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

นโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศ

(IT Governance Policy)

(ฉบับทบทวนปี 2568)

สารบัญ

พิมพ์พร

นโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศ (IT Governance Policy) (ฉบับปรับปรุงปี 2568)

บริษัทตระหนักถึงความสำคัญเรื่อง ระบบเทคโนโลยีสารสนเทศเข้ามามีบทบาทสำคัญในการขับเคลื่อนธุรกิจ รวมทั้ง ตระหนักถึงบทบาทและความสำคัญของเทคโนโลยีสารสนเทศในการประกอบธุรกิจหลักทรัพย์จัดการกองทุน จึงได้พิจารณาให้มีการบริหารความเสี่ยงและการรักษาความปลอดภัยในเรื่องดังกล่าวอย่างมีประสิทธิภาพเพื่อป้องกันความเสียหายที่อาจเกิดขึ้นจากการใช้เทคโนโลยีสารสนเทศในการดำเนินงาน ทั้งนี้ เพื่อให้สอดคล้องกับแนวทางของหน่วยงานกำกับภายนอก คณะผู้บริหารของบริษัทจึงกำหนดนโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศขึ้น เพื่อเป็นกฎระเบียบและข้อปฏิบัติในการควบคุมความปลอดภัยด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้องในการดำเนินธุรกิจของบริษัท

ทั้งนี้ เพื่อให้บริษัทสามารถกำกับดูแล ป้องกัน ควบคุม ติดตามการดำเนินงานของบริษัทอย่างมีประสิทธิภาพ สอดคล้องและเป็นไปในทิศทางเดียวกัน บริษัทจึงจัดทำนโยบายดังกล่าว เพื่อให้พนักงานและผู้บริหารทุกระดับได้รับทราบและนำไปปฏิบัติอย่างเคร่งครัด โดยที่ประชุมคณะกรรมการบริษัทครั้งที่ 5/2568 วันที่ 16 ธันวาคม 2568 ได้มีมติอนุมัตินโยบายนโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศ (IT Governance Policy) ดังมีรายละเอียดตามเอกสารแนบท้ายนี้

ผู้บังคับบัญชามีหน้าที่ต้องติดตามและแนะนำผู้ใต้บังคับบัญชาตามลำดับชั้น ในการปฏิบัติงานให้สอดคล้องกับนโยบาย ขั้นตอน และวิธีการปฏิบัติที่กำหนดไว้ในนโยบายฉบับนี้ โดยสม่ำเสมอ

คณะกรรมการบริษัท

ส่วนที่ 1 บทนำ

1.1 วัตถุประสงค์

บริษัท หลักทรัพย์จัดการกองทุน ไอร่า จำกัด (บริษัท) ตระหนักถึงความสำคัญเป็นอย่างยิ่งในบทบาทของการใช้เทคโนโลยีสารสนเทศในการประกอบธุรกิจบริหารจัดการลงทุน จึงได้พิจารณาให้มีการบริหารความเสี่ยงและการรักษาความปลอดภัยในเรื่องดังกล่าวอย่างมีประสิทธิภาพเพื่อป้องกันความเสียหายที่อาจเกิดขึ้นจากการใช้เทคโนโลยีสารสนเทศในการดำเนินงาน ทั้งนี้ เพื่อให้สอดคล้องกับแนวทางของหน่วยงานกำกับภายนอก คณะผู้บริหารของบริษัท จึงได้กำหนดนโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศขึ้น เพื่อเป็นกฎระเบียบและข้อปฏิบัติในการควบคุมความปลอดภัยด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้องในการดำเนินธุรกิจของบริษัท

อ้างถึงประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ที่ สธ. 38/2565 เรื่อง ข้อกำหนดในรายละเอียดเกี่ยวกับการจัดให้มีระบบเทคโนโลยีสารสนเทศ และประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ที่ สธ. 33/2567 เรื่อง ข้อกำหนดในรายละเอียดเกี่ยวกับการจัดให้มีระบบเทคโนโลยีสารสนเทศ (ฉบับที่ 2) เพื่อให้ผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสัญญาซื้อขายล่วงหน้า ใช้เป็นมาตรฐานในการประกอบธุรกิจ โครงสร้างการบริหารงาน ระบบงาน และการให้บริการ ในส่วนที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศที่มีประสิทธิภาพและเป็นไปในทิศทางเดียวกัน ผู้บริหารระดับสูงจะต้องมีบทบาทสำคัญในการบริหารจัดการการนำเทคโนโลยีสารสนเทศมาใช้ในการประกอบธุรกิจ รวมถึงมีหน้าที่ในการส่งทอดเป้าหมายตามภารกิจ กลยุทธ์ นโยบาย และแผนงานระดับองค์กรสู่เป้าหมายที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศภายใต้การกำกับดูแลของคณะกรรมการบริษัท เพื่อให้มั่นใจว่าการนำเทคโนโลยีสารสนเทศดังกล่าวมาใช้ในการประกอบธุรกิจ ช่วยให้ผู้ประกอบธุรกิจสามารถบรรลุเป้าหมายได้ตามที่กำหนดไว้ โดยมีการใช้ทรัพยากรอย่างเหมาะสม และมีการบริหารจัดการความเสี่ยงอย่างเหมาะสม สอดคล้องกับการกำกับดูแลกิจการที่ดี (Corporate Governance) บริษัทจึงได้กำหนดนโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศ (IT Governance Policy) เพื่อให้ผู้เกี่ยวข้องใช้เป็นแนวทางในการปฏิบัติงาน

1.2 คำจำกัดความ

การกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศ (IT Governance)	หมายถึง การบริหารงานด้านเทคโนโลยีสารสนเทศที่เชื่อมโยงระหว่างกระบวนการบริหารงานด้านเทคโนโลยีสารสนเทศ ทรัพยากร และข้อมูลที่มีประสิทธิภาพเพื่อสนับสนุนนโยบาย กลยุทธ์ เป้าหมายองค์กรและการบริหารความเสี่ยงที่เหมาะสม โดยมีการดำเนินการตามแนวทางการปฏิบัติที่ดีเกี่ยวกับการวางแผน การจัดการองค์กร การจัดหาการนำระบบงานออกมาใช้งานจริง การส่งมอบและการสนับสนุน รวมทั้งการรายงานและการติดตามผลการดำเนินงาน เพื่อให้มั่นใจว่าเทคโนโลยีที่นำมาใช้สามารถช่วยสนับสนุนกลยุทธ์และบรรลุวัตถุประสงค์ในเชิงธุรกิจรวมทั้งสร้างศักยภาพในการแข่งขันเพื่อเพิ่มมูลค่าให้องค์กร
โปรแกรมสำเร็จรูป	หมายถึง ระบบการคำนวณที่แสดงผลเป็นการวิเคราะห์เพื่อให้คำแนะนำเกี่ยวกับคุณค่าหรือความเหมาะสมในการลงทุนในหลักทรัพย์หรือสัญญาการซื้อขายล่วงหน้า
ซอฟต์แวร์ (Software)	หมายถึง ระบบหรือโปรแกรมคอมพิวเตอร์ ดังนี้ 1. ซอฟต์แวร์ระบบ (system software) เช่น ระบบปฏิบัติการ หรือโปรแกรม ตรวจจับไวรัส เป็นต้น

