MC GROUP

บริษัท แม็คกรุ๊ป จำกัด (มหาชน)

Mc group public company limited.

นโยบาย
การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
(Information Security Management System Policy: ISMS Policy)

สารบัญ

1. บทบาทและหน้าที่ด้านความมั่นคงปลอดภัย (Information Security Role and Responsibility)

บทบาท	หน้าที่ความรับผิดชอบ
กรรมการผู้จัดการบริษัทฯ หรือ ผู้บริหารสูงสุดของบริษัทฯ (Top Management)	บุคคลที่มีอำนาจหน้าที่ในการบริหารจัดการระบบความมั่นคงความปลอดภัย จัดสรรทรัพยากร รวมถึงการรับทราบและตัดสินใจ ดำเนินการประเด็นสำคัญต่าง ๆ ที่เกิดขึ้น
คณะกรรมการบริหารจัดการความมั่นคงปลอดภัย หรือ คณะ ISMS-C (ISMS Committee)	กลุ่มพนักงานที่ได้รับมอบหมายจากกรรมการผู้จัดการบริษัทฯ ให้มีอำนาจในการบริหารจัดการระบบบริหารจัดการความมั่นคงปลอดภัยตามขอบเขตของนโยบายนี้
คณะทำงานตรวจสอบระบบ ISMS หรือ คณะทำงานตรวจสอบ (Auditor Team)	กลุ่มพนักงานที่ได้รับมอบหมายจากบริษัทฯ ให้ทำหน้าที่ตรวจสอบระบบ ISMS ของบริษัทฯ ตามขอบเขตของนโยบายฉบับนี้ ซึ่งโดยรวมมีหน้าที่ ดังนี้ • จัดทำแผนการตรวจสอบและติดตามระบบ ISMS • นำเสนอรายงานผลการตรวจสอบเพื่อขอให้ผู้รับตรวจดำเนินการแก้ไขหรือป้องกันตามความจำเป็น • ประสานงานกับผู้ที่เกี่ยวข้องพร้อมติดตามการขอให้ดำเนินแก้ไขหรือปรับปรุงในสิ่งที่ตรวจพบและไม่สอดคล้องกับระบบ ISMS จนกระทั่งสามารถปิดสิ่งที่ตรวจพบนั้น
ตัวแทนการจัดการ (Information Security Management Representative: ISMR)	ผู้ที่ได้รับมอบหมายจากคณะกรรมการ ISMS-C ให้ศึกษา ทำความเข้าใจ และเป็นผู้แทนในการให้ข้อมูลเกี่ยวกับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศทั้งระบบตามข้อกำหนดของมาตรฐานที่บริษัทฯ นำมาประยุกต์ใช้ รวมถึง • ประสานงานระหว่างทีมงานและผู้จัดทำนโยบายความมั่นคงปลอดภัยข้อมูลสารสนเทศ (Information Security Policy) • เมื่อเปลี่ยนแปลงนโยบายความมั่นคงปลอดภัยข้อมูลสารสนเทศ (Information Security Policy) ต้องทำหน้าที่ แจ้งให้ทีมผู้ปฏิบัติงานทุกท่านได้รับทราบและชี้แจ้งทำความเข้าใจ นโยบายความมั่นคงปลอดภัยข้อมูลสารสนเทศ (Information Security Policy) ที่ประกาศใช้งานใหม่ • จัดเก็บและควบคุมบริหารจัดการเอกสารและข้อมูลที่เกี่ยวข้องตามความต้องการของระบบ ISMS ตลอดจนบันทึกต่าง ๆ ที่เกี่ยวข้องกับระบบ ISMS ที่ใช้งานอยู่ให้เป็นปัจจุบัน และควบคุมผู้เข้าถึงเอกสารดังกล่าว ตลอดจนดำเนินการควบคุมการอนุมัติการเปลี่ยนแปลงแก้ไขเอกสาร

บทบาท	หน้าที่ความรับผิดชอบ
	• ติดตามผลของความไม่สอดคล้องกับมาตรฐาน (Non-Conformity: NC) ที่เกิดขึ้นจากการตรวจสอบภายในและเสนอผลของการติดตามดังกล่าวในที่ประชุมฯ
พนักงานบริษัทฯ	มีหน้าที่ดำเนินการตามระบบ ISMS ของบริษัทฯ รวมถึงปฏิบัติตามนโยบาย ขั้นตอนปฏิบัติ กระบวนการ แผนการ คู่มือการปฏิบัติงานหรือเอกสารที่เกี่ยวข้องกับการดำเนินงานต่าง ๆ รวมถึงการรายงานด้านความมั่นคงปลอดภัยสารสนเทศต่าง ๆ

2. อภิธานคำศัพท์/คำย่อ (Glossary/Acronym)

อภิธานคำศัพท์/คำย่อ	คำอธิบาย
บริษัทฯ	บริษัท แม็คกรุ๊ป จำกัด (มหาชน)
ขอบเขตการดำเนินงาน (ISMS Scope of Work)	ขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ซึ่งดำเนินการให้กับบริษัทฯ รวมถึงพนักงานบริษัทฯ หรือผู้ให้บริการภายนอก ที่เกี่ยวข้องกับบริษัทฯ
ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System: ISMS) หรือ ระบบ ISMS	การบริหารจัดการความมั่นคงปลอดภัยโดยพิจารณาจากความเสี่ยงที่เกี่ยวข้องกับทรัพย์สินสารสนเทศของบริษัทฯ กำหนดมาตรการลดความเสี่ยง ดำเนินการตามมาตรการที่กำหนดไว้ เฝ้าระวัง (เพื่อตรวจสอบปัญหาที่เกี่ยวข้อง) ทบทวน รักษา และปรับปรุงความมั่นคงปลอดภัยสำหรับทรัพย์สินสารสนเทศให้ดียิ่งขึ้น ระบบ ISMS นี้มีจุดประสงค์เพื่อให้สอดคล้องกับการปฏิบัติตามมาตรฐาน ISO/IEC 27001:2022
ความมั่นคงปลอดภัย	การสร้างหรือการรักษาความมั่นคงปลอดภัยให้กับทรัพย์สินสารสนเทศที่บริษัทฯ ดูแลและรับผิดชอบ ทั้งนี้เพื่อป้องกันการสูญเสีย การสูญหาย การถูกขโมย การเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผยโดยไม่ได้รับอนุญาต การปลอมแปลง การปฏิเสธความรับผิดชอบ หรือ การกระทำใด ๆ ก็ตามที่ก่อให้เกิดการความเสียหายต่อองค์ประกอบทางด้านความมั่นคงปลอดภัย 3 ส่วน ดังนี้ • ความลับ (Confidentiality) คือ ทรัพย์สินสารสนเทศจะต้องสามารถเข้าถึงได้โดยผู้ที่ได้รับอนุญาตแล้วเท่านั้น • ความถูกต้อง (Integrity) คือ ทรัพย์สินสารสนเทศจะต้องมีความถูกต้องและสมบูรณ์การเปลี่ยนแปลงสามารถทำได้ แต่ต้องได้รับ

