

นโยบายและแนวปฏิบัติการบริหารจัดการ
ความเสี่ยงองค์กร



บริษัท ศิริรินทร์ จำกัด (มหาชน)

นโยบายและแนวปฏิบัติการบริหารจัดการความเสี่ยงองค์กร

บริษัท ศิครินทร์ จำกัด (มหาชน) (“บริษัท”) ตระหนักดีว่าความเสี่ยงเป็นปัจจัยสำคัญที่ส่งผลกระทบต่อความสำเร็จและความยั่งยืนขององค์กรในระยะยาว การบริหารความเสี่ยงอย่างเป็นระบบและครอบคลุมจึงเป็นกลไกสำคัญในการเสริมสร้างความสามารถในการแข่งขัน การบรรลุวิสัยทัศน์ พันธกิจ และเป้าหมายเชิงกลยุทธ์ของบริษัท ทั้งในด้านเศรษฐกิจ สังคม และสิ่งแวดล้อม

บริษัทจึงจัดทำนโยบายและแนวปฏิบัติการบริหารจัดการความเสี่ยงองค์กรฉบับนี้ขึ้น โดยยึดตามกรอบการบริหารความเสี่ยงของ COSO (Enterprise Risk Management Framework: 2017 Edition) พร้อมบูรณาการข้อกำหนด และแนวทางของประเทศ และสากลที่เกี่ยวข้อง เพื่อยกระดับการบริหารจัดการความเสี่ยงองค์กร และบูรณาการการบริหารจัดการความเสี่ยงให้เป็นส่วนหนึ่งของวัฒนธรรมองค์กร และกระบวนการตัดสินใจทุกระดับ

ขอบเขตนโยบาย

นโยบายและแนวปฏิบัติฉบับนี้ใช้บังคับกับบริษัท ศิครินทร์ จำกัด (มหาชน) (“บริษัท”) หมายถึง บริษัท ศิครินทร์ จำกัด (มหาชน) และบริษัทในกลุ่มของศิครินทร์ทุกบริษัท ซึ่ง “บริษัท” ที่จะกล่าวถึงในเอกสารฉบับนี้ โดยให้ครอบคลุมถึงการบริหารจัดการความเสี่ยงในทุกมิติที่เกี่ยวข้องกับการดำเนินธุรกิจ เพื่อให้สามารถบริหารจัดการความเสี่ยงได้อย่างรอบด้าน บูรณาการ และมีความต่อเนื่อง

วัตถุประสงค์

บริษัท ศิครินทร์ จำกัด (มหาชน) (“บริษัท”) ได้จัดทำนโยบายและแนวปฏิบัติการบริหารจัดการความเสี่ยงองค์กรขึ้น โดยมีวัตถุประสงค์เพื่อสร้างระบบการบริหารความเสี่ยงที่มีประสิทธิภาพ โปร่งใส และสามารถตรวจสอบได้ โดยระบบดังกล่าวจะต้องสามารถสนับสนุนกลยุทธ์และทิศทางการดำเนินงานขององค์กรในทุกมิติ ทั้งด้านการวางแผน การกำหนดนโยบาย และการปฏิบัติงานในระดับต่าง ๆ อย่างเป็นระบบและบูรณาการ นอกจากนี้ นโยบายและแนวปฏิบัตินี้มีเป้าหมายสำคัญในการเสริมสร้างศักยภาพของบริษัทในการเติบโตอย่างมั่นคงและยั่งยืน รวมถึงการสร้างคุณค่าร่วมระหว่างบริษัทกับผู้มีส่วนได้เสียทั้งภายในและภายนอกองค์กร อีกทั้งยังมุ่งหมายเพื่อเสริมสร้างความเชื่อมั่นให้แก่คณะกรรมการบริษัท ผู้บริหารระดับสูง และผู้มีส่วนได้เสียทุกกลุ่ม ว่าบริษัทมีความสามารถในการรับมือกับเหตุการณ์ไม่แน่นอน ความเปลี่ยนแปลงทางธุรกิจ และปัจจัยเสี่ยงที่อาจกระทบต่อเป้าหมายเชิงกลยุทธ์ขององค์กรได้อย่างทันท่วงทีและมีประสิทธิภาพ