	2. ซอฟต์แวร์ประยุกต์ (application software) เช่น โปรแกรมประมวลผลคำ (word processor) หรือโปรแกรมสำหรับการประชุมออนไลน์ เป็นต้น
ฮาร์ดแวร์ (Hardware)	หมายถึง อุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย รวมถึงอุปกรณ์อื่น ๆ ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศของบริษัท
ทรัพย์สินด้านเทคโนโลยีสารสนเทศ	หมายถึง ฮาร์ดแวร์ ซอฟต์แวร์ และข้อมูลที่เกี่ยวข้องกับการประกอบธุรกิจ โดยรวมถึงสิทธิในการใช้งานฮาร์ดแวร์และซอฟต์แวร์ เช่น สิทธิตามสัญญาอนุญาตใช้ซอฟต์แวร์ (software license) หรือสัญญาเช่าฮาร์ดแวร์ เป็นต้น
การปฏิบัติงานจากเครือข่ายภายนอกบริษัท (Teleworking)	หมายถึง การปฏิบัติงานที่มีการเข้าถึงระบบสารสนเทศที่มีความสำคัญโดยไม่ผ่านการเชื่อมต่อกับระบบเครือข่ายคอมพิวเตอร์ภายในของบริษัทโดยตรง
การใช้งานอุปกรณ์เคลื่อนที่ (Mobile device)	หมายถึง การปฏิบัติงานที่มีการใช้อุปกรณ์เคลื่อนที่ (Mobile device) เพื่อเข้าถึงระบบสารสนเทศที่มีความสำคัญ โดยผ่านการเชื่อมต่อกับระบบเครือข่ายคอมพิวเตอร์ภายในของบริษัทโดยตรง
สิ่งอำนวยความสะดวกในการประมวลผลข้อมูล (Information processing facilities)	หมายถึง อุปกรณ์ ระบบงาน หรือสภาพแวดล้อม ที่จำเป็นหรือมีส่วนช่วยให้การประมวลผลข้อมูลเป็นไปอย่างครบถ้วน ถูกต้อง และมีประสิทธิภาพ เช่น อุปกรณ์หรือโปรแกรมประมวลผลข้อมูล ระบบเครือข่ายคอมพิวเตอร์ ขั้นตอน หรือสถานที่ประมวลผลข้อมูล
ภัยคุกคามทางไซเบอร์	หมายถึง การกระทำหรือการดำเนินการใด ๆ โดยมิชอบ โดยการใช้คอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือโปรแกรมคอมพิวเตอร์ ซึ่งมุ่งหมายให้เกิดความเสียหาย ต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง รวมถึง ภยันตรายที่อาจจะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของ คอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

1.3 ขอบเขตและผลบังคับใช้ของนโยบาย

แนวทางปฏิบัติฉบับนี้ใช้เป็นแนวทางในการกำหนดหลักเกณฑ์อันว่าด้วยการปฏิบัติตามนโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศหรือข้อกำหนดของทางการอื่นใดที่เกี่ยวข้อง

ผู้ที่ต้องปฏิบัติตามแนวทางปฏิบัติฉบับนี้ ได้แก่ ผู้บริหารทุกระดับ พนักงานทุกคน รวมถึงตัวแทน และผู้ที่ได้รับมอบหมายจากบริษัท ต้องปฏิบัติตามแนวทางปฏิบัติฉบับนี้โดยเคร่งครัด

1.4 การตรวจสอบให้เป็นไปตามนโยบาย

บริษัทกำหนดให้มีการดำเนินงาน ดังนี้

- ผู้บริหารสูงสุดของแต่ละสายงานฯ ต้องดูแลผู้ใต้บังคับบัญชาของตนให้ปฏิบัติตามนโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศอย่างถูกต้อง
- หน่วยงานตรวจสอบหรือคณะกรรมการบริษัทพิจารณามอบหมายบุคคลที่เหมาะสมเพื่อตรวจสอบการปฏิบัติตามนโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ อย่างน้อยปีละครั้ง
- ส่วนงานที่เกี่ยวข้องต้องจัดให้มีการตรวจสอบด้านเทคนิคสำหรับอุปกรณ์คอมพิวเตอร์และโปรแกรม เพื่อให้มั่นใจว่าได้มีการปฏิบัติตามการควบคุมที่กำหนดไว้

- ส่วนงานที่เกี่ยวข้องต้องประกาศใช้และสื่อสารนโยบายให้แก่บุคคลที่เกี่ยวข้องอย่างทั่วถึง เพื่อให้สามารถปฏิบัติตามได้ เช่น จัดการฝึกอบรม เป็นต้น
- ส่วนงานที่เกี่ยวข้องต้องมีการติดตามการปฏิบัติงานของเจ้าหน้าที่ให้เป็นไปตามนโยบายอย่างเคร่งครัด
- ส่วนงานที่เกี่ยวข้องต้องมีขั้นตอนหรือวิธีปฏิบัติเพื่อให้มีการปฏิบัติตามนโยบายที่ได้กำหนดไว้อย่างครบถ้วน
- บริษัทต้องรายงานสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ทันที เมื่อมีกรณีที่ส่งผลกระทบต่อการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศที่มีนัยสำคัญ

1.5 การทบทวนนโยบาย

บริษัทกำหนดให้มีการทบทวนนโยบายอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีประกาศของทางการที่เกี่ยวข้องมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

ส่วนที่ 2 การปฏิบัติตามนโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศ (IT Governance Policy)

2.1 แนวทางปฏิบัติเกี่ยวกับการกำกับดูแลและการบริหารจัดการเทคโนโลยีสารสนเทศ

บริษัทกำหนดให้ผู้บริหารและหน่วยงานที่เกี่ยวข้องดำเนินการ ดังนี้

1. บริษัทควรจัดให้มีนโยบายการกำกับดูแลและการบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรเป็นลายลักษณ์อักษร ซึ่งนโยบายดังกล่าวต้องได้รับความเห็นชอบจากคณะกรรมการของบริษัทหรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของบริษัท
2. บริษัทควรจัดให้มีนโยบายการบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ซึ่งครอบคลุมถึงการระบุความเสี่ยง การประเมินความเสี่ยง การกำหนดเครื่องมือและมาตรการในการบริหารและจัดการความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้ การกำหนดตัวชี้วัดระดับความเสี่ยงรวมถึงการติดตามรายงานผลตัวชี้วัด และการกำหนดหน้าที่ความรับผิดชอบของผู้รับผิดชอบ
3. บริษัทควรจัดให้มีนโยบายการจัดสรรและบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศ ซึ่งครอบคลุมถึงการจัดสรรทรัพยากรให้เพียงพอต่อการดำเนินธุรกิจ และการกำหนดแนวทางเพื่อรองรับในกรณีที่ไม่สามารถจัดสรรทรัพยากรได้เพียงพอตามที่กำหนดไว้
4. บริษัทควรจัดให้มีนโยบายและมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ
5. บริษัทควรจัดให้มีการกำกับดูแลและบริหารจัดการด้านเทคโนโลยีสารสนเทศตามหลักเกณฑ์ดังต่อไปนี้
   - สื่อสารนโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศให้แก่บุคลากรของบริษัทที่เกี่ยวข้องอย่างทั่วถึง ในลักษณะที่สามารถเข้าถึงได้ง่าย เพื่อให้บุคลากรดังกล่าวเข้าใจและสามารถปฏิบัติตามนโยบายดังกล่าวได้อย่างถูกต้อง
   - กำหนดขั้นตอนและวิธีปฏิบัติงานให้เป็นไปตามนโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศ
   - ทบทวนหรือปรับปรุงนโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศ อย่างน้อยปีละ 1 ครั้ง โดยต้องทบทวนโดยไม่ชักช้าเมื่อมีเหตุการณ์ใด ๆ ซึ่งอาจส่งผลกระทบต่อการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศอย่างมีนัยสำคัญ และต้องปรับปรุงขั้นตอนและวิธีปฏิบัติงานให้สอดคล้องกับนโยบายที่มีการเปลี่ยนแปลงด้วย
6. บริษัทควรจัดให้มีระบบการควบคุมภายในสำหรับการปฏิบัติงานให้เป็นไปตามนโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศ ดังต่อไปนี้
   - จัดให้มีการตรวจสอบภายในและการสอบทานการปฏิบัติงานให้เป็นไปตามนโยบายนี้อย่างเป็นระบบ
   - มีการปรับปรุงแก้ไขข้อบกพร่องและติดตามการปรับปรุงแก้ไขดังกล่าวอย่างเป็นระบบ
   - จัดให้มีการติดตาม ตรวจสอบ และประเมินประสิทธิภาพของขั้นตอนการปฏิบัติงานของหน่วยงานที่ทำหน้าที่บริหารและจัดการ โดยผู้ตรวจสอบที่เป็นอิสระจากหน่วยงานดังกล่าว
     - การปฏิบัติงานให้เป็นไปตามนโยบายที่กำหนด
     - การรายงานการปฏิบัติงาน
   - จัดให้มีการประเมินตนเองในด้านประสิทธิภาพของขั้นตอนการปฏิบัติงาน (Control Self-assessment : CSA)

