AIRA Asset Management Company Limited 319 Chamchuri Square Building, 12th Floor, Phayathai Road, Pathumwan, Bangkok 10330
บริษัทหลักทรัพย์จัดการกองทุน ไอร่า จำกัด เลขที่ 319 อาคารจัตุรัสจามจุรี ชั้น 12 ถนนพญาไท แขวงปทุมวัน เขตปทุมวัน กรุงเทพมหานคร 10330
Tel. 0-2038-4499 ทะเบียนเลขที่ 0105560035008

นโยบายการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ

(IT Risk Management Policy)

ฉบับทบทวนปี 2568

สารบัญ

หน้า

เรื่อง นโยบายการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ (IT Risk Management Policy) ฉบับทบทวนปี 2568

บริษัทตระหนักถึงความสำคัญของการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ (IT Risk Management) อันอาจเกิดขึ้นจากปัจจัยภายในและภายนอกบริษัท ซึ่งอาจทำให้บริษัทไม่สามารถบรรลุเป้าหมายหรือวัตถุประสงค์ที่วางไว้ได้

ทั้งนี้ เพื่อให้บริษัท หลักทรัพย์จัดการกองทุน ไอร่า จำกัด มีการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศที่มีประสิทธิภาพ โดยสามารถระบุแนวทางในการจัดการความเสี่ยงให้อยู่ในระดับที่เหมาะสมหรือยอมรับได้ บริษัทจึงจัดทำนโยบายการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศเพื่อให้พนักงานและผู้บริหารทุกระดับที่เกี่ยวข้องได้รับทราบและนำไปปฏิบัติอย่างเคร่งครัด โดยที่ประชุมคณะกรรมการบริษัท ครั้งที่ 3/2568 เมื่อวันที่ 4 สิงหาคม 2568 ได้มีมติอนุมัตินโยบายการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ (IT Risk Management Policy)

อนึ่งผู้บังคับบัญชามีหน้าที่ติดตามและแนะนำผู้ใต้บังคับบัญชาตามลำดับชั้น ในการปฏิบัติงานให้สอดคล้องกับนโยบาย ขั้นตอน และวิธีการปฏิบัติที่กำหนดไว้ในนโยบายการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศฉบับนี้อย่างสม่ำเสมอ

คณะกรรมการบริษัท

1. วัตถุประสงค์และแนวทางการดำเนินการ

1.1 วัตถุประสงค์

เพื่อเป็นแนวทางในการบริหารจัดการ การบริหารความเสี่ยงระบบเทคโนโลยีสารสนเทศ ให้สอดคล้องกับกฎเกณฑ์ระเบียบของหน่วยงานกำกับดูแล สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ที่ สธ.38/2565 เรื่อง ข้อกำหนดในรายละเอียดเกี่ยวกับการจัดให้มี ระบบเทคโนโลยีสารสนเทศ ข้อ 5 (1) การกำกับดูแลและบริหารจัดการด้านเทคโนโลยีสารสนเทศ (Information Technology Governance) ตามภาคผนวก 2 ส่วนที่ 2 การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศในระดับองค์กร

1.2 แนวทางการดำเนินการ

1.2.1 การจัดให้มีโครงสร้างการกำกับดูแลและบริหารจัดการความเสี่ยงระบบเทคโนโลยีสารสนเทศ

1.2.2 การประเมินระดับความเสี่ยงเกี่ยวกับระบบเทคโนโลยีสารสนเทศ

1.2.3 การจัดให้มีกระบวนการบริหารจัดการความเสี่ยงระบบเทคโนโลยีสารสนเทศ เพื่อให้อยู่ในระดับที่องค์กรยอมรับได้

1.2.4 การสื่อสารนโยบาย

บริษัทต้องจัดให้มีการสื่อสารนโยบายการบริหารความเสี่ยงระบบเทคโนโลยีสารสนเทศ ให้แก่บุคคลที่เกี่ยวข้อง รับทราบตามบทบาทหน้าที่ ความรับผิดชอบ และสิทธิการเข้าถึงข้อมูล ในลักษณะที่สามารถเข้าถึงได้ง่าย เพื่อให้บุคคลที่เกี่ยวข้องดังกล่าวเข้าใจและสามารถปฏิบัติตามนโยบายได้อย่างถูกต้อง