หน้าที่และความรับผิดชอบ

คณะกรรมการบริษัท

- กำหนดนโยบาย ทิศทาง และกรอบการบริหารความเสี่ยงในระดับองค์กรให้สอดคล้องกับกลยุทธ์ของบริษัท
- อนุมัติระดับความเสี่ยงที่องค์กรสามารถยอมรับได้ (Risk Appetite)
- ทบทวนความเหมาะสมของระบบและกระบวนการบริหารความเสี่ยงอย่างน้อยปีละหนึ่งครั้ง
- ติดตามและกำกับดูแลการดำเนินงานด้านการบริหารความเสี่ยงของคณะกรรมการบริหารความเสี่ยงองค์กรและฝ่ายบริหาร
- ให้คำแนะนำเชิงนโยบาย และสนับสนุนการพัฒนาวัฒนธรรมองค์กรที่ตระหนักรู้ถึงความเสี่ยงอย่างต่อเนื่อง

คณะกรรมการบริหารความเสี่ยงองค์กร

- กำหนดแนวทาง กลยุทธ์ และแผนบริหารความเสี่ยงที่ครอบคลุมทุกมิติของความเสี่ยง
- พิจารณาความเสี่ยงเชิงระบบและความเสี่ยงระดับองค์กร รวมถึง Emerging Risks และ ESG Risks
- ติดตาม ประเมิน และปรับปรุงระบบบริหารความเสี่ยงให้ทันต่อบริบทที่เปลี่ยนแปลง
- ส่งเสริมการบูรณาการการบริหารความเสี่ยงในกระบวนการดำเนินงานของทุกหน่วยงาน
- รายงานผลการดำเนินงานด้านการบริหารความเสี่ยงต่อคณะกรรมการบริษัทตามระยะเวลาที่กำหนด

ผู้บริหารระดับสูง

- นำแนวนโยบายและแผนบริหารความเสี่ยงไปปฏิบัติให้เหมาะสมกับหน่วยงานในความรับผิดชอบ
- ส่งเสริมการวางแผนและตัดสินใจที่พิจารณาความเสี่ยงเป็นองค์ประกอบสำคัญ
- ติดตามและประเมินสถานการณ์ความเสี่ยงอย่างสม่ำเสมอ พร้อมเสนอแนวทางแก้ไขหรือพัฒนา
- สนับสนุนการพัฒนาศักยภาพด้านการบริหารความเสี่ยงแก่บุคลากรในหน่วยงาน
- รายงานผลการบริหารความเสี่ยงต่อคณะกรรมการบริหารความเสี่ยงองค์กรตามรอบเวลา

หน่วยงานปฏิบัติ / เจ้าของความเสี่ยง (Risk Owner)

- ระบุและประเมินความเสี่ยงที่เกี่ยวข้องกับการดำเนินงานในแต่ละสายงาน
- กำหนดมาตรการจัดการความเสี่ยง (Risk Treatment) ที่เหมาะสมกับระดับความเสี่ยงที่ระบุ
- ติดตามและปรับปรุงมาตรการควบคุมความเสี่ยงให้มีประสิทธิภาพสม่ำเสมอ
- จัดทำรายงานความเสี่ยงรายไตรมาส หรือเมื่อเกิดเหตุการณ์สำคัญ
- ประสานงานกับผู้บริหารระดับสูงเพื่อปรับปรุงกระบวนการหรือระบบควบคุมภายใน

