้องกับกลยุทธ์ขององค์กร เพื่อให้สามารถคาดการณ์และจัดการความเสี่ยงได้อย่างมีประสิทธิภาพ โปร่งใส และยั่งยืน โดยยึดถือหลักการบริหารความเสี่ยงตามมาตรฐานสากล ดังนี้

- 6.1 การบริหารความเสี่ยงเชิงรุก (FTSE Russell GRM04, GRI 102-15, SDG 9.1 และ SDG 16.6):** บริษัทบริหารความเสี่ยงโดยยึดหลักการเชิงรุก เพื่อคาดการณ์และระบุความเสี่ยงที่อาจเกิดขึ้นล่วงหน้า (Forward-looking) ลดผลกระทบที่อาจส่งผลกระทบต่อองค์กร และแปลงความเสี่ยงให้เป็นโอกาสในการพัฒนาและสร้างคุณค่าทางธุรกิจอย่างยั่งยืน
- 6.2 การบูรณาการการบริหารความเสี่ยงเข้ากับกลยุทธ์องค์กร (FTSE Russell GRM05, COSO ERM Principle 3, GRI 102-29, SDG 16.6):** บริษัทบูรณาการการบริหารความเสี่ยงเข้ากับกระบวนการวางแผนกลยุทธ์ การลงทุน การตัดสินใจทางธุรกิจ และการดำเนินงานประจำวัน เพื่อให้มั่นใจว่าทุกกระบวนการอยู่ภายใต้ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) และสอดคล้องกับเป้าหมายเชิงกลยุทธ์ขององค์กร
- 6.3 การกำหนดระดับความเสี่ยงที่ยอมรับได้ (FTSE Russell GRM04, GRM05, GRI 102-30, SDG 16.6):** บริษัทกำหนดระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) และค่าความเบี่ยงเบน (Risk Tolerance) เพื่อใช้เป็นกรอบในการตัดสินใจเชิงกลยุทธ์ และบริหารความเสี่ยงให้เหมาะสมกับสภาพแวดล้อมทางธุรกิจที่เปลี่ยนแปลงอย่างรวดเร็ว

- 6.4 การสร้างวัฒนธรรมแห่งความตระหนักรู้ด้านความเสี่ยง ( FTSE Russell GRM04, GRI 102-30, SDG 8.8 และ SDG 16.7):** บริษัทส่งเสริมให้ทุกหน่วยงานและพนักงานทุกระดับมีความเข้าใจและตระหนักถึงความเสี่ยงที่เกี่ยวข้องกับงานของตน โดยกำหนดให้ “ความเสี่ยงเป็นหน้าที่ของทุกคน (Risk is Everyone’s Responsibility)” พร้อมสนับสนุนให้การบริหารความเสี่ยงเป็นส่วนหนึ่งของวัฒนธรรมองค์กร เพื่อให้การจัดการความเสี่ยงเป็นความรับผิดชอบร่วมกันของทุกคน
- 6.5 การประเมินและควบคุมความเสี่ยงอย่างเป็นระบบ (FTSE Russell GRM04, GRM05, GRI 102-29, SDG 12.6):** บริษัทใช้กรอบการบริหารความเสี่ยงตามมาตรฐาน COSO ERM และ ISO 31000 ในการระบุ ประเมิน วิเคราะห์ และตอบสนองต่อความเสี่ยง โดยใช้ข้อมูลเชิงปริมาณและเชิงคุณภาพประกอบการตัดสินใจ เพื่อควบคุมความเสี่ยงให้อยู่ในระดับที่เหมาะสมและคุ้มค่าต่อการดำเนินงาน
- 6.6 การเปิดเผยและรายงานความเสี่ยงอย่างโปร่งใส (FTSE Russell GRM11 – Risk Disclosure, GRI 102-33, SDG 16.10):** บริษัทมุ่งมั่นเปิดเผยข้อมูลด้านความเสี่ยงและมาตรการบริหารความเสี่ยงที่มีนัยสำคัญอย่างโปร่งใสต่อคณะกรรมการตรวจสอบ คณะกรรมการบริหารความเสี่ยงและกำกับดูแลกิจการ รวมถึงผู้มีส่วนได้เสีย เพื่อสร้างความเชื่อมั่นและความโปร่งใสในการดำเนินธุรกิจ
- 6.7 การพัฒนาอย่างต่อเนื่องและการเรียนรู้จากเหตุการณ์ (FTSE Russell GRM05, COSO ERM Principle 20, GRI 102-30, SDG 4.7 และ SDG 16.6):** บริษัทให้ความสำคัญกับการพัฒนาและปรับปรุงระบบการบริหารความเสี่ยงอย่างต่อเนื่อง โดยอาศัยข้อมูลจากการติดตามประสิทธิภาพ การตรวจสอบภายใน และบทเรียนจากเหตุการณ์ที่เกิดขึ้น (Lessons Learned) เพื่อเพิ่มขีดความสามารถขององค์กรในการรับมือกับความไม่แน่นอนและสร้างความยืดหยุ่นในระยะยาว