- จัดให้ผู้ตรวจสอบที่เป็นอิสระเป็นผู้ประมวลผลและรายงานผลที่ได้จากการดำเนินการติดตามตรวจสอบประเมินผลของขั้นตอน และการประเมินตนเอง พร้อมทั้งรายงานข้อบกพร่องที่ตรวจพบและผลการปรับปรุงแก้ไขให้คณะกรรมการบริษัท คณะกรรมการตรวจสอบและผู้บริหารระดับสูงตามรอบการประเมินและตามรอบการติดตามการปรับปรุงแก้ไขข้อบกพร่องหรือโดยไม่ชักช้าเมื่อพบข้อบกพร่องที่มีนัยสำคัญ

2.2 บทบาทหน้าที่ของคณะกรรมการบริษัท และผู้บริหารระดับสูง

1. มีหน้าที่รับผิดชอบในการกำกับดูแลที่ดีหรือสร้างธรรมาภิบาลด้านเทคโนโลยีสารสนเทศในองค์กร โดยกำหนด กลยุทธ์ วัตถุประสงค์ และทิศทางดำเนินงานด้านเทคโนโลยีสารสนเทศให้สอดคล้องกับกลยุทธ์ขององค์กร
2. กำหนดแนวทางการควบคุมงานด้านเทคโนโลยีสารสนเทศ ประเมินวัดผล และบริหารจัดการความเสี่ยงที่เกี่ยวข้องกับการนำเทคโนโลยีมาใช้งาน
3. สามารถแต่งตั้งคณะกรรมการชุดย่อยซึ่งมีความรู้ความเข้าใจเชิงเทคนิคเพื่อทำหน้าที่รับผิดชอบการจัดการและการกำกับดูแลงานเทคโนโลยีสารสนเทศ และการบริหารความเสี่ยงที่เกี่ยวข้องกับการนำเทคโนโลยีมาใช้ เช่น
   - คณะกรรมการบริหารเพื่อทำหน้าที่และรับผิดชอบการจัดการและการกำกับดูแลงานด้านเทคโนโลยีสารสนเทศ การบริหารความเสี่ยงที่เกี่ยวข้องกับการนำเทคโนโลยีมาใช้
   - คณะกรรมการตรวจสอบเพื่อทำหน้าที่กำกับดูแลให้บริษัทมีการตรวจสอบภายในด้านเทคโนโลยีสารสนเทศ และมีระบบการควบคุมภายในที่เหมาะสม รวมถึงการสอบทานให้มีการปฏิบัติตามกฎระเบียบและกฎหมายที่เกี่ยวข้อง
   - คณะกรรมการบริหารความเสี่ยงมีหน้าที่กำหนดนโยบายการบริหารความเสี่ยงโดยรวมของบริษัทซึ่งครอบคลุมความเสี่ยงประเภทต่าง ๆ ที่สำคัญ รวมถึงความเสี่ยงด้านเทคโนโลยีสารสนเทศนอกจากนี้ต้องมีการติดตาม ดูแลการบริหารจัดการความเสี่ยงของบริษัทให้อยู่ในระดับที่เหมาะสม และมีการปฏิบัติตามนโยบายที่กำหนดไว้

2.3 แนวทางปฏิบัติของคณะกรรมการบริษัท

1. กลยุทธ์ด้านเทคโนโลยีสารสนเทศ
   - กำหนดทิศทางและกลยุทธ์ด้านเทคโนโลยีสารสนเทศและผสมผสานเข้ากับกลยุทธ์ด้านธุรกิจ
   - ประเมินผลการใช้เทคโนโลยีของทางบริษัทว่าเป็นไปตามเป้าหมายที่กำหนดไว้
   - ตัดสินใจเกี่ยวกับการลงทุนด้านเทคโนโลยี สร้างความสมดุลระหว่างระบบสนับสนุนองค์กร และการเปลี่ยนแปลงรูปแบบองค์กร และจัดโครงสร้างที่จะช่วยการขยายธุรกิจและการเข้าไปแข่งขันในธุรกิจใหม่
   - ส่งเสริมวัฒนธรรมองค์กรให้มีความร่วมมือประสานงานระหว่างหน่วยงาน
2. กำกับดูแลส่วนงานเทคโนโลยีสารสนเทศให้สามารถส่งเสริมงานที่มีคุณค่าตามที่กำหนดไว้ในกลยุทธ์
3. กำหนดนโยบายแนวทางการดำเนินการและกระบวนการจัดการความเสี่ยงของบริษัทโดยรวม เช่น ความเสี่ยงด้านเทคโนโลยีสารสนเทศ รวมถึงความเสี่ยงอื่น ๆ ที่สำคัญในการการปฏิบัติงาน
4. การบริหารจัดการทรัพยากรด้านเทคโนโลยีสารสนเทศอย่างมีประสิทธิภาพ พิจารณาความเหมาะสมของการลงทุนในโครงสร้างและศักยภาพของระบบเทคโนโลยีสารสนเทศ การวางแผนการลงทุนด้านกำลังคน

และการจัดหาบุคลากรทดแทน รวมถึงการลงทุนเกี่ยวกับการให้ความรู้ การพัฒนาและการฝึกอบรมเพื่อการปฏิบัติงานและพัฒนาการด้านเทคโนโลยี รวมถึงความรู้และทักษะการบริหารงานโครงการ

5. กำหนดให้มีการวัดผลงานหรือประสิทธิภาพ และติดตามการวัดผลเพื่อให้มั่นใจว่าสามารถบรรลุวัตถุประสงค์และสนับสนุนให้มีเครื่องมือเพื่อการวัดผล