ฝ่ายตรวจสอบภายใน

- ตรวจสอบประเมินความเหมาะสมและประสิทธิผลของกระบวนการบริหารความเสี่ยงอย่างเป็นระบบ
- ตรวจสอบการปฏิบัติตามนโยบาย มาตรฐาน และระเบียบที่เกี่ยวข้องกับความเสี่ยง
- ให้ข้อเสนอแนะแนวทางการปรับปรุงระบบบริหารความเสี่ยง เพื่อให้สามารถรองรับการเปลี่ยนแปลงได้อย่างยั่งยืน
- รายงานผลการตรวจสอบต่อคณะกรรมการตรวจสอบและคณะกรรมการบริษัท

พนักงาน

- ปฏิบัติงานภายใต้แนวทางการบริหารความเสี่ยงที่กำหนดไว้ในนโยบาย และคู่มือหรือแนวปฏิบัติที่เกี่ยวข้องในแต่ละหน่วยงาน
- ตระหนักถึงความเสี่ยงที่อาจเกิดขึ้นจากการปฏิบัติงานของตน และให้ความร่วมมือในการระบุ วิเคราะห์ และรายงาน ความเสี่ยงอย่างถูกต้องและทันเวลา
- ปฏิบัติตามมาตรการควบคุมความเสี่ยง รวมถึงแนวทางด้านความปลอดภัย กฎหมาย และจริยธรรมที่บริษัทกำหนดไว้อย่างเคร่งครัด
- แจ้งเหตุการณ์ความเสี่ยงหรือความผิดปกติที่พบเห็นผ่านช่องทางที่บริษัทกำหนด เช่น การรายงานต่อหัวหน้างาน โดยตรง หรือผ่านระบบแจ้งเหตุ (Incident Report)
- เข้าร่วมการฝึกอบรมและกิจกรรมสร้างการเรียนรู้ด้านการบริหารความเสี่ยงที่บริษัทจัดขึ้น เพื่อพัฒนาทักษะ ความเข้าใจ และความสามารถในการบริหารจัดการความเสี่ยงในบทบาทของตน
- มีส่วนร่วมในการสร้างวัฒนธรรมองค์กรที่ส่งเสริมความโปร่งใส การเรียนรู้จากความผิดพลาด และความรับผิดชอบร่วมกันในการป้องกันและลดผลกระทบจากความเสี่ยงในทุกระดับ

แนวปฏิบัติ

บริษัท ศิครินทร์ จำกัด (มหาชน) ได้กำหนดหลักการบริหารความเสี่ยงที่ครอบคลุมและเชื่อมโยงกับบริบทขององค์กรอย่างเป็นระบบ โดยยึดตามแนวปฏิบัติสากลด้านการบริหารความเสี่ยง อาทิ กรอบการบริหารความเสี่ยงของ COSO ERM 2017, มาตรฐาน ISO 31000 และแนวทางการเปิดเผยข้อมูลความเสี่ยงด้าน ESG และ Climate ตาม IFRS S1 และ S2 โดยหลักการบริหารความเสี่ยงของบริษัทแบ่งออกเป็น 5 ขั้นตอนสำคัญ ดังนี้

การระบุความเสี่ยง (Risk Identification)

การระบุความเสี่ยงเป็นขั้นตอนเริ่มต้นที่สำคัญ ซึ่งมีเป้าหมายเพื่อให้สามารถเข้าใจเหตุการณ์ที่อาจเกิดขึ้นและส่งผลกระทบต่อการบรรลุวัตถุประสงค์ขององค์กร ทั้งในระดับกลยุทธ์และการปฏิบัติการ โดยบริษัทกำหนดแนวทางดังนี้

