



นโยบายการบริหารความเสี่ยง Risk Management Policy

บริษัทได้มีการทบทวนนโยบายการบริหารความเสี่ยงของบริษัทให้สอดคล้องและเป็นไปในแนวทางเดียวกับ หลักการกำกับกิจการที่ดี สำหรับบริษัทจดทะเบียน CG Code 2560 ซึ่งคณะกรรมการบริษัท มิตรสิบลิสซิ่ง จำกัด (มหาชน) ในการประชุมเมื่อวันที่ 24 กุมภาพันธ์ 2569 ได้มีมติอนุมัติทบทวนนโยบายดังกล่าว

	สารบัญ	หน้า
1.	หลักการและเหตุผล	- 5 -
2.	ขอบเขต/แนวทางของนโยบาย	- 5 -
3.	ขอบเขตการกำกับดูแลความเสี่ยง	- 6 -
4.	การบริหารความเสี่ยง	- 6 -
5.	แผนการจัดการความเสี่ยง (Risk Management Plan)	- 8 -
6.	บันทึกคุณภาพ	- 9 -

วันที่ 3 พฤศจิกายน 2568

นโยบายการบริหารความเสี่ยง (Risk Management Policy)

1. หลักการและเหตุผล

บริษัท มิตรลิบ ลิสซิ่ง จำกัด (มหาชน) และบริษัทในเครือ (“บริษัท”) มีความมุ่งมั่นตลอดมาที่จะประกอบธุรกิจภายใต้หลักธรรมาภิบาลที่ดี ด้วยความรับผิดชอบต่อสังคม บริษัทจึงให้ความสำคัญกับการบริหารความเสี่ยง นโยบายฉบับนี้จัดทำขึ้นโดยมีวัตถุประสงค์เพื่อการบริหารความเสี่ยง นับเป็นเครื่องมือสำคัญและมีประโยชน์ในการบริหารจัดการองค์กรให้สามารถบรรลุ เป้าหมายและวัตถุประสงค์ตามที่กำหนดไว้ได้อย่างมีประสิทธิภาพประสิทธิผล ช่วยสร้างคุณค่า รักษาคุณค่า และทำให้เกิด คุณค่าที่แท้จริงขององค์กร ด้วยการบริหารจัดการปัจจัยและความคุมกิจกรรมทั้งกระบวนการดำเนินงานต่าง ๆ โดยลดมูลเหตุของแต่ ละโอกาสที่ก่อให้เกิดผลกระทบ ทั้งนี้ เพื่อให้ระดับและขนาดของผลกระทบที่จะเกิดขึ้นกับองค์กรในอนาคตอยู่ในระดับที่ ยอมรับได้ หรือควบคุมได้อย่างเป็นระบบทั่วทั้งองค์กร

2. ขอบเขต/แนวทางของนโยบาย

นโยบายฉบับนี้มีขอบเขตครอบคลุมถึงการปฏิบัติและการดำเนินงานของผู้บริหาร และพนักงานทุกคนในบริษัทได้เข้าใจเรื่องการบริหารความเสี่ยงที่สำคัญขององค์กร เพื่อตอบสนองความเสี่ยงที่จะเกิดขึ้นได้ทันต่อเหตุการณ์

โครงสร้างขององค์กรปัจจุบัน ประกอบด้วย คณะกรรมการบริหารความเสี่ยงซึ่งแต่งตั้งจากกรรมการบริษัท อย่างน้อย 3 คนโดยมีกรรมการอิสระ 1 คน

คณะกรรมการบริหารความเสี่ยง มีหน้าที่กำหนดนโยบาย และกรอบการดำเนินงาน, การบริหารความเสี่ยงของ บริษัท จัดให้บริษัทมีระบบบริหารความเสี่ยงทุกด้านครอบคลุมปัจจัยความเสี่ยงที่เกี่ยวข้องกับวิสัยทัศน์, เป้าหมาย, กลยุทธ์ทางธุรกิจ, การเงิน และการปฏิบัติการด้านอื่น ๆ พิจารณาถึงโอกาสที่จะเกิด และ ระดับความรุนแรงของผลกระทบ, กำหนดมาตรการในการป้องกัน, แก้ไขและผู้รับผิดชอบที่ชัดเจนรวมทั้งกำหนดมาตรการ ในการรายงานและการติดตามประเมินผล

