



นโยบายและแนวปฏิบัติด้านการบริหารความเสี่ยง

หมายเหตุ: นโยบายฉบับนี้ได้รับการอนุมัติโดยคณะกรรมการบริษัท

โดยมีผลบังคับใช้ ตั้งแต่วันที่ 1 ตุลาคม 2567

1. ความสำคัญ

บริษัท ซีพี แอ็กซ์ตรา จำกัด (มหาชน) ตระหนักว่า สภาพแวดล้อมในการดำเนินธุรกิจมีความซับซ้อน และเปลี่ยนแปลงอย่างรวดเร็ว ซึ่งอาจส่งผลกระทบต่อความสามารถในการบรรลุวัตถุประสงค์และเป้าหมายทางธุรกิจ จึงให้ความสำคัญกับการบริหารความเสี่ยงทั่วทั้งองค์กร และบูรณาการวัฒนธรรมด้านความเสี่ยง ซึ่งประกอบด้วยวิธีการริเริ่มโดยผู้นำองค์กร (Tone from the top) การรับผิดชอบต่อความเสี่ยง (Accountability) การสื่อสารที่มีประสิทธิภาพ (Effective Communication) การสร้างแรงจูงใจและการบริหารทรัพยากรบุคคล (Incentives & HR Practices) ให้อยู่ในทุกกระบวนการทำงาน เพื่อลดผลกระทบและความเสียหายทั้งที่เป็นตัวเงินและไม่เป็นตัวเงินจากความไม่แน่นอนในการดำเนินธุรกิจ โดยมุ่งเน้นบริหารจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ เพื่อให้ทุกกระบวนการดำเนินงานเป็นไปด้วยความโปร่งใส มีประสิทธิภาพ เกิดภาพลักษณ์ที่ดี สร้างมูลค่าเพิ่มให้แก่องค์กรและผู้มีส่วนได้เสียทั้งในระยะสั้นและระยะยาว

บริษัท ซีพี แอ็กซ์ตรา จำกัด (มหาชน) จึงจัดทำนโยบายและแนวปฏิบัติฉบับนี้ขึ้นให้สอดคล้องตามกลยุทธ์และเป้าหมายของบริษัท ซีพี แอ็กซ์ตรา จำกัด (มหาชน) และแนวทางการตอบสนองความคาดหวังของผู้มีส่วนได้เสีย รวมทั้งกรอบการบริหารความเสี่ยงทั่วทั้งองค์กรของ The Committee of Sponsoring Organization of the Treadway Commission – Enterprise Risk Management Integrating with Strategy and Performance 2017 (COSO-ERM 2017) และมาตรฐานการบริหารความเสี่ยงสากล ISO 31000 Risk Management เพื่อให้เกิดการบริหารความเสี่ยงอย่างเป็นระบบ มีประสิทธิภาพ ทำให้การดำเนินธุรกิจเป็นไปอย่างต่อเนื่องและเติบโตได้อย่างยั่งยืน

2. ขอบเขตนโยบาย

นโยบายและแนวปฏิบัตินี้ใช้บังคับกับบริษัท ซีพี แอ็กซ์ตรา จำกัด (มหาชน) ต่อไปนี้เรียกว่า “บริษัทฯ” หมายถึง บริษัท ซีพี แอ็กซ์ตรา จำกัด (มหาชน) และบริษัทในเครือทุกบริษัทที่บริษัท ซีพี แอ็กซ์ตรา จำกัด (มหาชน) มีอำนาจบริหาร ซึ่ง “บริษัทฯ” ที่จะกล่าวถึงในเอกสารฉบับนี้ให้หมายถึง บริษัทหนึ่ง ๆ ที่นำเอาเอกสารฉบับนี้ไปบังคับใช้ ทั้งนี้จะมีการทบทวนนโยบายฉบับนี้อาจน้อยปีละหนึ่งครั้ง หรือกรณีมีเหตุอันสมควร