## 7) การบริหารความเสี่ยง ผลกระทบ และการฟื้นฟู

ใช้กระบวนการบริหารความเสี่ยงตามกรอบ COSO Enterprise Risk Management (ERM) Framework เพื่อให้สามารถระบุ ประเมิน จัดการ และติดตามความเสี่ยงได้อย่างมีระบบ โดยมุ่งเน้นการลดผลกระทบเชิงลบและเสริมสร้างโอกาสเชิงบวกที่สนับสนุนความยั่งยืนขององค์กร โดยความเสี่ยง ผลกระทบ และการฟื้นฟูที่เกี่ยวข้องกับประเด็นตามนโยบายฉบับนี้ ได้รับการระบุ วิเคราะห์ และจัดลำดับความสำคัญผ่านกระบวนการประเมินสาระสำคัญและความเสี่ยงแบบบูรณาการของบริษัท (Vanachai Integrated Materiality and Risk Assessment: V-IMRA) ซึ่งเป็นกรอบการประเมินภายในที่ครอบคลุมทั้งมิติผลกระทบ (Impact Materiality) และมีติทางการเงิน (Financial Materiality) ตลอดห่วงโซ่คุณค่า

- **ผลลัพธ์จาก V-IMRA** ถูกนำไปบูรณาการเข้าสู่ระบบบริหารความเสี่ยงองค์กร (Enterprise Risk Management: ERM) เพื่อสนับสนุนการกำหนดนโยบาย การตัดสินใจเชิงกลยุทธ์ การ

กำหนดระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) และการสร้างคุณค่าอย่างยั่งยืนในระยะยาว

- **การระบุความเสี่ยง (Risk Identification):** บริษัทดำเนินการระบุความเสี่ยงที่อาจส่งผลกระทบต่อวัตถุประสงค์และกลยุทธ์ขององค์กรอย่างครอบคลุม ทั้งความเสี่ยงเชิงกลยุทธ์ (Strategic Risks) ความเสี่ยงด้านการปฏิบัติงาน (Operational Risks) ความเสี่ยงทางการเงิน (Financial Risks) ความเสี่ยงด้านกฎหมายและกฎระเบียบ (Compliance Risks) และความเสี่ยงด้านสิ่งแวดล้อม สังคม และธรรมาภิบาล (ESG Risks) นอกจากนี้ยังให้ความสำคัญกับความเสี่ยงที่เกิดขึ้นใหม่ (Emerging Risks) เช่น ความเสี่ยงจากการเปลี่ยนแปลงสภาพภูมิอากาศ การคุกคามทางไซเบอร์ หรือความผันผวนของเศรษฐกิจโลก เพื่อให้สามารถวางแผนรับมือได้อย่างทันถ่วงที

ความเสี่ยงและโอกาสที่เกี่ยวข้องกับความยั่งยืนซึ่งระบุผ่านกระบวนการประเมินความมีสาระสำคัญและความเสี่ยงแบบบูรณาการของวงษ์ (Vanachai Integrated Materiality and Risk Assessment: V-IMRA) จะถูกนำไปบูรณาการในกระบวนการระบุและประเมินความเสี่ยงของบริษัท โดยความเสี่ยงดังกล่าวจะได้รับการประเมินตามเกณฑ์ความน่าจะเป็นและระดับผลกระทบที่กำหนดไว้ และเมื่อมีความเหมาะสม จะถูกจัดประเภทเป็นความเสี่ยงเชิงกลยุทธ์ ความเสี่ยงด้านการดำเนินงาน ความเสี่ยงทางการเงิน ความเสี่ยงด้านการปฏิบัติตามกฎหมาย หรือความเสี่ยงด้านสิ่งแวดล้อม สังคม และธรรมาภิบาล (ESG) และบันทึกไว้ในทะเบียนความเสี่ยงขององค์กร (Enterprise Risk Register)

- **การประเมินความเสี่ยง (Risk Assessment):** บริษัทประเมินระดับความเสี่ยงโดยพิจารณาความเป็นไปได้ (Likelihood) และผลกระทบ (Impact) ที่อาจเกิดขึ้นต่อองค์กรในเชิงคุณภาพและเชิงปริมาณ เพื่อจัดลำดับความสำคัญของความเสี่ยงและวางแผนการจัดการให้เหมาะสม การประเมินความเสี่ยงจะพิจารณาทั้งในระดับองค์กร หน่วยงาน และโครงการ รวมถึงความเชื่อมโยงของความเสี่ยงระหว่างสายงาน เพื่อให้การตัดสินใจและการจัดสรรทรัพยากรเป็นไปอย่างมีประสิทธิภาพ
- **การจัดการและตอบสนองต่อความเสี่ยง (Risk Management and Response):** บริษัทกำหนดแนวทางการจัดการความเสี่ยงตามระดับความรุนแรงและลักษณะของความเสี่ยง โดยใช้วิธีการหลัก 4 รูปแบบ ได้แก่
  - **การหลีกเลี่ยงความเสี่ยง (Risk Avoidance)** – หยุดกิจกรรมหรือการตัดสินใจที่ก่อให้เกิดความเสี่ยงสูงกระบวนการอนุมัติภาษี (Tax Approval Process) – การตัดสินใจเรื่องสำคัญทางภาษี เช่น การวางแผนภาษีหรือธุรกรรมข้ามพรมแดน ต้องผ่านการอนุมัติจากคณะกรรมการบริหาร
  - **การลดความเสี่ยง (Risk Reduction)** – ดำเนินมาตรการเพื่อลดโอกาสหรือผลกระทบของความเสี่ยง