2.4 แนวทางปฏิบัติของผู้บริหารระดับสูง

1. ถ่ายทอดกลยุทธ์ นโยบาย และเป้าหมายลงไปในองค์กร และผสมผสานโครงสร้างของส่วนงานเทคโนโลยีสารสนเทศเข้ากับเป้าหมายองค์กร
2. กำหนดโครงสร้างองค์กรที่สนับสนุนการนำกลยุทธ์ด้านเทคโนโลยีสารสนเทศมาใช้ในทางปฏิบัติเพื่อให้มีการเผยแพร่ข้อมูลข่าวสารทางธุรกิจมากขึ้น
3. ปลูกฝังหน้าที่และความรับผิดชอบเกี่ยวกับการบริหารความเสี่ยงและการควบคุมเทคโนโลยีในองค์กร
4. จัดให้มีการวัดผลหรือประเมินผลงาน โดยกำหนดวิธีการวัดผลงานจากมูลค่าทางธุรกิจที่เกิดขึ้น รวมถึงความได้เปรียบในเชิงการแข่งขันที่เกิดจากการใช้เทคโนโลยีสารสนเทศเป็นตัวผลักดันประสิทธิภาพและสร้างประโยชน์ให้กับองค์กร
5. มุ่งเน้นไปที่ศักยภาพในการแข่งขันของธุรกิจหลักที่ต้องใช้เทคโนโลยีสารสนเทศสนับสนุนเพื่อเพิ่มคุณค่าการบริการให้แก่ลูกค้า
6. ให้ความสำคัญต่อกระบวนการเทคโนโลยีสารสนเทศเพื่อช่วยเพิ่มมูลค่าให้แก่ธุรกิจ เช่น การบริหารความเปลี่ยนแปลง การแก้ไขปัญหาที่เกิดขึ้น โดยผู้บริหารอาจต้องเข้ามามีส่วนร่วมโดยตรงในการกำหนดกระบวนการเหล่านี้ ตลอดจนกำหนดให้มีผู้มีหน้าที่รับผิดชอบดำเนินการตามกระบวนการนั้น
7. สร้างองค์กรที่มีความยืดหยุ่นและสามารถปรับตัวทันต่อเหตุการณ์ เป็นองค์กรแห่งการเรียนรู้โดยใช้เทคโนโลยีในการรวบรวมข้อมูลสารสนเทศ
8. เสริมสร้างการส่งมอบงานที่มีคุณค่า ด้วยการกำหนดมาตรฐานของเทคโนโลยี เช่น การตั้งคณะทำงานการทบทวนเทคโนโลยีสารสนเทศและสถาปัตยกรรมที่นำมาใช้ รวมทั้ง กำหนดให้มีการควบคุมการบริหารโครงการให้เป็นไปตามมาตรฐานที่กำหนด เพื่อให้ได้งานที่มีคุณค่าต่อองค์กรสูงสุด
9. ให้ความสำคัญต่อการบริหารต้นทุนและค่าใช้จ่ายด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม เพื่อให้องค์กรได้รับคุณค่าที่แท้จริงจากทรัพยากรด้านเทคโนโลยีสารสนเทศ โดยมีต้นทุนที่สมเหตุสมผล
10. กำหนดให้มีกลยุทธ์และระเบียบปฏิบัติให้ชัดเจนในการจัดหาทรัพยากรหรือการใช้บริการด้านเทคโนโลยีจากภายนอก รวมทั้งการจัดการสัญญากับบุคคลภายนอกและข้อตกลงการให้บริการ เพื่อตอบสนองความต้องการขององค์กร
11. จัดให้มีขั้นตอนการจัดทำ การติดตาม และการควบคุมการจัดทำรายงานเพื่อให้มั่นใจว่าสามารถจัดทำรายงานได้อย่างครบถ้วน ถูกต้อง และทันเวลา
12. จัดให้มีการรายงานการปฏิบัติตามนโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศให้คณะกรรมการบริษัททราบอย่างน้อยปีละ 1 ครั้ง และในกรณีที่เหตุการณ์ใด ๆ ซึ่งอาจส่งผลกระทบต่อการปฏิบัติตามนโยบายนี้อย่างมีนัยสำคัญ ต้องรายงานให้คณะกรรมบริษัททราบโดยไม่ชักช้า โดยเนื้อหาของรายงานควรครอบคลุมเรื่องดังต่อไปนี้
    - กิจกรรมที่เกี่ยวข้องกับการปฏิบัติงานด้านการบริหารความเสี่ยง หรือการจัดสรรและบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศ

- ความคืบหน้าของโครงการ (ถ้ามี)
- การปฏิบัติตามกฎระเบียบ ข้อบังคับ หรือข้อตกลงที่จัดทำกับบุคคลภายนอกและภายในบริษัท
- ความมีประสิทธิภาพของการนำเทคโนโลยีมาใช้ เช่น การติดตามระยะเวลาในการปฏิบัติงานที่ลดลงภายหลังการนำเทคโนโลยีมาปรับปรุงกระบวนการทำงาน และความสอดคล้องกับวัตถุประสงค์ของการนำเทคโนโลยีมาใช้
- ประเด็นปัญหาและอุปสรรค

2.5 การกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กร

บริษัทจะต้องจัดให้มีนโยบายที่เป็นลายลักษณ์อักษรในการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศอย่างน้อยในเรื่องต่อไปนี้ โดยนโยบายดังกล่าวต้องได้รับความเห็นชอบจากคณะกรรมการบริษัท หรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการบริษัท

1. นโยบายการบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ซึ่งครอบคลุมถึงการระบุความเสี่ยง การประเมินความเสี่ยง และการควบคุมความเสี่ยงให้อยู่ในระดับที่บริษัทยอมรับได้
2. นโยบายการจัดสรรและบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศ เพื่อให้เพียงพอต่อการดำเนินธุรกิจ และการกำหนดแนวทางเพื่อรองรับในกรณีที่ไม่สามารถจัดสรรทรัพยากรให้เพียงพอตามที่กำหนดไว้
3. นโยบายและมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

ทั้งนี้ บริษัทจะต้องจัดให้มีการกำกับดูแลและบริหารจัดการด้านเทคโนโลยีสารสนเทศตามหลักเกณฑ์ดังต่อไปนี้

1. จัดให้มีการสื่อสารนโยบายการกำกับดูแลและบริหารจัดการด้านเทคโนโลยีสารสนเทศให้แก่บุคลากรที่เกี่ยวข้องอย่างทั่วถึงในลักษณะที่สามารถเข้าถึงได้ง่าย เพื่อให้บุคลากรดังกล่าวสามารถเข้าใจและปฏิบัติตามนโยบายดังกล่าวได้อย่างถูกต้อง
2. กำหนดขั้นตอนการปฏิบัติงานให้เป็นไปตามนโยบายการกำกับดูแลและบริหารจัดการด้านเทคโนโลยีสารสนเทศ
3. ทบทวนหรือปรับปรุงนโยบายการกำกับดูแลและบริหารจัดการด้านเทคโนโลยีสารสนเทศอย่างน้อยปีละ 1 ครั้ง หรือทำการทบทวนอย่างไม่ชักช้าเมื่อมีเหตุการณ์ใด ๆ ซึ่งอาจส่งผลกระทบต่อการกำกับดูแลและบริหารจัดการด้านเทคโนโลยีสารสนเทศอย่างมีนัยสำคัญ และทำการปรับปรุงแนวปฏิบัติเพื่อให้สอดคล้องกับนโยบายที่เปลี่ยนแปลงไปด้วย
4. จัดให้มีการรายงานการปฏิบัติตามนโยบายการกำกับดูแลและบริหารจัดการด้านเทคโนโลยีสารสนเทศให้คณะกรรมการบริษัททราบอย่างน้อยปีละ 1 ครั้ง ในกรณีที่มีเหตุการณ์ใด ๆ ซึ่งอาจส่งผลกระทบต่อการปฏิบัติตามนโยบายดังกล่าวอย่างมีนัยสำคัญ ต้องรายงานให้คณะกรรมการบริษัทรับทราบโดยไม่ชักช้า
5. จัดให้มีระบบควบคุมภายในสำหรับการปฏิบัติงานให้เป็นไปตามนโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศ อย่างน้อยดังนี้
   - 5.1 มีการตรวจสอบภายในและการสอบทานการปฏิบัติงานให้เป็นไปตามนโยบายดังกล่าวอย่างเป็นระบบ
   - 5.2 มีการประเมินตนเองในด้านประสิทธิภาพของขั้นตอนการปฏิบัติงาน (control self-assessment : CSA)
   - 5.3 มีการปรับปรุงแก้ไขข้อบกพร่อง และติดตามการปรับปรุงแก้ไขดังกล่าวอย่างเป็นระบบ

2.6 การกำหนดนโยบาย มาตรการ โครงสร้างการบริหารจัดการ เพื่อรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