อภิธานคำศัพท์/คำย่อ	คำอธิบาย
	อนุญาตแล้วเท่านั้น • ความพร้อมใช้ (Availability) คือ ทรัพย์สินสารสนเทศจะต้องสามารถเข้าถึงได้เมื่อมีความจำเป็นต้องใช้งาน
นโยบายการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Policy)	แนวทางการปฏิบัติตามระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC 27001:2022 ที่ให้บริษัทฯ ได้ยึดเป็นแนวทางการดำเนินการหรือประยุกต์เข้ากับการดำเนินงานทางเทคโนโลยีสารสนเทศของบริษัทฯ
นโยบายความมั่นคงปลอดภัยข้อมูลสารสนเทศ (Information Security Policy)	ข้อกำหนด ระเบียบ แนวทางปฏิบัติ หรือสิ่งที่ต้องการให้พนักงานหรือผู้ที่เกี่ยวข้องอื่น ๆ ปฏิบัติตามที่เกี่ยวข้องกับสารสนเทศและเทคโนโลยีสารสนเทศของบริษัทฯ โดยทั่วไปนโยบายนี้จะมีการกำหนดให้จัดทำ ปรับปรุง รวมทั้งประกาศการใช้งานโดยคณะ ISMS-C ของบริษัทฯ การปฏิบัติตามจะส่งผลให้ลดความเสี่ยงต่าง ๆ ได้ เช่น ลดความเสี่ยงในการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต ลดการแพร่กระจายของโปรแกรมไม่พึงประสงค์ ลดการหยุดชะงักของระบบให้บริการต่าง ๆ เป็นต้น
มาตรการ (Control)	วิธีการที่ใช้ในการบริหารจัดการความเสี่ยง ซึ่งรวมถึงนโยบาย ขั้นตอนปฏิบัติ แนวทางปฏิบัติ วิธีปฏิบัติ หรือโครงสร้างของบริษัทฯ วิธีการเหล่านี้อาจเป็นการจัดการ การบริหาร วิธีการทางเทคนิค หรือเกิดจากกฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดที่องค์กรต้องปฏิบัติตาม
ทรัพย์สินสารสนเทศ	ทรัพย์สินสารสนเทศของบริษัทฯ ที่อยู่ในขอบเขตการดำเนินบริหารจัดการประกอบด้วยทรัพย์สินสารสนเทศในหมวดหมู่ต่าง ๆ เช่น ข้อมูล (Information) พนักงาน (People) ฮาร์ดแวร์ (Hardware) ซอฟต์แวร์ (Software) บริการที่ได้รับและใช้ประโยชน์จากระบบเทคโนโลยีสารสนเทศ (Service from Third-Party) เป็นต้น
ผู้ให้บริการภายนอก (Third-Party)	ผู้ให้บริการด้านเทคโนโลยีสารสนเทศให้กับบริษัทฯ เหตุการณ์ความเสี่ยง หมายถึง เหตุการณ์ที่มีโอกาสเกิดขึ้นได้และทำให้เกิดความเสียหายต่อทรัพย์สินสารสนเทศของบริษัทฯ เช่น ไวรัสทำให้ข้อมูลเสียหาย ข้อมูลสำคัญถูกขโมยซึ่งอาจทำให้บริษัทฯ สูญเสียข้อได้เปรียบด้านการแข่งขัน หน้าเว็บไซต์ถูกเปลี่ยนแปลงแก้ไขซึ่งอาจทำให้บริษัทฯ เสียชื่อเสียง
ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite หรือ Acceptable Level of Risk)	ค่าความเสี่ยงที่หากการประเมินเหตุการณ์ความเสี่ยงหนึ่งมีค่าน้อยกว่าค่าที่ยอมรับได้นี้จะถือว่าทรัพย์สินสารสนเทศที่เกี่ยวข้องกับเหตุการณ์ฯ มีความมั่นคงปลอดภัยเพียงพอ (และผู้ประเมินความเสี่ยงไม่จำเป็นต้องนำเสนอ

อภิธานคำศัพท์/คำย่อ	คำอธิบาย
	แผนการลดความเสี่ยงใด ๆ เพิ่มเติม)
แผนการลดความเสี่ยง (Risk Treatment Plan)	แผนการจัดการกับเหตุการณ์ความเสี่ยงสำหรับกรณีที่ผู้ประเมินความเสี่ยงได้ประเมินเหตุการณ์ความเสี่ยงหนึ่งและพบว่ามีความเสี่ยงเกินกว่าระดับความเสี่ยงที่ยอมรับได้ ผู้ประเมินความเสี่ยงจะต้องนำเสนอแผนการจัดการดังกล่าวต่อหัวหน้าทีมเพื่อพิจารณาอนุมัติการดำเนินการ
เอกสารแสดงการประยุกต์ใช้มาตรการ (Statement of Applicability: SoA)	เอกสารแสดงหรือระบุมาตรการข้อใดในมาตรฐาน ISO/IEC 27001:2022 ที่บริษัทฯ ได้มีการนำมาใช้งานและเหตุผลของการใช้ รวมทั้ง มาตรการข้อใดที่ไม่ได้นำมาใช้งานและเหตุผลที่ไม่ได้ใช้งาน
ระบบเทคโนโลยีสารสนเทศ (ระบบ) หรือโครงสร้างพื้นฐานสารสนเทศ หรือ สิ่งอำนวยความสะดวก (Facility)	ระบบเทคโนโลยีสารสนเทศของ บริษัท แม็คกรุ๊ป จำกัด (มหาชน) หรือโครงสร้างพื้นฐานสารสนเทศ หรือ สิ่งอำนวยความสะดวก (Facility) ของระบบ Cloud Computing และระบบ Monitoring ให้บริการ

3. นโยบายการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Policy)

เพื่อให้ระบบเทคโนโลยีสารสนเทศของ “องค์กร” มีการบริหารจัดการเป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่าง ๆ องค์กรจึงกำหนดนโยบายการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ โดยกำหนดให้มีมาตรฐาน (Standard) แนวปฏิบัติ (Guideline) ขั้นตอนปฏิบัติ (Procedure) ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและป้องกันภัยคุกคามต่าง ๆ ดังนี้

1. จัดทำนโยบายการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศเพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศขององค์กรให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล และเหมาะสมกับวัตถุประสงค์ขององค์กร
2. กำหนดขอบเขตของบริหารจัดการความมั่นคงปลอดภัยสารสนเทศโดยใช้แนวทางอ้างอิงตามมาตรฐาน ISO/IEC 27001:2022
3. เผยแพร่นโยบายการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับองค์กร ได้รับทราบและปฏิบัติตามอย่างเคร่งครัด
4. กำหนดมาตรฐาน แนวทางปฏิบัติและวิธีปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับองค์กร ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กรในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด อ้างอิงตามมาตรฐาน ISO/IEC 27001:2022

5. ดำเนินการสอบทาน ทบทวน และปรับปรุงนโยบายความมั่นคงปลอดภัยสารสนเทศตามรอบระยะเวลาอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่เป็นสาระสำคัญต่อการดำเนินงานของบริษัทฯ
6. มุ่งมั่นในการพัฒนาระบบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร และดำเนินการปรับปรุงแก้ไขอย่างต่อเนื่อง

4. วัตถุประสงค์ด้านความมั่งคงปลอดภัยสารสนเทศ (ISMS Objective)

วัตถุประสงค์ คือ ให้บริษัทฯ และบุคคลากรที่อยู่ในขอบเขตมีระบบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ การให้บริการภายในศูนย์ข้อมูลกลาง การให้บริการระบบสนันสนุนโครงสร้างพื้นฐานและระบบเครือข่ายภายในศูนย์ข้อมูลกลาง ของบริษัท แม็คกรุ๊ป จำกัด (มหาชน) เพื่อให้ผู้ใช้บริการมีความเชื่อมั่น และมั่นใจว่าระบบสารสนเทศสามารถทำงานได้อย่างมีประสิทธิภาพ โดยคำนึงถึงความปลอดภัย ความถูกต้อง พร้อมใช้ และปฏิบัติตามข้อกำหนดสากลมาตรฐาน ISO/IEC 27001:2022

5. ขอบเขตระบบบริหารความมั่งคงปลอดภัยสารสนเทศ (ISMS Scope)

ระบบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ การให้บริการภายในศูนย์ข้อมูลกลาง การให้บริการระบบสนันสนุนโครงสร้างพื้นฐานและระบบเครือข่ายภายในศูนย์ข้อมูลกลาง ของบริษัท แม็คกรุ๊ป จำกัด (มหาชน) ตั้งอยู่

- ศูนย์ข้อมูลกลาง (Data Center)
  - บริษัท แม็คกรุ๊ป จำกัด (มหาชน)
    ที่อยู่: 448, 450 ถนนอ่อนนุช เขตประเวศ กรุงเทพฯ 10250
- สำนักงานออฟฟิศ
  - แม็ค ดีไซน์ เซ็นเตอร์
    ที่อยู่: 2 ถนนสุขาภิบาล 2 ซอย 5 เขตประเวศ กรุงเทพฯ 10250
  - แม็ค สตูดิโอ
    ที่อยู่: 4 ถนนสุขาภิบาล 2 ซอย 7 เขตประเวศ กรุงเทพฯ 10250

กรอบการบริหารระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
ของ บริษัท แม็คกรุ๊ป จำกัด (มหาชน)

แม็คกรุ๊ป จำกัด (มหาชน) ใช้กรอบแนวทางการบริหารระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรอ้างอิงมาตรฐาน ISO/IEC 27001: 2022 โดยมีรายละเอียด ดังนี้

1. บริบทขององค์กร (Context of The Organization)

1.1 การทำความเข้าใจองค์กรและบริบทขององค์กร (Understanding the Organization and Its Context)

องค์กรต้องกำหนด ประเด็นภายในและภายนอกองค์กรที่เกี่ยวข้องกับจุดประสงค์ขององค์กรและที่ส่งผลต่อความสามารถในการบรรลุผลลัพธ์ตามที่ต้องการของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

1.2 การกำหนดความจำเป็นและความคาดหวังของผู้ที่เกี่ยวข้อง (Understanding the Needs and Expectations of Interested Parties)

องค์กรต้องกำหนด ผู้ที่เกี่ยวข้อง ซึ่งเป็นผู้ที่เกี่ยวข้องกับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ และความต้องการของผู้ที่เกี่ยวข้องเหล่านั้น ซึ่งเกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ

1.3 การกำหนดขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Determining the Scope of The Information Security Management System)

องค์กรต้องกำหนดกรอบและการประยุกต์ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศเพื่อระบุขอบเขตการดำเนินการ โดยการระบุขอบเขตองค์กรต้องพิจารณา ดังนี้

- ประเด็นภายในและภายนอกองค์กร
- ความคาดหวังของผู้ที่เกี่ยวข้อง
- การเชื่อมโยงและความสัมพันธ์ระหว่างกิจกรรมซึ่งดำเนินการโดยองค์กรและองค์กรอื่น ๆ
- ขอบเขตต้องสามารถเข้าถึงได้โดยจัดทำเป็นลายลักษณ์อักษร

1.4 ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System)

องค์กรต้องกำหนด ลงมือปฏิบัติ บำรุงรักษา และปรับปรุงอย่างต่อเนื่อง ต่อระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ให้ความสอดคล้องกับข้อกำหนดในเอกสารมาตรฐาน ISO/IEC 27001:2022

2. ภาวะผู้นำ (Leadership)

2.1 ภาวะผู้นำและการให้ความสำคัญ (Leadership and Commitment)

ผู้บริหารระดับสูง ต้องแสดงให้เห็นถึงภาวะผู้นำและการให้ความสำคัญต่อระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ โดย

- ต้องทำให้นโยบายความมั่นคงปลอดภัยสารสนเทศและวัตถุประสงค์ความมั่นคงปลอดภัยสารสนเทศมีการกำหนดขึ้นมาและมีความสอดคล้องกับทิศทางเชิงกลยุทธ์ขององค์กร
- ต้องทำให้มั่นใจว่ามีการรวมความต้องการของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ เข้ากับกระบวนการขององค์กร
- ต้องทำให้มีทรัพยากรที่จำเป็นสำหรับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศเพื่อใช้ในการดำเนินการ
- ต้องสื่อสารความสำคัญของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศที่สัมฤทธิ์ผลและของการดำเนินการตามความต้องการของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศที่กำหนดไว้
- ต้องทำให้มั่นใจว่าระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศบรรลุผลลัพธ์ตามที่ต้องการ
- ต้องสั่งการและสนับสนุนบุคลากรเพื่อนำสู่ความสัมฤทธิ์ผลของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
- ต้องส่งเสริมให้มีการปรับปรุงอย่างต่อเนื่อง
- ต้องสนับสนุนบทบาทการบริหารอื่น ๆ ภายใต้ขอบเขตความรับผิดชอบของเพื่อแสดงภาวะผู้นำของตนเอง

2.2 นโยบาย (Policy)