- **การถ่ายโอนความเสี่ยง (Risk Transfer)** – กระจายหรือโอนความเสี่ยงไปยังบุคคลที่สาม เช่น ผ่านประกันภัยหรือพันธบัตรทางธุรกิจ
- **การยอมรับความเสี่ยง (Risk Acceptance)** – ยอมรับความเสี่ยงในระดับที่อยู่ภายใต้เกณฑ์ที่องค์กรกำหนด (Risk Appetite)

มาตรการตอบสนองต่อความเสี่ยงจะต้องพิจารณาความคุ้มค่า (Cost-Benefit) และความเหมาะสมกับสภาพแวดล้อมทางธุรกิจ เพื่อให้เกิดประสิทธิภาพสูงสุดในการดำเนินงาน

- **การติดตามและการรายงาน (Monitoring and Reporting):** บริษัทมีระบบติดตามและทบทวนผลการบริหารความเสี่ยงอย่างต่อเนื่อง โดยมีการจัดทำรายงานผลการบริหารความเสี่ยงอย่างน้อยปีละ 2 ครั้ง เสนอคณะกรรมการบริหารความเสี่ยงและกำกับดูแลกิจการ และคณะกรรมการบริษัท ผลการติดตามจะถูกนำไปใช้ในการปรับปรุงแผนบริหารความเสี่ยง มาตรการควบคุมภายใน และกลยุทธ์องค์กร เพื่อเสริมสร้างประสิทธิภาพและความยืดหยุ่นขององค์กรในระยะยาว
- **การจัดการความพึ่งพาและความเชื่อมโยงของความเสี่ยง (Dependency and Interconnection Management):** บริษัทตระหนักถึงความเชื่อมโยงระหว่างความเสี่ยง (Risk Interdependency) ทั้งภายในและภายนอกองค์กร โดยเฉพาะในมิติของห่วงโซ่อุปทาน ความมั่นคงทางพลังงาน ทรัพยากรธรรมชาติ และการเปลี่ยนแปลงด้านสิ่งแวดล้อมและสังคม จึงดำเนินการบริหารความเสี่ยงร่วมกับพันธมิตรทางธุรกิจ คู่ค้า และผู้มีส่วนได้เสีย เพื่อเสริมสร้างความยืดหยุ่นของห่วงโซ่คุณค่าและลดความเสี่ยงจากการพึ่งพาในระยะยาว

(สอดคล้องกับ FTSE Russell GRM04, GRM05, GRM11, COSO ERM Principles 9, 10–12, GRI 102-15, GRI 102-29, GRI 102-30, GRI 102-33, SDG 12.2, SDG 12.6, SDG 13.1, SDG 16.6 และ SDG 17 – Partnerships for the Goals)

## 8) เป้าหมายและตัวชี้วัด

กำหนดเป้าหมายและตัวชี้วัดผลการดำเนินงานด้านการบริหารความเสี่ยง เพื่อให้มั่นใจว่าระบบการบริหารความเสี่ยงขององค์กรสามารถสนับสนุนการตัดสินใจเชิงกลยุทธ์ เพิ่มความยืดหยุ่นขององค์กร และสร้างคุณค่าระยะยาวให้แก่ผู้มีส่วนได้เสียทุกกลุ่ม

### เป้าหมายระยะสั้น (Short-Term Targets: 1–2 ปี):

- พนักงานระดับบริหารและปฏิบัติการ 100% ผ่านการอบรมหลักสูตรบริหารความเสี่ยง (ERM Awareness & Training)
- ทุกหน่วยงานดำเนินการประเมินความเสี่ยงหลักประจำปี และจัดทำแผนบริหารความเสี่ยง (Risk Action Plan) ครบถ้วน
- จัดตั้งและปรับปรุง ฐานข้อมูลความเสี่ยงองค์กร (Enterprise Risk Register) ให้สามารถเชื่อมโยงกับตัวชี้วัดผลการดำเนินงานของหน่วยงาน

**เป้าหมายระยะกลาง (Medium-term Targets: 3–5 ปี):**

- การบริหารความเสี่ยงได้รับการบูรณาการเข้ากับแผนกลยุทธ์ แผนงบประมาณ และการลงทุนอย่างน้อย 90% ของโครงการหลักขององค์กร
- ความเสี่ยงที่มีระดับ “สูงมาก” ได้รับการจัดการและลดระดับลงอย่างน้อย 50% ภายในระยะเวลา 3 ปี
- มีการดำเนินการตรวจสอบและประเมินความเสี่ยงในระดับโครงการ (Project Risk Review) สำหรับการลงทุนทุกโครงการที่มีมูลค่าสูงกว่า 500 ล้านบาท

**เป้าหมายระยะยาว (Long-term Targets: 5 ปีขึ้นไป):**

- บริษัทได้รับการยอมรับให้เป็นองค์กรต้นแบบด้านการบริหารความเสี่ยงและธรรมาภิบาลในอุตสาหกรรมวัสดุไม้ทดแทน
- การบริหารความเสี่ยงขององค์กรครอบคลุมทุกมิติของ ESG Risks และเชื่อมโยงกับเป้าหมายการพัฒนาอย่างยั่งยืน (SDGs)
- มีการสร้าง “วัฒนธรรมแห่งความยืดหยุ่น (Resilience Culture)” ในทุกระดับขององค์กร โดยพนักงานทุกคนตระหนักถึงบทบาทของตนในการบริหารความเสี่ยง