3. วัตถุประสงค์

- 3.1 เพื่อให้กรรมการ ผู้บริหาร และพนักงานมีแนวปฏิบัติในการบริหารความเสี่ยง และใช้เป็นส่วนหนึ่งของการตัดสินใจในการดำเนินงานให้เกิดเป็นวัฒนธรรมด้านความเสี่ยง
- 3.2 เพื่อให้เกิดระบบการบริหารความเสี่ยงที่มีประสิทธิภาพและเป็นแนวทางเดียวกันทั่วทั้งองค์กร
- 3.3 เพื่อให้ความเสี่ยงที่อยู่ในทุกกิจกรรมทางธุรกิจและกระบวนการทำงานได้รับการบริหารจัดการให้อยู่ในระดับที่ยอมรับได้

4. หน้าที่และความรับผิดชอบ

4.1 คณะกรรมการบริษัท

- 4.1.1 พิจารณานุมัตินโยบายและแนวปฏิบัติด้านการบริหารความเสี่ยง
- 4.1.2 พิจารณานุมัติระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) และกลยุทธ์การบริหารความเสี่ยง
- 4.1.3 กำกับดูแลการบริหารความเสี่ยงและความเพียงพอของการควบคุมภายใน รวมถึงให้เกิดการนำนโยบายไปปฏิบัติอย่างเป็นรูปธรรม

4.2 ผู้บริหาร

- 4.2.1 กำหนดข้อความแสดงความมุ่งมั่นในการยอมรับความเสี่ยง (Risk Appetite Statement) แผนการดำเนินงาน และตัวชี้วัดด้านการบริหารความเสี่ยงองค์กรที่สอดคล้องกับกลยุทธ์และวัตถุประสงค์ทางธุรกิจ
- 4.2.2 กำหนดเกณฑ์การประเมินความเสี่ยง (Risk Assessment Criteria) และระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) ให้เหมาะสมกับบริบททางธุรกิจ
- 4.2.3 กำหนดโครงสร้าง บทบาทหน้าที่และความรับผิดชอบด้านการบริหารความเสี่ยงพร้อมทั้งจัดให้มีระบบบริหารความเสี่ยงและการควบคุมภายใน
- 4.2.4 บริหารจัดการความเสี่ยงในการดำเนินงานให้อยู่ในระดับที่ยอมรับได้ โดยคำนึงถึงการบรรลุเป้าหมายขององค์กร ต้นทุนและผลตอบแทนทางธุรกิจ รวมถึงชื่อเสียงและภาพลักษณ์องค์กร
- 4.2.5 บริหารจัดการเหตุการณ์ในภาวะวิกฤต เพื่อลดผลกระทบและให้ธุรกิจกลับสู่ภาวะปกติ
- 4.2.6 ส่งเสริมให้เกิดวัฒนธรรมองค์กรที่ให้ความสำคัญกับการบริหารความเสี่ยงทั่วทั้งองค์กร
- 4.2.7 ติดตามดูแล บริหารจัดการ และสนับสนุนให้มีการปฏิบัติตามนโยบายและแนวปฏิบัติ
- 4.2.8 ติดตามปัจจัยสภาพแวดล้อมที่เปลี่ยนแปลงไป แนวโน้มที่จะทำให้แผนงานไม่บรรลุผลสำเร็จ หรือกรณีเกิดเหตุการณ์ความเสี่ยงที่เกิดขึ้น และนำข้อมูลที่ได้รับมาปรับปรุงแผนงานเป็นระยะ
- 4.2.9 สื่อสารนโยบายและแนวปฏิบัติเพื่อสร้างการตระหนักรู้ให้กับผู้บริหารและพนักงานทุกระดับ
- 4.2.10 สนับสนุนทรัพยากรและส่งเสริมให้เกิดความร่วมมือในการบริหารความเสี่ยงที่มีประสิทธิภาพทั่วทั้งองค์กร
- 4.2.11 รายงานผลการดำเนินงานด้านการบริหารความเสี่ยงต่อคณะกรรมการที่รับผิดชอบ