- พิจารณาความเสี่ยงจากทั้ง **ปัจจัยภายใน** (เช่น โครงสร้างองค์กร การดำเนินงาน ทรัพยากร บุคลากร ระบบเทคโนโลยี) และ **ปัจจัยภายนอก** (เช่น เศรษฐกิจ ภูมิรัฐศาสตร์ การเปลี่ยนแปลงสภาพภูมิอากาศ กฎระเบียบ และพฤติกรรมผู้บริโภค)
- เชื่อมโยงการระบุความเสี่ยงกับการวิเคราะห์บริบทองค์กร (Organizational Context) และปัจจัยด้านสิ่งแวดล้อม สังคม ธรรมชาติ (ESG) และความเสี่ยงด้านสภาพภูมิอากาศ (Climate-related Risk) โดยเฉพาะในระดับกลยุทธ์
- อ้างอิงจากข้อมูลประวัติความเสี่ยง เหตุการณ์ความผิดพลาด รายงานภายนอก และฐานข้อมูลอุตสาหกรรม เพื่อระบุความเสี่ยงเกิดใหม่ (Emerging Risks) อย่างสม่ำเสมอ
- ใช้เทคนิคต่าง ๆ เช่น SWOT, PESTEL, Scenario Planning, Brainstorming, RCSA (Risk & Control Self Assessment) ร่วมกับหน่วยงานที่เกี่ยวข้องในการระบุความเสี่ยง

การประเมินและจัดอันดับความเสี่ยง (Risk Assessment and Prioritization)

บริษัทใช้กระบวนการประเมินความเสี่ยงทั้งเชิงคุณภาพและเชิงปริมาณ เพื่อตัดสินใจว่า ความเสี่ยงใดควรได้รับการจัดการก่อนตามระดับความรุนแรง ดังนี้

- ประเมินความเสี่ยงโดยพิจารณา “ความเป็นไปได้ในการเกิด” (Likelihood) และ “ผลกระทบที่อาจเกิดขึ้น” (Impact) โดยใช้ตารางเมทริกซ์ความเสี่ยง (Risk Matrix)
- ประเมินผลกระทบทั้งในมิติ การเงิน (Financial Impact), ชื่อเสียง (Reputation Impact), ความปลอดภัยของผู้ป่วย/ลูกค้า, การไม่ปฏิบัติตามกฎหมาย, และ ผลกระทบทาง ESG
- กำหนดระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) และระดับความเสี่ยงที่องค์กรสามารถทนได้ (Risk Tolerance) ให้สอดคล้องกับลักษณะของความเสี่ยงแต่ละประเภท
- พิจารณาความเสี่ยงสะสมในระดับองค์กร (Risk Aggregation) และจัดลำดับความสำคัญของความเสี่ยง (Risk Prioritization) เพื่อจัดสรรทรัพยากรให้เหมาะสม

การตอบสนองต่อความเสี่ยง (Risk Response)

การตอบสนองต่อความเสี่ยงเป็นกระบวนการที่องค์กรกำหนดแนวทางปฏิบัติเพื่อลดหรือควบคุมผลกระทบของความเสี่ยงอย่างมีประสิทธิภาพ โดยบริษัทอาจเลือกแนวทางต่อไปนี้ได้อย่างหนึ่ง หรือบูรณาการแนวทาง โดยมีแนวทาง ดังนี้

- **การหลีกเลี่ยงความเสี่ยง (Avoidance):** หลีกเลี่ยงกิจกรรมหรือโครงการที่มีความเสี่ยงสูงโดยไม่จำเป็น
- **การลดความเสี่ยง (Mitigation):** พัฒนาแนวปฏิบัติหรือควบคุมภายในเพื่อลดโอกาสและผลกระทบของความเสี่ยง

- **การโอนความเสี่ยง (Transfer):** โอนภาระความเสี่ยงไปยังบุคคลที่สาม เช่น การทำประกัน หรือการทำสัญญา (Contractual Risk Transfer)
- **การยอมรับความเสี่ยง (Acceptance):** ยอมรับความเสี่ยงในระดับที่สามารถจัดการได้ภายใต้ความคุ้มค่าและทรัพยากรที่มีอยู่