**ตัวชี้วัดหลัก (Key Performance Indicators – KPIs)**

หมวด	ตัวชี้วัด (Indicators)	หน่วยวัด / เป้าหมาย	หน่วยงานรับผิดชอบ
<b>การบริหารความเสี่ยงเชิงกลยุทธ์</b>	สัดส่วนโครงการหรือแผนกลยุทธ์ที่มีการประเมินความเสี่ยงครบถ้วน	≥ 90%	ฝ่ายบริหารความเสี่ยง / คณะกรรมการบริหารความเสี่ยง
<b>การบริหารความเสี่ยงระดับปฏิบัติการ</b>	การบริหารความเสี่ยงระดับปฏิบัติการ จำนวนหน่วยงานที่ดำเนินการประเมินความเสี่ยงและจัดทำ Risk Action Plan ประจำปี	100%	หัวหน้าหน่วยงาน / คณะทำงานบริหารความเสี่ยง
<b>การอบรมและการสื่อสาร</b>	ร้อยละของพนักงานที่ผ่านการอบรมบริหารความเสี่ยงประจำปี	100%	ฝ่ายทรัพยากรบุคคล / ฝ่ายบริหารความยั่งยืน
<b>การจัดการความเสี่ยงสำคัญ</b>	จำนวนความเสี่ยงระดับสูง (High & Critical Risks) ที่ได้รับการลดระดับลงหลังการดำเนินการ	≥ 50%	คณะกรรมการบริหารความเสี่ยงและกำกับดูแลกิจการ
<b>การเปิดเผยข้อมูลและรายงาน</b>	ความครบถ้วนและความโปร่งใสของรายงานความเสี่ยงต่อคณะกรรมการ	100% ครบถ้วน 2 ครั้งต่อปี	หน่วยตรวจสอบภายใน / ฝ่ายบริหารความเสี่ยง

**การบูรณาการกับการประเมินผลการดำเนินงาน (Integration with Performance Evaluation):** ผลการดำเนินงานด้านการบริหารความเสี่ยงจะถูกนำมาประกอบการประเมินผลของผู้บริหารและหน่วยงาน เพื่อเสริมสร้างความรับผิดชอบและแรงจูงใจในการบริหารความเสี่ยงอย่างต่อเนื่องและเป็นรูปธรรม

(สอดคล้องกับเกณฑ์ FTSE Russell GRM04, GRM05, GRM11, COSO ERM Principle 6, GRI 102-29, GRI 102-30, SDG 4.7, SDG 9.1, SDG 12.6, SDG 16.6)

## 9) ห่วงโซ่อุปทาน และความรับผิดชอบต่อพันธมิตร

- **การประเมินและคัดเลือกคู่ค้าตามหลักความเสี่ยง (FTSE Russell GRM04, GRI 102-15, SDG 12.6 และ SDG 16.6):** บริษัทดำเนินการคัดเลือกและประเมินคู่ค้าทางธุรกิจโดยใช้แนวทางการบริหารความเสี่ยงเชิงรุก (Risk-Based Due Diligence) ครอบคลุมด้านการเงิน การปฏิบัติตามกฎหมาย การจัดการแรงงาน ความปลอดภัย สิ่งแวดล้อม และธรรมาภิบาล (ESG Criteria) เพื่อให้มั่นใจว่าคู่ค้ามีระบบบริหารจัดการที่โปร่งใสและสอดคล้องกับค่านิยมของบริษัท
- **การบริหารความเสี่ยงในห่วงโซ่อุปทาน (FTSE Russell GRM05, GRI 102-29, SDG 12.2 และ SDG 13.1):** บริษัทประเมินความเสี่ยงในห่วงโซ่อุปทานเป็นประจำ เช่น ความเสี่ยงจากการหยุดชะงักของวัตถุดิบ การขนส่ง หรือความล่าช้าในการส่งมอบ เพื่อเตรียมมาตรการป้องกันและแผนสำรอง (Contingency Plan) ที่เหมาะสม นอกจากนี้บริษัทได้บูรณาการการบริหารความเสี่ยงด้านสิ่งแวดล้อมและสังคม เช่น การจัดการทรัพยากร การปล่อยก๊าซเรือนกระจก และสิทธิมนุษยชนของแรงงานในห่วงโซ่อุปทาน เพื่อสร้างความยั่งยืนตลอดวงจรธุรกิจ
- **การตรวจสอบและติดตามผล (FTSE Russell GRM05, GRM11, GRI 205-3, SDG 16.6):** บริษัทดำเนินการตรวจสอบและติดตามคู่ค้าทางธุรกิจอย่างต่อเนื่อง เพื่อให้มั่นใจว่ามีการปฏิบัติตาม นโยบายบริหารความเสี่ยง และ จรรยาบรรณของคู่ค้า (Supplier Code of Conduct) โดยใช้กระบวนการประเมินภายในหรือผู้ตรวจสอบอิสระภายนอกตามความเหมาะสม หากพบว่าการละเมิดหรือไม่ปฏิบัติตามมาตรฐาน บริษัทจะดำเนินการปรับปรุง หรือพิจารณาระงับความร่วมมือทางธุรกิจตามขั้นตอนที่กำหนด
- **การบริหารความเสี่ยงจากบุคคลที่สาม (FTSE Russell GRM05, GRI 102-30, SDG 12.6 และ SDG 17):** บริษัทให้ความสำคัญกับการบริหารความเสี่ยงที่เกิดจากบุคคลที่สาม (Third Parties) เช่น ตัวแทน ผู้รับจ้าง และผู้ให้บริการ โดยใช้หลักการตรวจสอบสถานะ (Due Diligence) เพื่อประเมินความน่าเชื่อถือ ประวัติการดำเนินงาน และความสอดคล้องกับมาตรฐานด้าน ESG และธรรมาภิบาลของบริษัท กระบวนการดังกล่าวช่วยลดความเสี่ยงด้านชื่อเสียง กฎหมาย และการปฏิบัติที่อาจกระทบต่อองค์กรในระยะยาว
- **การสร้างพันธมิตรเชิงกลยุทธ์อย่างยั่งยืน (FTSE Russell GRM11 – Risk Disclosure and Partnership, GRI 102-43, SDG 17 – Partnerships for the Goals):** บริษัทส่งเสริมการสร้างความร่วมมือระยะยาวกับคู่ค้าและพันธมิตรทางธุรกิจที่มีแนวทางบริหารความเสี่ยงอย่างมี