1) การกำหนดนโยบาย

บริษัทจะต้องจัดให้มีการกำหนดนโยบายอย่างน้อยในเรื่องดังต่อไปนี้ ไว้เป็นลายลักษณ์อักษร เพื่อรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Policy)

1. นโยบายการใช้งานระบบสารสนเทศร่วมกันบนระบบเครือข่ายคอมพิวเตอร์เพื่อการประมวลผลตามความต้องการของผู้ใช้งาน (Cloud Computing) ซึ่งครอบคลุมประเด็นต่าง ๆ ดังต่อไปนี้
   - 1.1 วิธีการคัดเลือกและประเมินผู้ให้บริการ
   - 1.2 การทบทวนคุณสมบัติผู้ให้บริการ
   - 1.3 ข้อกำหนดเกี่ยวกับการใช้บริการ
   - 1.4 การตรวจสอบบันทึกหลักฐานต่าง ๆ ที่อาจส่งผลกระทบต่อการใช้บริการ
2. นโยบายการใช้งานระบบการเข้ารหัสข้อมูลและการบริหารกุญแจเข้ารหัสข้อมูลที่สามารถป้องกันการเข้าถึงหรือเปลี่ยนแปลงการแก้ไขข้อมูลที่เป็นความลับหรือมีความสำคัญ
3. นโยบายการรับส่งข้อมูลสารสนเทศผ่านระบบเครือข่ายภายในองค์กร และระหว่างเครือข่ายภายในองค์กรกับเครือข่ายภายนอกองค์กรให้มีความมั่นคงปลอดภัย
4. นโยบายควบคุมการเข้าถึงข้อมูลและสิ่งอำนวยความสะดวกในการประมวลผลข้อมูลต่าง ๆ (Information processing facilities) ให้สอดคล้องกับข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ
5. นโยบายเพื่อรองรับในกรณีที่บริษัท แต่งตั้งบุคคลอื่นเป็นผู้รับดำเนินการในงานที่เกี่ยวกับระบบสารสนเทศของบริษัทซึ่งครอบคลุมประเด็นต่าง ๆ ดังต่อไปนี้ เพื่อลดความเสี่ยงจากการเข้าถึงทรัพย์สินด้านเทคโนโลยีสารสนเทศอย่างไม่เหมาะสม
   - 5.1 วิธีการคัดเลือกและประเมินผู้รับดำเนินการ
   - 5.2 การทบทวนคุณสมบัติผู้รับดำเนินการ
   - 5.3 ข้อกำหนดเกี่ยวกับการใช้บริการ

2) การกำหนดมาตรการ

บริษัทจะต้องจัดให้มีมาตรการอย่างน้อยในเรื่องดังต่อไปนี้ เพื่อรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

1. ในกรณีที่มีการปฏิบัติงานจากเครือข่ายภายนอกบริษัท หรือมีการใช้อุปกรณ์เคลื่อนที่ จะต้องจัดให้มีมาตรการรักษาความปลอดภัยที่รัดกุมเพียงพอสำหรับข้อมูลที่มีความสำคัญ โดยเฉพาะการใช้อุปกรณ์เคลื่อนที่ ต้องจัดให้มีการลงทะเบียนอุปกรณ์เคลื่อนที่ก่อนการใช้งาน และทบทวนทะเบียนอุปกรณ์ดังกล่าวอย่างน้อยปีละ 1 ครั้งหรือเมื่อมีการยกเลิกการใช้งานหรือมีการเปลี่ยนอุปกรณ์เคลื่อนที่
2. ในกรณีที่มีการใช้ระบบเครือข่ายคอมพิวเตอร์เพื่อการประมวลผลตามความต้องการของผู้ใช้งาน (Cloud Computing) จะต้องจัดให้มีมาตรการที่ครอบคลุมเรื่องดังต่อไปนี้
   - 2.1 ข้อตกลงร่วมกันระหว่างผู้ให้บริการและบริษัท ซึ่งต้องมีรายละเอียดในเรื่องดังต่อไปนี้เป็นอย่างน้อย

พิมพ์พงษ์

2.1.1 หน้าที่และความรับผิดชอบของผู้ให้บริการ รวมถึงความรับผิดต่อบริษัทในกรณีที่ผู้ให้บริการไม่สามารถปฏิบัติตามข้อตกลงได้

2.1.2 ขั้นตอนการปฏิบัติงานที่เป็นไปตามมาตรฐานการรับรองความมั่นคงปลอดภัยด้านสารสนเทศในระดับสากล

2.1.3 มาตรการการรักษาความมั่นคงปลอดภัย การควบคุมการเข้าถึง และการเปิดเผยข้อมูลสารสนเทศ

2.1.4 การตรวจสอบการปฏิบัติงานจากผู้ตรวจสอบที่เป็นอิสระ

2.1.5 เงื่อนไขในกรณีที่ผู้ให้บริการจะให้ผู้ให้บริการรายอื่นรับดำเนินการช่วง (Subcontract of the cloud provider) และข้อกำหนดความรับผิดต่อความเสียหายที่อาจเกิดขึ้นจากการดำเนินการของผู้ให้บริการรายอื่น

2.2 คุณสมบัติด้านความปลอดภัยของผู้ให้บริการรายอื่นที่รับดำเนินการช่วงซึ่งเทียบเท่ากับผู้ให้บริการหรือเป็นไปตามมาตรฐานสากล

2.3 การติดตาม ประเมิน และทบทวนการให้บริการของผู้ให้บริการ

2.4 ขั้นตอนในการโอนย้ายข้อมูลไปยังให้ผู้ให้บริการรายใหม่ ในกรณีที่มีการเปลี่ยนแปลงผู้ให้บริการ

3) โครงสร้างการบริหารจัดการ

บริษัทจะต้องจัดให้มีโครงสร้างการบริหารงานเพื่อรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (organization of information security) ตามหลักเกณฑ์ดังต่อไปนี้

(1) กำหนดรายละเอียดเกี่ยวกับหน้าที่และความรับผิดชอบในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศเป็นลายลักษณ์อักษร และแนวทางในการปฏิบัติหน้าที่ ให้กับบุคลากรของบริษัท

(2) สอบทานการปฏิบัติงานเพื่อป้องกันความเสี่ยงในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศที่อาจเกิดขึ้นในการปฏิบัติหน้าที่

(3) จัดให้มีช่องทางในการติดต่อสำนักงาน หน่วยงานกำกับดูแลด้านเทคโนโลยีสารสนเทศ และหน่วยงานของผู้ให้บริการที่สนับสนุนการทำงานระบบสารสนเทศของบริษัท โดยต้องการปรับปรุงรายชื่อและช่องทางสำหรับติดต่อดังกล่าวให้เป็นปัจจุบัน

4) การบริหารจัดการเหตุการณ์

บริษัทจะต้องจัดให้มีการบริหารจัดการเหตุการที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (information security incident management) ให้เป็นไปตามหลักเกณฑ์ดังต่อไปนี้

(1) กำหนดขั้นตอนและกระบวนการในการบริหารจัดการเหตุการณ์ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ

(2) กำหนดผู้มีหน้าที่รับผิดชอบในการบริหารจัดการเหตุการณ์ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ

(3) รายงานต่อผู้มีหน้าที่รับผิดชอบในการบริหารจัดการเหตุการณ์ตาม (2) และสำนักงาน ก.ล.ต. โดยไม่ชักช้าเมื่อเกิดเหตุการณ์ดังกล่าว

(4) ทดสอบขั้นตอนและกระบวนการในการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศตาม (1) อย่างน้อยปีละ 1 ครั้ง โดยอย่างน้อยต้องครอบคลุมถึงการบริหารจัดการความเสี่ยงไซเบอร์ (cyber security drill)

(5) พิจารณาทบทวนขั้นตอนและกระบวนการในการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ หลังจากที่มีการทดสอบตาม (4) แล้วอย่างน้อยปีละ 1 ครั้ง