การกำหนดแนวทางตอบสนองต่อความเสี่ยงต้องมีการวิเคราะห์ต้นทุน-ประโยชน์ (Cost-benefit Analysis) และมีแผนการติดตามผลที่ชัดเจน

การติดตาม ตรวจสอบ และรายงาน (Monitoring and Reporting)

บริษัทจัดให้มีกระบวนการติดตาม ตรวจสอบ และรายงานความเสี่ยงอย่างเป็นระบบ เพื่อให้มั่นใจว่าการจัดการความเสี่ยงยังคงมีประสิทธิภาพ ดังนี้

- ติดตามสถานะของความเสี่ยงและมาตรการควบคุมอย่างต่อเนื่อง โดยใช้ตัวชี้วัดความเสี่ยงหลัก (Key Risk Indicators: KRIs)
- รายงานผลการบริหารความเสี่ยงให้คณะกรรมการบริหารความเสี่ยงองค์กร และคณะกรรมการบริษัททราบอย่างน้อยปีละสองครั้ง หรือกรณีเกิดเหตุการณ์ความเสี่ยงรุนแรง
- ตรวจสอบภายในเป็นกลไกสำคัญในการตรวจประเมินความเหมาะสมและประสิทธิภาพของกระบวนการบริหารความเสี่ยง
- รายงานความเสี่ยงด้าน ESG และ Climate ในรูปแบบที่สอดคล้องกับแนวทาง IFRS S1/S2, TCFD, GRI และข้อกำหนดของตลาดหลักทรัพย์

การบริหารความเสี่ยงเชิงบูรณาการ (Enterprise-wide Risk Integration)

บริษัทตระหนักว่าการบริหารความเสี่ยงที่มีประสิทธิภาพต้องเกิดจากการเชื่อมโยงเข้ากับระบบงานและการตัดสินใจหลักขององค์กร โดยมีแนวทางดังนี้

- บูรณาการการบริหารความเสี่ยงเข้ากับ การวางแผนกลยุทธ์องค์กร (Strategic Planning) และ การจัดสรรงบประมาณ (Capital Allocation)
- กำหนดให้ความเสี่ยงเป็นองค์ประกอบสำคัญในการตัดสินใจลงทุน โครงการใหม่ การขยายธุรกิจ หรือการเปลี่ยนแปลงนโยบายสำคัญ
- ผสานการบริหารความเสี่ยงเข้ากับ ระบบควบคุมภายใน (Internal Control System) และ การบริหารจัดการประสิทธิภาพ (Performance Management)

- ส่งเสริมให้วัฒนธรรมองค์กรตระหนักรู้และรับผิดชอบต่อความเสี่ยงในทุกระดับ ผ่านการอบรม การสื่อสาร และการกำหนดบทบาทเจ้าของความเสี่ยง (Risk Ownership)
- สนับสนุนการใช้เทคโนโลยีดิจิทัลเพื่อการประเมินและติดตามความเสี่ยง เช่น ระบบ Dashboard, Risk Register, Real-time Alerts

การฝึกอบรม

บริษัท ศิครินทร์ จำกัด (มหาชน) ให้ความสำคัญกับการเสริมสร้างความรู้ ความเข้าใจ และทักษะที่จำเป็นในด้านการบริหารความเสี่ยงให้แก่บุคลากรทุกระดับขององค์กรอย่างต่อเนื่อง โดยมีเป้าหมายเพื่อส่งเสริมให้การบริหารความเสี่ยงเป็นส่วนหนึ่งของวัฒนธรรมองค์กรและการทำงานประจำวัน บริษัทดำเนินการจัดให้มีการอบรมเชิงลึก (In-depth Training) และการให้ความรู้ (Awareness) ด้านการบริหารความเสี่ยงอย่างสม่ำเสมอ โดยครอบคลุมหัวข้อที่เกี่ยวข้องกับความเสี่ยงในเชิงกลยุทธ์ การปฏิบัติงาน ESG และการเปลี่ยนแปลงสภาพภูมิอากาศ ตลอดจนประเด็นด้านกฎหมาย การเงิน เทคโนโลยี และความปลอดภัยในโลกไซเบอร์