ธรรมาภิบาล โปร่งใส และสอดคล้องกับหลักการพัฒนาอย่างยั่งยืน โดยสนับสนุนการแลกเปลี่ยนข้อมูล การพัฒนาขีดความสามารถ และการปรับปรุงกระบวนการบริหารความเสี่ยงร่วมกัน

- **การรายงานและการเปิดเผยข้อมูล (FTSE Russell GRM11, GRI 102-33, SDG 16.10):** บริษัทเปิดเผยข้อมูลผลการบริหารความเสี่ยงในห่วงโซ่อุปทานอย่างโปร่งใส ผ่านรายงานความยั่งยืนประจำปี (Sustainability Report) และช่องทางการสื่อสารขององค์กร เพื่อแสดงความรับผิดชอบต่อผู้มีส่วนได้เสียและยกระดับมาตรฐานธรรมาภิบาลในอุตสาหกรรม

## 10) การบูรณาการกับกลยุทธ์องค์กร

### 10.1) การบูรณาการกับการกำหนดกลยุทธ์ (FTSE Russell GRM05, COSO ERM Principle 4, GRI 102-29, SDG 16.6):

- บริษัทนำผลการประเมินความเสี่ยงมาใช้เป็นข้อมูลสำคัญในการกำหนดแผนกลยุทธ์ การลงทุน และการจัดลำดับความสำคัญของโครงการ เพื่อให้มั่นใจว่าการตัดสินใจเชิงกลยุทธ์ทั้งหมดอยู่ภายใต้ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) และสอดคล้องกับเป้าหมายระยะยาวขององค์กร
- ผลลัพธ์จากการประเมินความมีสาระสำคัญและความเสี่ยงแบบบูรณาการของวงวนช่วย (Vanachai Integrated Materiality and Risk Assessment: V-IMRA) จะถูกนำมาพิจารณาร่วมกับการประเมินความเสี่ยงในระดับองค์กร เพื่อสนับสนุนการวางแผนเชิงกลยุทธ์ การจัดสรรเงินลงทุน และการตัดสินใจด้านการลงทุนที่มีนัยสำคัญ โดยมีเป้าหมายเพื่อให้มั่นใจว่าความเสี่ยงและโอกาสที่เกี่ยวข้องกับความยั่งยืนได้รับการพิจารณาอย่างรอบด้าน เชิงคาดการณ์ล่วงหน้า และบูรณาการเข้ากับกระบวนการตัดสินใจขององค์กรอย่างเป็นระบบ

### 10.2) การบูรณาการกับกรอบกลยุทธ์ FOREST | FUTURE | TOGETHER – for a Sustainable Living

- **FOREST – ธรรมาภิบาลและการใช้ทรัพยากรอย่างรับผิดชอบ:** การบริหารความเสี่ยงด้านสิ่งแวดล้อมและห่วงโซ่อุปทาน เพื่อป้องกันการใช้ทรัพยากรอย่างเกินจำเป็น สนับสนุนเศรษฐกิจหมุนเวียน และรักษาสมดุลระหว่างธุรกิจกับระบบนิเวศ
- **FUTURE – นวัตกรรมและความยืดหยุ่นขององค์กร:** การใช้กระบวนการบริหารความเสี่ยงเพื่อสนับสนุนการพัฒนาเทคโนโลยี การลงทุนในนวัตกรรม และการสร้างระบบบริหารจัดการที่ยืดหยุ่น รองรับความไม่แน่นอนของตลาดและสภาพแวดล้อม
- **TOGETHER - ความร่วมมือและความไว้วางใจจากผู้มีส่วนได้เสีย:** การบริหารความเสี่ยงในมิติทางสังคมและธรรมาภิบาล โดยสร้างความร่วมมือกับพนักงาน คู่ค้า และชุมชน เพื่อเสริมสร้างความเชื่อมั่นและลดความเสี่ยงเชิงชื่อเสียงขององค์กร