(6) จัดให้มีการประเมินผลการทดสอบตาม (4) และประเมินผลพิจารณาทบทวนตาม (5) โดยต้องรายงานผลต่อคณะกรรมการบริษัท หรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการบริษัท อย่างน้อยปีละ 1 ครั้ง ทั้งนี้ การดำเนินการดังกล่าวต้องกระทำโดยบุคคลที่เป็นอิสระจากผู้มีหน้าที่รับผิดชอบในการบริหารจัดการเหตุการณ์ตาม (2)

(7) จัดเก็บเอกสารหลักฐานที่เกี่ยวข้องกับการดำเนินการในการบริหารจัดการเหตุการณ์ดังกล่าวเป็นระยะเวลาไม่น้อยกว่า 2 ปีนับแต่วันที่จัดทำเอกสารนั้น โดยต้องเก็บรักษาไว้ในลักษณะที่พร้อมให้สำนักงาน ก.ล.ต. สามารถเรียกดูและตรวจสอบได้โดยไม่ชักช้า

5) การบริหารความต่อเนื่องในธุรกิจ

บริษัทต้องมีการบริหารความต่อเนื่องในธุรกิจในด้านความมั่นคงปลอดภัยของระบบสารสนเทศ (information security of business continuity management)ให้เป็นไปตามหลักเกณฑ์ดังต่อไปนี้

(1) กำหนดมาตรการรองรับสำหรับกรณีที่อาจเกิดเหตุการณ์ไม่พึงประสงค์

(2) กำหนดขั้นตอน กระบวนการดำเนินการ และการควบคุม เกี่ยวกับความมั่นคงปลอดภัยของระบบสารสนเทศให้สอดคล้องกับแผนบริหารความต่อเนื่องทางธุรกิจ

(3) กำหนดระยะเวลาในการกลับคืนสู่สภาพการดำเนินงานปกติของระบบสารสนเทศและจัดลำดับการกู้คืนระบบงานสารสนเทศที่มีความสำคัญให้สอดคล้องกับผลกระทบที่อาจเกิดขึ้น

(4) มีระบบสารสนเทศสำรองอยู่ในสภาพพร้อมใช้งาน ซึ่งต้องสอดคล้องกับระยะเวลาในการกลับคืนสู่สภาพการดำเนินงานตามปกติของระบบสารสนเทศตาม (3)

6) การสร้างความตระหนักรู้

บริษัทต้องสร้างความตระหนักรู้เกี่ยวกับนโยบายและมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศให้แก่บุคลากรของบริษัทและบุคคลภายนอก (human resource security) ที่มีการปฏิบัติงานโดยมีการเข้าถึงข้อมูลหรือระบบงานภายในองค์กร และดำเนินการให้บุคลากรดังกล่าวสามารถปฏิบัติหน้าที่ได้ตามนโยบายและมาตรการที่กำหนด ทั้งนี้ ตามหลักเกณฑ์ดังต่อไปนี้

(1) ให้ความรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศที่เกี่ยวข้องกับการปฏิบัติหน้าที่แก่บุคลากรของบริษัทและบุคคลภายนอกที่ปฏิบัติงานดังกล่าว

(2) สื่อสารให้บุคลากรของบริษัทและบุคลากรภายนอกที่ปฏิบัติงานดังกล่าว ระมัดระวังและงดเว้นการใช้งานระบบสารสนเทศในลักษณะที่อาจก่อให้เกิดความเสียหายแก่บริษัทหรือตลาดทุนโดยรวม หรือกระทบต่อความมั่นคงของประเทศ และต้องรายงานผู้มีหน้าที่รับผิดชอบในการบริหารจัดการเหตุการณ์ที่ส่งผล

พิมพ์พร

กระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศโดยไม่ชักช้าเมื่อพบความผิดปกติใด ๆ อย่างมีนัยสำคัญ

(3) กำหนดมาตรการในการลงโทษบุคลากรที่มีพฤติกรรมฝ่าฝืนหรือไม่ปฏิบัติตามนโยบายหรือหลักเกณฑ์เกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

2.7 การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศและการควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ

1) การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ

บริษัทต้องมีการบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (asset management) ให้เป็นไปตามหลักเกณฑ์ดังต่อไปนี้

(1) กำหนดบุคคลหรือหน่วยงานที่มีหน้าที่ดูแลรับผิดชอบทรัพย์สินด้านเทคโนโลยีสารสนเทศแต่ละประเภทตลอดอายุการใช้งานของทรัพย์สินดังกล่าว

(2) มีข้อกำหนดการใช้งานทรัพย์สินด้านเทคโนโลยีสารสนเทศที่เหมาะสม

(3) มีการทบทวนหน้าที่รับผิดชอบที่มีต่อทรัพย์สินด้านเทคโนโลยีสารสนเทศให้สอดคล้องกับหน้าที่ของผู้ปฏิบัติงานเมื่อมีการเปลี่ยนแปลงหน้าที่และความรับผิดชอบ

ทั้งนี้ ในส่วนของการบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศประเภทฮาร์ดแวร์หรือซอฟแวร์ บริษัทต้องมีการจัดทำและจัดเก็บทะเบียนทรัพย์สินดังกล่าวตลอดจนทบทวนทะเบียนดังกล่าวอย่างน้อยปีละ 1 ครั้งหรือเมื่อมีการเปลี่ยนแปลงทรัพย์สินด้านเทคโนโลยีสารสนเทศอย่างมีนัยสำคัญด้วย

การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศประเภทข้อมูล บริษัทต้องดำเนินการจัดประเภทข้อมูลดังกล่าวตามระดับชั้นความลับและจัดประเภททรัพย์สินด้านเทคโนโลยีสารสนเทศอื่น ๆ ตามลำดับความสำคัญเพื่อให้ทรัพย์สินด้านเทคโนโลยีสารสนเทศได้รับการปกป้องในระดับที่เหมาะสมตามระดับชั้นความลับหรือระดับความสำคัญ แล้วแต่กรณีด้วยและในกรณีที่เป็นข้อมูลสารสนเทศ บริษัทต้องมีกระบวนการการป้องกันการเปิดเผยเปลี่ยนแปลงแก้ไขหรือสร้างความเสียหายต่อข้อมูลสารสนเทศที่สำคัญ ที่ถูกจัดเก็บในสื่อบันทึกข้อมูลด้วย

2) มาตรการเพื่อสร้างความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อมของทรัพย์สินด้านเทคโนโลยีสารสนเทศ

บริษัทต้องมีมาตรการเพื่อสร้างความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (physical and environmental security) ของทรัพย์สินด้านเทคโนโลยีสารสนเทศตามหลักเกณฑ์ดังต่อไปนี้

(1) ประเมินความเสี่ยงและความสำคัญของทรัพย์สินด้านเทคโนโลยีสารสนเทศ

(2) กำหนดพื้นที่หวงห้ามและพื้นที่สำหรับจัดวางทรัพย์สินด้านเทคโนโลยีสารสนเทศที่มีความสำคัญให้มีความมั่นคงปลอดภัยและป้องกันมิให้บุคคลที่ไม่เกี่ยวข้องเข้าถึงพื้นที่ดังกล่าว

ในกรณีที่เป็นทรัพย์สินด้านเทคโนโลยีสารสนเทศฮาร์ดแวร์ บริษัทต้องมีมาตรการป้องกันทรัพย์สินดังกล่าวมิให้เกิดความเสียหาย สูญหาย ถูกโจรกรรม เข้าถึง หรือถูกใช้งานโดยบุคคลที่ไม่เกี่ยวข้อง เพื่อให้สามารถปฏิบัติงานได้อย่างต่อเนื่อง