4.3 ฝ่ายบริหารความเสี่ยง

- 4.3.1 พัฒนาเครื่องมือและขั้นตอนการปฏิบัติการบริหารความเสี่ยง เพื่อให้เจ้าของความเสี่ยง (Risk Owner) สามารถระบุ ประเมิน ติดตาม และรายงานความเสี่ยงในรูปแบบเดียวกันทั่วทั้งองค์กร
- 4.3.2 จัดให้มีการประเมินความเสี่ยงและการบริหารความเสี่ยงในทุกกิจกรรมทางธุรกิจที่อาจจะกระทบกับแผนการจัดการขององค์กร
- 4.3.3 จัดทำแผนบริหารความเสี่ยงองค์กร กระบวนการบริหารความเสี่ยงและการควบคุมภายในที่มีประสิทธิภาพให้สอดคล้องกับนโยบาย วัตถุประสงค์ กลยุทธ์ และบริบทขององค์กร รวมถึงการจัดการความต่อเนื่องของธุรกิจในทุกกิจกรรมทางธุรกิจ และกระบวนการทำงาน
- 4.3.4 ทบทวนทะเบียนความเสี่ยง (Risk Profile) และประสิทธิผลของการจัดการ รวมทั้งปรับปรุงแผนการดำเนินงานด้านการบริหารความเสี่ยงให้สอดคล้องกับสภาพแวดล้อมที่เปลี่ยนแปลงหรือมีแนวโน้มที่แผนงานจะไม่บรรลุผลสำเร็จ
- 4.3.5 ติดตามและประเมินผลการบริหารความเสี่ยงองค์กร รวมทั้งประสานงานกับเจ้าของความเสี่ยงเพื่อติดตามการบริหารความเสี่ยง
- 4.3.6 สื่อสารข้อมูลเกี่ยวกับผลการประเมินความเสี่ยง เพื่อให้หน่วยงานตรวจสอบภายในใช้ในการตรวจสอบประสิทธิผล ความเหมาะสม และความเพียงพอของการควบคุมภายใน
- 4.3.7 จัดทำรายงานผลการดำเนินงานด้านการบริหารความเสี่ยงต่อผู้บริหารและคณะกรรมการที่รับผิดชอบ

- 4.3.8 สร้างความตระหนักรู้ ความเข้าใจ และพัฒนาทักษะความสามารถในการบริหารความเสี่ยง รวมทั้งให้คำแนะนำด้านการบริหารความเสี่ยงแก่บุคลากร
- 4.3.9 ปลุกฝังวัฒนธรรมองค์กรที่ให้ความสำคัญกับการบริหารความเสี่ยงทั่วทั้งองค์กร

4.4 เจ้าของความเสี่ยง

- 4.4.1 ระบุ วิเคราะห์ ประเมิน วางแผนและกำหนดมาตรการการบริหารความเสี่ยงในส่วนงานที่รับผิดชอบ
- 4.4.2 ทบทวนความเสี่ยงใหม่ที่เกิดขึ้นในกระบวนการปฏิบัติงาน และวางแผนเพื่อลดความเสี่ยง
- 4.4.3 ดำเนินการ ติดตาม ควบคุมและดูแลความเสี่ยงให้เป็นไปตามแผนการบริหารความเสี่ยงและให้ทันต่อเหตุการณ์
- 4.4.4 รายงานสถานะของความเสี่ยงและความคืบหน้าของการบริหารความเสี่ยง

4.5 พนักงาน

- 4.5.1 เรียนรู้ ทำความเข้าใจและปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ มาตรฐานที่เกี่ยวข้อง และนโยบายและแนวปฏิบัติ
- 4.5.2 ดำเนินการและรายงานความเสี่ยงที่อาจส่งผลกระทบต่อการทำงานที่หรือเหตุการณ์ที่เกิดขึ้นในการบริหารความเสี่ยงให้กับผู้บังคับบัญชา