ผู้บริหารระดับสูงต้องกำหนด นโยบายความมั่นคงปลอดภัยสารสนเทศ ดังนี้

- มีความเหมาะสมต่อจุดประสงค์ขององค์กร
- รวมวัตถุประสงค์ความมั่นคงปลอดภัยสารสนเทศไว้ด้วยหรือกำหนดกรอบการปฏิบัติสำหรับการกำหนดวัตถุประสงค์ดังกล่าว
- รวมการให้ความสำคัญของผู้บริหารเพื่อให้สอดคล้องกับความต้องการที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ
- รวมถึงการให้ความสำคัญของผู้บริหารในการปรับปรุงอย่างต่อเนื่องต่อระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

โดย นโยบายความมั่นคงปลอดภัยสารสนเทศ ต้องมีสาระสำคัญ ดังนี้

- ต้องสามารถเข้าถึงได้โดยจัดทำเป็นลายลักษณ์อักษร
- ต้องมีการสื่อสารให้ทราบกันภายในองค์กร
- ต้องสามารถเข้าถึงได้โดยผู้ที่เกี่ยวข้องตามความเหมาะสม

2.3 บทบาท หน้าที่ความรับผิดชอบ และอำนาจหน้าที่ (Organizational Roles, Responsibilities and Authorities)

ผู้บริหารระดับสูงต้องทำให้หน้าที่ความรับผิดชอบและอำนาจหน้าที่ตามบทบาทที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ มีการมอบหมายและสื่อสารให้ได้รับทราบกัน ซึ่งผู้บริหารระดับสูงต้องมอบหมายหน้าที่ความรับผิดชอบและอำนาจหน้าที่ เพื่อวัตถุประสงค์ ดังนี้ ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศมีความสอดคล้องกับข้อกำหนดของเอกสารมาตรฐาน ISO/IEC 27001:2022 มีการรายงานประสิทธิภาพและประสิทธิผลของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศต่อผู้บริหารระดับสูง

3. การวางแผน (Planning) ด้านการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

3.1 การดำเนินการเพื่อจัดการกับความเสี่ยงและโอกาสเกิด (Actions to Address Risks and Opportunities)

3.1.1 การดำเนินการในภาพรวม

บริษัทฯ ต้องพิจารณาความเสี่ยงและโอกาสในการเกิดความเสี่ยงจากเหตุปัจจัยภายในและภายนอกองค์กรที่มีผลกระทบกับการดำเนินงาน รวมทั้งความต้องการและความคาดหวังของผู้ที่เกี่ยวข้องกับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ เพื่อวัตถุประสงค์ ดังต่อไปนี้

- ให้ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศบรรลุผลลัพธ์ตามที่ต้องการ
- ป้องกัน หรือ ลดผลที่ไม่พึงปรารถนา
- มีการปรับปรุงอย่างต่อเนื่อง โดยบริษัทฯ จะต้องจัดทำแผนที่สามารถจัดการกับความเสี่ยงและโอกาสในการเกิดความเสี่ยงได้ และการดำเนินงานตามแผนมีความสอดคล้องกับการดำเนินการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ และสามารถประเมินประสิทธิภาพและประสิทธิผลในการดำเนินการได้

3.2 การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Risk Assessment)

บริษัทฯ ต้องกำหนดและประยุกต์ ระเบียบปฏิบัติงานการประเมินความเสี่ยง (Risk Assessment) ในการบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ ควรมีหัวข้อดังต่อไปนี้

- กำหนด หรือ ปรับปรุงเกณฑ์ความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Risk Criteria) ซึ่งต้องรวมถึง เกณฑ์การยอมรับความเสี่ยง (Risk Acceptance Criteria) และ เกณฑ์สำหรับการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศให้สามารถนำไปใช้งานได้อย่างเหมาะสม

- ทำให้การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ และผลการประเมินที่ได้ต้องสอดคล้องถูกต้อง สามารถนำมาเปรียบเทียบและวิเคราะห์ผลได้
- ระบุความเสี่ยงที่มีผลกระทบกับ การสูญเสียความลับ ความถูกต้องสมบูรณ์ และความพร้อมใช้ของสารสนเทศภายในขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ และระบุผู้เป็นเจ้าของความเสี่ยง (Risk Owner) นั้น
- วิเคราะห์ความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Risk Analysis)
- ประเมินระดับโอกาสในการเกิดความเสี่ยงนั้น (Likelihood)
- ประเมินระดับผลกระทบเมื่อความเสี่ยงนั้นเกิดขึ้น (Impact)
- กำหนดระดับของความเสี่ยง (Risk Level) จากความสัมพันธ์ของระดับโอกาสในการเกิดความเสี่ยง กับ ผลกระทบเมื่อความเสี่ยงนั้นเกิดขึ้น
- ประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Risk Evaluation)
- เปรียบเทียบผลที่ได้การวิเคราะห์ความเสี่ยงกับเกณฑ์ที่กำหนดไว้
- จัดลำดับความเสี่ยงที่ต้องนำไปบรรเทาความเสี่ยงต่อไป (Prioritize)
- บริษัทฯ จะต้องจัดเก็บผลการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Risk Assessment Report) อย่างเป็นลายลักษณ์อักษร

3.3 การบรรเทาความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Risk Treatment)

บริษัทฯ ต้องกำหนดให้มีการบรรเทาความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศที่เกินเกณฑ์ยอมรับความเสี่ยงโดยมีแนวทางดำเนินการดังต่อไปนี้

- กำหนดทางเลือกที่เหมาะสมในการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Risk Optionโดยต้องนำผลการประเมินความเสี่ยงมาพิจารณาด้วย
- กำหนดมาตรการทั้งหมดที่จำเป็นเพื่อดำเนินการตามทางเลือกที่กำหนดไว้
- เปรียบเทียบมาตรการที่กำหนดไว้ข้างต้น กับมาตรการใน Annex A ของมาตรฐาน ISO/IEC 27001:2022 หรือมาตรการอื่นตามความเหมาะสม และตรวจสอบว่าไม่มีมาตรการข้อใดที่ละเลยไป
- จัดทำเอกสารแสดงการประยุกต์ใช้มาตรการ (Statement of Applicability: SoA) ซึ่งประกอบด้วย มาตรการที่จำเป็น
- คำอธิบายเหตุผลของการใช้มาตรการไม่ว่า มาตรการเหล่านั้นจะได้รับการปฏิบัติแล้วหรือไม่ก็ตาม และคำอธิบายเหตุผลของการไม่ใช้มาตรการจาก Annex A ของมาตรฐาน ISO/IEC 27001:2022 หรือมาตรการอื่นตามความเหมาะสม
- จัดทำแผนการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ และขอการรับรองจากผู้