คณะกรรมการบริหารความเสี่ยง กำหนดขอบเขตความเสี่ยงที่ยอมรับได้ของบริษัท (Risk Appetite) และมีตัวชี้วัดความเสี่ยงสำคัญ (Key Risk Indicator: KRI) เพื่อเป็นแนวทางในการบริหารธุรกิจ และมีการประสานเชื่อมโยงระบบการบริหารความเสี่ยงกับกระบวนการวางแผนกลยุทธ์ขององค์กร โดยกำหนดให้ผู้รับผิดชอบบริหารความเสี่ยง รายงานตรงกับสำนักงานประธานเจ้าหน้าที่บริหาร ที่รับผิดชอบงานวางแผนกลยุทธ์องค์กรและแผนงานธุรกิจ ทำหน้าที่ประสานงาน ติดตามความคืบหน้าของแผนปฏิบัติการในการควบคุมความเสี่ยงอย่างต่อเนื่อง ทำให้มั่นใจ

ได้ ว่าการบริหารความเสี่ยงสามารถบรรลุวัตถุประสงค์และเป้าหมายเชิงกลยุทธ์ตามที่กำหนดไว้

3. ขอบเขตการกำกับดูแลความเสี่ยง

กลุ่มบริษัทส่งเสริมให้พนักงานทั่วทั้งองค์กรได้รับรู้ และป้องกันความเสี่ยงที่จะเกิดขึ้นทั้งหมดตรวจสอบ ติดตาม และประเมินความเสี่ยงที่อาจเกิดขึ้นตามสภาพแวดล้อมที่เปลี่ยนแปลง ทั้งเหตุปัจจัยภายในและภายนอก องค์กร เพื่อให้พนักงานทุกคนมีความเข้าใจในการบริหารความเสี่ยง กลุ่มบริษัทได้กำหนดกรอบนโยบายในการบริหารความเสี่ยง ไว้ดังนี้

1. คณะกรรมการบริษัทมีหน้าที่ในการกำกับดูแลการบริหารความเสี่ยงของกลุ่มบริษัทเป็นไปด้วยความเหมาะสม และส่งเสริมให้พนักงานทุกคนมีส่วนร่วมในการบริหารความเสี่ยง จนกลายเป็นส่วนหนึ่งของวัฒนธรรมองค์กร
2. คณะกรรมการตรวจสอบช่วยสนับสนุนคณะกรรมการบริษัทในการปฏิบัติหน้าที่ในการสอบทาน ให้กลุ่มบริษัทมีระบบการควบคุมภายในที่ดีมีประสิทธิภาพ และติดตามการบริหารความเสี่ยง ของกลุ่มบริษัท
3. คณะกรรมการบริหารความเสี่ยงมีหน้าที่ในการจัดทำแผนบริหารความเสี่ยงที่มีประสิทธิผล ที่ทำให้ความเสี่ยงอยู่ในระดับที่ยอมรับได้ โดยใช้ การบริหารความเสี่ยงตามแนวทาง COSO ERM 2017

4. การบริหารความเสี่ยง

กลุ่มบริษัทตระหนักถึงความสำคัญของการบริหารความเสี่ยงและการควบคุมความเสี่ยงอย่างเป็นระบบ และมีประสิทธิภาพ, บริษัทกำหนดแผนงานการบริหารความเสี่ยงขององค์กรอย่างเหมาะสม โดยกลุ่มบริษัทพิจารณานำเอาระบบบริหารความเสี่ยงในองค์กร (Enterprise Risk Management: ERM) เป็นเครื่องมือการบริหารจัดการองค์กรเพื่อบ่งชี้เหตุการณ์ความเสี่ยง, ประเมินความเสี่ยง, จัดลำดับความสำคัญ และจัดการความเสี่ยง และการรายงาน ผลของความเสี่ยงประเภทต่างๆ ได้แก่