ในการสื่อสารนโยบายให้บุคคลภายนอก ควรพิจารณาถึงรายละอียดที่บุคคลภายนอกควรรู้ เพื่อให้สามารถปฏิบัติงานได้สอดคล้องกับนโยบายของบริษัท โดยคำนึงถึงความลับของการเปิดเผยข้อมูลด้วย

ในกรณีที่มีการเปลี่ยนแปลงนโยบาย ต้องสื่อสารให้บุคคลที่เกี่ยวข้องได้รับทราบอย่างทั่วถึง และต้องปรับปรุงขั้นตอนและวิธีปฏิบัติงานให้สอดคล้องกับการเปลี่ยนแปลงดังกล่าว

1.2.5 การกำหนดขั้นตอนและวิธีปฏิบัติงานให้เป็นไปตามนโยบาย

(1) บริษัทควรกำหนดขั้นตอนการปฏิบัติงานที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร เพื่อให้เจ้าหน้าที่ผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ สามารถปฏิบัติงานได้อย่างถูกต้องและเป็นไปตามนโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ

(2) บริษัทควรกำหนดวิธีปฏิบัติสำหรับการอนุมัติยกเว้น (exception) กรณีที่มีความจำเป็นให้ไม่สามารถปฏิบัติตามขั้นตอนและวิธีปฏิบัติงานที่กำหนดไว้ โดยจัดให้มีการประเมินความเสี่ยง ควบคุมความเสี่ยงอย่างเพียงพอเหมาะสม และขออนุมัติยกเว้นจากผู้มีอำนาจก่อนดำเนินการต่อไป พร้อมนี้ควรจัดเก็บหลักฐานการอนุมัติยกเว้นดังกล่าวอย่างเป็นลายลักษณ์อักษร

(3) บริษัทควรจัดให้มีการสอบทานความเหมาะสมของรายการขออนุมัติยกเว้นตลอดจนแนวทางการควบคุมความเสี่ยงอย่างน้อยปีละ 1 ครั้ง เพื่อทบทวนแนวทางการดำเนินการให้มีความเหมาะสมต่อความเสี่ยงที่อาจมีการเปลี่ยนแปลงไปตามสถาพแวดล้อมการประกอบธุรกิจและการใช้งานเทคโนโลยีสารสนเทศในการประกอบธุรกิจ

พิมพ์พร

1.2.6 การทบทวนนโยบาย

บริษัทต้องทบทวนหรือปรับปรุงนโยบาย อย่างน้อยปีละ 1 ครั้ง และโดยไม่ชักช้าเมื่อมีเหตุการณ์ใด ๆ ซึ่งอาจส่งผลกระทบต่อการกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างมีนัยสำคัญ