เป็นเจ้าของความเสี่ยง (Risk Owner) สำหรับแผนการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ และการยอมรับสำหรับความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศที่ยังเหลืออยู่

- บริษัทฯ จะต้องจัดเก็บแผนการบรรเทาความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ อย่างเป็นลายลักษณ์อักษร
- บริษัทฯ มีการจัดทำระเบียบปฏิบัติ เกี่ยวกับการชี้บ่ง การประเมิน และการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศตามขอบเขตที่ได้กำหนดไว้ โดยจะดำเนินการประเมินความเสี่ยงตามความถี่ที่กำหนดไว้

3.4 วัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศและแผนการบรรลุวัตถุประสงค์ (Information Security Objectives and Plans to Achieve Them)

บริษัทฯ ต้องกำหนดวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศสำหรับการปฏิบัติงานในแต่ละระดับงานที่เกี่ยวข้อง โดยมีวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ ดังนี้

- สอดคล้องกับนโยบายความมั่นคงปลอดภัยสารสนเทศ
- สามารถวัดได้ (ถ้าสามารถปฏิบัติได้)
- นำความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ ผลการประเมินและการจัดการความเสี่ยงที่เกี่ยวข้องมาพิจารณาด้วย
- มีการสื่อสารให้ผู้ที่เกี่ยวข้องได้รับทราบ และ มีการปรับปรุงตามความเหมาะสม

บริษัทฯ จะต้องจัดเก็บวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ ไว้เป็นลายลักษณ์อักษรเมื่อบริษัทฯ ทำการวางแผนงานจะต้องระบุหัวข้อ ดังต่อไปนี้

- สิ่งที่เกี่ยวข้องที่ต้องดำเนินการ
- ทรัพยากรที่จำเป็นต้องใช้
- ผู้รับผิดชอบในแต่ละการดำเนินการ
- ระบุระยะเวลาดำเนินการเสร็จ
- วิธีประเมินผลการปฏิบัติการ

3.5 การดำเนินการด้านเอกสาร (Documentation Requirement)

จัดทำเอกสารที่ประกอบแสดงให้เห็นถึงการดำเนินการบริหารจัดการระบบ ISMS โดยครอบคลุมอย่างน้อยดังนี้

- เอกสารนโยบายการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Policy)
- ขอบเขตการบริหารจัดการความมั่นคงปลอดภัยของระบบ ISMS
- ขั้นตอนปฏิบัติหรือมาตรการที่สนับสนุนระบบ ISMS

- เอกสารอธิบายรายละเอียดวิธีการประเมินความเสี่ยง
- เอกสารแผนการลดความเสี่ยง
- ขั้นตอนปฏิบัติที่ยืนยัน แผนวัดประสิทธิผล การจัดการและมาตรการของ ISMS กระบวนการและอธิบายวิธีการคำนวณการวัดประสิทธิผล
- บันทึกผลจากการปฏิบัติตามมาตรฐาน
- เอกสาร Statement of Applicability

3.6 การบริหารจัดการควบคุมเอกสารและบันทึก (Control of Document and Record)

ด้านการควบคุมเอกสารและข้อมูลของระบบ DCO จะเป็นผู้ดำเนินการบริหารจัดการและควบคุมด้านการควบคุมเอกสารและข้อมูล ตลอดจนบันทึกผลการปฏิบัติงานที่เกี่ยวข้องกับระบบ ISMS โดยจะปฏิบัติตามระเบียบปฏิบัติงานเรื่องการควบคุมเอกสารและข้อมูล และ ระเบียบปฏิบัติงานเรื่องการควบคุมบันทึก ตามลำดับ ตัวแทนฝ่ายบริหารเป็นผู้รับผิดชอบ ในการดูแลปรับปรุงหรือเปลี่ยนแปลงระเบียบดังกล่าว เพื่อให้ระบบ ISMS มีการดำเนินการตามมาตรฐานของบริษัทฯ ด้านการควบคุมเอกสารระบบ ISMS ให้มีคุณภาพต่อไป

3.7 หน้าที่ความรับผิดชอบของผู้บริหาร (Management Responsibility)

3.7.1 แนวทางการบริหารจัดการของผู้บริหาร

ผู้บริหารจะต้องให้ความสำคัญต่อการกำหนด การลงมือปฏิบัติ การดำเนินการ การเฝ้าระวัง การทบทวน การบำรุงรักษา และการปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยโดยดำเนินการดังต่อไปนี้

- กำหนดนโยบายการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Policy) ที่มีความมั่นคงปลอดภัยสอดคล้องกับทิศทางเชิงกลยุทธ์ของบริษัทฯ
- กำหนดวัตถุประสงค์และแผนงานสำหรับระบบ ISMS
- กำหนดบทบาทและหน้าที่ความรับผิดชอบทางด้านความมั่นคงปลอดภัย
- ต้องสื่อสาร และแจ้งให้ผู้ที่เกี่ยวข้องทั้งภายในและภายนอกบริษัทฯ ทราบถึงความสำคัญของการรักษาความมั่นคงปลอดภัย ความสำคัญของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศที่มีประสิทธิภาพประสิทธิผลตามความต้องการของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศที่กำหนดไว้ และการปฏิบัติตามนโยบายความมั่นคงปลอดภัยสารสนเทศ (IT Security Policy) รวมถึงกฎหมายต่าง ๆ ที่เกี่ยวข้อง เพื่อปรับปรุงหรือยกระดับการรักษาความมั่นคงปลอดภัยของบริษัทฯ
- จัดสรรทรัพยากรอย่างเพียงพอสำหรับการดำเนินการต่าง ๆ เช่นการกำหนด การลงมือปฏิบัติการดำเนินการ การเฝ้าระวัง การทบทวน การบำรุงรักษา และการปรับปรุงระบบ ISMS
- ต้องรายงานประสิทธิภาพในการดำเนินการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศที่

สำคัญให้ผู้บริหารระดับสูงสุด ได้รับทราบ

- กำหนดเกณฑ์การยอมรับความเสี่ยง และระดับความเสี่ยงที่ยอมรับได้ตามนโยบายการบริหารจัดการความเสี่ยง ในนโยบายความมั่นคงปลอดภัยสารสนเทศ (IT Security Policy)
- จัดให้มีการตรวจสอบประเมินระบบ ISMS ตามนโยบายการตรวจสอบและทบทวนระบบ ISMS ในนโยบายฉบับนี้
- ดำเนินการทบทวนระบบ ISMS ตามรอบระยะเวลาที่กำหนด
- ต้องทำให้ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศบรรลุประสิทธิภาพประสิทธิผลตามที่ต้องการ และต้องส่งเสริมให้ระบบมีการปรับปรุงอย่างต่อเนื่อง
- ต้องรวบรวมความต้องการของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ให้ดำเนินการเข้ากับกระบวนการขององค์กร
- ต้องสนับสนุนบทบาทการบริหารอื่น ๆ ภายใต้ขอบเขตความรับผิดชอบเพื่อแสดงภาวะผู้นำของตนเอง