5. แนวปฏิบัติ

- 5.1 ระบุและวิเคราะห์ความเสี่ยง (Risk Identification) ที่จะกระทบต่อการบรรลุวัตถุประสงค์ขององค์กร โดยพิจารณาสภาพแวดล้อมทางธุรกิจให้ครอบคลุมทุกปัจจัยทั้งความเสี่ยงที่เคยเกิดขึ้น ความเสี่ยงปัจจุบันและความเสี่ยงใหม่ ๆ (Emerging Risks) ที่อาจจะเกิดขึ้น
- 5.2 ประเมินและจัดลำดับความเสี่ยง (Risk Prioritization) ตามบริบทธุรกิจให้ครอบคลุมความเสี่ยงองค์กร อาทิ ความเสี่ยงด้านกลยุทธ์ (Strategic Risks) ความเสี่ยงด้านการดำเนินงาน (Operational Risks) ความเสี่ยงด้านการบริหารจัดการทางการเงิน (Financial Risks) ความเสี่ยงด้านการปฏิบัติตามกฎหมายและระเบียบ (Compliance Risks) ความเสี่ยงด้านชื่อเสียง (Reputation Risks) ความเสี่ยงด้านสิ่งแวดล้อม (Environmental Risks) ความเสี่ยงด้านเศรษฐกิจ (Economic Risks) ความเสี่ยงด้านสังคม (Social Risks)
- 5.3 จัดทำแผนกลยุทธ์การบริหารความเสี่ยงองค์กรที่เชื่อมโยงกับวิสัยทัศน์ พันธกิจ วัตถุประสงค์ และระดับความเสี่ยงที่ยอมรับได้
- 5.4 กำหนดมาตรการ และแผนการจัดการความเสี่ยง (Risk Treatment) ที่ช่วยลดผลกระทบและ/หรือโอกาสที่จะเกิดเหตุการณ์ความเสี่ยงให้อยู่ในระดับที่ยอมรับได้
- 5.5 กำหนดแผนการจัดการเหตุการณ์ที่ไม่เป็นไปตามแผนจัดการความเสี่ยง (Incident Management) ให้การดำเนินงานสามารถกลับคืนสู่สภาวะปกติโดยเร็วที่สุด
- 5.6 นำระบบเทคโนโลยีสารสนเทศมาใช้ในการบริหารความเสี่ยง โดยใช้ข้อมูลที่ชัดเจน (Clearly) ทันสมัย (Timely) เกี่ยวข้อง (Relevant) และที่พร้อมใช้ (Available Information) มาวิเคราะห์เพื่อประกอบการตัดสินใจ
- 5.7 สื่อสารข้อมูลและแนวทางการบริหารความเสี่ยงผ่านช่องทางต่าง ๆ ทั่วทั้งองค์กร โดยคำนึงถึงกฎหมาย ระเบียบที่เกี่ยวข้อง และมาตรฐานความมั่นคงปลอดภัยของข้อมูล

- 5.8 ทบทวนความเสี่ยง และติดตามดูแลการดำเนินงานและกระบวนการบริหารความเสี่ยงอย่างสม่ำเสมอ หรือกรณีที่มีการเปลี่ยนแปลงของสภาพแวดล้อมทางธุรกิจที่สำคัญ
- 5.9 จัดให้มีการทดสอบความสามารถในการรับภาวะวิกฤต (Stress Test) เป็นประจำ หรือเมื่อมีการเปลี่ยนแปลงจากปัจจัยเสี่ยงที่มีนัยสำคัญ
- 5.10 รายงานผลการประเมินความเสี่ยง ประสิทธิภาพของมาตรการจัดการและผลการดำเนินงานด้านการบริหารความเสี่ยง
- 5.11 ทบทวนและปรับปรุงการบริหารความเสี่ยงองค์กรให้สอดคล้องกับสภาพแวดล้อมในการดำเนินงานและมีประสิทธิภาพ

6. การฝึกอบรม

จัดให้มีการสื่อสารและถ่ายทอดนโยบายและแนวปฏิบัติด้านการบริหารความเสี่ยงผ่านการฝึกอบรม การประชุม หรือกิจกรรมในรูปแบบต่าง ๆ ที่เหมาะสม ให้แก่ผู้ที่เกี่ยวข้อง