2. นิยามและคำจำกัดความ

คำนิยาม	คำอธิบาย
เทคโนโลยีสารสนเทศ (information technology : IT)	เทคโนโลยีสารสนเทศที่นำมาใช้ในการดำเนินธุรกิจ ซึ่งครอบคลุมถึงข้อมูลหรือสารสนเทศ (data/information) ระบบปฏิบัติการ (operating system) ระบบงาน (application system) ระบบฐานข้อมูล (database system) ฮาร์ดแวร์ (hardware) และระบบเครือข่ายสื่อสาร (communication system)
ความเสี่ยงด้านเทคโนโลยีสารสนเทศ (information technology risk)	ความเสี่ยงที่อาจเกิดขึ้นจากการใช้เทคโนโลยีสารสนเทศ โดยรวมถึงความเสี่ยงที่เกิดจากภัยคุกคามทางไซเบอร์ ซึ่งส่งผลอย่างหนึ่งอย่างใดดังต่อไปนี้ (1) ผลกระทบต่อระบบงานหรือการปฏิบัติงานของผู้ประกอบกิจการ (2) ผลกระทบต่อความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและความเสี่ยงของข้อมูล (3) ผลกระทบต่อความมั่นคงของตลาดทุน
ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (information technology security)	การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) สภาพพร้อมใช้งาน (availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความรับผิดชอบ (accountibilitry) ความน่าเชื่อถือ (realiability) ความถูกต้องแท้จริง authentification) การห้ามปฏิเสธความรับผิด (non-repudiation)
บริษัท	บริษัทหลักทรัพย์จัดการกองทุน ไอร่า จำกัด
สำนักงาน	สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์
การใช้อุปกรณ์เคลื่อนที่ (mobile device)	การปฏิบัติงานที่มีการใช้อุปกรณ์เคลื่อนที่เพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศที่มีนัยสำคัญ โดยผ่านการเชื่อต่อกับระบบเครือข่ายคอมพิวเตอร์ภายในของผู้ประกอบธุรกิจโดยตรง
การใช้งานอุปกรณ์ส่วนตัว (Bring Your Own Device : BYOD)	การใช้งานอุปกรณ์ส่วนตัวของบุคลากรเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศ รวมถึงการเข้าถึงระบบอีเมล และตารางการประชุมของผู้ประกอบธุรกิจ ไม่ว่าจะกระทำผ่านแอปพลิเคชัน เว็บบราวเซอร์ หรือช่องทางใดๆ
การบริหารจัดการโครงการด้าน IT (IT project management)	การจัดหา พัฒนา หรือแก้ไขเปลี่ยนแปลงระบบ ที่มีผลกระทบอย่างมีนัยสำคัญต่อการให้บริการ การดำเนินธุรกิจ หรือโครงสร้างพื้นฐาน (infrastructure) ด้านเทคโนโลยีสารสนเทศ
การปฏิบัติงานจากเครือข่ายภายนอก (teleworking)	การปฏิบัติงานที่มีการเข้าถึงระบบเทคโนโลยีสารสนเทศที่มีนัยสำคัญโดยไม่ผ่านการเชื่อต่อกับระบบเครือข่ายคอมพิวเตอร์ภายในของบริษัทโดยตรง
ซอฟต์แวร์ (software)	ระบบหรือโปรแกรมคอมพิวเตอร์ ดังนี้

คำนิยาม	คำอธิบาย
	(1) ซอฟต์แวร์ระบบ (system software) เช่น ระบบปฏิบัติการ หรือ โปรแกรมตรวจจับไวรัส เป็นต้น (2) ซอฟต์แวร์ประยุกต์ (application software) เช่น โปรแกมประมวลผลคำ (word processor) หรือโปรแกรมสำหรับการประชุมออนไลน์ เป็นต้น
ทรัพย์สินด้านเทคโนโลยีสารสนเทศ	ฮาร์ดแวร์ ซอฟต์แวร์ และข้อมูลที่เกี่ยวข้องกับการประกอบธุรกิจ โดยรวมถึงสิทธิในการใช้งานฮาร์ดแวร์และซอฟต์แวร์ เช่น สิทธิตามสัญญาอนุญาตใช้ซอฟต์แวร์ (software license) หรือสัญญาเช่าฮาร์ดแวร์ เป็นต้น
บุคลากร	บุคลากรของบริษัท
บุคคลภายนอก (third party)	บุคคลภายนอกที่มีความเกี่ยวข้องกับบริษัท แต่ไม่รวมถึงลูกค้าที่ใช้บริการหรือผลิตภัณฑ์ของบริษัท (1) ผู้ให้บริการงานด้านเทคโนโลยีสารสนเทศ (2) ผู้ที่มีการเชื่อต่อกับระบบเทคโนโลยีสารสนเทศของบริษัท (3) ผู้ที่สามารถเข้าถึงข้อมูลสำคัญของบริษัทหรือข้อมูลของลูกค้าที่อยู่ภายใต้การควบคุมดูแลของบริษัท
แบบ RLA (Risk Level Assessment)	แบบการประเมินระดับความเสี่ยงเกี่ยวกับระบบเทคโนโลยีสารสนเทศซึ่งส่งผลต่อการดำเนินธุรกิจของผู้ประอบธุรกิจที่กำหนดไว้บนเว็บไซต์ของสำนักงาน
ประกาศที่ สธ. 38/2565	ประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ว่าด้วยข้อกำหนดในรายละเอียดเกี่ยวกับการจัดให้มีระบบเทคโนโลยีสารสนเทศ
ผู้ประกอบธุรกิจขนาดเล็ก	ผู้ประกอบธุรกิจที่เข้าลักษณะเป็นผู้ประกอบธุรกิจขนาดเล็กตามที่กำหนดในแบบ RLA (Risk Level Assessment)
ผู้ประกอบธุรกิจที่มีความเสี่ยงระดับต่ำ ระดับปานกลาง หรือระดับสูง	ผู้ประกอบธุรกิจที่มีผลการประเมินตามแบบ RLA (Risk Level Assessment) อยู่ในระดับต่ำ ระดับปานกลาง ระดับสูง แล้วแต่กรณี
ผู้ให้บริการงานด้าน IT	บุคคลภายนอกซึ่งบริษัทว่าจ้างหรือมอบหมายให้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ ซึ่งโดยปกติแล้วบริษัทต้องดำเนินการเอง เช่น การมอบหมายงานทั้งหมดของฝ่ายเทคโนโลยีสารสนเทศให้แก่บริษัทในเครือ เป็นต้น
เหตุการณ์ผิดปกติด้าน IT (IT incident)	เหตุการณ์ด้านเทคโนโลยีสารสนเทศ ที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (unwanted or unexpected) เช่น (1) ระบบเทคโนโลยีสารสนเทศ ของผู้ประกอบธุรกิจถูกบุกรุกหรือโจมตี (2) ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศถูกคุกคาม (3) ระบบเทคโนโลยีสารสนเทศหยุกชะงัก ไม่สามารถให้บริการได้
ฮาร์ดแวร์ (haraware)	อุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย รวมถึงอุปกรณ์อื่นๆที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจ
IT	เทคโนโลยีสารสนเทศ