- 1) **ความเสี่ยงด้านกลยุทธ์(Strategic Risk)** หมายถึง ความเสี่ยงที่เกิดจากการกำหนดและการนำแผนกลยุทธ์ที่ไม่เหมาะสม หรือไม่สอดคล้องกับปัจจัยภายในและภายนอก ส่งผลกระทบต่อรายได้ ชื่อเสียง หรือการดำรงอยู่ขององค์กร เช่น การเปลี่ยนแปลงนโยบาย, ความต้องการของลูกค้าที่เปลี่ยนแปลงไป เป็นต้น
- 2) **ความเสี่ยงทางการเงิน(Financial Risk)** หมายถึง ความเสี่ยงที่เกิดจากการสูญเสียทางการเงิน ซึ่งอาจเกิดจากปัจจัยภายนอกหรือภายในกิจการ เช่น การเปลี่ยนแปลงของตลาด, สภาพคล่องที่ลดลง หรือ การผิดนัดชำระหนี้ของลูกค้า เป็นต้น

- 3) ความเสี่ยงด้านการกำกับกฎระเบียบข้อบังคับ(Compliance Risk) หมายถึง ความเสี่ยงที่เกิดจากการไม่สามารถปฏิบัติตามกฎหมาย กฎระเบียบ หรือข้อบังคับต่าง ๆ ได้อย่างถูกต้องและทันเวลา
- 4) ความเสี่ยงด้านการดำเนินงาน(Operation Risk) หมายถึง ความเสี่ยงที่เกิดขึ้นจากกระบวนการทำงาน, เทคโนโลยี, บุคลากร หรือเหตุการณ์ภายนอก ที่อาจส่งผลกระทบต่อการบรรลุวัตถุประสงค์ขององค์กรในด้านการปฏิบัติงาน
- 5) ความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ (IT Risk) หมายถึง ความเสี่ยงของผลลัพธ์ที่ไม่พึงประสงค์ ความเสียหาย การสูญเสีย หรือความล้มเหลวที่อาจเกิดขึ้นจากการใช้ฮาร์ดแวร์, ซอฟต์แวร์, แอปพลิเคชัน, เครือข่าย หรือ ระบบสารสนเทศโดยรวม
- 6) ความเสี่ยงด้านความเสี่ยงด้านไซเบอร์ (Cyber Risk) หมายถึง ความเสี่ยงที่เกิดจากการโจมตีทางไซเบอร์ เช่น มัลแวร์, ฟิชซิง หรือภัยคุกคามจากภายใน ซึ่งจะนำไปสู่ความเสียหายต่อ ข้อมูล ระบบ หรือทรัพย์สินทางเทคโนโลยีสารสนเทศ ทำให้องค์กรเกิดความสูญเสียทางการเงิน การหยุดชะงักของธุรกิจ หรือความเสียหายต่อชื่อเสียง
- 7) ความเสี่ยงด้านการทุจริตคอร์รัปชัน (Corruption Risk) หมายถึง ความเสี่ยงที่เกิดจากการใช้อำนาจสาธารณะที่มีขอบเพื่อผลประโยชน์ส่วนตัว หรือการให้สินบน และความประพฤติทั้งหลายของบุคคลซึ่งได้รับมอบหมายหน้าที่และความรับผิดชอบในภาครัฐหรือเอกชนประพฤตินี้ฝ่าฝืนหน้าที่ของตน โดยไม่สมควรกับตำแหน่งหน้าที่ของตนในฐานะเจ้าพนักงานแห่งรัฐ เจ้าหน้าที่ในหน่วยงานเอกชน ตัวแทนหรือฐานะความสัมพันธ์อื่นๆ โดยมีมุ่งประสงค์ให้ได้รับประโยชน์ใดๆ โดยมีขอบสำหรับตนเองหรือผู้อื่น
- 8) ความเสี่ยงที่เกิดขึ้นใหม่ (Emerging risk) หมายถึง ความเสี่ยงที่เกี่ยวข้องกับประเด็น ESG ที่เกิดขึ้นใหม่ ซึ่งความเสี่ยงดังกล่าวอาจส่งผลกระทบต่อการทำงานของบริษัทในระยะยาว และบางกรณีอาจเกิดผลกระทบต่อบริษัทแล้ว
- 9) ความเสี่ยงด้านความยั่งยืน (ESG Risk) คือ ความเสี่ยงที่เกี่ยวข้องกับการดำเนินงานขององค์กรใน 3 มิติหลักของ ESG คือ สิ่งแวดล้อม (Environmental), สังคม (Social), และธรรมาภิบาล (Governance) ซึ่งความเสี่ยงเหล่านี้ อาจส่งผลกระทบต่อความสามารถในการทำกำไร ภาพลักษณ์ ชื่อเสียง ความน่าเชื่อถือ และความอยู่รอดขององค์กรในระยะยาว ทำให้องค์กรต้องบริหารจัดการความเสี่ยงเหล่านี้เพื่อสร้าง โอกาสและความยั่งยืน