3.8 การบริหารจัดการทรัพยากร

3.8.1 ด้านทรัพยากร ผู้บริหารจะต้องจัดสรรทรัพยากรด้านต่าง ๆ เท่าที่จำเป็น ดังต่อไปนี้

- กำหนด ลงมือปฏิบัติ ดำเนินการ เฝ้าระวัง ทบทวน บำรุงรักษา และปรับปรุงระบบ ISMS
- ให้ดำเนินการตามมาตรการหรือขั้นตอนปฏิบัติด้านความมั่นคงปลอดภัย
- ระบุข้อกฎหมายหรือระเบียบปฏิบัติที่เกี่ยวข้องที่องค์กรให้ความสำคัญในการจัดสรรทรัพยากรให้
- บำรุงรักษาความมั่นคงปลอดภัยอย่างพอเพียงโดยการเลือกใช้มาตรการทางด้านความมั่นคงปลอดภัยที่ถูกต้องและเหมาะสม
- ดำเนินการทบทวนกระบวนการและเอกสาร ตามความจำเป็น รวมถึงมีการดำเนินการเพิ่มเติมอย่างเหมาะสมต่อผลของการทบทวนนั้น ๆ
- ปรับปรุงความสัมฤทธิผลของระบบ ISMS

3.8.2 ด้านการอบรม การสร้างความตระหนักและการให้มีความรู้ความสามารถ

บริษัทฯ จะต้องดำเนินการเพื่อให้บุคลากรทั้งหมดมีความรู้ความสามารถตามหน้าที่ความรับผิดชอบระบบ ISMS โดยการครอบคลุมการดำเนินการ ดังนี้

- กำหนดความรู้ความสามารถที่จำเป็น สำหรับพนักงานตามหน้าที่ความรับผิดชอบและให้สอดคล้องกับการปฏิบัติตามระบบ ISMS (เช่น การอบรมการประเมินความเสี่ยง, การอบรมนโยบายและขั้นตอนปฏิบัติที่เกี่ยวข้องในระบบ ISMS เป็นต้น)

- จัดอบรมหรือใช้วิธีการให้ความรู้อื่น เพื่อเป็นการเสริมความรู้ของพนักงานตามความต้องการ
- ประเมินความสัมฤทธิผลของการเข้ารับการอบรม เช่น การกรอกแบบทดสอบ, การทดสอบก่อนอบรมหรือหลังการอบรม, การสอบตามการอบรม เป็นต้น
- เก็บรักษาบันทึกข้อมูลที่เกี่ยวข้องกับประวัติการศึกษา การฝึกอบรม ทักษะ ประสบการณ์และคุณสมบัติของพนักงาน โดยเน้นดำเนินการสร้างความตระหนักด้านความมั่นคงปลอดภัยที่อาจมีผลต่อการรักษาความมั่นคงปลอดภัยของบริษัทฯ

3.9 การสื่อสารให้ทราบ (Communication)

บริษัทฯ จะต้องกำหนดให้มีการสื่อสารข้อมูลที่จำเป็นตามระเบียบปฏิบัติงานการสื่อสารการดำเนินงาน (Operational Communication) เพื่อให้ผู้ที่เกี่ยวข้องทั้งภายในและภายนอกบริษัทฯ ที่เกี่ยวข้องกับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศรับทราบ โดยคำนึงถึงองค์ประกอบในการสื่อสาร ดังต่อไปนี้

- เรื่องที่ต้องการสื่อสาร
- เมื่อไรที่จะดำเนินสื่อสาร
- สื่อสารถึงผู้ที่เกี่ยวข้องท่านใด
- ผู้ที่รับหน้าที่ที่จะต้องไปสื่อสาร และใช้กระบวนการในการสื่อสารให้เกิดผล

3.10 การวางแผนการเปลี่ยนแปลงของระบบบริหารจัดการความมั่นคงปลอดภัย (Planning of changes)

ตารางการควบคุมการวางแผนการเปลี่ยนแปลงที่ส่งผลกระทบต่อระบบการบริหารจัดการ ISMS Planning of Change table

Type of ISMS Major Change	ISMS Major Change Planning process	ISMS Change Result
การเปลี่ยนแปลงเอกสารสำคัญ ISMS Document: Policies/Procedures/ Standard.	การวางแผนต้องมีการรายงานผู้บริหารและจัดให้มีการประชุมเพื่อรายงานก่อนการเปลี่ยนแปลงมากกว่า 7 วัน ก่อนการประกาศใช้	Management Review Presentation
การเปลี่ยนแปลงกระบวนการและขอบเขตของ ISMS Scope: Processes needed and interactions.	การวางแผนต้องมีการรายงานผู้บริหารและจัดให้มีการประชุมเพื่อรายงานก่อนการเปลี่ยนแปลงมากกว่า 60 วัน ก่อนการประกาศใช้	Management Review Presentation
การเปลี่ยนแปลงขอบเขตพื้นที่ให้บริการ ISMS Scope Location.	การวางแผนต้องมีการรายงานผู้บริหารและจัดให้มีการประชุมเพื่อรายงานก่อนการเปลี่ยนแปลงมากกว่า 60 วัน ก่อนการประกาศใช้	Management Review Presentation

Type of ISMS Major Change	ISMS Major Change Planning process	ISMS Change Result
การเปลี่ยนแปลงของบริบทองค์กรในขอบเขต ISMS Context of the Organization.	การวางแผนต้องมีการรายงานผู้บริหารและจัดให้มีการประชุมเพื่อรายงานก่อนการเปลี่ยนแปลงมากกว่า 30 วัน ก่อนการประกาศใช้	Management Review Presentation
การเปลี่ยนแปลงของกรอบการดำเนินงาน ISMS Framework.	การวางแผนต้องมีการรายงานผู้บริหารและจัดให้มีการประชุมเพื่อรายงานก่อนการเปลี่ยนแปลงมากกว่า 30 วัน ก่อนการประกาศใช้	Management Review Presentation
การเปลี่ยนแปลงคณะบริหาร คณะทำงาน หรือหัวหน้าทีม Committee, ISMR, Core Team member.	การวางแผนต้องมีการรายงานผู้บริหารและจัดให้มีการประชุมเพื่อรายงานก่อนการเปลี่ยนแปลงมากกว่า 30 วัน ก่อนการประกาศใช้	Management Review Presentation
การเปลี่ยนแปลงของวิธีการประเมินความเสี่ยง ISMS Risk Management Methodology.	การวางแผนต้องมีการรายงานผู้บริหารและจัดให้มีการประชุมเพื่อรายงานก่อนการเปลี่ยนแปลงมากกว่า 30 วัน ก่อนการประกาศใช้	Management Review Presentation
การเปลี่ยนแปลงวิธีการจัดการด้านเอกสาร ISMS Document Control process.	การวางแผนต้องมีการรายงานผู้บริหารและจัดให้มีการประชุมเพื่อรายงานก่อนการเปลี่ยนแปลงมากกว่า 7 วัน ก่อนการประกาศใช้	Management Review Presentation