(สอดคล้องกับ FTSE Russell GRM04–GRM11, GRI 102-30, SDG 8.8, SDG 12.6 และ SDG 17)

**10.3) การสนับสนุนการตัดสินใจเชิงกลยุทธ์ (FTSE Russell GRM05, COSO ERM Principle 6, GRI 102-29, SDG 16.6):** ผลการวิเคราะห์และรายงานความเสี่ยงจากระบบ ERM ถูกนำมาใช้เป็นข้อมูลประกอบในการตัดสินใจของคณะกรรมการบริหารและคณะกรรมการบริษัท เพื่อสร้างสมดุลระหว่างการเติบโตและความเสี่ยง (Risk-Return Balance) และสนับสนุนการสร้างคุณค่าทางเศรษฐกิจ สังคม และสิ่งแวดล้อมในระยะยาว

**10.4) การขับเคลื่อนค่านิยมองค์กรและวัฒนธรรมแห่งความยืดหยุ่น (FTSE Russell GRM04, GRM05, GRI 102-30, SDG 4.7 และ SDG 16.6):** บริษัทส่งเสริมให้การบริหารความเสี่ยงเป็นส่วนหนึ่งของค่านิยมองค์กร (Corporate Values) โดยผนวกแนวคิดเรื่องความรอบคอบ ความรับผิดชอบ และความโปร่งใสในการตัดสินใจเข้ากับวัฒนธรรมการทำงาน เพื่อสร้างองค์กรที่มีความยืดหยุ่น (Resilient Organization) และพร้อมรับมือกับการเปลี่ยนแปลงในอนาคต

## 11) การดำเนินงานและเครื่องมือ

- **กรอบการบริหารความเสี่ยงขององค์กร (FTSE Russell GRM04, COSO ERM Principle 1–3, GRI 102-29, SDG 16.6):** บริษัทใช้กรอบการบริหารความเสี่ยงตามมาตรฐาน COSO ERM (2017): Integrating with Strategy and Performance และ ISO 31000:2018 เพื่อให้การบริหารความเสี่ยงมีความเชื่อมโยงกับกลยุทธ์องค์กร และสามารถปรับตัวต่อการเปลี่ยนแปลงของสภาพแวดล้อมทางธุรกิจ โครงสร้างกรอบประกอบด้วยกระบวนการหลัก ได้แก่ การระบุ (Identify) การประเมิน (Assess) การจัดการ (Manage) การติดตามและรายงาน (Monitor & Report)
- **ระบบบริหารและการบูรณาการ (FTSE Russell GRM05, GRI 102-30, SDG 12.6 และ SDG 16.6):** บริษัทบูรณาการการบริหารความเสี่ยงเข้ากับระบบการจัดการหลักขององค์กร ได้แก่
  - ระบบบริหารความยั่งยืน (Sustainability Management System)
  - ระบบควบคุมภายใน (Internal Control System)
  - ระบบบริหารคุณภาพ (Quality Management System – ISO 9001)
  - ระบบอาชีวอนามัยและความปลอดภัย (ISO 45001)
  - ระบบสิ่งแวดล้อม (ISO 14001)การบูรณาการดังกล่าวช่วยให้ทุกหน่วยงานสามารถระบุและจัดการความเสี่ยงในกระบวนการของตนได้อย่างสอดคล้องและเป็นมาตรฐานเดียวกันทั่วทั้งองค์กร
- **เครื่องมือและเทคโนโลยีในการบริหารความเสี่ยง (FTSE Russell GRM04, GRM11, COSO ERM Principle 6–8, SDG 9.5 และ SDG 16.6):** บริษัทนำเทคโนโลยีและระบบสารสนเทศมาใช้ในการบริหารความเสี่ยง เช่น

- Enterprise Risk Register System: ระบบจัดเก็บข้อมูลความเสี่ยงขององค์กร เพื่อใช้ติดตามและอัปเดตสถานะความเสี่ยงแบบเรียลไทม์
- Risk Dashboard: เครื่องมือแสดงภาพรวมของระดับความเสี่ยงหลัก (Key Risk Indicators: KRIs) เพื่อสนับสนุนการตัดสินใจของผู้บริหาร
- Data Analytics Tools: ใช้ข้อมูลเชิงวิเคราะห์เพื่อตรวจจับแนวโน้มและสัญญาณเตือนล่วงหน้า (Early Warning Signals)
- Cybersecurity and Data Protection Tools: ป้องกันความเสี่ยงด้านเทคโนโลยีสารสนเทศและการรั่วไหลของข้อมูล
- **ระบบรายงานความเสี่ยง** (FTSE Russell GRM11 – Risk Disclosure, GRI 102-33, SDG 16.10): บริษัทจัดให้มีระบบรายงานความเสี่ยงที่โปร่งใสและเป็นระบบ เพื่อให้สามารถรายงานความเสี่ยงสำคัญ (Key Risks) และเหตุการณ์ที่อาจกระทบต่อองค์กรได้อย่างทันท่วงที โดยใช้ช่องทางต่อไปนี้
  - รายงานต่อคณะกรรมการบริหารความเสี่ยงและกำกับดูแลกิจการ (2 ครั้งต่อปี)
  - รายงานต่อคณะกรรมการบริษัท (รายครึ่งปี / รายปี)
  - รายงานเฉพาะกิจในกรณีที่เกิดเหตุการณ์วิกฤต (Crisis or Incident Reporting)ระบบดังกล่าวช่วยให้สามารถติดตามความเสี่ยงได้อย่างต่อเนื่องและเพิ่มความโปร่งใสในการสื่อสารภายในองค์กร
- **การเสริมสร้างศักยภาพและความตระหนักรู้** (FTSE Russell GRM05, GRI 102-30, SDG 4.7 และ SDG 16.6): บริษัทจัดให้มีการอบรมและกิจกรรมสร้างความตระหนักรู้เกี่ยวกับการบริหารความเสี่ยงอย่างต่อเนื่อง ทั้งในระดับผู้บริหารและพนักงาน เพื่อให้เข้าใจบทบาทหน้าที่และสามารถบริหารความเสี่ยงในขอบเขตความรับผิดชอบของตนได้อย่างเหมาะสม นอกจากนี้ ยังสนับสนุนการแลกเปลี่ยนประสบการณ์และแนวทางปฏิบัติที่ดี (Best Practices) ระหว่างหน่วยงาน เพื่อพัฒนาระบบบริหารความเสี่ยงขององค์กรให้มีประสิทธิภาพยิ่งขึ้น