3) **ควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ**

บริษัทต้องมีการควบคุมการเข้าถึงระบบและข้อมูลสารสนเทศ (access control) ให้เป็นไปตามหลักเกณฑ์ดังต่อไปนี้

(1) มีการบริหารจัดการบัญชีผู้ใช้งานโดยจำกัดการเข้าถึงข้อมูลสารสนเทศ ให้สามารถเข้าถึงได้เฉพาะบุคคลที่ได้รับสิทธิ์การเข้าถึงดังนี้

(ก) มีการลงทะเบียนบัญชีผู้ใช้งานระบบสารสนเทศ

(ข) มีการจัดสรรสิทธิ์การเข้าถึงระดับสูงอย่างจำกัดและมีการควบคุมการเข้าถึงสิทธิ์ดังกล่าวอย่างเคร่งครัด

(ค) มีขั้นตอนการบริหารจัดการในการกำหนดรหัสผ่านอย่างเหมาะสม

(ง) มีการติดตามและทบทวนระดับสิทธิ์การเข้าถึงอย่างสม่ำเสมอ

(2) มีข้อกำหนดให้ผู้ใช้งานปฏิบัติตามขั้นตอนการใช้งานและดูแลรับผิดชอบรหัสผ่านอย่างมั่นคงปลอดภัย

(3) มีการป้องกันมิให้มีการเข้าถึงระบบสารสนเทศและโปรแกรมประยุกต์ (application software) โดยไม่ได้รับอนุญาต ดังนี้

(ก) ควบคุมการเข้าถึงข้อมูลสารสนเทศและฟังก์ชั่นต่าง ๆ ในโปรแกรมประยุกต์ของผู้ใช้งานและผู้ดูแลระบบสารสนเทศ ให้สอดคล้องกับสิทธิ์ที่ได้รับ

(ข) ควบคุมการเข้าใช้งานระบบสารสนเทศและโปรแกรมประยุกต์

(ค) จัดให้มีระบบการบริหารจัดการรหัสผ่านที่มีความมั่นคงปลอดภัย

(ง) จำกัดการใช้งานโปรแกรมอรรถประโยชน์ต่าง ๆ (utility program) และจำกัดการเข้าถึงชุดคำสั่งควบคุมการทำงานของโปรแกรมอย่างเข้มงวด

2.8 การรักษาความมั่นคงปลอดภัยด้านการสื่อสารข้อมูลสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์และการรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ

1) การรักษาความมั่นคงปลอดภัยด้านการสื่อสารข้อมูลสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์ (Communication Security)

บริษัทต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยด้านการสื่อสารข้อมูลสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์ (communications security) ให้เป็นไปตามหลักเกณฑ์ดังต่อไปนี้

(1) มีการบริหารจัดการและควบคุมระบบเครือข่ายคอมพิวเตอร์อย่างมั่นคงและปลอดภัย โดยต้องสามารถป้องกันมิให้เกิดการกระทำที่มีความเสี่ยงต่อข้อมูลสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์

(2) จัดทำข้อตกลงการใช้บริการผ่านระบบเครือข่ายคอมพิวเตอร์ที่เกี่ยวกับวิธีการบริหารจัดการ คุณภาพการให้บริการ และกระบวนการรักษาความมั่นคงปลอดภัยของระบบเครือข่ายคอมพิวเตอร์กับผู้รับดำเนินการ

(3) แบ่งแยกระบบเครือข่ายคอมพิวเตอร์ตามความเหมาะสม โดยระบุขอบเขตของระบบเครือข่ายย่อยอย่างชัดเจน และมีกระบวนการควบคุมการเข้าถึงขอบเขตดังกล่าวอย่างเหมาะสม

(4) กำหนดมาตรการในการรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศที่มีการรับส่งผ่านระบบเครือข่ายคอมพิวเตอร์

พิมพ์พม

(5) ดำเนินการให้บุคลากรของบริษัทและผู้รับดำเนินการ (ถ้ามี) มีข้อตกลงเกี่ยวกับการรักษาความลับหรือไม่เปิดเผยข้อมูลที่มีความสำคัญ

2) การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ (Operation Security)

บริษัทต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ (operations security) ตามหลักเกณฑ์ดังต่อไปนี้

(1) กำหนดขั้นตอนการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศเพื่อให้การปฏิบัติงานนั้นเป็นไปอย่างถูกต้องและมั่นคงปลอดภัย

(2) มีมาตรการป้องกันและตรวจสอบโปรแกรมไม่ประสงค์ดี (malware) และมาตรการในการแก้ไขระบบสารสนเทศให้สามารถกลับมาใช้งานได้ตามปกติ

(3) มีการสำรองข้อมูลสำคัญทางธุรกิจ ระบบปฏิบัติการ โปรแกรมประยุกต์ ระบบงานคอมพิวเตอร์ และชุดคำสั่งที่ใช้ทำงาน ไว้อย่างครบถ้วน และต้องมีการทดสอบข้อมูลสำรองและกระบวนการกู้คืนข้อมูลอย่างน้อยปีละ 1 ครั้ง

(4) จัดเก็บและบันทึกหลักฐาน (logs) ต่าง ๆ ให้ครบถ้วนและเพียงพอสำหรับการตรวจสอบการล่วงรู้ข้อมูลภายในระหว่างหน่วยงานและบุคลากร การสอบทานการใช้งานข้อมูลและระบบสารสนเทศตามหน้าที่ที่ผู้ปฏิบัติงานได้รับมอบหมาย การตรวจสอบการเข้าใช้งานระบบสารสนเทศที่มีความผิดปกติหรือไม่เป็นไปตามกฎหมายหรือกฎเกณฑ์ที่เกี่ยวข้อง และการตรวจสอบตัวตนของลูกค้าที่ทำรายการซื้อขายผ่านระบบอิเล็กทรอนิกส์ ทั้งนี้ ต้องมีการติดตามและวิเคราะห์หลักฐานที่จัดเก็บสำหรับการใช้งานสารสนเทศที่มีความสำคัญให้สอดคล้องกับการประเมินความเสี่ยงขององค์กร

(5) มีขั้นตอนควบคุมการติดตั้งซอฟท์แวร์บนระบบงาน และมีมาตรการจำกัดการติดตั้งซอฟท์แวร์โดยผู้ใช้งานเพื่อให้ระบบปฏิบัติงานต่าง ๆ มีความถูกต้องครบถ้วนและน่าเชื่อถือ

(6) มีระบบในการบริหารจัดการกรณีช่องโหว่ทางเทคนิค (technical vulnerability management) ที่อาจเกิดขึ้นอย่างเพียงพอและเหมาะสมดังนี้

(ก) มีการทดสอบการเจาะระบบ (penetration test) กับระบบงานที่มีความสำคัญที่เชื่อมต่อกับระบบเครือข่ายภายนอก (untrusted network) โดยบุคคลที่เป็นอิสระจากหน่วยงานที่รับผิดชอบด้านเทคโนโลยีสารสนเทศ และเป็นไปตามการวิเคราะห์ความเสี่ยงและผลกระทบทางธุรกิจ (risk and business impact analysis) ดังนี้

- กรณีที่เป็นระบบงานสำคัญที่ประเมินแล้วมีความสำคัญสูง ต้องทดสอบอย่างน้อยทุก 3 ปีและเมื่อมีการเปลี่ยนแปลงระบบงานดังกล่าวอย่างมีนัยสำคัญ
- กรณีที่เป็นระบบงานที่มีความสำคัญอื่น ๆ ต้องทดสอบอย่างน้อยทุก 6 ปี

(ข) มีการประเมินช่องโหว่ของระบบ (vulnerability assessment) กับระบบงานที่มีความสำคัญทุกระบบอย่างน้อยปีละ 1 ครั้งและเมื่อมีการเปลี่ยนแปลงระบบงานดังกล่าวอย่างมีนัยสำคัญและรายงานผลไปยังหน่วยงานกำกับดูแลการปฏิบัติงานหรือหน่วยงานตรวจสอบภายในโดยไม่ชักช้า