4. การตรวจสอบและทบทวนระบบ ISMS (Monitoring and Review the ISMS)

4.1 การตรวจประเมินระบบ ISMS (Internal ISMS Audit)

- จัดทำมาตรการการตรวจประเมินระบบ ISMS ตาม ระเบียบปฏิบัติงานการตรวจประเมินระบบสารสนเทศ (Information System Audit Consideration) ในนโยบายความมั่นคงปลอดภัยสารสนเทศ (IT Security Policy) รวมถึงการตรวจสอดคล้องตามนโยบายความมั่นคงปลอดภัยสารสนเทศ (IT Security Policy) และเอกสารที่เกี่ยวข้องกับระบบ ISMS ทั้งหมด
- จัดให้มีการทำการตรวจประเมินระบบความมั่นคงปลอดภัยสารสนเทศ ได้แก่ นโยบาย ขั้นตอนปฏิบัติ คู่มือ หรือเอกสารอื่นที่เกี่ยวข้อง โดยรวมถึงการตรวจสอดคล้องทางด้านเทคนิค (Technical Compliance Checking) ตามขอบเขตที่ชัดเจน อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ
- กำหนดเกณฑ์ในการตรวจสอบ ขอบเขต ความถี่ และวิธีการที่ใช้ในการตรวจสอบ
- วางแผนการตรวจสอบโดยพิจารณาถึงสถานภาพและความสำคัญของกระบวนการและองค์ประกอบต่าง ๆ ที่จะได้รับการตรวจสอบ รวมทั้งติดตามผลการตรวจสอบจากครั้งต่าง ๆ ที่ผ่านมา
- การคัดเลือกผู้ตรวจสอบและดำเนินการตรวจสอบจะต้องคำนึงถึงการตรวจสอบตามหลักฐานความเป็นจริง และความเที่ยงธรรมของผู้ตรวจสอบ รวมทั้งผู้ตรวจสอบจะต้องไม่ตรวจสอบงานของตนเอง ข้อบกพร่องที่พบ จะได้รับการวิเคราะห์หาสาเหตุ และกำหนดแนวทางการแก้ไขที่เหมาะสม เพื่อป้องกันไม่ให้เกิดปัญหาซ้ำในอนาคต รวมถึงติดตามการแก้ไขข้อบกพร่อง
- ต้องระบุหน้าที่ความรับผิดชอบและข้อกำหนดต่าง ๆ ในตามแผนที่ระบุไว้และดำเนินการตรวจสอบ รวมทั้งการจัดทำรายงานผลการประเมินระบบ ISMS (ISMS Audit Report) และจัดเก็บบันทึกผลการตรวจสอบ พร้อมทั้งระบุจัดเก็บตามลำดับชั้นความลับที่เหมาะสม สอดคล้องตามนโยบายการจัดระดับชั้นและจัดการข้อมูลสารสนเทศ (Information Classification Labeling and Handling) ในนโยบายความมั่นคงปลอดภัยสารสนเทศ (IT Security Policy)
- ผู้บริหารจะต้องควบคุมให้มีการดำเนินการเพื่อแก้ไขความไม่สอดคล้องและสาเหตุที่เกี่ยวข้องอย่างเหมาะสม รวมทั้งจะต้องควบคุมให้มีการติดตามเพื่อตรวจสอบการดำเนินการเหล่านั้นให้สำเร็จลุล่วง

4.2 การทบทวนและจัดการระบบ ISMS (Management Review of the ISMS)

- ผู้บริหารแสดงความมุ่งมั่นและให้การสนับสนุนระบบ ISMS โดยการทบทวนการบริหารจัดการเพื่อให้มีความเหมาะสม ความเพียงพอ และความสัมฤทธิ์ผลการทบทวนของผู้บริหารควรครอบคลุมวาระการประชุมผู้บริหารอย่างน้อยด้านต่าง ๆ ดังต่อไปนี้
    - ทบทวนการนำเข้า (Review Input)
        - สถานะของการดำเนินการจากผลการทบทวนครั้งก่อน
        - การเปลี่ยนแปลงในประเด็นภายในและภายนอกองค์กรใด ๆ ที่อาจมีผลต่อระบบ

ISMS

- พิจารณาผล แนวโน้ม และเปรียบเทียบประสิทธิภาพและประสิทธิผลด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อปรับปรุง ในด้านต่าง ๆ ดังนี้
  - ความไม่สอดคล้องและการดำเนินการแก้ไข
  - ผลการเฝ้าระวังและวัดผล
  - ผลการตรวจประเมิน
  - ความสำเร็จตามวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ
- ข้อเสนอแนะกลุ่มที่มีความสนใจเป็นพิเศษ (Interested Parties)
- ผลการประเมินความเสี่ยงและสถานะของแผนลดความเสี่ยง
- โอกาสสำหรับการปรับปรุงอย่างต่อเนื่อง หรือคำแนะนำหรือข้อเสนอในการปรับปรุงต่าง ๆ หรืออาจรวมถึงหัวข้อในประเด็น ดังนี้
  - ทบทวนผลการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย
  - ความรู้ด้านเทคนิค, ระบบ หรือระเบียบปฏิบัติที่สามารถนำมาใช้ปรับปรุงระบบ ISMS ให้มีประสิทธิผล
  - ติดตามสถานะของการดำเนินการเชิงป้องกันหรือการดำเนินการเชิงแก้ไข
  - จุดอ่อนหรือภัยคุกคามที่ยังไม่ได้รับการกล่าวถึงในรายงานการประเมินความเสี่ยงครั้งที่ผ่านมา
  - ผลของการวัดความสัมฤทธิผล (Effectiveness Measurement) ของระบบ ISMS
  - ผลการติดตามการทบทวนครั้งก่อน
  - ผลการทบทวนของผู้บริหารจะต้องรวมถึงการตัดสินใจเกี่ยวกับโอกาสในการปรับปรุงอย่างต่อเนื่องและความจำเป็นสำหรับการเปลี่ยนแปลงต่อระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