คำนิยาม	คำอธิบาย
MFA	การยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication)
non-disclosure agreement	ข้อตกลงในการไม่เปิดเผยข้อมูล
privileged user	ผู้ใช้งานที่ได้รับสิทธิในการใช้งานในระดับสูง

3. โครงสร้างการกำกับดูแลและบริหารจัดการความเสี่ยงระบบเทคโนโลยีสารสนเทศ

3.1 บทบาทหน้าที่และความรับผิดชอบของคณะกรรมการบริษัท

บริษัทต้องดำเนินการให้มีการควบคุมดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ผ่านการกำกับดูแลโดยคณะกรรมการบริษัท เพื่อให้สอดคล้องกับระดับความเสี่ยงที่องค์กรยอมรับได้ โดยคำนึงถึงการบริหารและการจัดการความเสี่ยงขององค์กร (enterprise risk) (ถ้ามี)

3.2 โครงสร้างการกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

บริษัทต้องจัดให้มีโครงสร้างการกำกับดูแลและบริหารจัดการความเสี่ยงด้าน IT โดยอย่างน้อยต้องมีลักษณะ ดังนี้

(1) ทำให้เกิดการถ่วงดุลอย่างเป็นอิสระ

(2) สอดคล้องตามหลักการแบ่งแยกหน้าที่ 3 ระดับ (3 Lines of Defense: 3 LoDs) โดยมีการแบ่งแยกหน้าที่อย่างชัดเจนระหว่างการทำหน้าที่ด้าน IT ดังนี้

ก. ระดับที่ 1 (first line of defense) : การปฏิบัติงาน

ข. ระดับที่ 2 (second line of defense) : การบริหารความเสี่ยงและกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง

ค. ระดับที่ 3 (third line of defense) : การตรวจสอบ

3.3 การบริหารจัดการบุคลากร

บริษัทต้องบริหารจัดการบุคลากรที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ บริหารความเสี่ยงด้านเทคโนโลยีบุคลากรที่ใช้เทคโนโลยีในการปฏิบัติงานประจำวัน (user) อย่างเหมาะสม โดยต้องคำนึงถึงความรู้ความสามารถของบุคลากร ปริมาณงาน และการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ โดยต้องมีการดำเนินการอย่างน้อยในเรื่องดังต่อไปนี้