7. การขอคำแนะนำ

ในกรณีที่มิข้อสงสัยว่าการกระทำนั้นอาจฝ่าฝืนนโยบายและแนวปฏิบัติด้านการบริหารความเสี่ยง สามารถขอคำแนะนำจากผู้บังคับบัญชา หน่วยงานหรือบุคคลผู้รับผิดชอบด้านการบริหารความเสี่ยง ด้านกำกับปฏิบัติตามกฎเกณฑ์ ด้านการตรวจสอบภายใน หรือด้านกฎหมายก่อนตัดสินใจหรือดำเนินการใด ๆ

8. กฎหมาย กฎระเบียบและนโยบายที่เกี่ยวข้อง

- 8.1 คู่มือการบริหารความเสี่ยงทั่วทั้งองค์กรของบริษัท ซีพี แอ็กซ์ตรา จำกัด (มหาชน)
- 8.2 COSO (Committee of Sponsoring Organization of the Treadway Commission) Enterprise Risk Management Framework 2017
- 8.3 ISO 31000: 2018 Enterprise Risk Management Guidelines

9. ภาคผนวก

นโยบายและแนวปฏิบัตินี้ ประกอบด้วยภาคผนวก ดังต่อไปนี้

- 9.1 ภาคผนวก ก คำนิยาม

ภาคผนวก ก

คำนิยาม

1. กลยุทธ์

วิธีทางหรือแนวทางที่กำหนดขึ้นเพื่อนำไปสู่เป้าหมายองค์กร ซึ่งต้องกำหนดให้สอดคล้องกับพันธกิจและวิสัยทัศน์ รวมถึงสอดคล้องกับค่านิยมหลักและความเสี่ยงที่ยอมรับได้ การกำหนดกลยุทธ์ที่ชัดเจนจะทำให้เกิดการบริหารงาน และวางแผนการใช้ทรัพยากรอย่างมีประสิทธิภาพ นำไปสู่การตัดสินใจที่เหมาะสม

2. การควบคุมภายใน (Internal Control)

กระบวนการหรือขั้นตอนการทำงานที่กำหนดขึ้นโดยคณะกรรมการ ผู้บริหาร หรือพนักงานขององค์กร เพื่อดำเนินการควบคุมความเสี่ยง ให้เกิดความมั่นใจได้ว่า องค์กรจะสามารถบรรลุวัตถุประสงค์หลักที่เกี่ยวกับกลยุทธ์ องค์กร การดำเนินงาน การรายงานทางการเงิน และการปฏิบัติตามกฎหมาย

3. การบริหารเหตุการณ์ที่ไม่เป็นไปตามแผนบริหารความเสี่ยง (Incident management)

การบริหารเหตุการณ์ที่เกิดขึ้นเนื่องจากการบริหารความเสี่ยงไม่เป็นไปตามที่กำหนดไว้ เพื่อลดผลกระทบและแก้ไขเหตุการณ์ที่เกิดขึ้นให้การดำเนินงานกลับมาสู่ภาวะปกติโดยเร็วที่สุด รวมทั้งจัดทำมาตรการป้องกันไม่ให้เกิดขึ้นอีกในอนาคต

4. การบริหารความเสี่ยง

กระบวนการดำเนินงานขององค์กรที่เป็นระบบและต่อเนื่อง เพื่อช่วยให้องค์กรลดสาเหตุของโอกาสที่จะเกิดความเสียหาย โดยให้ระดับและขนาดของความเสียหายที่จะเกิดขึ้นอยู่ในระดับที่องค์กรยอมรับได้ ประเมินได้ ควบคุมได้ และตรวจสอบได้อย่างมีระบบ โดยคำนึงถึงการบรรลุวัตถุประสงค์หรือเป้าหมายขององค์กรเป็นสำคัญ

5. การตอบสนองความเสี่ยง

การพิจารณาเลือกวิธีการที่ควรกระทำเพื่อลดความเสี่ยงที่อาจเกิดขึ้นตามผลการประเมินความเสี่ยง ซึ่งพิจารณาจากโอกาสและผลกระทบ โดยเปรียบเทียบระดับความเสี่ยงที่เกิดขึ้นกับระดับความเสี่ยงที่ยอมรับได้ และความคุ้มค่าในการบริหารความเสี่ยงที่เหลืออยู่