(7) มีการตรวจสอบระบบสารสนเทศดังนี้

(ก) วางแผนการตรวจสอบระบบสารสนเทศให้สอดคล้องกับความเสี่ยงที่ได้ประเมินไว้

(ข) กำหนดขอบเขตในการตรวจสอบระบบสารสนเทศทางเทคนิคให้ครอบคลุมถึงจุดเสี่ยงที่สำคัญ โดยการตรวจสอบดังกล่าวต้องไม่กระทบต่อการปฏิบัติงาน

(ค) ตรวจสอบระบบสารสนเทศนอกเวลาทำงาน ในกรณีที่การตรวจสอบนั้นอาจส่งผลกระทบต่อความพร้อมในการใช้งานระบบดังกล่าว

2.9 หลักเกณฑ์เพิ่มเติมอื่น ๆ

1) การจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศ

บริษัทต้องมีหลักเกณฑ์ในการการจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศ (System acquisition , development and maintenance) ดังนี้

(1) มีข้อกำหนดในการจัดหา พัฒนา และการดูแลรักษาระบบสารสนเทศให้มีความมั่นคงปลอดภัย เมื่อมีระบบสารสนเทศใหม่หรือมีการปรับปรุงระบบเดิม

(2) จัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศ ในกรณีที่มีการเข้าถึงระบบการให้บริการการใช้งาน (application service)

(3) มีการควบคุมการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบสารสนเทศในทุกขั้นตอนให้เป็นไปตามขั้นตอนการควบคุมความมั่นคงปลอดภัยด้านสารสนเทศที่กำหนดไว้

(4) มีการทดสอบระบบสารสนเทศที่ได้รับการพัฒนาหรือแก้ไขเปลี่ยนแปลง เพื่อให้มั่นใจได้ว่าระบบสารสนเทศดังกล่าวทำงานได้อย่างมีประสิทธิภาพ สามารถประมวลผลได้อย่างถูกต้องครบถ้วนและเป็นไปตามความต้องการของผู้ใช้งาน

(5) ปรับปรุงแผนบริหารความต่อเนื่องทางธุรกิจให้สอดคล้องกับการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบสารสนเทศ

(6) มีการควบคุมบุคลากร ขั้นตอน และเทคโนโลยีสำหรับการพัฒนาระบบสารสนเทศให้มีความมั่นคงปลอดภัยตลอดขั้นตอนการพัฒนาระบบ

(7) มีการดูแล ติดตาม และควบคุมการพัฒนาระบบสารสนเทศของผู้รับดำเนินการให้เป็นไปตามข้อตกลงการใช้บริการ

(8) มีการทดสอบการทำงานของระบบสารสนเทศที่ได้รับการพัฒนา โดยผู้ใช้งานหรือผู้ทดสอบที่เป็นอิสระจากผู้พัฒนาระบบสารสนเทศดังกล่าว

2) การแต่งตั้งบุคคลอื่นเป็นผู้รับดำเนินการ

ในกรณีที่บริษัทมีการแต่งตั้งบุคคลอื่นเป็นผู้รับดำเนินการในงานที่เกี่ยวกับระบบสารสนเทศของบริษัท บริษัทต้องดำเนินการให้เป็นไปตามหลักเกณฑ์ดังต่อไปนี้

(1) มีข้อตกลงและกระบวนการควบคุมเกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศอย่างเป็นลายลักษณ์อักษรในการใช้บริการจากผู้รับดำเนินการ โดยบริษัทและผู้รับดำเนินการ ต้องมีการลงนามร่วมกันในข้อตกลงและกระบวนการดังกล่าว

(2) มีการติดตาม ประเมิน ทบทวน และตรวจสอบผู้รับดำเนินการอย่างสม่ำเสมอ

(3) มีการประเมินความเสี่ยงและกำหนดกระบวนการการบริหารจัดการความเสี่ยงในกรณีที่ผู้รับดำเนินการมีการเปลี่ยนแปลงกระบวนการ ขั้นตอน หรือวิธีการปฏิบัติงานในการรักษาความมั่นคงปลอดภัยในการปฏิบัติงาน หรือเปลี่ยนตัวผู้รับดำเนินการ

(4) มีมาตรการตรวจสอบดูแลให้ผู้รับดำเนินการปฏิบัติตามหลักเกณฑ์การปฏิบัติงานที่สำนักงาน ก.ล.ต. หรือคณะกรรมการกำกับตลาดทุน กำหนดเกี่ยวกับงานที่รับดำเนินการ รวมทั้ง ระเบียบวิธีปฏิบัติที่บริษัทกำหนดขึ้นเพื่อให้เป็นไปตามหลักเกณฑ์ดังกล่าว โดยอย่างน้อยมาตรการดังกล่าวต้องสามารถควบคุมให้ผู้รับดำเนินการไม่มีลักษณะที่จะทำให้มีเหตุอันควรเชื่อได้ว่ามีข้อบกพร่องหรือไม่มีความเหมาะสมเกี่ยวกับการควบคุมและการปฏิบัติงานอันดีของธุรกิจ

(5) มีแผนรองรับในกรณีที่เกิดเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (incident response policy)

(6) กำหนดสิทธิ์ในการเข้าตรวจสอบกระบวนการปฏิบัติงานของผู้รับดำเนินการและควบคุมให้การปฏิบัติงานเป็นไปตามข้อตกลงที่กำหนดไว้ เว้นแต่ในกรณีที่ผู้รับดำเนินการมีข้อจำกัดในการเข้าตรวจสอบการปฏิบัติงานดังกล่าว บริษัทต้องมีมาตรการเพื่อให้มั่นใจได้ว่าสามารถควบคุมการปฏิบัติงานของผู้รับดำเนินการให้เป็นไปตามข้อตกลงที่กำหนดไว้ได้

(7) มีข้อกำหนดให้ผู้รับดำเนินการยินยอมให้สำนักงาน ก.ล.ต. เรียกดู ตรวจสอบเอกสารหลักฐานที่เกี่ยวข้องหรือสามารถเข้าตรวจสอบการปฏิบัติงานของผู้รับดำเนินการ

นโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศ ฉบับนี้ ได้รับการอนุมัติจากที่ประชุมคณะกรรมการบริษัท ครั้งที่ 5/2568 เมื่อวันที่ 16 ธันวาคม 2568 โดยมีผลบังคับใช้ตั้งแต่วันที่ 16 ธันวาคม 2568

.....

(นางเสาวนีย์ กมลบุตร)

ประธานกรรมการบริษัท

บริษัทหลักทรัพย์จัดการกองทุน ไอร่า จำกัด

พิมพ์พ

ประวัติการทบทวนนโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศ (IT Governance Policy)

นโยบาย	ผลการทบทวน	ผู้ทบทวน	ผู้สอบทาน
นโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศ (IT Governance Policy) (ฉบับทบทวนปี 2568)	1. แก้ไขและเพิ่มเติมคำจำกัดความในนโยบายให้สอดคล้องกับประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ที่ สธ. 33/2567 เรื่อง ข้อกำหนดในรายละเอียดเกี่ยวกับการจัดให้มีระบบเทคโนโลยีสารสนเทศ (ฉบับที่ 2) 2. แก้ไขเลขที่ประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ที่ใช้อ้างอิงในหัวข้อ “วัตถุประสงค์”	พิมพ์พร กอเซ็ม นางสาวพิมพ์พร กอเซ็ม วันที่ 16/12/2568	..... นายธนิต เวียนวัฒนะ วันที่ 16/12/2568 ..... นายวุฒิพงษ์ วัชรมัย วันที่ 16/12/2568