- ทบทวนผล (Review Output) รวมถึงการตัดสินใจและการดำเนินการต่าง ๆ ดังนี้
  - ทบทวนผล (Review Output) รวมถึงการตัดสินใจและการดำเนินการต่าง ๆ ดังนี้
  - การปรับปรุงความสัมฤทธิผลของระบบบริหารจัดการความมั่นคงปลอดภัย
  - การปรับปรุงวิธีการวัดความสัมฤทธิผล (Effectiveness Measurement) ของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
  - การปรับปรุงผลการประเมินความเสี่ยงและแผนการลดความเสี่ยง
  - การปรับปรุงขั้นตอนปฏิบัติและมาตรการที่มีผลต่อความมั่นคงปลอดภัยสำหรับสารสนเทศ เช่น
    - ข้อกำหนดทางด้านความมั่นคงปลอดภัย

- ข้อกำหนดที่เกี่ยวข้องกับกฎ ระเบียบ หรือกฎหมาย
- ข้อกำหนดที่ระบุไว้ในสัญญา
- ระดับของความเสี่ยง และ/หรือ เกณฑ์สำหรับการยอมรับความเสี่ยงให้ครอบคลุมทุกประเด็นตามรอบระยะเวลาหรืออย่างน้อยปีละ 1 ครั้ง และจัดเก็บอย่างเป็นลายลักษณ์อักษรใน รายงานการประชุมของผู้บริหาร

- ผู้บริหารสนับสนุนทรัพยากรที่จำเป็นต่อการป้องกันทรัพย์สินสารสนเทศ ทั้งด้านบุคคลากร ผู้เชี่ยวชาญ (ทั้งภายในและภายนอก) ตลอดจนปัจจัยอื่น ๆ ตามความเหมาะสม
- ปรับปรุงประสิทธิผล (Effectiveness) ของระบบ ISMS ให้เป็นไปตามมาตรฐานที่กำหนดไว้

5. การปรับปรุงระบบ ISMS (ISMS improvement the ISMS)

5.1 การดำเนินการเชิงแก้ไข (Corrective Controls)

ต้องกำหนดการดำเนินการเชิงแก้ไข (Corrective Controls) ซึ่งเป็นการจัดการสาเหตุของความไม่สอดคล้องกับข้อกำหนดของระบบ ISMS ป้องกันการเกิดซ้ำปฏิบัติตามระเบียบปฏิบัติการแก้ไขและป้องกัน โดยพิจารณาถึงด้านต่าง ๆ ดังต่อไปนี้

- การระบุความไม่สอดคล้อง
- การระบุสาเหตุของความไม่สอดคล้อง
- การประเมินความจำเป็นในการดำเนินการเพื่อป้องกันไม่ให้ความไม่สอดคล้องนั้นเกิดขึ้นอีก
- การลงมือปฏิบัติการดำเนินการเชิงแก้ไขตามความจำเป็น
- การบันทึกข้อมูลผลการดำเนินการ
- การทบทวนการดำเนินการเชิงแก้ไขที่ได้ปฏิบัติไปแล้ว

5.2 การดำเนินการเชิงป้องกัน (Preventive Action)

ต้องกำหนดการดำเนินการเชิงป้องกัน (Preventive Action) ซึ่งเป็นการจัดการสาเหตุของความไม่สอดคล้องที่มีโอกาสเกิดขึ้นกับข้อกำหนดสำหรับระบบ ISMS เพื่อป้องกันไม่ให้เกิดขึ้นโดยปฏิบัติตามระเบียบปฏิบัติการแก้ไขและป้องกัน ใช้วิธีการประเมินความเสี่ยงและการดำเนินการเชิงป้องกันที่เหมาะสมกับผลกระทบของปัญหาที่มีโอกาสเกิดขึ้น โดยพิจารณาถึงด้านต่าง ๆ ดังนี้

- การระบุความไม่สอดคล้องที่มีโอกาสเกิดขึ้นและสาเหตุของความไม่สอดคล้อง
- การประเมินความจำเป็นในการดำเนินการเพื่อป้องกันการเกิดขึ้นของความไม่สอดคล้อง
- การลงมือปฏิบัติการดำเนินการเชิงป้องกันตามความจำเป็น
- การบันทึกข้อมูลผลการดำเนินการ
- การทบทวนการดำเนินการเชิงป้องกันที่ได้ปฏิบัติไปแล้ว

- ระบุความเสี่ยงที่เปลี่ยนไปและจัดระดับความสำคัญของการดำเนินการเชิงป้องกันโดยให้ความสำคัญกับความเสี่ยงที่มีระดับสูง เพื่อดำเนินการเชิงป้องกันกับเหตุการณ์นั้นก่อน

5.3 การปรับปรุงระบบ ISMS อย่างต่อเนื่อง (Continual Improvement for ISMS)

บริษัทฯ ต้องปรับปรุงระบบ ISMS อย่างต่อเนื่อง (Continual improvement for ISMS) เพื่อความสัมฤทธิผลของระบบ ISMS โดยใช้หัวข้อต่าง ๆ เหล่านี้เป็นเครื่องมือในการปรับปรุงให้ดียิ่งขึ้นในด้านต่าง ๆ ดังนี้

- นโยบายความมั่นคงปลอดภัยสารสนเทศ (IT Security Policy)
- วัตถุประสงค์ทางด้านความมั่นคงปลอดภัย
- ผลการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย
- ผลการวิเคราะห์เหตุการณ์ที่ได้รับการเฝ้าระวัง
- การดำเนินการเชิงป้องกันและแก้ไข
- การทบทวนระบบบริหารจัดการความมั่นคงปลอดภัยโดยผู้บริหาร

Document History

เลขที่การแก้ไข	**วันที่แก้ไข วัน-เดือน-ปี**	**เปลี่ยนแปลงโดย**	**ข้อสังเกต**
1.0	22-02-2567	กิติพงษ์ ภัทรพนาวัน	เวอร์ชั่นแรก

การอนุมัติ

ลายเซ็นด้านล่างแสดงถึงการอนุมัติเอกสารนี้เพื่อใช้ในพื้นที่ปฏิบัติงานของส่วนที่กำหนด

จัดทำโดย:	กิติพงษ์ ภัทรพนาวัน, ผู้จัดการ แผนกสนับสนุนโครงสร้างและระบบปฏิบัติการ	
ลายเซ็น: Kitiporg Pattanapanawan วันที่: 23/2/2567		

ตรวจสอบโดย:	วิชาติ อร่ามศรี, ผู้ช่วยผู้อำนวยการ แผนกสนับสนุนโครงสร้างและระบบปฏิบัติการ	
ลายเซ็น: วิชาติ อร่ามศรี วันที่: 23/2/2567		

อนุมัติโดย:	นพดล ตั้งเด่นชัย, ประธานเจ้าหน้าที่ แผนกเทคโนโลยีสารสนเทศ	
ลายเซ็น นพดล ตั้งเด่นชัย วันที่: 23/2/2567		