6. การทดสอบความสามารถในการรับภาวะวิกฤต

การทดสอบความสามารถขององค์กรในการรับมือกับเหตุการณ์ภาวะวิกฤตหรือความท้าทายในรูปแบบต่าง ๆ ที่อาจเกิดขึ้นภายใต้สถานการณ์จำลอง (Scenario) หรือเงื่อนไขตามแบบจำลอง

7. เกณฑ์การประเมินความเสี่ยง (Risk Assessment Criteria)

ขอบเขต เงื่อนไข ทั้งในเชิงปริมาณ เชิงคุณภาพ ที่กำหนดไว้ใช้อ้างอิง ประเมินความสำคัญ และระดับความเสี่ยงขององค์กร โดยพิจารณาจากระดับของโอกาส และผลกระทบของความเสี่ยง เกณฑ์การประเมินความเสี่ยงจะสะท้อนถึง

ค่านิยม นโยบาย วัตถุประสงค์ มุมมองของผู้มีส่วนได้เสีย รวมทั้งมาตรฐาน กฎหมาย นโยบาย และข้อกำหนดอื่น ๆ ทั้งภายในและภายนอกองค์กร

8. ข้อความแสดงความมุ่งมั่นในการยอมรับความเสี่ยง (Risk Appetite Statement: RAS)

ข้อความที่แสดงถึงความมุ่งมั่นขององค์กร ในการยอมรับหรือไม่ยอมรับความเสี่ยงใด ๆ เพื่อให้บุคลากรในองค์กร เข้าใจและตระหนักถึงความสำคัญและหน้าที่ความรับผิดชอบเกี่ยวกับความเสี่ยง ทำให้สามารถบรรลุวัตถุประสงค์และ เป้าหมายธุรกิจ และปลูกฝังวัฒนธรรมการด้านความเสี่ยงในองค์กร

9. ความเสี่ยง

ผลกระทบเชิงลบที่เกิดจากเหตุการณ์ไม่แน่นอนต่อการบรรลุวัตถุประสงค์ และเป้าหมายขององค์กร ทั้งที่เป็นตัวเงิน และไม่เป็นตัวเงิน

10. ความเสี่ยงใหม่ (Emerging Risks)

ความเสี่ยงที่เกิดขึ้นใหม่ หรือไม่เคยมีมาก่อน หรือเหตุการณ์ยังไม่ได้รับการพิจารณาความเสี่ยง ซึ่งอาจก่อให้เกิด ความเสียหายต่อการดำเนินงาน และความต่อเนื่องทางธุรกิจ โดยความเสี่ยงใหม่อาจเกี่ยวข้องกับกิจกรรมต่าง ๆ เช่น กระบวนการใหม่ เทคโนโลยีใหม่ สถานที่ทำงานรูปแบบใหม่ หรือการเปลี่ยนแปลงทางเศรษฐกิจ สังคม สิ่งแวดล้อม หรือการเปลี่ยนแปลงต่าง ๆ ในองค์กร

11. เจ้าของความเสี่ยง (Risk Owner)

บุคคล หรือหน่วยงาน ที่มีความรับผิดชอบและมีอำนาจในการจัดการความเสี่ยง ตั้งแต่การระบุ ประเมิน และวางแผน จัดการความเสี่ยง รวมถึงดูแลให้มีการดำเนินการตามมาตรการจัดการความเสี่ยงที่เกี่ยวข้อง

12. มาตรการจัดการความเสี่ยง (Risk Management / Mitigation / Control Measure)

มาตรการ หรือแนวทางที่องค์กรกำหนด และดำเนินการในการตอบสนองต่อความเสี่ยง ซึ่งอาจใช้แนวทางต่างๆ ตามที่ได้พิจารณา และอนุมัติให้ดำเนินการ

13. ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite)

ระดับของความเสี่ยงที่องค์กรตัดสินใจยอมรับ โดยยังคงความสามารถในการบรรลุวัตถุประสงค์ และเป้าหมายของ องค์กร รวมถึงกฎหมาย ระเบียบ และมาตรฐานที่เกี่ยวข้อง