5. แผนการจัดการความเสี่ยง (Risk Management Plan)

กลุ่มบริษัทได้กำหนดให้ทุกสาขางาน วิเคราะห์หาสาเหตุและผลกระทบของความเสี่ยง และประเมินมาตรการจัดการความเสี่ยง โดยพิจารณาถึงความเสี่ยงที่ยอมรับได้และต้นทุนที่เกิดขึ้นเพื่อพิจารณาเปรียบเทียบกับประโยชน์ที่จะได้รับ โดยพิจารณาทางเลือกในการตอบสนองความเสี่ยง(Risk Response) มี 5 วิธี ดังนี้

- 1) **การยอมรับความเสี่ยง (Risk Acceptance)** เป็นการยอมรับความเสี่ยงที่เกิดขึ้น เนื่องจากความเสี่ยงนั้นสามารถยอมรับได้ภายใต้การควบคุมที่มีอยู่ในปัจจุบัน ซึ่งไม่ต้องดำเนินการใดๆ กรณีนี้ใช้กับความเสี่ยงที่มีน้อย มีต้นทุนในการบริหารความเสี่ยงสูง
- 2) **การลดความเสี่ยง (Risk Reduction) หรือ การควบคุมความเสี่ยง (Risk Control)** เป็นการปรับปรุงระบบการทำงานหรือการออกแบบวิธีการใหม่เพื่อลดโอกาสที่จะเกิด หรือลดผลกระทบให้อยู่ในระดับที่องค์กรยอมรับได้
- 3) **การโอนความเสี่ยง (Risk sharing)** เป็นการกระจายหรือถ่ายโอนความเสี่ยงให้ผู้อื่นช่วยแบ่งความรับผิดชอบ เช่น การจ้างบุคคลภายนอกให้กระทำการแทน
- 4) **การหลีกเลี่ยงความเสี่ยง (Risk Avoidance)** เป็นการหลีกเลี่ยงเหตุการณ์ที่ก่อให้เกิดความเสี่ยง เป็นการจัดการความเสี่ยงที่อยู่ในระดับสูงมากและบริษัทไม่อาจยอมรับได้ จึงต้องตัดสินใจยกเลิกกิจกรรมนั้น หรือเปลี่ยนวัตถุประสงค์, เปลี่ยนแปลงกิจกรรม, การปรับเปลี่ยนรูปแบบการทำงาน, การลดขนาดของกิจกรรม หรือเลือกกิจกรรมที่สามารถยอมรับได้มากกว่า
- 5) **การติดตามความเสี่ยง (Risk Pursuance)** เป็นการดำเนินการตามความเสี่ยง" หรือ "การจัดการกับความเสียหาย" ที่เป็นส่วนหนึ่งของกระบวนการบริหารความเสี่ยง โดยครอบคลุมตั้งแต่การระบุ การประเมิน และการวางแผนการตอบสนองต่อความเสี่ยงนั้นๆ