## 12) การติดตาม รายงาน และความโปร่งใส

- **การติดตามและประเมินผล** (FTSE Russell GRM05, COSO ERM Principle 16, GRI 102-30, SDG 16.6): บริษัทบริหารจัดการให้มีการติดตามและประเมินผลการบริหารความเสี่ยงเป็นประจำ โดยพิจารณาความเหมาะสมของมาตรการควบคุม ความครอบคลุมของการประเมิน และประสิทธิภาพของกระบวนการบริหารความเสี่ยงในแต่ละหน่วยงาน ผลการติดตามจะถูกนำมาวิเคราะห์เพื่อปรับปรุงระบบและกระบวนการบริหารความเสี่ยงให้ทันสมัยและสอดคล้องกับสถานการณ์ปัจจุบัน
- **การรายงานภายใน** (FTSE Russell GRM05, GRM11, GRI 102-33, SDG 16.6):
  - ผลการคณะกรรมการบริหารความเสี่ยงและกำกับดูแลกิจการรายงานผลการประเมินความเสี่ยงและสถานะความเสี่ยงหลักต่อคณะกรรมการบริษัทเป็นประจำทุกไตรมาส

- หน่วยงานบริหารความเสี่ยงจัดทำรายงานสรุปความเสี่ยงรายเดือนต่อผู้บริหารระดับสูง เพื่อใช้ประกอบการตัดสินใจทางธุรกิจ
- หน่วยงานตรวจสอบภายในรายงานผลการประเมินระบบบริหารความเสี่ยงต่อคณะกรรมการตรวจสอบอย่างน้อยปีละ 1 ครั้ง

รายงานทั้งหมดต้องมีข้อมูลที่ถูกต้อง ครบถ้วน และสามารถตรวจสอบย้อนกลับได้ เพื่อเสริมสร้างความเชื่อมั่นในการตัดสินใจและกำกับดูแล

- **การเปิดเผยข้อมูลต่อสาธารณะ** (FTSE Russell GRM11 – Risk Disclosure and Transparency, GRI 102-33, SDG 16.10): บริษัทเปิดเผยข้อมูลด้านการบริหารความเสี่ยง และประเด็นความเสี่ยงที่มีนัยสำคัญใน รายงานความยั่งยืนประจำปี (Sustainability Report) และ รายงานประจำปี (Annual Report) เพื่อให้ผู้ถือหุ้น นักลงทุน หน่วยงานภาครัฐ และผู้มีส่วนได้เสียสามารถติดตาม ตรวจสอบ และประเมินความโปร่งใสขององค์กรได้อย่างต่อเนื่อง
- **การสื่อสารผลภายในองค์กร** (FTSE Russell GRM05, GRI 102-43, SDG 16.7): บริษัทจัดให้มี ช่องทางการสื่อสารภายใน เช่น อินทราเน็ต ประกาศภายใน หรือการประชุมประจำเดือน เพื่อ เผยแพร่ข้อมูลเกี่ยวกับความเสี่ยง ผลการประเมิน และแนวทางการจัดการความเสี่ยงที่สำคัญ เพื่อสร้างการรับรู้และความเข้าใจร่วมกันในทุกกระดับขององค์กร
- **การตรวจสอบและทวนสอบข้อมูล** (FTSE Russell GRM11, GRI 102-56, SDG 16.6): บริษัท ดำเนินการตรวจสอบและทวนสอบข้อมูลด้านการบริหารความเสี่ยงโดยหน่วยงานภายในและผู้ ตรวจสอบอิสระภายนอก เพื่อยืนยันความถูกต้อง ความครบถ้วน และความน่าเชื่อถือของ ข้อมูลที่เปิดเผย ทั้งในรายงานความยั่งยืนและรายงานประจำปี