ก. ต้องครอบคลุมในเรื่องกระบวนการคัดเลือกบุคลากรที่มีความรู้หรือประสบการณ์เพียงพอในการปฏิบัติหน้าที่ความเพียงพอของบุคลากรที่สอดคล้องกับปริมาณการใช้เทคโนโลยีสารสนเทศ โดยต้องมีการดำเนินการอย่างน้อยในเรื่องดังต่อไปนี้

ข. ข้อกำหนดหรือเงื่อนไขในสัญญาจ้างงานของบุคลากรควรระบุเรื่องความรับผิดชอบเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของสถาบันการเงินอย่างชัดเจน เพื่อป้องกันการรั่วไหลของข้อมูลหรือความเสียหายที่อาจเกิดขึ้นต่อทรัพย์สินด้านเทคโนโลยีสารสนเทศของสถาบันการเงิน

ค. การบริหารจัดการสิทธิของบุคลากรที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ โดยต้องปรับปรุงให้เป็นปัจจุบัน โดยเฉพาะเมื่อมีการเปลี่ยนแปลงตำแหน่งงานหรือสิ้นสุดการจ้างงาน รวมทั้งต้องสื่อสารให้ผู้ที่เกี่ยวข้องทราบถึงการเปลี่ยนแปลงดังกล่าว

ง. การส่งเสริมให้บุคลากรตระหนักถึงความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk awareness) เช่น การจัดอบรมให้ความรู้แก่บุคลากรเกี่ยวกับการใช้งานอุปกรณ์คอมพิวเตอร์ที่เชื่อต่อกับอินเทอร์เน็ตที่ถูกต้อง และการซักซ้อมแผนเพื่อเตรียมความพร้อมรับมือการโจมตีทางไซเบอร์

จ. กรณีการใช้บริการบุคคลภายนอก บริษัทต้องจัดให้มีแนวทางการบริหารจัดการความเสี่ยงจากบุคคลภายนอก (third party risk management)

4. การประเมินระดับความเสี่ยงเกี่ยวกับระบบเทคโนโลยีสารสนเทศ

บริษัทต้องมีการดำเนินการประเมินระดับความเสี่ยงเกี่ยวกับระบบเทคโนโลยีสารสนเทศซึ่งส่งผลต่อการดำเนินธุรกิจของบริษัท ตามแบบ RLA (Risk Level Assessment) และจัดส่งผลการประเมินดังกล่าวต่อสำนักงาน ภายในไตรมาสที่ 4 ของทุกปี ทั้งนี้ ตามแบบและวิธีการที่กำหนดไว้บนเว็บไซต์ของสำนักงาน ก.ล.ต.

ผลการประเมินระดับความเสี่ยง ต้องผ่านการพิจารณาจากคณะกรรมการ หรือผู้ที่ได้รับมอบหมายจากคณะกรรมการของบริษัท ให้รับผิดชอบในเรื่องดังกล่าว

5. กระบวนการบริหารจัดการความเสี่ยงระบบเทคโนโลยีสารสนเทศ

5.1 กรอบการดำเนินการบริหารจัดการความเสี่ยงระบบเทคโนโลยีสารสนเทศ (Framework)

ก. บริษัทต้องมีแนวทางการบริหารจัดการความเสี่ยงระบบเทคโนโลยีสารสนเทศ รวมถึงโครงการด้านเทคโนโลยีสารสนเทศ อย่างมีประสิทธิภาพและรัดกุม ภายใต้กรอบหลักการที่สำคัญ 3 ประการ คือ

(1) การรักษาความลับของระบบและข้อมูล (confidentiality)

(2) ความถูกต้องเชื่อถือได้ของระบบข้อมูล (integrity) และ

(3) ความพร้อมใช้งานของเทคโนโลยีสารสนเทศ (availability)

โดยอยู่บนพื้นฐานของการคุ้มครองข้อมูลและรักษาผลประโยชน์ของลูกค้า ให้อยู่ในระดับความเสี่ยงที่ยอมรับได้ ทั้งในภาวะปกติและภาวะวิกฤต