นอกจากนี้ บริษัทจะจัดให้มีการประเมินประสิทธิภาพของการฝึกอบรมผ่านการสอบวัดผล การประเมินตนเอง หรือการติดตามผลจากการปฏิบัติงานจริง เพื่อให้มั่นใจว่าบุคลากรสามารถประยุกต์ใช้ความรู้ที่ได้รับในบริบทการทำงาน และสามารถจัดการกับความเสี่ยงในหน้าที่ของตนได้อย่างเหมาะสม โดยเฉพาะในบริบทของการให้บริการด้านสุขภาพที่ต้องอาศัยการตัดสินใจภายใต้ความเสี่ยงและภาวะไม่แน่นอน

การเปิดเผยข้อมูลและความโปร่งใส

บริษัท ศิครินทร์ จำกัด (มหาชน) มุ่งมั่นในการดำเนินงานภายใต้หลักความโปร่งใสและตรวจสอบได้ โดยมีการเปิดเผยข้อมูลด้านการบริหารความเสี่ยงให้แก่ผู้มีส่วนได้เสียทุกกลุ่มผ่านช่องทางที่เหมาะสมและตามระยะเวลาที่เหมาะสม บริษัทจะดำเนินการเปิดเผยข้อมูลเกี่ยวกับกรอบการบริหารความเสี่ยง ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) การประเมินผลการจัดการความเสี่ยง ประเด็นความเสี่ยงที่มีนัยสำคัญ ตลอดจนแนวโน้มของความเสี่ยงเกิดใหม่ ผ่านรายงานประจำปี รายงานความยั่งยืน รายงาน One Report และเว็บไซต์ของบริษัท

การทบทวนและปรับปรุงนโยบาย

บริษัท ศิครินทร์ จำกัด (มหาชน) กำหนดให้มีการทบทวนและปรับปรุงนโยบายการบริหารความเสี่ยงระดับองค์กรเป็นประจำอย่างน้อยปีละหนึ่งครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญทางด้านกฎหมาย สภาพแวดล้อมทางธุรกิจ สถานการณ์ความเสี่ยง หรือความคาดหวังของผู้มีส่วนได้เสีย การทบทวนดังกล่าวจะดำเนินการโดยคณะกรรมการบริหารความเสี่ยงองค์กรร่วมกับฝ่ายบริหาร และฝ่ายที่เกี่ยวข้อง โดยอยู่ภายใต้การกำกับดูแลของคณะกรรมการบริษัท เพื่อให้มั่นใจว่านโยบายยังคงมีความทันสมัย สอดคล้องกับแนวโน้มของโลกรธุรกิจและการกำกับดูแลกิจการที่ดี ทั้งในระดับประเทศและระดับสากล นอกจากนี้ บริษัทจะใช้ผลจากการประเมินความเสี่ยง การตรวจสอบภายใน และข้อเสนอแนะจากผู้มีส่วนได้เสีย รวมถึงข้อมูลจากรายงานแนวโน้มความเสี่ยง (Risk Trend) เป็นข้อมูลประกอบการปรับปรุงนโยบาย เพื่อให้มั่นใจว่านโยบายมีความครอบคลุม มีประสิทธิผล และสามารถตอบสนองต่อความท้าทายใหม่ ๆ ได้อย่างเหมาะสม

นโยบายและแนวปฏิบัติการบริหารจัดการความเสี่ยงองค์กรฉบับนี้ มีผลบังคับใช้ตั้งแต่วันที่ 16 มกราคม 2568 เป็นต้นไป โดยมติของคณะกรรมการบริษัทในการประชุม ครั้งที่ 1/2568 เมื่อวันที่ 15 มกราคม 2568



(นายเสนีย์ จิตตเกษม)

ประธานกรรมการ