### 13) การทบทวนและพัฒนาอย่างต่อเนื่อง

- **การทบทวนนโยบาย** (FTSE Russell GRM07 – Board Oversight and Governance Integration, GRI 102-33, SDG 16.6): บริษัทดำเนินการทบทวนนโยบายการบริหาร ความเสี่ยงอย่างน้อยทุก 2 ปี หรือเมื่อมีการเปลี่ยนแปลงเชิงนโยบาย กฎหมาย โครงสร้างองค์กร หรือความเสี่ยงระดับกลยุทธ์ เพื่อให้แน่ใจว่านโยบายมีความเหมาะสม ครอบคลุม และสอดคล้อง กับเป้าหมายของบริษัทและมาตรฐานสากล
- **การประเมินประสิทธิผลของระบบ** (FTSE Russell GRM05, COSO ERM Principle 20, GRI 102-30, SDG 16.6): คณะกรรมการบริหารความเสี่ยงและกำกับดูแลกิจการร่วมกับหน่วย ตรวจสอบภายใน ดำเนินการประเมินประสิทธิผลของระบบบริหารความเสี่ยงเป็นประจำ โดย พิจารณาจากตัวชี้วัดหลัก (KPIs) ผลการตรวจสอบ และความสามารถในการบริหารความเสี่ยง ที่เกิดขึ้นจริง เพื่อนำผลการประเมินไปใช้ปรับปรุงระบบให้ตอบสนองต่อการเปลี่ยนแปลงได้ดี ยิ่งขึ้น
- **การพัฒนาอย่างต่อเนื่อง** (FTSE Russell GRM05, ISO 31000:2018, GRI 102-30, SDG 4.7 และ SDG 9.5): บริษัทส่งเสริมให้มีการเรียนรู้จากเหตุการณ์ความเสี่ยงจริง (Lessons

Learned) และผลการตรวจสอบ เพื่อปรับปรุงมาตรการควบคุมภายใน กระบวนการ และเทคโนโลยีที่ใช้ในการบริหารความเสี่ยงอย่างต่อเนื่อง นอกจากนี้บริษัทสนับสนุนการวิจัยและนวัตกรรม (Innovation) เพื่อยกระดับการบริหารความเสี่ยงให้มีความแม่นยำ คล่องตัว และเป็นเชิงรุกมากขึ้น

- **การพัฒนาองค์ความรู้และศักยภาพบุคลากร** (FTSE Russell GRM04–GRM05, GRI 102-43, SDG 4.7 และ SDG 17): บริษัทจัดให้มีการอบรมและแลกเปลี่ยนความรู้ด้านการบริหารความเสี่ยงอย่างต่อเนื่อง ทั้งภายในและภายนอกองค์กร เพื่อให้พนักงานทุกระดับเข้าใจแนวทางการประเมินและจัดการความเสี่ยงได้อย่างมีประสิทธิภาพ นอกจากนี้บริษัทส่งเสริมให้มีการแลกเปลี่ยนแนวปฏิบัติที่ดี (Best Practices) ระหว่างหน่วยงาน เพื่อสร้างวัฒนธรรมองค์กรแห่งการพัฒนาและเรียนรู้อย่างยั่งยืน

#### 14) ประวัติการทบทวนและปรับปรุงนโยบายการบริหารความเสี่ยงในระดับองค์กร

ฉบับที่	วันที่	เจ้าของนโยบาย	อนุมัติโดย	การเปลี่ยนแปลง / เหตุผลสำคัญ
1.0	11 พฤศจิกายน 2567	คณะกรรมการ บริหารความเสี่ยง และกำกับดูแล กิจการ	คณะกรรมการ บริษัท	จัดทำนโยบายฉบับแรก เพื่อวางกรอบการ บริหารความเสี่ยงขององค์กรให้สอดคล้อง กับหลักธรรมาภิบาลและข้อกำหนดของตลาด หลักทรัพย์แห่งประเทศไทย
2.0	11 พฤศจิกายน 2568	คณะกรรมการ บริหารความเสี่ยง และกำกับดูแล กิจการ	คณะกรรมการ บริษัท	ปรับปรุงแก้ไขให้สอดคล้องกับเกณฑ์ FTSE Russell ESG ด้านการกำกับดูแลและการ บริหารความเสี่ยง (GRM04–GRM11) กรอบ การบริหารความเสี่ยงองค์กรของ COSO (Enterprise Risk Management Framework, 2017) และ มาตรฐาน GRI 102-15 และ 102-30 โดยเสริมสร้าง โครงสร้างการกำกับดูแลและการกำกับ ติดตามให้มีความเข้มแข็ง บูรณาการความ เสี่ยงเชิงกลยุทธ์ ความเสี่ยงด้านการ ดำเนินงาน และความเสี่ยงด้าน ESG เข้าสู่ ระบบบริหารความเสี่ยงขององค์กรใน ภาพรวม ยกกระดับการเปิดเผยข้อมูลด้าน ความเสี่ยงให้มีความโปร่งใสและสอดคล้อง กันอย่างเป็นระบบ และผนวกการประเมิน สาระสำคัญและความเสี่ยงแบบบูรณาการ ของวนชัย (Vanachai Integrated Materiality and Risk Assessment: V- IMRA) เป็นข้อมูลนำเข้าหลักในกระบวนการ บริหารความเสี่ยงขององค์กร (Enterprise Risk Management: ERM) อย่างเป็นทางการ

นโยบายฉบับนี้ได้รับการอนุมัติและประกาศใช้เพื่อให้ผู้เกี่ยวข้องทุกฝ่ายรับทราบและนำไปปฏิบัติ