ข. กำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศให้สอดคล้องกับลักษณะการดำเนินธุรกิจ ปริมาณธุรกรรมความซับซ้อนของเทคโนโลยีสารสนเทศ และความเสี่ยงที่เกี่ยวข้อง เช่น ความเสี่ยงด้านปฏิบัติการ ความเสี่ยงด้านกลยุทธ์ ความเสี่ยงด้านชื่อเสียง และความเสี่ยงด้านกฎหมาย รวมถึงให้ความสำคัญกับการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศโดยถือเป็นส่วนหนึ่งของการบริหารความเสี่ยงในภาพรวมของสถาบันการเงิน (Enterprise Risk Management : ERM)

ค. มีการสร้างความรู้และความตระหนักรู้เรื่องความเสี่ยงด้านเทคโนโลยีสารสนเทศแก่กรรมการ ผู้บริหาร และพนักงานในองค์กรอย่างต่อเนื่องและมีประสิทธิภาพ

ง. มีการนำเสนอความเสี่ยงด้านเทคโนโลยีสารสนเทศต่อคณะกรรมการบริษัทหรือคณะกรรมการที่เกี่ยวข้องกับการบริหารจัดการและกำกับดูแลการด้านเทคโนโลยีสารสนเทศเป็นวาระประจำ

5.2 การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management)

บริษัทต้องดำเนินการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยจัดทำระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยครอบคลุมอย่างน้อยในเรื่องดังต่อไปนี้

พิมพ์พร

(1) การประเมินความเสี่ยง (risk assessment)

ก. การระบุความเสี่ยง (risk identification)

ต้องระบุถึงความเสี่ยงด้านเทคโนโลยีสารสนเทศซึ่งรวมถึงความเสี่ยงดังกล่าวอาจมีสาเหตุมาจากกระบวนการปฏิบัติงาน ระบบงาน บุคลากร หรือปัจจัยภายนอก

ข. การวิเคราะห์ความเสี่ยง (risk analysis)

ต้องเข้าใจและวิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อหาแนวทางนารจัดการความเสี่ยงที่เหมาะสม

ค. การประเมินค่าความเสี่ยง (risk evaluation)

ต้องประเมินถึงโอกาสที่ความเสี่ยงด้านเทคโนโลยีสารสนเทศจะเกิดขึ้นและผลกระทบต่อการปฏิบัติงานและดำเนินธุรกิจ รวมถึงกำหนดระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ยอมรับได้ (IT risk appetite)

(2) การจัดการความเสี่ยง (risk treatment)

บริษัทต้องมีแนวทางจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อให้ความเสี่ยงที่เหลืออยู่ (residual risk) อยู่ในระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ยอมรับได้

นอกจากนี้ บริษัทต้องกำหนดดัชนีชี้วัดความเสี่ยงด้านเทคโนโลยีสารสนเทศที่สำคัญ (IT key risk indicators) ที่เกี่ยวข้องกับการดำเนินธุรกิจ ให้สอดคล้องกับความสำคัญของเทคโนโลยีสารสนเทศแต่ละงาน เพื่อใช้ติดตามและทบทวนความเสี่ยง

(3) การติดตามและทบทวนความเสี่ยง (risk monitoring and review)

บริษัทต้องมีกระบวนการที่มีประสิทธิภาพในการติดตามและทบทวนความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อให้อยู่ภายใต้ระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ยอมรับได้ที่กำหนดไว้

(4) การรายงานความเสี่ยง (risk reporting)

บริษัทต้องรายงานระดับความเสี่ยงและผลการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ต่อคณะกรรมการที่ได้รับมอบหมายเป็นประจำ เช่น ตามรอบการประชุมของคณะกรรมการ

นโยบายการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ (IT Risk Management Policy) ฉบับทบทวนปี 2568 ฉบับนี้ ได้รับการอนุมัติจากที่ประชุมคณะกรรมการบริษัท ครั้งที่ 3/2568 เมื่อวันที่ 4 สิงหาคม 2568 โดยมีผลบังคับใช้ตั้งแต่วันที่ 4 สิงหาคม 2568

.....

(นางเสาวนีย์ กมลบุตร)

ประธานกรรมการบริษัท

บริษัท หลักทรัพย์จัดการกองทุน ไอร่า จำกัด

พิมพ์พร